TTC技術レポート
Technical Report

TR-M2M-0024v4.3.0
3GPP とのインタワーク

3GPP Interworking

2023 年 3 月 17 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

Telecommunication Technology Committee

TR-M2M-0024v4.3.0

3GPP とのインタワーク ［ 3GPP Interworking ］

＜参考＞ [Remarks]

１．国際勧告等の関連 [Relationship with international recommendations and standards]

本技術レポートは、oneM2M で作成された Technical Report TR-0024-V4.3.0 に準拠している。

[This Technical Report is transposed based on the Technical Report TR-0024-V4.3.0 developed by oneM2M.]

２．作成専門委員会 [Working Group]

oneM2M 専門委員会 [oneM2M Working Group]

oneM2M
Technical Report

Document Number	TR-0024-V4.3.0
Document Name:	3GPP_Interworking
Date:	2020-Mar-06
Abstract:	The document is a study of interworking between oneM2M Architecture and 3GPP Rel-16 architecture for Service Capability Exposure as defined in TS 23.682.

Template Version: January 2020 (Dot not modify)

This Specification is provided for future development work within oneM2M only. The Partners accept no liability for any use of this Specification.

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

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

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

1 Scope

The present document is a study of interworking between oneM2M Architecture and 3GPP Rel-16 architecture for Service Capability Exposure as defined in the release 15 version of 3GPP TS 23.682 [i.5]. The key objective and value is analyzed and described. The document also investigates the potential solution in oneM2M by evaluating the existing technical solutions.

2 References

2.1 Normative references

As informative publications shall not contain normative references this clause shall remain empty.

Not applicable.

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.

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] oneM2M TS-0002: "Requirements".

[i.3] 3GPP TS 22.101: "Service aspects; Service principles (Release 13)".

[i.4] 3GPP TS 22.115: "Service aspects; Charging and billing (Release 13)".

[i.5] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications (Release 16)".

[i.6] OMA API Inventory.

NOTE: Available at http://technical.openmobilealliance.org/Technical/technical-information/oma-api-program.

[i.7] OMA Service Exposure Framework.

NOTE: Available at http://member.openmobilealliance.org/ftp/Public_documents/ARCH/ServiceExposure.

[i.8] OMA Exposing Network Capabilities to M2M.

NOTE: Available at http://member.openmobilealliance.org/ftp/Public_documents/ARCH/ENCap-M2M.

[i.9] oneM2M TS-0001: "Functional Architecture ".

[i.10] 3GPP TS 29.336: "Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications (Release 13)".

[i.11] 3GPP TS 23.203: "Policy and charging control architecture (Release 13)".

[i.12] 3GPP TS 22.368: "Service requirements for Machine-Type Communications (MTC); Stage 1".

[i.13] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[i.14]	3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2".
[i.15]	3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".
[i.16]	3GPP TS 29.214: Technical Specification Group Core Network and Terminals;Policy and Charging Control over Rx reference point(Release 15)
[i.17]	3GPP TS 29.212: Technical Specification Group Core Network and Terminals;Policy and Charging Control (PCC); Reference points (Release 15)
[i.18]	3GPP TS 29.122: T8 reference point for Northbound APIs (Release 15)
[i.19]	3GPP TS 29.522: 5G System; Network Exposure Function Northbound APIs (Release 15).
[i.20]	oneM2M TS-0026: 3GPP Interworking.
[i.21]	oneM2M TR-0026: Vehicular Domain Enablement.

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Definitions and abbreviations extracted from ETSI deliverables can be useful to draft your own and can be consulted via the ***Terms and Definitions Interactive Database (TEDDI) (****http://webapp.etsi.org/Teddi/****).***

3.1 Definitions

Clause numbering depends on applicability.

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

Definition format

<defined term>: <definition>

Text used to clarify abstract rules by applying them literally. See example:

MM1 reference point: reference point between MMS Relay/Server and MMS User Agent

NOTE 1: <Explanation >.

EXAMPLE: < Clarifications >.

NOTE 2: <2nd explanation about the same definition.>

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

<symbol> <Explanation>

3.3 Abbreviations

Clause numbering depends on applicability.

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

Abbreviation format

<ACRONYM> <Explanation>

4 Conventions

The keywords "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 Introduction to 3GPP Service Capability Exposure

5.1 oneM2M Underlying Network related requirements

Following requirements are defined in oneM2M TS-0002 [i.2], but not implemented or partially implemented in release 1.

Most of these requirements except OSR-052 can be achieved through the 3GPP features addressed in the subsequent sections, with and without support by OMA API.

OSR-006: The oneM2M System shall be able to reuse the services offered by Underlying Networks to M2M Applications and/or M2M Services by means of open access models (e.g. OMA, GSMA OneAPI framework). Examples of available services are:

- IP Multimedia communications.
- Messaging.
- Location.
- Charging and billing services, including sponsoring data flows.
- Device information and profiles, including configuring expected communication patterns.
- Configuration and management of devices.
- Triggering, monitoring of devices.
- Small data transmission.
- Group management and group messaging.
- Configuring QoS.
- Receiving Reports about the condition of the underlying network.
- Partially implemented in Rel-1 (see note 1).

NOTE 1: Rel-1 covers: Location, Charging and billing services, Configuration and management of devices, Device information and profiles, Triggering.

OSR-045a: The oneM2M System shall be able to receive and utilize information provided by the Underlying Network about when an M2M Device can be reached.

- Not implemented in Rel-1.

OSR-051: Depending on availability of suitable interfaces provided by the Underlying Network the oneM2M System shall be able to request the Underlying Network to broadcast / multicast data to a group of M2M Devices in a specified area.

- Implemented in Rel-1 -> Not implemented in Rel-1. ??

OSR-052: The oneM2M System shall be able to select an appropriate Underlying Network to broadcast or multicast data depending on the network's broadcast/multicast support and the connectivity supported by the targeted group of M2M Devices/Gateways.

- Not implemented in Rel-1.

OPR-004: When suitable interfaces are provided by the Underlying Network, the oneM2M System shall have the ability to schedule traffic via the Underlying Network based on instructions received from the Underlying Network.

- Not implemented in Rel-1.

OPR-005: The oneM2M System shall be able to exchange information with M2M Applications related to usage and traffic characteristics of M2M Devices or M2M Gateways by the M2M Application. This should include support for the 3GPP feature called: "Time controlled" (see note 2).

- Not implemented in Rel-1.

NOTE 2: "Time controlled" is equivalent to the MTC Features specified in clause 7.2 of 3GPP TS 22.368 [i.12].

OPR-006: Depending on availability of suitable interfaces provided by the Underlying Network the oneM2M System shall be able to provide information related to usage and traffic characteristics of M2M Devices or M2M Gateways to the Underlying Network.

- Not implemented in Rel-1.

5.2 3GPP Release 13 MTC features

In 3GPP Release 13, requirements for "Service exposure with 3rd party service providers" features are specified in clause 29 of 3GPP TS 22.101 [i.3] and the "Charged party selection" feature is defined in sub-clause 5.1.3 of 3GPP TS 22.115 [i.4].

3GPP Release 13 architecture supports these features and they can be used to implement the oneM2M requirements as described in the previous clause.

These 3GPP features are not only intended for M2M communication, but also for human usable applications such as smartphone applications.

3GPP intends to expose these additional features through the 3GPP Service Capability Exposure Function (SCEF) as described in the following clause.

5.3 3GPP architecture for Service Capability Exposure

The 3GPP architecture for the Service Capability Exposure Function (SCEF) is defined in 3GPP TS 23.682 [i.5]. The specification includes two different architectures. One is for the "MTC Device triggering" feature and was specified in 3GPP release 11. The other one is for 3GPP Service exposure with 3rd party service providers features newly provided in Release 15 which is the focus of the present document. Refer to the following figure 5.3-1, taken from the release 15 version of 3GPP TS 23.682 [i.5].

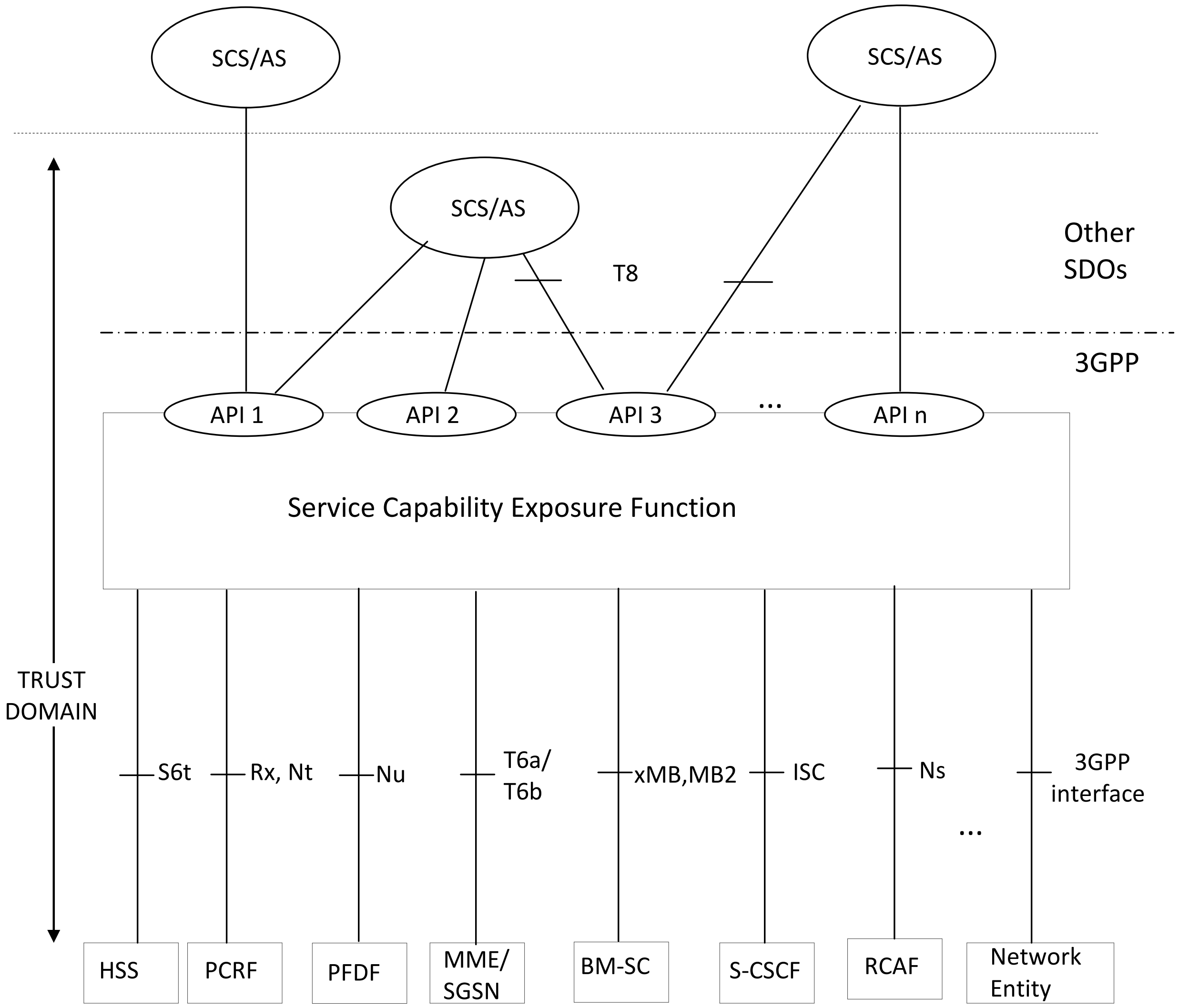


Figure 5.3-1: 3GPP Architecture for Service Capability Exposure

While 3GPP release 15 specifies the Service Capability Exposure Function (SCEF) as a 3GPP entity, residing in the trust domain of the 3GPP operator, 3GPP does not specify the APIs exposing these functions. Specification of these APIs is expected by external SDOs, e.g. OMA. As described in 3GPP TS 23.682 [i.5]. the SCEF covers services such as the ability to configure device communication patterns, configure the QoS of a data flow, sponsor a data flow, schedule data transfers, monitor a device's state, optimize a device's communication patterns for high latency applications, receive reports about the condition of the mobile core network, trigger devices, and send group messages via MBMS.

5.4 OMA API Program

5.4.1 Overview

The OMA API Program provides standardized interfaces to the service infrastructure residing within communication networks and on devices. Focused primarily between the service access layer and generic network capabilities, OMA API Program specifications allow operators and other service providers to expose device capabilities and network resources in an open and programmable way-to any developer community independent of the development platform. By deploying OMA APIs, fundamental capabilities such as SMS, MMS, Location Services, Payment and other core network assets are now exposed in a standardized way. Additional OMA APIs may be found in OMA API Inventory [i.6].

5.4.2 OMA work to be considered by oneM2M for 3GPP IWK

5.4.2.1 OMA Service Exposure Framework (Service Exposure)

OMA ARC WG is working to define the Service Exposure Framework specification [i.7] which covers non-functional capabilities that a network operator or a service provider should consider when it exposes the service capabilities through the Network APIs. Such non-functional capabilities implemented in the intermediation layer may include Authentication and Authorization, Infrastructural Policy, Business Policy, Assurance and Accounting.

OMA Service Exposure Framework can be considered as an OMA specified SCEF which can be used by oneM2M s platforms.

5.4.2.2 OMA Exposing Network Capabilities to M2M (ENCap-M)

Recently, OMA ARC WG is developing new APIs for exposing network capabilities to M2M applications and/or M2M service platforms.

The OMA work item "Exposing Network Capabilities to M2M" [i.8] lists requirements on standard APIs derived from use cases in which third parties, such as oneM2M or any other can leverage network capabilities to enrich the services or to streamline the operation. It also includes a gap analysis to identify any missing Network APIs to address above requirements and use cases. This enables utilization of the latest evolution in cellular networks, e.g. 3GPP.

6 Reference architecture

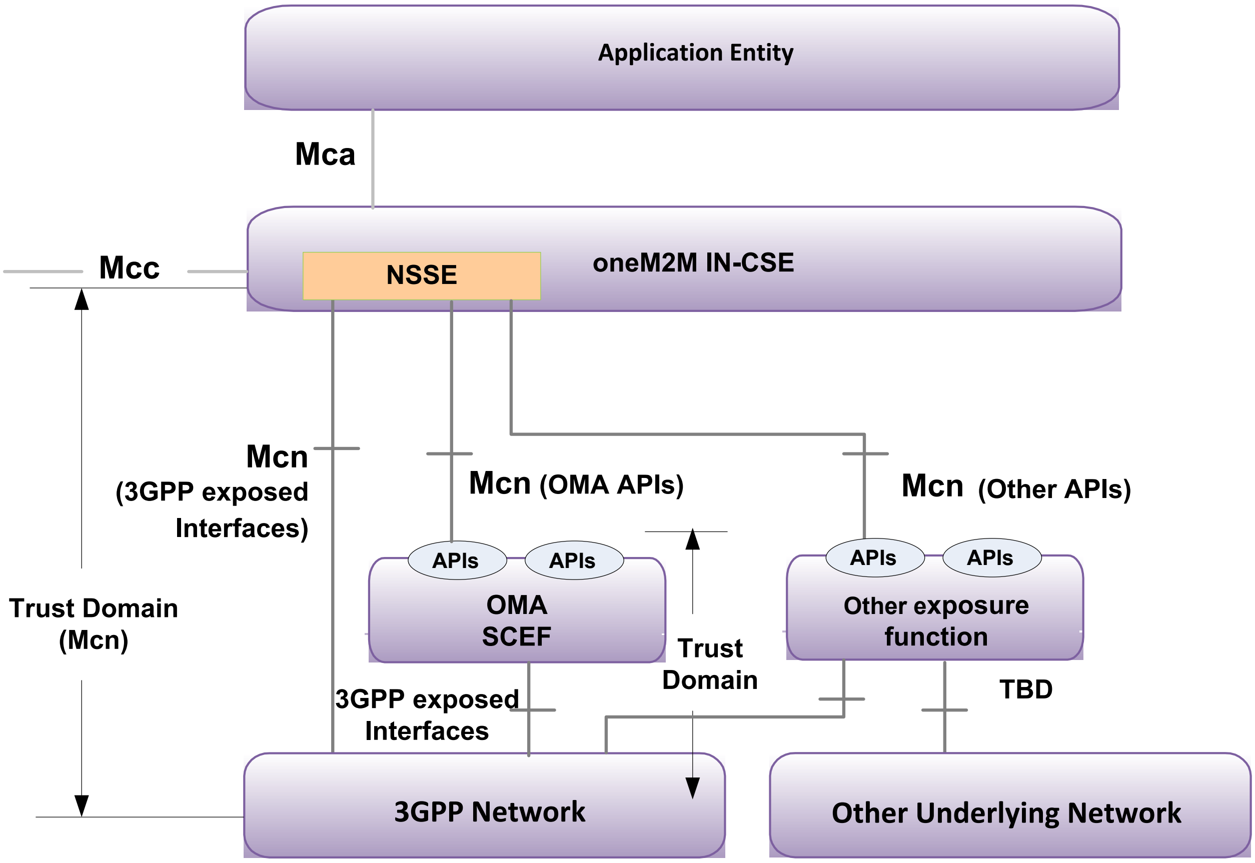


Figure 6-1: Interworking architecture

This architecture supports the following interworking modes:

- The NSSE invokes services of the underlying network directly via the reference points of the applicable nodes within the underlying network. This model is applicable to the case where the oneM2M service provider and the underlying network provider is the same or there is trust relation between both service providers if they are different.

- The NSSE exclusively invokes services of a 3GPP underlying network using OMA API.
- The NSSE invokes exclusively services of any underlying network using third party APIs.
- Any combination of the above, where some services are invoked using an API (OMA or third party depending on the underlying network) while other services are invoked directly with the underlying network using the applicable reference point.

The functionality supported by the NSSE is different depending on the interworking mode.

7 Potential impact for interworking with oneM2M

There are specific high level functions defined in 3GPP TS 23.682 [i.5], clause 4.5, such as device triggering, information storage, group message delivery, monitoring, high latency communications, network status reporting, background data transfer, communication patterns parameters provisioning, session QoS setting up, chargeable party changing.

According to the end-to-end oneM2M functional architecture described in oneM2M TS-0001 [i.9], all Common Services Functions (CSFs) reside within CSE may support those functions defined by 3GPP TS 23.682 [i.9] and no architecture functional changing.

The Network Service Exposure, Service Execution and Triggering (NSSE) CSF manages communications with the 3GPP MTC Release-13 Underlying Networks. The NSSE CSF may be deployed as SCEF using 3GPP defined interfaces (e.g. Rx, Tsp, etc.) bound to Mcn reference point. The NSSE CSF may also use OMA APIs or other APIs bound to Mcn reference point.

The Communication Management and Delivery Handling (CMDH) CSF may support those functions such as device triggering, group message delivery, monitoring, high latency communications, network status reporting, background data transfer, communication patterns parameters provisioning, session QoS setting up, chargeable party changing.

The Data Management and Repository (DMR) CSF may support those functions such as information storage, monitoring.

The Device Management (DMG) CSF may support monitoring function.

The Group Management (GMG) CSF may support group message delivery function.

The Location (LOC) CSF may support those functions such as monitoring, network status reporting.

Special authentication and authorization mechanisms for 3GPP Underlying Network such as IMSI, ACL, profile managements, policy control may be supported by the Security (SEC) CSF.

The Service Charging and Accounting (SCA) CSF may support those functions such as monitoring, chargeable party changing.

For supporting those functions, oneM2M system may add new attributes in existing resource types and changing existing service flows or create new resource types and new service flows. For detail, please refer to section 8 potential solutions for interworking with oneM2M.

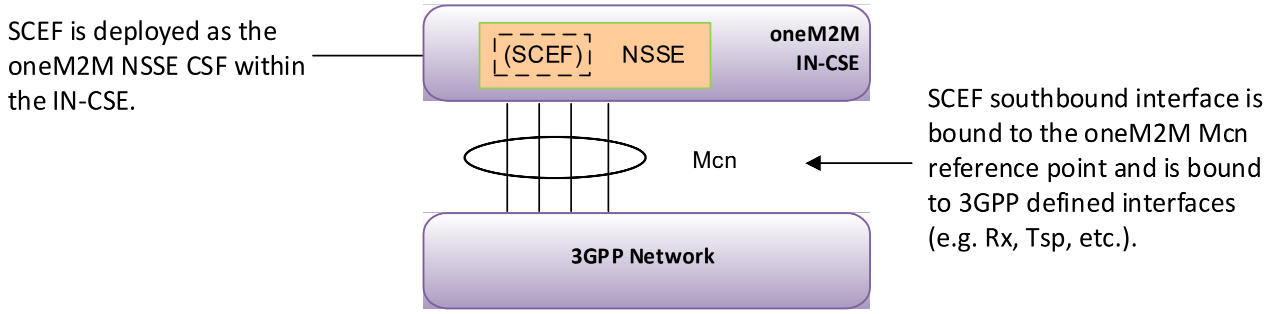
8 Potential solutions for interworking with oneM2M

8.1 Interworking Architecture with a 3GPP underlying network

8.1.1 Support through 3GPP Reference Points

Figure 8.1.1-1 depicts this architectural model.

In this case 3GPP services capabilities are exclusively invoked via the 3GPP reference points for the applicable 3GPP node.



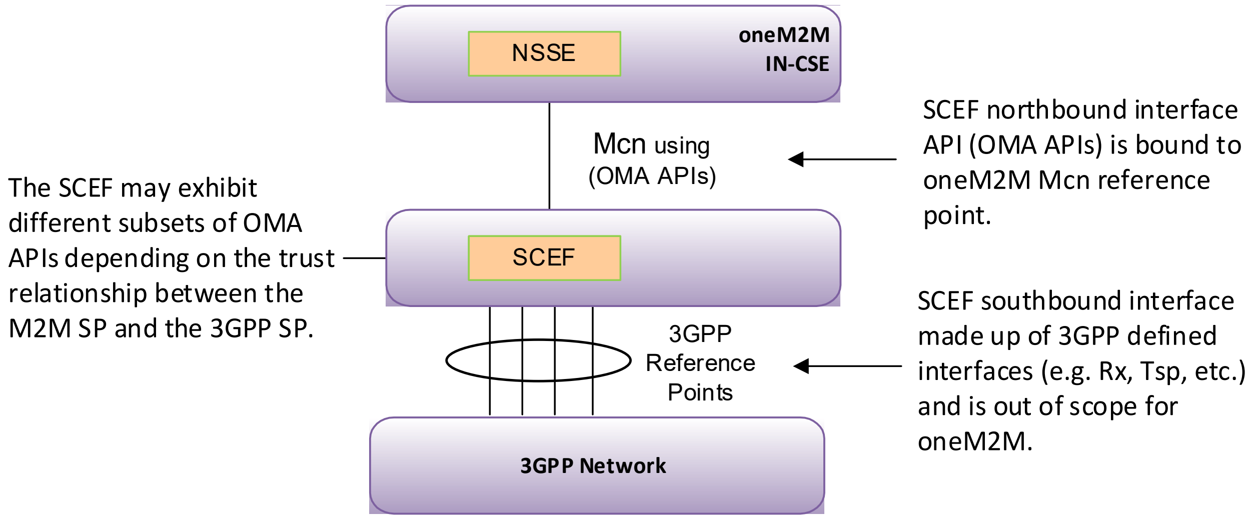
SCEF is deployed as the oneM2M NSSE CSF within the IN-CSE.

SCEF southbound interface is bound to the oneM2M Mcn reference point and is bound to 3GPP defined interfaces (e.g. Rx, Tsp, etc.).

Figure 8.1.1-1: oneM2M interworking with a 3GPP underlying network via 3GPP Reference Points

8.1.2 Support through SCEF API

Figure 8.1.2-1 depicts this architectural model. In this case 3GPP services capabilities are exclusively invoked via the SCEF API. Hence, the SCEF is fully implemented outside the oneM2M environment.



SCEF northbound interface API (OMA APIs) is bound to oneM2M Mcn reference point.

The SCEF may exhibit different subsets of OMA APIs depending on the trust relationship between the M2M SP and the 3GPP SP.

SCEF southbound interface made up of 3GPP defined interfaces (e.g. Rx, Tsp, etc.) and is out of scope for oneM2M.

Figure 8.1.2-1: oneM2M interworking with a 3GPP underlying network via SCEF API

8.1.3 Hybrid Mode

Figure 8.1.3-1 depicts this architectural model.

In this case 3GPP services capabilities are invoked on a per service basis which can include OMA or 3GPP SCEF API for some service, proprietary APIs for others, while some services can be invoked directly using the 3GPP reference points.

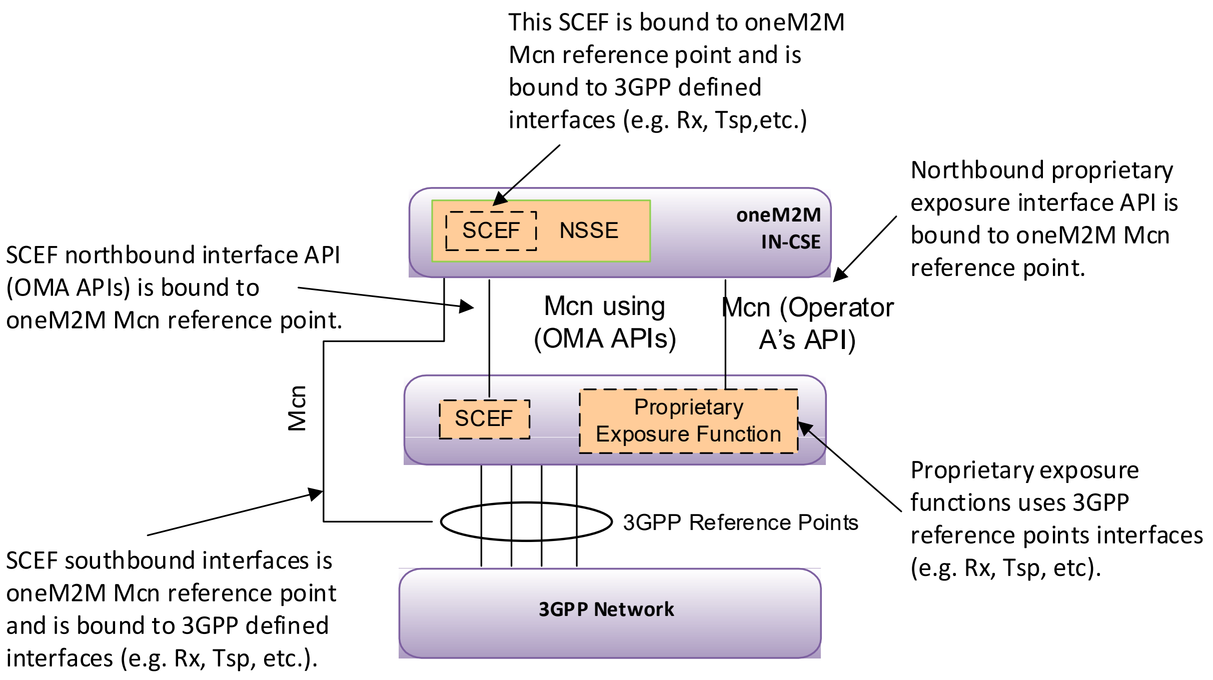

This SCEF is bound to oneM2M Mcn reference point and is bound to 3GPP defined interfaces (e.g. Rx, Tsp,etc.)
SCEF
NSSE
oneM2M
IN-CSE
Northbound proprietary exposure interface API is bound to oneM2M Mcn reference point.
SCEF northbound interface API (OMA APIs) is bound to oneM2M Mcn reference point.
Mcn using (OMA APIs)
Mcn (Operator A's API)
Mcn
SCEF
Proprietary Exposure Function
Proprietary exposure functions uses 3GPP reference points interfaces (e.g. Rx, Tsp, etc).
3GPP Reference Points
SCEF southbound interfaces is oneM2M Mcn reference point and is bound to 3GPP defined interfaces (e.g. Rx, Tsp, etc.).
3GPP Network

Figure 8.1.3-1: oneM2M interworking with a 3GPP underlying network in a hybrid mode

8.2 Configuration of Device Triggering Recall/Replace

8.2.1 Description

Device Triggering is the means by which a SCS sends information to the UE via the 3GPP network to trigger the UE to perform application specific actions that include initiating communication with the SCS for the indirect model or an AS in the network for the hybrid model. Device Triggering is required when an IP address for the UE is not available or reachable by the SCS/AS.

Device triggering recall/replace functionality allows a SCS to recall or replace previously submitted trigger messages which are not yet delivered to the UE.

8.2.2 Feature Gap Analysis

oneM2M uses the 3GPP Release-13 MTC feature for Device Trigger Recall/Replace to request to recall or replace previous Device Trigger message by using the oneM2M Device Tigger resource to provide the corresponding 3GPP information.

A signalling sequence for Device Trigger Recall/Replace is described in the clause 5.2.3 of 3GPP TS 23.682 [i.5]. Figure 8.2.2-1 provides the signalling sequence derived from the 3GPP specification with oneM2M terminologies mapping (3GPP TS 23.682 [i.5], figure 5.2.3.1-1).

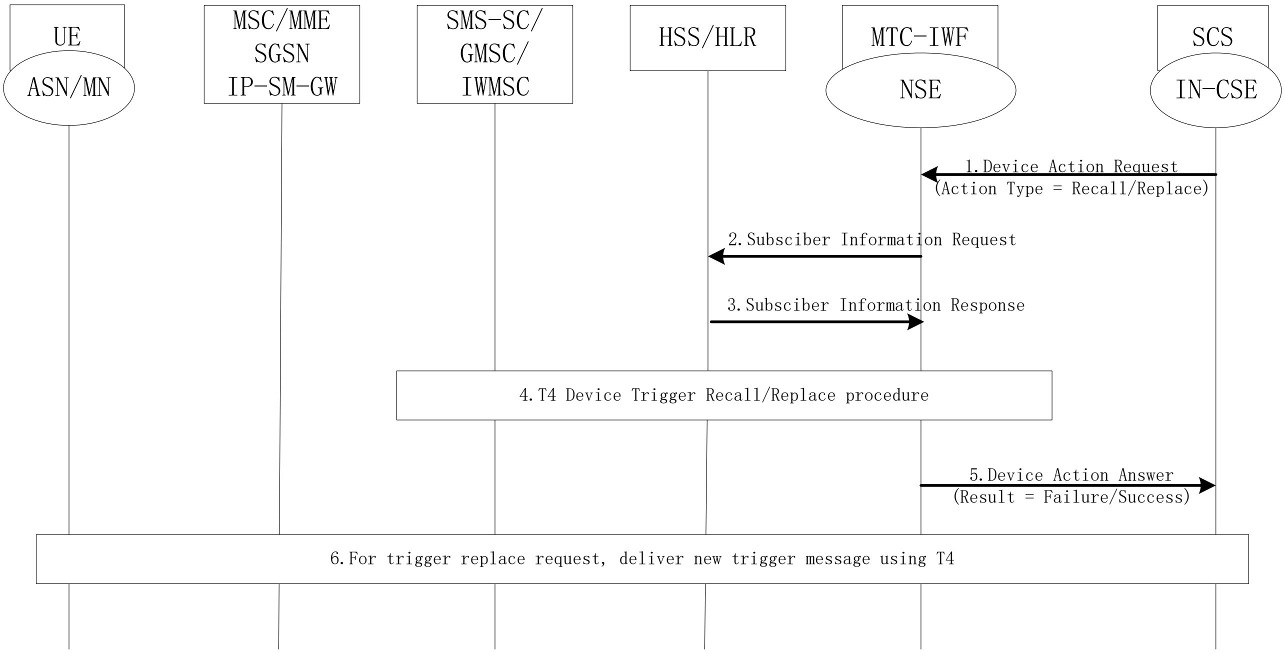

UE
ASN/MN
MSC/MME
SGSN
IP-SM-GW
SMS-SC/
GMSC/
IWMSC
HSS/HLR
MTC-IWF
NSE
SCS
IN-CSE
1.Device Action Request
(Action Type = Recall/Replace)
2.Subsciber Information Request
3.Subsciber Information Response
4.T4 Device Trigger Recall/Replace procedure
5.Device Action Answer
(Result = Failure/Success)
6.For trigger replace request, deliver new trigger message using T4

Figure 8.2.2-1: Device trigger recall/replace procedure over Tsp

1. The SCS determines it needs to recall/replace a trigger message that it has previously submitted. The SCS sends Device Action Request (External Identifier or MSISDN, SCS Identifier, old trigger reference number, new trigger reference number, validity period, priority, Application Port ID and trigger payload) message with action type set to "Trigger Recall Request" or "Trigger Replace Request". The SCS needs to include new trigger reference number, validity period, priority, Application Port ID and trigger payload for trigger replace request only. The old trigger reference number indicates the trigger reference number which was assigned to the previously submitted trigger message that the SCS wants to cancel. The new trigger reference number is assigned by the SCS to the newly submitted trigger message.

   If the SCS is not authorized to perform device triggering or the SCS has exceeded its quota or rate of trigger submission over Tsp, the MTC-IWF rejects the Device Action Request message with action type set to "Trigger Recall Request" or "Trigger Replace Request" by sending a Device Action Answer message with a cause value indicating the reason for the failure condition, and the flow stops at this step.

NOTE 1: The validity period in a trigger replace request needs to be greater than zero for the MTC-IWF to attempt its delivery.

2. The MTC-IWF sends a Subscriber Information Request (External Identifier or MSISDN and SCS Identifier) message to the HSS/HLR to determine if SCS is authorized to perform device triggering to the UE. This message is also to resolve the External Identifier or MSISDN to IMSI and retrieve the related HSS stored "Routing information" including the identities of the UE's serving CN node(s) which are needed for trigger replace request only.

NOTE 2: Optionally, mapping from External Identifiers to MSISDN is also provided for legacy SMS infrastructure not supporting MSISDN-less SMS.

3. The HSS/HLR sends the Subscriber Information Response (IMSI and/or MSISDN and related "Routing information" including the serving node(s) identities, cause) message. The IMSI and/or MSISDN and related "Routing information" including the serving node(s) identities in the Subscriber Information Response message is only needed for trigger replace request and not used by MTC-IWF for trigger recall request. HSS/HLR policy (possibly dependent on the VPLMN ID) may influence which serving node identities are returned. If the cause value indicates the SCS is not allowed to perform device triggering to this UE, or there is no valid subscription information, the MTC-IWF sends a Device Action Answer message with a cause value indicating the reason for the failure condition and the flow stops at this step. Otherwise this flow continues with step 4.

4. If trigger message which should be recalled or replaced was submitted to a SMS-SC as defined in clause 5.2.2 of 3GPP TS 23.682 [i.5], T4 device trigger replace procedure according to clause 5.2.3.2 of 3GPP TS 23.682 [i.5] or T4 device trigger recall procedure according to clause 5.2.3.3 of 3GPP TS 23.682 [i.5] is performed.

5. The MTC-IWF indicates trigger recall/replace success or failure in Device Action Answer message to the SCS. The MTC-IWF generates the necessary CDR information including the External Identifier or MSISDN and SCS Identifier.

   If recall/replace of a trigger is successful, this is reflected in the "Device Trigger Report" of the original trigger message (per step 7 in clause 5.2.1 of 3GPP TS 23.682 [i.5]) with delivery outcome "Recalled"/"Replaced".

NOTE 3: If recall/replace of a trigger failed because the trigger was already delivered or has expired, a "Device Trigger Report" of the original trigger will already have been created with the appropriate delivery outcome.

6. For trigger replace request, the new trigger message will be delivered to the UE immediately or when the UE is available following steps 4 - 9 as defined in clause 5.2.2 of 3GPP TS 23.682 [i.5].

A set of Device Trigger Recall/Replace parameters can be associated with a Device Trigger Recall/Replace request, as defined in table 8.2.2-1.

Table 8.2.2-1: Device Trigger Recall/Replace parameters

Parameter	Description
External Identifier or MSISDN	It is used to identify the corresponding External Identifiers in the delivery report. This can be also the MSISDN if used.
SCS Identifier	It is used to allow the SMS SC to send the trigger response back to the appropriate SCS.
old trigger reference number	This is to identify the previous device trigger request.
new trigger reference number	This is to identify the device trigger recall/replace request.
validity period	To indicate the time period for which the trigger request is valid.
priority	It is used to indicate the priority of trigger request.
SMS Application Port ID	It is used to route the short message to the triggering function in the UE.
trigger payload	The SMSC will store the Trigger payload until it receives the delivery confirmation.
NOTE 1: The Trigger Payload is stored as user data in SMS-SC. NOTE 2: Priority, Validity period and SMS Application Port ID are included in the Trigger payload.	

8.2.3 Key Issues and Requirements

8.2.3.1 Key SCEF NorthBound API Requirements

Number	Description	Notes
REQ-8.2-01	Device Triggering Request	
REQ-8.2-02	Device Trigger Recall/Replace Request	

8.2.3.2 Possible Impacts on the SCEF SouthBound Interface

N/A

8.2.3.3. Further 3GPP Requirements and Clarifications

N/A

8.2.3.4. oneM2M Key Issues

Provide support for Device Triggering Recall/Replace functionality.

Note: Solution 1 proposed in clause 8.2.4.1 implemented in Release 2.

8.2.4 Solution(s)

8.2.4.1 Solution1

8.2.4.1.1 Proposed resource types and attributes

This clause provides information of new resource types and new attributes including relationship with existing resource types and attributes.

The attribute *triggerReferenceNumber* is suggested to put under the <*remoteCSE*> resource in table 9.6.4-3 oneM2M TS-0001 [i.9].

Table 8.2.4.1.1-1: Attribute triggerReferenceNumber adds under <remoteCSE>

Attributes of <*remoteCSE*>	**Multiplicity**	**RW/ RO/ WO**	**Description**	**<*remoteCSEAnnc*> Attributes**
triggerReferenceNumber	0..1	RW	This is to identify device trigger request. This attribute is used only for device trigger and assigned by the IN-CSE.	NA

8.2.4.1.2 Proposed Flow(s)

Figure 8.2.4.1.2-1 depicts a generic procedure for device triggering recall/replace between oneM2M and 3GPP network.

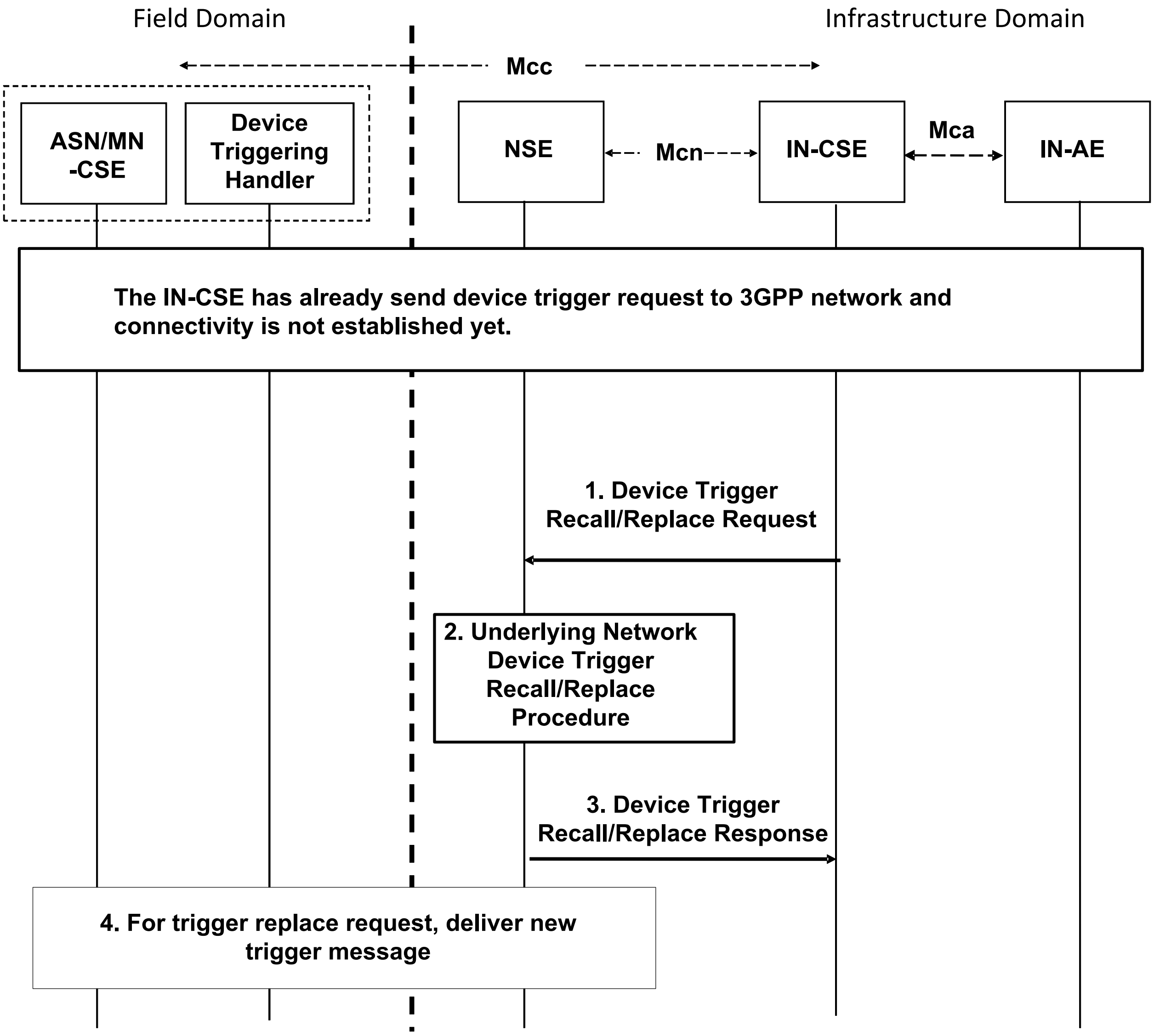

Field Domain
Infrastructure Domain
Mcc
ASN/MN -CSE
Device Triggering Handler
NSE
Mcn
IN-CSE
Mca
IN-AE
The IN-CSE has already send device trigger request to 3GPP network and connectivity is not established yet.
1. Device Trigger Recall/Replace Request
2. Underlying Network Device Trigger Recall/Replace Procedure
3. Device Trigger Recall/Replace Response
4. For trigger replace request, deliver new trigger message

Figure 8.2.4.1.2-1: General device triggering recall/replace procedure between oneM2M and 3GPP network

Pre-condition

The IN-CSE has already send device trigger request to 3GPP network and connectivity is not established yet.

Step-1: Device Trigger Recall/Replace request

IN-CSE issues the device trigger Recall/Replace request to 3GPP network.

Some information provided to 3GPP Network for device trigger recall/replace includes:

- M2M-Ext-ID associated with the ASN/MN-CSE as the target of the triggering request.
- IN-CSE ID which could be used by 3GPP network to authorize the IN-CSE for device trigger recall/replace.
- The old trigger reference number was assigned to the previously submitted trigger message that the IN-CSE wants to recall/replace.
- For trigger replace request, the new trigger reference number which is assigned by the IN-CSE to the newly submitted trigger message.

Step-2: 3GPP Network Device Trigger Recall/Replace procedure

Device Trigger Recall/Replace procedure is performed in 3GPP Network, which is specified in 3GPP TS 23.682 [i.5].

Step-3: Device Trigger Recall/Replace response

The IN-CSE receives a response for the Device Trigger Recall/Replace request via the Mcn reference point.

Step-4: For trigger replace request, deliver new trigger message.

For trigger replace request, the new trigger message will be delivered to the target Node as specified in 3GPP TS 23.682 [i.5].

8.3 Configuration of Traffic Patterns

8.3.1 Description

M2M devices that have predicable communication behaviour - e.g. in the form of repeating Traffic Patterns - may profit in terms of reduction of signalling, energy saving, fewer sleep/awake transitions, etc., when their Traffic Patterns are communicated to the underlying network.

EXAMPLE 1: 3GPP devices could use new 3GPP power savings features such as eDRX (extended discontinuous reception) and PSM (Power Saving Mode) on LTE devices.

Also the underlying network may benefit from being informed about a device's Traffic Patterns by the oneM2M System.

EXAMPLE 2: If the IN-CSE knows the device's Traffic Patterns and transmits them to an underlying 3GPP network, then this information may be used by a 3GPP network to set the device's "Maximum Response Time" (3GPP Term) to tune the UE's DRX and PSM parameters.

Thus the network benefits because the UE has fewer sleep/wake transitions and unnecessary signalling in the network is avoided. Also, if the IN-CSE knows when the device is awake then data may be sent to the device exactly at the time when the device is listening, thus requiring the network to buffer less data for unavailable devices.

The purpose of the Configuration of Traffic Patterns feature is to provide a means to the oneM2M System to inform the Underlying Network on parameters to be used for optimizing the processing at the Underlying Network for a specific Field Domain Node. The feature includes the following functionalities:

- An Application Entity (AE) or a Common Service Entity (CSE) shall be able to provide information on the communication behavior of a Field Domain Node (ASN or MN) to the underlying network.
- To that purpose the AE or CSE shall be able to set Traffic Patterns of a particular Field Domain Node via the Mca or Mcc reference point of a IN-CSE:
    - The Field Domain Node is addressed using the (CSE-ID, AE-IDs) of the Node.
- The IN-CSE shall in turn use the Mcn interface towards the Underlying Network to provide information on Traffic Patterns of the Field Domain Node:
    - The IN-CSE uses the M2M-Ext-ID to identify the Node towards the Underlying Network.

8.3.2 Feature Gap Analysis

8.3.2.1 Introduction

oneM2M uses the 3GPP Release-13 MTC feature for Configuration of Device Communication Patterns to configure Node Traffic Patterns in the Underlying Network (see section 8.3.5 Configuration of Node Traffic Patterns).
To that purpose the IN-CSE translates the oneM2M Node Traffic Pattern (TP) into a 3GPP Device Communication Pattern.

8.3.2.2 3GPP specific features

A signalling sequence for provisioning of CP parameters is described in the sub-clause 5.10.2 of 3GPP TS 23.682 [i.5]. Following figure 8.3.2.2-1 provides the signalling sequence derived from the 3GPP specification. Figure B.2.2.2-2 illustrates the terminology mapping between 3GPP and oneM2M, where the SCS is mapped to IN-CSE and the SCEF is mapped to NSE. In case the SCS is 3GPP network operator controlled, the SCEF may be deployed co-located with the SCS.

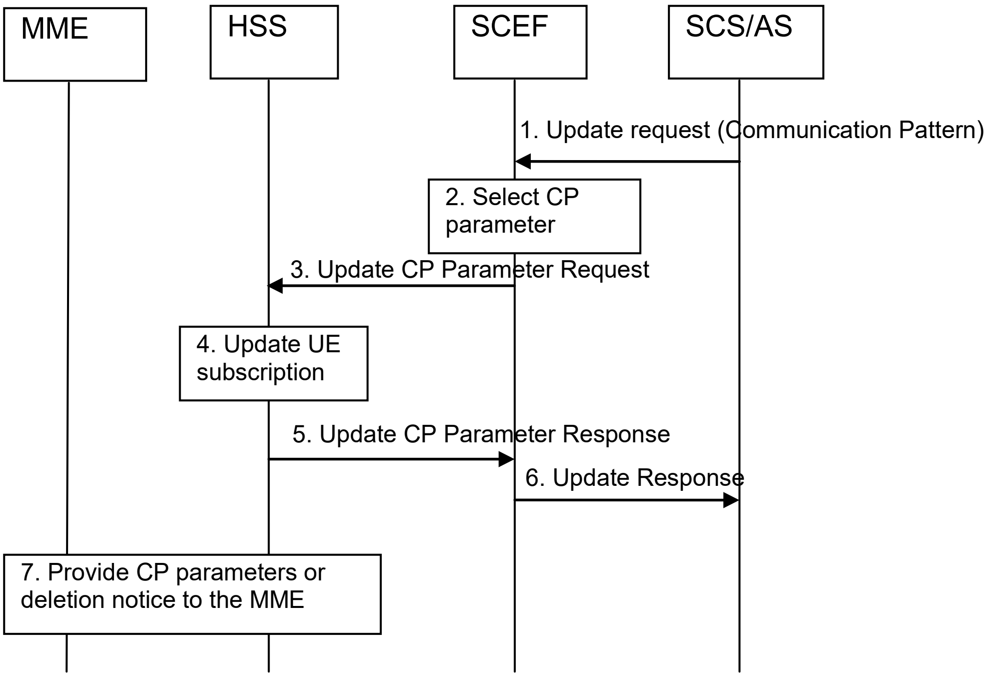

MME
HSS
SCEF
SCS/AS
1. Update request (Communication Pattern)
2. Select CP parameter
3. Update CP Parameter Request
4. Update UE subscription
5. Update CP Parameter Response
6. Update Response
7. Provide CP parameters or deletion notice to the MME

Figure 8.3.2.2-1: Signalling sequence for provisioning of CP Parameters

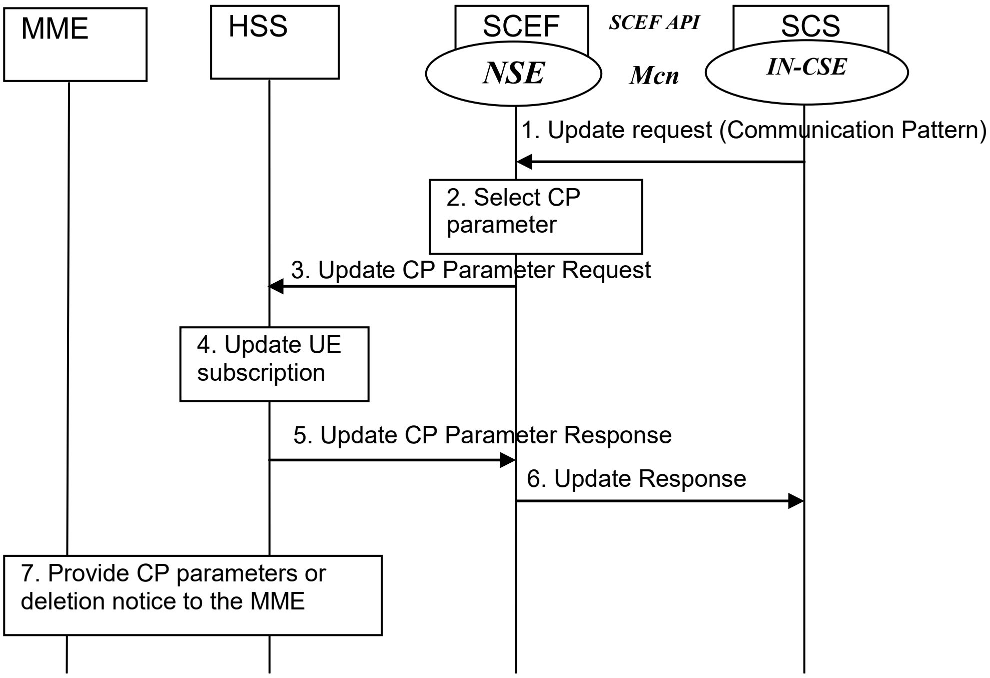

MME
HSS
SCEF
NSE
SCEF API
Mcn
SCS
IN-CSE
1. Update request (Communication Pattern)
2. Select CP parameter
3. Update CP Parameter Request
4. Update UE subscription
5. Update CP Parameter Response
6. Update Response
7. Provide CP parameters or deletion notice to the MME

Figure 8.3.2.2-2: 3GPP and oneM2M mapping

3GPP TS 23.682 [i.14] defines the request message of step 1 as below:

1. The SCS/AS sends an Update Request (External Identifier or MSISDN, SCS/AS Identifier, SCS/AS Reference ID(s), CP parameter set(s), validity time(s), SCS/AS Reference ID(s) for Deletion) message to the SCEF.

NOTE 1: The SCS/AS uses this procedure to add, change or delete some or all of the CP parameter sets of the UE, e.g. if the AS is aware that the UE has started or stopped moving for a significant time period, especially if the AS is instructing the UE to do so, then the SCS/AS provides the corresponding CP parameter set(s) and its validity time to the SCEF.

3GPP TS 23.682 [i.5] defines the request message of step 3 as below:

2. The SCEF sends Update CP Parameter Request (External Identifier or MSISDN, SCEF Reference ID(s), SCEF Address, CP parameter set(s), validity time(s), SCEF Reference ID(s) for Deletion) messages to the HSS for delivering the selected CP parameter set(s) per UE. There may be multiple CP parameter sets included in this message where each CP parameter set for addition or modification has been determined to be non-overlapping with other CP parameter sets either included in the message or already provisioned for a given UE. The SCEF derives the SCEF Reference (IDs) for CP parameter sets to be sent to the HSS based on the SCS/AS Reference ID(s) from the SCS/AS.

NOTE 2: A request for deletion of a CP parameter set from the SCS/AS may result in a request for modification of the non-overlapping CP parameter set by the SCEF.

EXAMPLE 1: In the case that the selected server NSE is a 3GPP HSS, the protocol of the S6t reference point defined by 3GPP is used for the request. The S6t uses one of Diameter Application protocols defined by 3GPP. The request on the S6t reference point for the configuration of the CP parameter sets (a CIR command) includes a User-Identifier AVP (either an External Identifier or a MSISDN of the UE), may include one or more AESE-Communication-Pattern AVP. An AESE-Communication-Pattern AVP includes a SCEF-ID AVP (represent the ID of the IN-CSE or M2M-SP-ID), may include a SCEF-Reference-ID AVP (assigned by the IN-CSE or M2M-SP to identify the configuration of CP parameter sets uniquely), may include one or more Communication-Pattern-Set AVP. A Communication-Pattern-Set AVP may include AVPs for Periodic-Communication-Indicator, Communication-Duration-Time, Periodic-Time, one or more Scheduled-Communication-Time, Stationary-Indication, and Validity-Time. Refer to the 3GPP TS 29.336 [] for the detailed protocol description.

3GPP TS 23.682 [i.5] defines the response message of step 5 as below:

3. The HSS sends Update CP Parameter Response (SCEF Reference ID, Cause) message to the SCEF. The cause value indicates successful subscription update or the reason of failed subscription update.

4. The actual parameters for the request and response messages in above steps 3 and 5 are defined by 3GPP TS 29.336 [], clauses 7 and 8 for S6t reference point.

EXAMPLE 2: In the case that the selected server NSE is a 3GPP HSS, the protocol of the S6t reference point defined by 3GPP is used for the response. The response on the S6t reference point for the configuration of the CP parameter sets (a CIA command) includes either Result-Code AVP or Experimental-Result AVP, may include a User-Identifier AVP if successful case, may include one or more AESE-Communication-Pattern-Config-Status AVP. An AESE-Communication-Pattern-Config-Status AVP includes the SCEF-Reference-ID AVP (same value in the request), may include the SCEF-ID (same value in the request) and an AESE-Error-Report AVP. Refer to the 3GPP TS29.336 for the detailed protocol description.

3GPP TS 23.682 [i.5] defines the response message of step 6 as below:

5. The SCEF sends the Update Response (SCS/AS Reference ID, Cause) message to inform the SCS/AS whether the provision of the CP parameter set(s) was successful.

8.3.2.3 oneM2M specific features

Note: in order to distinguish 3GPP terms from oneM2M terms the 3GPP “Communication Patterns” are called “Traffic Patterns” in oneM2M

A set of Traffic pattern (TP) parameters is associated with a Traffic Pattern of one or multiple field domain nodes and are defined in table 8.3.2.3-1.

A Field Domain Node may be associated with one or multiple Traffic Patterns. At any time only a single Traffic Pattern may be associated with a Field Domain Node.

The IN-CSE shall assure that different Traffic Patterns for a Node are not overlapping at any point in time.

A combination of the following TP parameters may be set for a Traffic Pattern.

Table 8.3.2.3-1: Traffic Pattern parameters

TP parameter	Description
TP Periodic communication indicator	Identifies whether the Node communicates periodically or not, e.g. only on demand.
TP Communication duration time	Duration interval time of periodic communication [may be used together with TP periodic communication indicator]. EXAMPLE: 5 minutes.
TP Time period	Interval Time of periodic communication [may be used together with TP periodic communication indicator]. Example: every hour.
TP Scheduled communication time	Time zone and Day of the week when the Node is available for communication. EXAMPLE: Time: 13:00-20:00, Day: Monday.
TP Stationary indication	Identifies whether the Node is stationary or mobile.
TP Data size indication	indicates the expected data size for the pattern.
TP Validity time	The time after which a TP becomes invalid once it had been set.

8.3.3 Key Issues and Requirements

8.3.3.1 Key SCEF NorthBound API Requirements

Number	Description	Notes
REQ-8.3-01	Create Traffic Patterns	
REQ-8.3-02	Update Traffic Patterns	
REQ-8.3-03	Delete Traffic Patterns	

8.3.3.2 Possible Impacts on the SCEF Southbound Interface

N/A

8.3.3.3. Further 3GPP Requirements and Clarifications

N/A

8.3.3.4. oneM2M Key Issues

Provide support for the configurations of Traffic Patterns.

8.3.4 Solution(s)

8.3.4.1 Solution1

8.3.4.1.1 Proposed resource types and attributes

This clause proposes the attribute *activityPatternElements* as a child of <*remoteCSE*> and <*AE*> resources for support of Traffic Patterns functionality.

The *activityPatternElements* attribute describes the anticipated availability of the CSE for communications. The set provides the anticipated activity timing pattern, and may provide additional information about the anticipated mobility status and expected data size to be exchanged. Each *activityPatternElements* item is comprised of triples (*scheduleElement*, *stationaryIndication*, *dataSizeIndicator*) with parameters shown and described in table 8.3.4-1.

Table 8.3.4-1: Parameters in *activityPatternElements* triple

Name	Description
scheduleElement	This parameter is composed from seven fields of second, minute, hour, day of month, month, day of week and year. This is a mandatory parameter in the triple. This parameter indicates the times when the entity is available to send and receive primitives.
stationaryIndication	It indicates the field node as 'Stationary (Stopping)' or 'Mobile (Moving)' for the traffic pattern. The default value is NULL, denoting that no *stationaryIndication* is provided
dataSizeIndicator	It indicates the expected data size for the traffic pattern. The default value is NULL, denoting that no *dataSizeIndicator* is provided.

Each parameter set described in Table 8.3.2.3-1 is derived by the CSE from information provided for AEs and CSEs, respectively, using information provided in one item of the *activityPatternElements* attribute. Therefore, a set can be derived when the list in the *activityPatternElements* attribute has more than one item. The parameter derivation is described in table 8.3.4-2 and exemplified below.

Table 8.3.4-2: Traffic parameter set

TP parameter set	Description	Derivation from *activityPatternElements*
TP Periodic communication indicator	Identifies whether the Node communicates periodically or not, e.g. only on demand.	If periodicity can be derived from the *scheduleElement* of the *activityPatternElements*, the indicator shall be set to TRUE. Otherwise, shall be set to FALSE.
TP Communication duration time	Duration interval time of periodic communication [may be used together with TP Periodic communication indicator]. Example: 5 minutes.	To be derived from the *scheduleElement* of the *activityPatternElements* as follows: - If a finite communication duration time can be derived, the derived value shall be used. - If only a start time is provided, a maximum value according to set defaults shall be used. - If no start time is provided, the value 0 shall be set.
TP Time period	Interval Time of periodic communication [may be used together with TP Periodic communication indicator]. Example: every hour.	If periodicity can be derived from the *scheduleElement* of the *activityPatternElements*, the derived periodicity value shall be set.
TP Scheduled communication time	Time and Day of the week when the Node is available for communication. Example: Time: 13:00, Day: Monday.	The start time derived from the current time and the *scheduleElement* of the *activityPatternElements* shall be set.
TP Stationary indication	Identifies whether the Node is stationary or mobile.	The *stationaryIndication* provided in the *activityPatternElements* shall be used. If no *stationaryIndication* is provided this optional parameter is not set.
TP Data size indication	Indicates the expected data size for the pattern.	The value of the *dataSizeIndicator* provided in the *activityPatternElements* shall be used. If no *dataSizeIndicator* is provided this optional parameter is not set.
TP Validity time	The time after which a TP parameter becomes invalid once it had been set.	If an end time can be derived from the *scheduleElement* of the *activityPatternElements,* the end time value shall be used. If no end time can be derived a maximum value according to set defaults shall be used.

Example: Consider an evaluation of an *activityPatternElements* attribute as follows:

scheduleElement (with the fields: second, minute, hour, day of month, month, day of week and year) *; 0-30 ; 2; *; Jan-Sept; Tues; 2017

*stationaryIndication: "*Moving"

dataSizeIndicator: 30kb

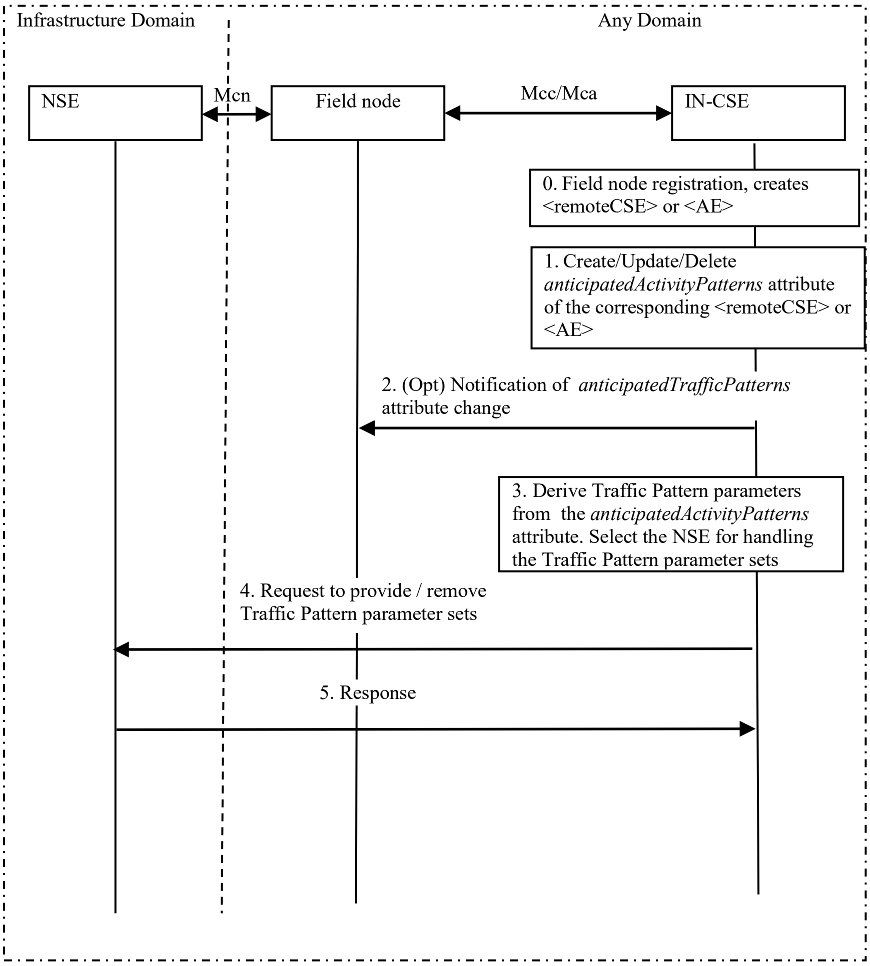
The following TP set shall be derived:

TP Periodic communication indicator: TRUE
TP Communication duration time: 30 min
TP Time period: 1 week
TP Scheduled communication time: Tues, 2:00
TP Stationary indication: "Moving"
TP Data size indication: 30kb
TP Validity time: 2 months (default maximum)

Note that the IN-CSE may use a single set of TP parameters for an entire group of Field Nodes if the corresponding *activityPatternElements* attributes are identical or if the IN-CSE can derive a common pattern for the group, corresponding to a common *activityPatternElements* attribute. How the parameters corresponding to a common *activityPatternElements* attribute are derived by the IN-CSE is implementation dependent, e.g. by computing the time superset. The parameters of this common *activityPatternElements* attribute are then used as described above to derive a single TP set for the group

8.3.4.1.2 Proposed Flow

This clause describes the procedure for resource management of Traffic Patterns to a set of field nodes.
Figure 8.3.4.1.2-1 depicts a general procedure for configuration of Traffic Patterns.



Infrastructure Domain
Any Domain
NSE
Mcn
Field node
Mcc/Mca
IN-CSE
0. Field node registration, creates <remoteCSE> or <AE>
1. Create/Update/Delete *anticipatedActivityPatterns* attribute of the corresponding <remoteCSE> or <AE>
2. (Opt) Notification of *anticipatedTrafficPatterns* attribute change
3. Derive Traffic Pattern parameters from the *anticipatedActivityPatterns* attribute. Select the NSE for handling the Traffic Pattern parameter sets
4. Request to provide / remove Traffic Pattern parameter sets
5. Response

Figure 8.3.4.1.2-1: General procedure for configuration of Traffic Patterns

Step-0: Field Node registration with IN-CSE.

The field node (ADN-AE or ASN/MN-CSE) registers with the IN-CSE. The respective <*AE*> and <*remoteCSE*> resources are created and linked to the corresponding <*node*> resource.

If the IN-CSE uses a single set of TP parameters for an entire group of Field Nodes, it is assumed that they are managed together using a <group> resource and that they are identified in the Underlying Network by a common External Group Identifier. The IN-CSE shall verify that the <*group*> resource membership consists solely of <*AE*> or <*remoteCSE*> resources.

Step-1: Anticipated behavior of a field domain AE or field domain Node is changed

The anticipated communication behaviour of the ADN-AE or ASN/MN-CSE is changed by updating the *activityPatternElements* attribute of either the <*AE*> or <*remoteCSE*>resource, respectively.

In the group case the anticipated communication behaviour of the group members is changed by updating the *activityPatternElements* attribute using a request targeting the <*fanoutPoint*> virtual resource.

Step-2: (Optional) Provide notifications of the Traffic Patterns changes

Optionally, the IN-CSE notifies the ADN-AE or ASN/MN-CSE that the anticipated communication schedule has been changed.

Step-3: The IN-CSE selects the server NSE to request for the configuration of the TP parameter sets and derives the TP parameter sets

If the IN-CSE selects the NSE by using the network identifier of the Field Domain Node (i.e. the M2M-Ext-ID or External Group Identifier) by which the Field Node can be identified in the NSE (see clause 7.1.8)

The IN-CSE derives the TP parameters as follows:

- For a Field Node hosting one or more AEs represented with a single <node> resource, using the values provided in all the *activityPatternElements* attribute for the <AE>s on this node.

- For a Field Node hosting an ASN or MN, using the values provided by the *activityPatternElements* attribute of the <*remoteCSE*> resource.

- For a group of Field Nodes, using the values provided by the *activityPatternElements* attribute of each <group> member.

Step-4: Request for the configuration of the TP parameter sets

For each field domain node received in the AE request the IN-CSE sends a request to provide TP parameter sets for the field domain node to the NSE, using the appropriate Mcn protocol. The request includes an identifier of the filed domain node and one or more TP parameter set(s) as defined at clause 8.3.3.

NOTE 2: If the Underlying Network is 3GPP-compliant, see clause 8.3.2 for more details.

Step-3: Response for the configuration of the TP parameter sets

The IN-CSE receives the response for the configuration of the TP parameter sets from the NSE. The response includes the result of the request.

NOTE 5: If the interaction with NSE in step 3 is unsuccessful, the IN-CSE has the choice to re-try it until successful.

Step-6: The Field Node TP changes are applied

After the notification in step 2, the Field Node (ASN/MN-CSE or ADN-AE) shall utilize the latest values provided by the *activityPatternElements* attribute.

8.4 Configuration of Background Data Transfers

8.4.1 Description

In the cellular network, management of the background mode traffic for M2M devices may result in significant gains for the network and improved battery life for devices. These gains may be obtained, for example, by minimizing the number network connection attempts and the time spent in connected radio state. and as such save network resources device power consumption.

The purpose of this feature is to provide a means to the oneM2M System to inform the Underlying Network of parameters that can be used for optimizing the background data traffic at the Underlying Network for a set of Field

Domain Node. Such parameters may include the expected amount of UEs in the set, a desired time window for the transfer and network area information. At the same time the oneM2M system may be informed of Underlying Network policies to be used for the given background data transfer request.

The feature includes following functionalities:

- An Application Entity (AE) or a Common Service Entity (CSE) will provide information on the background data transfer (e.g. expected data volume per UE) for a set of Field Domain Nodes (ASN or MN).
- The IN-CSE will in turn use the Mcn interface towards the Underlying Network to provide the background data transfer information to the Underlying Network.
- The IN-CSE may be provided with possible transfer policies for background data transfer by the Underlying Network, which may in turn be provided to the initiating Application Entity (AE) or a Common Service Entity (CSE).

8.4.2 Feature Gap Analysis

oneM2M uses the 3GPP Release-13 MTC feature for Background Data Transfer to request data transfers in the Underlying Network by using the oneM2M Background Data Transfer resource to provide the corresponding 3GPP information.

A signalling sequence for resource management for Background Data Transfer is described in the sub-clause 5.9 of 3GPP TS 23.682 [i.5]. Figure 8.4.2-1 provides the signalling sequence derived from the 3GPP specification with oneM2M terminologies mapping.

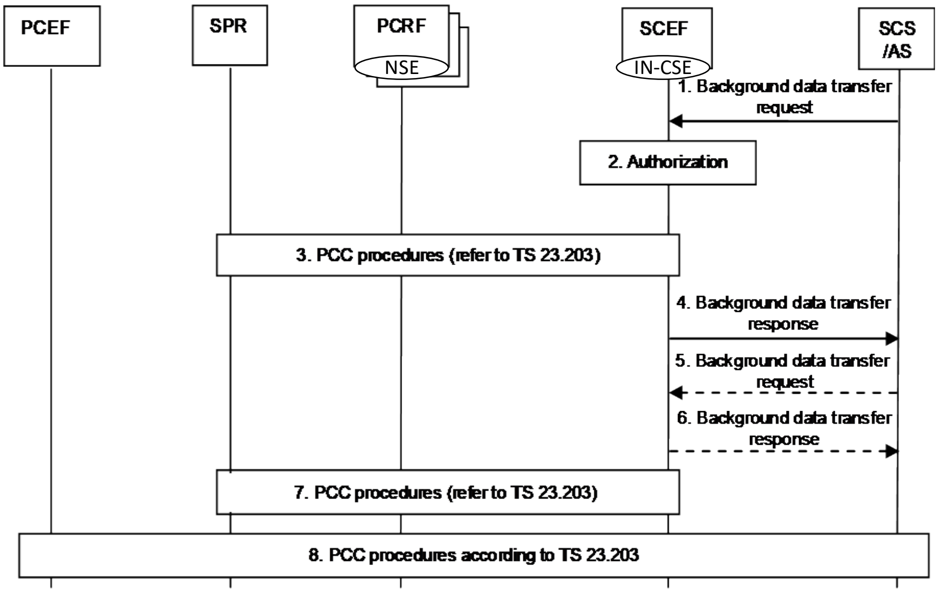

PCEF
SPR
PCRF
NSE
SCEF
IN-CSE
SCS /AS
1. Background data transfer request
2. Authorization
3. PCC procedures (refer to TS 23.203)
4. Background data transfer response
5. Background data transfer request
6. Background data transfer response
7. PCC procedures (refer to TS 23.203)
8. PCC procedures according to TS 23.203

Figure 8.4.2-1: Resource management for background data transfer

3GPP TS 23.682 [i.5] defines the IN-CSE step 3, referencing 3GPP TS 23.203 [i.11] clause 7.11.1.

3. The SCEF selects any of the available PCRFs and triggers the Negotiation for future background data transfer procedure with the PCRF. The SCEF forwards the parameters provided by the SCS/AS. The PCRF responds to the SCEF with the possible transfer policies and a reference ID.

3GPP TS 23.682 [i.5] defines the IN-CSE steps 7 and 8 as below, referencing also 3GPP TS 23.203 [i.11] clause 7.11.1.

7. The SCEF continues the Negotiation for future background data transfer procedure with the PCRF. The PCRF stores the reference ID and the new transfer policy in the SPR.
8. When the SCS/AS contacts the same or a different PCRF at a later point in time for an individual UE (via the Rx interface), the SCS/AS will provide the reference ID. The PCRF correlates the SCS/AS request with the transfer policy retrieved from the SPR via the reference ID. The PCRF finally triggers PCC procedures

according to 3GPP TS 23.203 [i.11] to provide the respective policing and charging information to the PCEF for the background data transfer of this UE.

NOTE 1: 3GPP TS 23.682 [i.5] indicates that SCS/AS contacts the PCRF to enable the background data transfer policy. This implies that the SCS/AS must have an interface to the SCEF to request the policy and another, diameter based Rx interface to activate the policy. It should be clarified if the SCS/AS may be able to activate the policy via the SCEF.

The referenced procedure in 3GPP TS 23.203 [i.11] clause 7.11.1. enables the negotiation between the oneM2M System and the Underlying Network about the time window and the related conditions for future background data transfers. Figure 8.4.2-2 provides the signalling sequence derived from the 3GPP specification with oneM2M terminologies mapping.

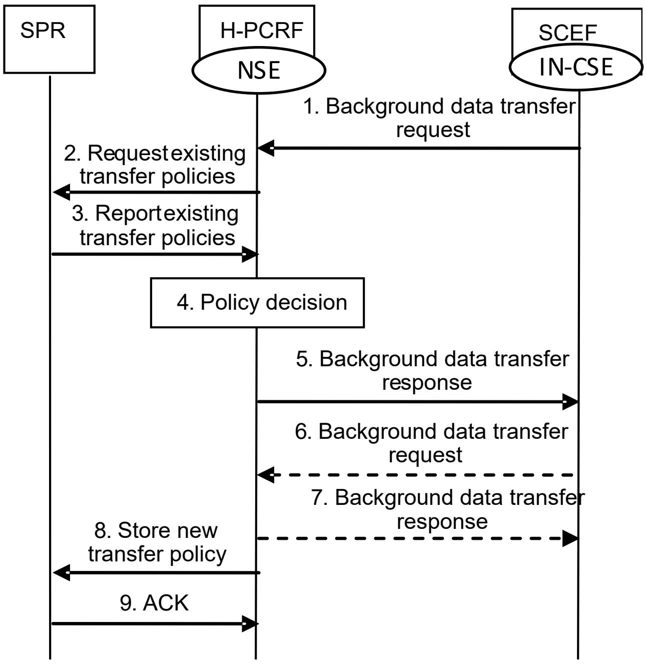

SPR
H-PCRF
NSE
SCEF
IN-CSE
1. Background data transfer request
2. Requestexisting transfer policies
3. Reportexisting transfer policies
4. Policy decision
5. Background data transfer response
6. Background data transfer request
7. Background data transfer response
8. Store new transfer policy
9. ACK

Figure 8.4.2-2: Negotiation for future background data transfer

This procedure enables the negotiation between the SCEF and the H-PCRF about the time window and the related conditions for future background data transfer (as described in 3GPP TS 23.203 [i.11], clause 6.1.16). The interaction between the SCEF and the H-PCRF is not related to an IP-CAN session and the H-PCRF associates the information provided by the SCEF to the policies belonging to the ASP and stored in the SPR.

3GPP TS 23.203 [i.11] clause 7.11.1 defines the IN-CSE step 1 of the negotiation for future background data transfer procedure as follows:

1. Based on an AF request, the SCEF sends a Background Data Transfer Request to the H-PCRF. The request contains ASP identifier, the volume of data to be transferred per UE, the expected amount of UEs, the desired time window and optionally, network area information (e.g. list of cell ids, TAs/RAs).

NOTE 2: The SCEF does not provide any information about the identity of the UEs potentially involved in the future background data transfer.

NOTE 3: A 3rd party application server is typically not able to provide any specific network area information and if so, the AF request is for the whole operator network.

3GPP TS 23.203 [i.11] clause 7.11.1 defines the IN-CSE steps 5-7 of the negotiation for future background data transfer procedure as follows:

5. The H-PCRF sends a Background data transfer response to the SCEF with the possible transfer policies and a reference ID.

NOTE 4: The SCEF forwards the information to the AF. The AF stores the reference ID for the future transfer of AF session information related to this background data transfer via the Rx interface.

6.-7. If the SCEF receives more than one transfer policy, the AF selects one of them and send another Background Data Transfer Request to inform the H-PCRF about the selected transfer policy. The H-PCRF sends a Background Data Transfer Response to the SCEF to acknowledge the selection.

NOTE 5: If the SCEF receives only one transfer policy, the AF is not required to confirm.

A set of Background Data Transfer (BDT) parameters can be associated with a background data transfer request, and a set of BDT parameters may contain references to transfer policies, as defined in tables 8.4.2-1 and 8.4.2-2.

Table 8.4.2-1: Background Data Transfer parameters

TP parameter	Description
Request Reference ID	A reference ID that is passed from the requester to IN-CSE and to the NSE in each request. The reference ID will be included in each response to associate it with the original request.
Volume per Node	Expected data volume for the background data transfer.
Number of nodes	Desired number of nodes for the background data transfer.
Desired Time Window	Desired time window for the background data transfer.
Possible Transfer Policies	List of ids of possible applicable transfer policies. Each policy may include a recommended time window, a charging rate and an aggregated maximum bitrate.
Selected Transfer Policy	If multiple polices are received from the Underlying Network, this attribute provides the id of the one selected for this transfer.

Table 8.4.2-2: Transfer Policy parameters

TP parameter	Description
Transfer Policy ID	Identifies the policy.
Recommended Time Window	Recommended time window for the background data transfer.
Charging Rate	Reference to a charging rate for this time window (see note).
Aggregated Maximum Bitrate	Optional maximum aggregated bitrate corresponding to the charging rate.
NOTE: It is expected that the Originator is configured to understand the reference to a charging rate based on an agreement with the operator of the Underling network.	

8.4.3 Key Issues and Requirements

8.4.3.1 Key SCEF NorthBound API Requirements

Number	Description	Notes
REQ-8.4-01	Background Data Transfer request/response	
REQ-8.4.02	Activate the Background Data Transfer Policy via the SCEF	See Note 1 clause 8.4.2

8.4.3.2 Possible Impacts on the SCEF SouthBound Interface

N/A

8.4.3.3. Further 3GPP Requirements and Clarifications

N/A

8.4.3.4. oneM2M Key Issues

Provide support for Background Data transfer functionality

8.4.4 Solution(s)

8.4.4.1 Solution1

8.4.4.1.1 Proposed resource types and attributes

This clause provides information of new resource types and new attributes including relationship with existing resource types and attributes.

Proposed new resource types are as below:

- Resource Type <backgroundDataTransfer>

NOTE: It is child resource of existing Resource Type <AE> or <node>.

Detailed information of new resource types is described in clause 8.4.4.1.1.1.

8.4.4.1.1.1 Resource Type <backgroundDataTransfer>

The <backgroundDataTransfer> resource represents the characteristics information (e.g. desired communication window, traffic policy, etc.) of a request for background data transfer and corresponding Underlying Network traffic policy. This information may be scheduled at application level processing. This resource type is used to share and negotiate information with other entities such as the underlying network entity (server NSE) which may optimize the background data transfer in the Underlying Network for AE/CSE.

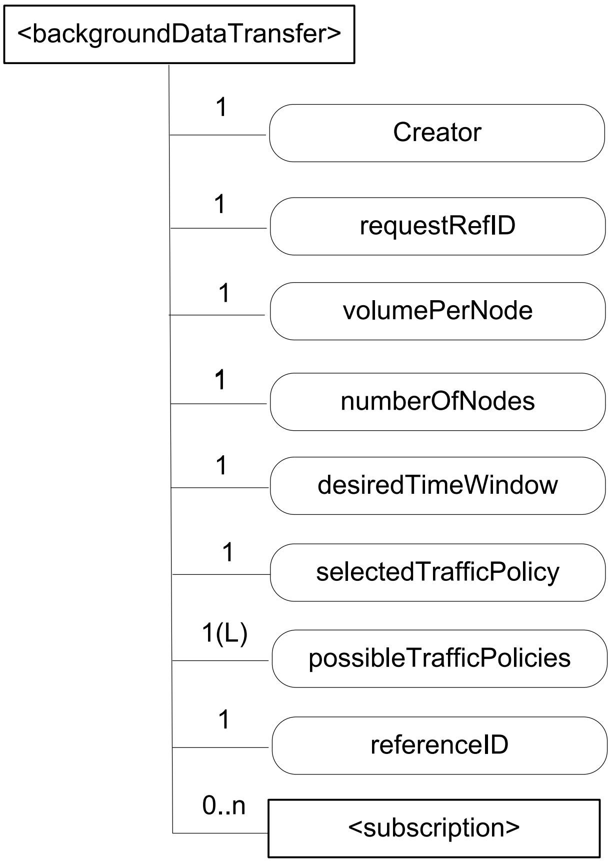


Figure 8.4.4.1.1.1-1: Structure of <backgroundDataTransfer> resource

The <*backgroundDataTransfer*> resource contains the child resources specified in table 8.4.4.1.1.1-1.

Table 8.4.4.1.1.1-1: Child resources of <backgroundDataTransfer> resource

Child Resources of <backgroundDataTransfer>	Child Resource Type	Multiplicity	Description	<backgroundDataTransfer> Child Resource Types
[variable]	*<subscription>*	0.. n	See clause 9.6.8 of oneM2M TS-0001 [i.9].	*<subscription>*

The *<backgroundDataTransfer>* resource contains the attributes specified in table 8.4.4.1.1.1-2.

Table 8.4.4.1.1.1-2: Attributes of <backgroundDataTransfer> resource

Attributes of *<deviceCharacteristics>*	Multiplicity	RW/ RO/ WO	Description	*<backgroundDataTransfer*Annc> Attributes
resourceType	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	MA
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	MA
labels	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	MA
announceTo	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
announcedAttribute	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
creator	1	WO	The AE-ID of the entity which created the resource. This can also be the CSE-ID of the IN-CSE if the IN-CSE created the resource.	OA
requestRefID	1	WO	A reference ID that is passed from the requester to IN-CSE and to the NSE in each request. The reference ID will be included in each response to associate it with the original request.	OA
volumePerNode	1	RW	Expected data volume for the background data transfer.	OA
numberOfNodes	1	RW	Desired number of nodes for the background data transfer.	OA
desiredTimeWindow	1	RW	Desired time window for the background data transfer.	OA
possibleTrafficPolicies	1(L)	RW	List of possible applicable transfer policies. Each policy may include a recommended time window, a charging rate and an aggregated maximum bitrate.	OA
selectedTrafficPolicy	1	RW	If multiple polices are received from the Underlying Network, this attribute provides the one selected policy from the list of possible traffic policies. The policy may include a recommended time window, a charging rate and an aggregated maximum bitrate.	OA
referenceID	1	RW	A reference ID that is offerd by the underlying network identities the traffic policy.	OA

8.4.4.1.2 Proposed Flow(s)

This clause describes the procedure for resource management of background data transfer to a set of field nodes.

Figure 8.4.4.1.2 depicts a general procedure for configuration of traffic policy for background data transfer based on AE's expectation. The procedure needs to be harmonized with the figures 8.4.2-1 and 8.4.2-2.

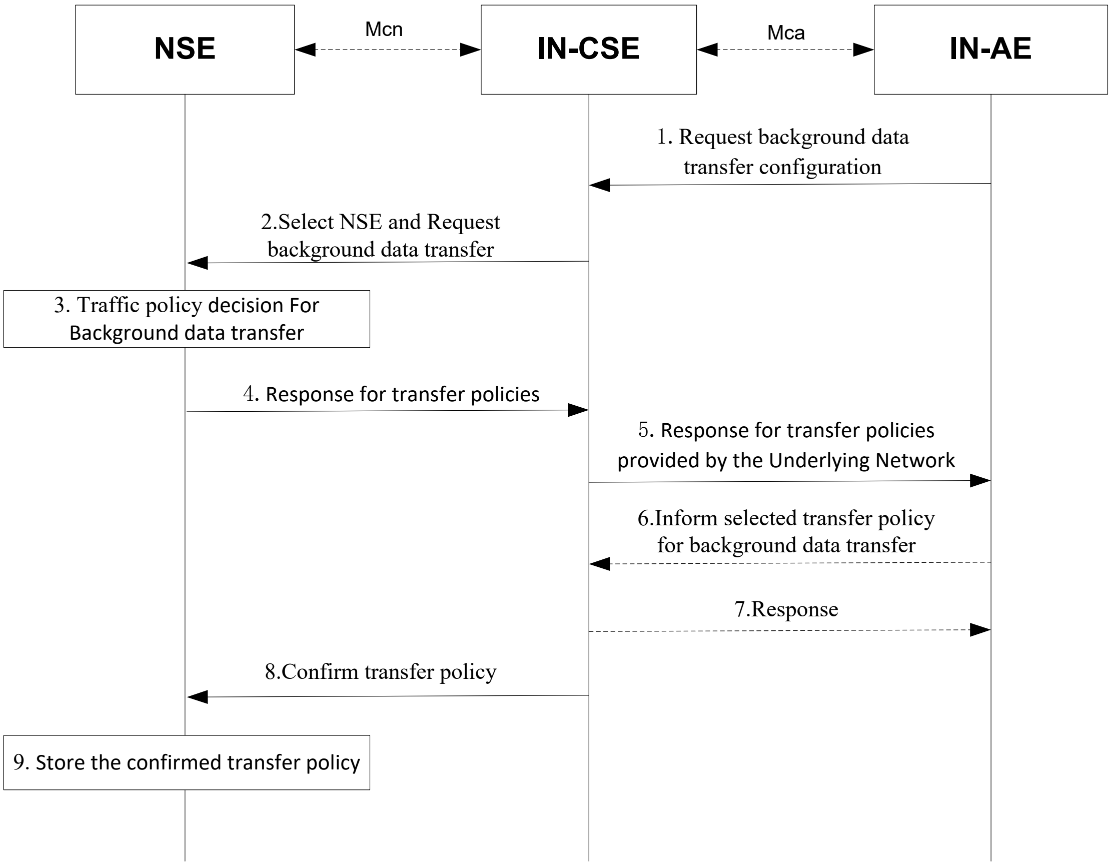

NSE
Mcn
IN-CSE
Mca
IN-AE
1. Request background data transfer configuration
2.Select NSE and Request background data transfer
3. Traffic policy decision For Background data transfer
4. Response for transfer policies
5. Response for transfer policies provided by the Underlying Network
6.Inform selected transfer policy for background data transfer
7.Response
8.Confirm transfer policy
9. Store the confirmed transfer policy

Figure 8.4.4.1.2-1: General Procedure for configuration of Background Data Transfer

Step-1 Request background data transfer configuration

An IN-AE requests IN-CSE negotiate with NSE in the Underlying Network to configure background data transfer by creating, updating or deleting a Background Data Transfer resource.

The request includes:

- the originator AE-ID of the requesting AE,
- a target identifier: i.e. the <backgroundDataTransfer> child resource of a <node> resource or an <AE> resource of requesting AE.
- a set of Background Data Transfer Parameters as indicated in table 8.4.4.1.1.1-2.

If the IN-CSE has received a request from an IN-AE to create, update or delete Background Data Transfer it checks if the request from the IN-AE is valid.

Step-2 Select NSE and Request background data transfer

The IN-CSE sends a request providing Background Data Transfer parameters to the selected NSE for negotiating background data transfer. The request includes an identifier of the requestor, the volume of data expected to be transferred per node, the expected amount of nodes, the desired time window and optionally, network area information.

NOTE: The IN-CSE selects any of available NSE before negotiation procedure, this is out of scope of the present document.

Step-3 Traffic policy decision for Background data transfer

The Underlying Network determines one or more applicable transfer policies based on requesting Background Data Transfer parameters.

Step-4 Response for transfer policies

The NSE responds to the IN-CSE with one or more applicable transfer policies and a reference ID.

Each transfer policy includes a recommended time window for the data transfer, and may provide a maximum aggregated bitrate and the charging rate applicable for the given time window.

Step-5 Response for transfer policies provided by the Underlying Network

The IN-CSE update background Data Transfer resource based on NSE response, and return a response to originator AE with the applicable transfer policies and the referenceID from the Underlying Network.

Step-6 (optional) Inform selected transfer policy for background data transfer

If more than one transfer policy was received from the Underlying Network, the Originator AE needs to select one of them. It then updates the Background Data Transfer resource with the selected transfer policy.

Step-7 (optional) Response for the selected transfer policy

Once the IN-CSE received the selected transfer policy, it returns a response to originator AE.

Step-8 Confirm the transfer policy

The IN-CSE informs confirmation for the transfer policy to the Underlying Network. If there was only one transfer offered in step-4, the IN-CSE responds a confirmation which means the transfer policy is known by originator AE. If more than one transfer policies was offered in step-4 and the originator AE selected one of them, the IN-CSE forwards the selected transfer policy with the reference ID to the NSE as a confirmation.

Step-9 Store the confirmed transfer policy

The Underlying Network stores the new transfer policy and the reference ID based on the confirmation.

8.5 Support for Group Messaging

8.5.1 Description

The Group Management (GMG) CSF is responsible for handling group related requests. The requests are sent to manage a group and its membership as well as to support the bulk operations at the Mca reference point. But the GMG currently does not support multicast capability and sends the same content message to the members of the group by means of unicast. It's costly and inefficient.

When the same content is sent to the members of a group that are located in a particular geographical area, 3GPP provides MBMS capabilities that may be used to efficiently distribute the message to the group members, enabling GMG to utilize the multicasting capability.

Pre-conditions:

1) The MBMS service area information provided by operator is configured in the oneM2M System;

2) External Group Identifiers for the devices have been pre-provisioned in the oneM2M System.

3) The mapping rule between the External Group Identifier of the device and the MBMS service area has been configured in the oneM2M System to determine whether the group has 3GPP MBMS capability or not.

GMG relies on 3GPP SCEF to provide: querying functionality to get MBMS service area information; negotiation functionality to confirm the MBMS bearer establishing time window, and transferring functionality to send the group message content to the UE.

8.5.2 Feature Gap analysis

oneM2M uses the 3GPP Release-13 MTC feature for Group Messaging, which involves message delivery using MBMS. For that purpose, the IN-CSE uses the oneM2M group management feature to define a 3GPP-external group. It also uses communications over the Mcn interface to authorize the originator of a group messaging procedure and for allocation of an external temporary group identifier, which is then used in group message delivery within the Underlying Networks.

A signalling sequence for Group Message delivery is described in the clause 5.5 of 3GPP TS 23.682 [i.5]. Figure 8.5.2-1 provides the signalling sequence derived from the 3GPP specification with oneM2M terminologies mapping (3GPP TS 23.682 [i.13], figure 5.5.1-1). It should be noted that the 3GPP group message delivery feature does not support all the scenarios, since for the UEs not supporting MBMS or for the UEs located in areas where MBMS is not deployed, the 3GPP group message delivery does not apply.

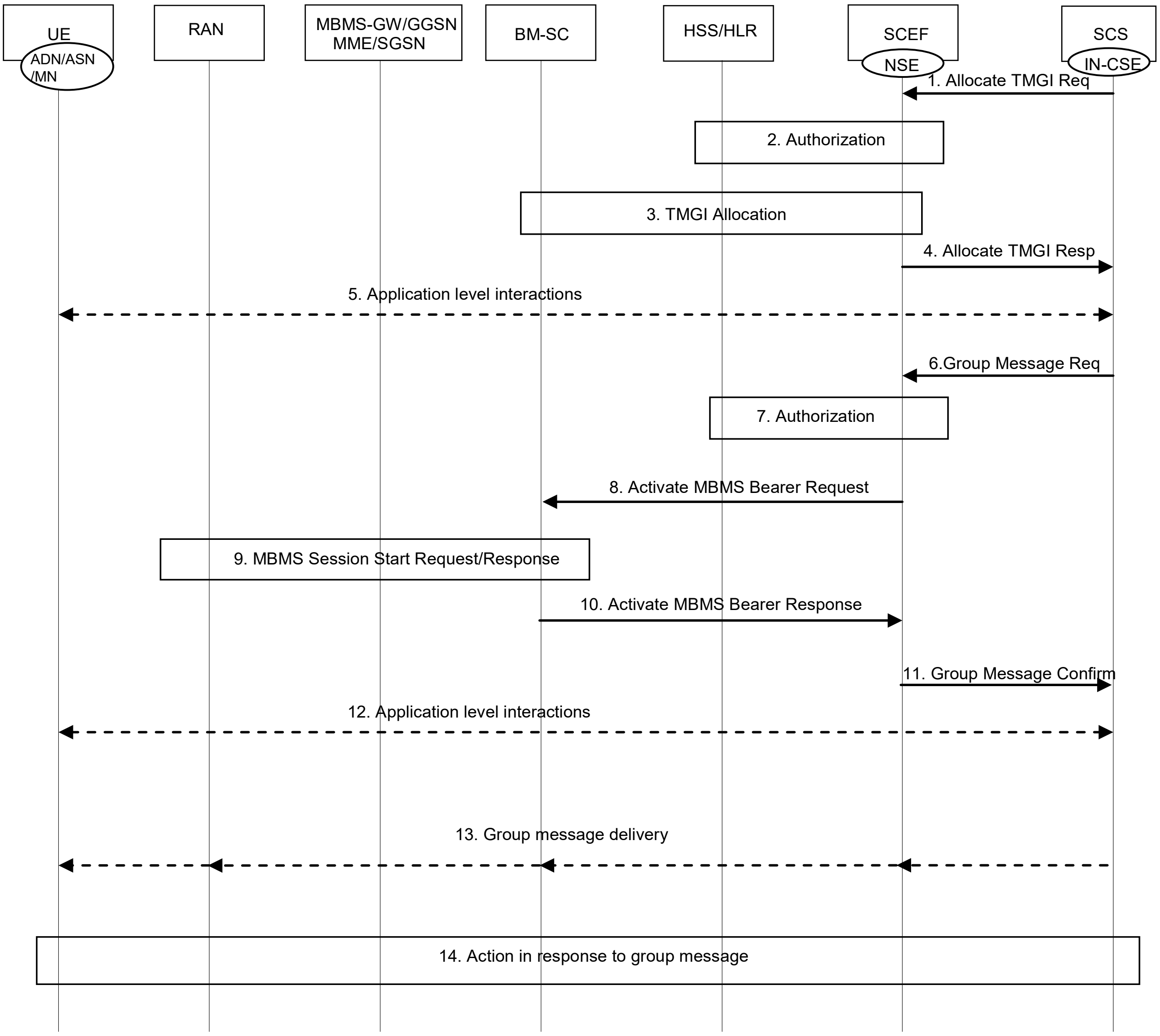

UE
ADN/ASN /MN
RAN
MBMS-GW/GGSN MME/SGSN
BM-SC
HSS/HLR
SCEF
NSE
SCS
IN-CSE
1. Allocate TMGI Req
2. Authorization
3. TMGI Allocation
4. Allocate TMGI Resp
5. Application level interactions
6.Group Message Req
7. Authorization
8. Activate MBMS Bearer Request
9. MBMS Session Start Request/Response
10. Activate MBMS Bearer Response
11. Group Message Confirm
12. Application level interactions
13. Group message delivery
14. Action in response to group message

Figure 8.5.2-1: Group message delivery using MBMS

Figure 8.5.2-1 describe the group message delivery using MBMS procedure, the involved SCEF northbound APIs are as described below.

Step1 SCS(IN-CSE) sends Allocate TMGI Req (External Group ID, SCS Identifier, location/area information) to SCEF.

Step4 SCEF sends Allocate TMGI Resp (SCS/AS Reference ID, TMGI and expiration time information) to SCS(IN-CSE).

Step6 SCS(IN-CSE) sends Group Message Req (External Group Identifier, SCS Identifier, location/area information, RAT(s) information, TMGI, start time) to SCEF.

Step11 SCEF sends Group Message Confirm (TMGI (optional), SCEF IP addresses/port) to SCS(IN-CSE)

In the Figure 8.5.2-1 there are some gaps as described below:

- Step1: The parameter *location/area information* is not used during the next steps. It may not be needed.
- Step2 and Step7: These steps are used to determine whether the SCS is authorized to request the service. But this step is not specified. The authorization may impact parameters in Step1 and Step6.
- Step6: The parameter *location/area information* and *RAT(s) information* are not used in the next steps since SCS has the TMGI information in Step 4. In addition, how to map these parameters to Step8 is not clear.
- Step13: In the TS 23.682[i.5] architecture, the interface between SCEF and SCS/AS is only API based. But in this step, it uses the IP address and port in user plane of SCEF to deliver the group message content. The mechanism to allow an SCS/AS to send the group message needs to be clarified. If this step is still over API, the parameter S*CEF IP addresses/port* may not be needed in Step11 and new Group Message Content Delivery API is needed in this step.
- Step14: Assuming the Group Message Content Delivery Request(SCS->SCEF) in step 13 is over API, the group message delivery status API is needed.
- Note that in Step 5/12 oneM2M needs to support application interaction to transfer the MBMS service information e.g. TMGI, start time from IN-CSE to UE.

The TMGI allocation procedure and the Activate MBMS Bearer Procedure in figure 8.5.2-1 are specified in 3GPP TS 23.468 [i.14]. Related descriptions are provided below, where the GCS AS is considered to be the SCEF.

3GPP TS 23.468 [i.14] provides the procedure used between the GCS AS and the BM-SC to allocate a set of TMGIs to the GCS AS.

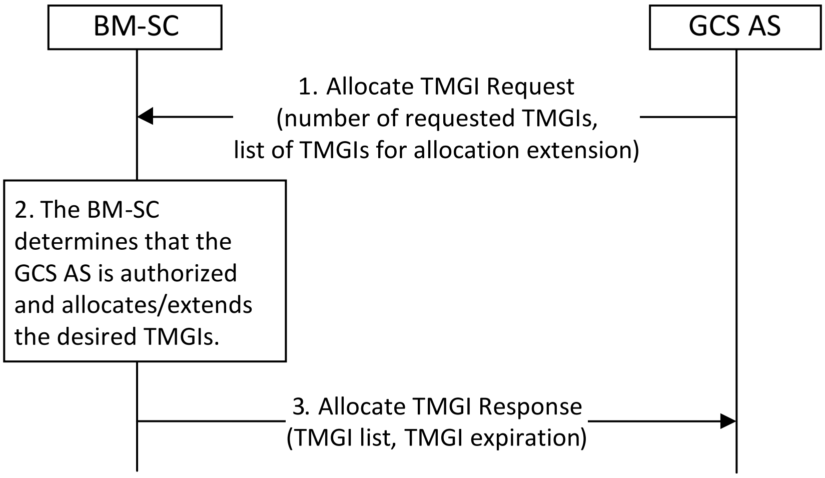

BM-SC
GCS AS
1. Allocate TMGI Request
(number of requested TMGIs,
list of TMGIs for allocation extension)
2. The BM-SC determines that the GCS AS is authorized and allocates/extends the desired TMGIs.
3. Allocate TMGI Response
(TMGI list, TMGI expiration)

Figure 8.5.2-2 (of 3GPP TS 23.468): TMGI Allocation Procedure [i.14]

1. When the GCS AS wishes to have the BM-SC allocate one or more TMGIs to it, the GCS AS sends an Allocate TMGI Request message to the BM-SC, including the number of requested TMGIs. The GCS AS may include a list of TMGIs that are already allocated to the GCS AS, and for which the GCS AS wishes to obtain a later expiration time. The number of TMGIs requested may be zero, if this procedure is used only to renew the expiration time for already allocated TMGIs.
2. The BM-SC determines whether the GCS AS is authorized to receive the TMGIs and allocates a set of TMGIs. The BM-SC determines an expiration time for the TMGIs. If a list of TMGIs has been received in the Allocate TMGI Request message, the BM-SC also determines whether the TMGIs are allocated to the requesting GCS AS and if yes, whether the expiration time for those TMGIs may be set to the new expiration time.
3. The BM-SC sends an Allocate TMGI Response message to the GCS AS indicating the list of allocated TMGIs, and an expiration time for those TMGIs.

3GPP TS 23.468 [i.14] provides the procedure used between the GCS AS and the BM-SC to activate an MBMS bearer.

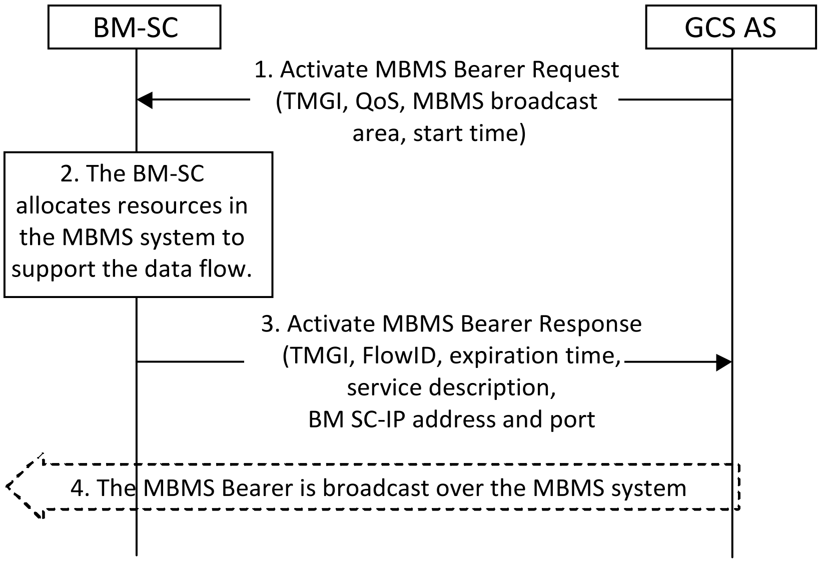

BM-SC
GCS AS
1. Activate MBMS Bearer Request (TMGI, QoS, MBMS broadcast area, start time)
2. The BM-SC allocates resources in the MBMS system to support the data flow.
3. Activate MBMS Bearer Response (TMGI, FlowID, expiration time, service description, BM SC-IP address and port
4. The MBMS Bearer is broadcast over the MBMS system

Figure 8.5.2-3 (of 3GPP TS 23.468): Activate MBMS Bearer Procedure [i.14]

1. When the GCS AS wishes to activate an MBMS bearer over MB2, the GCS AS sends an Activate MBMS Bearer Request message to the BM-SC, including the TMGI which represents the MBMS bearer to be started, QoS, MBMS broadcast area, and start time. The TMGI is optional. The QoS maps into appropriate QoS parameters of the MBMS bearer. The MBMS broadcast area parameter includes a list of MBMS Service Area Identities, or a list of cell IDs, or both.

NOTE 1: If the MBMS broadcast area parameter includes a list of MBMS Service Area Identities, the list of MBMS Service Area Identities is determined from information that may come from the UEs (e.g. list of cell IDs) or some other knowledge of where to establish the service (e.g. configuration).

2. If the TMGI was included, the BM-SC determines whether the GCS AS is authorized to use the TMGI. The BM-SC rejects the request if the TMGI is not authorized. If the TMGI was not included in the request, the BM-SC assigns an unused value for the TMGI. The BM-SC allocates a FlowID value corresponding to this TMGI and MBMS broadcast area. If the MBMS broadcast area parameter includes a list of cell IDs, the BM-SC may map the cell IDs into MBMS Service Area Identities subject to operator policy. The BM-SC then includes a list of MBMS Service Area Identities and, if available, the list of cell IDs in the MBMS Session Start message. If another MBMS bearer with the same TMGI is already activated, the BM-SC accepts the request only if the MBMS broadcast area in the new request is not partly or completely overlapping with any existing MBMS bearer(s) using the same TMGI as according to 3GPP TS 23.246 [i.15] and allocates a unique FlowID for the newly requested MBMS bearer. The BM-SC shall allocate MBMS resources to support content delivery of the MBMS bearer to the requested MBMS broadcast area using the Session Start procedure defined in 3GPP TS 23.246 [i.15].

3. The BM-SC sends an Activate MBMS Bearer Response message to the GCS AS, including the TMGI, the allocated FlowID, service description, BM-SC IP address and port number for the user-plane, and an expiration time. The service description contains MBMS bearer related configuration information as defined in 3GPP TS 26.346 [i.13] (e.g. radio frequency and MBMS Service Area Identities). If the BM-SC mapped the cell IDs into the MBMS Service Area Identities in Step 2, then the service description contains the MBMS Service Area Identities that the BM-SC included in the MBMS Session Start message. The expiration time is included only if the BM-SC has allocated a TMGI as a result of this procedure.

NOTE 2: The GCS AS can use the service description to provide information to the UE to access the MBMS bearer.

NOTE 3: Since the MBMS bearer is not necessarily established in all cells belonging to the MBMS SAIs in the Activate MBMS Bearer Response message, the list of MBMS SAIs provided by the BM-SC to the GCS AS does not guarantee that the MBMS bearer is available in all cells of the service area identified by the MBMS SAIs.

8.5.3 Key Issues and Requirements

8.5.3.1 Key SCEF NorthBound API Requirements

Table 8.5.3.1-1 SCEF NorthBound API requirements

Number	Description	Note
REQ-8.5.01	Support TMGI allocation	Step1: Allocate TMGI Request（SCS->SCEF）in clause 5.5.1 TS23.682 [i.5] Step4: Allocate TMGI Response(SCEF->SCS）in clause 5.5.1 TS23.682 [i.5]
REQ-8.5.02	Support TMGI bearer activation	Step6: Group Message Request(SCS-SCEF) in Clause 5.5.1 TS23.682 [i.5] Step11: Group Message Confirm(SCEF->SCS) in Clause 5.5.1 TS23.682 [i.5]

8.5.3.2 Potential impacts on the SCEF SouthBound Interface

Table 8.5.3.3-1 Potential impacts on the SCEF SouthBound Interface

Number	Description	Note
IMPACT-8.5.01	How does SCEF authorize the SCS during group message delivery? It needs to be specified if there any additional authorization critical for group message delivery beyond the general authorization of API framework.	Step2: authorization for TMGI allocation（SCEF<->HSS）in Clause 5.5.1 TS23.682 [i.5] Step7: authorization for Group message Request（SCEF<->HSS）in Clause 5.5.1 TS23.682 [i.5]

8.5.3.3 Further 3GPP requirements and clarifications

Table 8.5.3.1-2 Issues to be clarified by 3GPP (Stage 2)

Number	Description	Notes
ISSUE-8.5.01	The usage and format of parameter location/area information in the request needs to be clarified.	Allocate TMGI Request（SCS->SCEF）in step1 clause 5.5.1 TS23.682 [i.5]
ISSUE-8.5.02	The usage and format of parameter location/area information, as well as RAT(s) information need to be clarified.	Group Message Request(SCS->SCEF) in step6 clause 5.5.1 TS23.682 [i.5]
ISSUE-8.5.03	In the TS 23.682[i.5] architecture, the interface between SCEF and SCS/AS is only at the level of API. But in this step, it uses the IP address and port in user plane of SCEF to deliver the group message content delivery. The group message content delivery interface between SCEF and SCS/AS needs to be clarified.	Group Message Content Delivery Request(SCS->SCEF) in step 13 clause 5.5.1 TS23.682 [i.5]
ISSUE-8.5.04	Assuming the Group Message Content Delivery Request(SCS->SCEF) in step 13 is over API, the group message delivery status API is needed	Group Message Delivery Status Indication（SCEF->SCS） in step 14 clause 5.5.1 TS23.682 [i.5]

8.5.3.4. oneM2M Key Issues

Provide support for Group Messaging.

8.6 Support for Network status report

8.6.1 Description

The IN-CSE needs to know the NSE available in the operator network, for example, congestion level or an indication of the "no congestion" state for NSE.

An IN-CSE may request for being notified about the network status. The following methods are supported:

- The IN-CSE requests to be informed, one-time, about the network status by providing a geographical area. This procedure is referred to as one-time network status request.
- The IN-CSE requests to be informed, continuously, about the network status by providing a geographical area. This procedure is referred to as continuous network status request.

8.6.2 Feature Gap Analysis

8.6.2.1 Request procedure for one-time or continuous reporting of network status

This procedure is used by an SCS/AS to retrieve Network Status Indication from the network. This procedure can be used to request a one-time or continuous reporting of network status. Figure 8.6.2.1-1 illustrates the procedure.

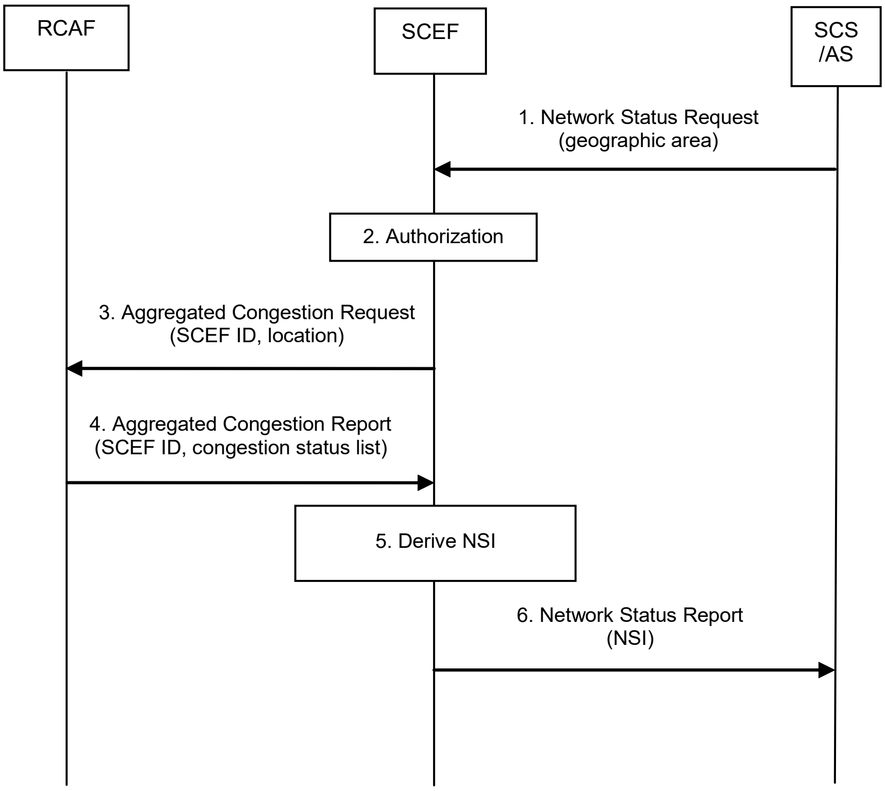

RCAF
SCEF
SCS /AS
1. Network Status Request (geographic area)
2. Authorization
3. Aggregated Congestion Request (SCEF ID, location)
4. Aggregated Congestion Report (SCEF ID, congestion status list)
5. Derive NSI
6. Network Status Report (NSI)

Figure 8.6.2.1-1: Request procedure for one-time or continuous reporting of network status

NOTE 1: Step 1 and 6 are outside of 3GPP scope, but are shown for informative purposes only.

1. When the SCS/AS needs to retrieve NSI, the SCS/AS sends a Network Status Request (Geographical area, SCS/AS Identifier, SCS/AS Reference ID, Duration, Threshold) message to the SCEF. Duration indicates the

time for which a continuous reporting is requested. The absence of Duration indicates a one-time reporting. Threshold indicates a range at which the SCS/AS wishes to be informed of the network status. Multiple Threshold values may be included.

NOTE 2: Geographical area specified by SCS/AS could be at cell level (CGI/ECGI), TA/RA level or other formats e.g. shapes (e.g. polygons, circles etc.) or civic addresses (e.g. streets, districts etc.) as referenced by OMA Presence API.

2. The SCEF authorizes the SCS/AS request for notifications about potential network issues. The SCEF stores SCS/AS Address, SCS/AS Reference ID, Duration, if present and Threshold if present. The SCEF assigns an SCEF Reference ID.

NOTE 3: Based on operator policies, if either the SCS/AS is not authorized to perform this request (e.g. if the SLA does not allow for it) or the SCS/AS has exceeded its quota or rate of submitting requests, the SCEF sends a Network Status Response (Cause) message with a Cause value appropriately indicating the error.

3. The SCEF assigns an SCEF Reference ID and identifies, based on local configuration, the RCAF(s) responsible for the provided Geographical Area. For every identified RCAF, the SCEF derives a Location Area from the Geographical Area provided by the SCS/AS. The Location Area is according to operator configuration either a 3GPP location area (e.g. list of TA/RAs, list of cell(s), list of eNodeBs etc.) or a sub-area of the Geographical Area provided by the SCS/AS. The SCEF sends an Aggregated Congestion Request (SCEF Reference ID, Location Area, Duration, Threshold) message to the identified RCAF(s). Duration indicates the time for which a continuous reporting is requested. The absence of Duration indicates a one-time reporting. The SCEF, based on operator policies, may chose a different Threshold value than the one indicated by the SCS/AS in step 1.

4. The RCAF examines the Aggregated Congestion Request message. If the SCEF provided a Duration, the RCAF stores the SCEF instructions and starts to monitor the set of cells or eNodeBs belonging to the Location Area for a change in the congestion status that is crossing a Threshold (if provided by the SCEF). The RCAF sends an Aggregated Congestion Report to the SCEF including the SCEF Reference ID and, depending on the operator configuration and current RCAF knowledge, the congestion status for every cell or eNodeB belonging to the Location Area requested by the SCEF.

5. The SCEF verifies whether the Network Status Request identified via the SCEF Reference ID is valid and active and stores the report. After receiving reports from all the involved RCAF(s) to which step 3 was executed, the SCEF derives the NSI for the requested Geographical Area by combining all reports with the same SCEF Reference ID in an operator configurable way (governed by SLAs, network topology, usage, etc.).

NOTE 4: Either exact values for congestion status, as reported by RCAF(s) to SCEF or abstracted values e.g. (High, Medium, Low) can be reported by the SCEF to the SCS/AS. The calculation and the reporting of the NSI to the SCS/AS depends on operator configuration (SLAs, network topology, usage, etc.), and is outside the scope of this specification.

6. The SCEF send a Network Status Report (SCS/AS Reference ID, NSI) message to the SCS/AS.

8.6.2.2 Report procedure for continuous reporting of network status

This procedure is used by the SCEF to report a change of Network Status Information (NSI) to the SCS/AS which requested a continuous reporting of network status. Figure 8.6.2.2-1 illustrates the procedure.

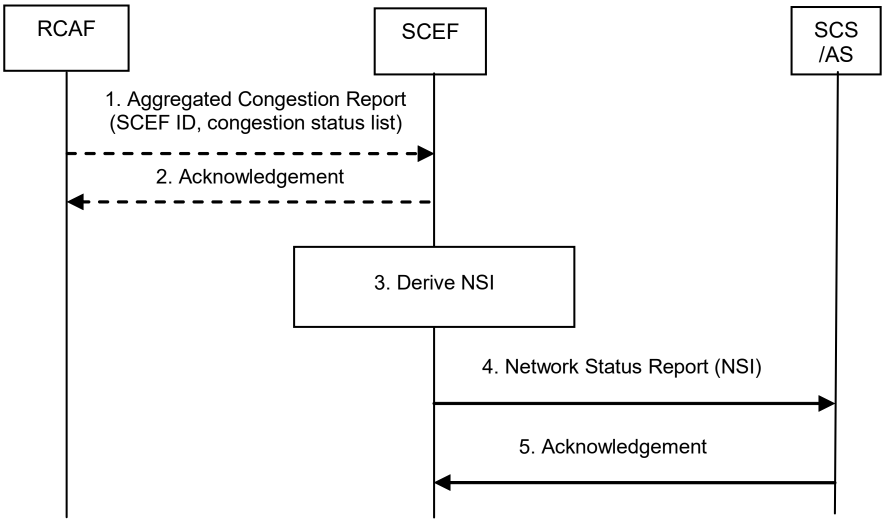

RCAF
SCEF
SCS
/AS
1. Aggregated Congestion Report
(SCEF ID, congestion status list)
2. Acknowledgement
3. Derive NSI
4. Network Status Report (NSI)
5. Acknowledgement

Figure 8.6.2.2-1: Report procedure for continuous reporting of network status

NOTE 1: Step 4 and 5 are outside of 3GPP scope, but are shown for informative purposes only.

1. The RCAF detects a change in the congestion status that is crossing a Threshold (if provided by the SCEF) for the set of cells or eNodeBs belonging to the Location Area requested by the SCEF. An Aggregated Congestion Report message is sent to this SCEF including the SCEF reference ID and, depending on the operator configuration, the congestion status for every cell or eNodeB belonging to the Location Area requested by the SCEF.

2. The SCEF acknowledges the report to the RCAF.

NOTE 2: Step 1 and 2 can happen multiple times and the Aggregated Congestion Report message can be sent by any of the involved RCAFs.

3. Whenever a new Aggregated Congestion Report message arrives, the SCEF stores the report and derives a new NSI for the requested geographical area by combining this report with all other reports having the same SCEF reference ID in an operator configurable way (governed by SLAs, network topology, usage, etc.).

NOTE 3: Either exact values for congestion status, as reported by RCAF(s) to SCEF or abstracted values e.g. (High, Medium, Low) can be reported by the SCEF to the SCS/AS. The calculation and the reporting of the NSI to the SCS/AS depends on operator configuration (SLAs, network topology, usage etc.), and is outside the scope of this specification.

4. Triggered by a NSI change (derived in step 3) that is crossing a Threshold (if provided by the SCS/AS), the SCEF sends a Network Status Report (SCS/AS Reference ID, NSI) message to the SCS/AS.

5. The SCS/AS acknowledges the report to the SCEF.

8.6.2.3 Removal procedure for continuous reporting of network status

This procedure is used for termination of the continuous reporting of network status. It can be triggered by the SCS/AS at any time before the Duration is over or if no Duration was provided. The SCEF will trigger this procedure when the Duration is over. Figure 8.6.2.3-1 illustrates the procedure.

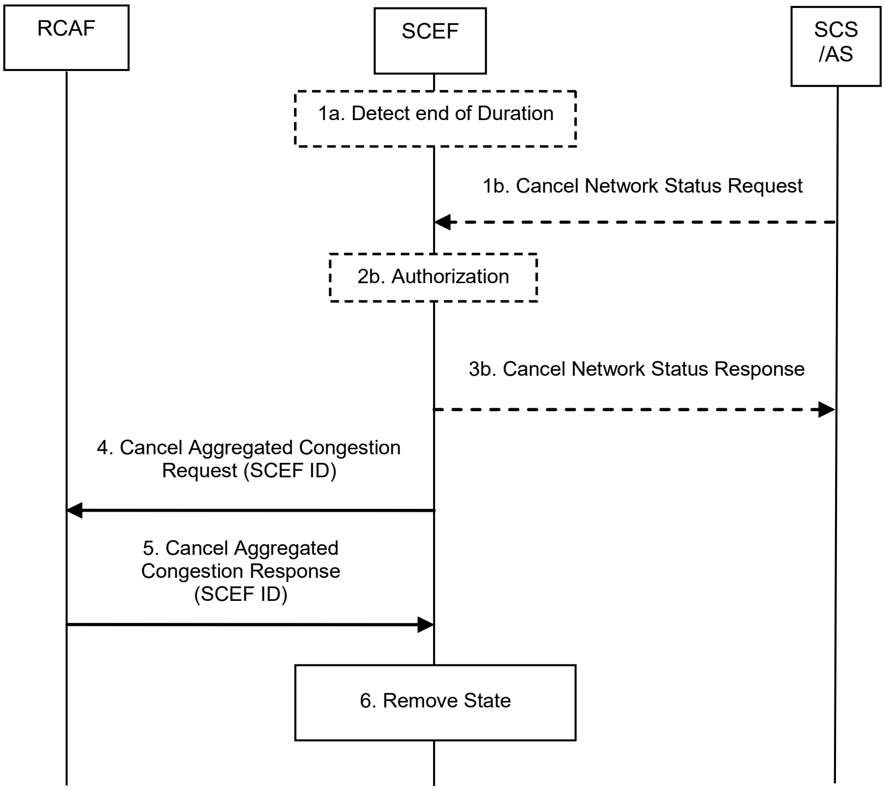

RCAF
SCEF
SCS
/AS
1a. Detect end of Duration
1b. Cancel Network Status Request
2b. Authorization
3b. Cancel Network Status Response
4. Cancel Aggregated Congestion Request (SCEF ID)
5. Cancel Aggregated Congestion Response (SCEF ID)
6. Remove State

Figure 8.6.2.3-1: Removal procedure for continuous reporting of network status

NOTE 1: Step 1b and 3b are outside of 3GPP scope, but are shown for informative purposes only.

1a. The SCEF detects that the requested Duration for an ongoing continuous reporting of network status to an SCS/AS is over and identifies the corresponding SCEF Reference ID.

1b. When the SCS/AS needs to terminate an ongoing continuous reporting of network status, the SCS/AS sends a Cancel Network Status Request (SCS/AS Identifier, SCS/AS Reference ID) message to the SCEF.

2b. The SCEF authorizes the SCS/AS request and identifies the corresponding SCEF Reference ID.

3b. If the SCS/AS requested to terminate an ongoing continuous reporting of network status in step 1b, the SCEF sends a Cancel Network Status Response (SCS/AS Reference ID) message to the SCS/AS.

4. The SCEF identifies the RCAF(s) involved in the continuous reporting represented by the SCEF Reference ID. The SCEF sends a Cancel Aggregated Congestion Request (SCEF Reference ID) message to the identified RCAF(s).

5. The RCAF removes the related SCEF instructions and stops monitoring the set of cells or eNodeBs belonging to the Location Area for a change in the congestion status. Afterwards, a Cancel Aggregated Congestion Response is sent to the SCEF including the SCEF Reference ID.

6. The SCEF removes all state information related to this continuous reporting represented by the SCEF Reference ID.

A set of Network issue report parameters can be associated with a network status request, as defined in table 8.6.2-1.

Table 8.6.2-1: Network issue report parameters

Parameter	Description
Reference ID	A reference ID that is passed from the requester to SCEF and to the NSE in each request. The reference ID will be included in each response to associate it with the original request.
Location Area	Location Area is according to operator configuration either a 3GPP location area or a sub-area of the Geographical Area provided by the SCS/AS.
Threshold	Threshold indicates a range at which the SCS/AS wishes to be informed of the network status. Multiple Threshold values may be included.
Duration	Duration indicates the time for which a continuous reporting is requested. The absence of Duration indicates a one-time reporting.
Network status information	Congestion level or an indication of the "no congestion" state for NSE.

8.6.3 Key Issues and Requirements

8.6.3.1 Key SCEF NorthBound API Requirements

Number	**Description**	**Notes**
REQ-8.6-01	Network Status request/response (one time)	
REQ-8.6-02	Network Status request/response (continuous)	
REQ-8.6-03	Remove Network Status configuration	
REQ-8.6-04	Network Status report	

8.6.3.2 Possible Impacts on the SCEF SouthBound Interface

N/A

8.6.3.3. Further 3GPP Requirements and Clarifications

N/A

8.6.3.4. oneM2M Key Issues

Provide support for the Network Status Report functionality

8.6.4 Solution(s)

8.6.4.1 Solution1

8.6.4.1.1 Proposed resource types and attributes

Proposed new resources are as below.

- Resource Type <n*etworkStatus*>

NOTE: It is child resource of existing Resource Types <*CSEBase*>.

Detailed information of new resource types is described in sub-clauses below.

8.6.4.1.1.1 Resource Type <networkStatus>

The <*networkStatus*> resource represents the characteristics of a request for network issue report using Underlying Network information.

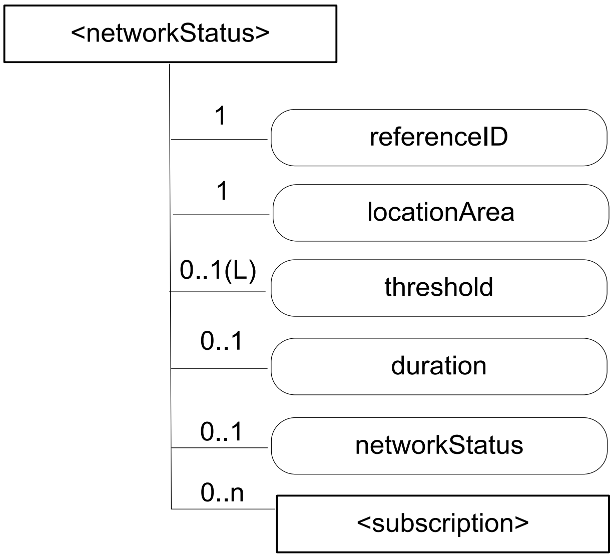


Figure 8.6.4.1.1.1-1: Structure of <networkStatus> resource

The <*networkStatus*> resource shall contain the child resources specified in table 8.6.4.1.1.1-1.

Table 8.6.4.1.1.1-1: Child resources of <networkStatus> resource

Child Resources of <*locationPolicy*>	Child Resource Type	Multiplicity	Description	<*networkStatusAnnc*> Child Resource Types
[variable]	*<subscription>*	0.. n	See clause 9.6.8 of oneM2M TS-0001 [i.9]	None

The <*networkStatus*> resource shall contain the attributes specified in table 8.6.4.1.1.1-2.

Table 8.6.4.1.1.1-2: Attributes of <networkStatus> resource

Attributes of *<networkStatus>*	Multiplicity	RW/ RO/ WO	Description	*<networkStatusA nnc>* Attributes
resourceType	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
resourceID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
resourceName	1	WO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
parentID	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
creationTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
lastModifiedTime	1	RO	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
expirationTime	1	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	MA
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	MA
labels	0..1 (L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	MA
announceTo	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
announcedAttribute	0..1(L)	RW	See clause 9.6.1.3 of oneM2M TS-0001 [i.9].	NA
creator	1	WO	The AE-ID of the entity which created the resource.	OA
referenceID	1	WO	A reference ID that is passed from the requester to IN-CSE and to the NSE in each request. The reference ID will be included in each response to associate it with the original request.	OA
locationArea	1	RW	Geographical area where AE needs to obtain the network status. It could be shapes (e.g. polygons, circles, etc.) or civic addresses (e.g. streets, districts, etc.)	OA
threshold	0..1(L)	RW	A range at which the AE wishes to be informed of the network status of NSE. Multiple threshold values may be included.	OA
duration	0..1	RW	The time for which a continuous reporting is requested. The absence of duration indicates a one-time reporting.	OA
networkStatus	0..1	RO	Congestion level for NSE. It could be defined as High, Medium, Low, and No congestion.	OA

8.6.4.1.2 Proposed Flow(s)

This clause describes the general procedure for network issue report service between oneM2M and 3GPP network.

8.6.4.1.2.1 Request procedure for one-time or continuous reporting of network status

This procedure is used by an oneM2M system to retrieve network status from the NSE. This procedure can be used to request a one-time or continuous reporting of network status. Figure 8.6.4.1.2.1-1 illustrates the procedure.

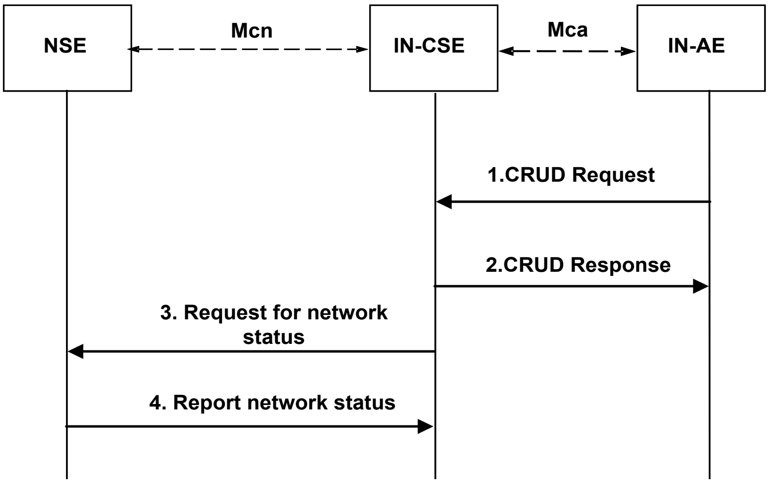


Figure 8.6.4.1.2.1-1: General procedure to support network status report between oneM2M and 3GPP network

Step-1: CRUD Request

AE can send CRUD Request to retrieve network status with providing Location Area, Duration, Threshold.

Step-2: CRUD Response

The IN-CSE sends a Response to the AE to acknowledge acceptance of the Request.

Step-3: Request for network status

The IN-CSE sends a Request message to the NSE including Location Area, Duration, Threshold. Duration indicates the time for which a continuous reporting is requested. The absence of Duration indicates a one-time reporting. The IN-CSE, based on operator policies, may chose a different Threshold value than the one indicated by the AE in step 1.

Step-4: Report network status

The NSE sends an one-time or continuous Report to the IN-CSE including depending on the operator configuration and current NSE knowledge, the congestion status for radio access network belonging to the Location Area requested by the IN-CSE.

8.6.4.1.2.2 Removal procedure for continuous reporting of network status

This procedure is used for termination of the continuous reporting of network status. It can be triggered by the AE at any time before the Duration is over. The IN-CSE will trigger this procedure when the Duration is over.
Figure 8.6.4.1.2.2-1 illustrates the procedure.

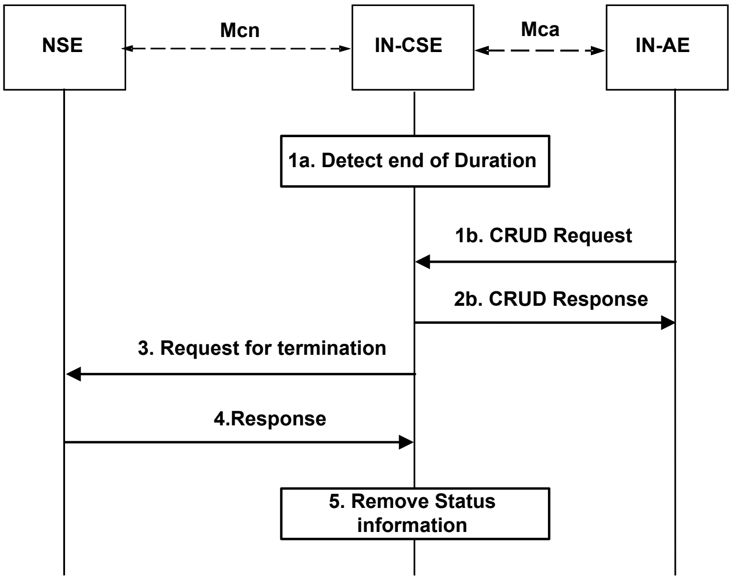

NSE
Mcn
IN-CSE
Mca
IN-AE
1a. Detect end of Duration
1b. CRUD Request
2b. CRUD Response
3. Request for termination
4.Response
5. Remove Status information

Figure 8.6.4.1.2.2-1: General procedure to support network status report between oneM2M and 3GPP network

Step-1a: Detect end of duration

The IN-CSE detects that the requested Duration for an ongoing continuous reporting of network status is over.

Step-1b: CRUD Request

When the AE needs to terminate an ongoing continuous reporting of network status, the AE sends a Request message to the IN-CSE.

Step-2b: CRUD Response

If the AE requested to terminate an ongoing continuous reporting of network status in step 1b, the IN-CSE sends a Response message to the AE.

Step-3: Request for termination

The IN-CSE sends a Request message to the NSE to an ongoing continuous reporting of network status.

Step-4: Response

The NSE removes the related instructions and stops monitoring the radio access network belonging to the Location Area for a change in the congestion status. Afterwards, the Response is sent to the IN-CSE.

Step-5: Remove status information

The IN-CSE removes all network status information related to this continuous reporting.

8.7 Control Plane Data Delivery

8.7.1 Description

3GPP Release 13 introduces the ability to send data to and from the UE in NAS messaging. 3GPP refers to this feature as "Control Plane (CP) CIoT Optimizations". Since no data plane set up is required when sending data to the MME/SGSN via NAS messaging, using CP CIoT optimizations results in a reduced total number of control plane messages that are required to send a short data transaction.

Control Plane (CP) CIoT Optimizations provide the UE with 3 new options for sending data to and from a remote server (IN-CSE / SCS).

- IP Data, via the P-GW
- Non-IP Data, via the P-GW
- Non-IP Data, via the SCEF

The ability to send data over the control plane is a mandatory feature NB-IoT UE's and an optional feature for WB-UE's. Figure 8.7.1-1 shows the 3 new control plane data paths alongside the existing data plane path.

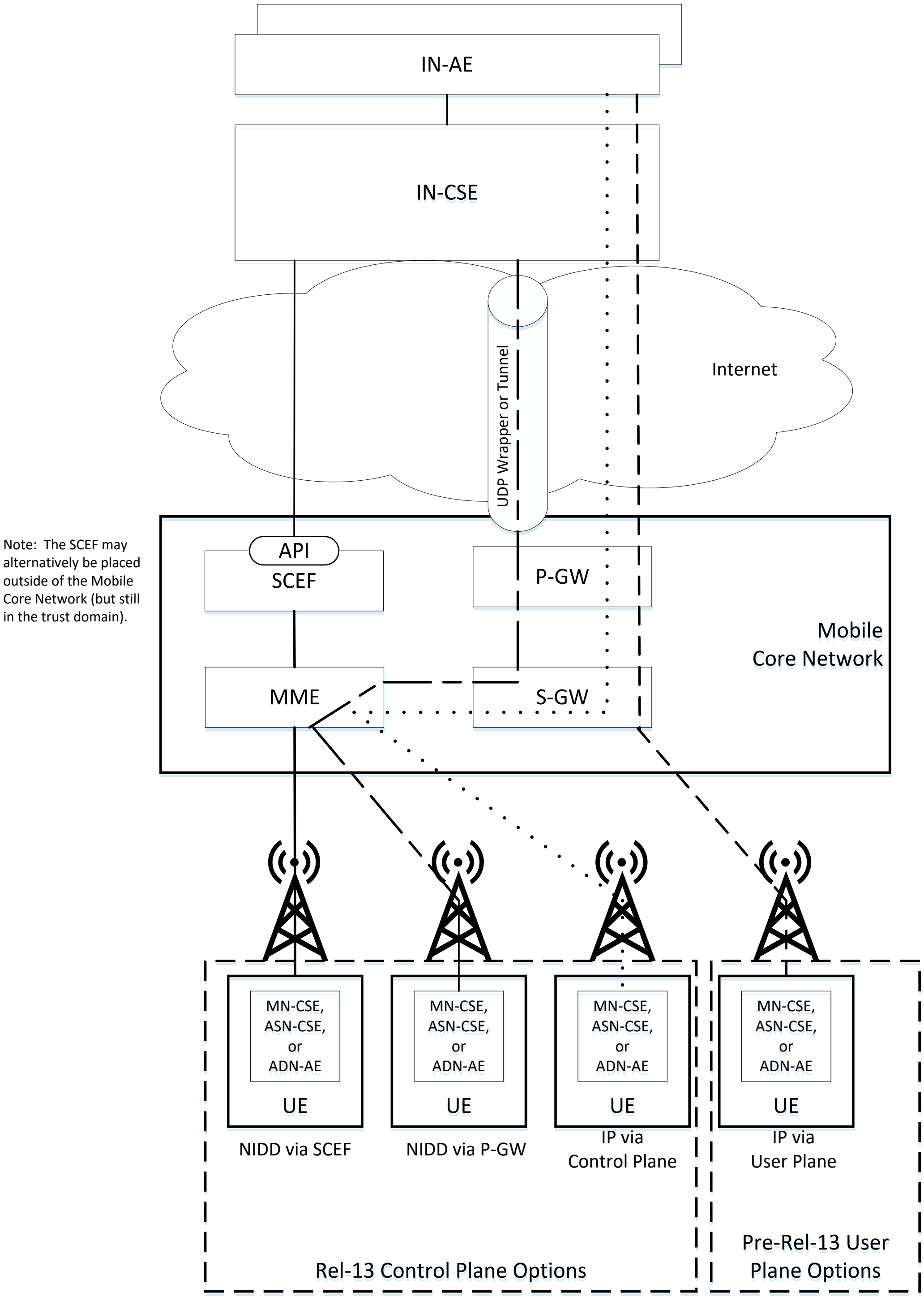


Figure 8.7.1-1 Small Data Delivery Options

When a PDN connection is established (e.g. in Attach or PDN Connectivity Request), the UE and Network determine which of the 4 paths shown in Figure 8.7.1-1 is used. In the Attach or PDN Connectivity Request, the UE indicates if the PDN type should be IP or non-IP and if the control plane should be used. The UE may also optionally indicate an APN name. If the UE does not provide an APN, the network will use the appropriate default APN from the UE's subscription. Note that the UE may have two default APN's in its subscription; a default IP APN and a default non-IP APN. When a non-IP APN is selected, the APN configuration will indicate if the PDN connection should be anchored at the SCEF or P-GW. Notice that the UE is not aware if its Non-IP PDN connection is anchored at the P-GW or the SCEF. However, the IN-CSE knows whether data is routed via the P-GW to the SCEF.

8.7.2 Feature Gap Analysis

8.7.2.1 Non-IP Data Delivery (NIDD)

8.7.2.1.1 Introduction

Non-IP data may be exchanged between the IN-CSE and the UE hosted MN-CSE, ADN-AE, or ASN-CSE. Non-IP data packets are opaque to the 3GPP Network; in other words, the 3GPP Network makes no assumptions of the contents or structure of the data packet. Non-IP data may be exchanged via the SCEF or the P-GW, depending on which node the UE's PDN Connection is anchored to.

> Note 1: The API's that are used to access the NIDD feature may be developed by standards organizations other than oneM2M (i.e. OMA). However, oneM2M still needs to develop a stage 3 specification to show how the Mcc and Mca reference points are bound to Non-IP. This binding is FFS.

Each Non-IP PDN connection has maximum packet size which is set by the 3GPP network. The SCEF or P-GW will signal the maximum packet size to the UE when the PDN connection is established. 3GPP does not define how the SCS (IN-CSE) knows the maximum packet size. The IN-CSE may be provisioned to know the maximum packet size for each APN or it may be signalled by the SCEF. Note that the maximum packet size may be as small as 128 bytes.

> Note 2: If the IN-CSE and UE hosted MN-CSE, ADN-AE, or ASN-CSE desire to exchange packets that are larger than 128 bytes, then segmentation and re-assembly will need to be performed in the IN-CSE and the UE hosted MN-CSE, ADN-AE, or ASN-CSE. It is for FFS how packet segmentation and re-assembly will be accomplished.

> Note 3: If the IN-CSE and UE hosted MN-CSE, ADN-AE, or ASN-CSE require some or all Non-IP data packets to be acknowledged, then it is for FFS how packets will be acknowledged.

Once a PDN connection is established, the UE hosted MN-CSE, ADN-AE, or ASN-CSE may use the PDN connection to send Non-IP data packets to the IN-CSE.

> Note 4: It is FFS what PoA is used by the UE hosted MN-CSE, ADN-AE, or ASN-CSE to reach the IN-CSE. The UE hosted MN-CSE, ADN-AE, or ASN-CSE should associate an APN with the IN-CSE; thus it is recommended that the PoA includes an APN.

Dedicated bearers are not supported for Non-IP data PDN connections and there is no concept of Port ID. Thus, a Non-IP PDN connection can only be associated with one IN-CSE to UE hosted MN-CSE, ADN-AE, or ASN-CSE connection. If one UE hosted MN-CSE, ADN-AE, or ASN-CSE needs to use NIDD to connect to more than one IN-CSE, then the UE needs to be provisioned with an APN for each connection. Separate PDN connections are used for each IN-CSE.

If more than one UE hosted MN-CSE, ADN-AE, or ASN-CSE uses NIDD to connect to the same IN-CSE, then each UE hosted MN-CSE, ADN-AE, or ASN-CSE needs to be associated with its own APN and to establish its own PDN connection.

8.7.2.1.2 Non-IP Data Delivery (NIDD) via the P-GW

8.7.2.1.2.1 Introduction

At each PDN connectivity request with PDN Type Non-IP, if the network finds that the APN configuration does not include an "Invoke SCEF selection indicator", then the P-GW option is used.

The P-GW decides at PDN connection establishment if Non-IP data should be sent via UDP or via a point-to-point tunneling technique between the P-GW and the AS. This information, as well as the tunnel parameters (i.e. IN-CSE IP address and port and source IP address and port) are pre-configured at the P-GW. The configuration is on a per-APN per-UE basis.

Once a PDN connection is established, the IN-CSE may use the PDN connection to send Non-IP data packets to the UE hosted MN-CSE, ADN-AE, or ASN-CSE. When Non-IP data is routed via the P-GW, the PoA that is associated with the UE hosted MN-CSE, ADN-AE, or ASN-CSE is an IP Address and Port number. The IP Address and Port number is used to route the Non-IP data packets to the 3GPP Network via the P-GW. The Non-IP packets may be tunneled or wrapped in a UDP packet. The P-GW will use the IP Address and Port Number to determine what UE and APN the packet is associated with.

> Note 1: It is FFS how the IN-CSE learns the IP Address and Port Number that is used to reach the UE hosted MN-CSE, ADN-AE, or ASN-CSE. The IP Address and Port Number may be provisioned in the IN-CSE per SLA or the IN-CSE may wait for the UE hosted MN-CSE, ADN-AE, or ASN-CSE to initiate contact and learn the IP Address and port number when the first Non-IP packet is received (i.e. by looking at the source IP Address and port of the UDP wrapper or tunnel). The IP address used by IN-CSE to reach the UE hosted MN-CSE, ADN-AE or ASN-CSE needs to provide routing through the same PGW as the one indicated by the APN configuration in the UE.

8.7.2.1.2.2 Mobile Originated NIDD procedure via the P-GW

Figure8.7.2.1.2.2-1 illustrates the procedure used by UE to send non-IP data to the IN-CSE via the P-GW.

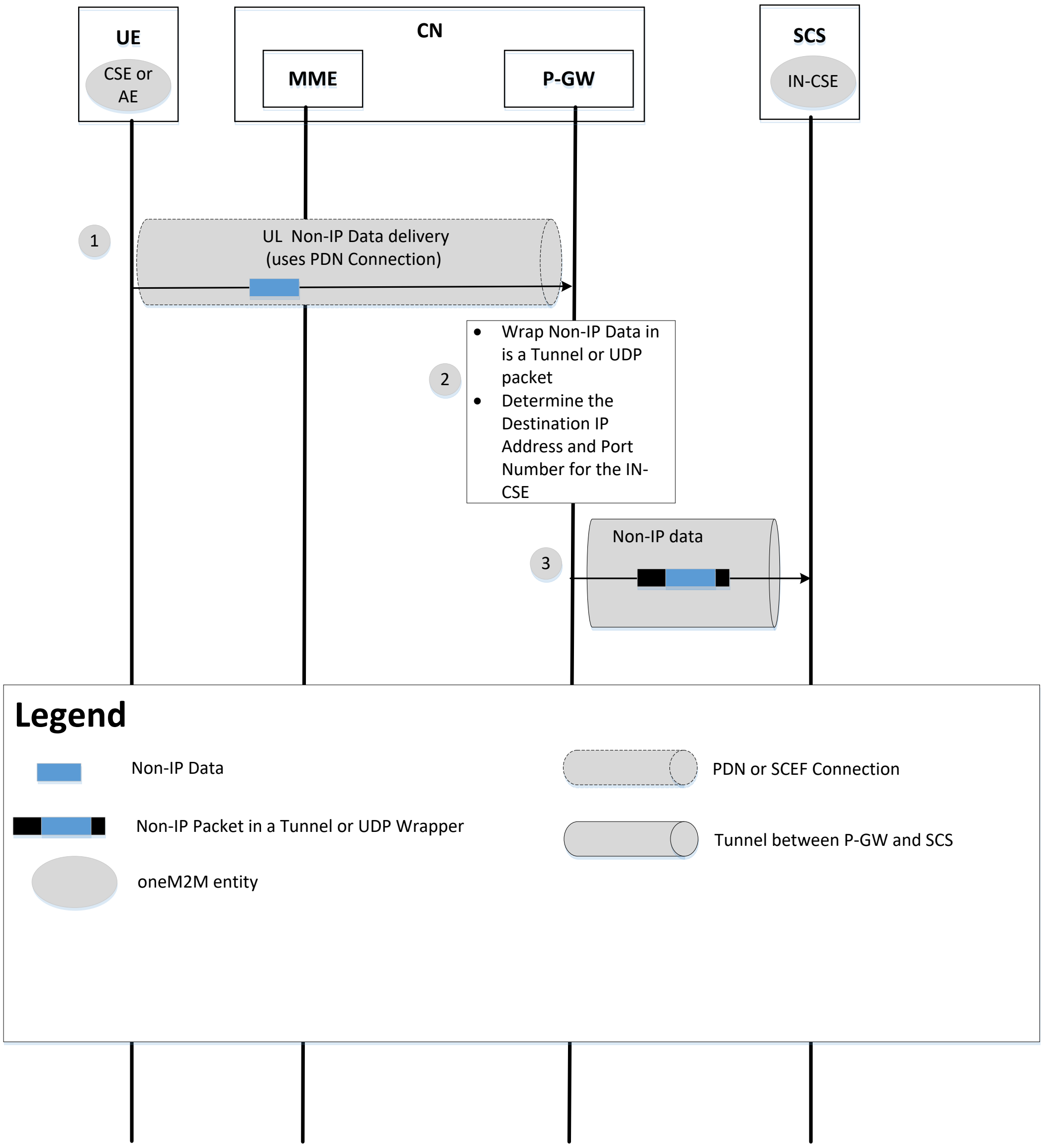

UE
CSE or AE
CN
MME
P-GW
SCS
IN-CSE
1
UL Non-IP Data delivery (uses PDN Connection)
2
Wrap Non-IP Data in is a Tunnel or UDP packet
Determine the Destination IP Address and Port Number for the IN-CSE
3
Non-IP data
Legend
Non-IP Data
Non-IP Packet in a Tunnel or UDP Wrapper
oneM2M entity
PDN or SCEF Connection
Tunnel between P-GW and SCS

Figure 8.7.2.1.2.2-1 MO NIDD procedure via P-GW

1. The UE sends a Non-IP data packet to the IN-CSE. The UE knows the target IN-CSE because it is associated with the APN and PDN Connection.

2. The P-GW wraps the non-IP data in a UDP wrapper or tunnels it to the IN-CSE using the pre-configured destination and source IP address and UDP port number.

3. The P-GW forwards the wrapped or tunnelled packet to the IN-CSE. The IN-CSE unwraps the received data and may note the source IP address and port number for further communications with the UE.

8.7.2.1.2.3 Mobile Terminated NIDD procedure via the P-GW

Figure 8.7.2.1.2.3-1 illustrates the procedure used by an IN-CSE to send non-IP data to a UE via the P-GW.

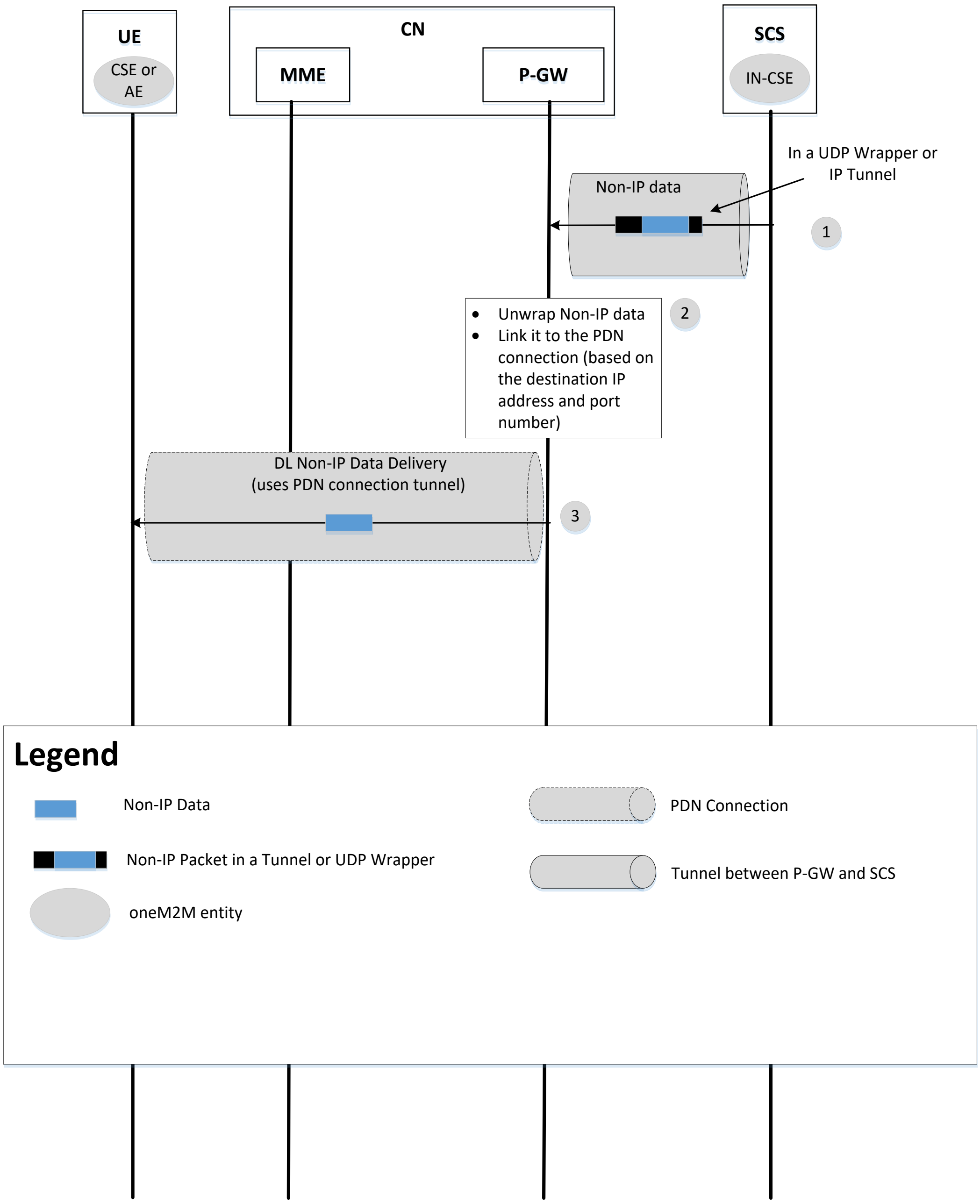

UE
CSE or AE
CN
MME
P-GW
SCS
IN-CSE
In a UDP Wrapper or IP Tunnel
Non-IP data
1
2
Unwrap Non-IP data
Link it to the PDN connection (based on the destination IP address and port number)
DL Non-IP Data Delivery
(uses PDN connection tunnel)
3
Legend
Non-IP Data
Non-IP Packet in a Tunnel or UDP Wrapper
oneM2M entity
PDN Connection
Tunnel between P-GW and SCS

Figure 8.7.2.1.2.3-1 MT NIDD procedure via P-GW

1. The IN-CSE sends a data packet (wrapped in UDP packet or tunnelled) to the PoA that is associated with the UE hosted MN-CSE, ADN-AE, or ASN-CSE (the PoA will be an IP address and port number).

2. The P-GW extracts the Non-IP data packet and uses the destination IP Address and Port Number to identify the UE is that is being addressed and the PDN connection.

3. The P-GW forwards the non-IP data to the UE. The UE identifies the source IN-CSE based on the APN that is associated with the PDN connection that used to receive the Non-IP data packet.

   Note 1: MT flows for both IP and non IP flow for devices that uses PSM and eDRX need to be specified. It is FFS as how to handle unreachable situation within oneM2M system.

8.7.2.1.3 Non-IP Data Delivery (NIDD) via the SCEF

8.7.2.1.3.1 Introduction

In TS 23.682, 3GPP defines an optional NIDD Configuration procedure that may be used by the IN-CSE to inform the SCEF that it expects Non-IP Data from a UE; the UE is identified with an External ID or MSISDN. The SCEF will send the UE identity and APN to the HSS to check that the SCEF is authorized to receive data from the UE / APN combination. Alternatively, the SCEF could be provisioned to know what UE / APN combinations will be anchored to it.

When the UE makes a PDN connectivity request with PDN Type Non-IP, if the APN configuration includes an "Invoke SCEF selection indicator" and an SCEF Identifier, then the SCEF routing option is used. A connection between the MME/SGSN and SCEF will be established when the PDN connection is established.

An API will be used by the SCEF and IN-CSE to exchange Non-IP data packets. When the IN-CSE sends a Non-IP packet to the SCEF it includes a UE identifier (e.g. External ID or MSISDN) and an APN. The combination UE/APN maps to a MN-CSE, ADN-AE, or ASN-CSE that is hosted on the UE.

Once a PDN connection is established, the IN-CSE may use the PDN connection to send Non-IP data packets to the UE hosted MN-CSE, ADN-AE, or ASN-CSE. When Non-IP data is routed via the SCEF, the PoA that is associated with the UE hosted MN-CSE, ADN-AE, or ASN-CSE is a UE Identity (e.g. External ID), APN, and SCEF ID combination. The SCEF will use the UE Identity and APN to determine what MME the Non-IP packet should be sent to and what EPS Bearer ID (EBI) that is associated with the UE.

Note 1: It is FFS how the IN-CSE learns the APN and UE Identity that is used to reach the UE hosted MN-CSE, ADN-AE, or ASN-CSE. This information may be provisioned in the IN-CSE per SLA. If there is only one MTC application that is hosted on the UE using Non-IP data, then the IN-CSE does not need to be aware of the APN.

8.7.2.1.3.2 SCEF Configuration for NIDD

Figure 8.7.2.1.3.2-1 illustrates a procedure through which the IN-CSE may configure the SCEF for future NIDD. This procedure is optional as the parameters may be pre-provisioned at the SCEF. The purpose is to provide the SCEF with information needed for non-IP communication between a specific AS and a specific UE. 3GPP aspects of the procedure are described in [i.16]. It is assumed that this procedure occurs prior to the UE's attachment to the network. If, at UE attachment, the SCEF has not been configured for NIDD with this procedure or by pre-provisioning, the SCEF may initiate the procedure or the SCEF may reject the PDN connection attempt.

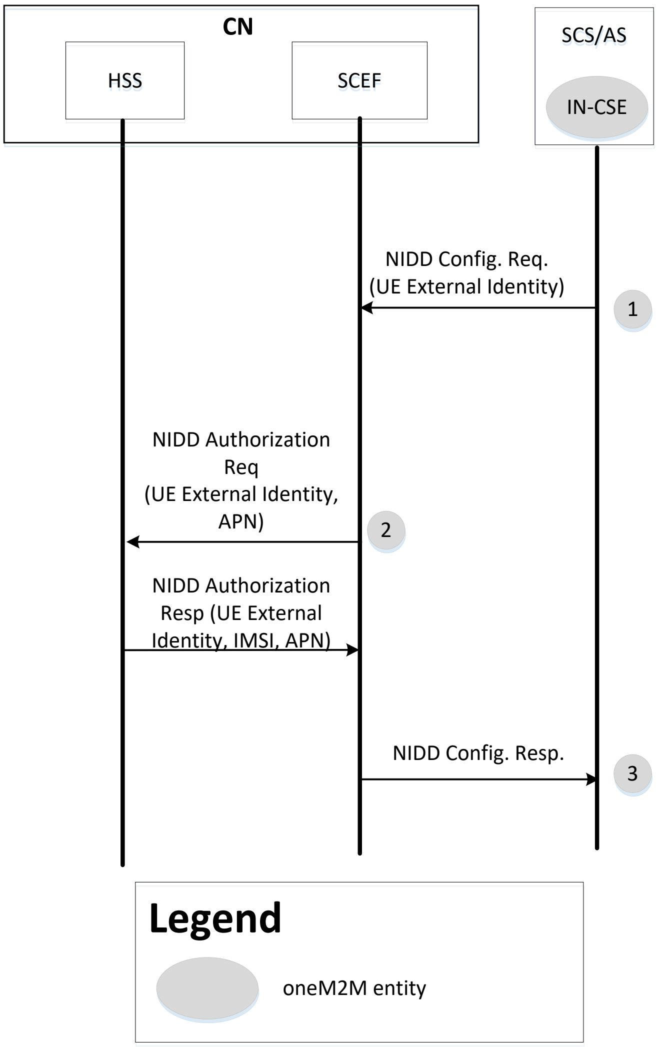


Figure 8.7.2.1.3.2-1 NIDD Configuration procedure at the SCEF

Note 1: Interactions within the 3GPP network are shown for informative purposes only, they are out of scope of oneM2M.

1. The IN-CSE sends an NIDD Configuration Request message to the SCEF. This step will be accomplished via an SCEF API call. The step is fully explained in TS 23.682, however the purpose of the procedure is to configure the SCEF to know that the IN-CSE is expecting Non-IP Data from the UE and for the SCEF to authorize it.

Note 2: Based on TS23.401 clause 4.3.17.8.3.2, when UE attaches “a PDN connection is established towards the selected SCEF”, which implies that more than one SCEF may be selected for each UE “. Based on 23.682 clauses 5.13.1 and 5.13.2 the SCEF connection to be established e.g. at UE attached relies upon a SCEF configuration procedure to be accomplished. This means that the IN-CSE is expected to be provisioned to use the same SCEF (for a specific UE) as the one selected by the network during the UE's attachment to the network.

2. The SCEF stores the UE Identity (External Identifier or MSISDN) and IN-CSE Identifier. The SCEF also authorizes the NIDD configuration request (for the received UE Identifier and APN combination) and obtains the UE’s IMSI.

3. The SCEF sends an NIDD Configuration Response message to the IN-CSE to acknowledge acceptance of the NIDD Configuration Request. This step is in response to API call of step 1.

Later, when the UE establishes the PDN Connection with the same APN, the UE's MME will contact the SCEF and perform a T6a establishment procedure. T6a refers to the reference point between the MME and SCEF. The procedure is used by the MME to provide the SCEF with an IMSI, EBI, and APN combination and it is used by the SCEF to provide the MME with the maximum Non-IP packet size. The IMSI, EBI, and APN will be needed by the SCEF when routing Non-IP Data between the IN-CSE and UE.

8.7.2.1.3.3 Mobile Terminated NIDD Procedure via the SCEF

Figure 8.7.2.1.3.3-1 illustrates the procedure used by an IN-CSE to send non-IP data to a UE via the SCEF, which assumes that the SCEF configuration procedure is completed.

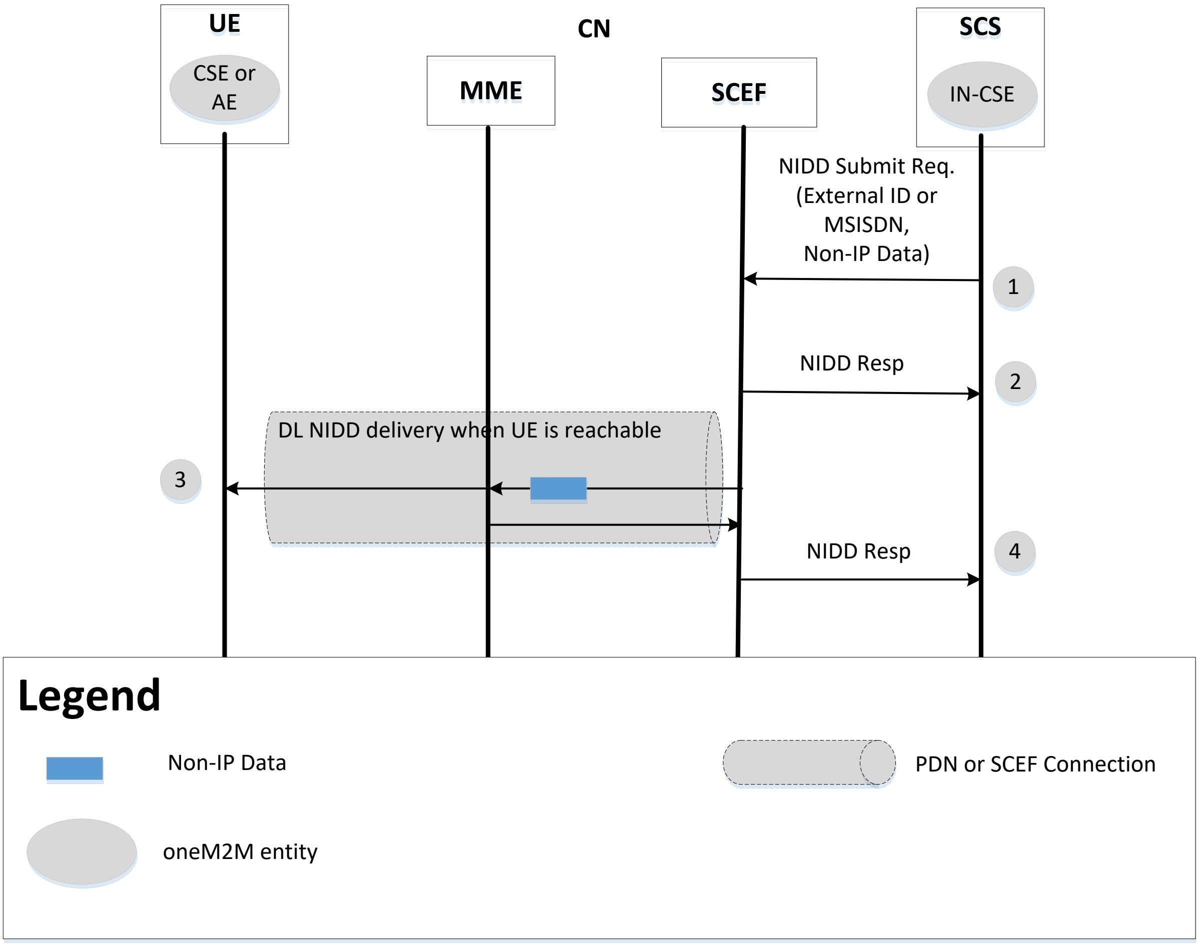


Figure 8.7.2.1.3.3-1 MT NIDD procedure via SCEF

1. The IN-CSE initiates the MT NIDD procedure by sending a Non-IP data packet towards the SCEF. A UE Identity (e.g. External ID), APN, and SCEF ID combination is used as the UE's PoA. This step will be accomplished via an SCEF API call.

   Optionally, if the UE is not reachable (i.e. in a deep sleep mode due to PSM or eDRX), the SCEF may respond to the IN-CSE that the UE is not reachable and indicate if the data is buffered or discarded. This step is in response to API call of step 1.

   Note 1: If the IN-CSE relies upon reachability monitoring to submit NIDD requests, the number of messages between the IN-CSE and SCEF would triple. It should be clarified if NIDD data buffering is supported by SCEF and how to provide configuration parameters, e.g. buffer size.

2. The MME uses the PDN connection to deliver the Non-IP data to the UE.

3. The SCEF indicates to the IN-CSE that the non-IP data packet was delivered. This step is in response to API call of step 1.

Note 2: The MT NIDD procedure cannot be executed on a group basis. The group message feature that is exposed by the SCEF relies on MBMS. When distributing the same non-IP data to a group of devices, the SCS/AS executes the MT NIDD procedure for each UE in the group, unless all UE's in the group support MBMS.

8.7.2.1.3.4 Mobile Originated NIDD Procedure via the SCEF

Figure 8.7.2.1.3.4-1 illustrates the procedure used by UE to send non-IP data to the IN-CSE via the SCEF.

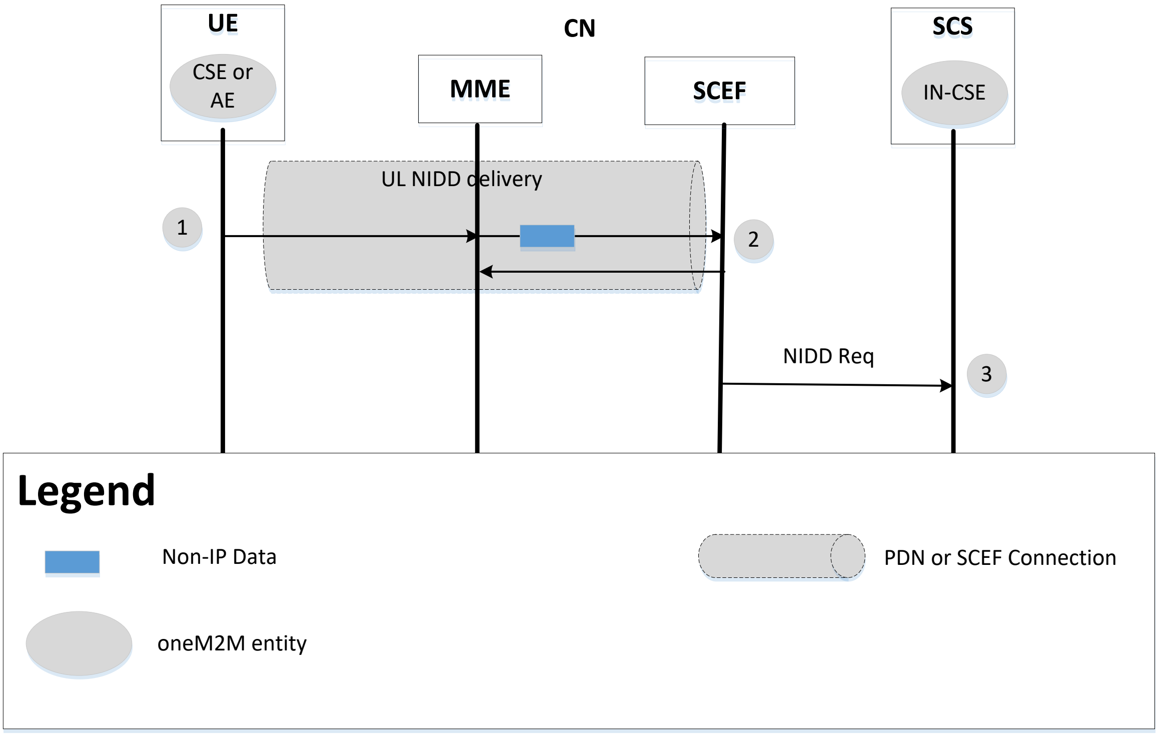


Figure 8.7.2.1.3.4-1 MO NIDD procedure via SCEF

1. The UE Hosted MN-CSE, ADN-AE, or ASN-CSE initiates UL NIDD procedures by sending non-IP data using the PDN connection. The target IN-CSE is identified based on the APN that is associated with the PDN connection.
2. The MME sends the Non-IP data packet, EBI, and IMSI to the SCEF. The SCEF uses the EBI and IMSI to determine the UE's External Identifier, APN, and the associated IN-CSE.
3. The SCEF sends the Non-IP Data, UE Identity (External ID or MSISDN), and APN to the IN-CSE.

8.7.2.2 IP Data Delivery via the Control Plane

When IP data is received at the IN-CSE, the IN-CSE is not aware of whether the UE sent the data to the eNodeB via the user or control plane. The UE Hosted MN-CSE, ADN-AE, or ASN-CSE is also largely unaware of whether its IP data is using the control plane or user plane path. However, some entity on the UE, such as the UE Hosted MN-CSE, ADN-AE, or ASN-CSE may need to indicate whether the PDN connection is better suited for the control or user plane.

8.7.3 Key Issues and Requirements

8.7.3.1 Key SCEF Northbound API Requirements

To enable the Service Layer to use NIDD the following functionality is required:

Number	Description	Notes
REQ-8.7-01	Support for SCEF configuration for NIDD procedure via SCEF	See clause 8.7.2.1.3.2
REQ-8.7-02	Support for NIDD submit request/response procedure for MT NIDD via SCEF	See clause 8.7.2.1.3.3
REQ-8.7-03	Support for NIDD submit request/response procedure for MT NIDD to a group or list of devices which is provided in the request.	See clause 8.7.2.1.3.3
REQ-8.7-04	Support for SCEF notification of MO NIDD.	See clause 8.7.2.1.3.4
REQ-8.7-05	In the case of MT NIDD for a group of devices, support for indication of NIDD receipt for each of the members of the group.	
REQ-8.7-06	Support for SCS/IN-CSE configuration of NIDD buffering in the network.	See Note 1 clause 8.7.2.1.3.3
REQ-8.7-07	Support for segmentation and re-assembly for NIDD.	See Note 2 clause 8.7.2.1.1
REQ-8.7-08	Support for optional acknowledgments for NIDD packet reception for MT cases.	See Note 3 clause 8.7.2.1.1
REQ-8.7-09	Support for identifying the UE Application (ASN/MN-CSE or ADN-AE) that is to receive the MT non-IP packet.	See clause 8.7.2.1.3.3
REQ-8.7-10	Support for identifying the SCS/AS that is to receive the MO non-IP packet.	See clause 8.7.2.1.3.4
REQ-8.7-11	Support for MTU discovery by SCS/AS	

8.7.3.2 Possible impacts on the SCEF Southbound Interface

Number	Description	Notes
IMPACT-8.7-01	Possible need for NIDD header pertaining to the UE application to receive MT NIDD packet.	See clause 8.7.2.1.3.3

8.7.3.3 Further 3GPP requirements and clarifications

Number	Description	Notes
ISSUE-8.7-01	For NIDD via P-GW: how does the SCS/AS learn the IP Address used to reach the UE hosted Service Layer such that the MT NIDD is routed to the UE via the P-GW	See Note 1 clause 8.7.2.1.2.1
ISSUE -8.7-02	If there are more than one SCEFs in the network, how does the SCS/AS (IN-CSE) discover and select the SCEF for a given UE?	See Note 2 clause 8.7.2.1.3.2
ISSUE -8.7-03	For NIDD via P-GW: NIDD MT flows for devices in PSM mode should be clarified.	See Note 1 clause 8.7.2.1.2.3
ISSUE -8.7-04	It should be clarified if and how acknowledgement for MO NIDD packet delivery is supported.	

8.7.3.4. oneM2M Key Issues

Provide support for use of Control Plane Data Delivery feature.

8.8 Monitoring event (Monitoring Type: UE reachability)

8.8.1 Description

The Network Service Exposure, Service Execution and Triggering (NSSE) CSF manages communications with the Underlying Networks for accessing network service functions over the Mcn reference point. When receiving downlink message from other CSFs and AEs to ADN/ASN/MN via 3GPP network, the NSSE CSF need get the UE reachability status from 3GPP network which is ADN/ASN/MN hosted before transferring the message. 3GPP support Monitoring Events feature to monitor specified events in 3GPP system to SCS/AS via SCEF, such as UE reachability.

The NSSE CSF is able to utilize this service to be notified when the UE becomes reachable for sending either SMS or downlink data to the UE. At the same time, the NSSE CSF could expose the UE reachability to other CSFs and AEs in Mcc and Mca reference point.

The NSSE CSF relies on the SCEF to provide functionality such as: configuring, detecting and reporting UE reachability event, configuring and monitoring UE sleep cycles, monitoring UE Idle Status, configuring Network Buffer Size, etc.

8.8.2 Feature Gap Analysis

8.8.2.1 PSM and eDRX timers

The IN-CSE can manage the underlying application and transport layer retransmission timers when it is communicating with an ASN/MN-CSE or ADN-AE that is hosted on a UE. This section addresses cases when S-GW buffering is enabled and when it is not enabled.

3GPP SA2 has defined power saving mode (PSM) and eDRX in order to reduce the power consumption for constrained M2M/IoT devices (i.e., UE in 3GPP) in [1]. When a UE is in deep sleep due to eDRX or PSM, it is not reachable for mobile terminated (MT) communication, in other words it is not able to receive the downlink traffic.

3GPP SA2 has also defined an Extended Buffering mechanism to buffer downlink (i.e., MT) traffic when a UE is not reachable. When the extended buffering feature is enabled, the S-GW will buffer the downlink traffic for a UE based on parameters, such as:

Maximum latency: can be used to configure how long a UE sleeps. It is defined in TS 23.682 as "*Optionally, Maximum Latency indicating maximum delay acceptable for downlink data transfers. Maximum Latency is used for setting the periodic TAU/RAU timer for the UE as it sets the maximum period after which a UE has to connect to the network again and thereby becomes reachable. Determined by the operator, low values for Maximum Latency may deactivate PSM.*"

Maximum Response Time: can be used to configure how long a UE stays reachable when it comes out of deep sleep. It is defined in TS 23.682 as "*Optionally, Maximum Response Time indicating the time for which the UE stays reachable to allow the SCS/AS to reliably deliver the required downlink data. Maximum Response Time is used for setting the Active Time for the UE. When the UE uses extended idle mode DRX, the Maximum Response Time is used to determine how early this monitoring event should be reported to the SCS/AS before the next Paging Occasion occurs*."

Suggested number of downlink packets: can be used to configure how many packets can be buffered for a UE. It is defined in TS 23.682 as "*Optionally, Suggested number of downlink packets indicating the number of packets that the Serving Gateway shall buffer in case the UE is not reachable*."

Active Time value (T3324): can be used to configure how long the UE maintains idle status when transitioning from ECM_CONNECTED to ECM_IDLE**.** It's suggested in TS23.682 as *"The Maximum Response Time value can be configured as desired Active Time value in the HSS"*

TAU/RAU Timer (T3412): can be used to configure the maximum period after which a UE has to connect to the network again and thereby becomes reachable. It's suggested in TS23.682 as" *Maximum Latency is used for setting the periodic TAU/RAU timer for the UE*"

3GPP TS 23.682 (v13.5.0) specifies that the above parameters are configured by the SCS/AS via the SCEF so that MME and S-GW know that the feature is enabled, how to configure the UE's sleep cycle, and how many packets to buffer. Note that the parameters that are provided by the SCEF are only guidance for the mobile core network. For example, the MME is not required to set Maximum Response Time equal to the UE's Active Time; local policies may dictate that the MME do otherwise.

8.8.2.2 Monitoring event configuration and deletion procedure (UE reachability)

The 3GPP defined term 'SCS' in the flows corresponds to oneM2M IN-CSE.

The service flows defined in 3GPP TS23.682 are used in the following section as informative information only. oneM2M focus is on the northbound APIs of SCEF.

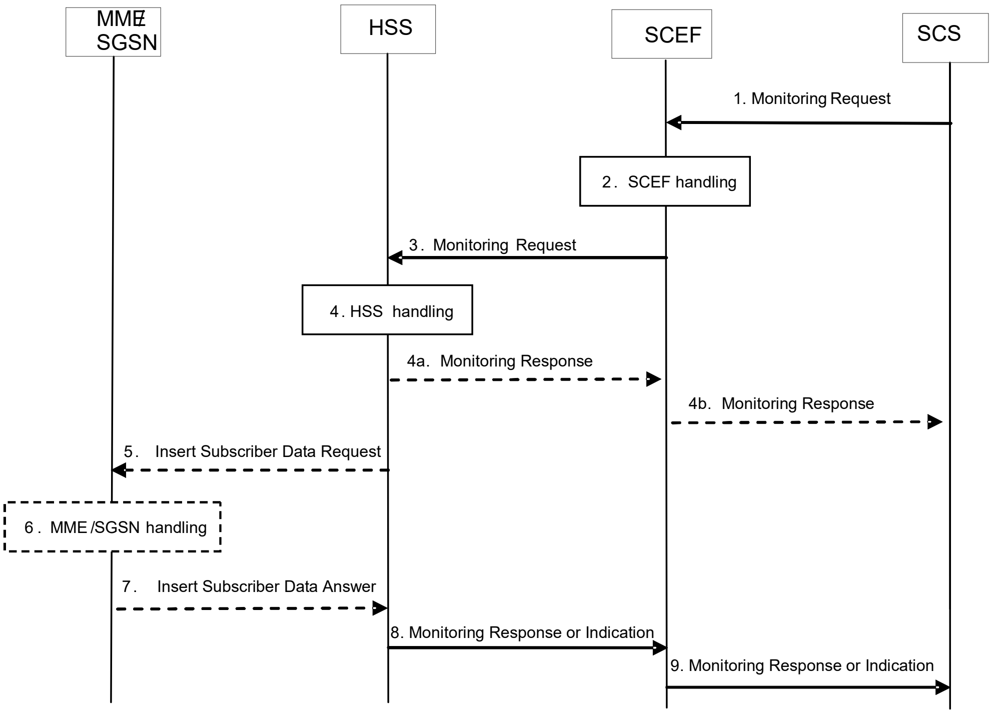


Figure 8.8.2.2-1: Monitoring event configuration and deletion via HSS procedure

Figure 8.8.2.2-1illustrates the procedure of configuring monitoring at the HSS or the MME/SGSN. The involved SCEF northbound APIs are as below:

Step1 SCS(IN-CSE) sends Monitoring Request (External Identifier(s) or MSISDN(s) or External Group ID, SCS/AS Identifier, SCS/AS Reference ID, Monitoring Type, Maximum Number of Reports, Monitoring Duration, Monitoring Destination Address, SCS/AS Reference ID for Deletion, Group Reporting Guard Time, Reachability Type, Maximum Latency, Maximum Response Time, Suggested number of downlink packets) to SCEF.

Step 4b SCEF sends Monitoring Response () to SCS (IN-CSE).

Step 9 SCEF sends Monitoring Response (SCS/AS Reference ID, Cause) to SCS (IN-CSE) for single UE.

SCEF sends Monitoring Indication () to SCS (IN-CSE) for group of UEs

There are some gaps for the SCEF northbound APIs.

- Step1: In TS23682, the parameter *Maximum Response Time* of Monitoring Request means the time for which the UE stays reachable to allow the SCS/AS to reliably deliver the required downlink data. And 3GPP suggest to "*Maximum Response Time is used for setting the Active Time for the UE in clause* 5.6.1.4" and "*The Maximum Response Time value can be configured as desired Active Time value in the HSS via O&M in clause* 4.5.4.". For

UE reachability is explained as “UE reachability indicates when the UE becomes reachable for sending either SMS or downlink data to the UE, which is detected when the UE transitions to ECM_CONNECTED mode”. The Active Time (T3324) is defined in TS24008 as “In S1 mode, timer T3324 is reset and started with its initial value, when the MS changes from EMM-CONNECTED mode to EMM-IDLE mode.” So there is time gap for the two parameters when UE stays in connected status.

- Step 4b: this step is used to indicate that Group processing is in progress from SCEF to SCS. But there is no parameter defined.
- Step 9: For group based processing, SCEF may send the Monitor Indication to the SCS. But there is no parameter defined.

8.8.2.3 Monitoring event reporting procedure

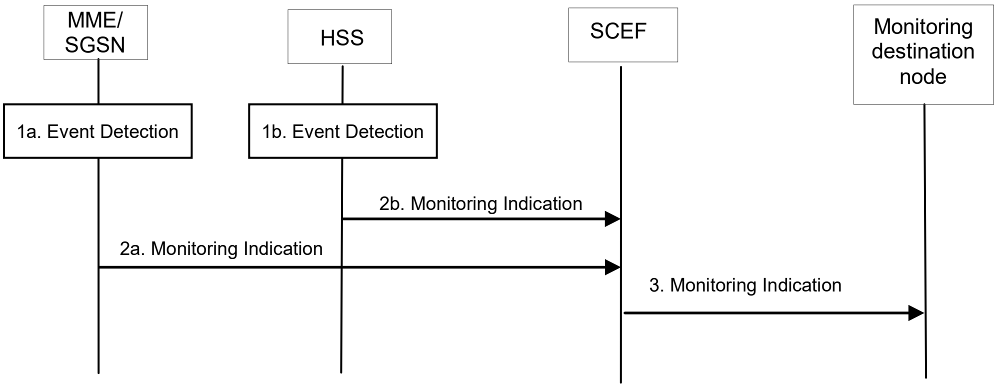

MME/
SGSN
HSS
SCEF
Monitoring destination node
1a. Event Detection
1b. Event Detection
2b. Monitoring Indication
2a. Monitoring Indication
3. Monitoring Indication

Figure 8.8.2.3-1: Monitoring event reporting procedure via HSS or MME

Figure 8.8.2.3-1 illustrates the common procedure flow of reporting Monitoring Events that are detected by the MME/SGSN or HSS. The Monitoring destination node should be IN-CSE in oneM2M perspective. The involved SCEF northbound APIs are as below:

Step 3 SCEF sends Monitoring Indication (SCS/AS Reference ID, External ID or MSISDN, Monitoring Information) for single UE to the Monitoring destination node (IN-CSE).

SCEF sends Monitoring Indication (SCS/AS Reference ID, External Group Identifier, External ID(s) or MSISDN(s), Monitoring Information) for group of UEs Monitoring destination node (IN-CSE).

There is one gap for the SCEF northbound APIs.

- Step 3, the parameter *Monitoring Information* is not specified.

8.8.2.4 Managing Retransmission Timers when Communicating with Sleeping Nodes

oneM2M has the resource <schedule> which contains scheduling information. The ADN-AE, MN-CSE, or an ASN-CSE that is hosted on a UE use this resource to indicate the access timer.

- A child <*schedule*> resource of the <*CSEBase*> and <*remoteCSE*> resources indicates the time periods when the CSE can send and receive the request.
- A child <*schedule*> resource of the <*AE*> resource indicates the time periods when the application of a node can be accessed.

The scheduleElement attribute of <schedule> represents the list of scheduled execution times. Each entry of the scheduleElement attribute consists of a line with 7 field values. The <schedule> resource is shown in the Table 1.

Table 8.8.2.4-1: Definition of m2m:scheduleEntry string format

Field Name	Range of values	Note
Second	0 to 59	
Minute	0 to 59	
Hour	0 to 23	
Day of the month	1 to 31	
Month of the year	1 to 12	
Day of the week	0 to 6	0 means Sunday
Year	20000 to 9999	

The <schedule> resource is used for the application layer to get the ASN/ADN/MN node status, which is similar with 3GPP above three timers.

An issue may arise from the fact that power saving intervals may be quite long, e.g. several days, and do not match with the re-transmission timer set by the application.

CoAP/UDP/IP protocols are widely applied in the MTC world. They have some parameters related to delay with default values defined, i.e. ACK_TIMEOUT (2 seconds), ACK_RANDOM_FACTOR (1.5) and MAX_RETRANSMIT (4). The maximum time from the first transmission of message to the time when the server gives up on receiving an acknowledgement is calculated with a formula: ACK_TIMEOUT * ((2 ** (MAX_RETRANSMIT + 1)) - 1) *ACK_RANDOM_FACTOR, which by applying default values of the parameters is equal to 93 seconds.

Other protocols used by MTC applications, such as MQTT/XMPP, rely on the re-transmission mechanism in TCP for reliable transmission, by default the initial SYN packet will be repeated 3 times.

If protocols such as CoAP or TCP are used and retransmission timers are small, the sleep period may not be set for a very long period, because the retransmission schemes in application/transport protocols are not designed to wait for such long time periods for a response message. On the other hand, if the sleep period is designed to be only several seconds, it seems this would violate the original intention to introduce PSM, i.e. saving the power consumption of the UE.

Issue 1: If the sleep time is larger than the retransmission timer, then the underlying application or transport layer protocols of the IN-CSE will send multiple retransmissions to the UE while it is sleeping. On the other hand, if the sleep time (Maximum Latency) is smaller than the retransmission timer, it may effectively disable the use of deep sleep modes or make the use of deep sleep inefficient.

In case that there is no buffering mechanism applied in the 3GPP network and the UE is in deep sleep, the IN-CSE may attempt to send data to the UE and the underlying application or transport layer protocol will retransmit the packet many times because it does not receive an ACK. The initial transmission and the retransmissions will be dropped.

In case where S-GW buffering is applied in 3GPP network and the UE is in deep sleep, the IN-CSE may attempt to send data to the UE but the underlying application or transport layer protocol will retransmit the packet many times because it will not receive an ACK. Depending on how “Suggested number of downlink packets” is set, the retransmitted packets may all end up in the buffer and will all be sent to the UE when it comes out of deep sleep.

Issue 2: Depending on how the S-GW buffer is configured, duplicate packets may be buffered and sent to the UE when it wakes up.

エラー! 参照元が見つかりません。 Figure 8.8.2.4-1illustrates the inefficient buffering and retransmission process due to the lack of coordination between the 3GPP network and the underlying application or transport layer retransmission timers. Specifically, IN-CSE may retransmit several times since it is not aware that UE is in deep sleep for a long time. In case that the buffering is enabled, S-GW will forward multiple duplicate MT data packets it buffered to UE once UE wakes up and becomes reachable. If the buffering is NOT enabled, all the data packets are dropped at S-GW, and UE won’t get any MT data.

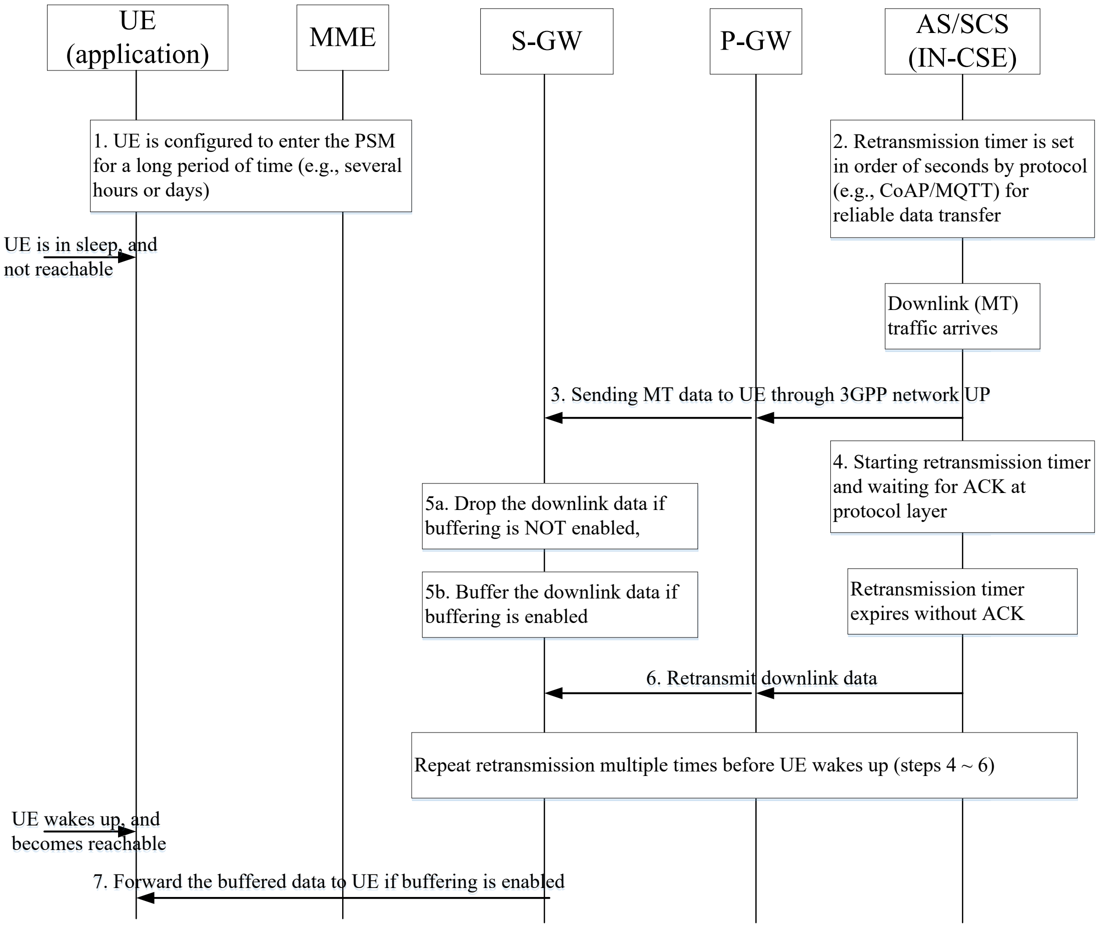

UE (application)
MME
S-GW
P-GW
AS/SCS (IN-CSE)
1. UE is configured to enter the PSM for a long period of time (e.g., several hours or days)
2. Retransmission timer is set in order of seconds by protocol (e.g., CoAP/MQTT) for reliable data transfer
UE is in sleep, and not reachable
Downlink (MT) traffic arrives
3. Sending MT data to UE through 3GPP network UP
4. Starting retransmission timer and waiting for ACK at protocol layer
5a. Drop the downlink data if buffering is NOT enabled,
5b. Buffer the downlink data if buffering is enabled
Retransmission timer expires without ACK
6. Retransmit downlink data
Repeat retransmission multiple times before UE wakes up (steps 4 ~ 6)
UE wakes up, and becomes reachable
7. Forward the buffered data to UE if buffering is enabled

Figure 8.8.2.4-1: Inefficient Buffering and Underlying Application or Transport Layer Retransmission mechanism

For cases where the IN-CSE is assumed to know, based on application layer signaling, when then UE is sleeping and it is unlikely that the IN-CSE will send data when the UE is sleeping, the IN-CSE should ensure that "Suggested number of downlink packets" is set to 1 so that the UE does not receive duplicate copies of the same packet. Although protocols such as CoAP and TCP can detect and discard duplicate packets, it is inefficient to send multiple packets on the UE's air interface. In this scenario, where "Suggested number of downlink packets" is set to 1, the IN-CSE should also ensure that multiple packets are not allowed to be in simultaneously in transmit towards the UE.

For cases where it cannot be assumed that the IN-CSE knows when then UE is sleeping, the IN-CSE should use the SCEF to determine when the UE is sleeping and when it is awake, so that underlying application or transport layer retransmission timers can be adjusted. For example, a reachability event notification from the SCEF (as defined in section 5.6.1.4 of TS 23.682) could be used as an indication to the IN-CSE that the UE is not in deep sleep and that a relatively small retransmission timer value can be used. When the IN-CSE has not been in communication for a relatively long period of time, a longer retransmission timer value, based on the UE's sleep time, can be used. By configuring "Suggested number of downlink packets" to a larger value and allowing multiple (different) packets to be in transit to the UE at the same time, the IN-CSE can ensure that larger amounts of data can be sent during sleep and will be received by the UE when it wakes up.

Issue 3: <schedule> of UE conflicts with PSM related timers, and may interrupt the UE PSM.

In UE PSM as shown in Figure 8.8.2.4-2, the red pillar means the US is in connected status, the black rectangle means the UE is in Idle State and the grey part means UE is in PSM.

The Active timer value should indicate the time for which the UE stays Idle State.

The monitor Report of UE reachability from MME to SCS, the start time should be from when the UE becomes connected. But how long UE stays in connected status depends on if there is a UE mobile originated event like data transfer or signaling and is not fixed. This means that the time which UE stays reachable is not fixed. If the Active Time value is equal the Maximum Response Time, then in the figure below, step 6, when the IN-CSE receives a reachability report, the UE is still reachable even after Maximum Response Time.

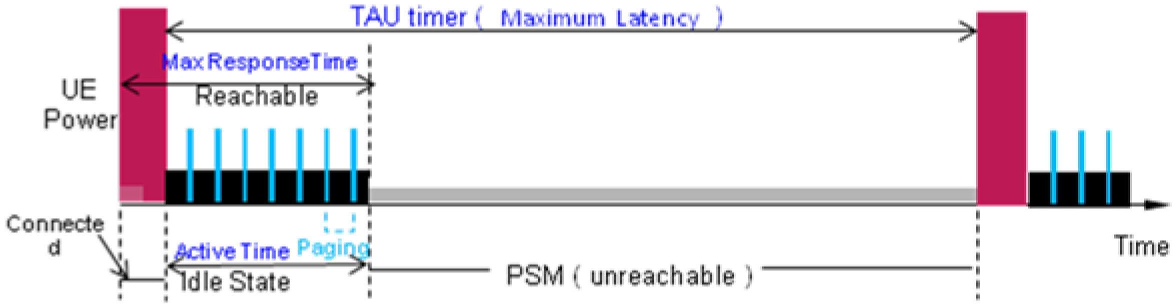


Figure 8.8.2.4-2 PSM related timers

If the <schedule> of ASN-CSE is set in PSM period which is in the grey part above, and the ASN-CSE wants to report data, the UE will deactivate PSM and change to connected status. It increases the power consumption of the terminal.

So the <schedule> needs to be synchronized with 3GPP PSM related timer to optimize power consumption. For example, IN-CSE may use Maximum Response Time to set the TAU timer and Maximum Latency to set Active Time value, then IN-CSE may set the start time of <schedule> to the time the UE changes to idle state, and the period of <schedule> may be the Maximum Response Time and Maximum Latency.

For example, the Active timer of the UE is 30 minutes, and the TAU timer of UE is 6 hours. The Start time of UE change to idle status is 8:00 am. So the schedule could be set to: * 0-30 2,8,14,20 ****.

In case of the ASN-CSE hosted on UE, the ASN-CSE will establish connection on 2:00-2:30, 8:00-8:30, 14:00-14:30, 20:00-20:30.

Figure 8.8.2.4-3 shows an example flow for adjusting the underlying application or transport layer retransmission timer through the event monitoring of UE reachability defined in TS 23.682. This could prevent IN-CSE retransmitting duplicate MT traffic when UE is in deep sleep.

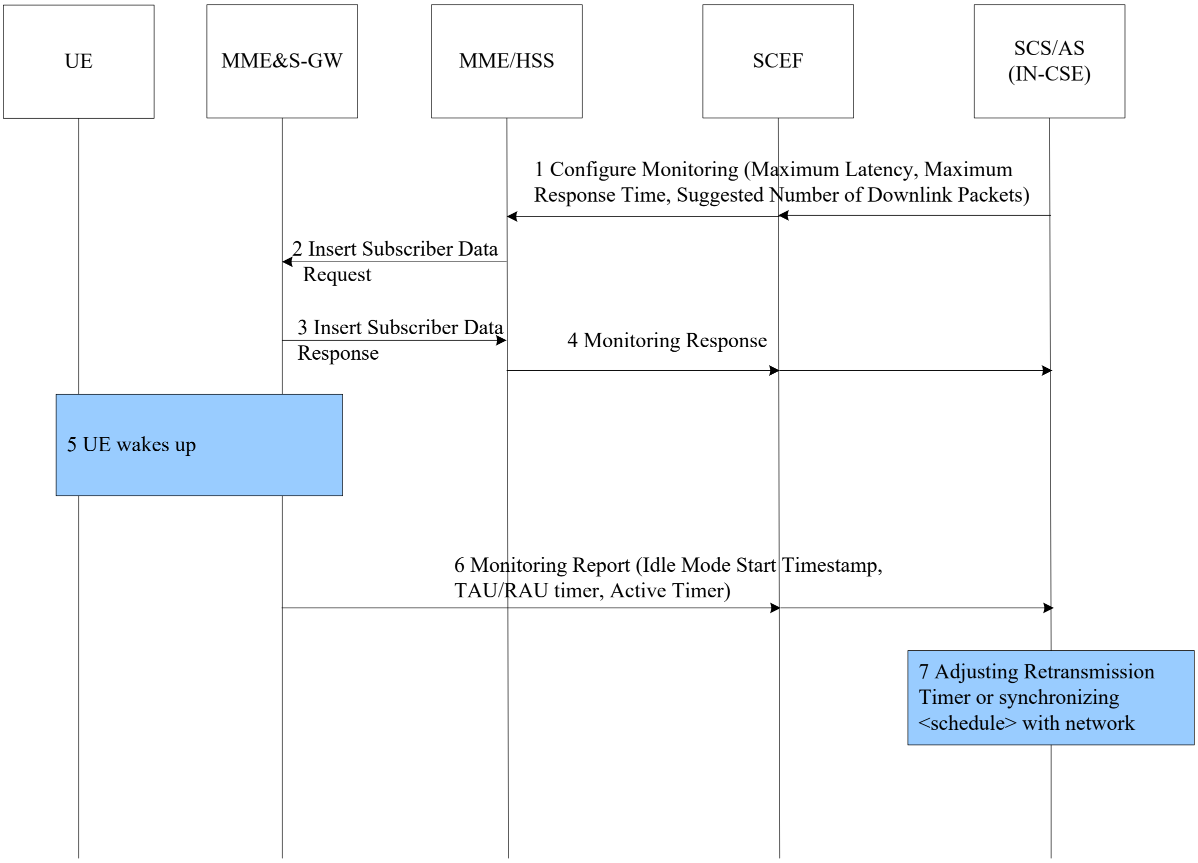

UE
MME&S-GW
MME/HSS
SCEF
SCS/AS (IN-CSE)
1 Configure Monitoring (Maximum Latency, Maximum Response Time, Suggested Number of Downlink Packets)
2 Insert Subscriber Data Request
3 Insert Subscriber Data Response
4 Monitoring Response
5 UE wakes up
6 Monitoring Report (Idle Mode Start Timestamp, TAU/RAU timer, Active Timer)
7 Adjusting Retransmission Timer or synchronizing <schedule> with network

Figure 8.8.2.4-3: Adjusting Underlying Application and Transport Layer Retransmission Timer or Synchronizing Application Layer <schedule> through Event Monitoring

The oneM2M system should take the information above into consideration in the when dealing with sleeping UEs and should expose information to the underlying application or transport layer so that retransmission timers may be optimized.

8.8.3 Key Issues and Requirements

8.8.3.1 Key SCEF NorthBound API Requirements

Table 8.8.3.1-1 SCEF northbound API requirements

Number	Description	Notes
REQ-8.8-01	Configure UE reachability event	Step1 Monitoring Request（SCS->SCEF） in clause 5.6.1.4 TS 23.682[i.5] Step 4b Monitoring Response (SCEF->SCS) in clause 5.6.1.4 Step 9 Monitoring Response or Indication(SCEF->SCS) in clause 5.6.1.4
REQ-8.8-02	Report the UE reachability status	Step 3 Monitoring Indication in clause 5.6.3.3
REQ-8.8-03	Configure UE sleep cycles (i.e. Maximum Latency and Maximum Response Time)	See clause 8.8.2.4
REQ-8.8-04	Monitoring the UE sleep cycles (e.g. last Assigned Active Timer and Periodic Tracking Area Update	See clause 8.8.2.4

	Timer)	
REQ-8.8-05	Monitoring the UE Idle Status (i.e. Idle Mode Start Timestamp)	See clause 8.8.2.4
REQ-8.8-06	Configure Network Buffer Size (i.e. Suggested Number of Downlink Packets)	See clause 8.8.2.4

8.8.3.2 Possible impacts on the SCEF Southbound Interface

N/A

8.8.3.3 Further 3GPP requirements and clarifications

Table 8.8.3.3-3 Issues to be clarified by 3GPP (Stage 2)

Number	Description	Notes
ISSUE-8.8-01	The relationship between parameter Maximum Response Time and Active Time Value of PSM should be clarified.	Step1 Monitoring Request(SCS->SCEF) in clause 5.6.1.4 TS 23.682[i.5]
ISSUE-8.8-02	The parameter Monitoring Information of UE reachability status is not specified	Monitoring Indication（SCEF->SCS）in clause 5.6.3.3 TS 23.682[i.5]

8.8.3.4. oneM2M Key Issues

Provide support for Monitoring of UE reachability.

8.8.4 oneM2M solution

8.8.4.1 Overview

There is resource <schedule> in oneM2M which contains scheduling information. The usage of the <*schedule*> resource is slightly different depending on the associated resource type, such as follows:

- A child <*schedule*> resource of the <*CSEBase*> and <*remoteCSE*> resources shall indicate the time periods when the CSE can send and receive the request.
- A child <*schedule*> resource of the <*AE*> resource shall indicate the time periods when the application of a node can be accessed.

  NOTE: How the <*schedule*> *r*esource under <*CSEBase*> and <*remoteCSE*> for the same device are used for clarification in oneM2M.

In 3GPP, the UE reachability indicates when the UE becomes reachable for sending either SMS or downlink data to the UE. In the 3GPP interworking architecture of oneM2M, the UE can host ADN-AE/ASN-CSE/MN-CSE. So the resource <*schedule*> of the CSE/AE should be mapped to UE reachability.

But there is no specification about how to keep the <*schedule*> consistent between the registree CSE and registrar CSE when the <*schedule*> are the child resource of <*CSEBase*> and <*remoteCSE*>. To avoid inconsistent, the <*schedule*> of <*CSEBase*> should announce to <*remoteCSE*>.

8.8.4.2 Resource Structure

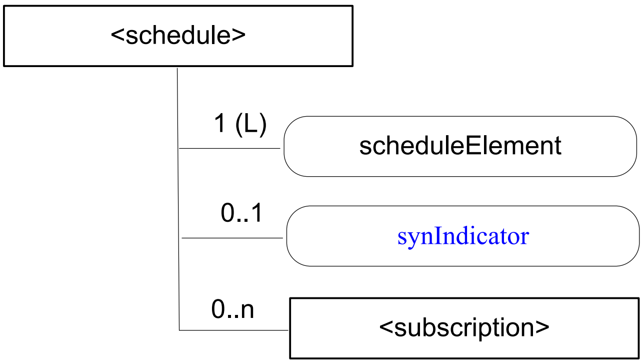


Figure 8.8.5.2-1: Structure of <*schedule*> resource

Table 8.8.5.2-1: Attributes of <*schedule*> resource

Attributes of <*schedule*>	**Multiplicity**	**RW/ RO/ WO**	**Description**	**<*scheduleAnnc*> Attributes**
synIndicator	0..1	RW	• Network：the schedule of CSE/AE is synchronized with network • Device：the schedule of CSE/AE is not synchronized with network.	NA

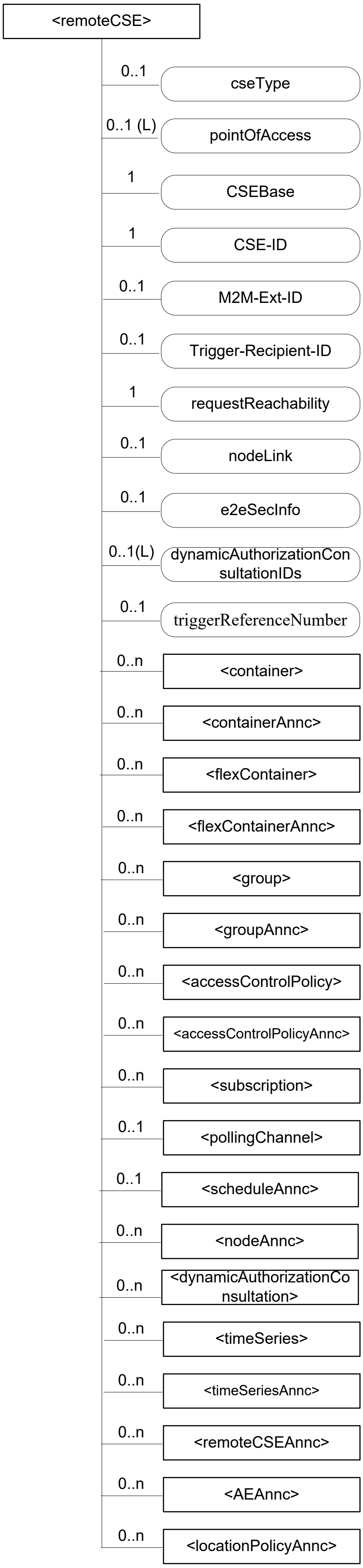

<remoteCSE>
0..1
cseType
0..1 (L)
pointOfAccess
1
CSEBase
1
CSE-ID
0..1
M2M-Ext-ID
0..1
Trigger-Recipient-ID
1
requestReachability
0..1
nodeLink
0..1
e2eSecInfo
0..1(L)
dynamicAuthorizationConsultationIDs
0..1
triggerReferenceNumber
0..n
<container>
0..n
<containerAnnc>
0..n
<flexContainer>
0..n
<flexContainerAnnc>
0..n
<group>
0..n
<groupAnnc>
0..n
<accessControlPolicy>
0..n
<accessControlPolicyAnnc>
0..n
<subscription>
0..1
<pollingChannel>
0..1
<scheduleAnnc>
0..n
<nodeAnnc>
0..n
<dynamicAuthorizationConsultation>
0..n
<timeSeries>
0..n
<timeSeriesAnnc>
0..n
<remoteCSEAnnc>
0..n
<AEAnnc>
0..n
<locationPolicyAnnc>

Figure 8.8.5.2-2: Structure of *<remoteCSE>* resource

Table 8.8.5.2-2: Child resources of *<remoteCSE>* resource

Child Resources of *<remoteCSE>*	Child Resource Type	Multiplicity	Description	*<remoteCSEAnnc>* Child Resource Types
[variable]	*<scheduleAnnc>*	0..1	This resource defines the reachability schedule information of the node. See clause 9.6.9 for *<schedule>*.	*<scheduleAnnc>*

8.8.4.3 UE Create the <*schedule*> in IN-CSE

8.8.4.3.1 ServiceFlow

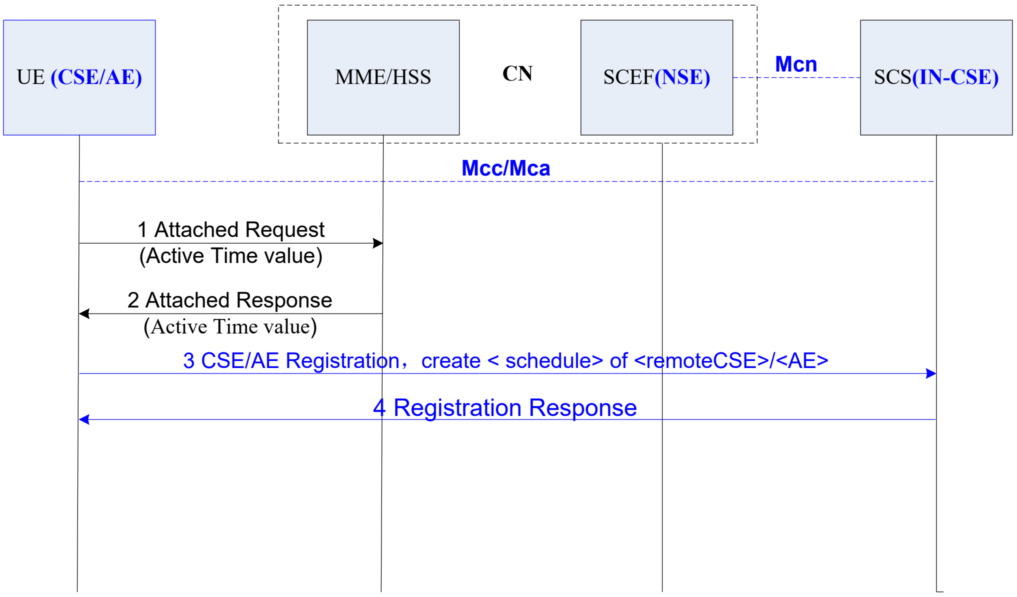


Figure 8.8.5.3-1: Service flow of <*schedule*> creation

Step 001: CSE/AE (UE) performs Initial Attach procedure of 3GPP to negotiate the active time value for PSM parameter with network.

Step 002: The network returns the Initial Attach with the active time value for PSM parameter.

Step 003: CSE/AE (UE) performs the oneM2M registration procedure with mobile original message to IN-CSE (SCS)

If the CSE hosts on the UE, CSE shall announce the <*schedule*> to the <*remoteCSE*> of IN-CSE which includes that synIndicator is Device. If the AE hosts on the UE, the AE shall create the initial <*schedule*> of <*AE*> of the IN-CSE which includes that synIndicator is Device.

Step 004: The IN-CSE (SCS) send the registration response with mobile original response message to the CSE/AE (UE).

8.8.4.4 IN-CSE Synchronize <schedule> from 3GPP network

8.8.4.4.1 ServiceFlow

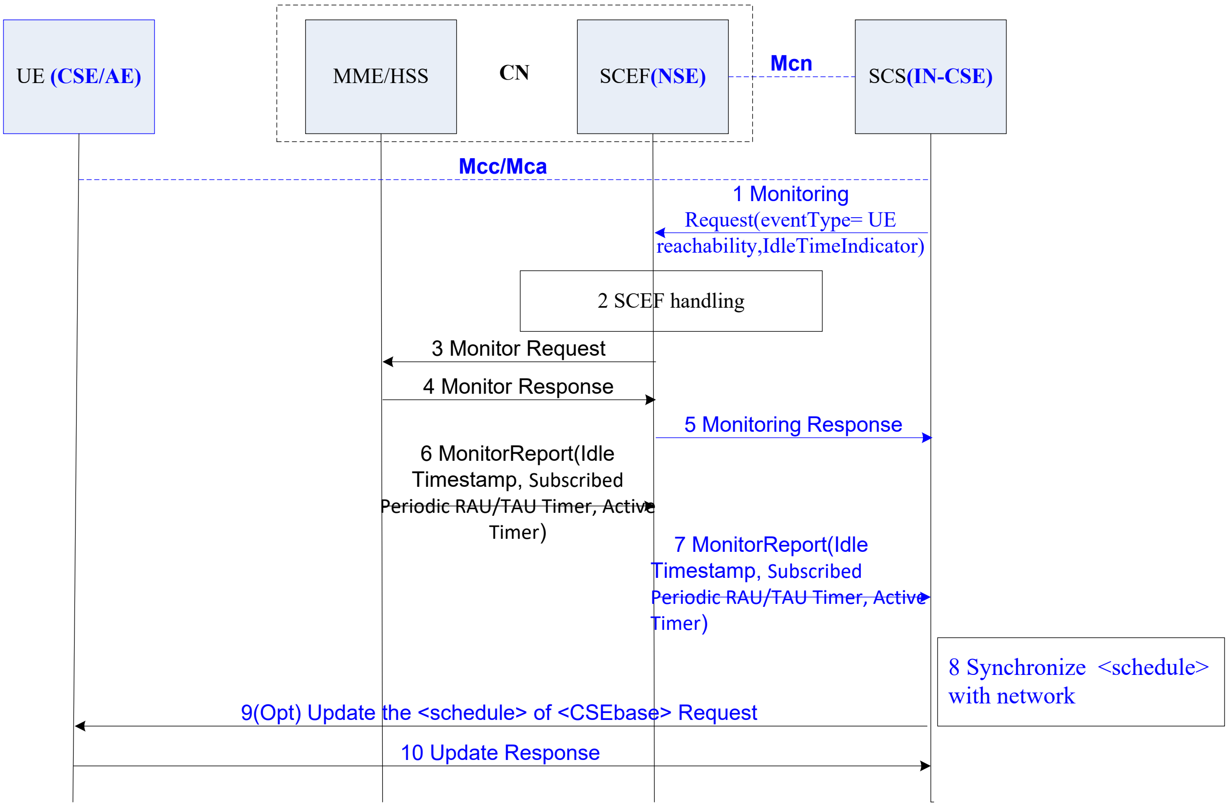

UE (CSE/AE)
MME/HSS
CN
SCEF(NSE)
Mcn
SCS(IN-CSE)
Mcc/Mca
1 Monitoring Request(eventType= UE reachability,IdleTimeIndicator)
2 SCEF handling
3 Monitor Request
4 Monitor Response
5 Monitoring Response
6 MonitorReport(Idle Timestamp, Subscribed Periodic RAU/TAU Timer, Active Timer)
7 MonitorReport(Idle Timestamp, Subscribed Periodic RAU/TAU Timer, Active Timer)
8 Synchronize <schedule> with network
9(Opt) Update the <schedule> of <CSEbase> Request
10 Update Response

Figure 8.8.4.4.1-1: Service flow of <schedule> synchronization from 3GPP network

Step 001: The IN-CSE(SCS) sends a Monitoring Request (External Identifier(s) or MSISDN(s), SCS Identifier, SCS Reference ID, Monitoring Type, Maximum Number of Reports, Monitoring Duration, Monitoring Destination Address, IdleTimeIndication), and sets Monitoring Type to "UE Reachability" and IdleTimeIndication to “True”.

Step 002-Step 004: 3GPP interworking handling the Monitor Request Information， more detail can reference 3GPP TS23.682[i.5]

NOTE: There is new requirement for monitoring type “UE Reachability” for 3GPP from oneM2M in clause 8.8.3.1, refer the detail in clause 8.8.2.4. The parameters in Step 001 will refer the 3GPP new version TS 23.682[i.5].

Step 005: The SCEF (NSE) sends a Monitoring Response (SCS Reference ID, Cause) message to the IN-CSE (SCS) to acknowledge acceptance of the Monitoring Request of the identified monitoring event configuration.

Step 006: The MME sends a Monitoring Report (Idle Timestamp, Subscribed Periodic RAT/TAU timer, Active Timer) to SCEF when detecting the UE status change to Idle.

Step 007: The SCEF sends a Monitoring Report (Idle Timestamp, Subscribed Periodic RAT/TAU timer (optional), Active Time (optional)) to the IN-CSE (SCS) when receiving the Monitoring Report from MME.

NOTE1: There is new requirement for monitoring type “UE Reachability” for 3GPP R14 from oneM2M in clause 8.8.3.1, refer the detail in clause 8.8.2.4. The parameters in Step 001 will refer the 3GPP new version TS 23.682[i.5].

NOTE: **Step 008:** The IN-CSE synchronize the <*schedule*> of the CSE/AE(UE) with the network: set the start time of <schedule> to the time the UE changes to idle state, and the period of <*schedule*> shall be the Active time value and TAU timer. IN-CSE updates the *synIndicator* of <*schedule*> to Network.

For example, the Active time value of the UE is 30 minutes, and the TAU timer of UE is 6 hours. The Start time of UE change to idle status is 8:00 am. So the schedule could be set to: * 0-30 2, 8, 14, 20 ***.

In case of the ASN-CSE hosted on UE, the ASN-CSE will establish connection on 2:00-2:30, 8:00-8:30, 14:00-14:30, and 20:00-20:30

Step 009: The IN-CSE sends update request to the CSE/AE (UE) to update the <*schedule*> if the UE hosts <*CSEBase*> resource.

Step 0010: The CSE/AE (UE) sends the response message to IN-CSE.

8.8.4.5 Delivery Downlink Data When CSE/AE in PSM

8.8.4.5.1 ServiceFlow

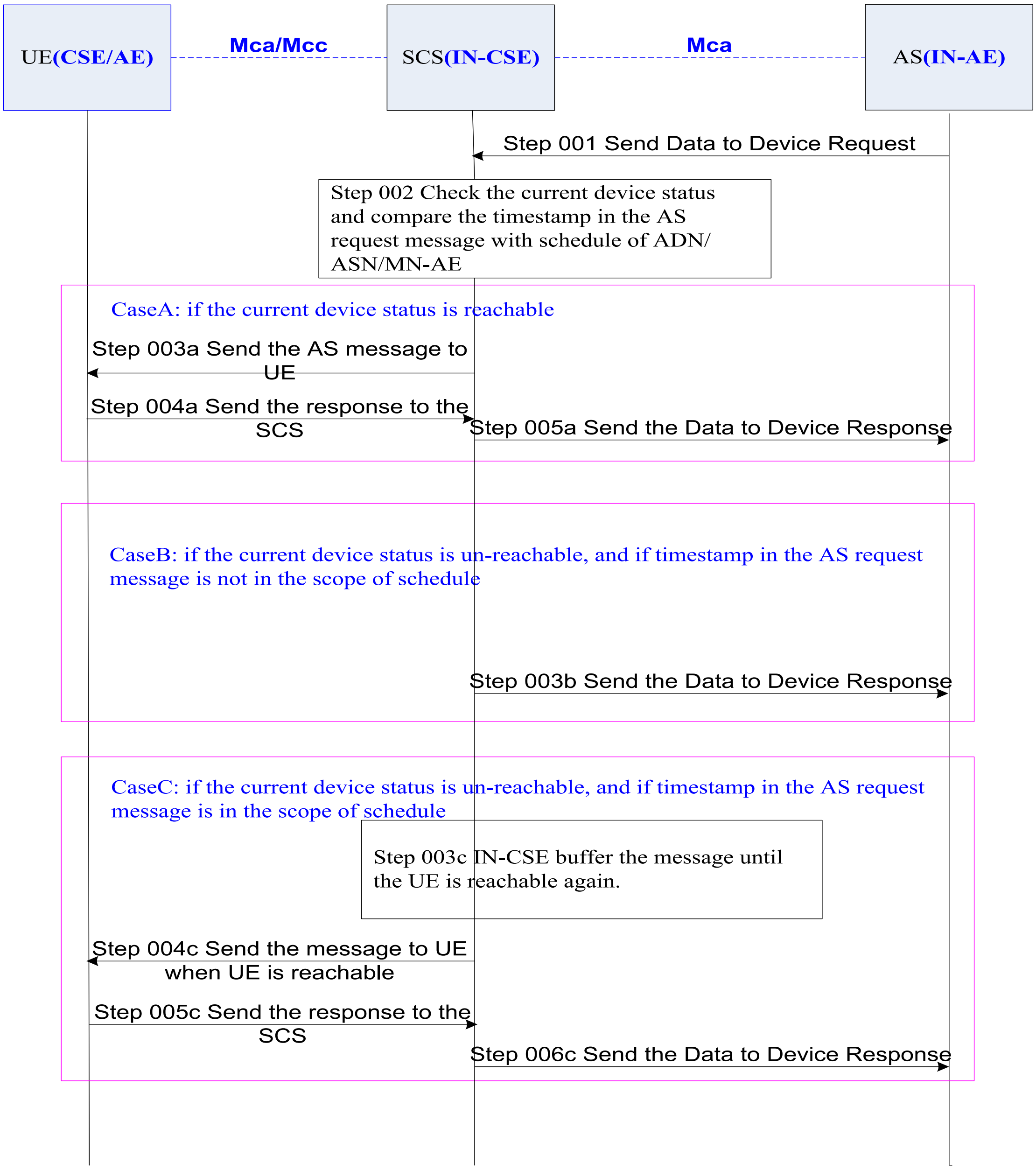

UE(CSE/AE)
Mca/Mcc
SCS(IN-CSE)
Mca
AS(IN-AE)
Step 001 Send Data to Device Request
Step 002 Check the current device status and compare the timestamp in the AS request message with schedule of ADN/ ASN/MN-AE
CaseA: if the current device status is reachable
Step 003a Send the AS message to UE
Step 004a Send the response to the SCS
Step 005a Send the Data to Device Response
CaseB: if the current device status is un-reachable, and if timestamp in the AS request message is not in the scope of schedule
Step 003b Send the Data to Device Response
CaseC: if the current device status is un-reachable, and if timestamp in the AS request message is in the scope of schedule
Step 003c IN-CSE buffer the message until the UE is reachable again.
Step 004c Send the message to UE when UE is reachable
Step 005c Send the response to the SCS
Step 006c Send the Data to Device Response

Figure 8.8.4.3.1-1: Service flow of Delivery Downlink Data When CSE/AE in PSM

Step 001: AS (IN-AE) sends the data to the CSE/AS (UE) message request, the target address is the resource ID of CSE/AE hosted on the UE;

Step 002: IN-CSE (SCS) checks the local <*schedule*> of target CSE/AE (UE) which indicates the pre-defined reachable schedule information of targeted CSE/AE (UE). If the synIndicator of <*schedule*> is Network, IN-CSE(SCS) check the reachable status of target CSE/AE(UE) in current time

Case A: if the target CSE/AE (UE) current status is reachable

- Step 003a: IN-CSE(SCS) sends the downlink data to UE (CSE/AE) directly;
- Step 004a: the UE (CSE/AE) sends the response message to the IN-CSE(SCS);
- Step 005a: IN-CSE(SCS) sends response message to the AS(IN-AE);

Case B: if the target CSE/AE (UE) current status is unreachable, IN-CSE would calculate the next reachable time based on the <*schedule*>, and check the ***Operation Execution Time*** or ***Request Expiration Timestamp*** in the AS request message is whether earlier than the next reachable time or not, if yes, or the ***Operation Execution Time*** or ***Request Expiration Timestamp*** absent in the request, then go to Step 003b,

- Step 003b: IN-CSE(SCS) sends error response message to the AS(IN-AE) which indicates the message can not be delivered to the target CSE/AE(UE);

Case C: if the device current status is unreachable and the ***Operation Execution Time*** and ***Request Expiration Timestamp*** in the AS (IN-AE) request message are both later than the next reachable time, then got Step 003c:

- Step 003c: IN-CSE(SCS) buffers the message until the UE (CSE/AE) is reachable again;
- Step 004c: IN-CSE(SCS) sends the downlink data request message to the target UE (CSE/AE) before the ***Operation Execution Time*** and ***Request Expiration Timestamp*** expire;
- Step 005c: the UE (CSE/AE) sends the response message to the IN-CSE(SCS);
- Step 006c: IN-CSE(SCS) sends response message to the AS(IN-AE);

8.9 Monitoring event (Monitoring Type: Location Reporting)

8.9.1 Description

The Location (LOC) CSF allows AEs to obtain geographical location information of Nodes (e.g. ASN, MN) for location-based services in Mca reference point. The LOC CSF obtains and manages geographical location information based on requests from AEs residing on either a local Node or a remote Node. The LOC CSF interacts with any of the following:

- a location server in the Underlying Network;
- a GPS module in an M2M device; or
- information for inferring location stored in other Nodes.

The functions supported by the LOC CSF are as follows:

- Requests other Nodes to share and report their own or other Nodes' geographical location information with the requesting AEs.
- Provides means for protecting the confidentiality of geographical location information.

The Monitoring Events feature is intended for monitoring of specific events in 3GPP system and making such monitoring events information available via the SCEF.

This monitoring event *Location Reporting* allows the SCS/AS to request either the Current Location or the Last Known Location of a UE. The supported location accuracy is at either cell level (CGI/ECGI), eNodeB, TA/RA level. Only

One-time Reporting is supported for the Last Known Location. One-time and Continuous Location Reporting are supported for the Current Location. For Continuous Location Reporting the serving node(s) sends a notification every time it becomes aware of a location change, with the granularity depending on the requested accuracy.

The Location (LOC) CSF is able to utilize this service to get the node (which is ASN/MN/ADN hosting on the UE) location information from 3GPP network.

The LOC CSF relies on 3GPP SCEF to provide functions such as: Configure Location Reporting event, Detect the Location Reporting event and Report the Location information.

8.9.2 Feature Gap Analysis

The 3GPP defined term 'SCS' in the flows corresponds to oneM2M IN-CSE.

The service flows defined in 3GPP TS23.682 are used in the following section as informative information only. oneM2M focus is on the northbound APIs of SCEF.

8.9.2.1 Monitoring event configuration and deletion procedure (Location Reporting)

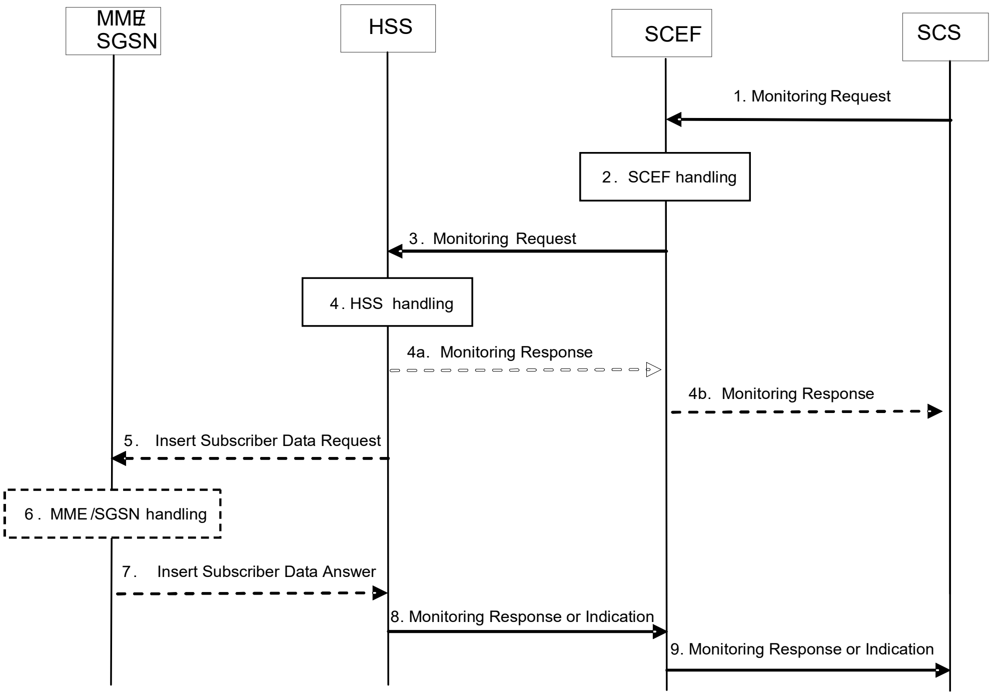


Figure 8.9.2.1-1: Monitoring event configuration and deletion via HSS procedure

Figure 8.9.2.1-1 illustrates the procedure of configuring monitoring at the HSS or the MME/SGSN. The involved SCEF northbound APIs are as below:

Step1: SCS(IN-CSE) sends Monitoring Request (External Identifier(s) or MSISDN(s) or External Group ID, SCS/AS Identifier, SCS/AS Reference ID, Monitoring Type, Maximum Number of Reports, Monitoring Duration, Monitoring Destination Address, SCS/AS Reference ID for Deletion, Group Reporting Guard Time, Location Type, Accuracy) to SCEF.

Step 4b: SCEF sends Monitoring Response () to SCS (IN-CSE).

Step 9: SCEF sends Monitoring Response (SCS/AS Reference ID, Cause) or Indication () to SCS (IN-CSE).

There are some gaps for the SCEF northbound APIs.

- Step 1 The Accuracy parameter indicates desired level of accuracy of the requested location information. In [2] TS23.682 notes that "*the format of parameter Accuracy should refer OMA Presence API* ". When 3GPP define this API, the format of parameter *Accuracy* should be specified.
- Step 4b This step is used to indicate that Group processing is in progress from SCEF to SCS. But there is no parameter defined.
- Step 9 For group based processing, SCEF may send the Monitor Indication to the SCS. But there is no parameter defined. At the same time, this step could report of the current or last known location depending on what was requested, the SCEF would map eNodeB-ID/cell-ID/RAI/TAI to geo-location before reporting to the SCS/AS. But there is no parameter indicating geo-location information.

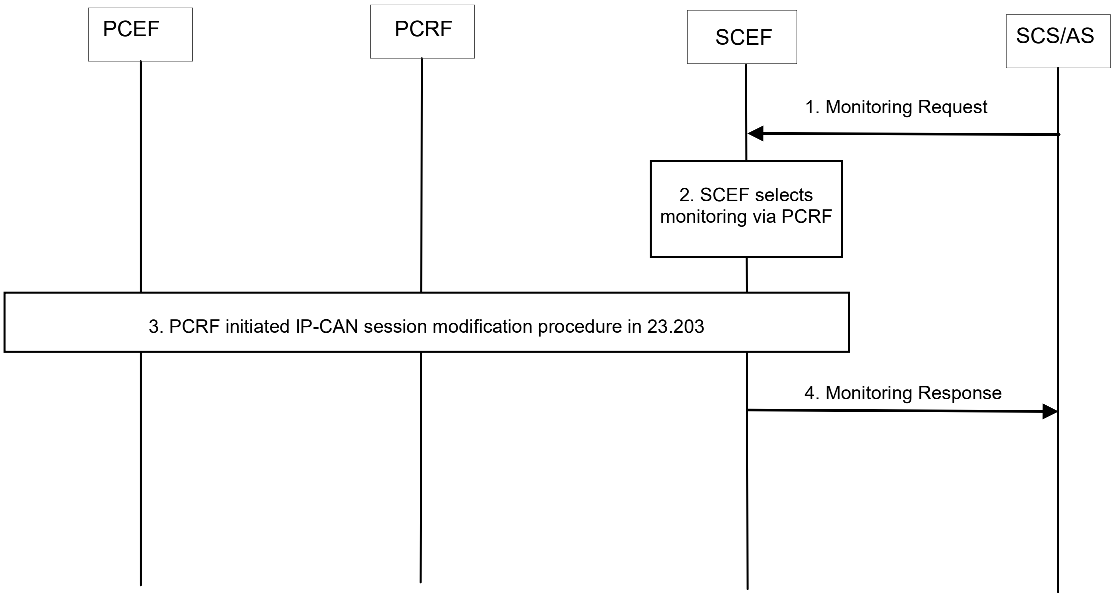

PCEF
PCRF
SCEF
SCS/AS
1. Monitoring Request
2. SCEF selects monitoring via PCRF
3. PCRF initiated IP-CAN session modification procedure in 23.203
4. Monitoring Response

Figure 8.9.2.1-2: Requesting monitoring via PCRF

Figure 8.9.2.1-2 illustrates the procedure to request monitoring events reporting via PCRF. The only one-time report is supported by PCRF.

The procedure using SCEF northbound APIs is described below:

Step1: SCS sends Monitoring Request (External Identifier(s) or MSISDN(s), SCS/AS Identifier, Monitoring Type ("Location Reporting" for a single UE), Priority, Monitoring Duration, Monitoring Destination Address, UE IP address and service information, Location Type) to SCEF

Step4: SCEF sends Monitoring Response (SCS/AS Reference ID, Cause) to SCS (IN-CSE)

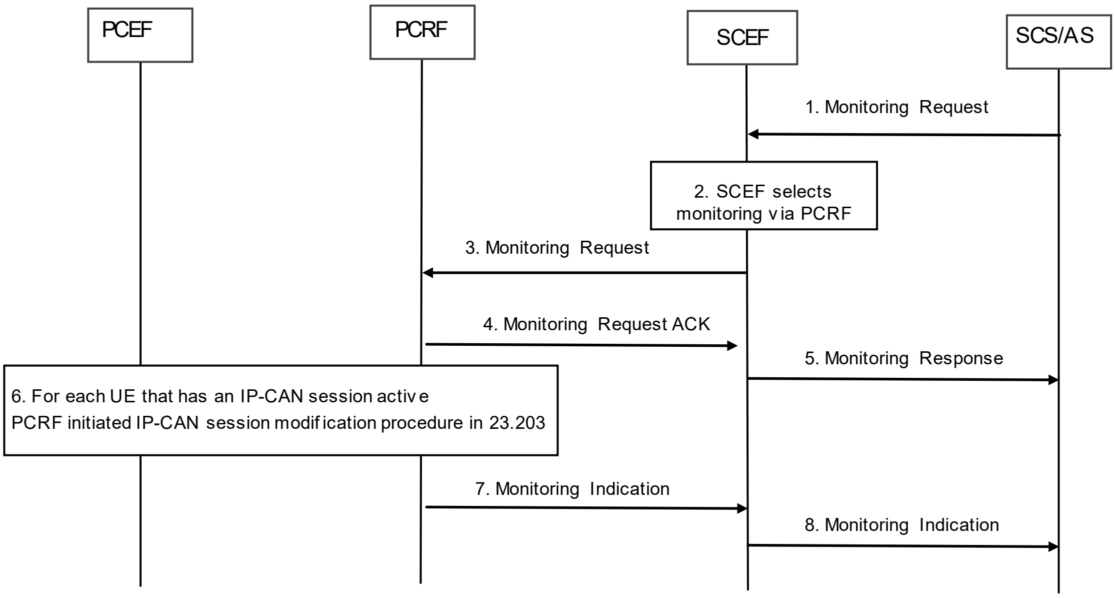

PCEF
PCRF
SCEF
SCS/AS
1. Monitoring Request
2. SCEF selects monitoring via PCRF
3. Monitoring Request
4. Monitoring Request ACK
5. Monitoring Response
6. For each UE that has an IP-CAN session active PCRF initiated IP-CAN session modification procedure in 23.203
7. Monitoring Indication
8. Monitoring Indication

Figure 8.9.2.1-3: Requesting monitoring via PCRF for a group of UEs

Figure 8.9.2.1-3 illustrates the procedure to request monitoring events reporting via PCRF for a group of UEs. For monitoring for a group of UEs, the SPR is configured with the External Group Identifier the UE belongs to.

The procedure using SCEF northbound APIs is described below:

Step1 SCS (IN-CSE) sends Monitoring Request (External Identifier(s) or MSISDN(s) or External Group ID, SCS/AS Identifier, SCS/AS Reference ID, Monitoring Type, Maximum Number of Reports, Monitoring Duration, Monitoring Destination Address, SCS/AS Reference ID for Deletion, Group Reporting Guard Time, Location Type) to SCEF.

Step5 SCEF sends Monitoring Response (SCS/AS Reference ID) to SCS(IN-CSE)

Step8 SCEF sends Monitoring Indication including multiple instances of the 4-tuple (SCS/AS Reference ID, UE IP address, External Group Identifier, Cause) to SCS (IN-CSE)

There are some gaps for the SCEF northbound APIs.

- Step1 It is the same API interface for Monitoring Request for the single UE and group of UE, but whether PCRF support group of UE or not is not definite. The new API should be needed to distinguish it.
- Step1 There is no *Accuracy* parameter to indicate desired level of accuracy of the requested location information comparing with the parameters in Step1 Figure 8.9.2.1-1

8.9.2.2 Monitoring event reporting procedure

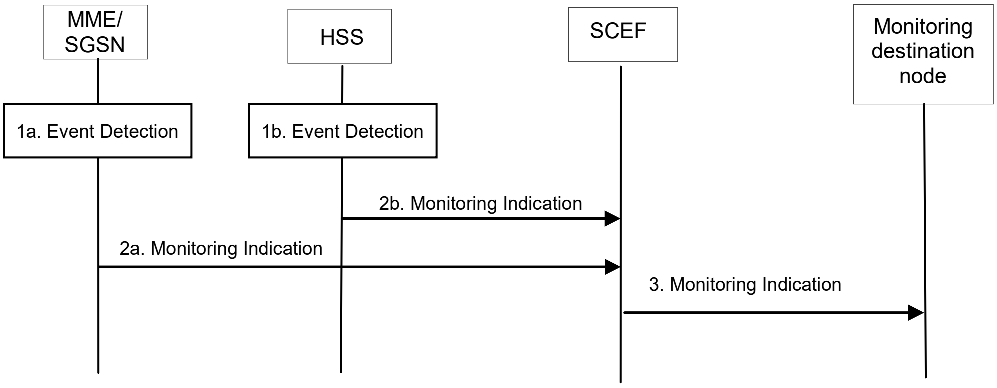


Figure 8.9.2.2-1: Monitoring event reporting procedure via HSS or MME

Figure 8.9.2.2-1 illustrates the common procedure flow of reporting Monitoring Events that are detected by the MME/SGSN or HSS. The Monitoring destination node should be IN-CSE in oneM2M perspective. The involved SCEF northbound APIs are as below:

Step 3 SCEF sends Monitoring Indication (SCS/AS Reference ID, External ID or MSISDN, Monitoring Information) for single UE to the Monitoring destination node (IN-CSE.).

SCEF sends Monitoring Indication (SCS/AS Reference ID, External Group Identifier, External ID(s) or MSISDN(s), Monitoring Information) for group of UEs to the Monitoring destination node (IN-CSE.).

There is one gap for the SCEF northbound APIs.

- Step 3, The SCEF maps the reported 3GPP system specific location information to a geo-location and reports it. At last the parameter *Monitoring Information* of geo-location is not specified.

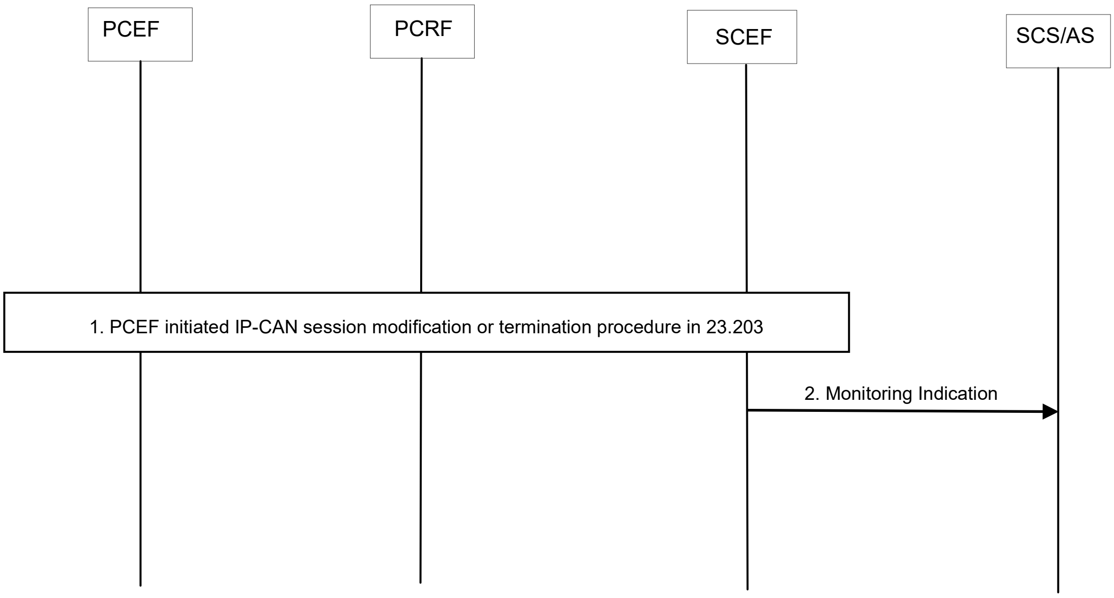

PCEF
PCRF
SCEF
SCS/AS
1. PCEF initiated IP-CAN session modification or termination procedure in 23.203
2. Monitoring Indication

Figure 8.9.2.2-2: Reporting event procedure

The Figure 8.9.2.2-2 illustrates the procedure to report Monitoring Events via PCRF. The involved SCEF northbound APIs are as below:

Step 2: SCEF sends Monitoring Indication(SCS/AS Reference ID, UE Identity, and Monitoring Information) to SCS(IN-CSE).

There is one gap for the SCEF northbound APIs.

- Step 2 The SCEF maps the reported 3GPP system specific location information to a geo-location and reports it. At last the parameter *Monitoring Information* of geo-location is not specified.

8.9.3 Key Issues and Requirements

8.9.3.1Key SCEF NorthBound API Requicements

Table 8.9.3.1-1 Requirements on SCEF NorthBound interface

Number	SCEF API Requirements	Note
REQ-8.9.01	Support UE Location Reporting Monitoring Configuration	Step1: Monitoring Request（SCS->SCEF）in clause 5.6.1&5.6.4 TS23.682 [i.5] Step 4b Monitoring Response in clause 5.6.1 &5.6.4 TS23.682 [i.5]

REQ-8.9.02	Support UE Location Reporting	Monitoring Indication clause 5.6.3 & 5.6.5 TS23.682 [i.5]

8.9.3.2 Potential impact on SCEF SouthBound Interface

Table 8.9.3.2-1 Potential impacts on the SCEF SounthBound Interface

Number	Description	Note
IMPAC-8.9.01	How SCEF choose HSS or PCRF to support UE location Reporting monitor event should be clarified (SCEF-HSS/PCRF).	

8.9.3.3 Further 3GPP requirements and clarifications

Table 8.9.3.3-1 Issues to be clarified by 3GPP (Stage 2)

Number	Description	Note
ISSUE-8.9.01	The format of parameter Accuracy should be sepecified	Step 1 Monitoring Request（SCS->SCEF）in clause 5.6.1 TS23.682 [i.5]
ISSUE-8.9.02	Parameters should be defined to indicate that Group processing is in progress from SCEF to SCS.	Step 4b Monitoring Response（SCEF->SCS）i in clause 5.6.1 TS23.682 [i.5]
ISSUE-8.9.03	Parameters should be defined for group based processing.	Step 9 Monitoring Indication（SCEF->SCS）in clause 5.6.3 TS23.682 [i.5]
ISSUE-8.9.04	The new API should indicate whether 3GPP supports group of UEs.	Step1: Monitoring Request（SCS->SCEF）in clause 5.6.4 TS23.682 [i.5]
ISSUE-8.9.05	The parameter Accuracy may be missing	Step1: Monitoring Request（SCS->SCEF）in clause 5.6.4 TS23.682 [i.5]
ISSUE-8.9.06	The parameter Monitoring Information of UE geo-location should be specified	Monitoring Indication（SCEF->SCS）in 5.6.3 & 5.6.5 TS23.682 [i.5]

8.9.3.4. oneM2M Key Issues

Provide support for Monitoring of UE location.

8.10 Support for Group Communication Patterns and Group Monitoring

8.10.1 Description

In 3GPP TS 23.682, 3GPP has defined an External Group Identifier. Section 4.6.3 says "*A subscription used for MTC may have one or several IMSI-Group Identifier(s) (see TS 23.003 [4]) that are stored in the HSS.*" The External Group Identifier is used on the interface between the SCS/AS and SCEF.

The Monitoring and Communication Pattern provisioning procedures in TS 23.682 allow the SCS/AS to use the External Group Identifier to configuring monitoring events for groups of devices and configure communication patterns for groups of devices. TS 23.682 says "*When the External Group Identifier is used in the communication pattern provisioning or monitoring event configuration and deletion procedures, the HSS is able to resolve the External Group Identifier to an IMSI-Group Identifier.*"

8.10.2 Feature Gap Analysis

8.10.2.1 Group Monitoring

The procedure for Monitoring Event configuration from TS 23.682 is shown in Figure 8.10.2.1-1. It is defined for monitoring specific events in 3GPP system and making such monitoring events information available via the SCEF to SCS/AS. Events such as changes in association of the UE and UICC and/or new IMSI-IMEI-SV association, UE reachability, location change, loss of connectivity, communication failure, roaming status, and availability after DDN failure may be monitored.

As stated in TS 23.682, *"If the SCS/AS wants to configure Monitoring Event for the group of UEs, the SCS/AS can send Monitoring Request message including External Group Identifier and Group Reporting Guard Time." (step 1)*

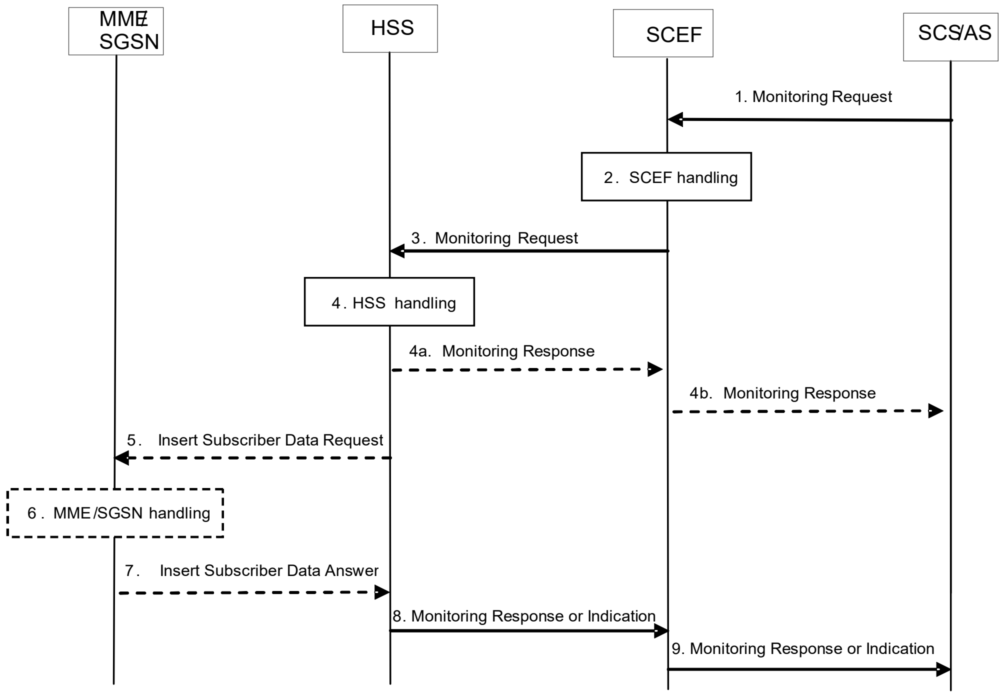


Figure 8.10.2.1-1. Monitoring event configuration and deletion via HSS procedure

8.10.2.2 Communication Patterns for a Group of UEs

The SCEF allows the SCS/AS to provide the network with predictable communication patterns of a UE in order to enable network resource optimizations for such UE(s). The procedure for configuring communication patterns from TS 23.682 is shown in Figure 8.10.2.2-1.

As stated in TS 23.682, "*The SCS/AS sends an Update Request (External Identifier or MSISDN or External Group Identifier, SCS/AS Identifier, SCS/AS Reference ID(s), CP parameter set(s), validity time(s), SCS/AS Reference ID(s) for Deletion) message to the SCEF.*" (step 1)

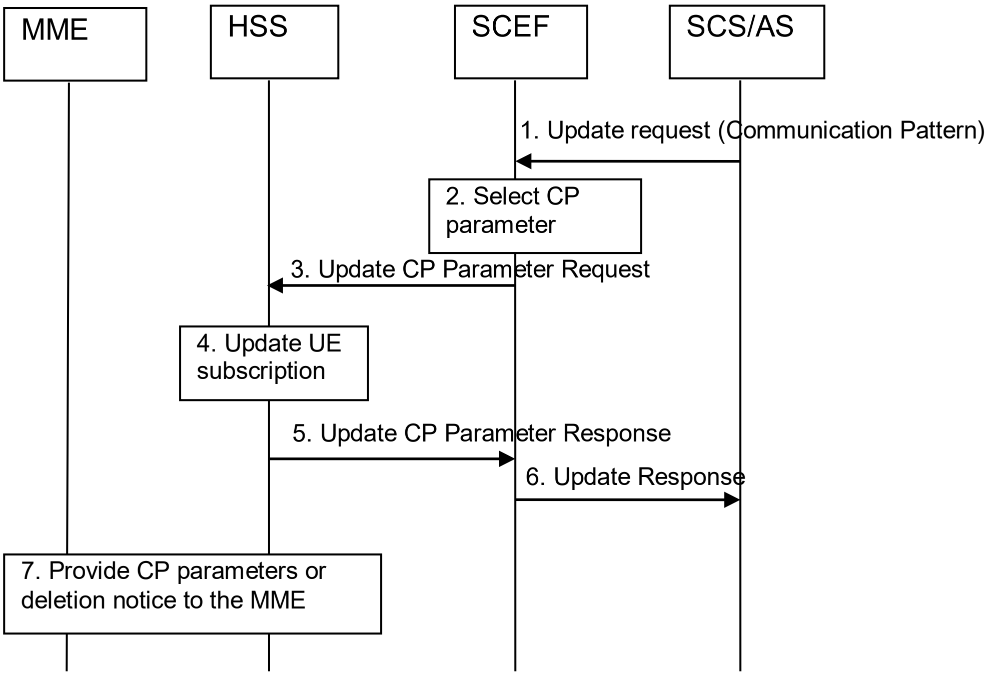

MME
HSS
SCEF
SCS/AS
1. Update request (Communication Pattern)
2. Select CP parameter
3. Update CP Parameter Request
4. Update UE subscription
5. Update CP Parameter Response
6. Update Response
7. Provide CP parameters or deletion notice to the MME

Figure8.10.2.2-1 Signalling sequence for provisioning of CP Parameters

8.10.2.3 Analysis

The group monitoring and group communication pattern provisioning procedures are not very flexible in the sense that the group members are fixed. This limits the cases where they can be leveraged by the Service Layer, since it does not allow for operations using grouping based on service logic

For example, consider a use case where a vending machine company distributes and maintains many vending machines in a shopping mall. The company wants all of the machines to use the same communications patterns so that they areeasily managed. For example, new pricing information can be distributed to all devices at 6:00 am. However, when machines are moved in and out of the mall the vending company may no longer want them to be part of the group. For example, some machines may be moved to a school; thus healthier food options have been added or different prices should be used.

Moreover, the vending company might expose its machines to advertising companies that provide content which gets updated regularly. The advertising companies are not allowed to change the pre-provisioned information, but they should be able to use service logic for grouping: e.g. machines used for products from a brand name vs. another.

To enable use cases using grouping based on service logic, e.g. for monitoring and group communication pattern provisioning procedures, addition the following functionality is required at the SCEF.

Procedures for group management via SCEF, for example, create a group, and modify group membership

8.10.3 Key Issues and Requirements

8.10.3.1 Key SCEF NorthBound API Requirements

Number	Description	Notes
REQ-8.10-01	Group management procedures e.g. create, delete, modify group membership, i.e. association between External Group Identifier and External Identifiers.	See clause 8.10.2.3

8.10.3.2 Possible impacts on the SCEF Southbound Interface

N/A

8.10.3.3. Further 3GPP requirements and clarifications

N/A

8.10.3.4. oneM2M Key Issues

Provide support for use of Group Management feature.

8.11 Support for Low Access Priority

8.11.1 Description

Starting with Release 10, 3GPP has identified signalling congestion control as one of the key issues to be addressed for MTC communications. The solution adopted introduces the concept of "Low Priority Indications" which allow communications from certain MTC devices or applications to be treated as a low priority. A subscriber may configure UEs for low access priority per an agreement with its operator. The agreement may include a specific pricing, so the low access priority use is reflected in CDRs.

8.11.2 Feature Gap Analysis

Support for Low Access Priority is enabled by configuring UEs, per agreement with operators, via a simple flag. On the M2M device, low access priority is used by applications or users that tolerate being deferred when competing with other devices for network resources. UEs may be configured for low access priority and provide indications when performing a NAS procedure or establishing an RRC connection, as described in TS 23.060 and TS 23.401.

When the UE provides the Low Access Priority indication (e.g. in the attach request) to the MME/SGSN during NAS signaling, it is used by the MME/SGSN to help determine if the request should be accepted.

The core network considers the device as 'low access priority' for the lifetime of the connection. The CN may choose to terminate the connection and it may reject messages with a backoff time which may be longer under overload/congestion. The network is also allowed to command the UE to move to a state where is does not need to generate further signaling messages and/or does not reselect the PLMN. Consequently, the application needs to be designed to be tolerant to delays when accessing the network.

The UE configuration for Low Access Priority may be provided at the time of production (on UE/USIM) or performed via OMA Device Management procedures or OTA (Over-the-air) interface. This information is not available in the subscription information stored in the HSS/HLR, hence the network is not able to identify a 'low access priority' device unless the device indicates low access priority in the NAS or RRC procedures.

A subscriber may also, by agreement with its operator, configure the UEs with a permission for overriding Low Access Priority. CDRs show whether the UE activated the PDN connection with or without low access priority.

The existing Low access Priority mechanism depends on the UE providing the indication. However in many scenarios the SCS/AS may be in a better position to determine the importance of the communication with the device than device itself. Mobile Network Operators in particular may be interested in having more dynamic control of this feature without Device Management operations at the UE.

Communication with an M2M device may be critical under specific circumstances meaningful only at Service Layer level. For example, consider the case where sensors are used for monitoring of backup equipment of a power plant. Normally the sensor readings are infrequent and use Low Access Priority. However, when the main power plant has an emergency, the sensors associated with the backup equipment should not be treated as low priority. The Application Server used for management and monitoring is best suited to make this determination based on the status of the platform, sensor locations, etc. This information may be used to override the Low Access Priority indication in the network for selected devices.

8.11.3 Key Issues and Requirements

8.11.3.1 Key SCEF NorthBound API Requirements

Number	Description	Notes
REQ-8.11-01	Configure UE connection for Low Access Priority	See clause 8.11.2
REQ-8.11-02	Configure override of Low Access Priority for a UE connection	See clause 8.11.2

8.11.3.2 Possible Impacts on the SCEF Southbound Interface

N/A

8.11.3.3. Further 3GPP Requirements and Clarifications

N/A

8.11.3.4. oneM2M Key Issues

Provide support for use of Low Access Priority.

8.12 Setting up an AS session with required QoS procedure

8.12.1 Description

3GPP supports to set up an IP flow to a UE with a specific QoS (e.g. low latency or jitter) and priority handling by the 3rd party service provider (AS/SCS session) via T8 API. oneM2M can use this functionality to support between IN-CSE and UE communication management. AE can specify the resources with a QoS level parameter which referss to pre-defined QoS information between oneM2M and 3GPP operator. oneM2M can map the operation of the specified resources from IN-CSE to the target UE to the 3GPP IP flow, negotiate the QoS with 3GPP network, and request 3GPP network to delivery the operation with the QoS.

8.12.2 Feature Gap Analysis

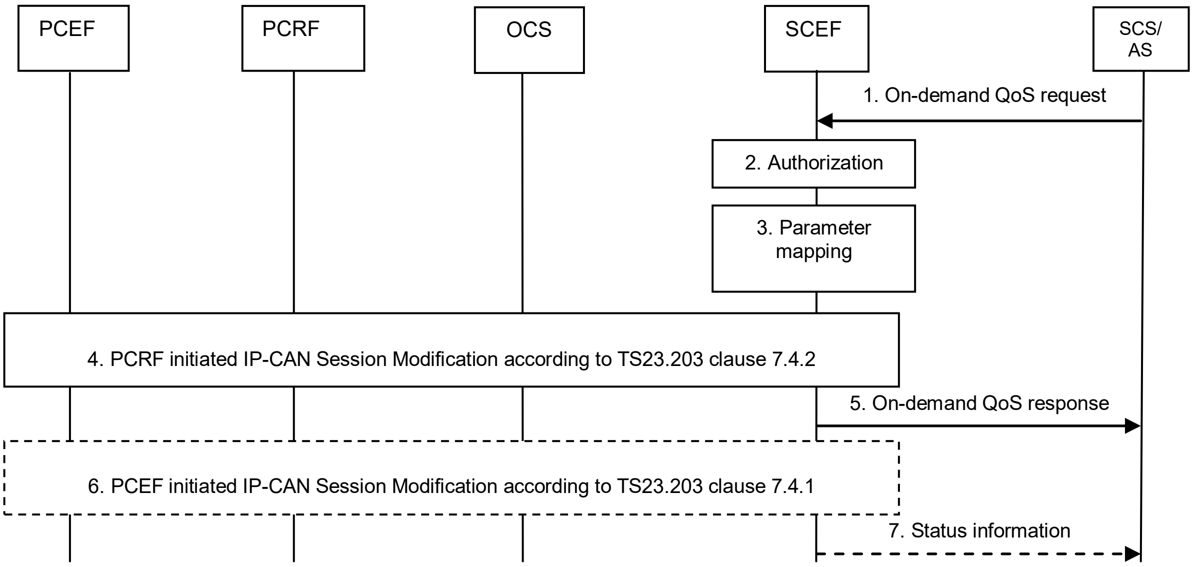

PCEF
PCRF
OCS
SCEF
SCS/ AS
1. On-demand QoS request
2. Authorization
3. Parameter mapping
4. PCRF initiated IP-CAN Session Modification according to TS23.203 clause 7.4.2
5. On-demand QoS response
6. PCEF initiated IP-CAN Session Modification according to TS23.203 clause 7.4.1
7. Status information

Figure 8.12.2-1: Setting up an AS session with required QoS

Figure 8.x.2-1illustrates the procedure of Setting up an AS session with required QoS which is speficied in the section 5.11 of the 3GPP TS23.682[i.5]. The involved SCEF northbound APIs are as below:

Step 1: When setting up the connection between SCS/AS and the UE with required QoS for the service, the SCS/AS sends an On-demand QoS request message (UE IP address, SCS/AS Identifier, Description of the application flows, QoS reference) to the SCEF. Optionally, a period of time or a traffic volume for the requested QoS can be included in the SCS/AS request.

Step 5: The SCEF sends an On-demand QoS response message (TLTRI, Result) to the SCS/AS. Result indicates whether the QoS request is granted or not.

Step 7: If the SCEF gets informed by the PCRF about bearer level events for the Rx session (e.g., transmission resources are released/lost) the SCEF sends a Status information message (SCS/AS Identifier, TLTRI, Status) to the SCS/AS. The status indicates the bearer level event received from the PCRF.

There are some gaps in oneM2M to support the SCEF northbound APIs.

- Step 1: The parameter Description of the application flows describe the data flow which requires QoS. According to Table 5.2.1.2.8-1 of 3GPP TS29.122 [i.18], this parameter shall contain UL and/or DL IP flow description between the SCS and targeted UE. In oneM2M architecture, the SCS is mapped to the IN-CSE. All the messages between IN-AE and targeted UE will go through the IN-CSE. The same IP flow between the IN-CSE and targeted UE can not be used to distinguish the messages from different IN-AEs or different services in the Figure 8.12.2-1.

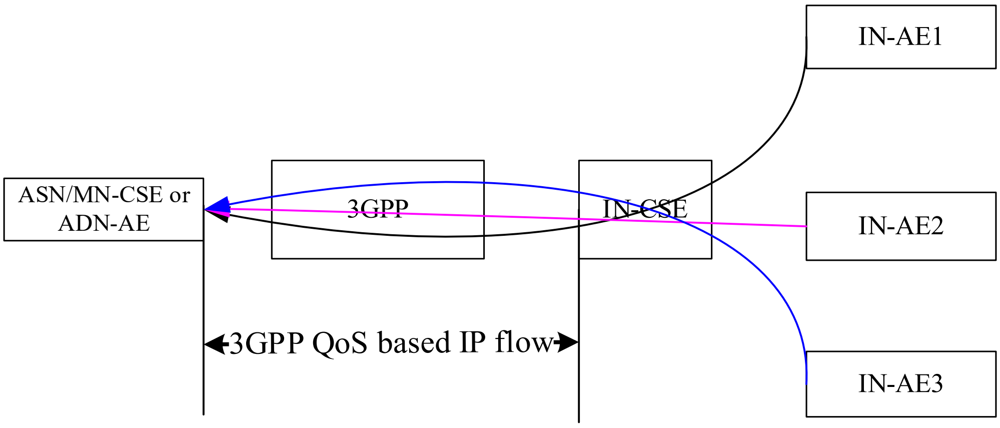


Figure 8.12.2-2 Message Flow between IN-AE and targeted UE

The parameter QoS reference identifies a pre-defined QoS information between the SCS and 3GPP operator. In oneM2M, the content and format of QoS reference has not been defined yet.

Note: The procedure that IN-AE communicates with the targeted ADN-AE without going through IN-CSE is out of the oneM2M scope.

- Step 7: The parameter Status indicates the bearer level event received from the 3GPP network. According to the Table 5.2.1.2.6-1: Definition of the EventReport data type and Table 5.2.1.3.3: Enumeration Event of 3GPP TS29.122 [i.18], 3GPP supports rich status information to the IN-CSE. But oneM2M does not support how to proceed this information when receiving the notification from 3GPP.

- **Table 5.2.1.2.6-1: Definition of the EventReport data type**

Attribute name	Data type	Cardinality	Description
Event	Event	1	Indicates the event reported by the SCEF.
accumulatedUsage	AccumulatedUsage	0..1	Contains the applicable information corresponding to the event.
flowIds	array(integer)	0..N	Identifies the IP flows that were sent during event subscription

- **Table 5.2.1.3.3-1: Enumeration Event**

Enumeration value	Description
SESSION_TERMINATION	Indicates that Rx session is terminated.
LOSS_OF_BEARER	Indicates a loss of a bearer.
RECOVERY_OF_BEARER	Indicates a recovery of a bearer.
RELEASE_OF_BEARER	Indicates a release of a bearer.
USAGE_REPORT	Indicates the usage report event.

8.12.3 Key Issues and Requirements

8.12.3.1 Key SCEF NorthBound API Requirements

N/A

8.12.3.2 Possible Impacts on the SCEF Southbound Interface

N/A

8.12.3.3. Further 3GPP Requirements and Clarifications

N/A

8.12.3.4. oneM2M Key Issues

Provide support for Setting up an session with 3GPP with required QoS functionality.

8.12.4 oneM2M solution

8.12.4.1 Resource Structure

8.12.4.1.1 Resource Type *e2eQosSession*

The <*e2eQosSession*> resource defines end-to-end (E2E) QoS session requirements for the exchange of oneM2M request and response primitives between oneM2M entities. This resource consists of a set of QoS parameters and an applicable set of oneM2M entities that exchange oneM2M requests and responses with one another and function as the session endpoints. A Hosting CSE uses the information configured within this resource to configure and manage E2E QoS between these session endpoints. For example, the Hosting CSE can manage the establishment and tear-down of QoS session(s) in underlying network(s) that interconnect oneM2M entities with one another, A Hosting CSE can also use this information to manage the scheduling and store-and-forwarding of requests and responses that it performs at the oneM2M service layer. When establishing a QoS session in an underlying network, a Hosting CSE can configure the QoS parameters based on the requirements defined by the <*e2eQosSession*> resource. For cases where the oneM2M entities are separated by multiple hops, each hop may require the establishment and configuration of a separate underlying network QoS session. For this case, a Hosting CSE can coordinate with its registrar and registree CSEs to assist it with the configuration of a QoS session in each respective underlying network involved in a multi-hop E2E QoS session such that the E2E QoS requirements defined within the <*e2eQosSession*> can be satisfied across the multiple hops.

Note – This current solution supports the 0-hop scenario and the 1-hop scenario involving a <*e2eQosSession*> Hosting CSE that is the registrar CSE of the session endpoints. The details for how an E2E QoS session is supported for multiple hop scenarios is for FFS.

The following are some examples of E2E oneM2M communication flows that an <*e2eQosSession*> resource Hosting CSE can manage using this QoS information.

Example #1

A first oneM2M entity that is a session endpoint sends a request to the <*e2eQosSession*> resource Hosting CSE and the *To* parameter targets a remote oneM2M entity that is also a session endpoint of the same QoS session. The <*e2eQosSession*> resource Hosting CSE can establish an individual underlying network QoS session between itself and each of the session endpoints such that each underlying network QoS session meets the QoS requirements defined in the <*e2eQosSession*> resource. In doing so, the E2E exchange of oneM2M request and response primitives between the session endpoint entities meets the E2E QoS requirements defined in the <*e2eQosSession*> resource.

Example #2

A first oneM2M entity that is a session endpoint is a subscriber to a <*flexContainer*> resource that is hosted by the <*e2eQosSession*> resource Hosting CSE. A second oneM2M entity, that is also a session endpoint of the same QoS session, sends a request to update the <*flexContainer*> resource. The update results in a notification being sent to the first oneM2M entity. The <*e2eQosSession*> resource Hosting CSE can establish an individual underlying network QoS session between itself and each of the session endpoints such that each underlying network QoS sessions meets the QoS requirements defined in the <*e2eQosSession*> resource. In doing so, the E2E exchange involving the second oneM2M entity sending the <*flexContainer*> update request and the resulting notification request that is sent to the first oneM2M entity meets the E2E QoS requirements defined in the <*e2eQosSession*> resource.

The <*e2eQosSession*> resource contains the child resources specified in table 8.12.4.1.1-1.

Table 8.12.4.1.1-1: Child resources of <*e2eQosSession*> resource

Child Resources of <*e2eQosSession*>	Child Resource Type	Multiplicity	Description	<*e2eQosSession*> Child Resource Types
[variable]	<*subscription*>	0..n	See oneM2M TS-0001 [i.17] clause 9.6.8.	<*subscription*>

The <*e2eQosSession*> resource contains the attributes specified in table 8.12.4.1.1-2.

Table 8.12.4.1.1-2: Attributes of <*e2eQosSession*> resource

Attributes of <*e2eQosSession*>	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See oneM2M TS-0001 [i.18] clause 9.6.1.3
resourceID	1	RO	See oneM2M TS-0001 [i.19] clause 9.6.1.3
resourceName	1	WO	See oneM2M TS-0001 [i.20] clause 9.6.1.3
parentID	1	RO	See oneM2M TS-0001 [i.21] clause 9.6.1.3
creationTime	1	RO	See oneM2M TS-0001 [i.22] clause 9.6.1.3
lastModifiedTime	1	RO	See oneM2M TS-0001 [i.23] clause 9.6.1.3
expirationTime	1	RW	See oneM2M TS-0001 [i.24] clause 9.6.1.3
accessControlPolicyIDs	0..1 (L)	RW	See oneM2M TS-0001 [i.25] clause 9.6.1.3
dynamicAuthorizationConsultationIDs	0..1 (L)	RW	See oneM2M TS-0001 [i.26] clause 9.6.1.3.
Labels	0..1 (L)	RW	See oneM2M TS-0001 [i.27] clause 9.6.1.3.
announceTo	0..1(L)	RW	See oneM2M TS-0001 [i.28] clause 9.6.1.3
sessionEndpoints	1	WO	Indicates the oneM2M endpoints within one oneM2M E2E QoS session. The end points include AE-IDs or CSE-IDs. If an AE-ID is used and the AE is not a Registree of the <*e2eQosSession*> Hosting CSE, then the AE-ID will be formatted as a SP-Relative-AE-ID or Absolute-AE-ID to allow the <*e2eQosSession*> Hosting CSE to extract the CSE-ID of the CSE that hosts the destination endpoint <AE> resource.
e2eQosRequirements	1(L)	RW	Defines the E2E QoS requirements expressed as a list of tuples. Each tuple in the list defines a single QoS session requirement applicable to the bi-directional exchange of oneM2M requests and responses between all the endpoints. Each tuple in the list contains the set of elements as defined below in table 8.12.4.1.1-3.
e2eQosPolicies	0..1(L)	RW	Defines E2E session QoS policies expressed as a list of tuples. Each tuple in the list defines a single policy that the <*e2eQosSession*> Hosting CSE uses to manage the session. Each tuple in the list contains the set of elements as defined below in table 8.12.4.1.1-4.

Table 8.12.4.1.1-3: Elements of an *e2eQosRequirements* tuple

Name	Mandatory/Optional	Description
qosLevel	M	Defines the required QoS level for this session. Expressed as a range from 0 (lowest) to 100 (highest). How a <*e2eQosSession*> Hosting CSE uses this parameter to manage the QoS of a session is implementation dependent (e.g. a Hosting CSE may map this value to an underlying network operator's session QoS parameter values).
resourceIDList	O	Defines the resource identifier list between the endpoints which the QoS requirement applies to. If a Resource-ID is used and the resource is not hosted by the <e2eQosSession> Hosting CSE, then it will be formatted as a SP-Relative-Resource-ID or Absolute-Resource-ID to allow the <e2eQosSession> Hosting CSE to extract the CSE-ID of the CSE that hosts the destination endpoint resource. The use of a Resource-ID enables a destination E2E QoS session endpoint to be defined at the granularity of an individual targeted resource.
sessionSchedule	O	Defines the time periods for when bi-directional exchange of oneM2M requests and responses between the session endpoints at the specified *qosLevel* is required to be enabled. If this parameter is not specified, then the scheduling of the oneM2M requests and responses between the session endpoints will be managed at the discretion of the <*e2eQosSession*> Hosting CSE based on the specified *qosLevel*. The schedule is composed of seven fields consisting of second, minute, hour, day of month, month, day of week and year.
numOfRequests	O	Defines the minimum number of requests required to be transferred at the specified *qosLevel* via the bi-directional exchange of oneM2M requests and responses between the session endpoints. If this parameter is not specified, then the number of requests and responses allowed between the session endpoints will be managed at the discretion of the <*e2eQosSession*> Hosting CSE based on the specified *qosLevel*.
numOfBytes	O	Defines the minimum number of bytes required to be transferred at the specified *qosLevel* via the bi-directional exchange of oneM2M requests and responses between the session endpoints. If this parameter is not specified, then the number of bytes allowed to be transferred between the session endpoints will be managed at the discretion of the <*e2eQosSession*> Hosting CSE based on the specified *qosLevel*.

Table 8.12.4.1.1-4: Elements of an *e2eQosPolicy* tuple

Name	Mandatory/Optional	Description
status	M	When the *e2eQosStatus* attribute of the <*e2eQosSession*> resource transitions to the value specified in this element, the <*e2eQosSession*> Hosting CSE performs the action specified in the *action* element. The following are the allowed *status* values: - FAILED - DISABLED - USAGE_EXHAUSTED
action	M	Defines a session related action that is performed by the <*e2eQosSession*> Hosting CSE when the value of an *e2eQosStatus* attribute of the <*e2eQosSession*> resource transitions to the value specified by the *status* element. The following are the allowed *action* values: - RE-ENABLE: The <*e2eQosSession*> Hosting CSE will attempt to re-enable the E2E QoS session in a manner that is consistent with the *e2eQosRequirements.* - DISABLE: The <*e2eQosSession*> Hosting CSE will disable the E2E QoS session (if already not disabled). - DELETE: The Hosting CSE will delete the E2E QoS session

8.12.4.1.2 Resource Type *CSEBase*

Table 8.12.4.1.2-1 Child resources of <*CSEBase*> resource

Child Resources of <*CSEBase*>	Child Resource Type	Multiplicity	Description
[variable]	<*e2eQosSession*>	0..1	

8.12.4.1.3 Resource Type *remoteCSE*

Table 8.12.4.1.3-1: Child resources of <*remoteCSE*> resource

Child Resources of <*remoteCSE*>	Child Resource Type	Multiplicity	Description	<*remoteCSEAnnc*> Child Resource Types
[variable]	<*e2eQosSession*>	0..1	See clause 8.12.4.1.1	< *e2eQosSession Annc*>

8.12.4.1.4 Resource Type *AE*

Table 8.12.4.1.4-1: Child resources of <*AE*> resource

Child Resources of <*AE*>	Child Resource Type	Multiplicity	Description	<*AEAnnc*> Child Resource Types
[variable]	<*e2eQosSession* >	0..1	See clause 8.12.4.1.1	< *e2eQosSession Annc*>

8.12.4.2 Create E2E QoS procedure

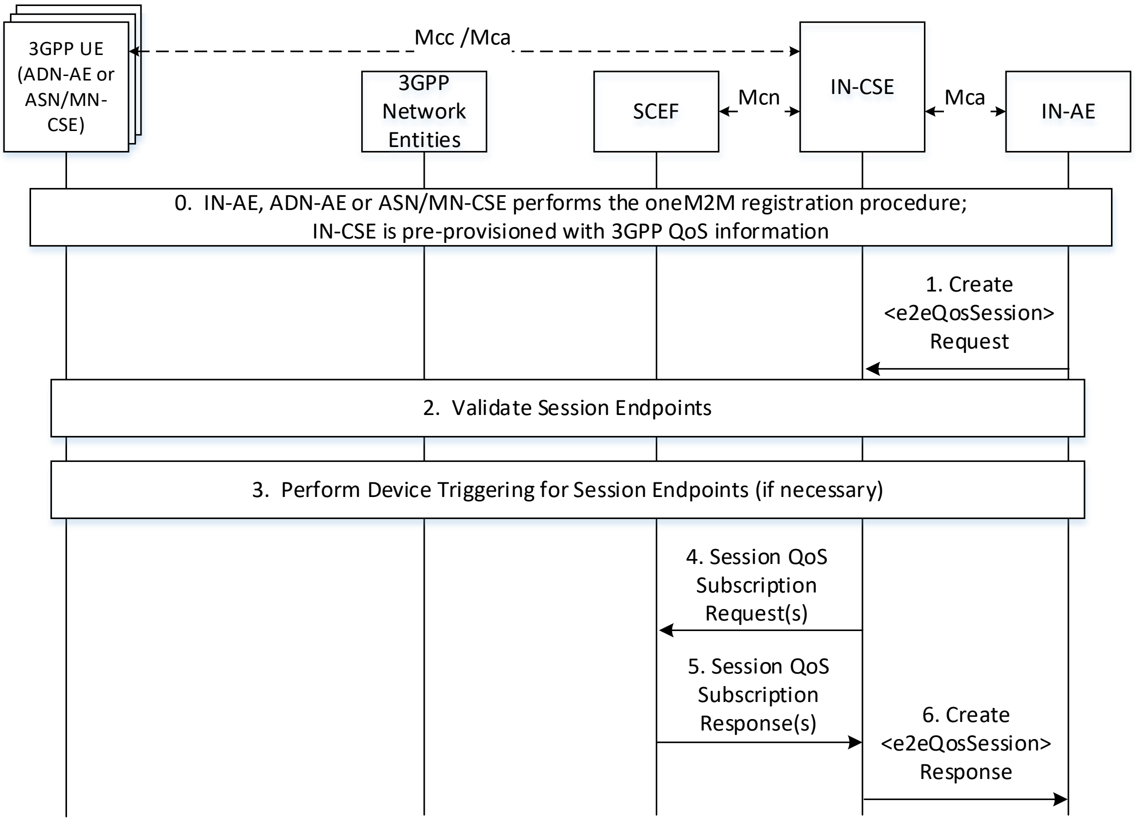

3GPP UE (ADN-AE or ASN/MN-CSE)
Mcc /Mca
3GPP Network Entities
SCEF
Mcn
IN-CSE
Mca
IN-AE
0. IN-AE, ADN-AE or ASN/MN-CSE performs the oneM2M registration procedure;
IN-CSE is pre-provisioned with 3GPP QoS information
1. Create <e2eQosSession> Request
2. Validate Session Endpoints
3. Perform Device Triggering for Session Endpoints (if necessary)
4. Session QoS Subscription Request(s)
5. Session QoS Subscription Response(s)
6. Create <e2eQosSession> Response

Figure 8.12.4.2-1: Create E2E QoS procedure

Step 0: The IN-AE, ADN-AE or ASN/MN-CSE performs oneM2M registration. The IN-CSE is pre-provisioned with 3GPP QoS Information based on a SLA with the MNO.

The IN-AE, ADN-AE or ASN/MN-CSE performs the oneM2M registration procedure. Then the IN-CSE gets the *pointOfAccess* network registration information of ASN/MN-CSE or ADN-AE.

The IN-CSE uses the pre-provisioned 3GPP QoS information to translate oneM2M QoS parameters defined in <*e2eQosSession*> resources into the QoS parameters defined by the MNO and used over the SCEF T8 interface.

Step 1: An AE or CSE sends a <e2eQosSession> CREATE request to the IN-CSE. The <e2eQosSession> CREATE request includes the following information:

- *To* parameter is configured with the Resource-ID of an <*AE*>, <*remoteCSE*> or <*CSEBase*> resource hosted by the IN-CSE
- *From* parameter is configured with the AE-ID or CSE-ID of the Originator

  NOTE: The Originator of the <*e2eQosSession*> CREATE request may be an entity specified in the *sessionEndpoints* attribute. Alternatively, it may be a different entity.
- *sessionEndpoints* attribute is set to a list consisting of one or more AE-IDs and/or CSE-IDs representing the endpoints of the E2E QoS session.
- *e2eQosRequirements* attribute is configured with a list of one or more tuples. Each tuple in the list has the following elements:
  - *qosLevel* element is set to a value between 0 and 100.
  - *resourceIDList* element is set to a list of resource identifiers the QoS requirement applies to.
  - *sessionSchedule* element may be set. If set, it consists of seven fields of second, minute, hour, day of month, month, day of week and year.

- *numOfRequests* element may be set. If set, it consists of the minimum number of requests required to be transferred at the specified *qosLevel.*

- *numOfBytes* element may be set. If set, it consists of the minimum number of bytes required to be transferred at the specified *qosLevel.*

- *e2eQosPolicies* attribute may be set. If set, it is configured with 1 or more tuples. Each tuple has the following elements:

  - *status* element is set with a value of FAILED, DISABLED or USAGE_EXHAUSTED

  - *action* element is set with a value of RE-ENABLE or DISABLE

Step 2: The IN-CSE validates the E2E QoS session endpoint entities.

The IN-CSE receives and validates the <*e2eQosSession*> CREATE request. The IN-CSE validates the *sessionEndpoints* attribute. The IN-CSE performs this check by first confirming that each AE-ID and/or CSE-ID configured within the *sessionEndpoints* attribute matches an AE-ID and CSE-ID of one of its Registree AEs or CSEs.

The IN-CSE also checks that at least one tuple is configured in the *e2eQosRequirements* attribute and that the *qosLevel* element and *resourceIDList* in this tuple is configured. The IN-CSE also checks that all other mandatory attributes and parameters in the request are present and their values comply with their supported data types. The IN-CSE also checks that the values of all other optional attributes and parameters in the request comply with their supported data types and are properly formatted. If these checks are successful, the IN-CSE creates the <*e2eQosSession*> according to the request. Then the IN-CSE proceeds to Step 3. Otherwise, the IN-CSE proceeds to Step 6 and returns a ***Response Status Code*** indicating BAD_REQUEST error.

Step 3: If necessary, the IN-CSE triggers the E2E QoS session endpoint entities.

If entities specified in the *sessionEndpoints* attribute are registered to the IN-CSE and use an underlying 3GPP network, the IN-CSE checks the connection (e.g. TCP) with the *sessionEndpoints.* If the *sessionEndpoints* do not have an active 3GPP PDN connection to the IN-CSE (i.e. ASN/MN-CSE or ADN-AE *pointOfAccess* information is not configured or IN-CSE detects failed communication with ASN/MN-CSE or ADN-AE when the connection is based on TCP), the IN-CSE can send a device trigger request to the corresponding ASN/MN-CSE or ADN-AE to have it establish a connection (e.g. based on TCP) to the IN-CSE.

NOTE: If the *sessionSchedule* element is configured, the IN-CSE can use the schedule information to determine whether to perform this step during the processing of the <*e2eQosSession*> CREATE request or sometime thereafter (e.g. closer to the time when scheduled communication via the session is required).

Step 4: The IN-CSE sends QoS Session Subscription Request(s) to the SCEF.

For each QoS session endpoint that connects to the IN-CSE via an underlying 3GPP network connection and that has an active PDN connection, the IN-CSE sends a AsSessionWithQoSSubscription Request to the SCEF.

NOTE: If the *sessionSchedule* element is configured, the IN-CSE can use the schedule information to determine whether to perform this step during the processing of the <*e2eQosSession*> CREATE request or sometime thereafter (e.g. closer to the time when scheduled communication via the session is required).

Each AsSessionWithQoSSubscription Request from the IN-CSE to the SCEF contains information as specified in 3GPP TS 29.122 [i.18]. Such information includes:

- An HTTP POST method is used

- *URI* is set to *{apiRoot}/3gpp-as-session-with-qos/v1/{scsAsId}/subscriptions/.* The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.

- The request payload includes an *AsSessionWithQoSSubscription* data structure as specified in 3GPP TS 29.122 [i.18] with the following attributes:

  - *supportedFeatures* is set to a string value of "0" indicating the IN-CSE does not support the QoS Session negotiable features specified in 3GPP TS 29.122 [i.18].

  - *notificationDestination* is set to a URI that the SCEF can target QoS session related notifications towards. The value of this URI shall be based on internal IN-CSE policies.

- *flowInfo* includes the following attributes:
    - *flowId* is set to a integer value that describes the IP flow. A value is assigned by the IN-CSE according local policy. The value that is used is unique within the scope of the IN-CSE.
    - *flowDescriptions* is an array of strings configured with two entries. The first entry in the array is an IP flow description for oneM2M requests and responses flowing from the IN-CSE to the QoS session endpoint applicable to this request. The second entry in the array is an IP flow description for oneM2M requests and responses flowing in the reverse direction from the QoS session endpoint to the IN-CSE.
        - Entry #1 in the *flowDescriptions* array includes the following attributes:
            - *direction* is set to a value of *"*out"
            - *source IP address* is set to the IP address of the IN-CSE and *destination IP address* is set to the IP addresses configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.
            - *protocol*: is set to a value of *"*TCP" or "UDP" based on the underlying transport configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request. For example, "TCP" is set if the protocol configured in the *pointOfAccess* is HTTP, MQTT or WebSocket. "UDP" is set if the protocol configured is CoAP.
            - *source port* is set to the port of the IN-CSE and *destination port* is set to the port configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.
        - Entry #2 in the *flowDescriptions* array includes the following attributes:
            - *direction* is set to a value of *"*in"
            - *source IP address* is set to the IP address configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request and *destination IP address* is set to the IP address of the IN-CSE.

              NOTE: The order is reversed from the order used in Entry #1.
            - *protocol*: is set to a value of *"*TCP" or "UDP" based on the underlying transport configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request. For example, "TCP" is set if the protocol configured in the *pointOfAccess* is HTTP, MQTT or WebSocket. "UDP" is set if the protocol configured is CoAP.
            - *source port* is set to the port configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request and *destination port* is set to the port of the IN-CSE.

              NOTE: The order is reversed from the order used in Entry #1.
- *qosReference* is set to a pre-provisioned string value that maps to the *qosLevel*. This mapping is based on a SLA with the MNO. The *qosReference* serves as an identifier of the pre-defined QoS information pre-provisioned into the IN-CSE based on a SLA with the MNO.
- *ueIpvAddr* is set to the IPv4 address (if applicable) configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

- *ueIpvAddr* is set to the IPv6 address (if applicable) configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

- *usageThreshold* includes the following attributes:

    - *duration* is set to the amount of time in seconds that the QoS session is requested to remain active. The IN-CSE computes this duration by inspecting all of the <*e2eQosSession*> resources that it hosts and that have a session endpoint that matches the session endpoint applicable to this request. For any matches found, the IN-CSE will aggregate the *sessionSchedule* elements (if any) configured within the list of *e2eQosRequirements* tuples of these <*e2eQosSession*> resources. Based on the aggregated *sessionSchedule* elements and local policies, the IN-CSE will determine a duration of time to request. If no *sessionSchedule* elements are configured, the IN-CSE will base its determination solely on local policies.

    - *totalVolume* is set to a total number of bytes of data that are required to be exchanged between the IN-CSE and the session endpoint applicable to this request. The IN-CSE shall compute this number of bytes by inspecting all of the <*e2eQosSession*> resources that it hosts and that have a session endpoint that matches the session endpoint applicable to this request. For any matches found, the IN-CSE will sum all of the *numOfBytes* elements (if any) configured within the list of *e2eQosRequirements* tuples of these <e2eQosSession> resources. Based on the *numOfBytes* elements and local policies, the IN-CSE will determine an amount to request. If no *numOfBytes* elements are configured, the IN-CSE will base its determination solely on local policies.

- *sponsorInfo* may be set. If set, the value is a string based on a SLA with the MNO.

- *ethFlowInfo, macAddr, requestTestNotification* and *websockNotifConfig* are not supported by the present document and are not included.

Step 5: SCEF sends QoS Session Response(s) to IN-CSE.

The SCEF handles the AsSessionWithQoSSubscription Request together with the Mobile Core Network. The SCEF sends an AsSessionWithQoSSubscription Response that contains information as specified in 3GPP TS 29.122 [i.18] to the IN-CSE.

The message includes the following information.

- A response code of 201 CREATED

- The *URI* of the QoS Session Subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/ 3gpp-as-session-with-qos/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.

- The response payload will include a *AsSessionWithQoSSubscription* data structure as specified in 3GPP TS 29.122 [i.18] that includes the attributes present in the request along with the following additional attributes:

    - *self* is configured with a URI to the resource created by the SCEF for the request

Step 6: The IN-CSE returns response to Originator.

8.12.4.3 QoS Session request processing procedure

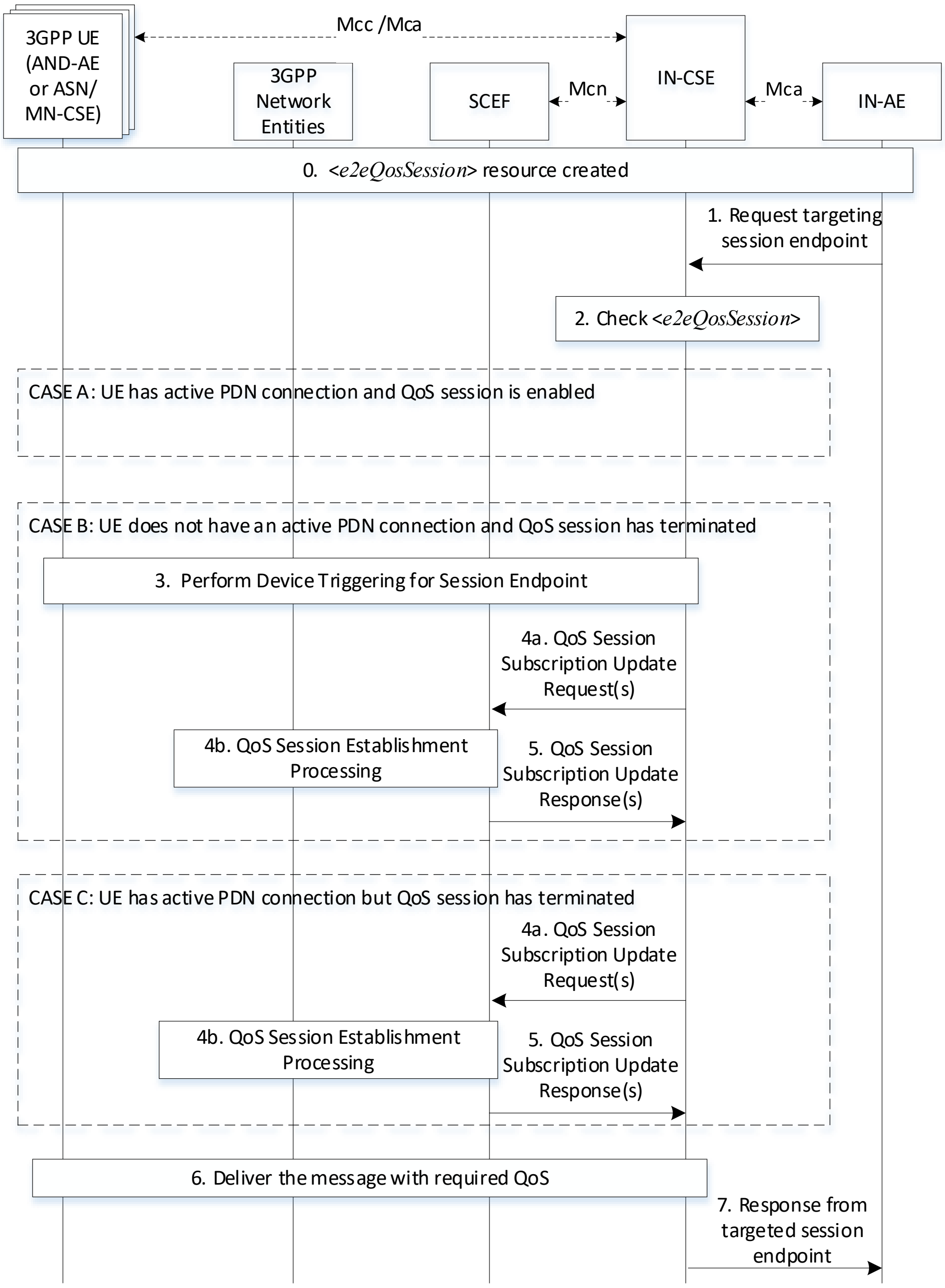

Mcc /Mca
3GPP UE (AND-AE or ASN/ MN-CSE)
3GPP Network Entities
SCEF
Mcn
IN-CSE
Mca
IN-AE
0. <e2eQosSession> resource created
1. Request targeting session endpoint
2. Check <e2eQosSession>
CASE A: UE has active PDN connection and QoS session is enabled
CASE B: UE does not have an active PDN connection and QoS session has terminated
3. Perform Device Triggering for Session Endpoint
4a. QoS Session Subscription Update Request(s)
4b. QoS Session Establishment Processing
5. QoS Session Subscription Update Response(s)
CASE C: UE has active PDN connection but QoS session has terminated
4a. QoS Session Subscription Update Request(s)
4b. QoS Session Establishment Processing
5. QoS Session Subscription Update Response(s)
6. Deliver the message with required QoS
7. Response from targeted session endpoint

Figure 8.12.4.3-1: Setting up 3GPP session with required QoS

Step 0: <e2eQosSession> created and IN-CSE creates QoS Session Subscription to SCEF

Step 1: The IN-AE sends a request that targets a E2E QoS session endpoint (e.g. ASN/MN-CSE)

The IN-AE sends a request to the IN-CSE that targets an entity that is configured as an E2E QoS session endpoint within a <*e2eQosSession*> resource hosted by the IN-CSE.

Step 2: The IN-CSE receives and processes the request and checks <*e2eQosSession*> resources

The IN-CSE processes the received request and obtains the targeted end point from the *To* parameter. Then IN-CSE checks the targeted end point and *From* parameters to see if they match with any *sessionEndpoints* configured within the <*e2eQosSession*> resources hosted by the IN-CSE. If a match is found, the IN-CSE then checks *To* parameter in the request to see if the resource ID matches with any *resourceIDList* of the *e2eQosRequirements* configured within the same <*e2eQosSession*> resource. If a match is found, the IN-CSE checks whether the QoS session is enabled or not. The IN-CSE also checks whether the entity targeted by the request has an active 3GPP PDN connection and is reachable by the IN-CSE.

CASE A: Both of these checks are successful. The IN-CSE proceeds to Step 6.

CASE B: The targeted entity has an inactive 3GPP PDN connection (i.e. ASN/MN-CSE or ADN-AE *pointOfAccess* information is not configured or IN-CSE detects failed communication with ASN/MN-CSE or ADN-AE) then the IN-CSE proceeds to Step 3.

CASE C: The targeted entity has an active 3GPP PDN connection (i.e. ASN/MN-CSE or ADN-AE *pointOfAccess* information is configured), but the QoS session has been disabled (*e2eQosStatus* is set to DISABLED or USAGE_EXHAUSTED). The IN-CSE proceeds to Step 4.

Step 3: The IN-CSE triggers the targeted E2E QoS session endpoint entity.

The targeted entity is registered to the IN-CSE and uses an underlying 3GPP network, but does not have an active 3GPP PDN connection to the IN-CSE, the IN-CSE sends a device trigger request to the entity to have it establish a 3GPP PDN connection to the IN-CSE. The IN-CSE then checks whether the QoS session is enabled or not. If the QoS session has been disabled (*e2eQosStatus* is set to DISABLED or USAGE_EXHAUSTED) the IN-CSE proceeds to Step 4, otherwise Step 6.

Step 4: The IN-CSE sends a request to update the QoS Session Subscription to re-enable the QoS session

If the configured *e2eQosRequirements* permit the IN-CSE to request that the QoS session be re-enabled when the *e2eQosStatus* is set to DISABLED or USAGE_EXHAUSTED, the IN-CSE may execute this step. Otherwise, the IN-CSE can either choose to continue processing the request in a best-effort fashion or generate an error indicating that it is unable to process the request since the QoS session is not enabled.

For each QoS session endpoint that connects to the IN-CSE via an underlying 3GPP network connection and that has an active PDN connection, the IN-CSE sends a AsSessionWithQoSSubscription Request to the SCEF.

The IN-CSE sends a request to update to AsSessionWithQoSSubscription Request from the IN-CSE to the SCEF contains information as specified in 3GPP TS 29.122 [i.18]. Such information includes:

- An HTTP PUT method is used
- *URI* is set to *{apiRoot}/3gpp-as-session-with-qos/v1/{scsAsId}/subscriptions/{subscriptionID}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.
- The request payload includes an *AsSessionWithQoSSubscription* data structure as specified in 3GPP TS 29.122 [i.18] with the following attributes:
    - *supportedFeatures* is set to a string value of "0" indicating the IN-CSE does not support the QoS Session negotiable features specified in 3GPP TS 29.122 [i.18].
    - *notificationDestination* is set to a URI that the SCEF can target QoS session related notifications towards. The value of this URI shall be based on internal IN-CSE policies.
    - *flowInfo* includes the following attributes:
        - *flowId* is set to a integer value that describes the IP flow. A value is assigned by the IN-CSE according local policy. The value that is used is unique within the scope of the IN-CSE.
        - *flowDescriptions* is an array of strings configured with two entries. The first entry in the array is an IP flow description for oneM2M requests and responses flowing from the IN-CSE to the QoS session endpoint applicable to this request. The second entry in the array is an IP flow description for oneM2M requests and responses flowing in the reverse direction from the QoS session endpoint to the IN-CSE.
            - Entry #1 in the *flowDescriptions* array includes the following attributes:
                - *direction* is set to a value of *"*out"
                - *source IP address* is set to the IP address of the IN-CSE and *destination IP address* is set to the IP addresses configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

        - *protocol*: is set to a value of "TCP" or "UDP" based on the underlying transport configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request. For example, "TCP" is set if the protocol configured in the *pointOfAccess* is HTTP, MQTT or WebSocket. "UDP" is set if the protocol configured is CoAP.

        - *source port* is set to the port of the IN-CSE and *destination port* is set to the port configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

    - Entry #2 in the *flowDescriptions* array includes the following attributes:

        - *direction* is set to a value of "in"

        - *source IP address* is set to the IP address configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request and *destination IP address* is set to the IP address of the IN-CSE.

          NOTE: The order is reversed from the order used in Entry #1.

        - *protocol*: is set to a value of "TCP" or "UDP" based on the underlying transport configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request. For example, "TCP" is set if the protocol configured in the *pointOfAccess* is HTTP, MQTT or WebSocket. "UDP" is set if the protocol configured is CoAP.

        - *source port* is set to the port configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request and *destination port* is set to the port of the IN-CSE.

          NOTE: The order is reversed from the order used in Entry #1.

- *qosReference* is set to a pre-provisioned string value that maps to the *qosLevel*. This mapping is based on a SLA with the MNO. The *qosReference* serves as an identifier of the pre-defined QoS information pre-provisioned into the IN-CSE based on a SLA with the MNO.

- *ueIpvAddr* is set to the IPv4 address (if applicable) configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

- *ueIpvAddr* is set to the IPv6 address (if applicable) configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

- *usageThreshold* includes the following attributes:

    - *duration* is set to the amount of time in seconds that the QoS session is requested to remain active. The IN-CSE computes this duration by inspecting all of the <*e2eQosSession*> resources that it hosts and that have a session endpoint that matches the session endpoint applicable to this request. For any matches found, the IN-CSE will aggregate the *sessionSchedule* elements (if any) configured within the list of *e2eQosRequirements* tuples of these <e2eQosSession> resources. Based on the aggregated *sessionSchedule* elements and local policies, the IN-CSE will determine a duration of time to request. If no *sessionSchedule* elements are configured, the IN-CSE will base its determination solely on local policies.

    - *totalVolume* is set to a total number of bytes of data that are required to be exchanged between the IN-CSE and the session endpoint applicable to this request. The IN-CSE shall compute this number of bytes by inspecting all of the <*e2eQosSession*> resources that it hosts and that have a session endpoint that matches the session endpoint applicable to this request. For any matches found, the IN-CSE will sum all of the *numOfBytes* elements (if any) configured within the list of *e2eQosRequirements* tuples of these <e2eQosSession> resources. Based on the *numOfBytes* elements and local policies, the IN-CSE will determine an amount to request. If no *numOfBytes* elements are configured, the IN-CSE will base its determination solely on local policies.

- *sponsorInfo* may be set. If set, the value is a string based on a SLA with the MNO.
- *ethFlowInfo, macAddr, requestTestNotification* and *websockNotifConfig* are not supported by the present document and are not included.

Step 5: SCEF sends QoS Session Response(s) to IN-CSE.

The SCEF handles the AsSessionWithQoSSubscription Request together with the Mobile Core Network. The SCEF sends an AsSessionWithQoSSubscription Response that contains information as specified in 3GPP TS 29.122 [i.18] to the IN-CSE.

The message includes the following information.

- A response code of 200 OK
- The response payload will include a *AsSessionWithQoSSubscription* data structure as specified in 3GPP TS 29.122 [i.18] that includes the attributes present in the request along with the following additional attributes:

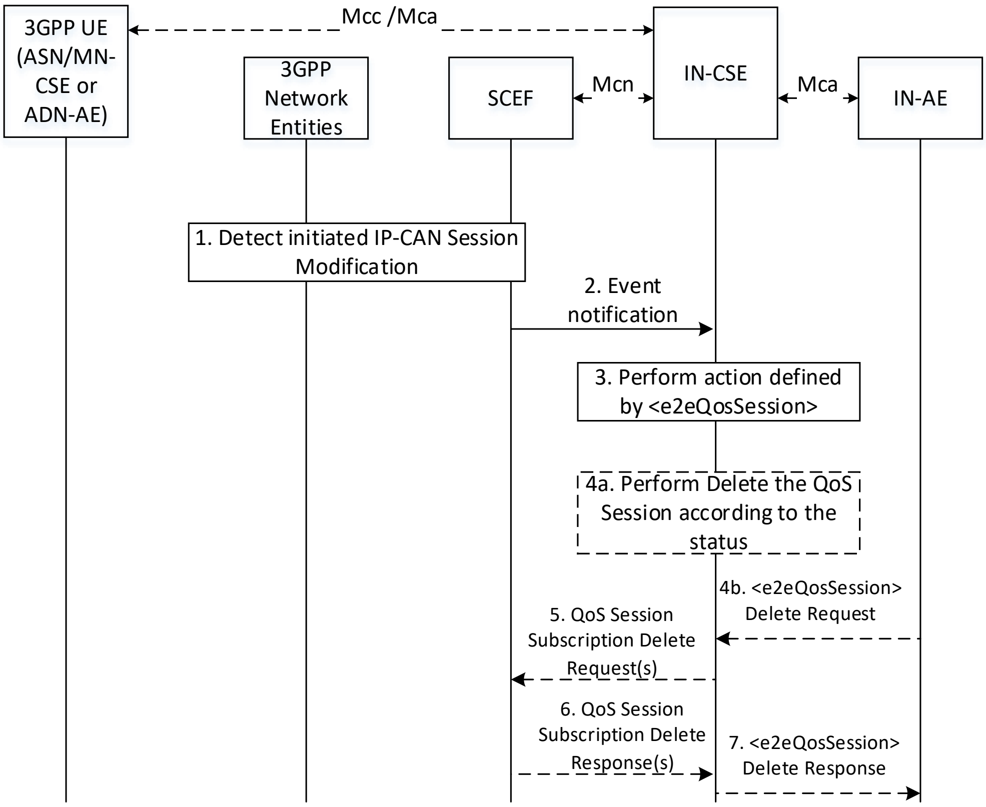
Step 6: The IN-CSE updates the <*e2eQosSession*> resource and returns response to Originator.

If the QoS session is enabled, the IN-CSE forwards the request to the targeted session endpoint entity. After receiving a response back from the targeted session endpoint, the IN-CSE prepares a response for the Originator (IN-AE). If the QoS session is disabled and the IN-CSE is un-successful in re-enabling it, then the IN-CSE can either choose to continue processing the request in a best-effort fashion or generate an error indicating that it is unable to process the request since the QoS session is disabled.

Step 7: The IN-CSE updates the <*e2eQosSession*> resource and returns response to Originator.

IN-CSE sends response to the IN-AE.

8.12.4.4 3GPP QoS status monitoring and report procedure



3GPP UE (ASN/MN-CSE or ADN-AE)
Mcc /Mca
3GPP Network Entities
SCEF
Mcn
IN-CSE
Mca
IN-AE
1. Detect initiated IP-CAN Session Modification
2. Event notification
3. Perform action defined by <e2eQosSession>
4a. Perform Delete the QoS Session according to the status
4b. <e2eQosSession> Delete Request
5. QoS Session Subscription Delete Request(s)
6. QoS Session Subscription Delete Response(s)
7. <e2eQosSession> Delete Response

Figure 8.12.4.4-1: 3GPP QoS status report procedure

Step 1: The 3GPP network entities detect a bearer level event.

The 3GPP entities may notify the SCEF about bearer level events for the Rx session (e.g., transmission resources are released/lost) with an IP-CAN Session Modification as described in TS 23.203[i.11].

Step 2: SCEF sends Status notification message to IN-CSE.

When the SCEF receives information of a status change in step 1, the SCEF creates and sends an Event Notification message to the IN-CSE as specified in 3GPP TS 29.122 [i.18].

The Event Notification request includes the following:

- *event* indicates the event reported by the SCEF and is configured with one of the following enumerated values as specified in 3GPP TS 29.122 [i.18]
  - SESSION_TERMINATION, LOSS_OF_BEARER, RECOVERY_OF_BEARER, RELEASE_OF_BEARER, USAGE_REPORT.
- *accumulatedUsage* indicates the amount of time in seconds that the QoS session was used and the amount of data bytes transferred via the QoS session when *event* is USAGE_REPORT. This notification is sent when the usage exceeds the values defined in the *usageThreshold* configured in the AsSessionWithQoSSubscription.
- *flowIds* is configured with the same value of *flowId* in the AsSessionWithQoSSubscription.

Step 3: IN-CSE performs the action according to the status

When the IN-CSE receives the Event Notification, the IN-CSE will map the *event* and *accumulatedUsage* to the QoS session status of <*e2eQosSession*> and performs the action according to the status.

3GPP event	oneM2M QoS session status
SESSION_TERMINATION	DISABLED
LOSS_OF_BEARER	DISABLED
RELEASE_OF_BEARER	DISABLED
RECOVERY_OF_BEARER	ENABLED
USAGE_REPORT	ENABLED (if accumaltedUsage indicates duration/volume has not been exhausted) USAGE_EXHAUSTED (if accumaltedUsage indicates duration/volume has been exhausted)

Step 4 (Optional): IN-CSE requests to delete QoS Session.

If the *e2eQosPolicies* attribute of the <*e2eQosSession*> resource is configured, then the IN-CSE evaluates and performs the configured action(s).

For example, if the configured action is DELETE when status equals DISABLED, then the IN-CSE will delete any existing QoS Session Subscription(s) to the underlying 3GPP network and also delete the <e2eQosSession> resource.

An IN-AE can also issue a request to delete an <e2eQosSession> resource. When the IN-CSE receives this request, it will delete any existing QoS Session Subscription(s) to the underlying 3GPP network and also delete the <e2eQosSession> resource.

Step 5 (Optional): IN-CSE sends delete request(s) for any existing QoS Session Subscription(s) to the underlying 3GPP network

The IN-CSE sends a DELETE request targeting the URI of the subscription resource corresponding to this AsSessionWithQoSSubscription.

For each QoS session subscription associated with the <*e2eQosSession*> resource being deleted, the IN-CSE sends a AsSessionWithQoSSubscription DELETE Request to the SCEF. The request to delete a AsSessionWithQoSSubscription contains information as specified in 3GPP TS 29.122 [i.18]. Such information includes:

- An HTTP DELETE method is used
- *URI* is set to *{apiRoot}/3gpp-as-session-with-qos/v1/{scsAsId}/subscriptions/{subscriptionID}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.

Step 6 (Optional): SCEF sends QoS Session Response(s) to IN-CSE.

The SCEF handles the AsSessionWithQoSSubscription DELETE Request together with the Mobile Core Network. The SCEF sends an AsSessionWithQoSSubscription DELETE Response that contains information as specified in 3GPP TS 29.122 [i.18] to the IN-CSE.

The message includes the following information.

- A response code of 204 No Content

If the IN-CSE receives a 204 No Content response code from the SCEF, it deletes the <*e2eQosSession*> resource. Otherwise, the IN-CSE does not delete the <*e2eQosSession*> resource.

Step 7 (Optional): IN-CSE returns response to IN-AE.

The IN-CSE sends a DELETE response back to the IN-AE.

8.13 Monitoring event (Monitoring Type: Number of UEs in an Area)

8.13.1 Description

The 3GPP SCEF functionality described in 3GPP TS 29.122 [i.18] supports APIs for monitoring specific events such as Number of UEs in an Area.. Based on the reports, the IN-CSE can start/stop throttling of requests initiated by or targeted towards its registree AEs and CSEs that are hosted on UEs residing in this geographical area to help manage the congestion levels in the Underlying 3GPP network.

TS-0026 [i.20] supports the ReportingNetworkStatus API to allow an IN-CSE to be notified of the network congestion status in a geographical area in the Underlying 3GPP network. The API is available if an MNO supports RAN Congestion Awareness Function (RCAF) in the 3GPP network, which reports the network congestion status in a geographical area to the SCEF. ETSI ISG MEC supports the number of E-RAB active defined in RNIS API, and a list of UEs in a particular location defined in Location service API. Table 8.13.1-1 shows the APIs comparison between MonitoringEvent API (Number of UEs in an Area) and ReportingNetworkStatus API.

Feature	MonitoringEvent API (Number of UEs in an Area)	ReportingNetworkStatus API
Number of UEs	✓	N/A
External Identifier of UE	✓	N/A
Congestion Level	N/A	✓ Indicate abstracted value (High, Medium, Low) or exact value (between 0 and 31)
Continuous reporting	N/A	✓
Support of 5G NEF	✓	T.B.D

Table 8.13.1-1: APIs comparison between MonitoringEvent API (Number of UEs in an Area) and ReportingNetworkStatus API

Below are some possible use cases for use of the monitoring event for the number of UEs in an area. It is assumed that the IN-CSE is triggered to perform the procedure by its local policy and uses the location information deployed by an MNO (e.g. eNBs, CGIs).

1) Use case 1: Congestion analysis with the External Identifiers of ADN-AEs and ASN/MN-CSEs hosted on UEs in an area.

In this use case it may be assumed that Area A is identified as a congested area by using ReportingNetworkStatus API. An M2M Service Provider wants to ensure that a particular group of ASN/MN-CSEs and/or ADN-AEs hosted on UEs in Area A maintains a high quality of service by performing additional monitoring procedures. The group may be identified in the Underlying Network by an External Group Identifier available at the IN-CSE. The IN-CSE sends a Monitoring Event Request with the External Group Identifier and the location information of Area A to the corresponding SCEF. When the IN-CSE receives a Monitoring Event Response from the SCEF, the IN-CSE receives the number of group member UEs found at the Area A.

Note that and the External Identifier(s) of the registree ASN/MN-CSEs/ADN-AEs may or may not be provided in the response, depending on MNO configuration of MME/SGSN.

Based on this information, the IN-CSE can take necessary measures such as adjusting other monitoring procedures for the group. Based on this information the IN-CSE may take other actions, such as modifying the <*schedule*> resource of the group members.. Upon detecting an updated *scheduleElement,* the group members will modify when they send requests and make themselves available to receive requests.

2) Use case 2: Congestion analysis for Edge/Fog Computing (Fog Node communicates with a SCEF via IN-CSE)

- The use case is described in clause 6.20 High-precision Road Map using Edge/Fog Computing of TR-0026 [i.21]. In order to minimize the amount of data that needs to be sent from or toward devices and to minimize the amount of processing required by an IN-CSE, a Fog Node sends a request of the congestion status of Area A to the IN-CSE. The IN-CSE retrieves a Monitoring Event for the number of UEs in Area A to SCEF via T8 API. After receiving a Monitoring Event Notification, the IN-CSE sends a response of the congestion status of Area A to the Fog Node. Then the Fog Node analyzes the congestion level in Area A. Based on the congestion level analysis, the Fog Node starts throttling of requests initiated by or targeted towards ADN-AEs and ASN/MN-CSEs hosted on UEs in the Area A.

- It is assumed that the Fog Node communicates with a SCEF via the IN-CSE.

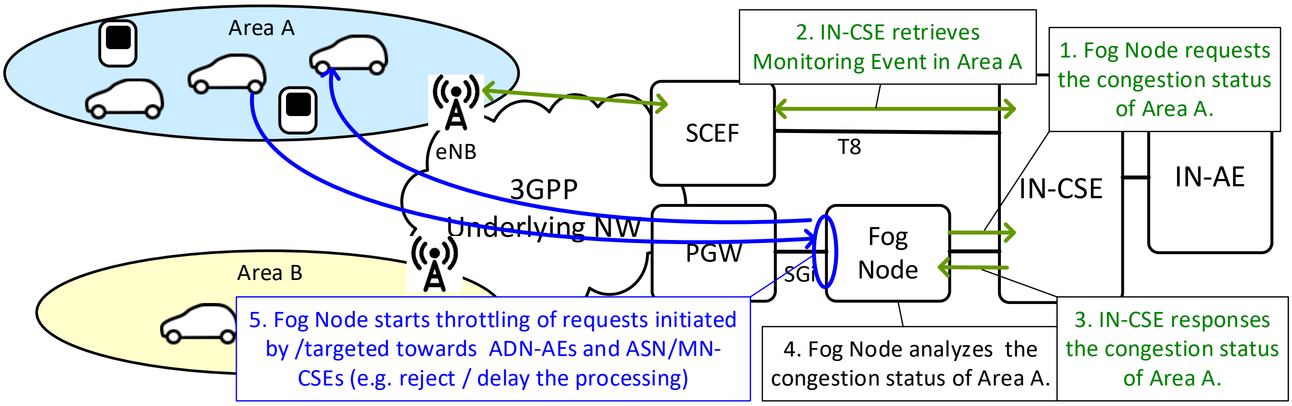

Area A
eNB
3GPP
Underlying NW
Area B
SCEF
T8
PGW
SGi
Fog
Node
IN-CSE
IN-AE
2. IN-CSE retrieves Monitoring Event in Area A
1. Fog Node requests the congestion status of Area A.
5. Fog Node starts throttling of requests initiated by /targeted towards ADN-AEs and ASN/MN-CSEs (e.g. reject / delay the processing)
4. Fog Node analyzes the congestion status of Area A.
3. IN-CSE responses the congestion status of Area A.

Figure 8.13.1-1: Use case 2: Congestion analysis with Edge/Fog Computing (Fog Node communicates with a SCEF via IN-CSE)

3) Use case 3: Congestion analysis for Edge/Fog Computing (Fog Node communicates with a SCEF directly via T8 IF)

The use case is described in clause 7.3.1 and 7.3.2 of TR-0052, which provide oneM2M Platform Optimization Scenarios by using Monitoring Event API for the number of UEs in an area.

In this case, the Fog Node hosts a MN-CSE and retrieves congestion information from 3GPP Underlying Network by communicating with a SCEF directly via T8 interface. The communication procedure with the Fog Node is currently FFS by WI-0080 Edge and Fog Computing.

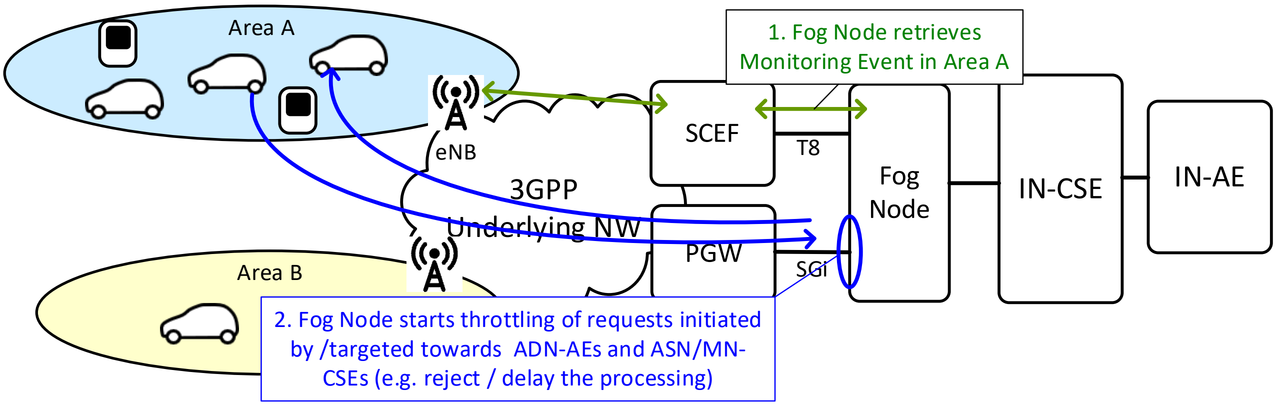

Area A
eNB
3GPP
Underlying NW
Area B
SCEF
T8
PGW
SGi
Fog
Node
IN-CSE
IN-AE
1. Fog Node retrieves Monitoring Event in Area A
2. Fog Node starts throttling of requests initiated by /targeted towards ADN-AEs and ASN/MN-CSEs (e.g. reject / delay the processing)

Figure 8.13.1-2: Use case 3: Congestion analysis with Edge/Fog Computing (Fog Node communicates with a SCEF directly via T8 IF)

4) Use case 4: Congestion analysis of 4G UEs and 5G UEs

- If a 3GPP Underlying Network supports both SCEF and NEF, the IN-CSE can retrieve the number of 4G UEs and 5G UEs in each area and analyze the congestion level at the areas.

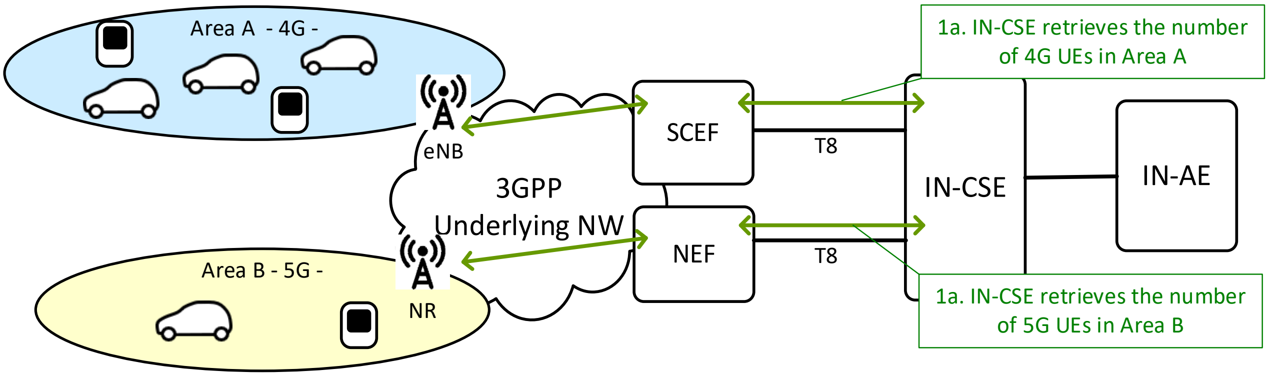

Area A - 4G -
1a. IN-CSE retrieves the number of 4G UEs in Area A
eNB
SCEF
T8
3GPP Underlying NW
IN-CSE
IN-AE
NEF
T8
Area B - 5G -
NR
1a. IN-CSE retrieves the number of 5G UEs in Area B

Figure 8.13.1-3: Use case 4: Congestion analysis of 4G UEs and 5G UEs

8.13.2 Feature Gap Analysis

The 3GPP defined term 'SCS' in the flows corresponds to oneM2M IN-CSE. The service flows defined in 3GPP TS23.682 [i.5] are used in the following section as informative information only. The oneM2M focus is on the T8 API of SCEF.

8.13.2.1 Monitoring event configuration via MME/SGSN.

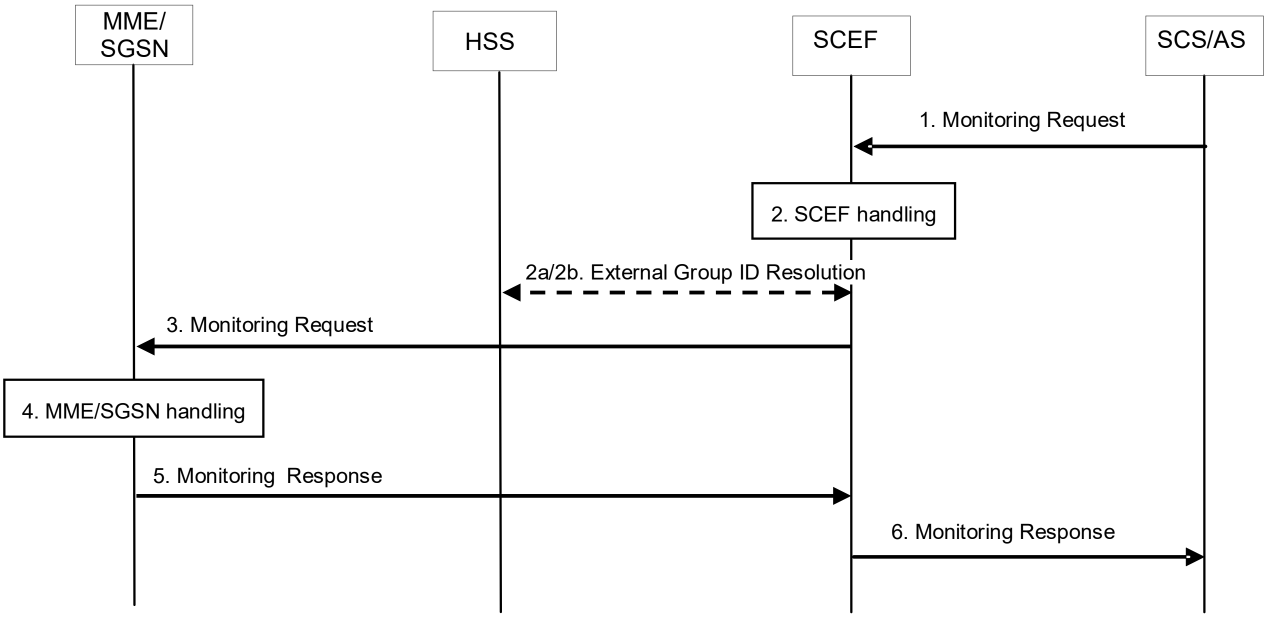


Figure 8.13.2.1-1: Monitoring event configuration via MME/SGSN [i.5]

Figure 8.13.2.1-1 illustrates the procedure of Monitoring event configuration via MME/SGSN, described in 3GPP TS23.682 [i.5]. The monitoring event Number of UEs in an area is applicable for the monitoring event configuration via MME/SGSN, and allows the SCS/AS to ask for the number of UEs that are in the geographic area described by the SCS/AS. The SCS/AS may request information about the UEs that the 3GPP network knows, by its normal operation, to be within the area (Last Known Location). For this monitoring event, only one-time reporting is supported. When the SCS/AS includes External Group Identifier(s) in the monitoring request, the MME/SGSN counts the number of UEs in the geographic area per External Group Identifier.

The involved steps are described below:

Step 1: SCS (IN-CSE) sends a Monitoring Request to the SCEF. The SCS sets Monitoring Type to "Number of UEs present in a geographic area (NUMBER_OF_UES_IN_AN_AREA)" and adds Location Type and Location Area before sending Monitoring Request to the SCEF. The request may optionally include External Group Identifier(s).

Step 6: The SCEF sends a Monitoring Response (Monitoring Event Report, Cause) message to the SCS (IN-CSE) to acknowledge acceptance of the Monitoring Request and to provide the requested monitoring information in Monitoring Event Report parameter. When External Identifiers are included in the results that are received from the MME(s)/SGSN(s) in step 5, they are included by SCEF in the response to the SCS/AS.

Table 8.13.2.1-1 shows the parameters for the Monitoring event API for the number of UEs in a geographic area, as described in 3GPP TS 29.122 [i.18]. , Table 8.13.2.1-2 and Table 8.13.2.1-3 show the parameters to be provided to indicate the location via *locationArea* and *locationArea5G,* respectively.

Table 8.13.2.1-1: Parameters for Number of UEs in a geographic area

Parameter	Cardinality	Description
supportedFeatures	0..1	supportedFeatures is used to negotiate the supported optional features of the API. This attribute shall be provided in the POST request and in the response of successful resource creation. If it is set to the value of “8” (Number_of_UEs_in_an_area_notification), it indicates support for the number of UEs present in a given geographic area notifications and the feature supports the pre-5G (e.g. 4G) requirement. If it is set to the value of “12” (Number_of_UEs_in_an_area_notification_5G), it indicates support for the number of UEs present in a given geographic area notifications and the feature supports the 5G requirement (only be supported in 5G).
notificationDestination	1	A URI of a notification destination that T8 message shall be delivered to.
monitoringType	1	Enumeration of monitoring type. It indicates "NUMBER_OF_UES_IN_AN_AREA".
maximumNumberOfReports	0..1	Identifies the maximum number of event reports to be generated by the HSS, MME/SGSN. For this monitoring event only One-time reporting is supported and the parameters shall be ignored by the SCEF if present in the request.
monitorExpireTime	0..1	Identifies the absolute time at which the related monitoring event request is considered to expire.
locationType	0..1	If "monitoringType" is "NUMBER_OF_UES_IN_AN_AREA", this parameter shall be included to identify whether the request is for Current Location or Last known Location. In this 3GPP release, locationType shall be set to "LAST_KNOWN_LOCATION".
locationArea	0..1	If "monitoring-Type" is "NUMBER_OF_UES_IN_AN_AREA", this parameter may be included to indicate the area within which the SCS/AS requests the number of UEs, described in Table 8.13.2.1-2. The *supportedFeatures* “Number_of_UEs_in_an_area_notification” is applicable for this parameter.
locationArea5G	0..1	If "monitoring-Type" is "NUMBER_OF_UES_IN_AN_AREA", this parameter may be included to indicate the area within which the SCS/AS requests the number of UEs, described in Table 8.13.2.1-3. The *supportedFeature* “Number_of_UEs_in_an_area_notification_5G” is applicable for this parameter.
externalGroupId	0..1	Identifies a user group as defined in 3GPP TS 23.682 [i.5]. It is used on the interface between the SCS/AS and the SCEF and on the interface between the SCEF and the HSS.
addExtGroupIds	0..N	Identifies a user group as defined in 3GPP TS 23.682 [i.5]. For the feature "Number_of_UEs_in_an_area notification", "*externalGroupId*" may be included for single group and "*addExtGroupIds*" may be included for multiple groups but not both.
self	0..1	Link to this resource. This parameter shall be supplied by the SCEF in responses.
uePerLocationReport	0..1	If "monitoringType" is "NUMBER_OF_UES_IN_AN_AREA", this parameter shall be included to indicate the number of UEs found at the location.
externalIds	0..N	Each element indicates an External Identifier of the UE.

Table 8.13.2.1-2: Parameters of locationArea

Parameter	Cardinality	Description

cellId	0..N	Indicates a Cell Global Identification of the user which identifies the cell the UE is registered.
enodeBId	0..N	Indicates an eNodeB in which the UE is currently located.
routingAreaId	0..N	Identifies a Routing Area Identity of the user where the UE is located.
trackingAreaId	0..N	Identifies a Tracking Area Identity of the user where the UE is located.
geographicArea	0..N	Identifies a geographic area of the user where the UE is located.
civicAddress	0..N	Identifies a civic address of the user where the UE is located.

Table 8.13.2.1-3: Parameters of locationArea5G

Parameter	Cardinality	Description
geographicAreas	0..N	Identifies a list of geographic area of the user where the UE is located.
civicAddresses	0..N	Identifies a list of civic addresses of the user where the UE is located.
nwAreaInfo	0..1	This IE represents the network area information of the user where the UE is located.

8.13.3 Key Issues and Requirements

8.13.3.1 Key SCEF NorthBound API Requirements

N/A

8.13.3.2 Potential impact on SCEF SouthBound Interface

N/A

8.13.3.3 Further 3GPP requirements and clarifications

N/A

8.13.3.4. oneM2M Key Issues

- Provide support for number of UEs in an area in Monitoring event.
- Provide support for configuration of 3GPP External Group Identifier for ASN-CSE/MN-CSE hosted on a UE .

8.13.4 oneM2M Solutions

8.13.4.1 Solution 1

8.13.4.1.1 Impacted Resources and Attributes

To implement this solution, the following attributes are proposed:

- The new attribute *M2M-Ext-Group-ID* corresponding to the *externalGroupId* as specified in 3GPP TS29.122 [i.18] is added to the <*AE*> resource.
- The *externalGroupID* attribute for the <*remoteCSE*> resource is renamed as *M2M-Ext-Group-ID* and the description of the *M2M-Ext-Group-ID* is updated to be more generic and consistent with *M2M-Ext-ID* attribute.

8.13.4.1.1.1 Modified <remoteCSE > resource

The *externalGroupID* attribute for the <*remoteCSE*> resource is renamed as *M2M-Ext-Group-ID* and the description of the *M2M-Ext-Group-ID* is updated as shown in the table below.

Table 8.13.4.1.1.1-1: Modified attribute of <*remoteCSE*> resource

Attributes of <*remoteCSE*>	Multiplicity	RW/ RO/ WO	Description	<*remoteCSEAnnc*> Attributes
M2M-Ext-Group-ID	0..1	RW	Supported when Registrar CSE is an IN-CSE. It is used by an M2M Service Provider (M2M SP) when services targeted to a group of M2M Devices are requested from the Underlying Network. It is assumed to be a globally unique ID exposed by the underlying network to identify a group of M2M Devices (e.g. ADN, ASN, MN) for group related services.	OA

8.13.4.1.1.2 Modified <AE> resource

New attribute for the <*AE*> resource is proposed as shown in the table below.

Table 8.13.4.1.1.2-1: New Attributes of <*AE*> resource

Attributes of <*remoteCSE*>	Multiplicity	RW/ RO/ WO	Description	<*remoteCSEAnnc*> Attributes
M2M-Ext-Group-ID	0..1	RW	Supported when Registrar CSE is an IN-CSE. It is used by an M2M Service Provider (M2M SP) when services targeted to a group of M2M Devices are requested from the Underlying Network. It is assumed to be a globally unique ID exposed by the underlying network to identify a group of M2M Devices (e.g. ADN, ASN, MN) for group related services.	OA

8.13.4.1.2 Proposed Flow

8.13.4.1.2.1 Monitoring event for Number of UEs in an Area

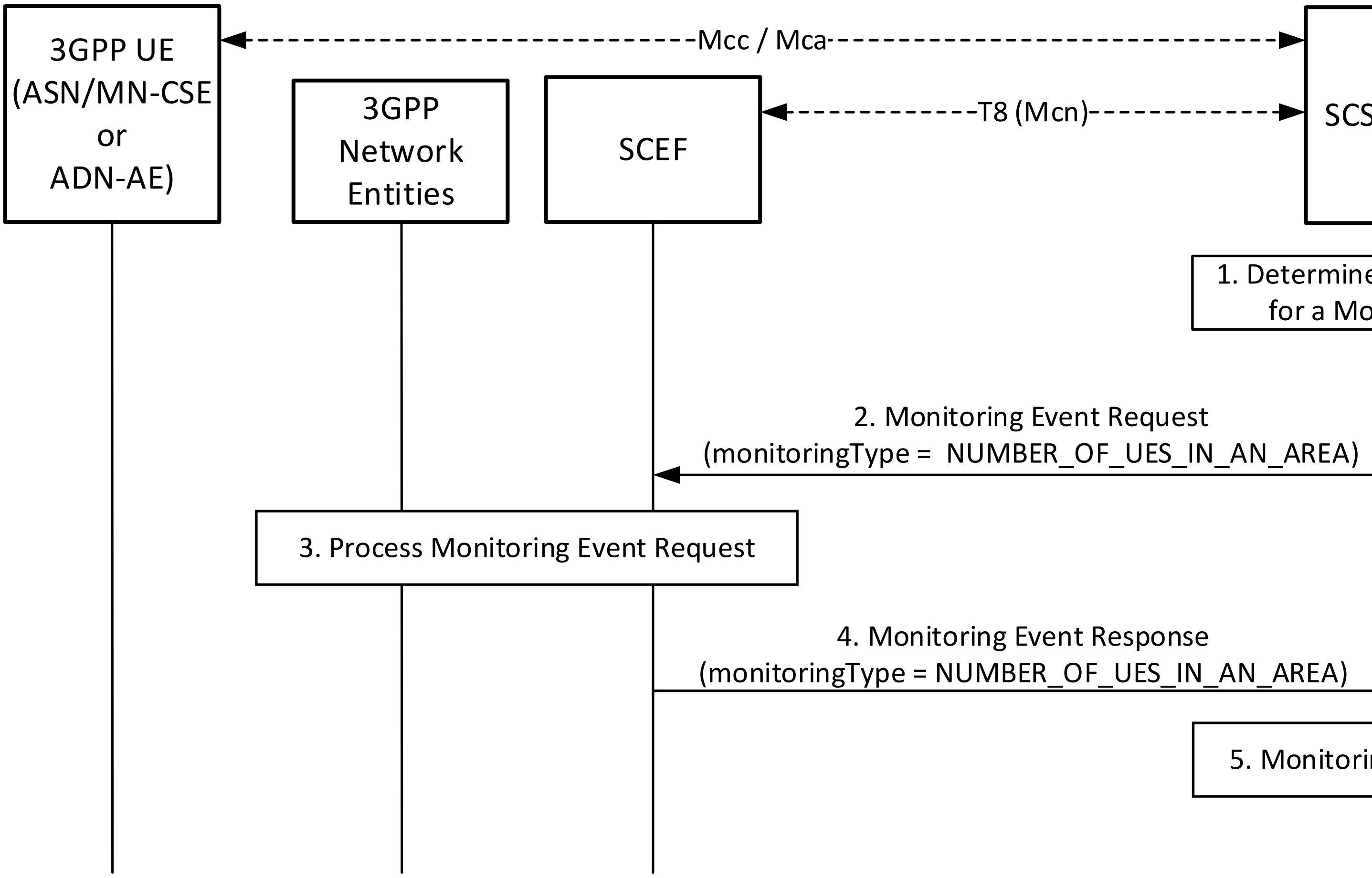

3GPP UE (ASN/MN-CSE or ADN-AE)
Mcc / Mca
3GPP Network Entities
SCEF
T8 (Mcn)
SCS
1. Determine
for a Mo
2. Monitoring Event Request (monitoringType = NUMBER_OF_UES_IN_AN_AREA)
3. Process Monitoring Event Request
4. Monitoring Event Response (monitoringType = NUMBER_OF_UES_IN_AN_AREA)
5. Monitori

Figure 8.13.4.1.2.1-1: Monitoring event for Number of UEs in an Area

Pre-conditions:

There is a relationship in place between the Service Provider and MNO allowing the IN-CSE to request Monitoring events for number of UEs present in an area. The method for establishing this relationship is outside the scope of the present document.

An ASN/MN-CSE or ADN-AE registers with the IN-CSE and configures the *M2M-Ext-ID* attribute of its <*remoteCSE*> or <*AE*> resource. The IN-CSE examines the *M2M-Ext-ID* and recognizes that it is associated with an MNO that it has a relationship with.

If the deployment uses External Group Identifier as described in 3GPP TS29.122 [i.18], when ASN/MN-CSEs or ADN-AEs register with the IN-CSE they uses *externalGroupId* information to configure the *M2M-Ext-Group-ID* of the corresponding <*remoteCSE*> or <*AE*> resources (see clause 8.x.4.1.2.2 for changes UE Attach with oneM2M Registration Procedure when *M2M-Ext-Group-ID* is configured).

The IN-CSE is configured to be able to determine a location area (i.e. *locationArea* and/or *locationArea5G*) of interest in the Underlying Network. The IN-CSE may use its location services or other location information. How the location area of interest is determined is outside the scope of the present document.

The IN-CSE is configured with system defaults for:

- The specified actions to generate the network congestion levels based on the number of UEs in an area.
- The specified actions to take based on the severity of each congestion level.

The configuration methods for these system defaults are outside the scope of the present document.

The ADN-AE's or the ASN/MN-CSE's <*node*> resource hosted on the IN-CSE has a child <*schedule*> resource and the IN-CSE has permissions to update it. The ADN-AE or the ASN/MN-CSE has a <*subscription*> for its <*schedule*> resource and when it receives a notification from the IN-CSE, it updates its communication schedule accordingly.

Step 1: IN-CSE determines to send a Monitoring Event Request for number of UEs in a geographic area.

The IN-CSE determines to send to a SCEF a Monitoring Event Request for number of UEs present in an area of interest. If applicable, the IN-CSE may determine only the number of UEs within the group identified by the *M2M-Ext-Group-ID*. If *M2M-Ext-Group-ID* information is not applicable, all the UEs present in the area will be identified.

Step 2: IN-CSE sends a Monitoring Event Request for the number of UEs in the area.

The IN-CSE sends a Monitoring Event Request for the geographical area of interest to the SCEF. The Monitoring Event Subscription request from the IN-CSE to the SCEF will comply with 3GPP TS 29.122 [i.18] as follows:

- An HTTP POST method will be used
- *URI* will be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/.* The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload will include a *MonitoringEventSubscription* data structure as specified in 3GPP TS 29.122 [i.18] with the following attributes:
    - *notificationDestination* will be set to a URI that the SCEF can target Location Reporting notifications towards. The value of this URI will be based on internal IN-CSE policies.
    - *monitoringType* will be set to NUMBER_OF_UES_IN_AN_AREA indicating the number of UEs in a given geographic area
    - *monitorExpireTime* is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE will configure this time based on Service Provider and MNO policies.
    - *locationType* will be set to LAST_KNOWN_LOCATION.
    - *supportedFeatures* will be set to a string value of "8" and/or "12" indicating support for Location Reporting notifications. If it is set to the value of "8" (Number_of_UEs_in_an_area_notification), the feature supports the pre-5G (e.g. 4G) requirement. If it is set to the value of "12" (Number_of_UEs_in_an_area_notification_5G), the feature supports the 5G requirement (only be supported in 5G).
    - *locationArea* and/or *locationArea5G* will be included to indicate the area of interest within which the IN-CSE requests the number of UEs. If *supportedFeatures* is set to the value of "8", the *locationArea* attribute is applicable. If *supportedFeatures* is set to the value of "12", the *locationArea5G* attribute is applicable.
    - *externalGroupId* will be set to the *M2M-Ext-Group-ID* if the deployment uses the External Group Identifier in step 0 and if the IN-CSE monitoring request targets identifying the number of UEs from a specific group in the area.
    - *requestTestNotification, websockNotifConfig, addExtGroupIds*, *maximumNumberOfReports* and *groupReportGuardTime* are not supported by the present document and will not be included.

Step 3: SCEF processes the Monitoring Event Request.

The SCEF processes the Monitoring Request together with the 3GPP network entities as described in 3GPP TS 29.122 [i.18].

Step 4: SCEF sends a Monitoring Event Response.

The SCEF sends a Monitoring Event Response to the IN-CSE to acknowledge the request has been accepted. This response is described in 3GPP TS 29.122 [i.18] and includes the following information.

- A response code of 201 CREATED.

- The *URI* of the Monitoring Event Subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.
- The response payload will include a *MonitoringEventReport* data structure as specified in 3GPP TS 29.122 [i.18] that includes the attributes present in the request along with the following additional attributes:
  - *ueCount* is configured to indicate the number of UEs found at the location. If an *externalGroupId* has been provided in the request, the count indicates the number of UEs from the given group which are found at the location.
  - *externalIds* is configured to indicate External Identifier(s) of the UEs included in the number of UEs found denoted by *ueCount.*

    Note that and the External Identifier(s) information may or may not be provided in the response, depending on MNO configuration of MME/SGSN.
  - *self* is configured with a URI to the resource created by the SCEF for the request.

Step 5: Monitoring Event handling at the IN-CSE.

The IN-CSE may use the information provided in the Monitoring Event Report to modify the <*schedule*> resource of the group members such that they modify the times they send or receive requests.

How the IN-CSE determines the use of the information received from the monitoring event is outside the scope of the current document and may be based on agreements with the MNO.

8.13.4.1.2.2 Enhancements to support configuration of 3GPP External Group Identifier

The UE Attach with oneM2M Registration Procedure is depicted in clause 6.3 of TS-0026 [i.20]. The following modifications are introduced in the procedure in Step 2a and 2b in order to support the new attribute for the 3GPP External Group Identifier as described in clause 8.13.4.1.1.

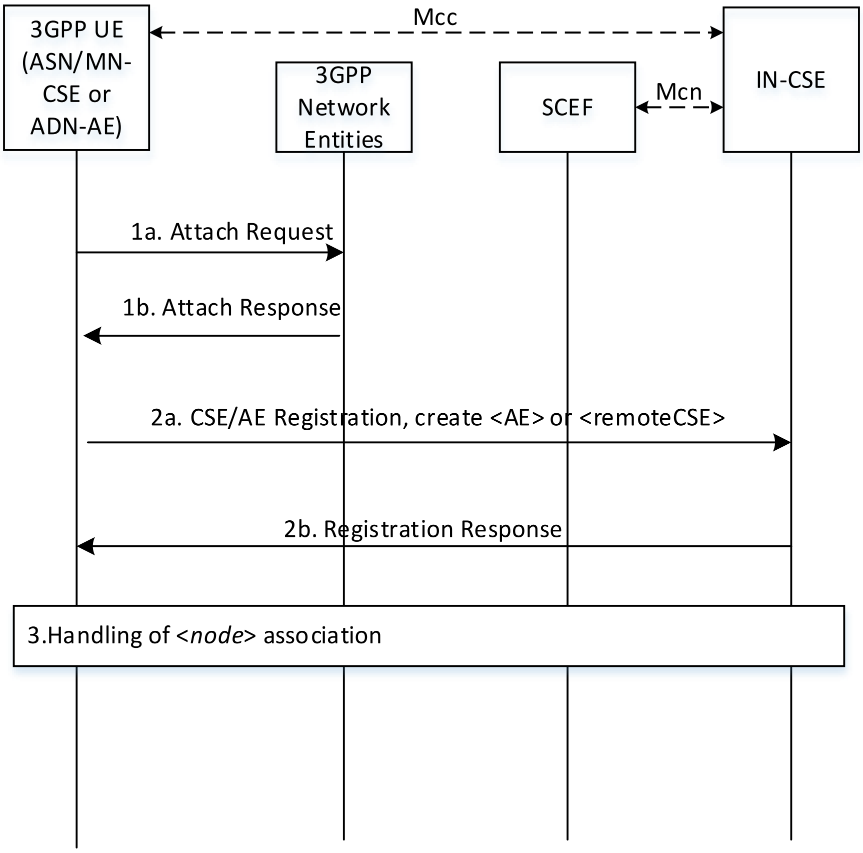

3GPP UE (ASN/MN-CSE or ADN-AE)
Mcc
3GPP Network Entities
SCEF
Mcn
IN-CSE
1a. Attach Request
1b. Attach Response
2a. CSE/AE Registration, create <AE> or <remoteCSE>
2b. Registration Response
3.Handling of <*node*> association

Figure 8.13.4.1.2.2-1 UE Attach Procedure with oneM2M Registration

All the steps not detailed below are executed as specified in clause 6.3 of TS-0026 [i.20].

Steps 2a and 2b: oneM2M Registration Request and Response

Information provided by the ASN/MN-CSE or ADN-AE(s) to the IN-CSE at this time will include, in addition to the other parameters specified (e.g. Trigger-Recipient-ID, etc.) the *M2M-Ext-Group-ID* used in the deployment. Note that not all the deployment UEs need to be provisioned with the same *M2M-Ext-Group-ID.*

In addition to the processing specified in clause 6.3 of TS-0026 [i.20] for this step: If configured, the *externalGroupId*s for each ASN/MN-CSE or ADN-AE(s) are stored as *M2M-Ext-Group-ID* attributes of the corresponding <*AE*> or <*remoteCSE*> resources created at this time.

9 UE Device Connection Efficiency

9.1 Introduction

In TS-0026 3GPP Interworking, clause 5 describes how oneM2M entities may be deployed in a 3GPP Network.

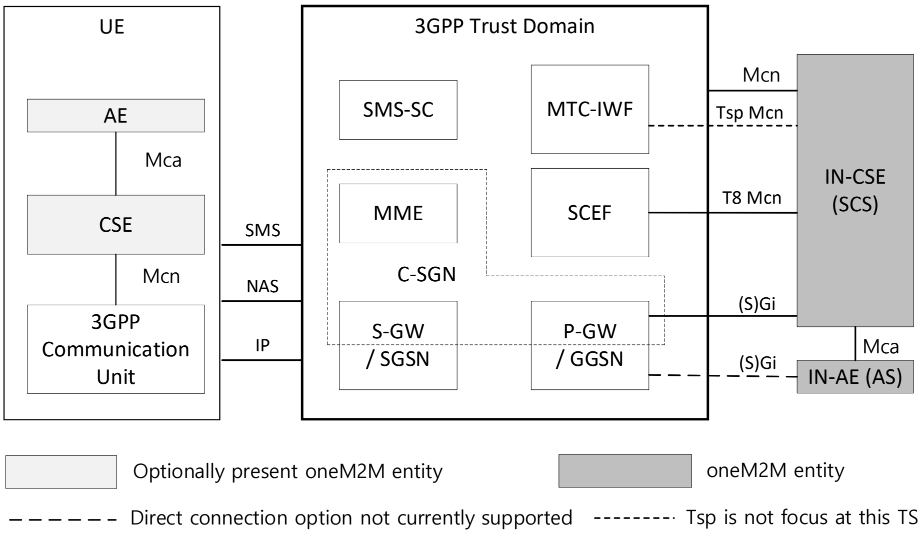


Figure 9.1-1: oneM2M Interfaces to the 3GPP Network

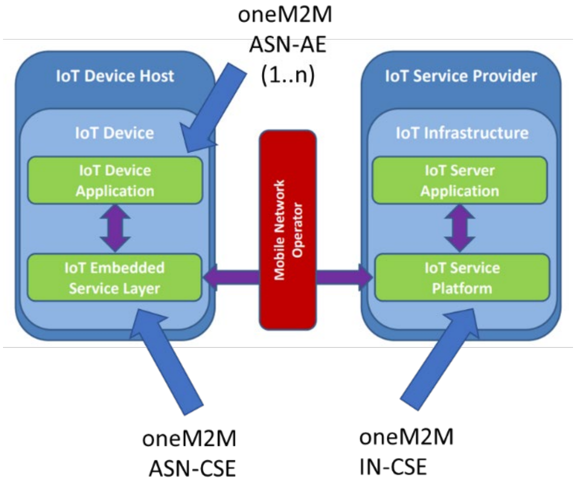
TS-0026 discusses how an IN-CSE can offer value-added features to a 3GPP deployment based on the SCEF features added in 3GPP Rel 10-15.

In this deployment the UE can optionally host a oneM2M AE and/or CSE. Specifically, The “MTC Applications” hosted on the UE may be deployed as follows:

- Application only: UE may be an ADN oneM2M entity
- Application and CSE: UE may be an ASN or MN oneM2M entity
- CSE only: UE may be a MN oneM2M entity
- Neither application nor CSE: UE may be a NoDN.

While TS-0026 discusses the possibility of a CSE being present on the UE, the specification does not describe what features or value-added services may be offered by the CSE hosted on the UE.

GSMA has published TS.34 IoT device Connection Efficiency Guidelines V 5.0, 08 January 2018, that defines requirements for an IoT Service architecture that includes an IoT Service and an IoT Device hosted on a UE to operate in a manner that is consistent with the design and deployment of the mobile network.



An initial analysis of TS.34 indicates that oneM2M has the basic framework in place to support these requirements. The gaps that need to be addressed in oneM2M are the capabilities that are specific to GSMA TS.34 device functionality. There are three main categories of functionality that IoT Devices hosted on a cellular device need to implement.

1. Communication management, where the device ensures that it operates according to communication policies, that may be dynamic based on mobile network condition.
2. Fault handling procedures, where the device handles unexpected events in a manner that does not impact the operation of the mobile network.
3. Management of the device components and policies that control the device behavior.

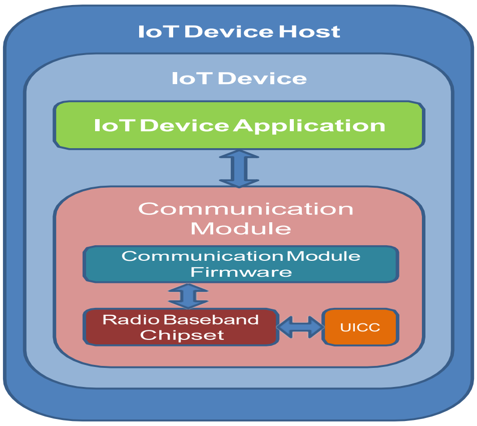
oneM2M has CMDH and Device Management services that are intended for these precise uses. The following sections will define the features and capabilities that a CSE hosted on a UE should implement to ensure safe operation on mobile networks.

By including these features in TS-0026, we can enhance the value-added services that oneM2M offers to address operational concern of MNOs.

9.2 Key Issues

9.2.1 Key Issue 1: <Device Management>

From GSMA TS.34 the following device Architecture is shown.



IoT Device Host – The application specific environment containing the IoT Device e.g. vehicle, utility meter, security alarm etc.

IoT Device – The combination of both the IoT Device Application and the Communication Module.

IoT Device Application – The application software component of the IoT Device that controls the Communications Module and interacts with an IoT Service Platform via the communications module.

Communication Module – The communications component which provides wide area (2G, 3G, 4G) radio connectivity. Comprising of Communications Module Firmware, Radio Baseband Chipset and UICC

Communications Module Firmware – The functionality within the Communications Module that provides an API to the IoT Device Application and controls the Radio Baseband Chipset.

Radio Baseband Chipset – The functionality within the communications module that provides connectivity to the mobile network.

UICC – The smart card used by a mobile network to authenticate devices for connection to the mobile network and access to network services.

Figure 1: Generalised IoT Device Architecture

9.2.1.1 Key issue details

There are multiple firmware and chipset parameters that SHALL be manageable from the Service Provider, or MNO. This issue leads to the need for additional customizations of <managementObject> resources, specific to mobile devices.

9.2.1.2 Potential requirements

Editor's Note: This clause will describe the potential requirements arising from the key issue.

EDITORS NOTE: New <managementObject> specializations and defined call flows when an oneM2M entities uses these resources.

9.2.2 Key Issue 2: <Communication Management>

Several requirements in GSMA TS.34 discuss the need to monitor the amount of communication, aggregate small communications into fewer large communications, etc. These requirements are aligned with the CMDH functionality described in TS-0001.

9.2.2.1 Key issue details

9.2.2.2 Potential requirements

Editor's Note: This clause will describe the potential requirements arising from the key issue.

EDITORS NOTE: examine existing policies for desired behaviors and possibly enhance the existing cmdh policies.

9.2.3 Key Issue 3: <Fault handling behaviors>

9.2.3.1 Key issue details

Several requirements in GSMA TS.34 discuss how to handle communication failures. For example:

TS.34_4.2_REQ_011	The IoT Embedded Service Layer should always be prepared to handle situations when communication requests fail. Communication retry mechanisms implemented within an IoT Device can vary and will depend on the importance and volume of downloaded data. Possible solutions can be: • Simple counting of failed attempts since the data connection was first established (often the easiest solution). • Monitoring the number of failed attempts within a certain period of time. For example, if the data connection is lost more than five times within an hour, then the request can be suspended. This can be a more reliable technique to avoid short but regular connection problems, such as when a device is moving away from one network cell to another. The data connection can be lost when the device switches between cells, but when the cell is providing good coverage; the request can be processed successfully. Depending upon the IoT Service, no communication request by the IoT Embedded Service Layer should ever be retried indefinitely – the request should eventually timeout and be abandoned. Note: The requirements contained within section 5.2 of this document describe the functionality that, when implemented within the Communications Module to monitor IoT Embedded Service Layer behaviour, ensures the retry mechanisms implemented within the IoT Embedded Service Layer do not prevent the normal operation of the mobile network.

9.2.3.2 Potential requirements

Editor's Note: This clause will describe the potential requirements arising from the key issue.

EDITORS NOTE These issues may require a combination of <managementObjects> and <cmdhPolicies>

9.3 Solutions

Editor's Note: This clause will contain the solutions that address the key issues in this area.

9.3.1 Solution 1: <solution name>

Editor's Note: Solutions within the area are not in any particular order but they are added incrementally (n = 1, 2, 3…) when new solution is identified. 'y' refers to the area.

9.3.1.1 Introduction

Editor's Note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the area.

<Text>

9.3.1.2 Solution details

Editor's Note: This clause will describe the solution.

<Text>

9.3.1.3 Evaluation

Editor's Note: This clause will contain a variety of evaluations of this solution.

EDITORS NOTE: Each evaluation will include the requirement ID(s) from GSMA TS.34 that is solved with the proposed solution

9.4 Conclusions

Editor's Note: This clause will contain the evaluation between the solutions, and the conclusions.

EDITORS NOTE: This will be a consolidated list of the requirements that are met by the solutions proposed.

Annex A : 5G NEF Northbound APIs

The NEF Northbound APIs are a set of APIs defining the related procedures and resources for the interaction between the NEF (Network Exposure Function) and the AF (Application Function). The APIs are specified in 3GPP TS 29.522 [i.19] of Release 15 (5G Phase1) and applicable for the architecture for 5GS (5G System). The APIs specify RESTful APIs that allow the AF to access the services and capabilities provided by 3GPP network entities and securely exposed by the NEF. The protocol level information of the NEF APIs refers to T8 APIs as specified in 3GPP TS 29.122 [i.18] such as the usage of HTTP, content type, notification, error handling, feature negotiation and the conventions for Open API specification files. Thus, some NEF APIs can be used for oneM2M TS-0026.

Table A-1 describes the northbound APIs which are applicable for both EPS and 5GS as defined in 3GPP TS29.522 [i. 19].

Table A-1: Reused APIs applicable for both EPS and 5GS [i.19]

API Name	Differences
ResourceManagementOfBdt	The "Bdt_5G" feature as described in 3GPP TS 29.122 [i.18] shall be supported in 5G.
PfdManagement	
MonitoringEvent	The "Number_of_UEs_in_an_area_notification_5G" feature as described in 3GPP TS 29.122 [i.18] shall be supported in 5G.
DeviceTriggering	
CpProvisioning	The "ExpectedUMT_5G" feature as described in 3GPP TS 29.122 [i.18] shall be supported in 5G.
ChargeableParty	The "EthChgParty_5G" feature as described in 3GPP TS 29.122 [i.18] shall be supported in 5G.
AsSessionWithQoS	The "EthAsSessionQoS_5G" feature as described in 3GPP TS 29.122 [i.18] shall be supported in 5G.

NOTE: PfdManagement, ChargeableParty and AsSessionWithQoS are currently not supported in oneM2M TS-0026.

History

Publication history		
V2.0.0	<30 Aug 2016>	Publication
V2.4.0	<28 Feb 2019>	

Draft history (to be removed on publication)		
V4.0.0	<22 May 2019>	This version of the document is based on TR-0024v2.4.0
V4.1.0	<03 Jun 2019>	SDS-2019-0079R05-TR-0024-3GPP_QoS_Solution_of_Resource SDS-2019-0130R03-TR-0024-3GPP_QoS_Solution_of_ServiceFlow
V4.2.0	<23 Aug 2019>	SDS-2019-0346-TR0024_UE_Device_connection_efficiency
V4.3.0	<06 Mar 2020>	SDS-2020-0037R01-TR-0024_E2E_QoS_Session_Editor's_Note_Cleanup_R4