oneM2M
Technical Report

Document Number	TR-0024-V2.0.0
Document Name:	3GPP_Rel13_IWK
Date:	2016-August-30
Abstract:	The document is a study of interworking between oneM2M Architecture and 3GPP Rel-13 architecture for Service Capability Exposure as defined in TS 23.682 V13.2.0.

Template Version:03June 2015 (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

1 Scope

The present document is a study of interworking between oneM2M Architecture and 3GPP Rel-13 architecture for Service Capability Exposure as defined in the release 13 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 13)".

[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".

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 uderlying 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 13 which is the focus of the present document. Refer to the following figure 5.3-1, taken from the release 13 version of 3GPP TS 23.682 [i.5].

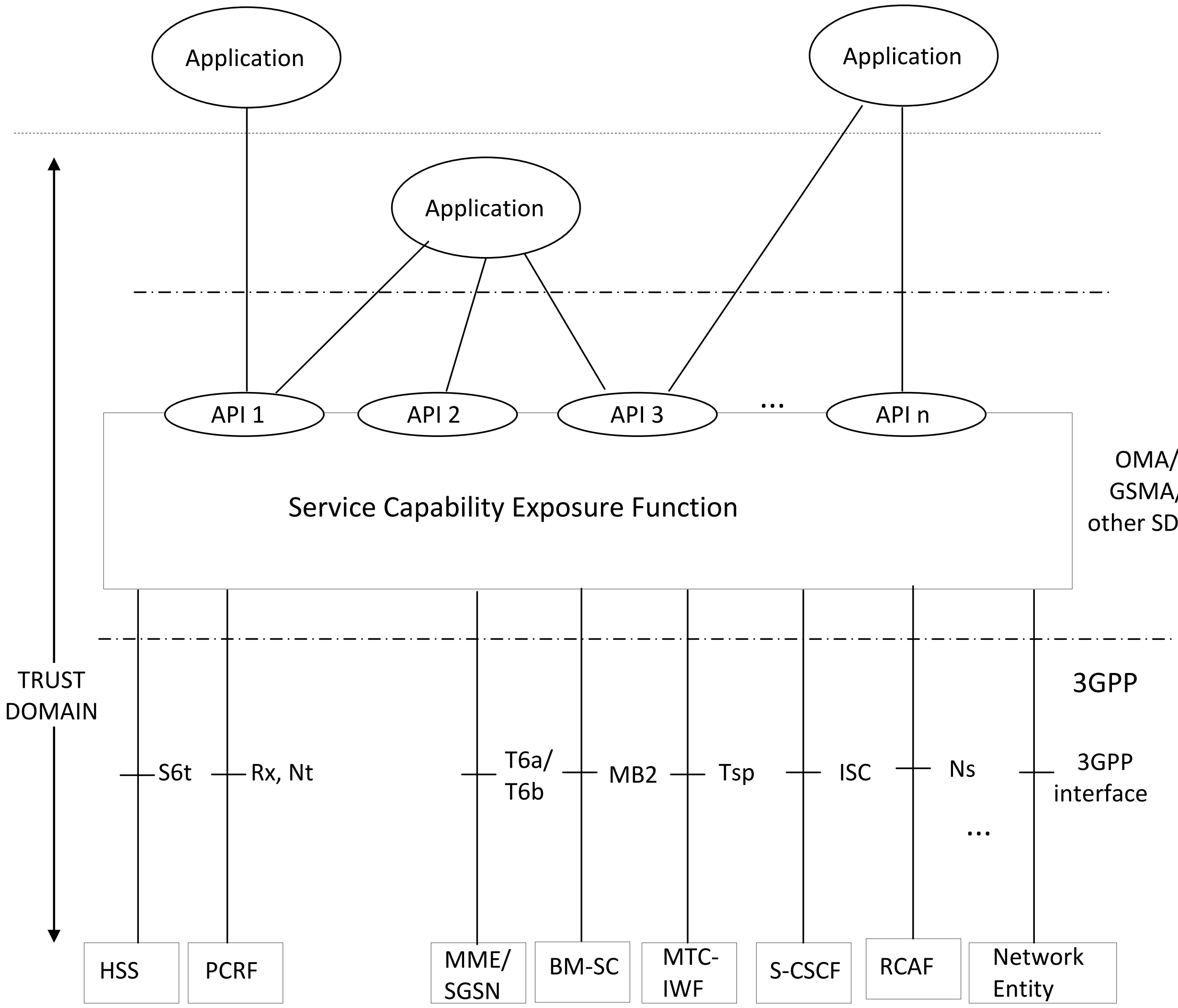


Figure 5.3-1: 3GPP Architecture for Service Capability Exposure

While 3GPP release 13 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 the ability to configure device communication patterns, the QoS of a data flow, sponsor a data flow, scheduling data transfers, monitor a device's state, optimizing 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 (ServiceExposure)

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

Editor's Note: this clause describes the reference architecture of 3GPP interworking.

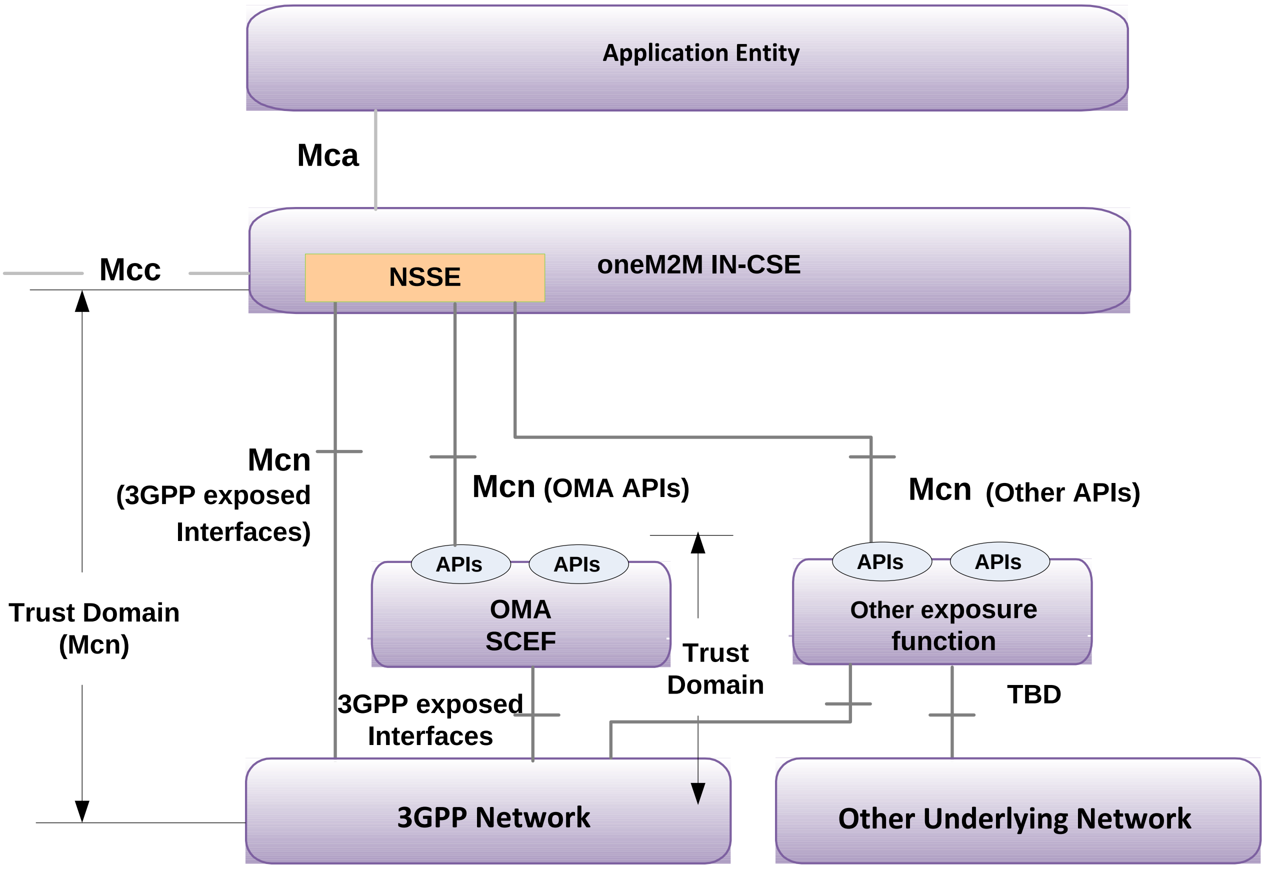


Figure 6-1: Interworking architecture

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

Editor's Note: this clause propose the enhancements based on architecture defined by oneM2M. What mechanisms can be reused and what need to be newly defined.

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 flowsor 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 Exclusive 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.

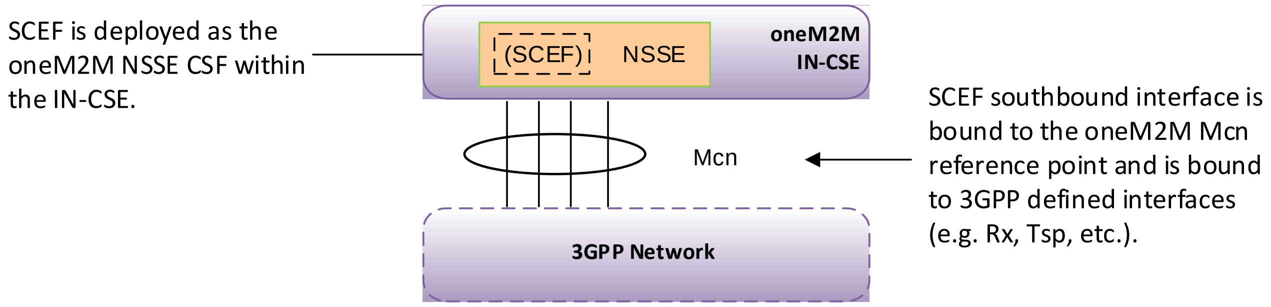

SCEF is deployed as the oneM2M NSSE CSF within the IN-CSE.
(SCEF)
NSSE
oneM2M
IN-CSE
Mcn
SCEF southbound interface is bound to the oneM2M Mcn reference point and is bound to 3GPP defined interfaces (e.g. Rx, Tsp, etc.).
3GPP Network

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

8.1.2 Exclusive Support through OMA API

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

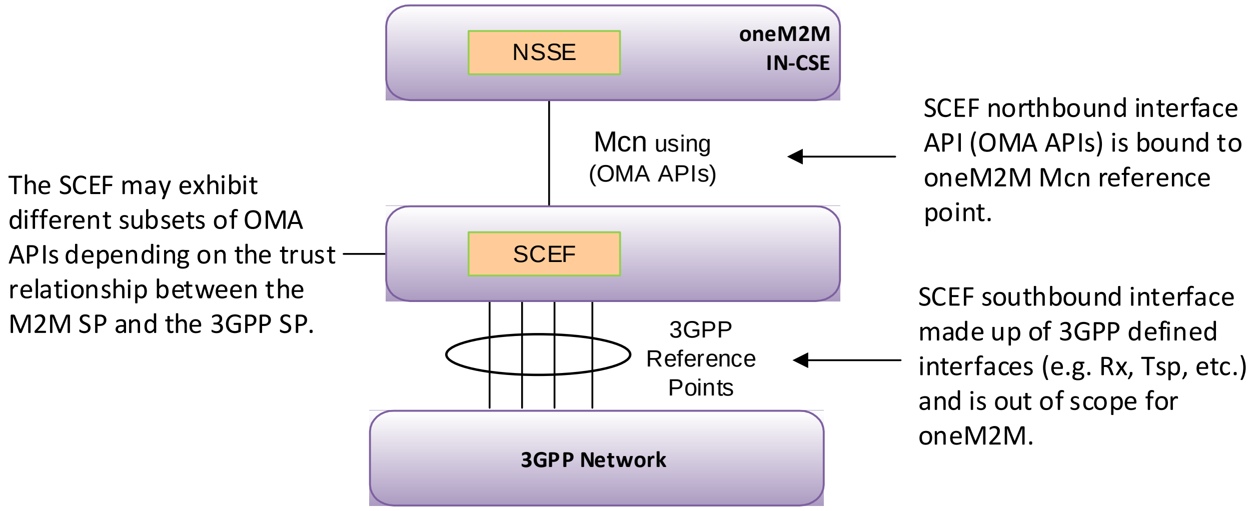

NSSE
oneM2M
IN-CSE
Mcn using
(OMA APIs)
SCEF northbound interface API (OMA APIs) is bound to oneM2M Mcn reference point.
The SCEF may exhibit different subsets of OMA APIs depending on the trust relationship between the M2M SP and the 3GPP SP.
SCEF
3GPP
Reference
Points
SCEF southbound interface made up of 3GPP defined interfaces (e.g. Rx, Tsp, etc.) and is out of scope for oneM2M.
3GPP Network

Figure 8.1.2-1: oneM2M interworking with a 3GPP underlying network via OMA 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 API for some service, proprietary APIs for others and finally some services can be invoked directly using the 3GPP reference points.

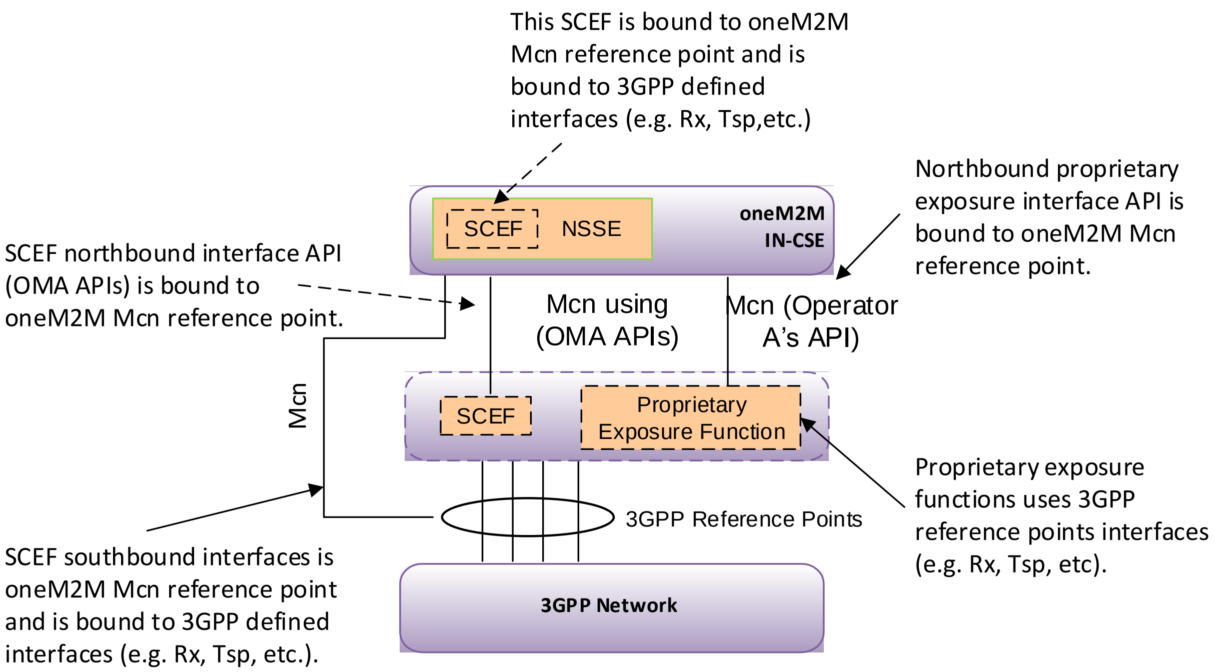

This SCEF is bound to oneM2M Mcn reference point and is bound to 3GPP defined interfaces (e.g. Rx, Tsp,etc.)
Northbound proprietary exposure interface API is bound to oneM2M Mcn reference point.
SCEF
NSSE
oneM2M
IN-CSE
SCEF northbound interface API (OMA APIs) is bound to oneM2M Mcn reference point.
Mcn 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 3GPP Release-13 MTC procedure

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).

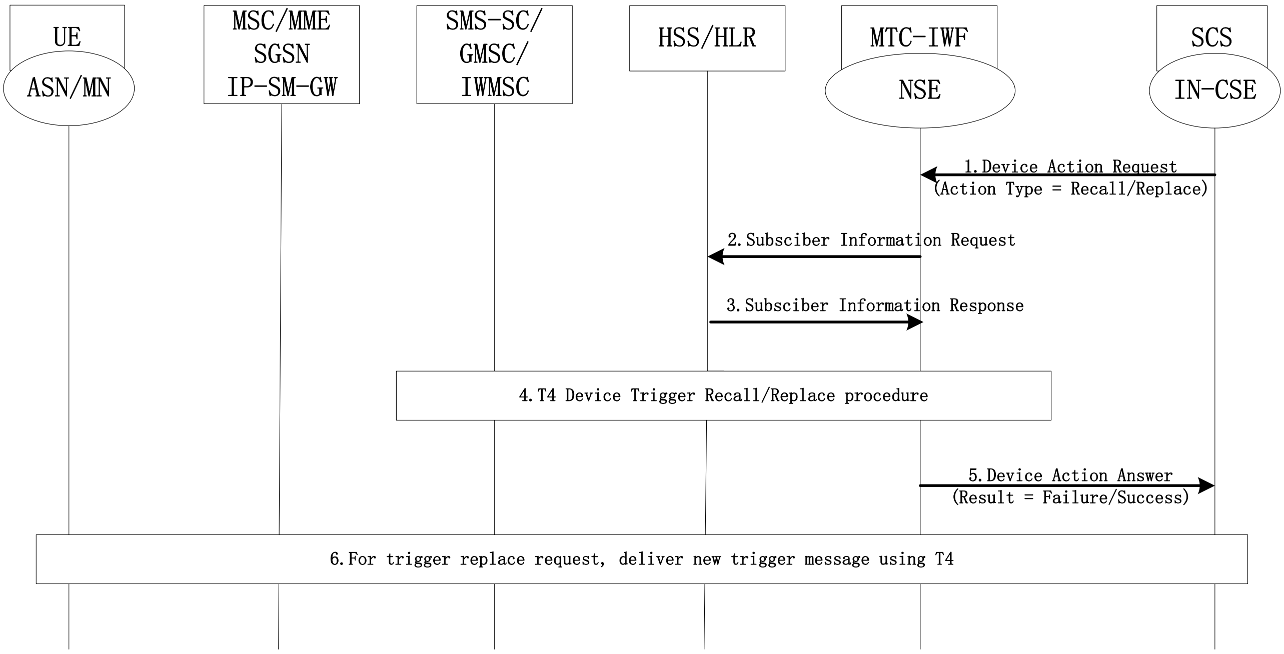

UE
ASN/MN
MSC/MME
SGSN
IP-SM-GW
SMS-SC/
GMSC/
IWMSC
HSS/HLR
MTC-IWF
NSE
SCS
IN-CSE
1.Device Action Request
(Action Type = Recall/Replace)
2.Subsciber Information Request
3.Subsciber Information Response
4.T4 Device Trigger Recall/Replace procedure
5.Device Action Answer
(Result = Failure/Success)
6.For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

8.2.3 3GPP Parameters

A set of Device Trigger Recall/Replace parameters can be associated with a Device Trigger Recall/Replace request, as defined in table 8.2.3-1.

Table 8.2.3-1: 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.	

8.2.4 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.

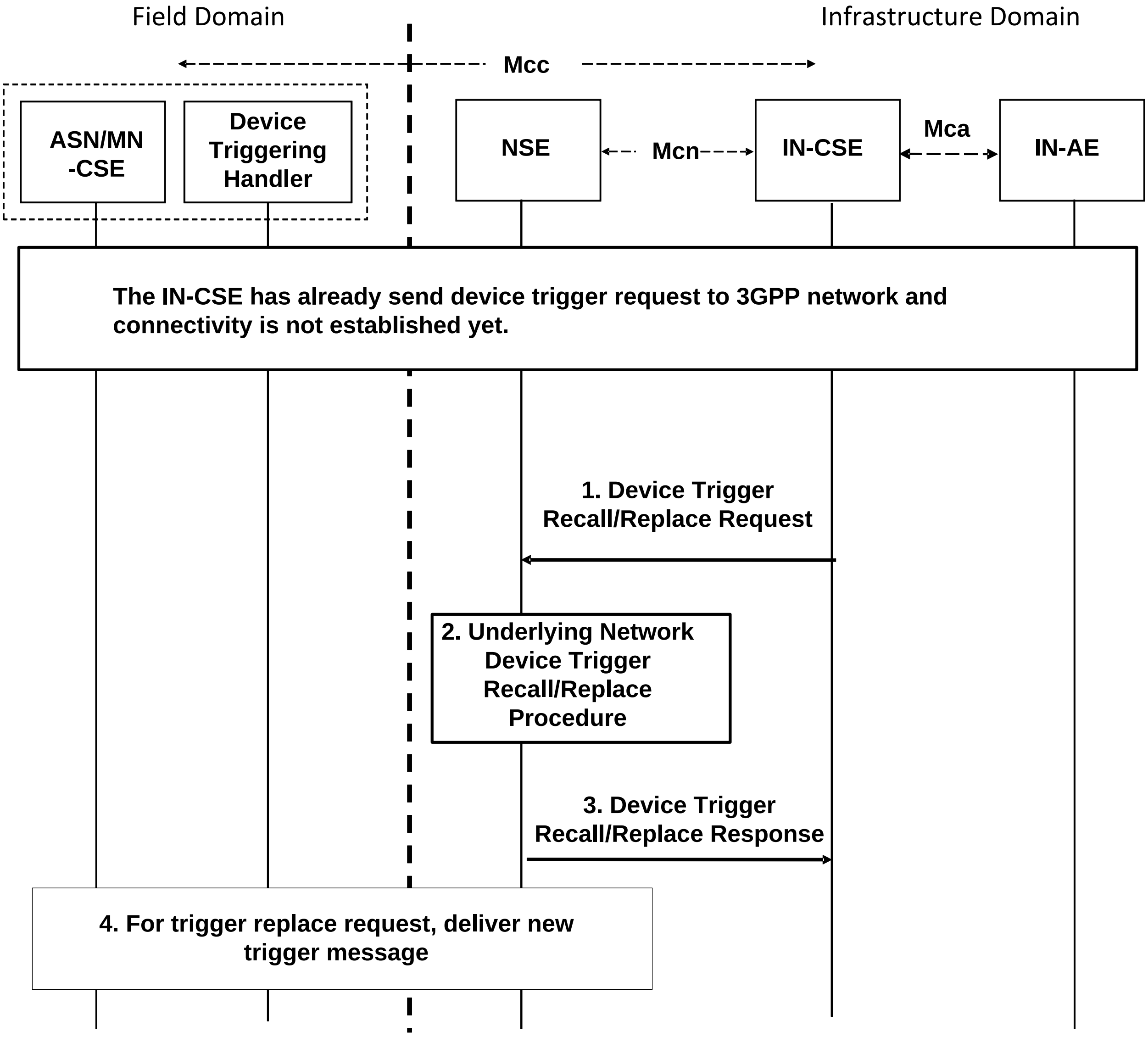

Field Domain
Infrastructure Domain
Mcc
ASN/MN -CSE
Device Triggering Handler
NSE
Mcn
IN-CSE
Mca
IN-AE
The IN-CSE has already send device trigger request to 3GPP network and connectivity is not established yet.
1. Device Trigger Recall/Replace Request
2. Underlying Network Device Trigger Recall/Replace 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 - can 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 can 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 can 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 will benefit because the UE will have fewer sleep/wake transitions and unnecessary signalling in the network can be avoided. Also, if the IN-CSE knows when the device is awake then data can 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 that can 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 (NodeID, 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 a the Field Domain Node:
    - The IN-CSE uses the M2M-Ext-ID to identify the Node towards the Underlying Network.

8.3.2 3GPP Release-13 MTC Procedure

oneM2M uses the 3GPP Release-13 MTC feature for Configuration of Device Communication Patterns in the Underlying Network by using the oneM2M Traffic Patterns resources to provide the corresponding 3GPP information. To that purpose the IN-CSE translates the oneM2M Traffic Patterns (TP) resource into a 3GPP Device Communication Pattern (CP) parameters.

A signalling sequence for provisioning of CP parameters is described in the clause 5.10.2 of 3GPP TS 23.682 [i.5]. Figure 8.3.2-1 provides the signalling sequence derived from the 3GPP specification with oneM2M terminologies mapping.

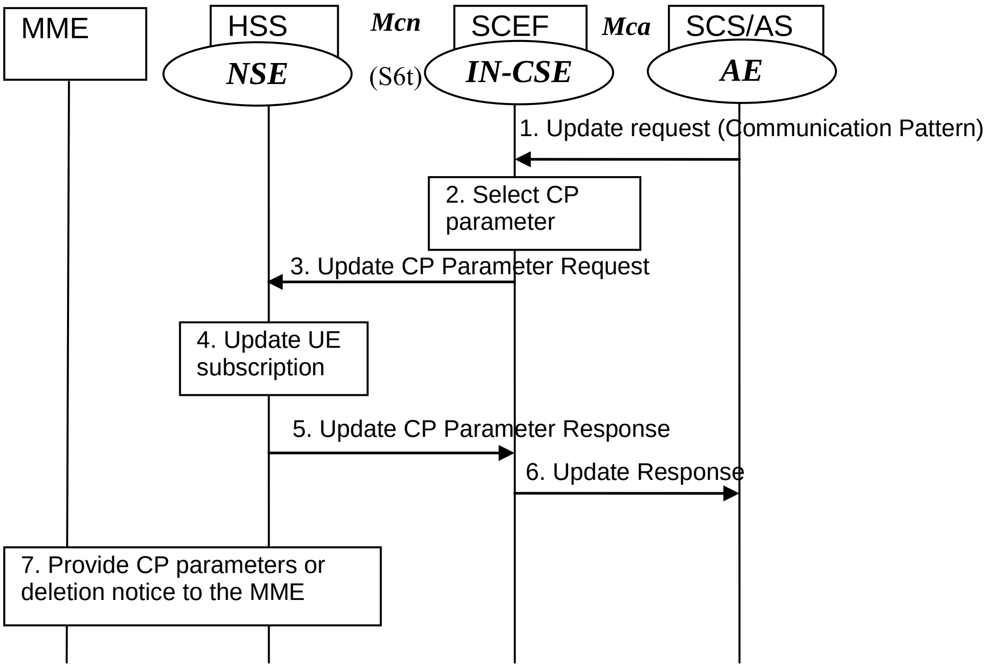

MME
HSS
NSE
Mcn
(S6t)
SCEF
IN-CSE
Mca
SCS/AS
AE
1. Update request (Communication Pattern)
2. Select CP parameter
3. Update CP Parameter Request
4. Update UE subscription
5. Update CP Parameter Response
6. Update Response
7. Provide CP parameters or deletion notice to the MME

Figure 8.3.2-1: Signalling sequence for provisioning of CP Parameters

3GPP TS 23.682 [i.5] makes assumptions for SCS/AS and SCEF of step 1 and step 2 as below.

==== Begin citation from 3GPP TS 23.682 [i.5] =====

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. The interface between SCEF and SCS/AS is outside the scope of 3GPP and the messages in the Figure are exemplary.

2. *The SCEF checks if the SCS/AS is authorized to send CP requests. The SCEF filters and the selects the CP parameter sets(s) for add/modify/delete based on operator policy or configuration.*

NOTE 2: If there are several CP parameter sets active for one UE, then the SCEF assures that the different CP parameter sets are not overlapping, e.g. based on the Scheduled communication time and/or Communication duration time parameters.

EXAMPLE 1: For example, one CP parameter set may indicate that the UE is scheduled to communicate at 04:00 every day for 30 seconds, and another CP parameter set may indicate that the UE is scheduled to communicate at 23:30 every day for 45 seconds. These would be non-overlapping CP parameter sets.

EXAMPLE 2: As a second example, if one CP parameter set indicated that the UE is scheduled to communicate at 04:00 every day for 30 seconds and another CP parameter set indicated that the UE is scheduled to communicate at 04:00 every day for 90 seconds, the two CP parameter sets would be overlapping.

In this release, to avoid receiving CP parameter sets from multiple SCEFs that might be overlapping, the HSS shall accept CP parameter sets from only a single SCEF for a given UE.

==== End citation from 3GPP TS 23.682 [i.5] =====

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

==== Begin citation from 3GPP TS 23.682 [i.5] =====

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 3: 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.

==== End citation from 3GPP TS 23.682 [i.5] =====

EXAMPLE: 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 Identifeir 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.

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

==== Begin citation from 3GPP TS 23.682 [i.5] =====

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.

==== End citation from 3GPP TS 23.682 [i.5] =====

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.

The actual parameters for the request and response messages in above steps 3 and 5 are defined by 3GPP TS 29.336 [i.10], clauses 7 and 8 for S6t reference point.

8.3.3 3GPP Parameters

A set of Traffic pattern (TP) parameters can be associated with a Traffic Pattern of one or multiple field domain nodes and are defined in table 8.3.3-1.

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

Table 8.3.3-1: 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.

8.3.4 Solution(s)

8.3.4.1 Solution1

8.3.4.1.1 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 <trafficCharacteristics>:
  - Note: It is child resource of existing Resource Type <AE> or <node>.
- Resource Type <trafficPattern>.

NOTE: It is child resource of new Resource Type <trafficCharacteristics>.

Detailed information of new resource types are described in subclauses below.

8.3.4.1.1.1 Resource Type <trafficCharacteristics>

The <*trafficCharacteristics*> resource represents the characteristic information (e.g. communication pattern, mobility pattern, etc.) of a field domain node. This information may be detected or scheduled by application level processing. This resource type is used to share information with other entities such as the underlying network entity (server NSE) of the field domain node which may optimize the processing of the underlying network for the specific field domain node.

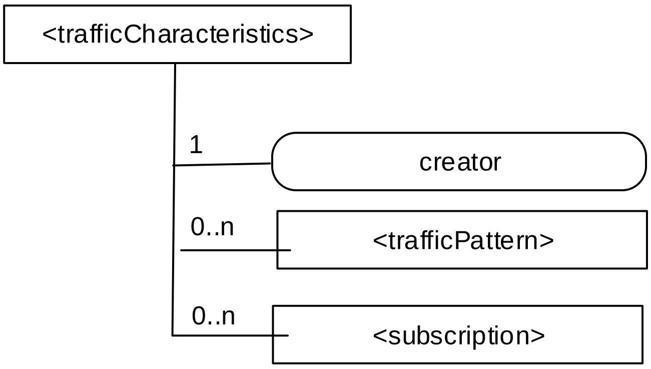


Figure 8.3.4.1.1.1-1: Structure of <*trafficCharacteristics*> resource

The <*trafficCharacteristics*> resource shall contain the child resources specified in table 8.3.4.1.1.1-1.

Table 8.3.4.1.1.1-1: Child resources of <*trafficCharacteristics*> resource

Child Resources of <*trafficCharacteristics*>	**Child Resource Type**	**Multiplicity**	**Description**	**<trafficCharacteristicsAnnc> Child Resource Types**
[variable]	<*subscription*>	0..n		<subscription>
[variable]	<*trafficPattern*>	0..n	See clause 8.3.4.1.1.2. A source AE can create multiple number of <trafficPattern> resources for a single target AE of field domain node. In this case the source AE assures that different communication patterns are not overlapping at any point in time.	<trafficPatternAnnc>

The <trafficCharacteristics> resource shall contain the attributes specified in table8.3.4.1.1.1-2.

Table 8.3.4.1.1.1-2: Attributes of <*trafficCharacteristics*> resource

Attributes of <*deviceCharacteristics*>	**Multiplicity**	**RW/ RO/ WO**	**Description**	**<trafficCharacteristicsAnnc> 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

8.3.4.1.1.2 Resource Type <trafficPattern>

The <*trafficPattern*> resource represents the communication pattern and the mobility pattern of a field domain node to be shared with other entities such as the underlying network entity (NSE) of the field domain node which may optimize the processing of the underlying network for the specific field domain node by using this information.

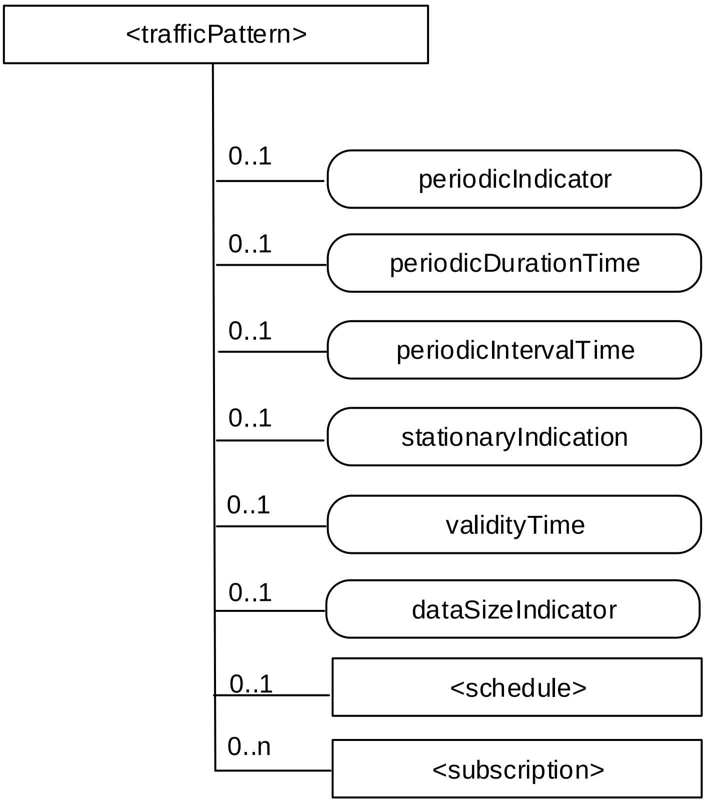


Figure 8.3.4.1.1.2-1: Structure of *<trafficPattern>* resource

The *<trafficPattern>* resource shall contain the child resources specified in table 8.3.4.1.1.2-1.

Table 8.3.4.1.1.2-1: Child resources of *<trafficPattern>* resource

Child Resources of *<trafficPattern>*	Child Resource Type	Multiplicity	Description	<trafficPatternAnnc> Child Resource Types
[variable]	*<subscription>*	0..n		<subscription>
[variable]	*<schedule>*	0..1	It provides the mask for the day of week, the starting time and end time for communication. If it is not provided this shall be interpreted as 'anytime' at the NSE.	<scheduleAnnc>

The <trafficPattern> resource shall contain the attributes specified in table 8.3.4.1.1.2-2.

Table 8.3.4.1.1.2-2: Attributes of <*trafficPattern*> resource

Attributes of <*trafficPattern*>	**Multiplicity**	**RW/ RO/ WO**	**Description**	**<trafficPatternAnnc> 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
provideToNSE	0..1	RW	It indicates as 'TRUE' or 'FALSE' whether the traffic pattern shall be provided to a NSE	OA
periodicIndicator	0..1	RW	It indicates as 'Periodical' or 'On demand'.	OA
periodicDurationTime	0..1	RW	It provides the time in seconds of the duration of the periodic communication.	OA
periodicIntervalTime	0..1	RW	It provides the time in seconds of the interval for periodic communication.	OA
stationaryIndication	0..1	RW	It indicates as 'Stationary (Stopping)' or 'Mobile (Moving)'.	OA
dataSizeIndicator	0..1	RW	It indicates the expected data size for the pattern	OA
validityTime	0..1	RW	It contains the point of time when the informed <trafficPattern> information to the NSE becoming invalid and shall be deleted at the NSE.	OA

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.

The procedure needs to be harmonized with the figure 8.3.2-1.

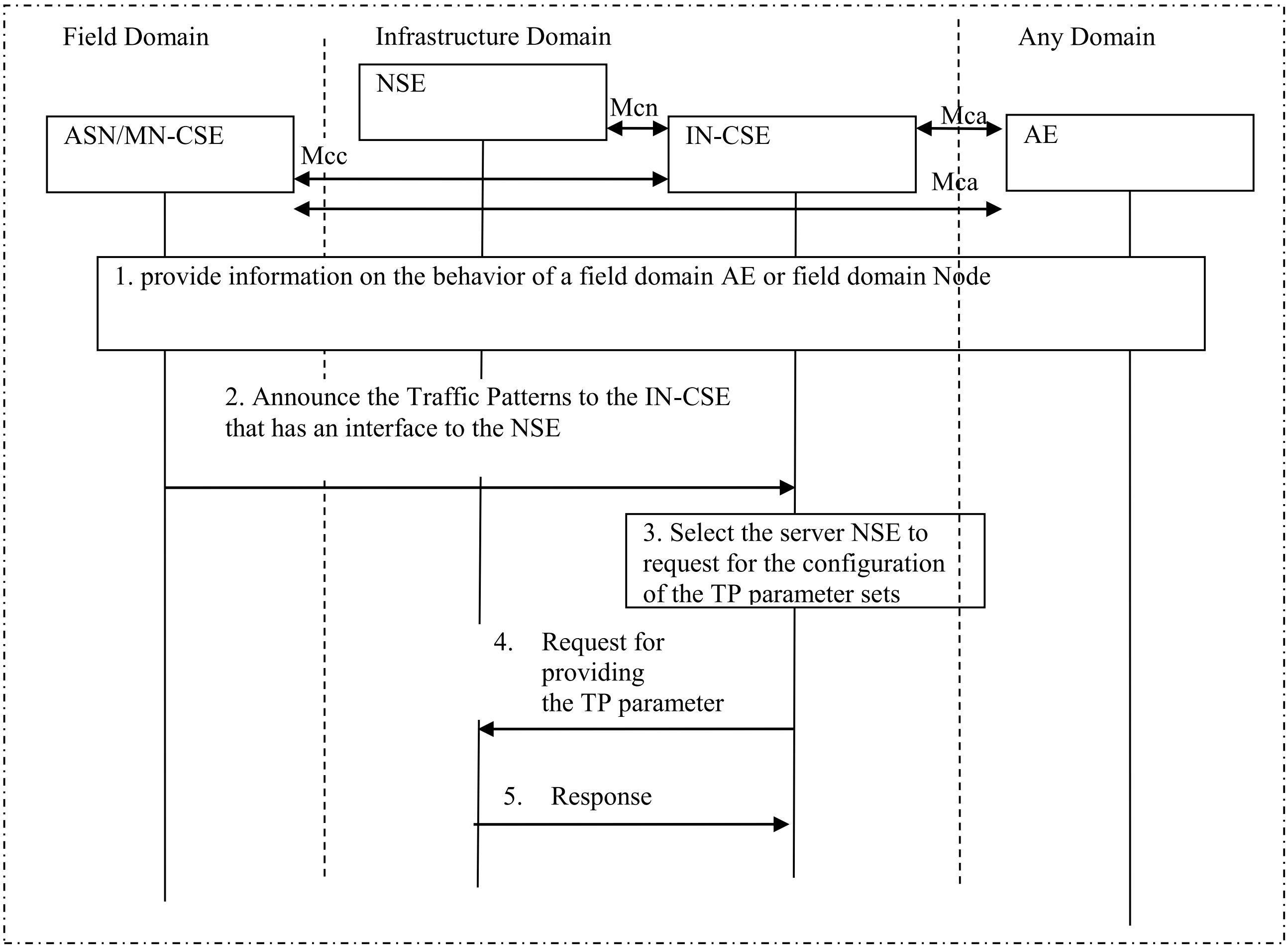

Field Domain
Infrastructure Domain
Any Domain
NSE
Mcn
Mca
ASN/MN-CSE
IN-CSE
AE
Mcc
Mca
1. provide information on the behavior of a field domain AE or field domain Node
2. Announce the Traffic Patterns to the IN-CSE that has an interface to the NSE
3. Select the server NSE to request for the configuration of the TP parameter sets
4. Request for providing the TP parameter
5. Response

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

Step-1: Provide information on the behavior of a field domain AE or field domain Node

An AE (IN-AE or an AE of the Field Domain Node that reports its communication behaviour) provides the hosting CSE (i.e. ASN/MN-CSE) of the field domain AE/Node with information on the communication behavior of the AE/Node (i.e. TP parameter sets) by creating, updating or deleting its Traffic Patterns (TP).

The AE may provide TP parameter sets for a group of field domain nodes .

The request shall include:

- the originator AE-ID of the requesting AE;
- a target identifier: i.e. the <trafficCharacteristics> child resource of a <node> resource or an <AE> resource of the field domain node or a group identifier of multiple field domain AEs/nodes for which the Traffic Patterns is provided; and
- a set of TP parameters as indicated in table 8.3.3-1.

The request may include multiple of TP parameter set(s) and validity time(s).

If the hosting CSE has received a request from an AE to create, update or delete Traffic Patterns it shall check if the request from the AE is valid (see note 1).

NOTE 1: Apart from checking access rights of the AE the validation of the request from the AE could include:

- Consistency with <schedule> resources supported by an M2M SP in various M2M entities (MN-CSE, ASN) hosting this AE/Node.
- If there are several TP parameter sets active for one Field Domain Node, then the original resource hosting CSE assures that the different TP parameter sets are not overlapping.

Step-2: Announce the Traffic Patterns to the IN-CSE that has an interface to the NSE

If the hosting CSE recognizes an announcement procedure is needed, it shall announce the Traffic Patterns received from the AE to the IN-CSE that has an interface to the NSE contained in the "AnnounceTo" attribute of the Traffic Patterns resources based on the existing announcement procedures.

Step-3: Select the server NSE to request for the configuration of the TP parameter sets

If the IN-CSE receives an announced Traffic Patterns and the IN-CSE recognizes the configuration of the Traffic Patterns at the NSE is needed by checking "provideToNSE" attribute, the IN-CSE shall perform subsequent steps.

For the configuration of the TP parameter sets for a specific field domain node, the IN-CSE selects the NSE by using the identifier of the Field Domain Node (i.e. the M2M-Ext-ID) by which the Node can be identified in the NSE.

NOTE 2: The correct server NSE can be found by following of a chain of links of multiple resources in the IN-CSE, e.g. the nodeLink in the AEAnnc resource of a target AE of field domain node linking to the nodeAnnc resource having the hostedCSELink linking to the remoteCSE resource having the M2M-Ext-ID linking to the UNetwork-ID of the server NSE. (See clauses 7.1.8 and 7.1.9 in oneM2M TS-0001 [i.9].)

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

Step-5: 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 4: If the Underlying Network is 3GPP-compliant, see clause 8.3.2 for more details.

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 3GPP Release-13 MTC procedure

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.

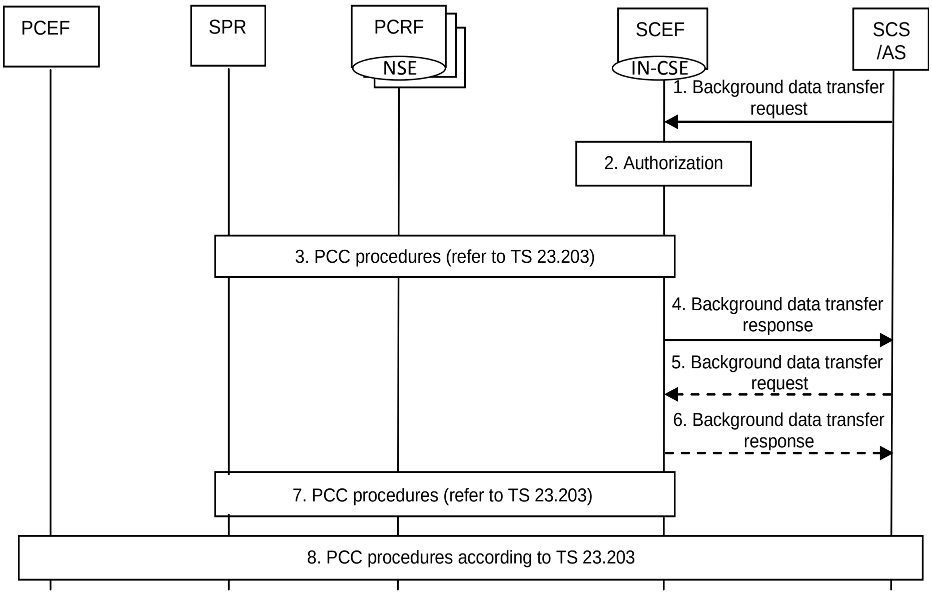

PCEF
SPR
PCRF
NSE
SCEF
IN-CSE
SCS
/AS
1. Background data transfer request
2. Authorization
3. PCC procedures (refer to TS 23.203)
4. Background data transfer response
5. Background data transfer request
6. Background data transfer response
7. PCC procedures (refer to TS 23.203)
8. PCC procedures according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

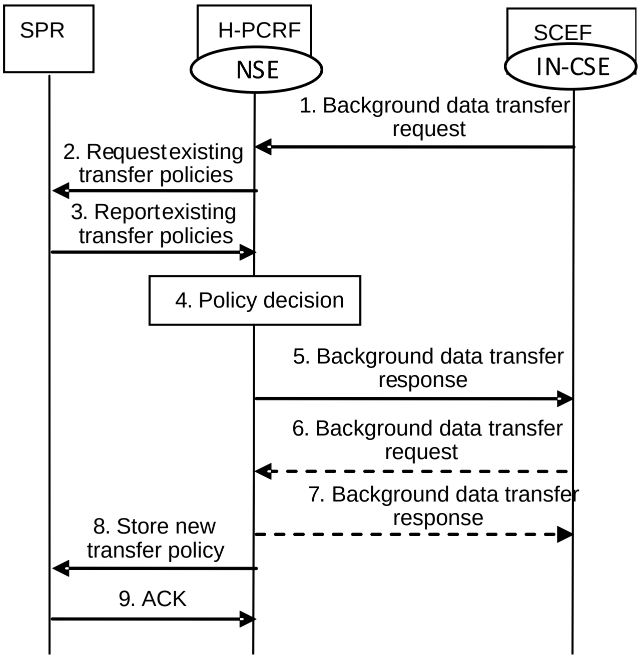
3. The SCEF selects any of the available PCRFs and triggers the Negotiation for future background data transfer procedure with the PCRF. The SCEF forwards the parameters provided by the SCS/AS. The PCRF responds to the SCEF with the possible transfer policies and a reference ID.

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.

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. Request existing transfer policies
3. Report existing 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 1: The SCEF does not provide any information about the identity of the UEs potentially involved in the future background data transfer.

NOTE 2: 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 3: 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 4: If the SCEF receives only one transfer policy, the AF is not required to confirm.

8.4.3 3GPP Parameters

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 8.4.3-1 and 8.4.3-2.

Table 8.4.3-1: 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 8.4.3-2: 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.	

8.4.4 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 are 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.

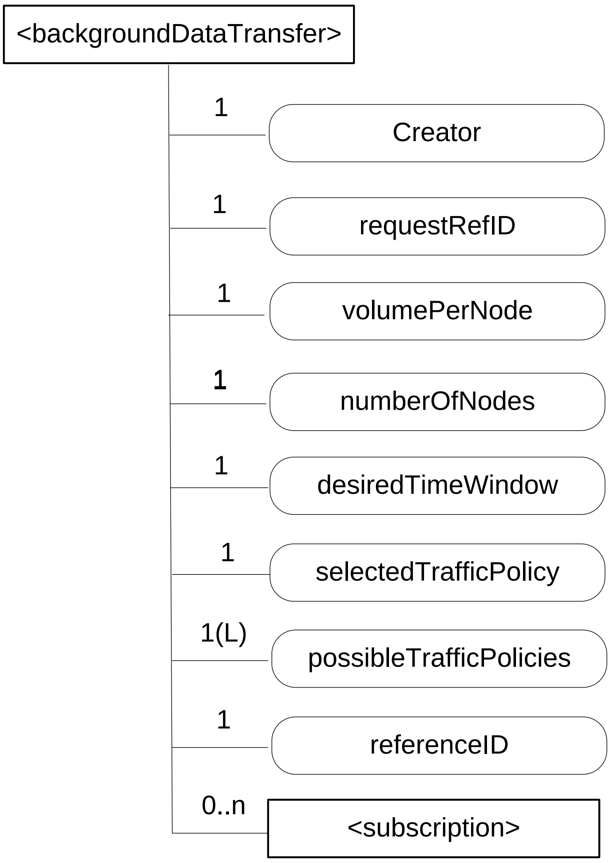


Figure 8.4.4.1.1.1-1: Structure of *<backgroundDataTransfer>* resource

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 identies 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 expection. The procedure needs to be harmonized with the figures 8.4.2-1 and 8.4.2-2.

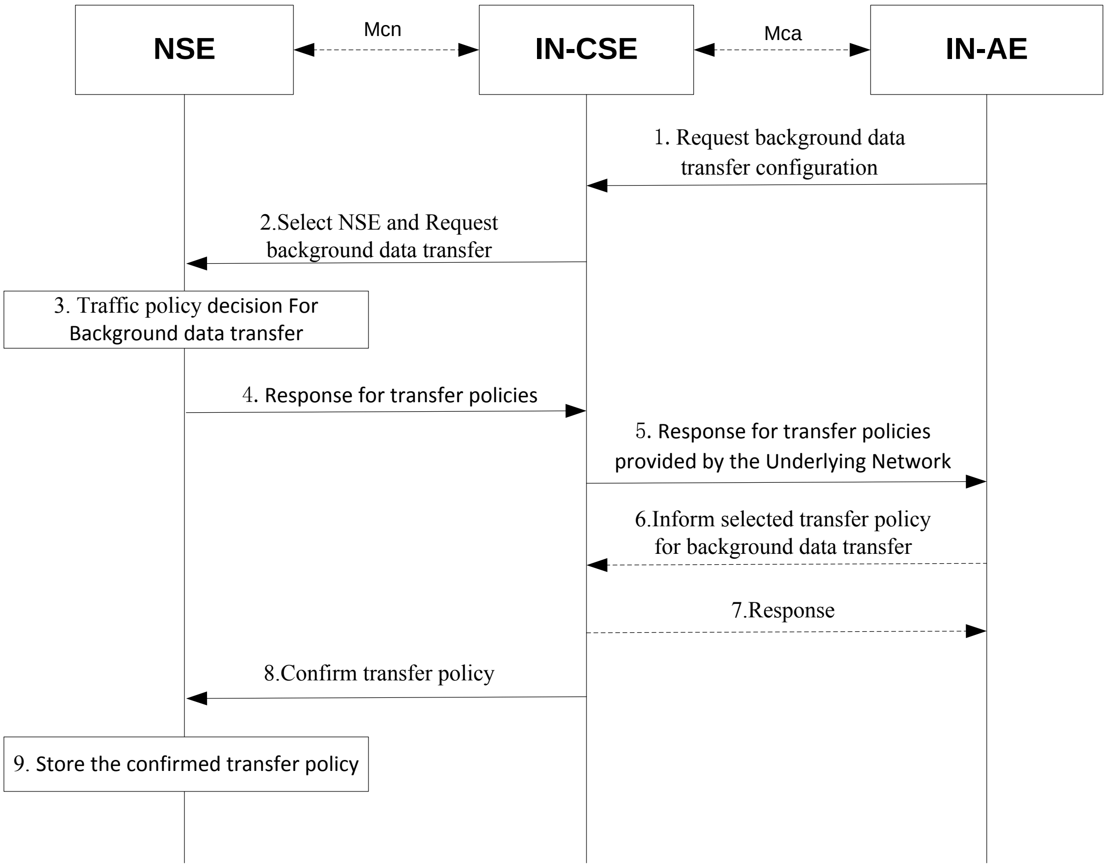

NSE
Mcn
IN-CSE
Mca
IN-AE
1. Request background data transfer configuration
2.Select NSE and Request background data transfer
3. Traffic policy decision For Background data transfer
4. Response for transfer policies
5. Response for transfer policies provided by the Underlying Network
6.Inform selected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

M2M deployments lends themselves to the use of group operations in many ways, from coordinated management to signalling reduction and resource utilization optimizations. For example, in many M2M deployments it is desirable to charge devices as a group, send messages to a group, trigger groups of devices, and monitor devices as a group.

The Group Messaging feature is intended to efficiently distribute the same content to the members of a group. 3GPP has considered several solutions for implementation, including the use of cell broadcast, MBMS and via PDN connections. The 3GPP Release 13 procedure makes use of MBMS for group message delivery and may be re-used for general group message delivery purposes (not limited to MTC devices). The group message delivery using MBMS has limited applicability and does not support all the scenarios, e.g. UEs not supporting MBMS, UEs located in areas where MBMS is not deployed. The feature involves the use of MBMS entities such as BM-SC (Broadcast Multicast Service Centre) to allocate a TMGI (Temporary Mobile Group Identity) for a specific MBMS user service.

8.5.2 3GPP Release-13 MTC procedure

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). And it should be noted that the 3GPP group message delivery feature does not support all the scenarios, for the UEs not supporting MBMS or the UEs located in areas where MBMS is not deployed, the 3GPP group message delivery can not be applied.

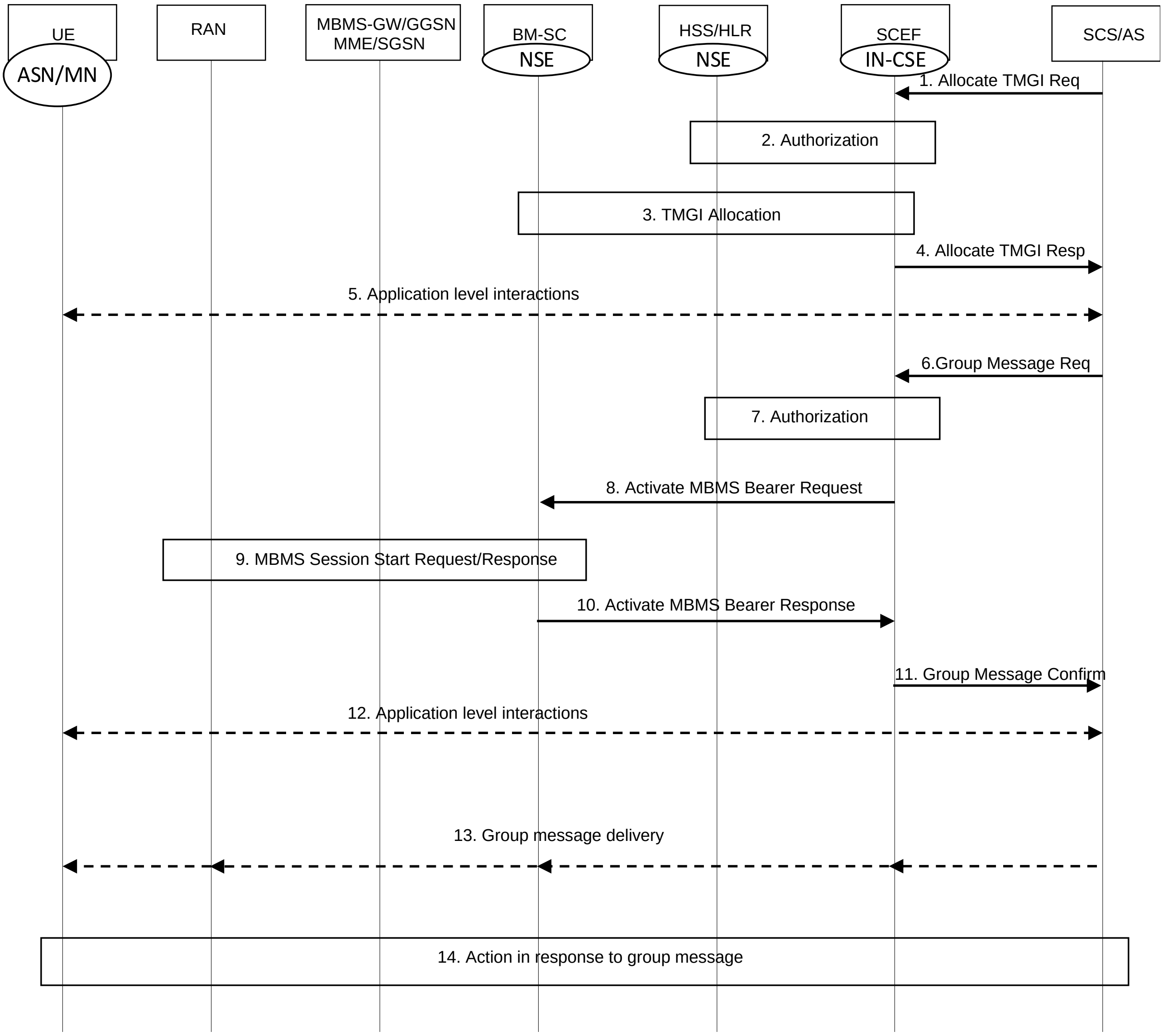

UE
ASN/MN
RAN
MBMS-GW/GGSN
MME/SGSN
BM-SC
NSE
HSS/HLR
NSE
SCEF
IN-CSE
SCS/AS
1. Allocate TMGI Req
2. Authorization
3. TMGI Allocation
4. Allocate TMGI Resp
5. Application level interactions
6.Group Message Req
7. Authorization
8. Activate MBMS Bearer Request
9. MBMS Session Start Request/Response
10. 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

3GPP TS 23.682 [i.5] describes group message delivery using MBMS as follows:

NOTE 1: Steps 1-5 can be skipped if a valid TMGI allocation already exists or if the MBMS bearer activation is performed without TMGI pre-allocation.

NOTE 2: The interactions between the SCEF and the SCS/AS (in steps 1, 4, 6, 11 and 13) are outside the scope of 3GPP and are shown for informative purposes only.

1. If there is no assigned TMGI for an External Group Id, the SCS/AS sends the Allocate TMGI Request (External Group ID, SCS Identifier) message to the SCEF. The SCS/AS may determine the IP address(es)/port(s) of the SCEF by performing a DNS query using the External Group Identifier or using a locally configured SCEF identifier/address. The SCEF checks that the SCS/AS is authorized to request TMGI allocation.

2. The SCEF determines whether the SCS/AS is authorized to request TMGI allocation.

NOTE 3: The authorization of TMGI allocation for the group and acquisition of the BM-SC routing information are not specified in this release of the specification.

3. The SCEF initiates TMGI allocation by the BM-SC (see TMGI Allocation Procedure specified in 3GPP TS 23.468 [i.14]).

4. The SCEF sends the received TMGI and expiration time information to the SCS/AS.

NOTE 4: The SCEF may cache the serving BM-SC Identity information and mapping between External Group ID and TMGI.

5. Application level interactions may be applied for the devices of specific group to retrieve the related MBMS service information, e.g. TMGI, start time. Application level interactions between the UE and the SCS/AS are out of scope of this specification.

6. The SCS/AS sends the Group Message Request (External Group Identifier, SCS Identifier, location/area information, RAT(s) information, TMGI, start time) message to the SCEF. The location/area information indicated by the SCS/AS may be the geographic area information.

7. The SCEF checks that the SCS/AS is authorised to send a group message request. If this check fails the SCEF sends a Group Message Confirm message with a cause value indicating the reason for the failure condition and the flow stops at this step. In this case, the SCS/AS may subsequently release the TMGI allocated at step 3 by requesting an explicit de-allocation, or may rely on the expiration timer.

NOTE 5: Authorization of Group Message delivery using MBMS towards a specific group is not specified in this release of the specification.

8. The SCEF sends an Activate MBMS Bearer Request (MBMS broadcast area, TMGI, QoS, start time) message to the BM-SC (see 3GPP TS 23.468 [i.14]).

NOTE 6: The SCEF maps between location/area information provided by the SCS/AS and the MBMS broadcast area for the distribution of the content to the group based on configuration in the operator domain. The SCEF needs to be aware that the selected MBMS broadcast area may result in broadcast of the content over an area larger than the area that may be indicated by SCS/AS.

9. BM-SC performs the Session Start procedure (see MBMS Session Start procedure specified in 3GPP TS 23.246 [i.15]).

10. The BM-SC sends an Activate MBMS Bearer Response to the SCEF (see 3GPP TS 23.468 [i.14]).

11. The SCEF sends a Group Message Confirm (TMGI (optional), SCEF IP addresses/port) message to the SCS/AS to indicate whether the Request has been accepted for delivery to the group.

12. Application level interactions may be applied for the devices of specific group to retrieve the related MBMS service information, e.g. TMGI, start time. Application level interactions between the UE and the SCS/AS are out of scope of this specification.

13. At or after the requested start time, but before the expiration time, the SCS/AS transfers the content to be delivered to the group to the SCEF using the IP address and port received at step 11. SCEF delivers the contents to BM-SC via MB2-U, using the IP address and port received at step 9. The BM-SC transfers the corresponding content to UEs. To avoid that potential responses to the broadcast message by high numbers of devices are sent at almost the same time, the SCS/AS makes sure the UEs are provided with a response time window if it expects the UEs to respond to the delivered content.

NOTE 7: Subsequent to this step, it is up to the SCS/AS if the MBMS bearers will be kept active and allocated and for how long. The mechanisms defined in 3GPP TS 23.468 [i.14] can be used by the SCEF to release the MBMS resources.

14. In response to the received content, the UE may initiate immediate or later communication with the SCS/AS.

NOTE 8: The UE application ensures distribution of any responses within the response time window.

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]. The related normal texts are shown as below, where the GCS AS can be considered as the SCEF.

Figure 5.1.2.2.1-1 in the 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.

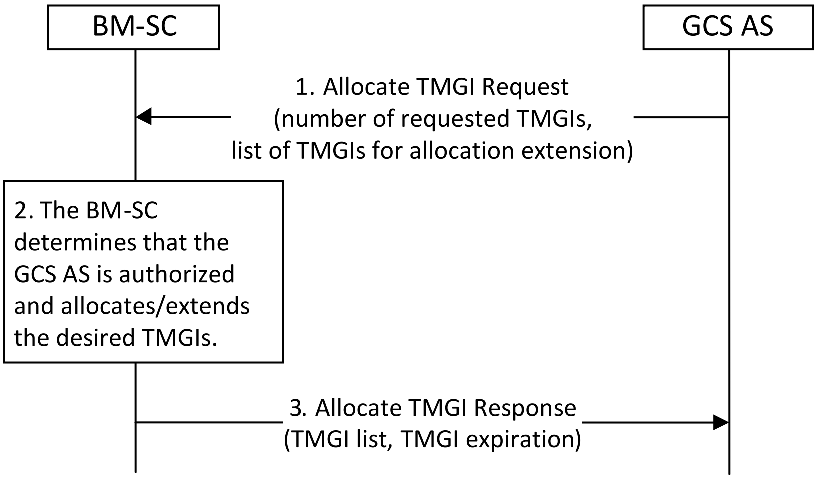

BM-SC
GCS AS
1. Allocate TMGI Request
(number of requested TMGIs,
list of TMGIs for allocation extension)
2. The BM-SC determines that the GCS AS is authorized and allocates/extends the desired TMGIs.
3. Allocate TMGI Response
(TMGI list, TMGI expiration)

Figure 5.1.2.2.1-1 (of 3GPP TS 23.468): TMGI Allocation Procedure

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 shall determine 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 can be set to the new expiration time.

3. The BM-SC shall send an Allocate TMGI Response message to the GCS AS indicating the list of allocated TMGIs, and an expiration time for those TMGIs.

Figure 5.1.2.3.2-1 in the 3GPP TS 23.468 [i.14] provides the procedure used between the GCS AS and the BM-SC to activate an MBMS bearer.

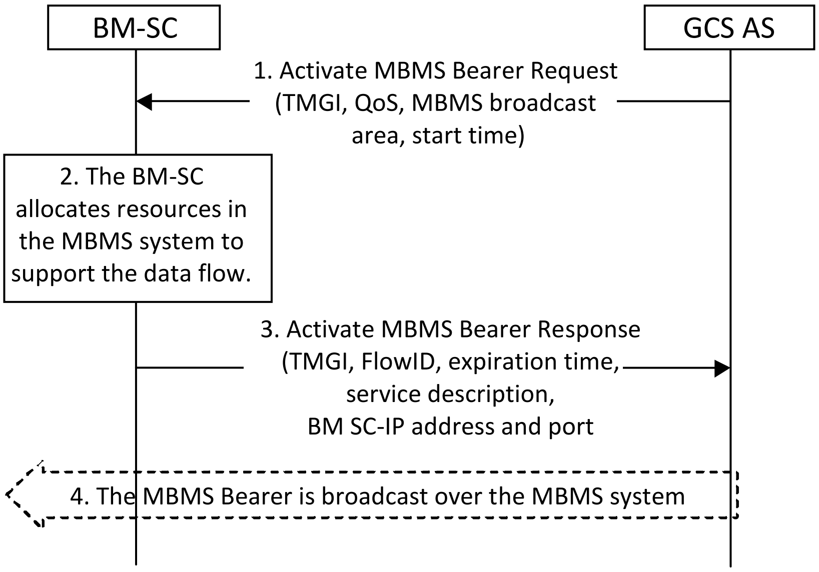

BM-SC
GCS AS
1. Activate MBMS Bearer Request
(TMGI, QoS, MBMS broadcast
area, start time)
2. The BM-SC allocates resources in the MBMS system to support the data flow.
3. Activate MBMS Bearer Response
(TMGI, FlowID, expiration time,
service description,
BM SC-IP address and port
4. The MBMS Bearer is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

Figure 5.1.2.3.2-1 (of 3GPP TS 23.468): Activate MBMS Bearer Procedure

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 shall be mapped into appropriate QoS parameters of the MBMS bearer. The MBMS broadcast area parameter shall include a list of MBMS Service Area Identities, or a list of cell IDs, or both.

NOTE 9: 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 shall determine whether the GCS AS is authorized to use the TMGI. The BM-SC shall reject the request if the TMGI is not authorized. If the TMGI was not included in the request, the BM-SC shall assign 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 shall then include 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 shall accept 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 shall allocate 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 shall send 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 shall contain 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 10: The GCS AS can use the service description to provide information to the UE to access the MBMS bearer.

NOTE 11: 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 3GPP Parameters

This section provides information regarding the parameters necessary to accomplish the group messaging feature.

Table 8.5.3-1: Group messaging parameters

Parameter	Description
TMGI	Temporary Mobile Group Identity. A TMGI can be used to identify one MBMS Bearer Service.
Expiration time	Expiration time indicate the time after which the TMGI is invalid.
MBMS broadcast area	The MBMS broadcast area parameter shall include a list of MBMS Service Area Identities, or a list of cell IDs, or both.
FlowID	FlowID relates the TMGI and the location area where need to broadcast group message.
Start time	Start time indicates the time the BM-SC is ready to send data.
QoS	The requested QoS of the delivery of the group message.
BM-SC IP address and port number	IP address and port number for the user-plane, which is allocated by the BM-SC towards SCEF.
serviceDescription	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).

8.5.4 Solution(s)

8.5.4.1 Solution1

8.5.4.1.1 Overview

The SCEF can either be deployed inside or outside the IN-CSE, and in this sub clause, only the case, where the SCEF is implemented inside the IN-CSE, is described. In order to enable the IN-CSE(SCEF) reuse 3GPP group message delivery procedure using MBMS specified in 3GPP TS 23.682 [i.5], the following aspects need to be considered or processed at the IN-CSE:

1) The IN-CSE can be configured with the basic 3GPP network information, e.g. the serving BM-SC identity or the IP address information and the mapping between the location/area information provided by AE and the MBMS broadcast area of the 3GPP network.

When the UE registers to the IN-CSE via the 3GPP network, the IN-CSE determines whether the UE is in the coverage of the 3GPP MBMS service, according to the location information comes from UE and the local configuration. If the UE support the 3GPP MBMS service, the IN-CSE can record the 3GPP MBMS service capability under the node resource of the UE, e.g. using the <deviceCapability>.

8.5.4.1.2 Proposed resource types and attributes

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

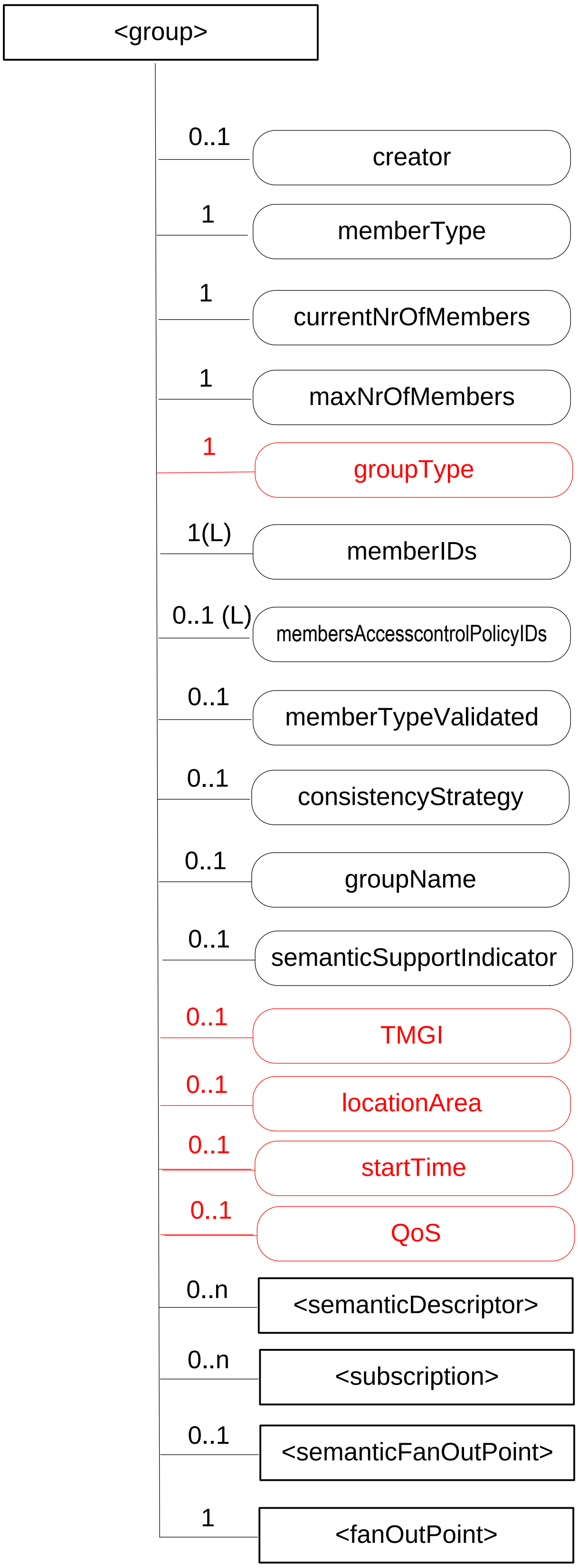


Figure 8.5.4.1.2-1

Table 8.5.4.1.2-1

Attributes of <*group*>	Multiplicity	RW/ RO/ WO	Description	<*groupAnnc*> Attributes
groupType	1	RW	Indicating the underlying network type of the group, e.g. 3GPP MBMS group. If the underlying networks of the group members are different, it is the type of 'mixed'.	NA
TMGI	0..1	RO	This attribute only present when the groupType is 3GPP MBMS. TMGI can be used to identify one group messaging service.	NA
locationArea	0..1	RW	locationArea indicates the area within which data of group messaging are sent.	NA
startTime	0..1	RW	This attribute only present when the groupType is 3GPP MBMS. startTime indicates the time the data is ready to be sent.	NA
QoS	0..1	RW	This attribute only present when the groupType is 3GPP MBMS. QoS indicates the AE requested QoS of the delivery of the group message.	NA

8.5.4.1.3 Proposed Flow(s)

This clause describes the general procedure for group message delivery using MBMS.

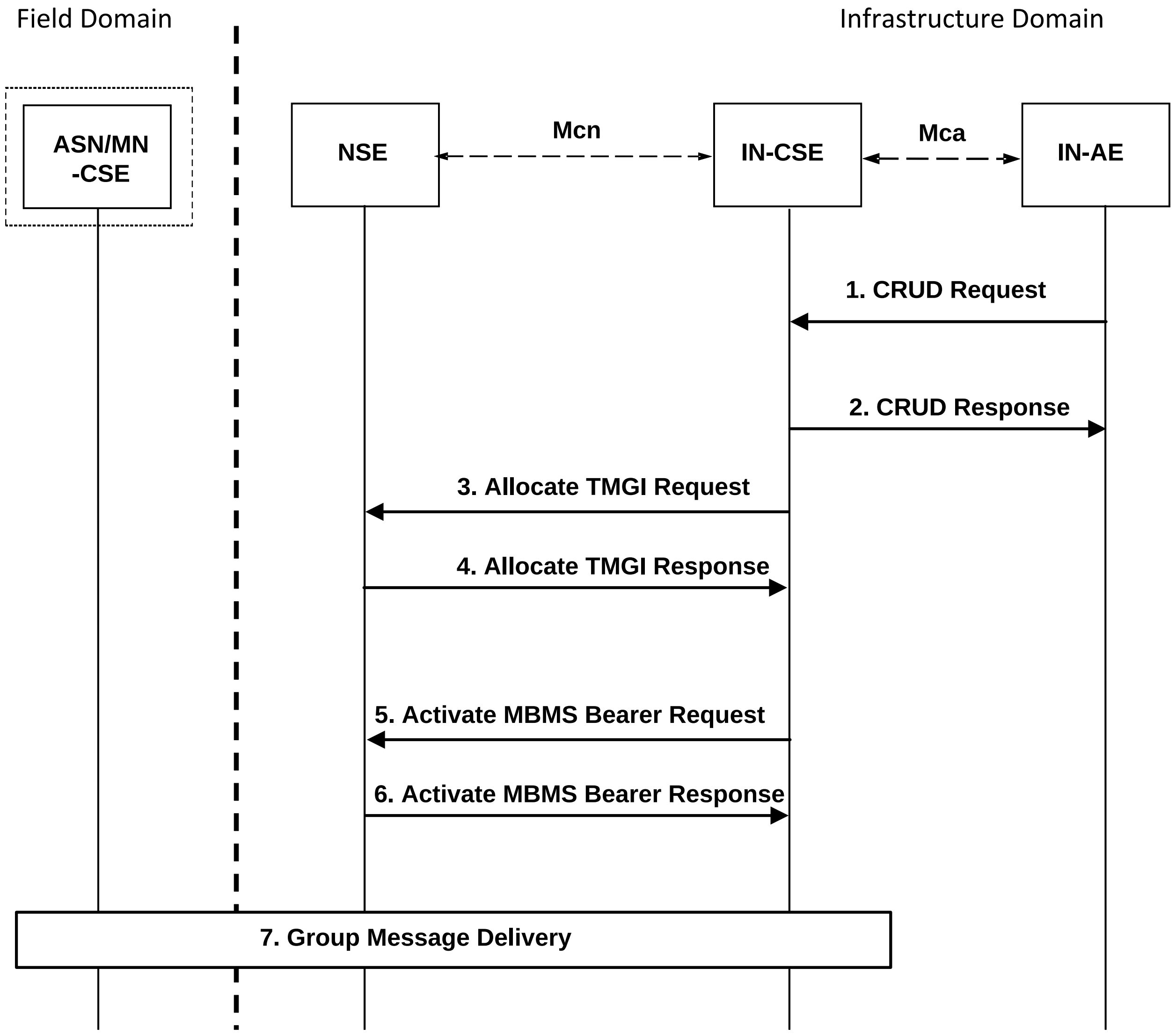


Figure 8.5.4.1.3-1: General group message delivery procedure

Step-1: Group Message Request

The AE sends the CRUD Request message to the IN-CSE to request sending group message. The group message request includes the group resourceID, location/area information, start time, QoS and the requested content.

Step-2: Authorization and determing the 3GPP underlying network group

The IN-CSE sends the response to the AE. The IN-CSE checks the type of the group to determine how to delivery the group message to the group members. If the group is of 3GPP MBMS group, or the group has a sub group which is the type of 3GPP MBMS group, the IN-CSE further verifies whether the AE is authorized to use the 3GPP MBMS group message delivery function. If the AE is authorized, then the SCEF function of the IN-CSE deliver the group message to the 3GPP MBMS group via the MBMS group message procedure, as specified in 3GPP TS 23.682 [i.5] and 3GPP TS 23.468 [i.14]. The 3GPP MBMS group corresponds to the group concept used in 3GPP TS 23.682 [i.5] and the resourceID of the 3GPP MBMS group corresponds to the External Group ID used in 3GPP TS 23.682 [i.5].

NOTE 1: In the group creation procedure, when the IN-CSE receives the group creation request from the AE, it should check the underlying networks of the group members. If all the group members are in the coverage of 3GPP MBMS service, the group type should be '3GPP MBMS'. If part of the group members are in the coverage of 3GPP MBMS sevice, the IN-CSE should create a sub group of the type '3GPP MBMS' for these group members, to facilitate the group message delivery in the future.

Step-3: Allocate TMGI Request

The IN-CSE shall send an Allocate TMGI Request message to request the NSE to allocate one or more TMGI. The request message shall include the number of requested TMGIs. The IN-CSE may include a list of TMGIs that are already allocated to the IN-CSE, and for which the IN-CSE 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.

Step-4: Allocate TMGI Response

The NSE shall send an Allocate TMGI Response message to the IN-CSE indicating the list of allocated TMGIs, and an expiration time for those TMGIs.

NOTE 2: The IN-CSE internally manages the TMGIs allocated to it, and it should know the expiration time of the TMGIs. If there is available valid TMGI, the IN-CSE can directly assign a TMGI to a specific group and the step 3 and step 4 can be skipped.

Step-5: Activate MBMS Bearer Request

The IN-CSE sends an Activate MBMS Bearer Request message to the NSE, including the TMGI which represents the MBMS bearer to be started, QoS, MBMS broadcast area, and start time. The TMGI is optional, and in this case, the NSE will allocate a new TMGI to the IN-CSE. The QoS shall be mapped into appropriate QoS parameters of the MBMS bearer. The MBMS broadcast area parameter shall include a list of MBMS Service Area Identities, or a list of cell IDs, or both.

NOTE 3: 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).

Step-6: Activate MBMS Bearer Response

The NSE sends an Activate MBMS Bearer Response to the IN-CSE, including the TMGI, the allocated FlowID, service description, NSE 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). The expiration time is included only if the NSE has allocated a TMGI as a result of this procedure.

NOTE 4: The IN-CSE can use the service description to provide information to the UE to access the MBMS bearer.

Step-7: Group message delivery

The IN-CSE transfers the content to be delivered to the group via the 3GPP network. In response to the received content, the ASN/MN-CSE may immediate or later communication with the IN-CSE.

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 3GPP Release-13 MTC procedure

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.

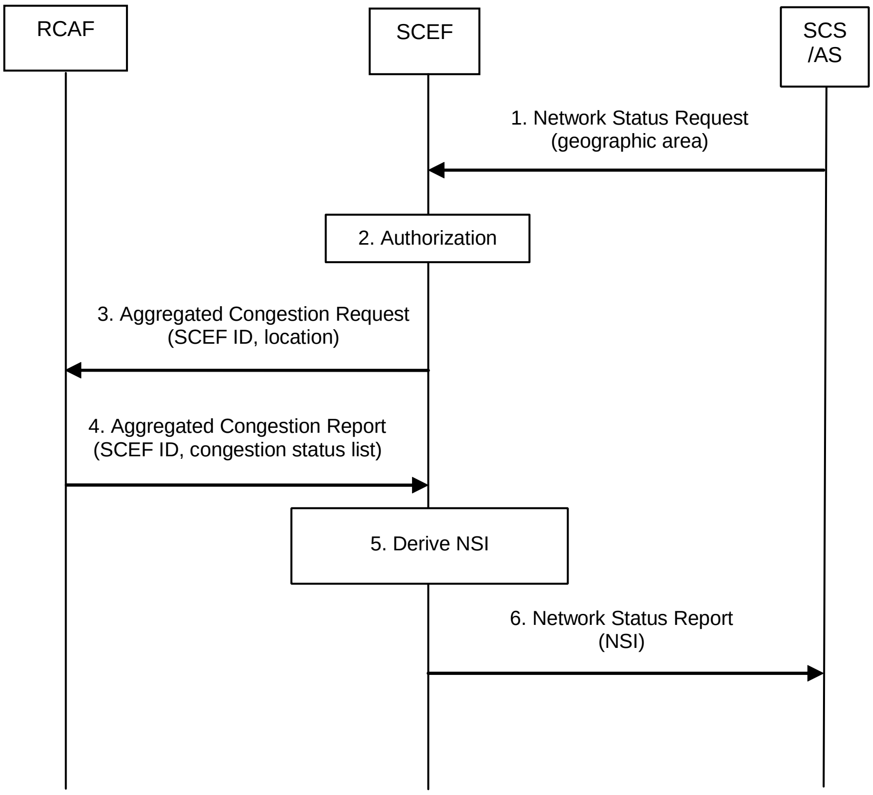

RCAF
SCEF
SCS
/AS
1. Network Status Request
(geographic area)
2. Authorization
3. Aggregated Congestion Request
(SCEF ID, location)
4. Aggregated Congestion Report
(SCEF ID, congestion status list)
5. Derive NSI
6. Network Status Report
(NSI)

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.

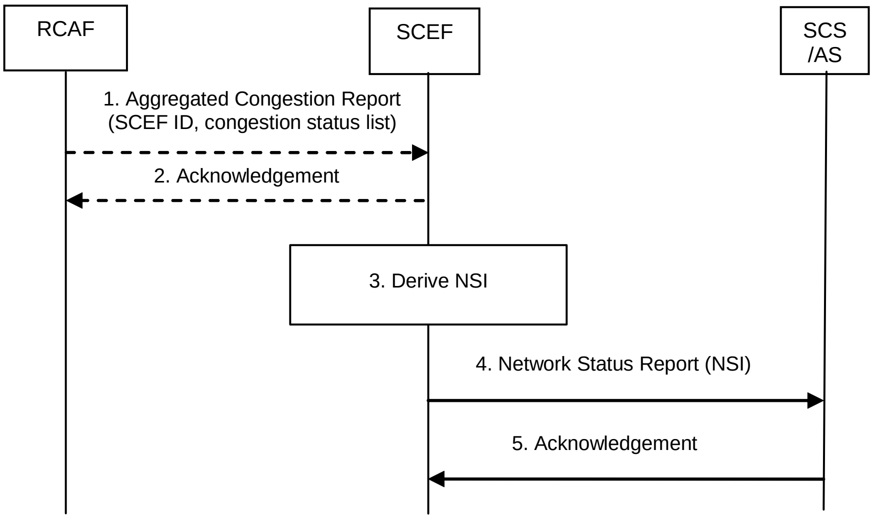

RCAF
SCEF
SCS /AS
1. Aggregated Congestion Report (SCEF ID, congestion status list)
2. Acknowledgement
3. Derive NSI
4. Network Status Report (NSI)
5. Acknowledgement

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.

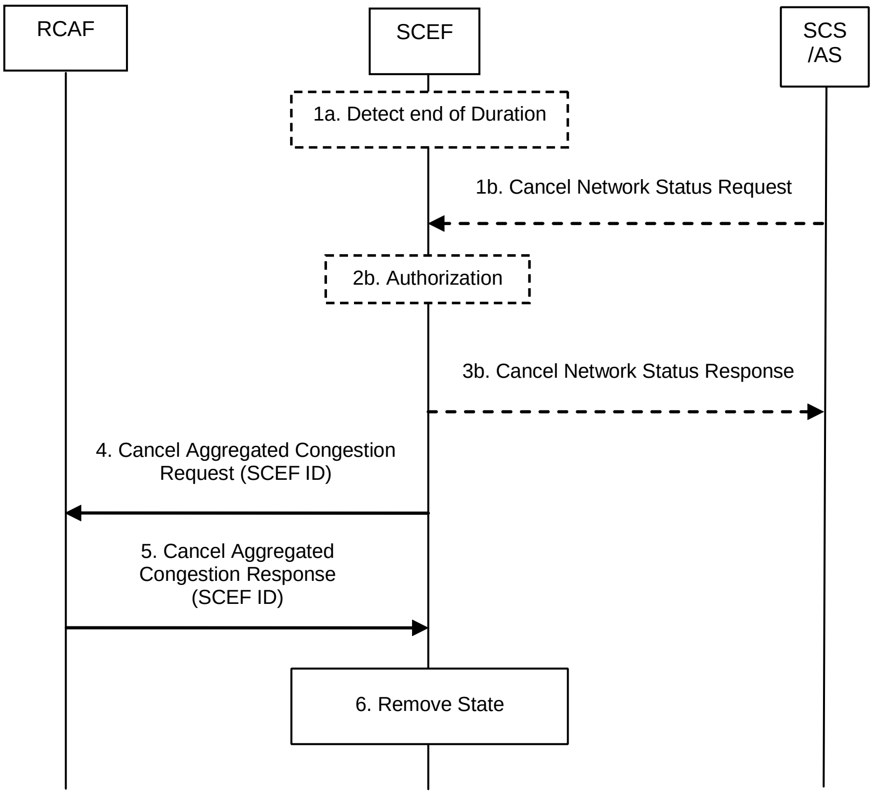

RCAF
SCEF
SCS
/AS
1a. Detect end of Duration
1b. Cancel Network Status Request
2b. Authorization
3b. Cancel Network Status Response
4. Cancel Aggregated Congestion Request (SCEF ID)
5. Cancel Aggregated Congestion Response (SCEF ID)
6. Remove State

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 indentifies 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 indentifies 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.

8.6.3 3GPP Parameters

A set of Network issue report parameters can be associated with a newwork stauts request, as defined in table 8.6.3-1.

Table 8.6.3-1: 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.

8.6.4 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 are described in subclauses 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.

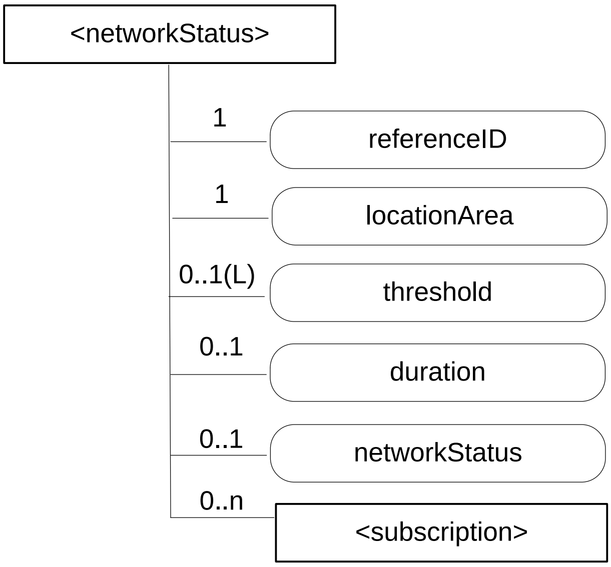


Figure 8.6.4.1.1.1-1: Structure of <*networkStatus*> resource

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**	**<*networkStatus*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.	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.

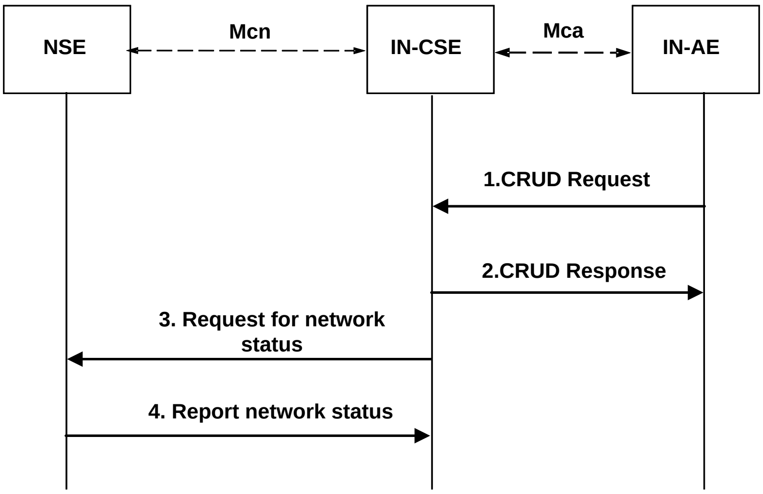


Figure 8.6.4.1.2.1-1: General procedure to support network status report between oneM2M and 3GPP network

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 an 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.

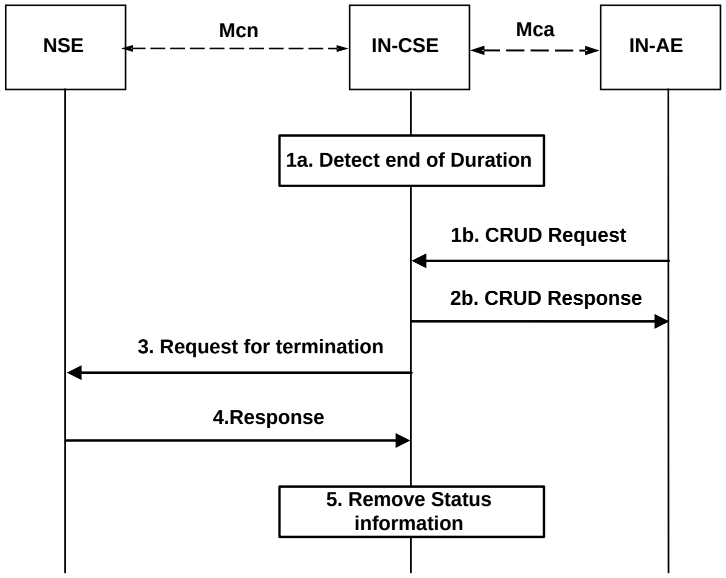

NSE
Mcn
IN-CSE
Mca
IN-AE
1a. Detect end of Duration
1b. CRUD Request
2b. CRUD Response
3. Request for termination
4.Response
5. Remove Status information

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.

History

Publication history		
V2.0.0	30-Aug-2016	Publication