ETSI TS 118 126 V4.7.1 (2026-02)

TECHNICAL SPECIFICATION

3GPP Interworking
(oneM2M TS-0026 version 4.7.1 Release 4)

Reference
RTS/oneM2M-0026r04v1

Keywords
3GPP, interworking, IoT, M2M

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Partnership Project oneM2M (oneM2M).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies interworking between the oneM2M service layer and an underlying 3GPP network, so that relevant 3GPP features defined for Cellular IoT can be used by the oneM2M service layer for the benefit of IoT applications.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

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

[1] ETSI TS 118 101: "oneM2M; Functional Architecture (oneM2M TS-0001)".

[2] ETSI TS 123 682: " Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements to facilitate communications with packet data networks and applications (3GPP TS 23.682 Release 15)".

[3] ETSI TS 118 104: "oneM2M; Service Layer Core Protocol (oneM2M TS-0004)".

[4] ETSI TS 129 122: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; T8 reference point for Northbound APIs (3GPP TS 29.122 Release 15)".

[5] ETSI TS 118 111: "oneM2M; Common Terminology (oneM2M TS-0011)".

[6] Open API™ Initiative: "OpenAPI 3.0.0 Specification".

[7] ETSI TS 129 154: "Universal Mobile Telecommunications System (UMTS); LTE; Service capability exposure functionality over Nt reference point (3GPP TS 29.154 Release 15)".

[8] ETSI TS 129 368: "Universal Mobile Telecommunications System (UMTS); LTE; Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS) (3GPP TS 29.368 Release 15)".

[9] ETSI TS 129 500: "5G; 5G System; Technical Realization of Service Based Architecture; Stage 3 (3GPP TS 29.500 Release 15).

[10] ETSI TS 129 571: "5G ; 5G System; Common Data Types for Service Based Interfaces; Stage 3 (3GPP TS 29.571 Release 15)".

[11] ETSI TS 123 203: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture (3GPP TS 23.203 Release 15)".

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.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] oneM2M Drafting Rules.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 118 111 [5] and the following apply:

Mca: Reference Point for M2M Communication with AE

Mcc: Reference Point for M2M Communication with CSE

Mcc': Reference Point for M2M Communication with CSE of different M2M Service Provider

Mcn: Reference Point for M2M Communication with NSE

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
ADN	Application Dedicated Node
ADN-AE	AE which resides in the Application Dedicated Node
AE	Application Entity
AE/CSE	Application Entity/Common Services Entity
AE-ID	Application Entity Identifier
API	Application Program Interface
AS	Application Server
ASN	Application Service Node
ASN/MN	Application Service Node/Middle Node
ASN-AE	Application Entity that is registered with the Common Services Entity at Application Service Node
ASN-CSE	CSE which resides in the Application Service Node
BDT	Background Data Transfer
CioT	Cellular IoT
CMDH	Communication Management and Delivery Handling
CP	Communication Patterns
CRUD	Create Retrieve Update Delete
CSE	Common Services Entity
CSE-ID	Common Service Entity Identifier
CSE-PoA	CSE Point of Access
CSF	Common Services Function

DDN	Downlink Data Notification
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRX	Discontinuous Reception
eDRX	Extended Discontinuous Reception
FQDN	Fully Qualified Domain Name
GGSN	Gateway GPRS Support Node
GMG CSF	Group Management CSF
GPRS	General Packet Radio Service
HTTP	HyperText Transfer Protocol
ID	Identifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IN	Infrastructure Node
IN-AE	Application Entity that is registered with the Common Services Entity in the Infrastructure Node
IN-CSE	CSE which resides in the Infrastructure Node
IP	Internet Protocol
M2M	Machine to Machine
MBMS	Multimedia Broadcast Multicast Service
MME	Mobility Management Entity
MN	Middle Node
MN-AE	Application Entity that is registered with the Common Services Entity in Middle Node
MN-CSE	CSE which resides in the Middle Node
MNO	Mobile Network Operator
MO	Mobile Originated
MT	Mobile Terminated
MTC	Machine Type Communications
MTC-IWF	Machine Type Communications Interworking Function
N/A	Not Applicable
NAT	Network Address Translation
NIDD	Non-IP Data Delivery
NoDN	Non-oneM2M Node
NSE	Network Service Entity
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PDP	Packet Data Protocol
PGW	PDN Gateway
PoA	Point of Access
PSM	Power Savings Mode
RAU	Routing Area Update
RDS	Reliable Data Service
SCEF	Service Capability Exposure Function
SCS	Service Capability Server
SLA	Service Layer Agreement
SMS	Short Message Service
TAU	Tracking Area Update
TMGI	Temporary Mobile Group Identity
TP	Traffic Patterns
TR	Technical Report
TS	Technical Specification
UE	User Equipment
UL	Uplink
URI	Uniform Resource Identifier

4 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

5 oneM2M Architecture for 3GPP cellular IoT interworking with oneM2M

5.1 Introduction

The present document introduces a baseline architecture for supporting 3GPP interworking and 3GPP Cellular Internet of Things (CioT) features such as IP and non-IP data Control Plane Data Delivery. It describes how the oneM2M system may leverage the IoT related features and services that 3GPP added in Release 10 through Release 15. Features and services may be accessed by an ADN-AE, MN-CSE, or an ASN-CSE that is hosted on a UE and an IN-CSE that is able to access services that are exposed by a MNO.

Figure 5.1-1 shows, at a high level, how 3GPP interfaces with external entities. A more detailed picture can be found in ETSI TS 123 682 [2].

The 3GPP Trust Domain provides three interfaces to SCS for MTC:

i) IP based interface at SGi reference point;

ii) RESTful API interface at T8 reference point;

iii) Diameter based interface at Tsp reference point.

The Service Capability Server (SCS) is a 3GPP term that refers to an entity which connects to the 3GPP Trust Domain to communicate with UEs used for Machine Type Communication (MTC).

The SCS offers services to MTC Applications that are hosted on the UE or in an Application Server (AS). The SCS connects to the underlying 3GPP network as follows:

- Via the Sgi interface for IP based data plane communication between the SCS and 3GPP Trust Domain for MTC.
- Via the MTC Interworking Function (MTC-IWF) through the Tsp interface which is based on Diameter protocol as defined in ETSI TS 129 368 [8]. In this case, SCS shall support the Diameter protocol.
- Via Service Capability Exposure Function (SCEF) through the T8 interface which is based on a RESTful API as defined in ETSI TS 129 122 [4]. In this case, the SCS shall support the HTTP protocol.

MTC Applications on the UE interact with the underlying 3GPP network via 3 different methods. MTC Applications may use the underlying 3GPP network to send IP packets to and from the SCS and/or other MTC Applications. MT SMS messages (i.e. device triggers) may be received by MTC Applications that are hosted on the UE and MTC Applications may use SMS messages to send data to the SCS and/or other MTC Applications. Also, NAS messaging may be used to send and receive non-IP data, send and receive IP data, configure power savings mode, configure extended idle mode DRX, configure low priority indicators, etc.

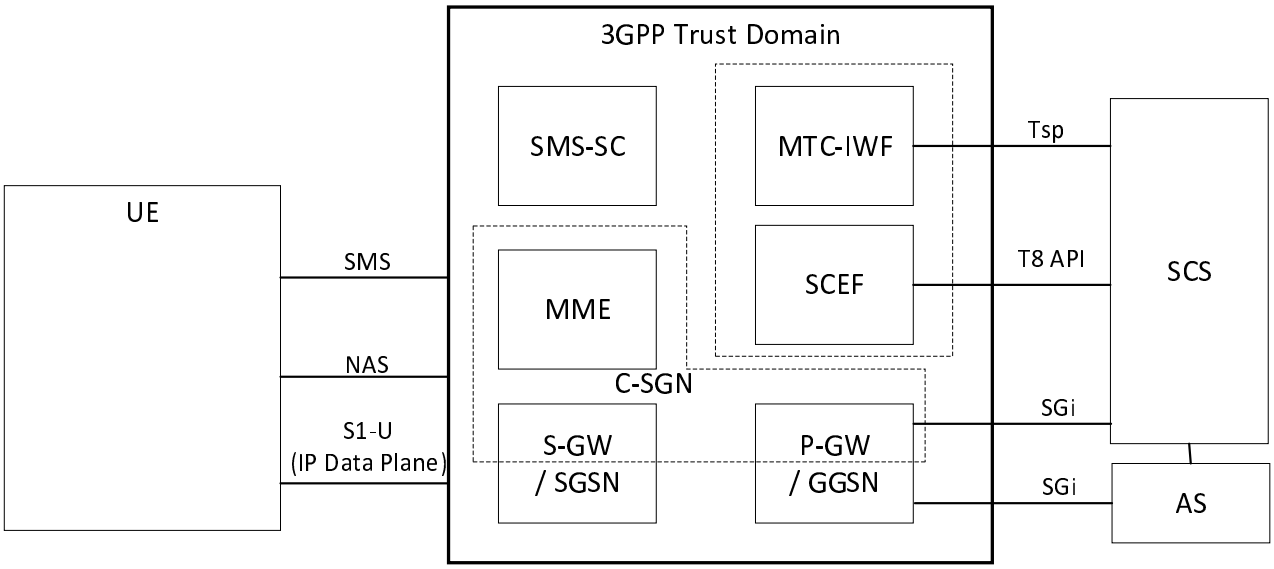

Figure 5.1-1: 3GPP IoT Related Interfaces

5.2 Functional mapping between 3GPP and oneM2M

Figure 5.2-1 shows an architecture and functional mapping for the 3GPP Trust Domain which describes how oneM2M functional entities may access features and services that are exposed by 3GPP.

The "MTC Applications" hosted on the UE may be deployed as follows:

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

The SCS may be an IN-CSE, and the "MTC-Applications" or ASs that are hosted in an external network may be IN-AEs.

The "3GPP Trust Domain" in Figures 5.1-1 and Figure 5.2-1 captures the functional entities that shall be part of the 3GPP domain (the network). Although Figure 5.2-1 shows that the IN-CSE and IN-AE are outside of the 3GPP Domain, the IN-CSE may be part of the operator domain.

Figure 5.2-1 also shows the oneM2M reference points Mcn, Mcc and Mca. The Mcc reference point enables communication between CSEs such as the CSE shown on the left-hand side and the IN-CSE shown on the right-hand side of Figure 5.2-1.

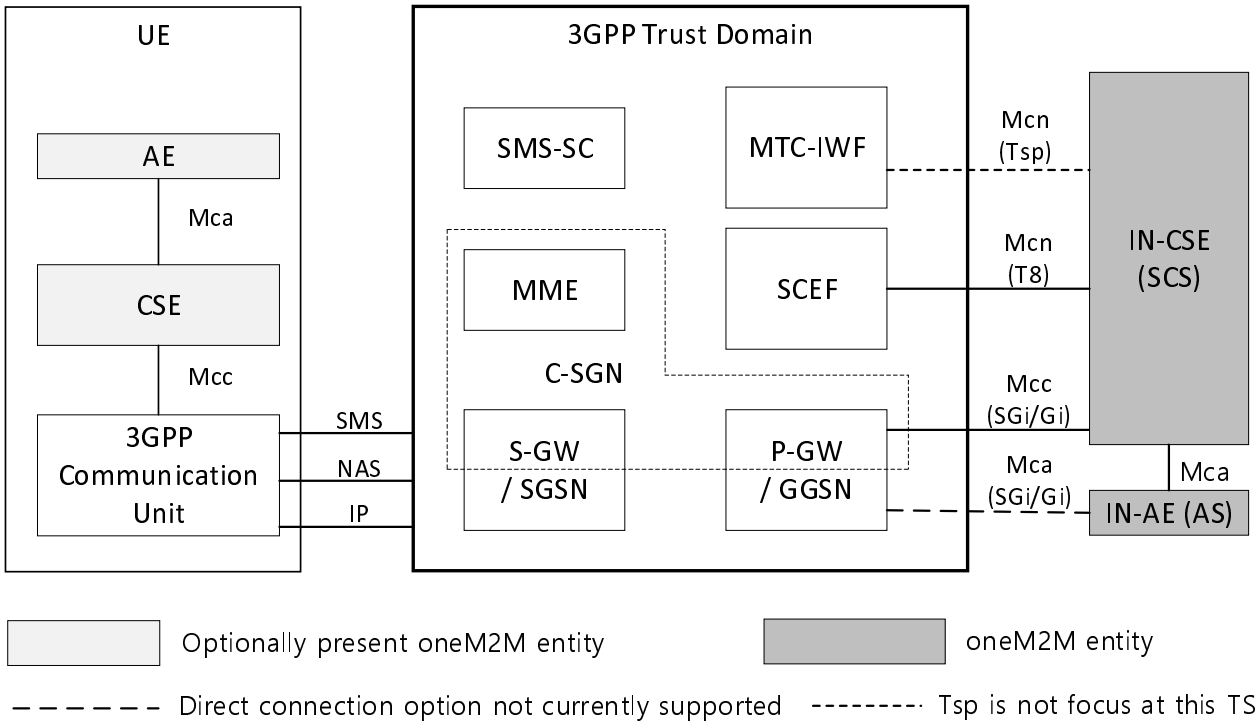

Figure 5.2-1: oneM2M Interfaces to the underlying 3GPP Network

Several implementation options for the placement of the oneM2M IN-CSE relative to the SCEF and the underlying 3GPP network are envisioned. In all implementations, the SCEF always resides within 3GPP domain.

In some options the IN-CSE and the SCEF are deployed by a MNO and are both part of the operator domain. In other options the SCEF is part of the 3GPP domain and the IN-CSE is not part of the operator domain.

In all options, services within the IN-CSE may access the network services that are exposed by the SCEF via the T8 reference point APIs.

5.3 3GPP Cellular IoT Features and Services

The SCEF exposes the following services to the IN-CSE. The present document describes how the IN-CSE may access each service:

1) Non-IP Data Delivery, see clause 7.1.
2) UE Context Information Storage, see clause 7.2.
3) High Latency Communication - Extended S-GW and SCEF Buffering, see clause 7.3.
4) Monitoring Events, see clause 7.4.
5) SMS Based Device Triggering, see clause 7.5.
6) Configuring Communication Patterns, see clause 7.6.
7) Group Messaging (via MBMS), see clause 7.7.
8) Mobile Core Network Issue Reports, see clause 7.8.
9) Configuring Session QoS, see clause 7.9.
10) Background Data Transfer, see clause 7.10.
11) Configuring Session Sponsorship, see clause 7.11.
12) Network Parameter Configuration - Configuring PSM and eDRX, see clause 7.12.

A UE hosted ADN-AE, MN-CSE, or ASN-CSE may access the following features that may be exposed by the 3GPP modem. The present document describes how the UE hosted ADN-AE, MN-CSE, or ASN-CSE may access each service:

1) Non-IP Data Delivery, see clause 7.1.
2) High Latency Communication - Configuring PSM and eDRX, see clause 7.3.
3) SMS Based Device Triggering, see clause 7.5.
4) Group Messaging (via MBMS), see clause 7.7.

5.4 SCEF T8 API

The T8 APIs are a set of APIs defining the related procedures and resources for the interaction between the SCEF and the IN-CSE (SCS). The APIs are RESTful and based on the HTTP protocol. The architectural level description of the T8 APIs is defined in ETSI TS 123 682 [2]. The protocol level description of the T8 APIs including how the individual T8 requests and responses are mapped to HTTP and encoded in JSON as defined in ETSI TS 129 122 [4].

The present document defines how an IN-CSE interworks with a SCEF via the T8 APIs. For each of the supported SCEF services, the present document defines how the individual requests and responses are configured, sent and received by the IN-CSE and SCEF. Details are also provided for how an IN-CSE generates and processes T8 requests and responses using the T8 HTTP protocol binding and JSON message encodings.

The intent of the present document is to complement ETSI TS 123 682 [2] and ETSI TS 129 122 [4] and care has been taken to minimize duplication of information. It is assumed that the reader of the present document is knowledgeable of the T8 APIs as defined in ETSI TS 123 682 [2] and ETSI TS 129 122 [4].

6 Connectivity Establishment

6.1 Overview

ADN-AE, ASN/MN-CSE and the serving CSE (SCS) communicate after completion of the underlying 3GPP network bearer establishment and discovery of the serving CSE (SCS). Data can then traverse between the oneM2M entities over the IP connection in the underlying 3GPP network over the 3GPP Gi/SGi interface. Figure 6.1-1 depicts the connectivity between the ADN-AE, ASN/MN-CSE and the CSE (SCS).

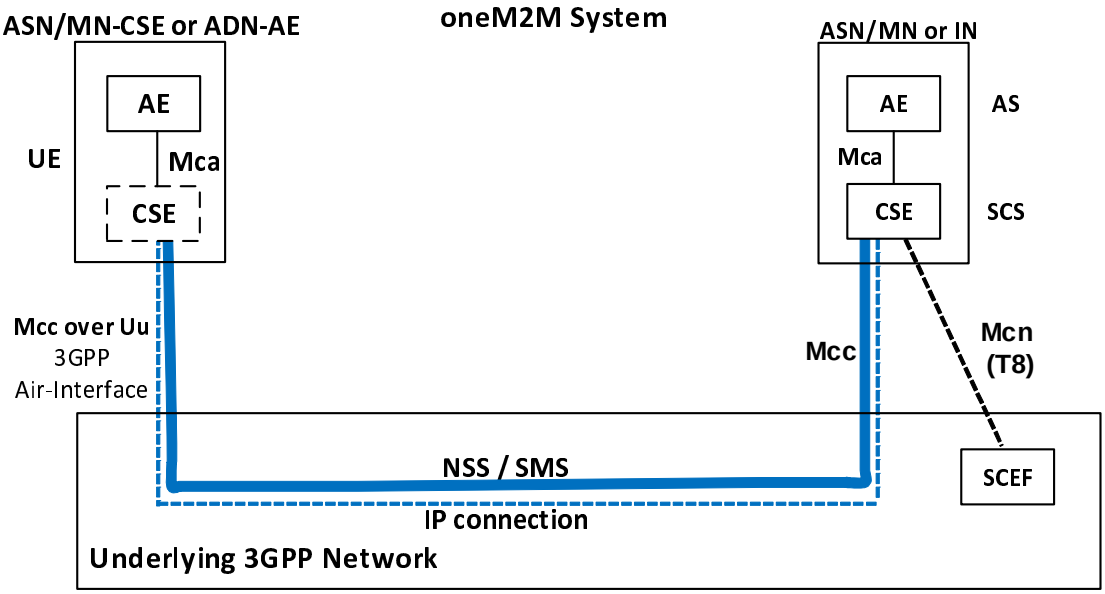

Figure 6.1-1: Connectivity Establishment between ASN/MN-CSE or ADN-AE and CSE (SCS)

For ADN/ASN/MN initiated connectivity establishment, it is assumed that there is no connectivity previously established, i.e. no association between the ASN/MN-CSE or ADN-AE and the serving CSE (SCS) exists. When the ASN/MN-CSE or ADN-AE needs to send data to the serving CSE (SCS) it first discovers the serving CSE (SCS), which is located in a packet data network, and establishes a connection. Two methods can be used, as follows:

1) Use of DHCP and DNS.

2) Pre-configuration.

For serving CSE (SCS) initiated connectivity establishment, it is assumed that there is no connectivity previously established between the ASN/MN-CSE or ADN-AE and the serving CSE (SCS). When the serving CSE (SCS) needs to contact the ASN/MN-CSE to send data or request data, connectivity between them is established. This connectivity is triggered by the serving CSE (SCS).

The ASN/MN-CSE or ADN-AE requests the DNS server address from the DHCP server followed by requesting the serving CSE IP address from the DNS server.

6.2 IP connectivity

6.2.1 ASN/MN-CSE Pre-configuration

The ASN/MN-CSE or ADN-AE is preconfigured with the fully qualified domain name (FQDN) of the serving CSE (SCS) or the IP address of the serving CSE (SCS). If the FQDN is known, DNS resolution is used to obtain the IP address.

6.2.2 ASN/MN-CSE or ADN-AE Initiated Connectivity Establishment Procedure

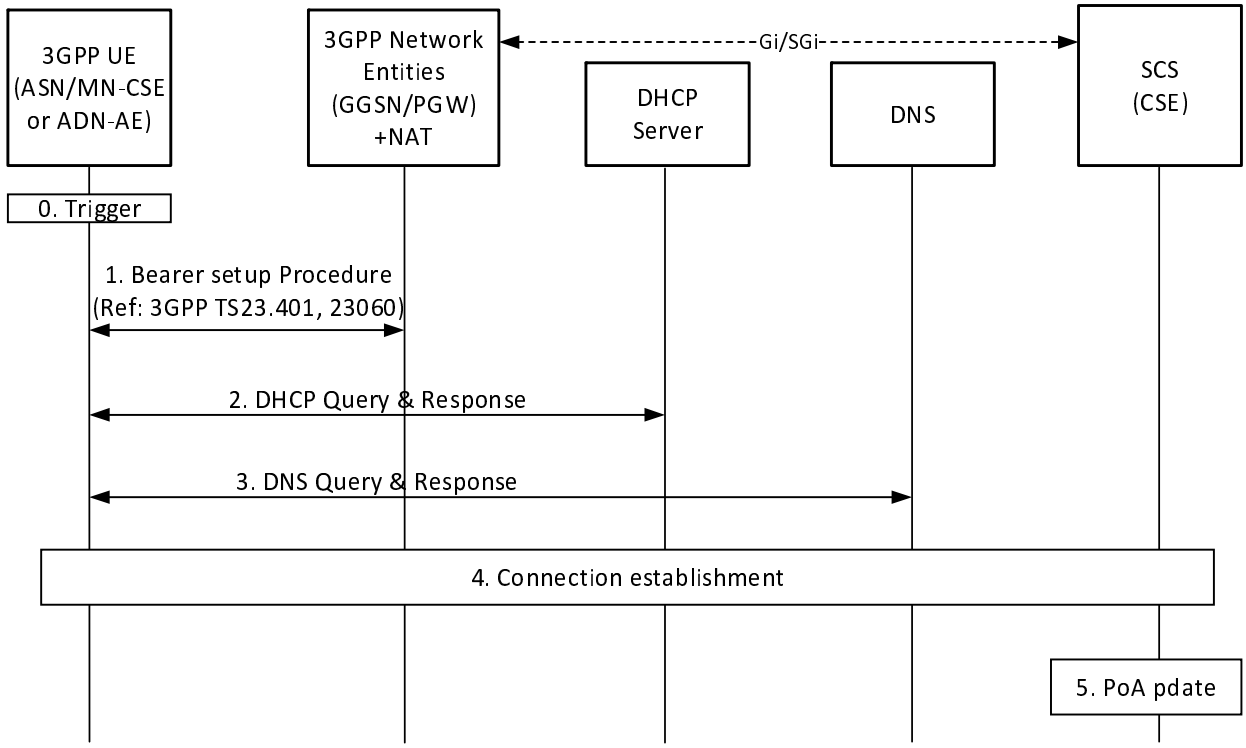

Figure 6.2.2-1: ASN/MN-CSE or ADN-AE initiated connectivity establishment

Step 0: Trigger

Subsequent procedures are triggered either when the ASN/MN-CSE or ADN-AE powers on or resulting from Device Triggering.

Step 1: Bearer Setup Procedure

Establish a 3GPP bearer(s) if not already available by using the procedures available in the underlying 3GPP network.

Step 2: DHCP Query & Response

The ASN/MN-CSE or ADN-AE sends a query to a DHCP server to find a particular DNS server IP address. The DHCP server responds with the IP address of a corresponding DNS server. Additionally, it is also possible to include one or a list of domain names, i.e. FQDNs of target CSEs (SCS).

Step 3: DNS Query & Response

The ASN/MN-CSE or ADN-AE performs a DNS query to retrieve the CSE(s) (SCS) IP addresses from which one is selected. If the response does not contain the IP addresses, an additional DNS query is needed to resolve a Fully Qualified Domain Name (FQDN) of the serving CSE (SCS) to an IP address.

Step 4: Connection Establishment

After reception of domain name and IP address of an CSE (SCS), the ASN/MN-CSE or ADN-AE can initiate communication towards the CSE (SCS) via the IP connection. The CSE (SCS) at this time shall be informed which Trigger Recipient ID of the ASN/MN-CSE or ADN-AE or the AE-PoA of the ADN-AE to use for establishing communication.

Step 5: CSE-PoA Update

Once the M2M Service Connection (Mcc or Mca) is established to the CSE (SCS), the CSE-PoA of the ASN-CSE/MN-CSE or the AE-PoA of the ADN-AE shall be updated with the new established IP address.

6.2.3 CSE (SCS) initiated connectivity establishment procedure

See clause 7.1 for NIDD based connection establishment and clause 7.5 for 3GPP Based Device Triggering.

6.3 UE Attach with oneM2M Registration Procedure

After a UE attaches to an underlying 3GPP network and establishes a data (i.e. PDN/PDP) connection, assuming it has not been registered previously with the oneM2M platform, it will initiate a oneM2M registration procedure. The oneM2M part of the procedure corresponds to the generic one described in clause 10.2.2 of ETSI TS 118 101 [1], where the Registrar CSE is the CSE (SCS).

If the UE hosts one or more ADNs, the registration will result in the CSE (SCS) hosting one or more corresponding <*AE*> resources for the UE. If the UE hosts an ASN or a MN, the registration of the ASN/MN-CSE will result in the CSE (SCS) hosting a corresponding <*remoteCSE*> resource for the ASN/MN-CSE. The flow is depicted in Figure 6.3-1.

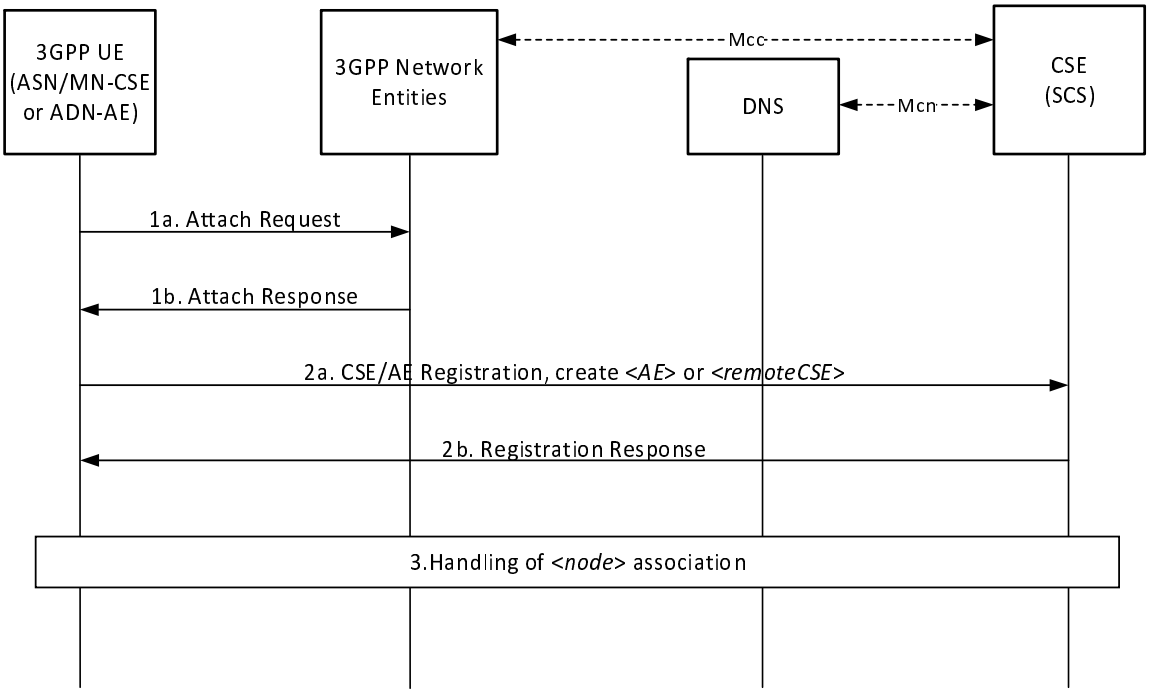

Figure 6.3-1: UE Attach Procedure with oneM2M Registration

Steps 1a and 1b: UE Attach Request and Response

The UE determines that it needs to perform the 3GPP Attach procedure.

The underlying 3GPP Network responds to the UE Attach request.

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

The UE Hosting an ADN or an ASN/MN registers to the oneM2M infrastructure, by performing the registration procedure detailed in clause 10.2.2 of ETSI TS 118 101 [1]:

- If the UE hosts an ADN, the registration procedure of the ADN-AE(s) will include the creation of corresponding <*AE*> resource(s) being hosted at the CSE (SCS).
- If the UE hosts an ASN or MN, the registration procedure of the ASN/MN-CSE will include the establishment of a security association and the creation of a <*remoteCSE*> resource, corresponding to the registree CSE, to be hosted at the CSE (SCS).

The CSE (SCS) responds to the UE hosted ADN-AE(s) or ASN/MN-CSE request for registration.

These steps allow the UE hosted ADN-AE(s) or ASN/MN-CSE to provide the CSE (SCS) with information needed for communication and providing services, e.g. *pointOfAccess*. In return, the CSE (SCS) provides the UE with oneM2M specific information, e.g. by assigning AE-ID(s) or CSE-ID to the registree(s), respectively

Information provided by the ASN/MN-CSE or ADN-AE(s) to the CSE (SCS) at this time shall include:

- *M2M-Ext-ID*, *Trigger-Recipient-ID* as attributes of <*AE*> or <*remoteCSE*>, if available.
- *externalGroupID* as an attribute of <*AE*> or <*remoteCSE*>, if available.
- *nodeLink* as an attribute of the <*AE*> or <*remoteCSE*> resources, providing the resource identifier of a corresponding <*node*> resource, if pre-provisioned at the UE.

Step 3: Handling of association with a <*node*> resource

If in Step 2, the CSE (SCS) receives a valid *nodeLink* (as an attribute of the <*AE*> or <*remoteCSE*> resources) it means that the <*node*> resource storing the node specific information for this UE exists. For a UE hosted ASN/MN, the CSE (SCS) shall ensure that the *hostedCSELink* attribute of the corresponding <*node*> resource contains the resource identifier of the <*remoteCSE* > resource. For a UE hosted ADN, the CSE (SCS) shall ensure that the *hostedAELinks* attribute of the corresponding <*node*> resource includes the resource identifier of all the corresponding <*AE* > resources.

If in Step 2, the CSE (SCS) does not receive a valid *nodeLink* (as an attribute of the <*AE*> or <*remoteCSE*> resources) or the attribute is not present, the CSE (SCS) shall create a <*node*> resource for this UE. The CSE (SCS) shall populate the *nodeLink* attribute of the <*AE*> or <*remoteCSE*> resources with the resource identifier of the newly created <*node*> resource. For a UE hosted ASN/MN, the CSE (SCS) shall also populate the *hostedCSELink* attribute of the <*node*> resource with the resource identifier of the <*remoteCSE* > resource. For a UE hosted ADN, the CSE (SCS) shall ensure that the *hostedAELinks* attribute of the <*node*> resource includes the resource identifiers of all the corresponding <*AE*> resources.

If the following resources do not exist for this underlying 3GPP network, the CSE (SCS) may:

- Create a <*schedule*> resource as a child of the <*node*> representing the UE, which represents the communication schedule for the underlying 3GPP network where the Attach procedure was completed. While no specific scheduling information is available, the <*schedule*> may reflect that communications are available continuously. The CSE (SCS) may set the networkCoordinated attribute, based on the UE pre-provisioned information or local policies, to indicate if the schedule should be coordinated with the underlying 3GPP network.
- Create the [*activeCmdhPolicy]* resource as a child of the <*node*> resource representing the UE, providing the active communication policies for the underlying 3GPP network where the Attach procedure was completed. The CSE (SCS) shall populate the *mgmtLink* of the active *[cmdhNwAccessRule]* with a link to the <*schedule*> resource created for the communication schedule with this underlying 3GPP network.

7 Interworking with CioT network features exposed to service layer

7.1 Cellular IoT non-IP data delivery(NIDD)

7.1.1 SCEF-based NIDD

7.1.1.1 SCEF Configuration for NIDD

The 3GPP SCEF Non-IP Data Delivery (NIDD) functionality supports an API to allow the exchange of Non-IP data between an IN-CSE and an MN-CSE, ADN-AE, or ASN-CSE hosted on a UE. Via this SCEF NIDD API, an IN-CSE may exchange oneM2M request and response primitives with an MN-CSE, ADN-AE, or ASN-CSE hosted on a UE.

NOTE: The exchange of oneM2M primitives over the Mcn reference point via NIDD is an extension upon the capability defined within ETSI TS 118 101 [1] and ETSI TS 118 104 [3] to exchange oneM2M primitives over the Mca and Mcc reference points. The same procedures defined by ETSI TS 118 101 [1] and ETSI TS 118 104 [3] for exchanging oneM2M primitives over the Mca and Mcc are also applicable to Mcn via NIDD unless otherwise stated in the present document.

The SCEF NIDD API supports an NIDD Configuration procedure that may be used by the IN-CSE to inform the SCEF that it expects Non-IP Data from a UE hosting an MN-CSE, ADN-AE, or ASN-CSE. Figure 7.1.1.1-1 illustrates this procedure. If the NIDD Configuration procedure is performed, the IN-CSE should perform the procedure before a UE attaches and attempts to establish a Non-IP PDN connection to the SCEF.

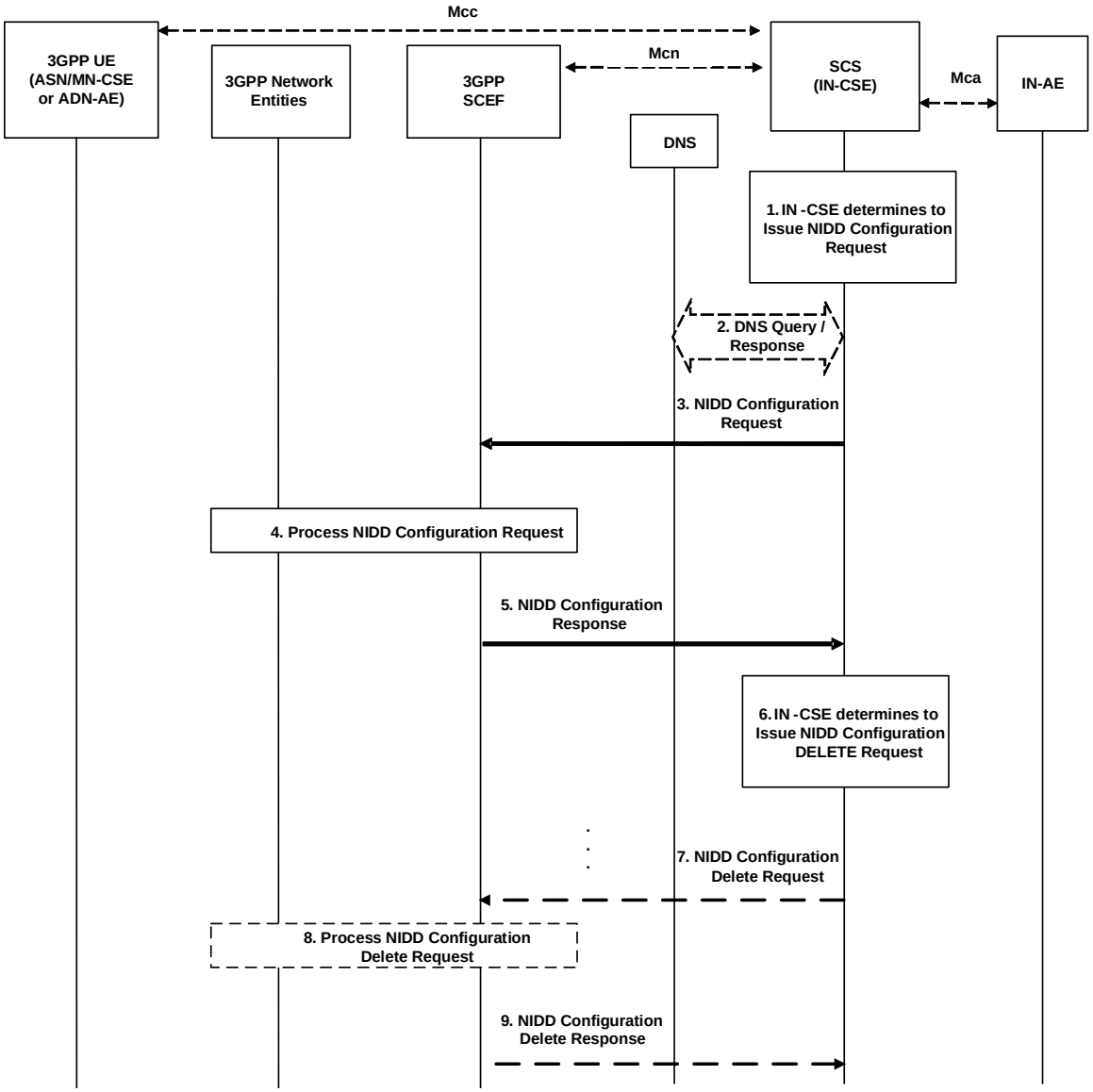

Figure 7.1.1.1-1: NIDD Configuration Request

Pre-conditions:

The IN-CSE is configured with the *M2M-Ext-ID* of a UE and an indication that the ASN/MN-CSE or ADN-AE hosted on this UE uses NIDD to exchange oneM2M primitives with the IN-CSE. This information is configured in the *nodeID* and *niddRequired* attributes, respectively of the <*serviceSubscribedNode*> resource corresponding to the UE.

There is a relationship in place between the Service Provider and MNO allowing the IN-CSE to perform NIDD Configuration Requests to the underlying 3GPP network. The method for establishing this relationship is outside the scope of the present document.

Step 1: IN-CSE determines to issue NIDD Configuration Request

If the *niddRequired* attribute of a <*serviceSubscribedNode*> resource associated with a UE hosting an ASN/MN-CSE or ADN-AE is set to TRUE, then the IN-CSE shall issue a NIDD Configuration Request to the proper SCEF.

Step 2 (Optional): DNS Query/Response

To determine which SCEF to contact, an IN-CSE may determine the IP address(es)/port(s) of the proper SCEF by performing a DNS query using the *M2M-Ext-ID* of the UE hosting the ASN/MN-CSE or ADN-AE. This *M2M-Ext-ID* shall be configured in the *nodeID* attribute of the <*serviceSubscribedNode*> resource associated with the UE. Alternatively, an IN-CSE may use a pre-configured SCEF identifier. The method for pre-configuring a SCEF identifier into the IN-CSE is outside the scope of the present document.

Step 3: NIDD Configuration Request

The IN-CSE issues a NIDD Configuration Request for a particular ASN/MN-CSE or ADN-AE hosted on a UE. The request is configured as follows:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-nidd/v1/{scsAsId}/configurations/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *NiddConfiguration* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *M2M-Ext-ID* of the UE hosting the targeted ASN/MN-CSE or ADN-AE.
  - *notificationDestination* shall be set to a URI of the IN-CSE that the SCEF will deliver MO NIDD data to.
  - *duration* specifies the lifetime of the NIDD Configuration and shall be set per SLA between the Service Provider and MNO. The SCEF may change the NIDD *duration* value.
  - *pdnEstablishmentOption* may be used to indicate the IN-CSE's default preference for how the SCEF should process a MT NIDD Request from the IN-CSE if the UE has not yet established a Non-IP PDN connection to the SCEF. This value shall be set based on SLA with the MNO.
  - *reliableDataService* shall be set to TRUE or FALSE to indicate that the Reliable Data Service is enabled or disabled based on IN-CSE preferences.
  - *rdsPorts* shall be set to the source and destination ports used for MO and MT NIDD between the IN-CSE and the ASN/MN-CSE or ADN-AE hosted on the UE. This field shall be set if *reliableDataService* is set to TRUE.
  - *supportedFeatures* shall be set to a string value of "0" indicating no support for group message delivery over NIDD, NIDD notifications over Websocket, testing of NIDD notifications or MT_NIDD_modification_cancellation.
  - *msisdn, requestTestNotification, websockNotifConfig and niddDownlinkDataTransfers* are not supported by the present document and shall not be included.

Step 4: Process NIDD Configuration Request

The SCEF processes the request.

Step 5: NIDD Configuration Response

If the NIDD Configuration Request is successfully processed, the SCEF responds indicating the request was accepted. The message includes the following information:

- A response code of 201 CREATED.
- The *URI* of the NIDD Configuration resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{configurationId}* segment is configured by the SCEF.

- The response payload will include a *NiddConfiguration* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *maximumPacketSize* is set to the maximum supported NIDD packet size that can be transferred to the UE by the SCEF. This value is configured by the SCEF per SLA with the MNO.
  - *status* is set to a value that indicates the NIDD configuration status (e.g. ACTIVE).
  - *self* is configured with a URI to the resource created by the SCEF for the request.

If the response indicates that the request was accepted, the IN-CSE shall use the *maximumPacketSize* as a limit on the maximum size MT NIDD Request it shall initiate towards the corresponding UE specified in the NIDD Configuration Request.

If the NIDD Configuration Request results in an error, the IN-CSE shall not use NIDD for the corresponding UE until the error is resolved. See clause 8.3 for a list of possible error scenarios.

Step 6 (Optional): NIDD Configuration Delete Request

If the IN-CSE detects that <*serviceSubscribedNode*> is deleted or the <*serviceSubscribedNode*> *niddRequired* attribute is updated to FALSE, then the IN-CSE shall issue a NIDD Configuration Delete Request for the UE. The request is configured as follows:

- An HTTP DELETE method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*configurationId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the NIDD Configuration was created.
- The request shall not contain a payload.

Step 7 (Optional): Process NIDD Configuration Delete Request

The SCEF processes the request.

Step 8 (Optional): NIDD Configuration Delete Response

The SCEF responds with a 204 NO CONTENT that indicates the NIDD Configuration was cancelled.

7.1.1.2 SCEF-based Mobile Terminated NIDD

The SCEF API supports a Mobile Terminated (MT) NIDD procedure that may be used by the IN-CSE to send downlink non-IP data to a UE hosting an MN-CSE, ADN-AE, or ASN-CSE. Figure 7.1.1.2-1 illustrates this procedure.

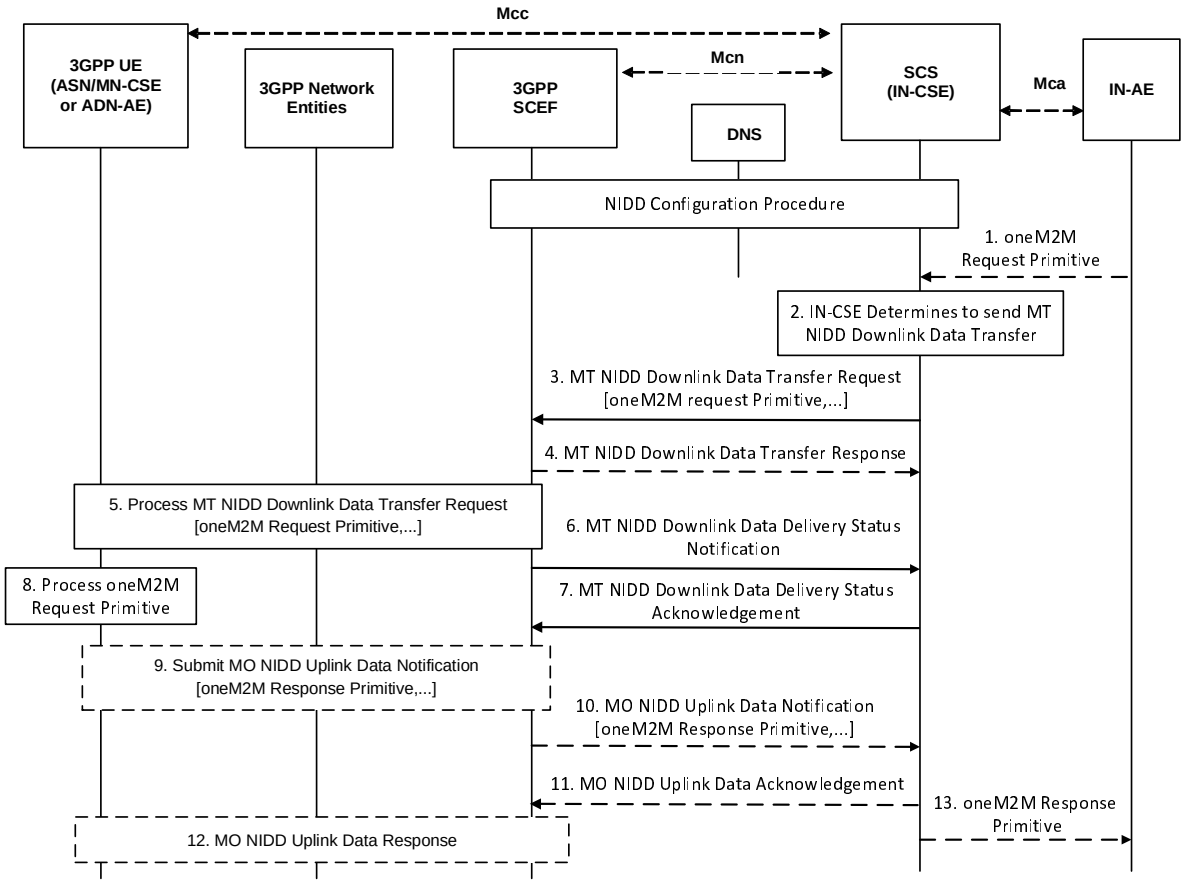

Figure 7.1.1.2-1: SCEF-based Mobile Terminated NIDD

Pre-conditions:

The NIDD Configuration procedure defined in clause 7.1.1.1 completes successfully.

Step 1 (Optional): Application issues oneM2M Request Primitive

An AE (e.g. IN-AE) may issue a oneM2M request targeting an ASN/MN-CSE or ADN-AE.

Step 2: IN-CSE determines to issue a SCEF-based Mobile Terminated NIDD Downlink Data Transfer Request

The IN-CSE shall only issue a SCEF-based Mobile Terminated (MT) NIDD Downlink Data Transfer Request if the NIDD Configuration Request for the targeted ASN/MN-CSE or ADN-AE hosted on a UE was successful and the size of the oneM2M request primitive to be sent in the MT NIDD Request is less than or equal to the *maximumPacketSize* defined in the NIDD Configuration response.

Step 3: MT NIDD Downlink Data Transfer Request

The IN-CSE issues a MT NIDD Downlink Data Transfer Request for a particular ASN/MN-CSE or ADN-AE hosted on a UE. The request is configured as follows:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries.* The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{configurationId}* segment shall be configured with the {*configurationId*} returned by the SCEF when the NIDD Configuration was performed by the IN-CSE for this ASN/MN-CSE or ADN-AE.
- The request payload shall include a *NiddDownlinkDataTransfer* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *M2M-Ext-ID* of the UE hosting the targeted ASN/MN-CSE or ADN-AE.

- *maximumLatency* may be set to indicate the maximum delay acceptable for MT data and used to configure the buffer duration in the underlying 3GPP network; a maximum latency of 0 indicates that buffering is not allowed. If maximum latency is not provided, the SCEF determines the acceptable delay based on local policies.

- *priority* may be set to indicate the priority of the non-IP data packet relative to other non-IP data packets. If a priority is not provided, the SCEF determines the acceptable delay based on local policies.

- *pdnEstablishmentOption* may be used to indicate the IN-CSE's default preference for how the SCEF should process a MT NIDD request from the IN-CSE if the UE has not yet established a Non-IP PDN connection to the SCEF. If a PDN Connection Establishment Option is not provided with the non-IP packet, the SCEF uses the PDN Connection Establishment Option that was provided during NIDD Configuration to decide how to handle the absence of a PDN connection.

- *reliableDataService* (optional) shall be set to TRUE or FALSE to indicate that Reliable Data Service acknowledgement is required or not.

- *rdsPort* shall be set to the source and destination ports used for MO and MT NIDD between the IN-CSE and the ASN/MN-CSE or ADN-AE hosted on the UE.

- *data* shall be configured with a oneM2M primitive to send to the UE hosting the targeted ASN/MN-CSE or ADN-AE.

NOTE 1: The use of a PUT request to replace an existing MT NIDD Downlink Data Transfer request and a GET request to read the parameters associated with an existing MT NIDD Downlink Data Transfer request by the IN-CSE are not used by the present document.

Step 4: MT NIDD Downlink Data Transfer Response

If the targeted UE does not have an active NIDD PDN connection to the SCEF, the SCEF may buffer the request until the UE establishes the connection. The SCEF may also trigger the UE to establish a NIDD PDN connection to the SCEF. Alternatively, the SCEF may generate an error.

The SCEF may return a MT NIDD Downlink Data Transfer Response to the IN-CSE to indicate if the request is buffered, a trigger has been generated, or an error has occurred. The fields of the response are populated as follows:

- A response code of 200 OK or 201 CREATED:

  - 200 OK is returned if the delivery of the NIDD Downlink Data Transfer Request was successful.

  - 201 CREATED is returned if the SCEF accepted and buffered the NIDD Downlink Data Transfer Request to be performed later.

- The *URI* of the NIDD Downlink Data Transfer resource created by the SCEF, for the case when response code is 201 CREATED. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries/{downlinkDataDeliveryId}*. The *{apiRoot}, {scsAsId}* and *{configurationId}* segments match those in the request. The *{downlinkDataDeliveryId}* segment is configured by the SCEF.

- The response payload will include a *NiddDownlinkDataTransfer* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:

  - *deliveryStatus* is used to indicate a success or an appropriate error cause value as defined in ETSI TS 129 122 [4].

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

  - *requestedRetransmissionTime is configured with the absolute time at which the SCEF expects the IN-CSE to retransmit the MT NIDD Downlink Data Transfer Request.*

If an error occurs while processing the NIDD Downlink Data Transfer Request, the SCEF will respond with an error code as defined in ETSI TS 129 122 [4]. See clause 8.3 for further details on the actions an IN-CSE shall take when receiving an error from the SCEF.

If the MT NIDD Downlink Data Transfer Request results in an error, the IN-CSE shall forward a corresponding oneM2M error to the Originator of the request. See clause 8.3 for a list of possible error scenarios.

Step 5: Process MT NIDD Downlink Data Transfer Request

If the UE targeted by the MT NIDD Downlink Data Transfer Request has an active NIDD PDN connection to the SCEF, the SCEF interacts with the 3GPP Core Network to process the request and deliver it to the targeted UE.

NOTE 2: If a MT NIDD Downlink Data Transfer Request is received with non-IP data for a request that is already buffered, then the buffered data is replaced by the SCEF. If a MT NIDD Downlink Data Transfer Request is received with no non-IP data for a request that is already buffered, then the buffered data is purged by the SCEF.

Step 6 (Optional): MT NIDD Downlink Data Delivery Status Notification

If the SCEF returned a 202 ACCEPTED response in Step 4 indicating that it buffered the NIDD Downlink Data Request to be performed later, then after completing the processing of the MT NIDD Downlink Data Transfer Request, the SCEF returns a MT NIDD Downlink Data Delivery Status Notification configured as follows:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the NIDD Configuration Request.
- The request payload includes a *NiddDownlinkDataDeliveryStatusNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *niddDownlinkDataTransfer* is configured with the URI of the corresponding MT NIDD Downlink Data Transfer resource.
  - *deliveryStatus* is set by the SCEF to indicate the delivery status NIDD Downlink Data Transfer request.
  - *requestedRetransmissionTime* is configured with the absolute time at which the SCEF expects the IN-CSE to retransmit the MT NIDD Downlink Data Transfer Request.

Step 7: MT NIDD Downlink Data Delivery Status Acknowledgement

After receiving a MT NIDD Downlink Data Delivery Status Notification, the IN-CSE responds with a 204 NO CONTENT acknowledging the notification.

Step 8: Process oneM2M Request Primitive

The ASN/MN-CSE or ADN-AE hosted on the UE targeted by the MT NIDD Downlink Data Transfer Request processes the oneM2M request primitive delivered within the MT NIDD Downlink Data Transfer Request. If the oneM2M request primitive requires a response, the ASN/MN-CSE or ADN-AE hosted on the UE prepares the oneM2M response primitive. Otherwise a response is not returned.

Step 9 (Optional): MO NIDD Uplink Data Notification

The UE acknowledges the RDS packet and the ASN/MN-CSE or ADN-AE generates a oneM2M response primitive and issues a MO NIDD Uplink Data Notification to deliver the response primitive back to the Originator. The MO NIDD Uplink Data Notification to deliver the oneM2M response primitive shall be addressed to the same port numbers that were received in step 5 and the request shall indicate that an RDS acknowledgement is desired.

Step 10 (Optional): MO NIDD Uplink Data Notification

When the SCEF receives the MO NIDD Uplink Data Notification, it finds the corresponding T8 Destination Address (URI) of the IN-CSE based on the NIDD Configuration that has been successfully performed. The SCEF then forwards the oneM2M primitive carried in the MO NIDD Uplink Data Notification to the IN-CSE configured as follows:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the NIDD Configuration Request.

- The request payload includes a *NiddUplinkDataNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *niddConfiguration* is configured with the URI of the NIDD Configuration resource to which this notification is related to.
  - *externalId* is set to the *M2M-Ext-ID* of the UE hosting the targeted ASN/MN-CSE or ADN-AE that originated the MO NIDD Uplink Data Notification.
  - *reliableDataService* shall be set to TRUE or FALSE to indicate whether the Reliable Data Service acknowledgement is enabled or not.
  - *rdsPort* indicates the source and destination ports that were provided in the MO NIDD Uplink Data Notification.
  - *data* is configured with a oneM2M response primitive sent by the UE hosting the Originator ASN/MN-CSE or ADN-AE.

Step 11 (Optional): MO NIDD Uplink Data Acknowledgement

After receiving a MT NIDD Uplink Data Delivery Notification, the IN-CSE responds with a 204 NO CONTENT acknowledging the notification.

Step 12 (Optional): MO NIDD Uplink Data Response

The SCEF sends an NIDD Uplink Data Response to the UE and processes the MO NIDD Uplink Data Acknowledgement from the IN-CSE.

Step 13 (Optional): Return oneM2M Response Primitive to Application

If an AE (e.g. IN-AE) was the Originator of the corresponding oneM2M request primitive, the IN-CSE shall return the oneM2M response primitive to the AE.

If an NIDD request results in an error, the IN-CSE shall forward a corresponding oneM2M error to the Originator of the oneM2M request primitive. See clause 8.3 for a list of possible error scenarios.

7.1.1.3 SCEF-based Mobile Originated NIDD

The SCEF API supports a Mobile Originated (MO) NIDD procedure that may be used by a UE hosting an ASN/MN-CSE or ADN-AE to send uplink non-IP data to an IN-CSE. Figure 7.1.1.3-1 illustrates this procedure.

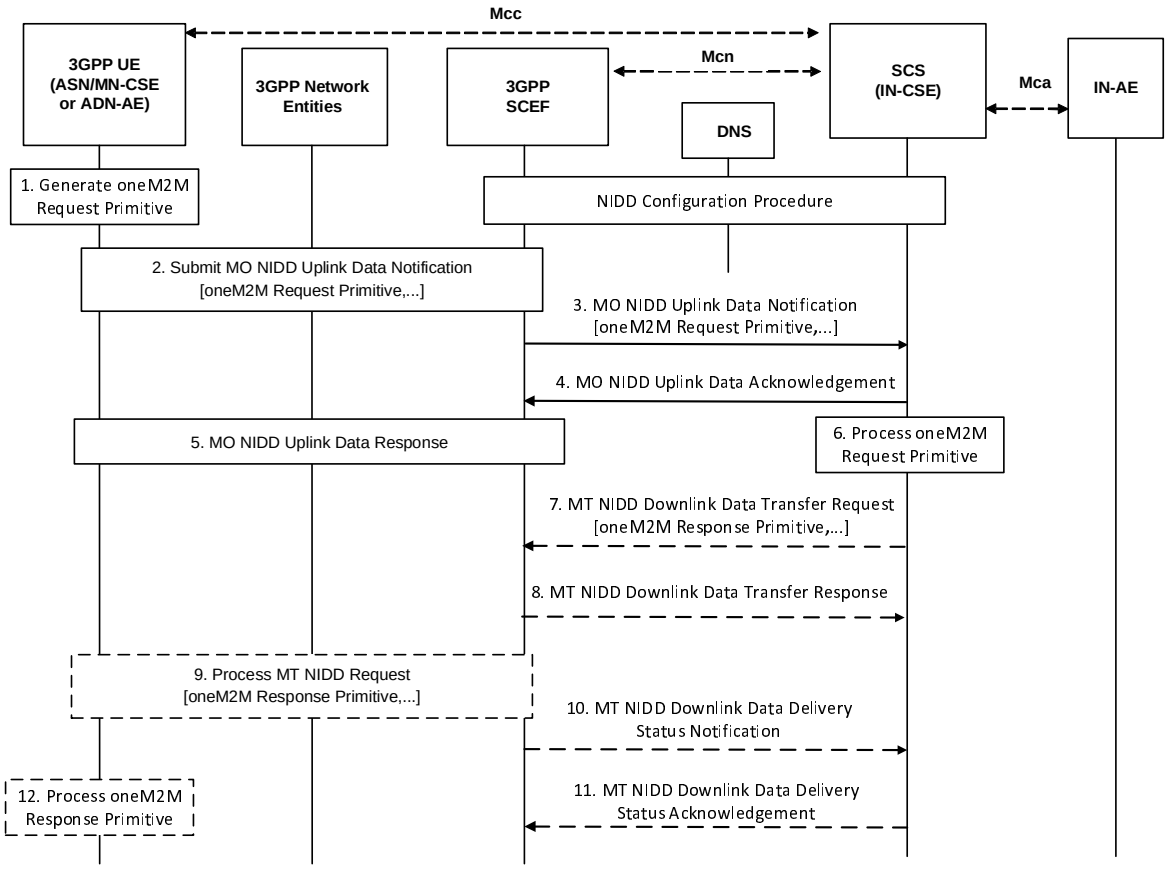

Figure 7.1.1.3-1: SCEF-based Mobile Originated NIDD

Pre-conditions:

The NIDD Configuration procedure defined in clause 7.1.1.1 completes successfully.

Step 1: oneM2M Request Primitive Generation

The ASN/MN-CSE or ADN-AE hosted on a UE generates a oneM2M request primitive targeting the IN-CSE.

Step 2: MO NIDD Uplink Data Notification

The ASN/MN-CSE or ADN-AE issues a MO NIDD Uplink Data Notification to deliver the primitive to the IN-CSE. When the request is sent, the UE shall indicate that an RDS acknowledgment is requested. The RDS source and destination port numbers shall be set to the same values that were provided to the SCEF by the IN-CSE during NIDD Configuration. The port numbers are pre-provisioned in the ASN/MN-CSE or ADN-AE.

Step 3: MO NIDD Uplink Data Notification

When the SCEF receives the MO NIDD Uplink Data Notification, it finds the corresponding T8 Destination Address of the IN-CSE based on the NIDD Configuration that has been successfully performed. The SCEF then forwards the oneM2M request primitive carried in the MO NIDD Uplink Data Notification to the IN-CSE configured as follows:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the NIDD Configuration Request.
- The request payload includes a *NiddUplinkDataNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *niddConfiguration* is configured with the URI of the NIDD Configuration resource to which this notification is related to.

- *externalId* is set to the *M2M-Ext-ID* of the UE hosting the targeted ASN/MN-CSE or ADN-AE that originated the MO NIDD Uplink Data Notification.
- *reliableDataService* is set to TRUE or FALSE by the SCEF to indicate that Reliable Data Service is enabled or not.
- *rdsPort* indicates the source and destination ports that were provided in the MO NIDD Uplink Data Notification.
- *data* is configured with a oneM2M request primitive sent by the UE hosting the Originator ASN/MN-CSE or ADN-AE.

Step 4: MO NIDD Uplink Data Acknowledgement

After receiving a MT NIDD Uplink Data Delivery Notification, the IN-CSE responds with a 204 NO CONTENT acknowledging the notification.

Step 5: MO NIDD Uplink Data Response

The SCEF sends an RDS acknowledgment to the UE and the SCEF processes the MO NIDD Uplink Data Acknowledgement from the IN-CSE.

Step 6: Process oneM2M Request Primitive

The IN-CSE processes the oneM2M request primitive that was delivered in the MO NIDD Uplink Data Notification. If the oneM2M request primitive requires a response, the IN-CSE shall prepare the oneM2M response primitive.

Step 7 (Optional): Return oneM2M Response Primitive

The IN-CSE may generate a oneM2M response primitive if a response is required. If a response is required, the IN-CSE shall issue a MT NIDD Downlink Data Transfer Request to deliver it to the ASN/MN-CSE or ADN-AE hosted on the UE that originated the corresponding oneM2M request primitive. The IN-CSE shall only issue a SCEF-based Mobile Terminated (MT) NIDD Downlink Data Transfer Request if the size of the oneM2M response primitive to be sent in the request is less than or equal to the NIDD Max Packet Size established during the corresponding the NIDD Configuration procedure for the UE.

The message is configured as follows:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{configurationId}* segment shall be configured with the {*configurationId*} returned by the SCEF when the NIDD Configuration was performed by the IN-CSE for this ASN/MN-CSE or ADN-AE.
- The request payload shall include a *NiddDownlinkDataTransfer* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *M2M-Ext-ID* of the UE hosting the targeted ASN/MN-CSE or ADN-AE.
  - *maximumLatency* may be set to indicate the maximum delay acceptable for MT data and used to configure the buffer duration in the underlying 3GPP network; a maximum latency of 0 indicates that buffering is not allowed. If maximum latency is not provided, the SCEF determines the acceptable delay based on local policies.
  - *priority* may be set to indicate the priority of the non-IP data packet relative to other non-IP data packets. If a priority is not provided, the SCEF determines the acceptable delay based on local policies.
  - *pdnEstablishmentOption* may be used to indicate the IN-CSE's default preference for how the SCEF should process a MT NIDD request from the IN-CSE if the UE has not yet established a Non-IP PDN connection to the SCEF. If a PDN Connection Establishment Option is not provided with the non-IP packet, the SCEF uses the PDN Connection Establishment Option that was provided during NIDD Configuration to decide how to handle the absence of a PDN connection.
  - *reliableDataService* (optional) shall be set to TRUE or FALSE to indicate that Reliable Data Service acknowledgement is required or not.

- *rdsPort* shall be set to the source and destination ports used for MO and MT NIDD between the IN-CSE and the ASN/MN-CSE or ADN-AE hosted on the UE.

- *data* shall be configured with a oneM2M response primitive to send to the UE hosting the targeted ASN/MN-CSE or ADN-AE.

Step 8 (Optional): MT NIDD Downlink Data Transfer Response

If the targeted UE does not have an active NIDD PDN connection to the SCEF, the SCEF may buffer the request until the UE establishes the connection. The SCEF may also trigger the UE to establish a NIDD PDN connection to the SCEF. Alternatively, the SCEF may generate an error.

The SCEF may return a MT NIDD Downlink Data Transfer Response to the IN-CSE to indicate if the request is buffered, a trigger has been generated, or an error has occurred. The fields of the response are populated as follows:

- A response code of 200 OK or 201 CREATED:

  - 200 OK is returned if the delivery of the NIDD Downlink Data Transfer was successful.

  - 201 CREATED is returned if the SCEF accepted and buffered the NIDD Downlink Data Request to be performed later.

- The *URI* of the NIDD Downlink Data Transfer resource created by the SCEF for the case when response code is 201 CREATED. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries/{downlinkDataDeliveryId}*. The *{apiRoot}*, *{scsAsId}* and *{configurationId}* segments match those in the request. The *{downlinkDataDeliveryId}* segment is configured by the SCEF.

- The response payload will include a *NiddDownlinkDataTransfer* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:

  - *deliveryStatus* is used to indicate a success or an appropriate error cause value as defined in ETSI TS 129 122 [4].

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

  - *requestedRetransmissionTime* is configured with the absolute time at which the SCEF expects the IN-CSE to retransmit the MT NIDD Downlink Data Transfer Request.

If the MT NIDD Downlink Data Transfer Request results in an error such that the IN-CSE is not able to return a oneM2M response primitive to the Originator of the request, the IN-CSE shall drop the response. See clause 8.3 for a list of possible error scenarios.

Step 9 (Optional): Process MT NIDD Downlink Data Transfer Request

If the UE targeted by the MT NIDD Downlink Data Transfer Request has an active NIDD PDN connection to the SCEF, the SCEF interacts with the 3GPP Core Network to process the request and deliver it to the targeted UE. The UE responds with an RDS acknowledgment.

NOTE: If an MT NIDD Downlink Data Transfer Request is received with non-IP data that is equal to a request that is already buffered, then the buffered data is replaced by the SCEF. If an MT NIDD Downlink Data Transfer Request is received with no non-IP data that is equal to a request that is already buffered, then the buffered data is purged by the SCEF.

Step 10 (Optional): MT NIDD Downlink Data Delivery Status Notification

After completing the processing of the MT NIDD Downlink Data Transfer Request, the SCEF returns a MT NIDD Downlink Data Delivery Status Notification configured as follows:

- An HTTP POST method is used.

- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the NIDD Configuration Request.

- The request payload includes a *NiddDownlinkDataDeliveryStatusNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *niddDownlinkDataTransfer* is configured with the URI of the corresponding MT NIDD Downlink Data Transfer resource.
  - *deliveryStatus* is set by the SCEF to one of the status codes defined in ETSI TS 129 122 [4] to indicate if the request was delivered successfully or not.
  - *requestedRetransmissionTime* is configured with the absolute time at which the UE will be reachable in the event that the UE is not reachable.

Step 11 (Optional): MT NIDD Downlink Data Delivery Status Acknowledgement

After receiving a MT NIDD Downlink Data Delivery Status Notification, the IN-CSE responds with a 204 NO CONTENT acknowledging the notification.

Step 12 (Optional): Process oneM2M Request Primitive

The ASN/MN-CSE or ADN-AE hosted on the UE targeted by the MT NIDD Request processes the oneM2M response primitive delivered within the MT NIDD Request.

7.2 UE context information storage

Not supported in oneM2M Release 4.

7.3 High latency communications

Not supported in oneM2M Release 4.

7.4 Monitoring events

7.4.1 UE Reachability monitoring

The 3GPP SCEF functionality described in ETSI TS 129 122 [4] supports APIs for monitoring specific events such as UE Reachability status. This allows an SCS to request to receive reports when a device becomes reachable for receiving either SMS or downlink data. In the 3GPP interworking architecture of oneM2M, the UE hosts an ADN with one or more AEs or an ASN/MN-CSE. The UE Monitoring flow in Figure 7.4.1-1 takes place after the UE has attached to the underlying 3GPP Network and the ADN-AE(s) or ASN/MN-CSE register with the IN-CSE.

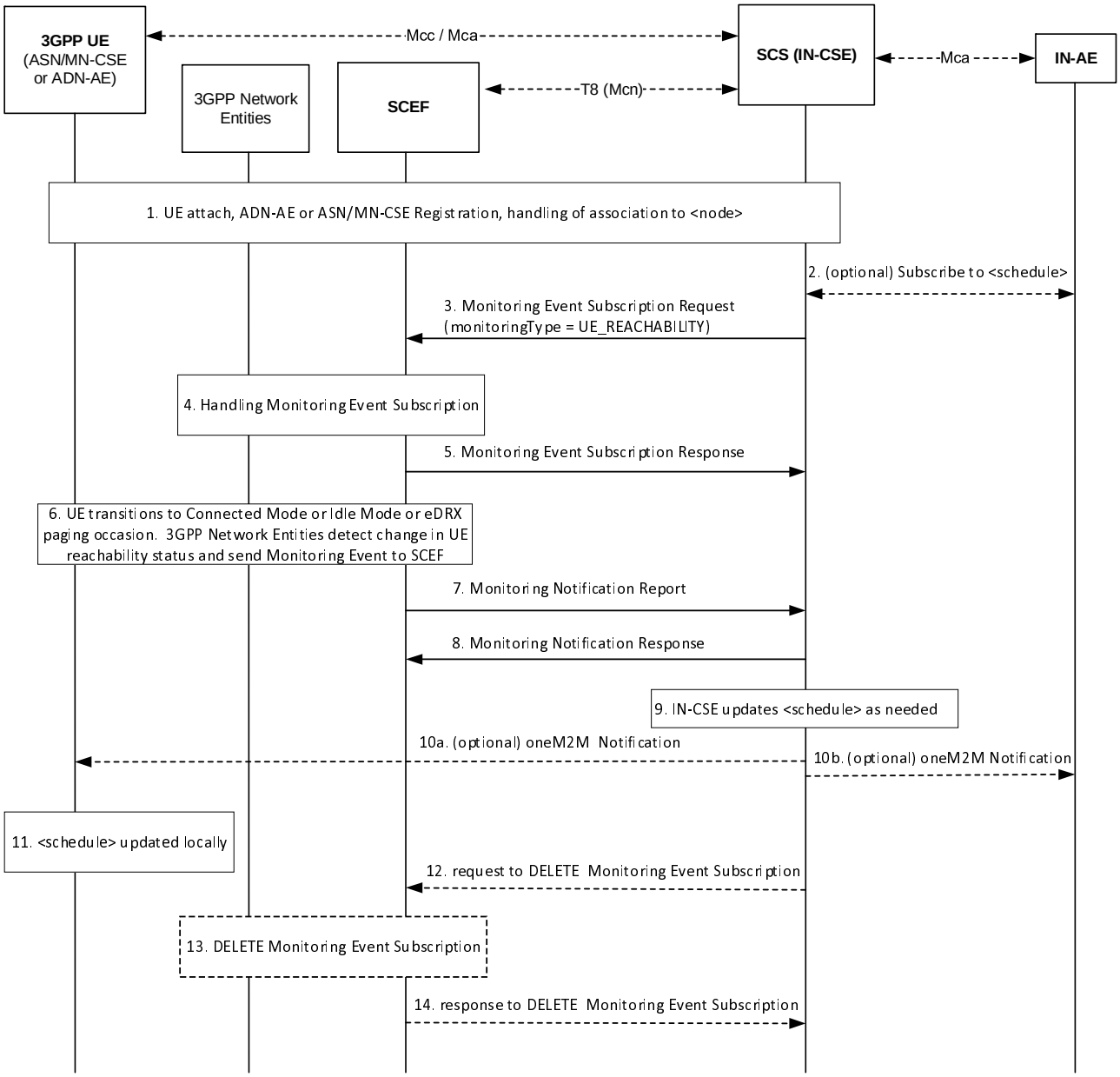

Figure 7.4.1-1: UE Reachability monitoring

Step 1: UE attaches to the underlying 3GPP network and registers to IN-CSE

The UE attaches to the underlying 3GPP network and the ADN-AE(s) or ASN/MN-CSE hosted on the UE perform the oneM2M registration procedure, as detailed in clause 6.3. The IN-CSE hosts the corresponding <*AE*> or <*remoteCSE*> resources for the registree and an associated <*node*> resource.

Step 2 (Optional): Subscribe to <schedule>

As described in clause 6.3, if at the time of ADN-AE(s) or ASN/MN-CSE registration to the IN-CSE a child <*schedule*> resource of the <*node*> resource representing the UE does not exist, the IN-CSE shall create it. If an IN-AE, ADN-AE(s) or ASN/MN-CSE is interested in receiving notifications when this <*schedule*> resource is updated by the IN-CSE, based on UE reachability notifications from the underlying 3GPP network, it may subscribe to this <*schedule*> resource.

Step 3: Request for Monitoring Event Subscription to monitor the UE reachability

The IN-CSE sends a Monitoring Event Subscription request to the SCEF to monitor the reachability of a UE. The creation of one or more subscriptions to the node <*schedule*> in step 2 may be used to trigger the monitoring request if the *networkCoordinated* attribute of the <*schedule*> resource is set to TRUE.

The Monitoring Event Subscription request from the IN-CSE to the SCEF shall comply with ETSI TS 129 122 [4]. The Monitoring Event Subscription request is configured as follows:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *MonitoringEventSubscription* (API for Monitoring Event Subscription) data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *M2M-Ext-ID* of the UE.
  - *notificationDestination* shall be set to a URI that the SCEF can target UE Reachability notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - *monitoringType* shall be set to UE_REACHABILITY.
  - *reachabilityType* shall be set to DATA.
  - *idleStatusIndication* shall be set to TRUE or FALSE. A setting of TRUE will result in the SCEF sending notifications to the IN-CSE when the UE transitions into PSM idle mode. These notifications will be in addition to any notifications sent to the IN-CSE when the UE transitions into connected mode or receives an eDRX paging occasion. A setting of FALSE (default) will result in the SCEF not sending notifications when the UE transitions into PSM idle mode. A setting of TRUE is only applicable for UEs supporting PSM. How the IN-CSE determines whether a UE supports PSM, eDRX or both is out of scope of the present document and may be configured based on Service Provider and MNO policies.
  - *supportedFeatures* shall be set to a string value of "2" indicating support for UE-Reachability notifications.
  - *maximumNumberOfReports* is optional and may be set to a maximum number of event reports to be generated by the 3GPP network entities e.g. HSS or MME/SSGN. If used, the IN-CSE shall configure this value based on Service Provider and MNO policies.
  - *monitorExpireTime* is optional and may be set to an absolute time at which the UE reachability monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *msisdn, ipv4Addr, ipv6Addr, externalGroupId, requestTestNotification, websockNotifConfig, groupReportGuardTime, maximumLatency, maximumResponseTime* and *suggestedNumberOfDlPackets* are not supported by the present document and shall not be included.

Step 4: Handling in the 3GPP Network Entities

The SCEF processes the Monitoring Event Subscription request together with the 3GPP network entities, as described in ETSI TS 129 122 [4].

Step 5: Response to Monitoring Event Subscription

If the Monitoring Event Subscription Request is successfully processed, the SCEF responds indicating the request was accepted. The message includes the following information:

- A response code of 201 CREATED.
- The *URI* of the Monitoring Event Subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.
- The response payload will include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a URI to the resource created by the SCEF for the request.
  - *monitoringEventReport* may be included if a monitoring event report is available.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 6: Detection of UE changing reachability mode and reporting to SCEF

Later, when the UE transitions to connected mode (for a UE using Power Saving Mode or extended idle mode DRX) or the UE becomes reachable for paging (for a UE using extended idle mode DRX) or the UE transitions to idle mode (for a UE using Power Saving Mode), the 3GPP network entities (e.g. HSS) detect the condition and send a Monitoring Event Report for UE reachability with Idle Status Information including Idle Status Timestamp, Periodic RAU/TAU timer, Active Time, eDRX Cycle Length) to the SCEF.

Step 7: SCEF sends Monitoring Notification to IN-CSE

When the SCEF receives information of status change in step 6, the SCEF creates and sends a Monitoring Notification message for UE reachability to the IN-CSE as specified in ETSI TS 129 122 [4].

Otherwise, the Monitoring Notification message is sent with appropriate information in accordance with the monitoringType.

The Monitoring Notification report for UE_REACHABILITY is configured as follows:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request.
- The request payload will include a *MonitoringNotification* (API for Monitoring Notification) data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.
  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.
  - *cancelInd* shall be ignored by the IN-CSE if present since it is not supported by the present document.
  - *monitoringEventReports* configured with one or more UE Reachability monitoring reports wherein each report includes the following fields as defined in ETSI TS 129 122 [4]:
    - *externalIDs* configured with the one or more *externalId* that shall be included the same value of *M2M-Ext-ID* of the UE at step 3.
    - *monitoringType* configured with UE_REACHABILITY.
    - *idleStatusInfo* configured with information such as *activeTime, edrxCycleLength, suggestedNumberOfDlPackets, idleStatusTimestamp, periodicAUTimer* as defined in ETSI TS 129 122 [4].
    - *reachabilityType* configured with a type of reachability as defined in ETSI TS 129 122 [4].

Step 8: UE Reachability Monitoring Notification Response

After receiving a UE Reachability Monitoring Notification, the IN-CSE responds with a 204 NO CONTENT acknowledging the notification.

Step 9: UE Reachability Monitoring Notification Handling at the IN-CSE

The IN-CSE uses the information provided in the UE Reachability Monitoring Event Report as follows:

- If *idleStatusInfo* information is provided in the report, the IN-CSE shall change the *scheduleElement* of the UE's node <*schedule*> resource such that the duration of the *scheduleElement* is set to the value of the *activeTime* parameter configured in the *idleStatusInfo*.

Step 10a and 10b: (Optional) Notifications are sent to the entities which subscribed to changes in the <*schedule*> resources. This may include notifications sent to the ADN-AE(s) or ASN/MN-CSE hosted on the UE, if they have subscriptions to their respective <*schedule*> resources.

Step 11: Notification of schedule update

Upon receiving notification of <*schedule*> resource updates, the ADN-AE(s) or ASN/MN-CSE hosted on the UE process the notification and should update their local <*schedule*> resources (if applicable) with the same values.

Step 12 (Optional): request to delete Monitoring Event Subscription

The IN-CSE sends a DELETE request targeting the URI of the subscription resource corresponding to this Monitoring Event Subscription. This step may be triggered by the IN-CSE when the <*node*> or <*schedule*> resources associated with a UE are deleted or when the *networkCoordinated* attribute of the <*schedule*> resource affiliated with a UE is set to FALSE.

The request is configured as follows:

- An HTTP DELETE method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}* which is identical to step 3. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the *MonitoringEventSubscription* was created.
- The request shall not contain a payload.

Steps 13 and 14 (Optional): Handling in 3GPP Network Entities and response to delete Monitoring Event Subscription

The SCEF processes the request to delete the Monitoring Event Subscription together with the 3GPP Network Entities.

The SCEF responds to the IN-CSE with a response either a code of 200 OK or 204 NO CONTENT indicating that it has successfully deleted the Monitoring Event Subscription.

7.4.2 UE Availability after DDN Failure

The 3GPP SCEF functionality described in ETSI TS 129 122 [4] supports APIs for monitoring of events such as UE Availability after a Downlink Data Notification (DDN) Failure. When communicating with UEs which sleep for a long time, if downlink packets are not delivered, the underlying 3GPP network recognizes that the UE is not available by a lack of a response within a reasonable time.

Per this feature, the IN-CSE can subscribe and be notified every time the UE becomes reachable after the network fails to deliver a downlink packet. For example, when this option is set and the IN-CSE receives no response to downlink traffic towards a UE, the IN-CSE can assume that the network failed to deliver the packet because the UE was sleeping and not because of Network Issues. The network later sends a notification to the IN-CSE when the UE becomes reachable.

In the underlying 3GPP network, this feature involves an entry in the UE subscription, so it is an ongoing event that needs explicit deletion to cancel further reports and it is different than the UE Reachability Monitoring Request. The feature is particularly suitable when there is just one IN-CSE.

The IN-CSE may also request Idle Status Indication. If Idle Status Indication is supported by the underlying 3GPP network, when the UE transitions into Idle mode, the report includes the time at which the UE transitioned into Idle mode, the active time and the periodic TAU/RAU time granted to the UE.

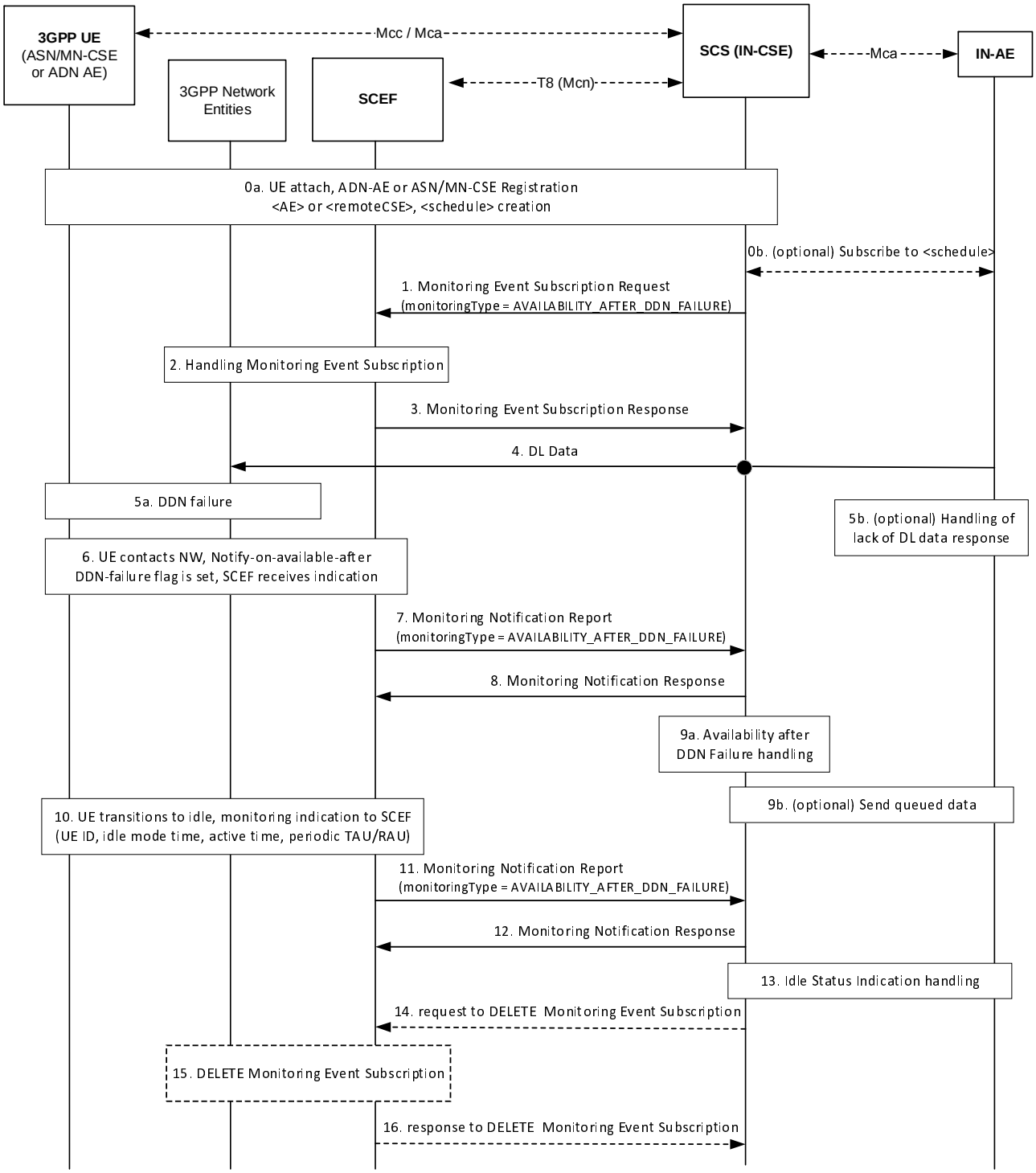

Figure 7.4.2-1: Availability after DDN Failure monitoring

Step 0: UE Attach and oneM2M Registration Procedures

The UE attaches to the underlying 3GPP network and the ADN-AE(s) or ASN/MN-CSE hosted on the UE perform the oneM2M registration procedure, as detailed in clause 6.3. The IN-CSE hosts the corresponding <*AE*> or <*remoteCSE*> resources and an associated <*node*> resource for the registrees. During this procedure, a <*schedule*> resource is created as a child of the <*node*> resource. The UE hosted ADN-AE(s) or ASN/MN may subscribe to the node <*schedule*> resource.

If an IN-AE is interested in the reachability status of the UE, it may subscribe to the <*schedule*> resource if the *networkCoordinated* attribute of <*schedule*> resource is set to TRUE (step 0b, optional).

Step 1: IN-CSE sends a Monitoring Event Subscription Request to SCEF to monitor the UE Availability after a DDN Failure

This step may be triggered by the IN-CSE based on implementation options, for example after a certain number of downlink data delivery failures have occurred. The creation of a <*schedule*> child resource of a <*node*> resource may also be used to trigger the monitoring request if the *networkCoordinated* attribute of the <*schedule*> resource is set to TRUE.

The Monitoring Event Subscription request from the IN-CSE to SCEF contains information as specified in ETSI TS 129 122 [4]. Such information includes:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *M2M-Ext-ID* of the UE.
  - *notificationDestination* shall be set to a URI that the SCEF can target DDN Failure notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - *monitoringType* shall be set to AVAILABILITY_AFTER_DDN_FAILURE.
  - *idleStatusIndication* shall be set to TRUE or FALSE. A setting of TRUE will result in the SCEF sending notifications to the IN-CSE when the UE transitions into PSM idle mode. These notifications will be in addition to any notifications sent to the IN-CSE when the UE transitions into connected mode or receives an eDRX paging occasion. A setting of FALSE (default) will result in the SCEF not sending notifications when the UE transitions into PSM idle mode. A setting of TRUE is only applicable for UEs supporting PSM. How the IN-CSE determines whether a UE supports PSM, eDRX or both is out of scope for the present document and may be configured based on Service Provider and MNO policies.
  - *supportedFeatures* shall be set to a string value of "7" indicating support for availability after DDN Failure notifications.
  - *maximumNumberOfReports* is optional and may be set to a maximum number of event reports to be generated by 3GPP network entities e.g. HSS or MME/SSGN. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *monitorExpireTime* is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - msisdn, ipv4Addr, ipv6Addr, externalGroupId, requestTestNotification, websockNotifConfig, groupReportGuardTime, maximumLatency and maximumResponseTime are not supported by the present document and shall not be included.

NOTE: It is recommended that Idle Status monitoring is enabled in conjunction with the Availability after DDN Failure monitoring. This enables the IN-CSE to update the <*schedule*> resource with updated timing information, once the UE transitions to idle again.

Steps 2 and 3: Monitoring Event Subscription Request Handling in the underlying 3GPP network

The SCEF handles the Monitoring Event Subscription Request together with the Mobile Core Network, as described in ETSI TS 123 682 [2]. The SCEF sends a Monitoring Event Subscription Response message to the IN-CSE to acknowledge acceptance of the Monitoring Event Subscription Request.

The message includes the following information:

- A response code of 201 CREATED.

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

- The response payload will include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:

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

  - *monitoringEventReport* may be included if a monitoring event report is available.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 4: DL Data is sent to the UE

Downlink data is sent to the UE which, in the underlying 3GPP network, involves sending a Downlink Data Notification (DDN) message to the MME, and MME initiates paging of UE.

Step 5a: DDN Failure

The underlying 3GPP network diagnoses a DDN Failure when, after DDN, no response to the UE paging is received and if the UE is in PSM mode (not every DDN failure triggers this event), the UE subscription is updated to reflect that a notification of availability should be sent after this DDN failure.

Step 5b: Request failure handling

The IN-CSE may also diagnose the failure when no response to the DL data has been received. It is up to implementation if the IN-CSE changes the node <*schedule*> resource at this point to indicate that communications are not available (e.g. by using a keyword such as "NULL"), or just records it as a one-time response failure. Other alternatives for implementation are, for example, for the IN-CSE to change the node <*schedule*> resource to indicate that communications are not available only after a pre-provisioned number of requests fail. The IN-CSE may also buffer future requests or enlarge its buffer size.

Step 6: Available after DDN Failure

At a later time, the UE contacts the network, e.g. to perform a TAU, or as it executes a service request. The underlying 3GPP network notes that the UE is available and that an availability notification is requested in the subscription. A Monitoring Indication that the UE is available is sent to the SCEF.

Step 7: SCEF sends a DDN Failure Monitoring Notification Request to IN-CSE

When the SCEF receives information of status change to available communication, the SCEF creates and sends a Monitoring Notification message for AVAILABILITY_AFTER_DDN_FAILURE to the IN-CSE as specified in ETSI TS 129 122 [4].

Otherwise, the Monitoring Notification message is sent with appropriate information in accordance with the *monitoringType*.

The SCEF sends a DDN Failure Monitoring Notification Report to the IN-CSE as specified in ETSI TS 129 122 [4], indicating that the UE is available, including:

- An HTTP POST method is used.

- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request.

- The request payload will include a *MonitoringNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:

  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.

  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.

- *cancelind* shall be ignored by the IN-CSE if present since it is not supported by the present document.
- *monitoringEventReports* configured with one or more DDN Failure monitoring reports wherein each report includes the following fields as defined in ETSI TS 129 122 [4]:
  - *externalIDs* configured with one or more externalID that will be configured with the same values of *M2M-Ext-ID* of the UE in step 1.
  - *monitoringType* configured with AVAILABILITY_AFTER_DDN_FAILURE.
  - *idleStatusInfo* configured with information such as *activeTime, edrxCycleLength, suggestedNumberOfDlPackets, idleStatusTimestamp, periodicAUTimer* as defined in ETSI TS 129 122 [4].

Step 8: DDN Failure Monitoring Notification Response

After receiving a DDN Failure Monitoring Notification, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Steps 9a and 9b: Availability after DDN Failure Handling at the IN-CSE

The IN-CSE uses the information provided in the Monitoring Notification Report to update the node <*schedule*> to indicate that the UE is available.

A new *scheduleElement* shall be created that indicates that the node is available for communication starting immediately and will remain available for at least the duration specified by the Maximum Response Time parameter.

Later (step 9b, optional) IN-AE(s) or the IN-CSE may decide to resend data queued for the UE.

Step 10: UE transitions to Idle

UE transitions to idle mode. If Idle Status Indication was requested during Monitoring Event configuration, and the MCN supports Idle Status Indication, then the SCEF is provided with an indication which includes the time at which the UE transitioned into idle mode, the active time and the periodic TAU/RAU timer values.

Step 11: SCEF sends a UE Reachability Monitoring Event Notification Request to IN-CSE

The SCEF provides a Monitoring Event Notification Request to the IN-CSE as specified in ETSI TS 129 122 [4], including:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request.
- The request payload will include a *MonitoringNotification* (API for Monitoring Notification) data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.
  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.
  - *cancelind* shall be ignored by the IN-CSE if present since it is not supported by the present document.
  - *monitoringEventReports* configured with one or more UE Reachability monitoring reports wherein each report includes the following fields as defined in ETSI TS 129 122 [4]:
    - *externalIDs* configured with one or more *externalIDs* that will be configured with the same values of *M2M-Ext-ID* of the UE as step 1.
    - *monitoringType* configured with UE_REACHABILITY.
    - *idleStatusInfo* configured with information such as *activeTime, edrxCycleLength, suggestedNumberOfDlPackets, idleStatusTimestamp, periodicAUTimer* as defined in ETSI TS 129 122 [4].

Step 12: Monitoring Event Notification Response

After receiving a Monitoring Event Notification, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Step 13: UE Idle mode indication Handling at the IN-CSE

The IN-CSE uses the UE Idle status information to update the <*schedule*> child resource of the <*node* > resource.

The IN-CSE changes the <*schedule*> resource such that:

- The start of the *scheduleElement* is based on the Idle Timestamp, with a periodicity equal to the TAU/RAU Timer.
- The duration of the *scheduleElement* indicates the Active Time value.

When any traffic is received from the node or an Availability Notification is received for the node, any *scheduleElement*(s) that were created based on prior Idle Status Indications shall be deleted for the node. A new *scheduleElement* shall be created that indicates that the node is available for downlink communication starting immediately and will remain available for at least the duration specified by the Maximum Response Time parameter.

Step 14 (Optional): IN-CSE sends request to SCEF to delete Monitoring Event Subscription

The IN-CSE sends a DELETE request targeting the URI of the subscription resource corresponding to this Monitoring Event Subscription. This step may be triggered by IN-CSE when the <node> or <schedule> resources associated with a UE are deleted or when the *networkCoordinated* attribute of the <*schedule*> resource affiliated with a UE is set to FALSE.

The request is configured as follows:

- An HTTP DELETE method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}* which is identical to step 1. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the *MonitoringEventSubscription* was created.
- The request shall not contain a payload.

Steps 15 and 16 (Optional): Monitoring Event Subscription Delete Request Handling in the underlying 3GPP network

The SCEF handles the request to delete Monitoring Event Subscription together with the 3GPP network entities. The SCEF returns a response to the IN-CSE with a response code of 204 NO CONTENT to acknowledge the Monitoring Event Subscription has been deleted.

7.4.3 UE Communication Failure

The 3GPP SCEF Event Monitoring functionality described in ETSI TS 129 122 [4] supports an API to allow an IN-CSE to be informed when the UE communication failure occurs. Informing the IN-CSE that UEs have suffered communication failures in the underlying 3GPP network helps optimize communications. For example, the IN-CSE may stop attempting to communicate with the UE if it is aware of repeated communication failures.

The UE Communication Failure Monitoring flow is assumed to take place after the UE has attached to the underlying 3GPP Network and registered with the IN-CSE.

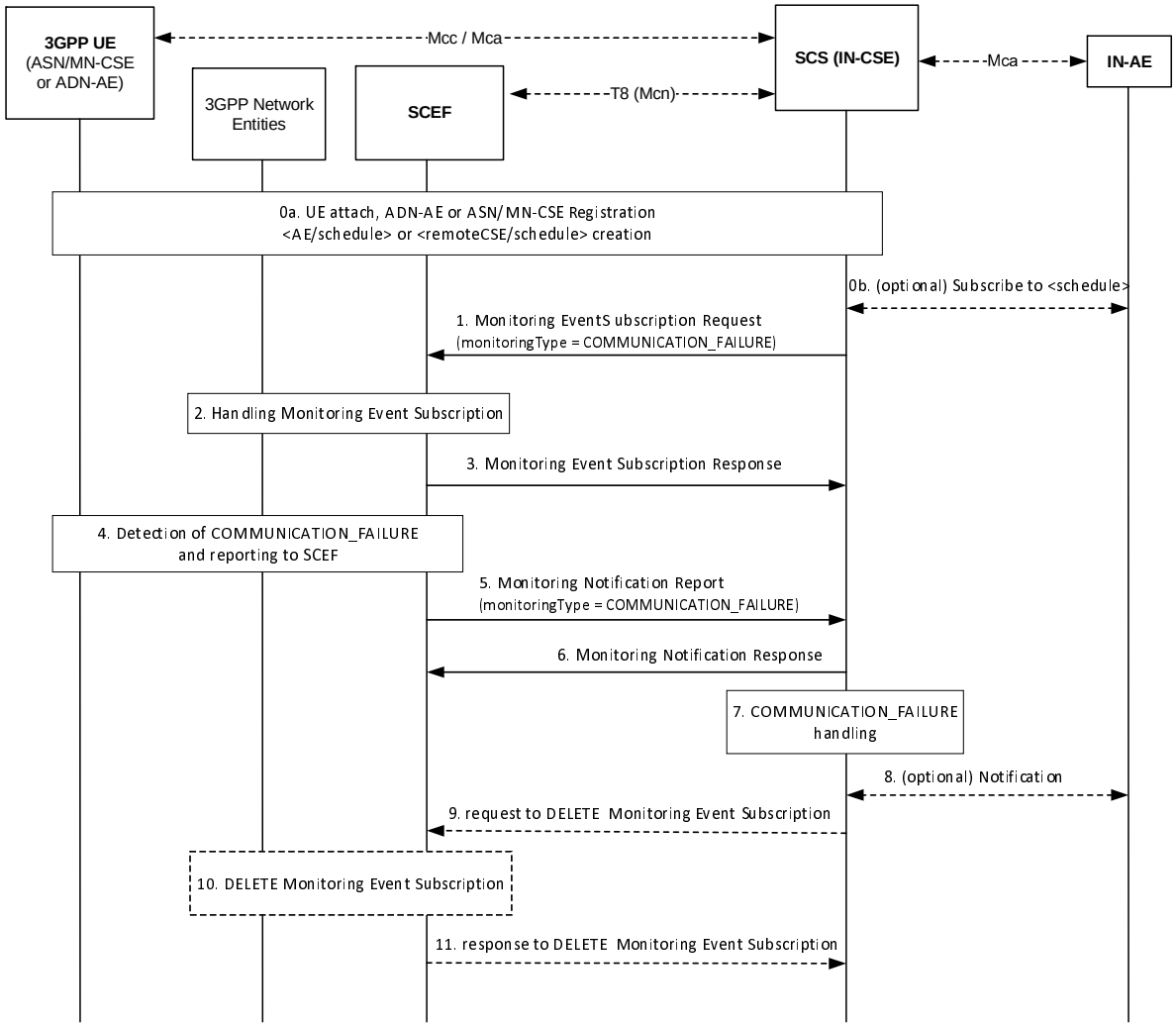

Figure 7.4.3-1: Communication Failure monitoring

Step 0: UE Attach and oneM2M Registration Procedures

The UE attaches to the underlying 3GPP network and the ADN-AE(s) or ASN/MN-CSE hosted on the UE perform the oneM2M registration procedure, as detailed in clause 6.3. The IN-CSE hosts the corresponding <*AE*> or <*remoteCSE*> resources and an associated <*node*> resource for the registree. During this procedure, a <*schedule*> resource is created as a child of the <*node*> resource. The UE hosted ADN-AE(s) or ASN/MN may subscribe to the node <*schedule*> resource.

If an IN-AE is interested in the communication failure status of the UE, it may subscribe to the node <schedule> resource (step 0b, optional).

Step 1: IN-CSE sends a Monitoring Event Subscription Request to SCEF to monitor the UE Communication Failure

This step may be triggered by an IN-CSE based on implementation options, for example when a type of communication requiring high reliability is scheduled to occur. The creation of a <*schedule*> child resource of a <node> resource may also be used to trigger the monitoring request if the *networkCoordinated* attribute of <*schedule*> resource is set to TRUE.

The Monitoring Event Subscription request from the IN-CSE to SCEF contains information as specified in ETSI TS 129 122 [4]. Such information includes:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.

- The request payload shall include a *MonitoringEventSubscription* (API for Monitoring Event Subscription) data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *M2M-Ext-ID* of the UE.
  - *notificationDestination* shall be set to a URI that the SCEF can target Communication Failure notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - *monitoringType* shall be set to COMMUNICATION_FAILURE.
  - *supportedFeatures* shall be set to a string value of "6" indicating support for Communication Failure notifications.
  - *maximumNumberOfReports* is optional and may be set to a maximum number of event reports to be generated by 3GPP network entities e.g. HSS or MME/SSGN. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *monitorExpireTime* is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *msisdn, ipv4Addr, ipv6Addr, externalGroupId, requestTestNotification, websockNotifConfig, groupReportGuardTime, maximumLatency* and *maximumResponseTime* are not supported by the present document and shall not be included.

NOTE: It is recommended that Idle Status monitoring is enabled in conjunction with the Availability after DDN Failure monitoring. This enables the IN-CSE to update the <*schedule*> resource with updated timing information, once the UE transitions to idle again.

Steps 2 and 3: Monitoring Event Subscription Request Handling in the underlying 3GPP Network

The SCEF handles the Monitoring Event Subscription Request together with the 3GPP network entities, as described in ETSI TS 129 122 [4]. The SCEF sends a Monitoring Event Subscription Response message to the IN-CSE to acknowledge acceptance of the Monitoring Event Subscription Request.

The message includes the following information:

- A response code of 201 CREATED.
- The *URI* of the Monitoring Event Subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.
- The response payload will include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a URI to the resource created by the SCEF for the request.
  - *monitoringEventReport* may be included if a monitoring event report is available.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 4: Detection of Communication Failure and reporting to SCEF

Later, when the UE communication failure occurs the condition is detected in the underlying 3GPP network and the SCEF receives a Monitoring Event Report.

Step 5: SCEF sends UE Communication Failure Monitoring Event Notification Request to IN-CSE

When the SCEF receives information of status change of the UE, the SCEF sends a Monitoring Notification Report to the IN-CSE for UE communication failure information as specified in ETSI TS 129 122 [4].

Otherwise, the Monitoring Notification message is sent with appropriate information in accordance with the *monitoringType*.

The Monitoring Notification report for COMMUNICATION_FAILURE includes:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request.
- The request payload will include a *MonitoringNotification* (API for Monitoring Notification) data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.
  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.
  - *cancelind* shall be ignored by the IN-CSE if present since it is not supported by the present document.
  - *monitoringEventReports* configured with one or more Communication Failure monitoring reports wherein each report includes the following fields as defined in ETSI TS 129 122 [4]:
    - *externalID* configured with one or more *externalID* that will be configured with the same value of *M2M-Ext-ID* of the UE as step 1.
    - *monitoringType* configured with COMMUNICATION_FAILURE.
    - *failureCause* configured with a reason of communication failure such as *bssgpCause*, *causeType*, *gmmCause*, *ranapCause*, *ranNasCause*, *s1ApCause* and *smCause*.

Step 6: UE Communication Failure Monitoring Event Notification Response

After receiving a UE Communication Failure Monitoring Notification for communication failure, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Step 7: Communication Failure Handling at the IN-CSE

The IN-CSE uses the information provided in the Monitoring Notification Report to update the *scheduleElement* of the <*schedule*> resource to indicate that no communications are currently available (e.g. by using a keyword such as "NULL"). Local IN-CSE policies may specify events/ thresholds further defining when the IN-CSE may provide the <*schedule*> resource update. For example, the update may be provided only after repeated communication failures are received within a timespan, or only if high reliability communications are expected. It is recommended that UE Reachability monitoring is also enabled in conjunction with the Communication Failure monitoring. This enables the IN-CSE to provide updated timing information in the <*schedule*> resource, once the UE becomes reachable again.

Step 8 (Optional): Notifying subscribers

Optionally, notifications may be sent to the subscribers of the <*schedule*> resource.

Step 9 (Optional): IN-CSE sends request to SCEF to delete Monitoring Event Subscription

The IN-CSE sends a DELETE request targeting the URI of the subscription resource corresponding to this Monitoring Event Subscription. This step may be triggered by IN-CSE when an ADN-AE(s) or ASN/MN-CSE hosted on the UE de-registers from the IN-CSE or when the *networkCoordinated* attribute of the <*schedule*> resource affiliated with an ADN-AE or ASN/MN-CSE hosted on a UE is set to FALSE.

The request is configured as follows:

- An HTTP DELETE method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}* which is identical to step 1. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the *MonitoringEventSubscription* was created.
- The request shall not contain a payload.

Steps 10 and 11 (Optional): Monitoring Event Subscription Delete Request Handling in the underlying 3GPP network

The SCEF handles request to delete the Monitoring Event Subscription together with the 3GPP network entities. The SCEF responds to the IN-CSE with a response code of 204 NO CONTENT to acknowledge the Monitoring Event Subscription has been deleted.

7.4.4 UE Loss of Connectivity

An IN-CSE can communicate with large numbers of devices, many of which are reachable for short periods of time. An IN-CSE may want to be informed when devices are not reachable to the underlying 3GPP network, to better manage its communications. For example, IN-AEs which normally communicate with the device might not attempt communications if neither signalling or user plane communication are available.

The 3GPP SCEF functionality described in ETSI TS 129 122 [4] supports APIs for monitoring specific events such as UE Loss of Connectivity Monitoring. The Loss of Connectivity Monitoring Event subscription allows the IN-CSE to provide to the network a Maximum Detection Time, which indicates the maximum period of time without any communication between the UE and Network after which the IN-CSE is to be informed that the device is considered to be unreachable.

The Maximum Detection Time of loss of connectivity is on the order of 1 minute to multiple hours. A timer with the order of magnitude of a few minutes can only apply to a limited number of devices due to the network signalling cost.

NOTE 1: In the underlying 3GPP Network, the Maximum Detection Time of loss of connectivity can be used to determine the order of magnitude of the Periodic Update timer.

The UE Loss of Connectivity Monitoring flow is assumed to take place after the UE has attached to the underlying 3GPP Network and registered with the IN-CSE.

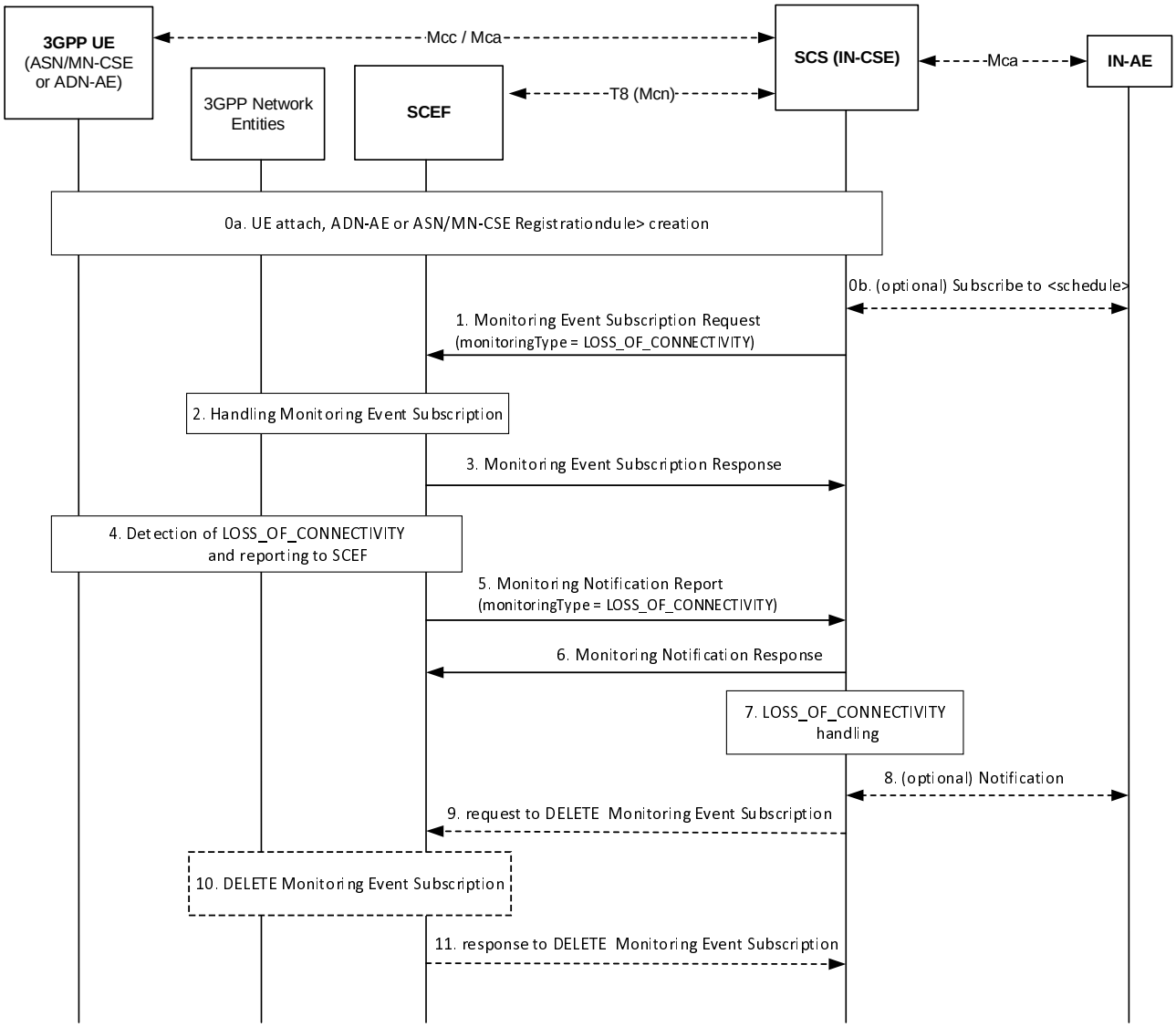

Figure 7.4.4-1: Loss of Connectivity monitoring

Step 0: UE Attach and oneM2M Registration Procedures

The UE attaches to the underlying 3GPP network and the ADN-AE(s) or ASN/MN-CSE hosted on the UE perform the oneM2M registration procedures, as detailed in clause 6.3. The IN-CSE hosts the corresponding <*AE*> or <*remoteCSE*> resources for the registree, and an associated <*node*> resource. During this procedure, a <*schedule*> resource is created as a child of the <*node*> resource and the *networkCoordinated* attribute of the <*schedule*> resource is set to TRUE.

If an IN-AE is interested in the reachability status of the UE, it may subscribe to the <*schedule*> resource (step 0b, optional).

Step 1: IN-CSE sends a Monitoring Request to SCEF to monitor the UE Loss of Connectivity

This step may be triggered by the IN-CSE on creation of a <*schedule*> child resource of a <node> resource if the *networkCoordinated* attribute of the <*schedule*> resource is set to TRUE.

The Monitoring Event Subscription request from the IN-CSE to SCEF contains information as specified in ETSI TS 129 122 [4]. Such information includes:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.

- The request payload shall include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *M2M-Ext-ID* of the UE.
  - *notificationDestination* shall be set to a URI that the SCEF can target Loss of Connectivity notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - *monitoringType* shall be set to LOSS_OF_CONNECTIVITY.
  - *supportedFeatures* shall be set to a string value of "1" indicating support for Loss of Connectivity notifications.
  - *maximumNumberOfReports* is optional and may be set to a maximum number of event reports to be generated by 3GPP network entities e.g. HSS or MME/SSGN. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *monitorExpireTime* is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *msisdn, ipv4Addr, ipv6Addr, externalGroupId, requestTestNotification, websockNotifConfig, groupReportGuardTime, maximumLatency, maximumResponseTime* and *suggestedNumberOfDlPackets* are not supported by the present document and shall not be included.
  - *maximumDetectionTime* shall be set per IN-CSE pre-provisioning. This value should be set to a value that is longer than the length of time of inactive communications as configured in the <*schedule*> resource.
  - *msisdn, ipv4Addr, ipv6Addr, externalGroupId, requestTestNotification, websockNotifConfig, groupReportGuardTime, maximumLatency and maximumResponseTime* are not supported by the present document and shall not be included.

Steps 2 and 3: Monitoring Request Handling in the underlying 3GPP network

The SCEF handles the Monitoring Event Subscription Request together with the 3GPP network entities, as described in ETSI TS 129 122 [4]. The SCEF sends a Monitoring Event Subscription Response message to the IN-CSE to acknowledge acceptance of the Monitoring Event Subscription Request.

The message includes the following information:

- A response code of 201 CREATED.
- The *URI* of the Monitoring Event Subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.
- The response payload will include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a URI to the resource created by the SCEF for the request.
  - *monitoringEventReport* may be included if a monitoring event report is available.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 4: Detection of Loss of Connectivity and reporting to SCEF

Later, when the UE loses connectivity, the 3GPP network entities (e.g. MME) detect the condition and sends a Monitoring Event Report to SCEF.

Step 5: SCEF sends UE Loss of Connectivity Monitoring Notification Request to IN-CSE

The SCEF sends a Monitoring Event Notification Request to the IN-CSE when receiving the Monitoring Report that contains information as specified in ETSI TS 129 122 [4]. Such information includes:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request.
- The request payload will include a *MonitoringNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.
  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.
  - *cancelind* shall be ignored by the IN-CSE if present since it is not supported by the present document.
  - *monitoringEventReports* configured with one or more Loss of Connectivity monitoring reports wherein each report includes the following fields as defined in ETSI TS 129 122 [4]:
    - *externalIDs* configured with one or more *externalID* that will be configured with the same value of *M2M-Ext-ID* of the UE as step 1.
    - *monitoringType* configured with LOSS_OF_CONNECTIVITY.
    - *lossOfConnectReason* configured with the reason for loss of connectivity as defined in ETSI TS 129 122 [4].

Step 6: UE Loss of Connectivity Monitoring Event Notification Response

After receiving a UE Loss of Connectivity Monitoring Notification, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Step 7: Loss of Connectivity Handling at the IN-CSE

The IN-CSE uses the information provided in the Monitoring Notification Report to update the <*schedule*> child resource of the <*node*> resource to indicate that no communications are currently available (e.g. by using a keyword such as "NULL"). Updates to the <*schedule*> resource will be performed only if its *networkCoordinated* attribute is set to TRUE.

NOTE 2: It is recommended that UE Reachability monitoring is also enabled in conjunction with the Loss of Connectivity monitoring. This enables the IN-CSE to provide updated timing information in the <*schedule*> resource, once the UE becomes reachable again.

Step 8 (Optional): Notifying subscribers

Optionally, if IN-AEs have subscribed to changes in the <*schedule*> resources a notification will be sent to the subscribers.

Step 9 (Optional): IN-CSE sends request to SCEF to delete Monitoring Event Subscription

The IN-CSE sends a DELETE request targeting the URI of the subscription resource corresponding to this Monitoring Event Subscription. This step may be triggered by IN-CSE when an ADN-AE(s) or ASN/MN-CSE hosted on the UE de-registers from the IN-CSE or when the *networkCoordinated* attribute of the <*schedule*> resource affiliated with an ADN-AE or ASN/MN-CSE hosted on a UE is set to FALSE.

The request is configured as follows:

- An HTTP DELETE method shall be used.

- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}* which is identical to step 1. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the *MonitoringEventSubscription* was created.

- The request shall not contain a payload.

Steps 10 and 11 (Optional): Monitoring Event Subscription Delete Request Handling in the underlying 3GPP network

The SCEF handles the request to delete Monitoring Event Subscription together with the 3GPP network entities. The SCEF responds to the IN-CSE with a response code of 204 NO CONTENT to acknowledge the Monitoring Event Subscription has been deleted.

7.4.5 Detecting Change of IMSI-IMEI(SV) Association

The 3GPP SCEF Event Monitoring functionality described in ETSI TS 129 122 [4] supports an API that allows the IN-CSE to be informed when the SIM card of one physical device is placed in another physical device. This condition is detected by the underlying 3GPP network when the association between the International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI/IMEISV) changes.

An IN-CSE may request to receive notifications from an underlying 3GPP network when the association between the IMSI and IMEI(SV) changes for a given UE that hosts one or more ASN/MN-CSEs or ADN-AEs registered to the IN-CSE. Based on this notification, the IN-CSE may then ignore incoming requests from these ASN/MN-CSEs or ADN-AEs.

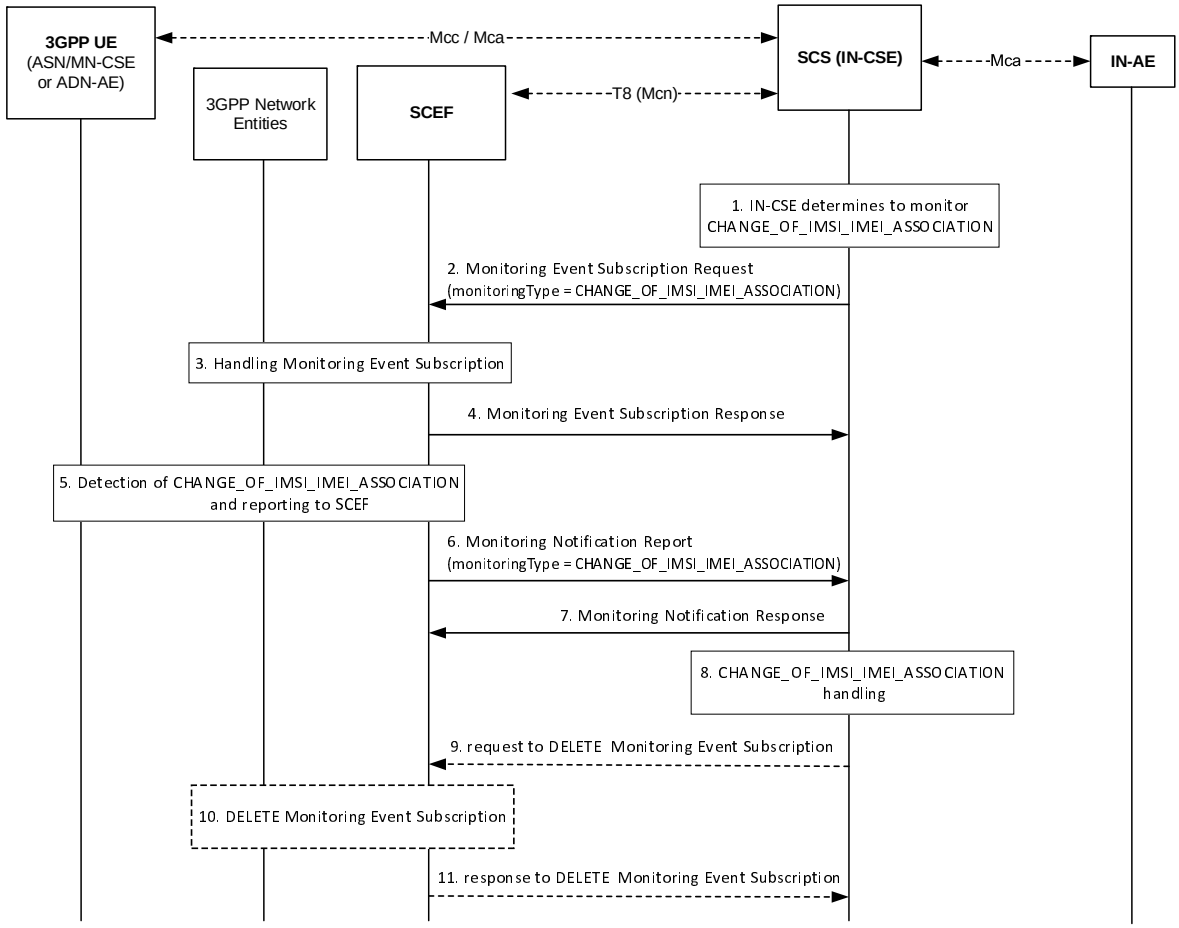

Figure 7.4.5-1: Change of IMSI-IMEI(SV) Association Monitoring Request and Notification

Pre-conditions:

There is a relationship in place between the IN-CSE and MNO allowing the IN-CSE to request notifications for IMSI-IMEI(SV) association changes.

An ASN/MN-CSE or ADN-AE registers with the IN-CSE and configures the *M2M-Ext-ID* attribute of its <*remoteCSE*> or <*AE*> resource. The IN-CSE examines the *M2M-Ext-ID* and recognizes that it is associated with an MNO that it has a relationship with. The relationship allows the IN-CSE to request notifications when the device's IMSI-IMEI(SV) association changes.

Step 1: IN-CSE requests notification for changes in IMSI-IMEI(SV) association

The IN-CSE determines whether it wants a notification if the IMSI-IMEI(SV) association of a particular UE hosting one or more ASN/MN-CSEs or ADN-AEs changes. This determination may be based on whether the IN-CSE has an established relationship with the MNO that supports this capability and provisioned policies.

Step 2: Monitoring Event Subscription Request

The IN-CSE sends a request to be notified when the device's IMSI-IMEI(SV) association changes. The Monitoring Event Subscription Request contains information as specified in ETSI TS 129 122 [4] which includes the following:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *M2M-Ext-ID* of the UE.
  - *notificationDestination* shall be set to a URI that the SCEF can target Change of IMSI/IMEI Association notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - *monitoringType* shall be set to CHANGE_OF_IMSI_IMEI_ASSOCIATION.
  - *supportedFeatures* shall be set to a string value of "4" indicating support for Change of IMSI/IMEI Association notifications.
  - *maximumNumberOfReports* is optional and may be set to a maximum number of event reports to be generated by 3GPP network entities e.g. HSS or MME/SSGN. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *monitorExpireTime* is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *associationType* shall be set to IMEI or IMEISV. The type that is used is based on IN-CSE policies which may be based on the relationship between the Service Provider and MNO.
  - *msisdn, ipv4Addr, ipv6Addr, externalGroupId, requestTestNotification, websockNotifConfig, groupReportGuardTime, maximumLatency, maximumDetectionTime* and *maximumResponseTime* are not supported by the present document and shall not be included.

Step 3: Process Monitoring Event Subscription Request

The SCEF processes the Monitoring Event Subscription request together with 3GPP network entities.

Step 4: Monitoring Event Subscription Response

The SCEF sends a Monitoring Event Subscription Response message to the IN-CSE to acknowledge acceptance of the Monitoring Event Subscription Request.

The message includes the following information:

- A response code of 201 CREATED.

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

- The response payload will include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:

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

  - *monitoringEventReport* may be included if a monitoring event report is available.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 5: Detect change in IMSI-IMEI(SV) association

The 3GPP network entities monitor and detect an IMSI-IMEI(SV) association change and reports Monitoring Event Report to SCEF.

Step 6: Monitoring Notification report

When the SCEF receives information of status change on IMSI-IMEI(SV) association, the SCEF sends a Monitoring Notification to the corresponding *notificationDestination* of the IN-CSE that was configured in the Monitoring Event Subscription Request and that contains information as specified in ETSI TS 129 122 [4].

Otherwise, the MonitoringNotification message is sent with appropriate information in accordance with the monitoringType.

The Monitoring Notification report for CHANGE_OF_IMSI_IMEI_ASSOCIATION includes:

- An HTTP POST method is used.

- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request at step 2.

- The request payload will include a *MonitoringNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:

  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.

  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.

  - *cancelind* shall be ignored by the IN-CSE if present since it is not supported by the present document.

  - *monitoringEventReports* configured with one or more Loss of Connectivity monitoring reports wherein each report includes the following fields as defined in ETSI TS 129 122 [4]:

    - *externalIDs* configured with one or more *externalID* that will be configured with the same value of *M2M-Ext-ID* of the UE as step 2.

    - *monitoringType* configured with CHANGE_OF_IMSI_IMEI_ASSOCIATION.

    - *associationType* configured with IMSI-IMEI or IMSI-IMEISV.

Step 7: Monitoring Notification Response

After receiving a Change of IMSI-IMEI Association Monitoring Event Notification, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Step 8: Process Notification

The IN-CSE shall stop servicing requests from any ASN/MN-CSEs or ADN-AEs having an *M2M-Ext-ID* matching the one indicated in the report. To block these requests, the IN-CSE may tear down any active security associations (e.g. D/TLS sessions) between the IN-CSE and these ADN-AEs or ASN/MN-CSEs. In addition, the IN-CSE may also deny new security association establishment requests from any ADN-AEs or ASN/MN-CSEs that have an *M2M-Ext-ID* matching the one indicated in the report until the restriction is removed via administrative means which are outside the scope of the present document.

Step 9 (Optional): IN-CSE sends request to SCEF to delete Monitoring Event Subscription

The IN-CSE sends a DELETE request targeting the URI of the subscription resource corresponding to this Monitoring Event Subscription. This step may be triggered by IN-CSE when an ADN-AE(s) or ASN/MN-CSE hosted on the UE de-registers from the IN-CSE.

The request is configured as follows:

- An HTTP DELETE method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}* which is identical to step 2. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the *MonitoringEventSubscription* was created.
- The request shall not contain a payload.

Steps 10 and 11 (Optional): Monitoring Event Subscription Delete Request Handling in the underlying 3GPP network

The SCEF handles the request to delete Monitoring Event Subscription together with the 3GPP network entities. The SCEF responds to the IN-CSE with a response code of 204 NO CONTENT to acknowledge the Monitoring Event Subscription has been deleted.

7.4.6 Roaming Status

The 3GPP SCEF Monitoring functionality described in ETSI TS 129 122 [4] supports an API to allow an IN-CSE to be informed when the roaming status of a UE in the underlying 3GPP network changes.

An IN-CSE may request to receive indications from an underlying 3GPP network when the roaming status of a 3GPP UE hosting an ASN/MN-CSE or ADN-AE changes. Based on these indications, the IN-CSE may buffer requests for ASN/MN-CSEs or ADN-AEs that are hosted on roaming UEs and send these requests when they are no longer roaming. The determination of whether to buffer requests may be based on system policies that are outside the scope of the present document. An IN-CSE may also make the roaming status of ASN/MN-CSEs or ADN-AEs available to IN-AEs such that they can use this status to determine whether to avoid and or delay communications until they are no longer roaming.

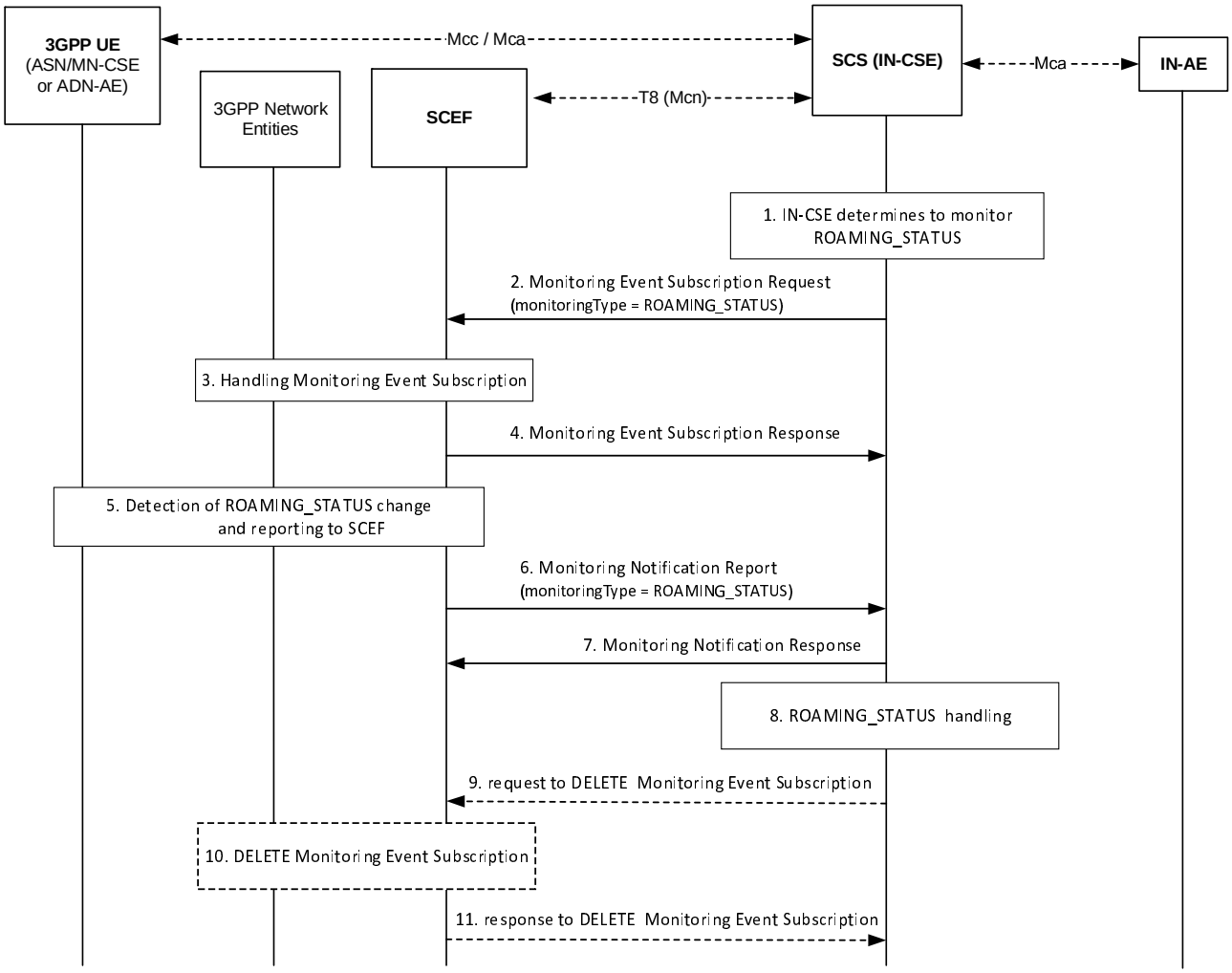

Figure 7.4.6-1: Request for Roaming Status Indications

Pre-conditions:

There is a relationship in place between the IN-CSE and MNO allowing the IN-CSE to request Roaming Status Reports from the underlying 3GPP network. The method for establishing this relationship is outside the scope of the present document.

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

The ASN/MN-CSE or ADN-AE or IN-CSE creates a <*node*> resource. This <*node*> resource has *roamingStatus* and *networkID* attributes.

An IN-AE may subscribe to the IN-CSE to receive notifications when the roaming status of a ASN/MN-CSE or ADN-AE changes. This subscription is made to the *roamingStatus* and/or *networkID* attributes of the <*node*> resource.

The IN-CSE may be configured with policies to control whether to buffer requests targeting ASN/MN-CSEs or ADN-AEs hosted on 3GPP UEs that are roaming. The method for configuring these policies is outside the scope of the present document.

Step 1: IN-CSE determines to monitor Roaming Status Request

If the IN-CSE can resolve the *M2M-Ext-ID* to a SCEF and IN-CSE policies allow for it, the IN-CSE issues a Roaming Status Request.

NOTE: These IN-CSE policies are outside the scope of the present document.

Step 2: Request Monitoring Event Subscription to monitor Roaming Status

The IN-CSE requests to monitor roaming status reports using Monitoring Event Subscription which has specified in ETSI TS 129 122 [4] for a particular ASN/MN-CSE or ADN-AE hosted on a UE. The fields of the *MonitoringEventSubscription* API are populated as follows:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *M2M-Ext-ID* of the UE.
  - *notificationDestination* shall be set to a URI that the SCEF can target Roaming Status notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - *monitoringType* shall be set to ROAMING_STATUS.
  - *supportedFeatures* shall be set to a string value of "5" indicating support for Roaming Status notifications.
  - *maximumNumberOfReports* is optional and may be set to a maximum number of event reports to be generated by 3GPP network entities e.g. HSS or MME/SSGN. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *monitorExpireTime* is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *pLMNIndication* shall be set to TRUE or FALSE to indicate whether the IN-CSE wants to know the identity of the PLMN that the UE is attached to.
  - *msisdn, ipv4Addr, ipv6Addr, externalGroupId, requestTestNotification, websockNotifConfig, groupReportGuardTime, maximumLatency, maximumDetectionTime* and *maximumResponseTime* are not supported by the present document and shall not be included.

Step 3: Process Monitoring Event Subscription to monitor Roaming Status

The SCEF processes the Monitoring Event Subscription request together with 3GPP network entities as described in ETSI TS 129 122 [4].

Step 4: Response for Monitoring Event Subscription to monitor Roaming Status

The SCEF sends a Monitoring Event Subscription Response message to the IN-CSE to acknowledge acceptance of the Monitoring Event Subscription Request.

The message includes the following information:

- A response code of 201 CREATED.
- The *URI* of the Monitoring Event Subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.
- The response payload will include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a URI to the resource created by the SCEF for the request.
  - *monitoringEventReport* may be included if a monitoring event report is available.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 5: Detect Roaming Status Change in 3GPP network entities

When the 3GPP network entities detect the change of UE roaming status, the 3GPP network entities report Monitoring Event Report to the SCEF.

Step 6: Monitoring Notification for Roaming Status from SCEF to IN-CSE

When the SCEF receives information of roaming status, the SCEF sends a Monitoring Notification to the corresponding *notificationDestination* of the IN-CSE that was configured in the Monitoring Event Subscription Request and that contains information as specified in ETSI TS 129 122 [4].

Otherwise, the MonitoringNotification message is sent with appropriate information in accordance with the monitoringType.

The Monitoring Notification report for roaming status includes:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request.
- The request payload will include a *MonitoringNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.
  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.
  - *cancelind* shall be ignored by the IN-CSE if present since it is not supported by the present document.
  - *monitoringEventReports* configured with one or more change of Roaming Status monitoring reports wherein each report includes the following fields as defined in ETSI TS 129 122 [4]:
    - *externalIDs* configured with one or more *externalID* that will be configured with the same values of the *M2M-Ext-ID* of the UE as step 2.
    - *monitoringType* configured with ROAMING_STATUS.
    - *plmnId* if *pLMNIIndication* in the Monitoring Event Subscription was set to TRUE, this parameter is included and indicate the UE's serving PLMN.
    - *roamingStatus* is configured with ROAMING or NOT_ROAMING.

Step 7: Response for Monitoring Notification from IN-CSE to SCEF

After receiving a Monitoring Notification on roaming status, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Step 8: Process Monitoring Notification at IN-CSE

The IN-CSE shall update the *roamingStatus* and *networkID* attributes of the <*node*> resource that is linked to <*AE*> or <*remoteCSE*> resources having a *M2M-Ext-ID* attribute that matches the *M2M-Ext-ID* configured in the Roaming Status Request.

In addition, the IN-CSE may determine to delay or reject the processing of requests targeting ASN/MN-CSEs or ADN-AEs hosted on roaming UEs via one or more of the following approaches. How the IN-CSE makes this determination is outside the scope of the present document and may be based on policies and agreements with the MNO:

- An IN-CSE may reject requests that target ASN/MN-CSEs or ADN-AEs hosted on roaming UEs. If an IN-CSE rejects a request due to a roaming UE, it shall return a corresponding response code informing the cause of rejection is due to lack of accessibility to a roaming network node.

- An IN-CSE may delay the processing of requests (i.e. buffer) that target ASN/MN-CSEs or ADN-AEs hosted on roaming UEs:
  - If the request is a blocking request, the IN-CSE should not delay the processing of the request and should instead reject the request with a corresponding response code informing the cause of rejection is due to the destination node is roaming.
  - If the request includes an Event Category that is set to immediate the IN-CSE should not delay the processing of the request and should instead reject the request with a corresponding response code informing the cause of rejection is due to the destination node is roaming. In this case, the IN-AE may decide to resubmit the request with the Event Category set to "bestEffort" or "latest" to indicate the IN-CSE may buffer the request.

Step 9 (Optional): Request to delete Monitoring Event Subscription on Roaming Status

The IN-CSE sends a DELETE request targeting the URI of the subscription resource corresponding to this Monitoring Event Subscription. This step may be triggered by IN-CSE when an ADN-AE(s) or ASN/MN-CSE hosted on the UE de-registers from the IN-CSE.

The request is configured as follows:

- An HTTP DELETE method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the *MonitoringEventSubscription* was created.
- The request shall not contain a payload.

Steps 10 and 11 (Optional): Process Roaming Status Cancellation Request

The SCEF handles the request to delete Monitoring Event Subscription together with the 3GPP network entities. The SCEF responds to the IN-CSE with a response code of 204 NO CONTENT to acknowledge the Monitoring Event Subscription has been deleted.

7.4.7 Location Reporting

7.4.7.1 Introduction

The 3GPP SCEF Event Monitoring functionality described in ETSI TS 129 122 [4] supports an API to allow an IN-CSE to be informed when the 3GPP network entities detect the current location of a UE as well as the last known location of UE. This clause provides details on how the IN-CSE's oneM2M <*locationPolicy*>, <*container*> and <*contentInstance*> resources are used to interwork with the T8 API and provide location monitoring capability for an ASN/MN-CSE or ADN-AE hosted on a 3GPP UE. To interwork the 3GPP location reporting functionality with oneM2M, the <*locationPolicy*>, <*container*> and <*contentInstance*> resources and corresponding procedures are used.

7.4.7.2 Location updating triggered by retrieval

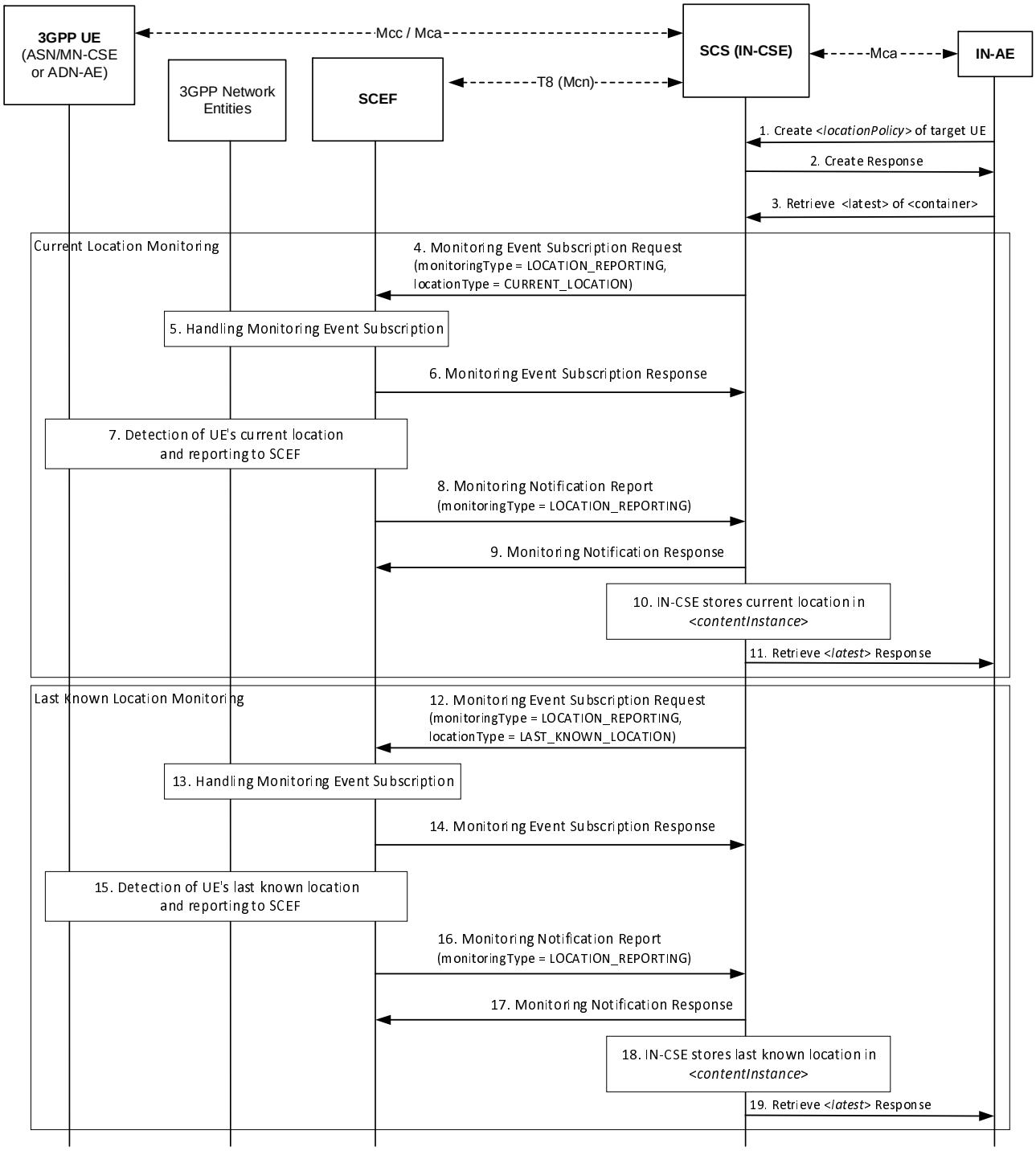

Figure 7.4.7.2-1: Location updating triggered by retrieving

Step 1: Request for creation of <*locationPolicy*>

The IN-AE sends a < *locationPolicy*> create request which shall include following parameters as specified in clause 9.6.10 of ETSI TS 118 101 [1]:

- *locationSource* shall be set to Network Based.
- *locationUpdatePeriod* shall not be present or set to 0.
- *locationTargetID* shall be set to the *M2M-Ext-ID* of the targeted UE hosting an ASN/MN-CSE or ADN-AE.

- *locationServer* shall not be present.
- *locationContainerID* shall not be present.
- *locationInformationType* shall be set to position fix.
- *retrieveLastKnownLocation* shall be configured with either TRUE or FALSE based on the requirements of the IN-AE.
- *locationUpdateEventCriteria* shall not be present.

Step 2: Responds to creation <*locationPolicy*>

IN-CSE shall create the <*locationPolicy*> resource and corresponding <*container*> resource for storing location information based on the procedure specified in clause 10.2.9 of ETSI TS 118 101 [1].

Step 3: Retrieve Request for <*latest*>

The IN-AE sends a RETRIEVE request to the <*latest*> child resource of the <*container*> resource linked to the to <*locationPolicy*> created in Step 2.

Step 4: Request Monitoring Event Subscription to get Current Location

The IN-CSE checks the *locationSource* attribute of the <*locationPolicy*> resource that is linked to the <*container*> targeted by the RETRIEVE request in Step 3. If the *locationSource* attribute is set to Network Based and the *locationUpdatePeriod* attribute is set to zero or NULL, then the IN-CSE shall request a Monitoring Event Subscription to get current location to the SCEF. The Monitoring Event Subscription request shall contain the following information as specified in ETSI TS 129 122 [4]:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - externalId shall be set to the locationTargetID.
  - notificationDestination shall be set to a URI that the SCEF can target Location Reporting notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - monitoringType shall be set to LOCATION_REPORTING.
  - supportedFeatures shall be set to a string value of "3" indicating support for Location Reporting notifications.
  - maximumNumberOfReports is optional and may be set to a maximum number of event reports to be generated by 3GPP network entities e.g. HSS or MME/SSGN. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - monitorExpireTime is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - locationType shall be set to CURRENT_LOCATION.
  - accuracy shall be set by the IN-CSE (e.g. CGI_ECGI, ENODEB, TA_RA, PLMN or TWAN_ID).
  - msisdn, ipv4Addr, ipv6Addr, externalGroupId, requestTestNotification, websockNotifConfig, groupReportGuardTime, maximumLatency, maximumDetectionTime and maximumResponseTime are not supported by the present document and shall not be included.

Steps 5: Process Monitoring Event Subscription to get Current Location

The SCEF handles request for Monitoring Event Subscription together with 3GPP network entities based on the procedure defined in ETSI TS 129 122 [4].

Step 6: Response to Monitoring Event Subscription for Current Location

The SCEF sends a Monitoring Event Subscription Response message to the IN-CSE to acknowledge acceptance of the Monitoring Event Subscription Request.

The message includes the following information:

- A response code of 201 CREATED.
- The *URI* of the Monitoring Event Subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}* which is identical to step 4. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.
- The response payload will include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a URI to the resource created by the SCEF for the request.
  - *monitoringEventReport* may be included if a monitoring event report is available.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 7: Detect Current Location of UE

The 3GPP network entities detect the current location of UE and the SCEF receives a Monitoring Event Report for the location of UE.

Step 8: SCEF sends Monitoring Notification Report to IN-CSE

When the SCEF receives a current location information from the 3GPP network entities, the SCEF sends Monitoring Notification Report to the IN-CSE that contains information as specified in ETSI TS 129 122 [4]. Otherwise, the MonitoringNotification message is sent with appropriate information in accordance with the *monitoringType*.

The Monitoring Notification report for LOCATION_REPORTING for current location shall include:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request.
- The request payload will include a *MonitoringNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.
  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.
  - *cancelind* shall be ignored by the IN-CSE if present since it is not supported by the present document.
  - *monitoringEventReports* configured Location Reporting monitoring report(s) wherein a report includes the following fields as defined in ETSI TS 129 122 [4]:
    - *externalID* configured with the same value of *M2M-Ext-ID* of the UE as step 4.
    - *monitoringType* configured with LOCATION_REPORTING.
    - *locationInfo* configured with the UE's current location information (e.g. *ageOfLocationInfo*, *cellId*, *enodeBId*, *routingAreaId*, *trackingAreaId*, *plmmId* and *twanId*).

Step 9: Response to Monitoring Notification for Current Location

After receiving a Monitoring Notification for current location, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Steps 10 and 11: Current Location Event Notification Handling at the IN-CSE

The IN-CSE shall create a new <*contentInstance*> child resource of the <*container*> targeted by the RETRIEVE request in Step 3. The IN-CSE shall store the UE's current location in this <*contentInstance*> and send the retrieve response for <*latest*> which is contains the current location to the IN-AE. The response shall include the newly created <*contentInstance*>.

Step 12: Request for 2nd attempt Monitoring Event Subscription to get Last Known Location

If the Monitor Indication in Step 6 indicates a failure, then the IN-CSE shall send a Monitoring Event Subscription to the SCEF to get the last known location if the *retrieveLastKnownLocation* attribute of the <*locationPolicy*> is set to TRUE. The Monitoring Event Subscription request shall contain the following information as specified in ETSI TS 129 122 [4]:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/* which is identical to step 4. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to the *locationTargetID* which shall be identical to step 4.
  - notificationDestination shall be set to a URI that the SCEF can target Location Reporting notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - *monitoringType* shall be set to LOCATION_REPORTING.
  - *supportedFeatures* shall be set to a string value of "3" indicating support for Location Reporting notifications.
  - *maximumNumberOfReports* is optional and may be set to a maximum number of event reports to be generated by 3GPP network entities e.g. HSS or MME/SSGN. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *monitorExpireTime* is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *locationType* shall be set to LAST_KNOWN_LOCATION.
  - *accuracy* shall be set by the IN-CSE (e.g. *CGI_ECGI*, *ENODEB*, *TA_RA*, *PLMN* or *TWAN_ID*).
  - *msisdn*, *ipv4Addr*, *ipv6Addr*, *externalGroupId*, *requestTestNotification*, *websockNotifConfig*, *groupReportGuardTime*, *maximumLatency*, *maximumDetectionTime* and *maximumResponseTime* are not supported by the present document and shall not be included.

Step 13: Process Monitoring Event Subscription to get Last Known Location

The SCEF handles Monitoring Event Subscription Request together with 3GPP network entities based on the procedure defined in ETSI TS 129 122 [4].

Step 14: Response to Monitoring Event Subscription for Last Known Location

The SCEF responds a Monitoring Event Subscription to get Last Known Location information to the IN-CSE to acknowledge acceptance of the Monitoring Event Subscription Request.

The message includes the following information:

- A response code of 201 CREATED.

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

- The response payload will include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:

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

  - *monitoringEventReport* may be included if a monitoring event report is available.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 15: Detect Last Known Location of UE

The 3GPP network entities detect the last known location of UE and SCEF receives Monitoring Event Report for the last known location of UE.

Step 16: SCEF sends Monitoring Notification for Last Known Location to IN-CSE

When the SCEF receives a last known location information from the 3GPP network entities, the SCEF sends Monitoring Notification Report to the IN-CSE that contains information as specified in ETSI TS 129 122 [4]. Otherwise, the Monitoring Notification message is sent with appropriate information in accordance with the *monitoringType*.

The Monitoring Notification report for LOCATION_REPORTING for last known location shall include:

- An HTTP POST method is used.

- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request.

- The request payload will include a *MonitoringNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:

  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.

  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.

  - *cancelind* shall be ignored by the IN-CSE if present since it is not supported by the present document.

  - *monitoringEventReports* configured Location Reporting monitoring report(s) wherein a report includes the following fields as defined in ETSI TS 129 122 [4]:

    - *externalID* configured with the same value of *M2M-Ext-ID* of the UE as step 12.

    - *monitoringType* configured with LOCATION_REPORTING.

    - *locationInfo* configured with the UE's last known location information (e.g. *ageOfLocationInfo*, *cellId*, *enodeBId*, *routingAreaId*, *trackingAreaId*, *plmmId* and *twanId*).

Step 17: Response to Monitoring Notification

After receiving a Monitoring Notification for last known location, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Steps 18 and 19: Current Location Reporting Event Handling at the IN-CSE

The IN-CSE shall create a new <*contentInstance*> child resource of the <*container*> initiated by the RETRIEVE request in Step 3. The IN-CSE shall store the UE's last known location in this <*contentInstance*> and send the retrieve response to IN-AE for <*latest*> which is contains the last known location. The response shall include the newly created <*contentInstance*>.

7.4.7.3 Location updating triggered by location change

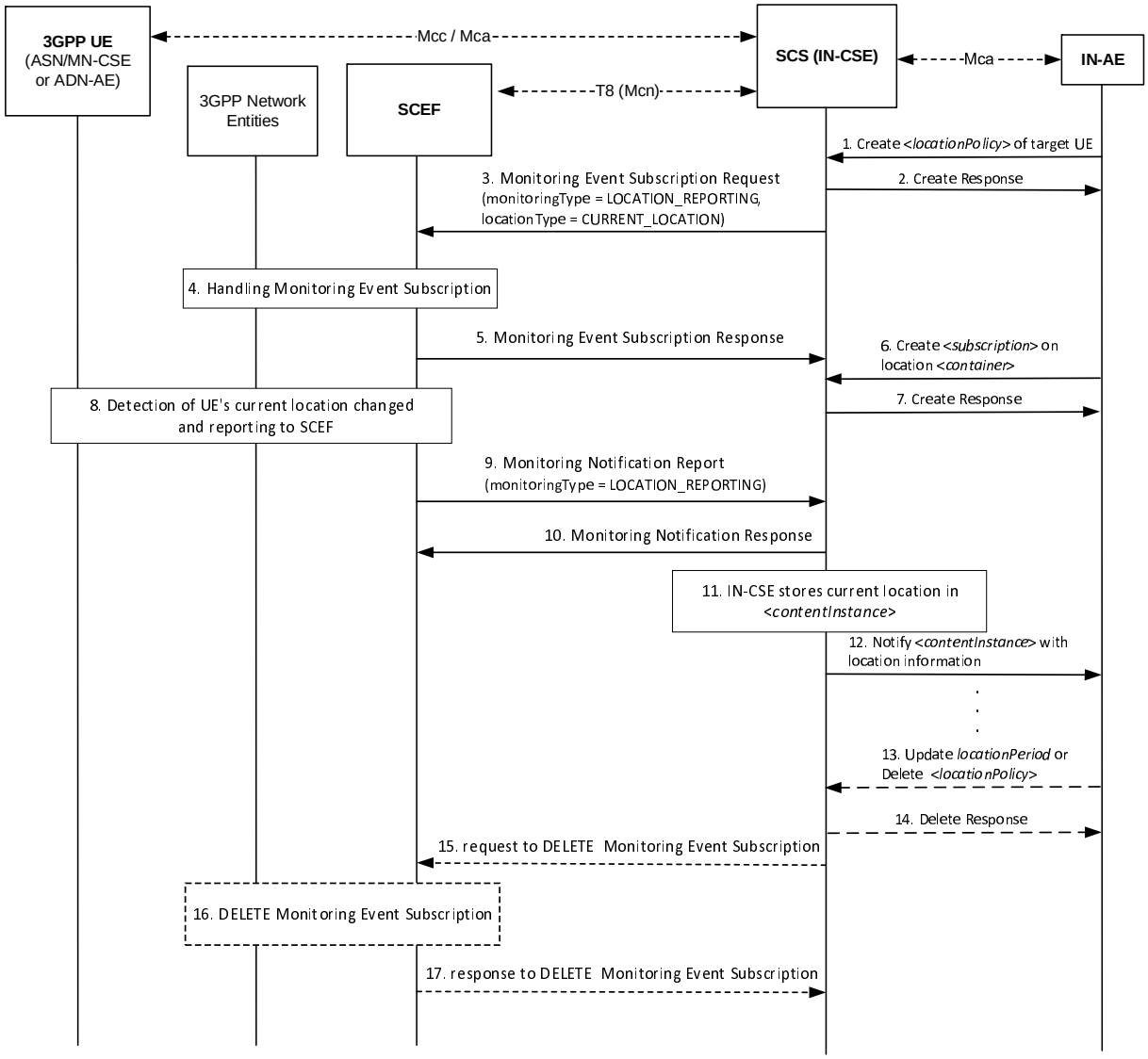

Figure 7.4.7.3-1: Location updating triggered by location change

Step 1: Request for creation of <*locationPolicy*>

The IN-AE sends <*locationPolicy*> CREATE request which shall be included following parameters as specified in clause 9.6.10 of ETSI TS 118 101 [1]:

- *locationSource* shall be set to Network Based.
- *locationUpdatePeriod* shall not be present or set to 0.
- *locationTargetID* shall be set to the *M2M-Ext-ID* of the targeted UE hosting an ASN/MN-CSE or ADN-AE.
- *locationServer* shall not be present.
- *locationContainerID* shall not be present.
- *locationInformationType* shall be set to position fix.
- *retrieveLastKnownLocation* shall not be configured.
- *locationUpdateEventCriteria* shall be set to LocationChange.

Step 2: Responds to creation <*locationPolicy*>

IN-CSE shall create the <*locationPolicy*> resource and corresponding <*container*> resource for storing location information and return a response based on the procedure specified in clause 10.2.9 of ETSI TS 118 101 [1].

Step 3: Request Monitoring Event Subscription to get Current Location

The IN-CSE sends Monitoring Event Subscription to SCEF. The request contains information as specified in ETSI TS 129 122 [4]. Such information includes:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - externalId shall be set to the locationTargetID.
  - notificationDestination shall be set to a URI that the SCEF can target Location Reporting notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - monitoringType shall be set to LOCATION_REPORTING.
  - supportedFeatures shall be set to a string value of "5" indicating support for Location Reporting notifications.
  - maximumNumberOfReports is optional and may be set to a maximum number of event reports to be generated by 3GPP network entities e.g. HSS or MME/SSGN. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - monitorExpireTime is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - locationType shall be set to CURRENT_LOCATION.
  - accuracy shall be set by the IN-CSE (e.g. CGI_ECGI, ENODEB, TA_RA, PLMN or TWAN_ID).
  - msisdn, ipv4Addr, ipv6Addr, externalGroupId, requestTestNotification, websockNotifConfig, groupReportGuardTime, maximumLatency, maximumDetectionTime and maximumResponseTime are not supported by the present document and shall not be included.

Step 4: Process Monitoring Event Subscription to get Current Location

The SCEF handles request for Monitoring Event Subscription together with 3GPP network entities based on the procedure defined in ETSI TS 129 122 [4].

Step 5: Response to Monitoring Event Subscription for Current Location

The SCEF sends a Monitoring Event Subscription Response message to the IN-CSE to acknowledge acceptance of the Monitoring Event Subscription Request.

The message includes the following information:

- A response code of 201 CREATED.
- The *URI* of the Monitoring Event Subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.

- The response payload will include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a URI to the resource created by the SCEF for the request.
  - *monitoringEventReport* may be included if a monitoring event report is available.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 6: Request for Creation of <*subscription*>

The IN-AE sends the <*subscription*> CREATE request of <*container*> which stores location information to the IN-CSE.

Step 7: Response for Creation of <*Subscription*>

The IN-CSE sends the response to the IN-AE.

Step 8: Detect Current Location change of UE

The 3GPP network entities send a Monitoring Event Report for the current Indication to SCEF when detecting a change in location of the UE hosting an ASN/MN-CSE or ADN-AE.

Step 9: Report Monitoring Notification for Current Location from SCEF to IN-CSE

The SCEF sends a Monitoring Notification Report to the IN-CSE that contains information as specified in ETSI TS 129 122 [4].

Otherwise, the Monitoring Notification message is sent with appropriate information in accordance with the *monitoringType*.

The Monitoring Notification report for LOCATION_REPORTING for current location shall include:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Monitoring Event Subscription Request.
- The request payload will include a *MonitoringNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.
  - *configResults* is used for group-based monitoring and shall be ignored by the IN-CSE if present since group-based monitoring is not supported by the present document.
  - *cancelind* shall be ignored by the IN-CSE if present since it is not supported by the present document.
  - *monitoringEventReports* configured Location Reporting monitoring report(s) wherein a report includes the following fields as defined in ETSI TS 129 122 [4]:
    - *externalID* configured with the same value of *M2M-Ext-ID* of the UE as step 3.
    - *monitoringType* configured with LOCATION_REPORTING.
    - *locationInfo* configured with the UE's current location information (e.g. *ageOfLocationInfo*, *cellId*, *enodeBId*, *routingAreaId*, *trackingAreaId*, *plmmId* and *twanId*).

Step 10: Response to Monitoring Notification for Current Location

After receiving a Location Reporting Monitoring Notification, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Step 11: Handling Monitoring Notification for Current Location at the IN-CSE

The IN-CSE shall create a new <*contentInstance*> child resource of the <*container*> resource created in Step 2. The IN-CSE shall store the UE's current location in this <*contentInstance*> resource.

Step 12: Notify <*contentInstance*>

IN-CSE sends a NOTIFY request to the IN-AE. The NOTIFY includes the <*contentInstance*> with the UE's current location.

Step 13 (Optional): The IN-AE sends a request to update the *locationUpdatePeriod* to 0 or <*locationPolicy*> is deleted.

Step 14 (Optional): The IN-CSE sends a response to the IN-AE.

Step 15 (Optional): IN-CSE requests to SCEF to delete Monitoring Event Subscription

The IN-CSE sends a DELETE request targeting the URI of the subscription resource corresponding to this Monitoring Event Subscription. This step may be triggered by IN-CSE when an ADN-AE(s) or ASN/MN-CSE hosted on the UE de-registers from the IN-CSE.

The request is configured as follows:

- An HTTP DELETE method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}* which is identical to step 3. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the *MonitoringEventSubscription* was created.
- The request shall not contain a payload.

Steps 16 and 17 (Optional): Monitoring Event Subscription Delete Request Handling in the Underlying 3GPP network

The SCEF handles request to delete the Monitoring Event Subscription together with the 3GPP network entities. The SCEF responds to the IN-CSE with a response code of 204 NO CONTENT to acknowledge the Monitoring Event Subscription has been deleted.

7.4.8 Number of UEs in an Area

The 3GPP SCEF functionality described in ETSI TS 129 122 [4] supports an API to allow an IN-CSE to ask for the number of UEs that are in the geographic area described by the IN-CSE. Based on the reports, MNOs may be able to predict the general congestion status of each area based on the number of UEs.

A particular group of ASN/MN-CSEs and/or ADN-AEs hosted on UEs in an area may be identified in the underlying 3GPP network by an External Group Identifier available at the IN-CSE. The IN-CSE sends a Monitoring Event Request with the External Group Identifier and a geographic area to the corresponding SCEF. When the IN-CSE receives a Monitoring Event Response from the SCEF, the IN-CSE receives the number of group member UEs found at the area. Note that and the External Identifier(s) of the registree ASN/MN-CSEs/ADN-AEs may or may not be provided in the response, depending on MNO configuration of MME/SGSN. Based on this information, the IN-CSE can take necessary measures such as adjusting other monitoring procedures for the group. The IN-CSE may also take other actions, such as modifying the <*schedule*> resource of the group members. Upon detecting an updated *scheduleElement*, the group members will modify when they send requests and make themselves available to receive requests.

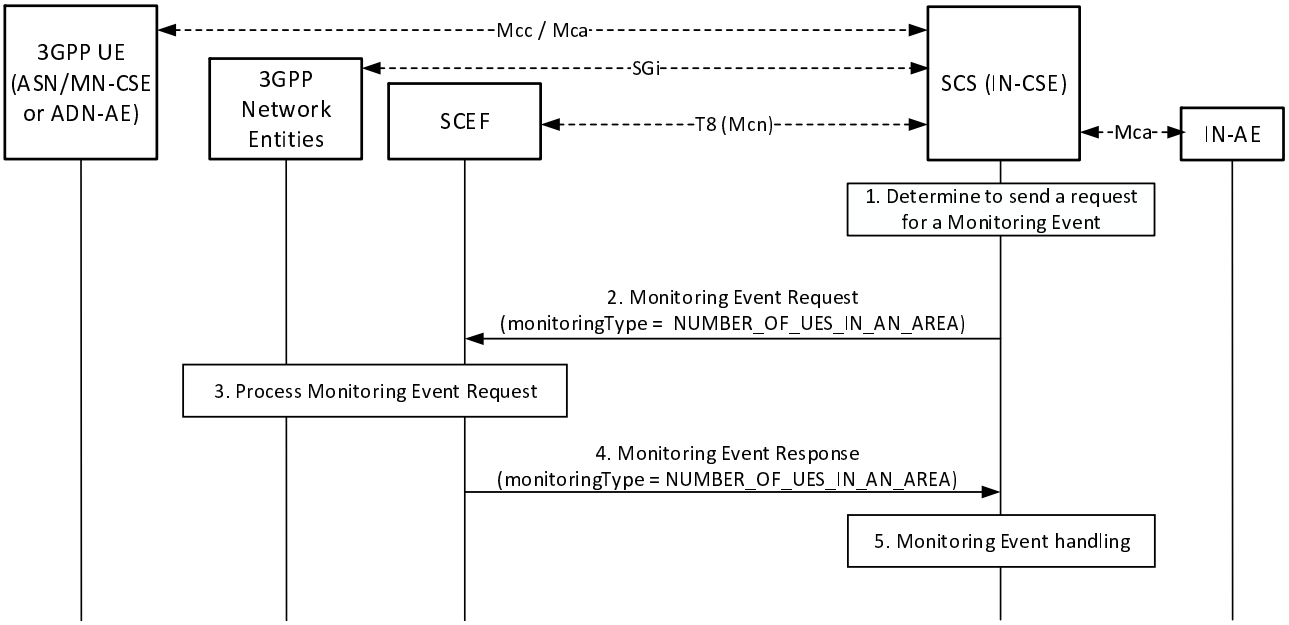

Figure 7.4.8-1: Monitoring for Number of UEs in an Area

Pre-conditions:

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

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

If the deployment uses External Group Identifier (*externalGroupId*) as described in ETSI TS 129 122 [4], when ASN/MN-CSEs or ADN-AEs register with the IN-CSE, then they use *externalGroupId* information to configure the *externalGroupID* of the corresponding <*remoteCSE*> or <*AE*> resources (see clause 6.3 when *externalGroupID* is configured).

The IN-CSE is configured to be able to determine a location area (i.e. *locationArea* and/or *locationArea5G*) of interest in the underlying 3GPP network. The IN-CSE may use its location services or other location information. How the location area of interest is determined is outside the scope of the present document.

The IN-CSE is configured with system defaults for:

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

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

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

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

The IN-CSE determines to send to a SCEF a Monitoring Event Request for number of UEs present in an area of interest. The IN-CSE may determine the *externalGroupID* of a group of interest in the request, in which case the Monitoring Event Request is for the number of group-member UEs present in the area of interest.

The IN-CSE gets the *externalGroupID* information according to the attribute *externalGroupID* of the resource <*remoteCSE*> and <*AE*> of the UEs which location are in the area of interest. If there are multiple *externalGroupIDs*, the IN-CSE determines by local policy to send this request by each *externalGroupID* or send this request without *externalGroupID*.

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

The IN-CSE sends a Monitoring Event Request for the geographical area of interest to the SCEF. The Monitoring Event Subscription request from the IN-CSE to the SCEF shall comply with ETSI TS 129 122 [4] as follows:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *MonitoringEventSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *monitoringType* shall be set to NUMBER_OF_UES_IN_AN_AREA indicating the number of UEs in a given geographic area.
  - *monitorExpireTime* is optional and may be set to an absolute time at which the monitoring event request is considered to expire. If used, the IN-CSE shall configure this time based on Service Provider and MNO policies.
  - *locationType* shall be set to LAST_KNOWN_LOCATION.
  - *supportedFeatures* shall be set to a string value of "8" and/or "12" indicating support for Location Reporting notifications. If it is set to the value of "8" (Number_of_UEs_in_an_area_notification), the feature supports the pre-5G (e.g. 4G) requirement. If it is set to the value of "12" (Number_of_UEs_in_an_area_notification_5G), the feature supports the 5G requirement (only be supported in 5G).
  - *locationArea* and/or *locationArea5G* shall be included to indicate the area of interest within which the IN-CSE requests the number of UEs. If *supportedFeatures* is set to the value of "8", the *locationArea* attribute is applicable. If *supportedFeatures* is set to the value of "12", the *locationArea5G* attribute is applicable.
  - *externalGroupId* shall be set to the *externalGroupID* if in step 1 the IN-CSE monitoring request targets identifying the number of UEs from a specific group in the area and the IN-CSE determined an *externalGroupID* to be monitored.
  - *maximumNumberOfReports* shall be set to an integer value of "1" indicating one-time reporting.
  - *requestTestNotification, websockNotifConfig, addExtGroupIds* and *groupReportGuardTime* are not supported by the present document and shall not be included.

Step 3: SCEF processes the Monitoring Event Request

The SCEF processes the Monitoring Request together with the 3GPP network entities as described in ETSI TS 129 122 [4].

Step 4: SCEF sends a Monitoring Event Response

The SCEF sends a Monitoring Event Response to the IN-CSE to acknowledge the request has been accepted. This response is described in ETSI TS 129 122 [4] and includes the following information:

- A response code of 200 OK.

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

- The response payload shall include a *MonitoringEventReport* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:

    - *ueCount* is configured to indicate the number of UEs found at the location. If an *externalGroupId* has been provided in the request, the count indicates the number of UEs from the given group which are found at the location.

    - *externalIds* is configured to indicate External Identifier(s) of the UEs included in the number of UEs found denoted by *ueCount.*

    - Note that and the External Identifier(s) information may or may not be provided in the response, depending on MNO configuration of MME/SGSN.

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

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 5: Monitoring Event handling at the IN-CSE

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

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

7.5 3GPP Based Device triggering

7.5.1 General Procedure for 3GPP Based Device Triggering

An IN-CSE may initiate a device trigger to an ASN/MN-CSE or ADN-AE hosted on a 3GPP UE to cause it to establish a connection to the IN-CSE, enrol to a MEF, register to the IN-CSE, update its PoA, or perform a CRUD operation on a specified resource. The IN-CSE may initiate the device trigger itself (implicit) or it may be initiated by a request that the IN-CSE receives from an AE (explicit).

Whenever the IN-CSE sends a device trigger to an ASN/MN-CSE or ADN-AE hosted on a 3GPP UE, the device triggering procedure as described in ETSI TS 129 122 [4] shall be used as the basis for the procedures defined below.

This procedure supports an ASN/MN-CSE or ADN-AE that is hosted on a 3GPP UE that is directly connected to an underlying 3GPP network.

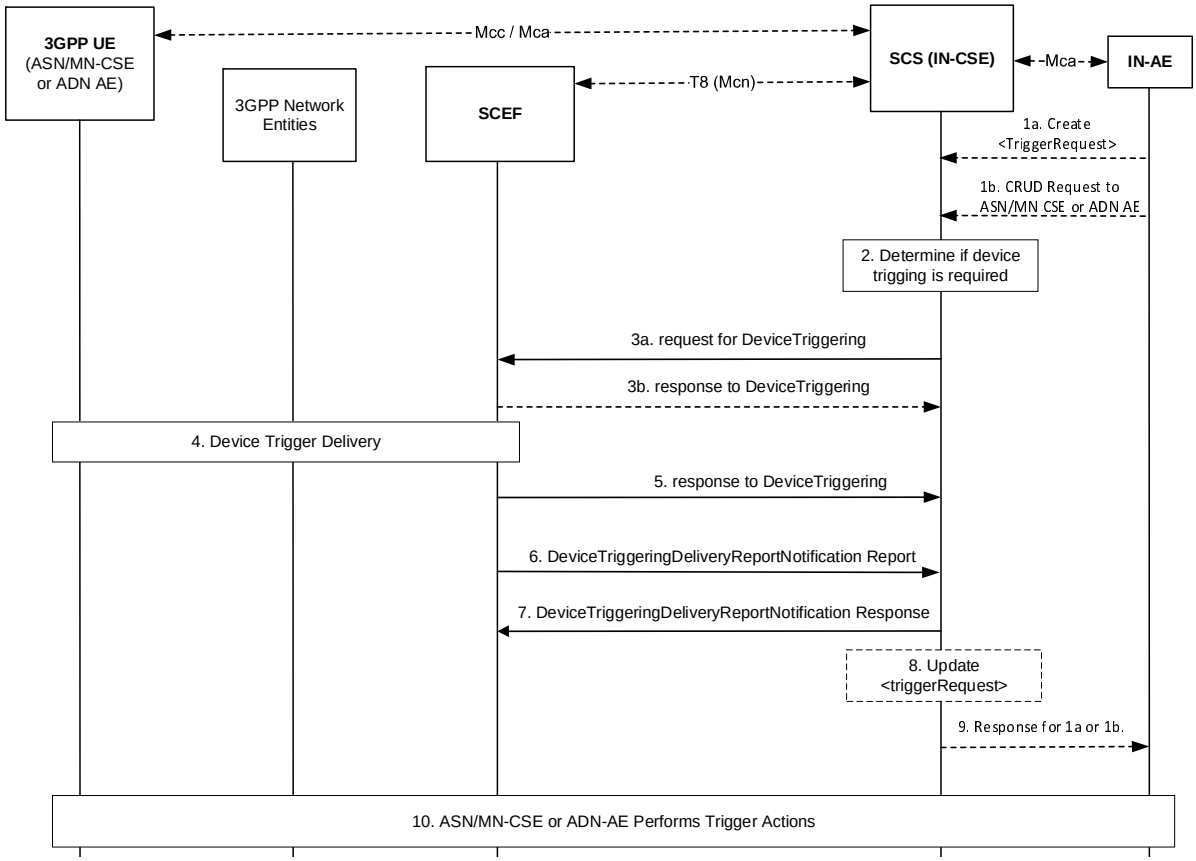

Figure 7.5.1-1: General Procedure for Device Triggering

Pre-conditions

The UE that hosts the ASN/MN-CSE or ADN-AE is available to receive the Device Trigger Request using one of the connectivity establishment methods described in clause 6.

Step 1 (Optional): Request targeted to ASN/MN-CSE or ADN-AE

An AE may initiate a device trigger to an ASN/MN-CSE or ADN-AE explicitly by creating or updating a <*triggerRequest*> resource as specified in clause 9.6.49 of ETSI TS 118 101 [1]. Alternatively, an AE may initiate a device trigger to an ASN/MN-CSE or ADN-AE implicitly by issuing a request to an IN-CSE that requires device triggering. For example, if an IN-CSE receives a request to perform a CRUD operation targeting an ASN/MN-CSE or ADN-AE hosted on a 3GPP UE that is not reachable by the IN-CSE, the IN-CSE may generate a trigger request.

Step 2: Determine if Device Triggering is required

The IN-CSE determines whether to send a device trigger to the targeted ASN/MN-CSE or ADN-AE. Further details are provided in clause 8.3.3.2.1 of ETSI TS 118 101 [1].

If device trigger was initiated by an AE, initiating AE determines device trigger.

Step 3a: Request for Device Triggering

The IN-CSE or AE sends the Device Triggering request that contains information as specified in ETSI TS 129 122 [4]. Such information includes:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-device-triggering/v1/{scsAsId}/transactions*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.

- The request payload shall include a *DeviceTriggering* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *supportedFeatures* shall be set to a string value of "0" indicating that trigger notifications over Websockets or trigger notification test events are not supported.
  - *validityPeriod* shall be set to either the *triggerValidityTime* attribute of the <*triggerRequest*> resource if the trigger request is initiated by an AE.
  - *triggerPayload* shall be configured as described in clause 8.3.3.2.1 of ETSI TS 118 101 [1] and clause 9.2.1 of ETSI TS 118 104 [3]. An empty payload indicates that the targeted ASN/MN-CSE or ADN-AE shall re-establish connectivity with the IN-CSE.
  - *externalId* shall be set to the *M2M-Ext-ID* of the targeted UE hosting an ASN/MN-CSE or ADN-AE.
  - *applicationPortID* shall be set to *Trigger-Recipient-ID* attribute of the <*triggerRequest*> resource, if specified.
  - *notificationDestination* shall be configured with a URI that the SCEF can target Device Trigger notifications towards. The value of this URI shall be based on internal IN-CSE policies or IN-CSE identifier.
  - *priority* may be set to either PRIORITY or NO_PRIORITY per internal IN-CSE policies and/or agreements between the Service Provider and MNO or the *triggerPriority* attribute of the <*triggerRequest*> resource.
  - *msisdn*, *requestTestNotification* and *websockNotifConfig* are not supported by the present document and shall not be included.

General Exceptions

The SCEF is not reachable when IN-CSE tries to send DeviceTriggering message. In this case the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to ERROR_NSE_NOT_FOUND after a prior timeout period (IN-CSE local policy).

Step 3b (Optional): Response to Device Triggering request

The SCEF may send a Device Triggering response to the IN-CSE to acknowledge the successful reception of the Device Trigger request before the request is delivered to the targeted UE as specified in ETSI TS 129 122 [4]. Otherwise an HTTP error status code as defined in clause 8.3 may be returned. The response includes the following information:

- A response code of 201 CREATED.
- The *URI* of the device triggering resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-device-triggering/v1/{scsAsId}/transactions {transactionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{transactionId}* segment is configured by the SCEF.
- The response payload will include a *DeviceTriggering* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a URI to the resource created by the SCEF for the request.
  - *deliveryResult* configured with one of the following status for confirmation:
    - TRIGGERED: that the request for device triggering has been received and is accepted by the SCEF but has not yet been delivered. In this case the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_TRIGGERED.

General Exceptions

If the SCEF responds with one of the error response codes defined in clause 8.3, the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_FAILED.

Step 4: Device Trigger Delivery procedure

The device trigger message shall be delivered to the UE hosting the ASN/MN-CSE or ADN-AE.

Step 5: Response to DeviceTriggering

The SCEF may send a Device Trigger response to the IN-CSE to acknowledge the successful delivery of the Device Trigger request to the targeted UE as specified in ETSI TS 129 122 [4]. Otherwise an HTTP error status code defined in clause 8.3 may be returned. The response includes the following parameters:

- A response code of 201 CREATED.
- The *URI* of the device triggering resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-device-triggering/v1/{scsAsId}/transactions {transactionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{transactionId}* segment is configured by the SCEF.
- The response payload will include a *DeviceTriggering* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* parameter configured with a URI to the resource created by the SCEF for the Device Trigger request.
  - *deliveryResult* is included in the HTTP response to indicate one of the following status for delivery of the device trigger:
    - SUCCESS: that the device triggering delivery is successfully completed. In this case the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_DELIVERED.
    - UNKNOWN: that indicates any unspecified errors. In this case the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_FAILED.
    - FAILURE: that this trigger encountered an error during delivery or processing and is deemed permanently undeliverable. In this case the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_FAILED.
    - EXPIRED: that the validity period expired when processing the device triggering request. In this case the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_EXPIRED.
    - TERMINATE: that the delivery of the device triggering request is terminated by the IN-CSE. In this case the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_TERMINATED.

General Exceptions

If the SCEF responds with one of the error response codes defined in clause 8.3, and the device trigger was initiated by an AE via a <*triggerRequest*> resource, the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_FAILED.

Step 6: Device Triggering Delivery Report Notification request

The SCEF sends a Device Triggering Delivery Report Notification message to the *{notification_uri}* of the IN-CSE with the results of the trigger delivery outcome. This message is defined in ETSI TS 129 122 [4] and shall include the following:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Device Triggering Request.
- *transaction* is configured with a link to the related device triggering transaction resource to which this notification is related to.
- The request payload will include a *deliveryResult* data structure as specified in ETSI TS 129 122 [4]. The IN-CSE shall process the deliveryResult and update the *triggerStatus* attribute of the <*triggerRequest*> as defined in Step 5.

Step 7: Device Triggering Delivery Report Notification response

After receiving a Device Triggering Delivery Report Notification request, the IN-CSE or AE returns a HTTP response having a response code of 204 NO CONTENT and no payload.

Steps 8 (optional) and 9: IN-CSE Updates <triggerRequest> and Response to 1a or 1b

If the device trigger was initiated by an AE via a <*triggerRequest*> resource, then the IN-CSE shall update *triggerStatus* attribute of <*triggerRequest*> resource.

Step 10: ASN/MN-CSE or ADN-AE performs trigger actions

If the trigger has no payload, the ASN/MN-CSE or ADN-AE shall re-establish connectivity with the IN-CSE. Otherwise, based on the type of trigger request received, the ASN/MN-CSE or ADN-AE performs the corresponding trigger actions such as establish connectivity with the IN-CSE, enrol with the MEF, register to the IN-CSE, update its PoA, or execute a CRUD request on a specified resource.

Further details are described in clause 8.3.3.2.1 of ETSI TS 118 101 [1] and clause 9.2.1 of ETSI TS 118 104 [3].

7.5.2 3GPP Based Device Trigger Recall/Replace Procedure

Figure 7.5.2-1 shows a procedure for a 3GPP based Device Trigger Recall (i.e. cancel a trigger request) and Replace (i.e. update a trigger request) between oneM2M and an underlying 3GPP network.

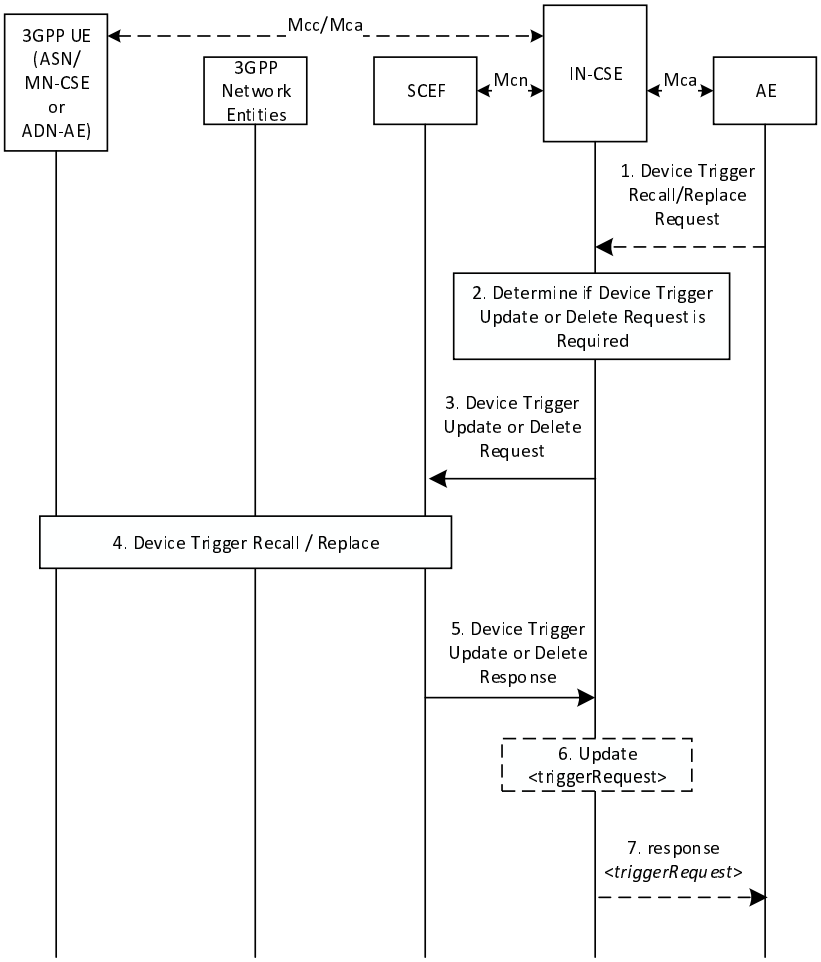

Figure 7.5.2-1: 3GPP Based Device Triggering Recall/Replace Procedure

Pre-condition

The IN-CSE has already sent a device trigger request to the underlying 3GPP network. The IN-CSE has stored the previous device trigger information, e.g. trigger reference number, etc.

Step 1 (Optional): IN-AE Trigger Recall/Replace Request

An AE issues a request to the IN-CSE to recall/replace a trigger (via a DELETE or UPDATE of a <*triggerRequest*> resource) that results in the IN-CSE generating a trigger recall/replace request to the underlying 3GPP network.

Step 2: Determine if Device Triggering is required

The IN-CSE determines whether to send a Device Trigger Recall/Replace Request to the targeted ASN/MN-CSE or ADN-AE. Further details are provided in clause 8.3.3.2.1 of ETSI TS 118 101 [1].

Step 3: Device Trigger Recall or Replace Request

After identifying the proper SCEF, the IN-CSE sends a Trigger UPDATE (Replace) or DELETE (Recall) Request to the SCEF targeting the *transactionID* of the Device Trigger.

For an UPDATE (Replace) request, the request shall contain one or more of the following fields:

- An HTTP PUT method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-device-triggering/v1/{scsAsId}/transactions/{transactionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*transactionId*} segment is the resource identifier of the trigger being replaced.
- The request payload shall include a *DeviceTriggering* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *supportedFeatures* shall be set to a string value of "0" indicating that trigger notifications over Websockets or trigger notification test events are not supported.
  - *validityPeriod* shall be set to either the *triggerValidityTime* attribute of the <*triggerRequest*> resource if the trigger request is initiated by an AE.
  - *triggerPayload* shall be configured as described in clause 8.3.3.2.1 of ETSI TS 118 101 [1] and clause 9.2.1 of ETSI TS 118 104 [3]. An empty payload indicates that the targeted ASN/MN-CSE or ADN-AE shall re-establish connectivity with the IN-CSE.
  - *externalId* shall be set to the *M2M-Ext-ID* of the targeted UE hosting an ASN/MN-CSE or ADN-AE.
  - *applicationPortID* shall be set to *Trigger-Recipient-ID* attribute of the <*triggerRequest*> resource, if specified.
  - *notificationDestination* shall be configured with a URI that the SCEF can target Device Trigger notifications towards. The value of this URI shall be based on internal IN-CSE policies or IN-CSE identifier.
  - *priority* may be set to either PRIORITY or NO_PRIORITY per internal IN-CSE policies and/or agreements between the Service Provider and MNO or the *triggerPriority* attribute of the <*triggerRequest*> resource.
  - *msisdn*, *requestTestNotification* and *websockNotifConfig* are not supported by the present document and shall not be included.

For a DELETE (Recall) request, the request shall contain one or more of the following fields:

- An HTTP DELETE method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-device-triggering/v1/{scsAsId}/transactions/{transactionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*transactionId*} segment is the resource identifier of the trigger being recalled.
- The request shall not contain a payload.

General Exceptions

If the SCEF is not reachable when IN-CSE tries to send Device Triggering request, then the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to ERROR_NSE_NOT_FOUND after a prior timeout period (defined by IN-CSE local policy).

Step 4: Device Trigger Recall/Replace Handling

The SCEF recalls or replaces the trigger as described in ETSI TS 123 682 [2].

Step 5: Device Trigger Recall/Replace Response

The SCEF sends a Device Trigger Response to the IN-CSE.

If the request was to replace the Device Trigger, then the response is returned by the SCEF with a 200 OK response code and a payload that includes an updated *DeviceTriggering* data structure as specified in ETSI TS 129 122 [4]. The *DeviceTriggering* data structure also includes the *deliveryResult* configured with REPLACED to indicate that the request to replace the device triggering request has been accepted by the SCEF.

If the request was to recall the Device Trigger, then the response is returned by the SCEF with a 204 NO CONTENT response code and no payload is included.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Steps 6 and 7 (Optional): Process Device Trigger Recall/Replace Response

The IN-CSE processes the Device Trigger Recall/Replace Response. If the recall/replace request was initiated by an AE, the IN-CSE updates the corresponding <*triggerRequest*> resource as described in clause 8.3.3.2.1 of ETSI TS 118 101 [1].

For a device trigger replace, the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_REPLACED if the device trigger was initiated by an AE via a <*triggerRequest*> resource.

For a device trigger recall, the IN-CSE shall delete the <*triggerRequest*> resource if the device trigger recall was initiated by an AE via a delete request targeting the <*triggerRequest*> resource.

If the SCEF responds with one of the error response codes defined in clause 8.3, and the device trigger was initiated by an AE via a <*triggerRequest*> resource, the IN-CSE shall update the *triggerStatus* attribute of the <*triggerRequest*> to TRIGGER_FAILED.

7.6 Configuration of Traffic Patterns

oneM2M uses the 3GPP MTC feature for Configuration of Device Communication Patterns to configure Node Traffic Patterns in the underlying 3GPP network (see clause 8.3.5 Configuration of Node Traffic Patterns of ETSI TS 118 101 [1]).

To that purpose the IN-CSE translates the oneM2M Node Traffic Pattern (TP) into a 3GPP Device Communication Pattern. The generic oneM2M procedure for configuration of Node Traffic Patterns is shown in Figure 7.6-1.

The underlying 3GPP network signalling sequence for provisioning of CP parameters is described in ETSI TS 123 682 [2].

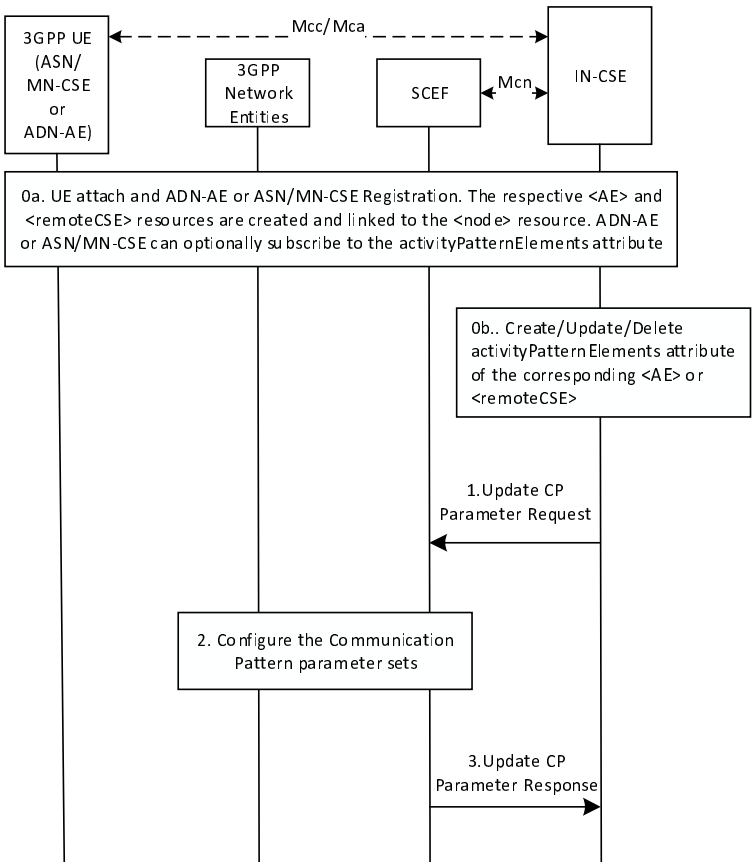

Figure 7.6-1: General procedure for oneM2M configuration of Traffic Patterns

Pre-conditions:

There is a relationship in place between the IN-CSE and MNO allowing the IN-CSE to request Configuration of Device Communication Patterns. The method for establishing this relationship is outside the scope of the present document.

Step 0: UE Attach and oneM2M Registration Procedures

The UE attaches to the underlying 3GPP network and the ADN-AE(s) or ASN/MN-CSE hosted on the UE perform the oneM2M registration procedure, as detailed in clause 6.3. The IN-CSE hosts the corresponding <*AE*> or <*remoteCSE*> resources and an associated <*node*> resource for the registree. During this procedure, the ADN-AE or ASN/MN-CSE can create an *activityPatternElements* attribute indicating the anticipated communication patterns.

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

Step 1: IN-CSE sends to the SCEF a Communication Patterns Configuration request

This step is triggered by the create/update/delete of *activityPatternElements* attribute of either the <*AE*> or <*remoteCSE*> resource. The IN-CSE derives the communication patterns from the *activityPatternElements.*

The IN-CSE selects the SCEF based on the *M2M-Ext-ID*'s of the registree ASN/MN-CSE or ADN-AEs (e.g. either a DNS lookup on the *M2M-Ext-ID* or the based on the domain portion of the *M2M-Ext-ID*'s.).

When the first *activityPatternElements* for a given a UE is initially configured, the IN-CSE shall generate a Communication Patterns Configuration creation request that contains the following information as specified in ETSI TS 129 122 [4]:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-cp-parameter-provisioning/v1/{scsAsId}/subscriptions*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.

- The request payload shall include a *CpInfo* data structure as specified in ETSI TS 129 122 [4] with the following attributes:

  - externalId shall be set to M2M-Ext-ID.

  - supportedFeatures shall be set to a string value of "0" indicating no support for the expected UE geographical movement feature in oneM2M Release 4.

  - cpParameterSets - This is a set of communication/traffic pattern parameters indicating an anticipated communication schedule of all the ADN-AEs or ASN/MN-CSE hosted on the UE. The IN-CSE configures this parameter with the aggregated communication/traffic patterns of all ADN-AEs or ASN/MN-CSE hosted on the UE. The IN-CSE derives the aggregated communication/traffic patterns using the activityPatternElements attributes of the corresponding <AE> and <remoteCSE> resources. For a UE hosting one or more AEs, the IN-CSE uses the values provided in all the activityPatternElements attributes for the <AE>s hosted on this UE. For a UE hosting an ASN/MN-CSE, the IN-CSE uses the values provided by the activityPatternElements attribute of the <remoteCSE> resource. The IN-CSE shall configure the cpParameterSets as follows:

    - *setId* shall be assigned based on internal IN-CSE policies. This parameter will serve as a suggested name for the {*apiRoot*}/3gpp-cp-parameter-provisioning/v1/{scsAsId}/subscriptions/{subscriptionId}/cpSets/{setId} resource created by the SCEF. The SCEF may override this suggested name in which case, the SCEF will provide an updated value back in the response.

    - *validityTime* may be configured by the IN-CSE with an expiration time of the communication/traffic pattern of the UE. For example, the IN-CSE may configure this attribute with a value that is aligned with the *expirationTime*(s) of the corresponding <AE> or <remoteCSE> resource(s) associated with the ADN-AE(s) or ASN/MN-CSE hosted on the UE.

    - *periodicCommunicationIndicator* shall be set by the IN-CSE. If the *activityPatternElements* are configured with a repeating periodic communication pattern (e.g. detectable via the use of wildcards and/or step values in the *activityPatternElements*), then a PERIODICALLY enumerated value shall be used. Otherwise an ON_DEMAND enumerated value shall be used.

    - *communicationDurationTime* shall only be set by the IN-CSE if the *periodicCommunicationIndicator* is configured with a value PERIODICALLY. The IN-CSE shall configure this parameter with the time interval when the UE is actively communicating as specified within the *activityPatternElements* of the ADN-AE(s) or ASN/MN-CSE hosted on the UE. The value shall be expressed as a time duration in seconds.

    - *periodicTime* shall only be set by the IN-CSE if the *periodicCommunicationIndicator* is configured with a value PERIODICALLY. The IN-CSE shall configure this parameter with the duration of time separating active communication periods as specified within the *activityPatternElements* of the ADN-AE(s) or ASN/MN-CSE hosted on the UE. The value shall be expressed as a time duration in seconds.

    - *scheduledCommunicationTime* shall be set by the IN-CSE if the *activityPatternElements* of the ADN-AE(s) or ASN/MN-CSE specify certain days of the week and/or specific start and end times in the day that the UE actively communicates.

    - *stationaryIndication* and *expectedUmts* are not supported by the present document and shall not be included in the *cpParameterSets.*

  - *msisdn* and *externalGroupId* are not supported by the present document and shall not be included.

Once a Communication Patterns Configuration has been created for a given UE, an IN-CSE shall keep it updated if/when any *activityPatternElements* for the ADN-AE(s) or ASN/MN-CSE hosted on a given UE are modified or deleted. To perform the update, the IN-CSE shall generate a Communication Patterns Configuration update request that contains the following information as specified in ETSI TS 129 122 [4]:

- An HTTP PUT method shall be used.

- *URI* shall be set to {*apiRoot*}/3gpp-cp-parameter-provisioning/v1/{*scsAsId*}/subscriptions/{*subscriptionId*}/cpSets/{*setId*}. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} and {*setId*} segment are configured by the SCEF and returned to the IN-CSE in the Communication Patterns Configuration creation response.

- The request payload shall include an updated *CpInfo* data structure as specified in ETSI TS 129 122 [4]. The IN-CSE shall configure the *CpInfo* data structure based on the aggregated values of all the *activityPatternElements* of the ADN-AE(s) or ASN/MN-CSE that are hosted on the corresponding UE. The configuration of the individual *CpInfo* attributes shall follow the same rules as specified in the Communication Patterns Configuration create request above.

If/when all the *activityPatternElements* for the ADN-AE(s) or ASN/MN-CSE hosted on a given UE are deleted or contain communication schedules that have elapsed, the IN-CSE may generate a Communication Patterns Configuration delete request that contains the following information as specified in ETSI TS 129 122 [4]:

- An HTTP DELETE method shall be used.

- *URI* shall be set to {*apiRoot*}/3gpp-cp-parameter-provisioning/v1/{*scsAsId*}/subscriptions/{*subscriptionId*}. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} segment is configured by the SCEF and returned to the IN-CSE in the Communication Patterns Configuration creation response.

Once a Communication Patterns Configuration for a given UE has been deleted, the IN-CSE can create a new Communication Patterns Configuration, using the same procedure described above, if/when an *activityPatternElements* for an ADN-AE or ASN/MN-CSE hosted on the UE is configured.

General Exceptions

The SCEF is not reachable when IN-CSE tries to send Communication Patterns Configuration request. In this case the IN-CSE will not be able to configure the communication patterns of the UE in the underlying 3GPP network. Whether the IN-CSE continues to service requests for ADN-AE(s) or ASN/MN-CSE hosted on UEs that the IN-CSE is outside the scope of the present document.

Step 2: Communication Patterns Configuration Handling in the underlying 3GPP network

The underlying 3GPP network elements store the new/updated CP parameter set along with the associated SCEF *id* and validity time.

Step 3: SCEF sends Communication Patterns Configuration Response to IN-CSE

The SCEF authorizes the request and responds to acknowledge it accepted and processed the request.

A response to a Communication Patterns Configuration create request includes the following information:

- If the result is successful, the SCEF will return a response code of 201 CREATED. If all communication/ traffic pattern parameters are not provisioned successfully, the SCEF will return a response code of 500 Internal Server Error which includes the report within the attribute *cpReports* with a list of failed *setId* (s) and the corresponding failure code (e.g. MALFUNCTION or OTHER_REASON) as specified in ETSI TS 129 122 [4]. In this case, the IN-CSE may retry the request. Alternatively, the IN-CSE may return a ***Response Status Code*** indicating "REQUESTED_ACTIVITY_PATTERN_NOT_PERMITTED" to the ADN-AE(s) or ASN/MN-CSE hosted on the UE. Then the ADN-AE(s) or ASN/MN-CSE hosted on the UE may retry their request with a different *activityPatternElements* attribute value.

- The *URI* of the Communication Patterns Configuration subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-cp-parameter-provisioning/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.

- The response payload will include a *CpInfo* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:

    - self - a link to the Communication Patterns Configuration resource {apiRoot}/3gpp-cp-parameter-provisioning/v1/{scsAsId}/subscriptions/{subscriptionId}/cpSets/{setId}.

A response to a Communication Patterns Configuration update request includes the following information:

- If the result is successful, the SCEF will return a response code of 200 OK. If all communication/ traffic pattern parameters are not provisioned successfully, the SCEF will return one of the following response codes:
  - 409 Conflict which includes the report within the attribute *cpReports* with a list of failed *setId* (s) and the failure code "SET_ID_DUPLICATED" as specified in ETSI TS 129 122 [4]. In this case, the IN-CSE may return a ***Response Status Code*** indicating "REQUESTED_ACTIVITY_PATTERN_NOT_PERMITTED" to the ADN-AE(s) or ASN/MN-CSE hosted on the UE. Then the ADN-AE(s) or ASN/MN-CSE hosted on the UE may retry their request with a different *activityPatternElements* attribute value.
  - 500 Internal Server Error which includes the report within the attribute *cpReports* with a list of failed *setId* (s) and the corresponding failure code (e.g. MALFUNCTION or OTHER_REASON) as specified in ETSI TS 129 122 [4]. In this case, the IN-CSE may retry the request. Alternatively, the IN-CSE may return a ***Response Status Code*** indicating "REQUESTED_ACTIVITY_PATTERN_NOT_PERMITTED" to the ADN-AE(s) or ASN/MN-CSE hosted on the UE. Then the ADN-AE(s) or ASN/MN-CSE hosted on the UE may retry their request with a different *activityPatternElements* attribute value.
- The response payload will include an updated *CpInfo* data structure as specified in ETSI TS 129 122 [4].

A response to a Communication Patterns Configuration delete request includes the following information:

- A response code of 204 NO CONTENT.
- The response will not contain a payload.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

7.7 Group message delivery using MBMS

7.7.1 Overview

The Group Management (GMG) CSF is responsible for handling group related requests. The requests are sent to manage a group and its membership as well as to perform fanout operations to group member resources. When the same content is sent to the members of a group that are located in a particular geographical area, 3GPP provides MBMS capabilities that may be used to efficiently distribute the message to the group members using multicasting.

7.7.2 Resource Structure

Refer to the clause 9.6.44 Resource Type <*localMulticastGroup*> of ETSI TS 118 101 [1].

7.7.3 Procedures

7.7.3.1 Create MBMS Group

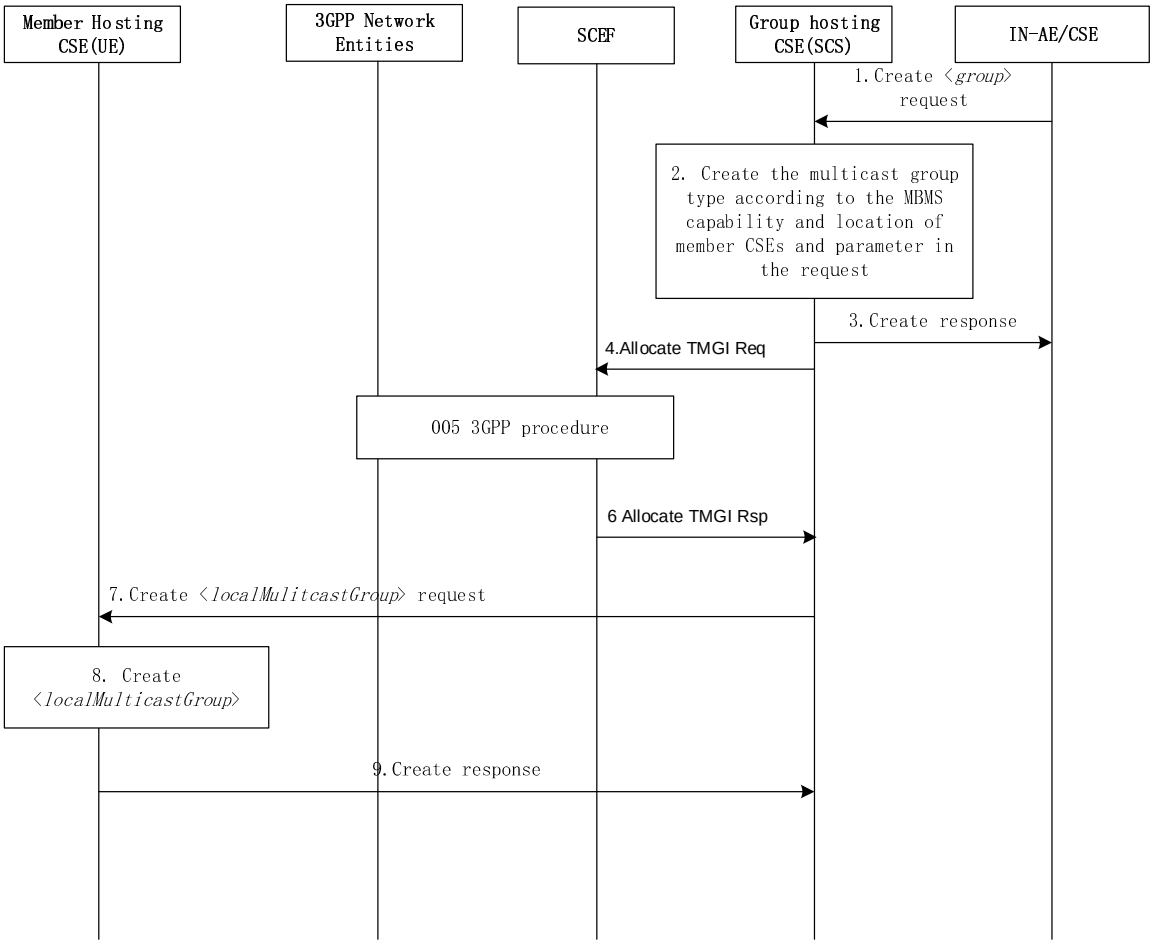

Figure 7.7.3.1-1: Service Flow of MBMS Group Creating

Pre-conditions:

1) The MBMS service area information provided by the MNO is configured in the oneM2M System.

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

Step 1: The IN-AE sends a <*group*> create request to the Group Hosting CSE.

Step 2: The Group Hosting CSE checks if the *multicastCapability* attribute of the <*remoteCSE*> resource for more than two member Hosting CSEs are configured with a value of MBMS and have the same *externalGroupID*. If so, the Group Hosting CSE then creates the <*group*> as specified in clause 10.2.7.2 of ETSI TS 118 101 [1] and the *multicastType* attribute of the Multicast Group Information is set to 3GPP_MBMS_group as specified in clause 10.2.7.13 of ETSI TS 118 101 [1].

Step 3: The Group Hosting CSE sends the response to the IN-AE/CSE.

Step 4: The Group Hosting CSE sends the Allocate TMGI Request to the SCEF. The request shall contain the following information as specified in ETSI TS 129 122 [4]:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-group-message-delivery-mb2 /v1/{scsAsId}/*tmgi-allocation. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.

- The request payload shall include a *TMGIAllocation* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalGroupId* shall be set to the *externalGroupID* of Member Hosting CSEs.
  - *mbmsLocArea* may be set to location information of Member Hosting CSEs per the accuracy policy.
  - *supportedFeatures* shall be set to a string value of "0" indicating no support for notifications over Websockets or notification test events.

General Exceptions

The SCEF is not reachable when Hosting CSE (i.e. IN-CSE) tries to send Allocate TMGI Request In this case the IN-CSE will not be able to get an allocated TMGI from the underlying 3GPP network. Hence the IN-CSE will not be able to use multicast functionality for this group. The IN-CSE may service requests for the group using unicast functionality if applicable.

Step 5: The Allocate TMGI Request is processed by the underlying 3GPP network based on the procedure defined in ETSI TS 123 682 [2].

Step 6: The SCEF sends the Allocate TMGI Response to the Group Hosting CSE. The response will contain the following information as specified in ETSI TS 129 122 [4]:

- A response code of 201 CREATED.
- The *URI* of the Communication Patterns Configuration subscription resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-group-message-delivery-mb2 /v1/{scsAsId}/*tmgi-allocation*/{tmgi}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{tmgi}* segment is configured by the SCEF.
- The response payload will include a *TMGIAllocation* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a link to the {*apiRoot*}/3gpp-group-message-delivery-mb2 /v1/{*scsAsId*}/tmgi-allocation/{*tmgi*} resource created by the SCEF for the request.
  - *tmgi* is configured with the identity of a particular MBMS bearer service.
  - *tmgiExpiration* is configured with absolute time at which the TMGI is considered to expire.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 7: The Group Hosting CSE stores the *tmgi* and *tmgiExpiration* in the local Multicast Group Information and sends <*localMulticastGroup*> creation requests to the Member Hosting CSEs via unicast which contain mandatory attributes specified in clause 9.6.44 of ETSI TS 118 101 [1]. If the *multicastType* is 3GPP_MBMS_group, the request contains the *tmgi* and *responseTimeWindow*.

Steps 8 and 9: These steps are specified in clause 10.2.7.14 of ETSI TS 118 101 [1].

7.7.3.2 Group message delivery using MBMS

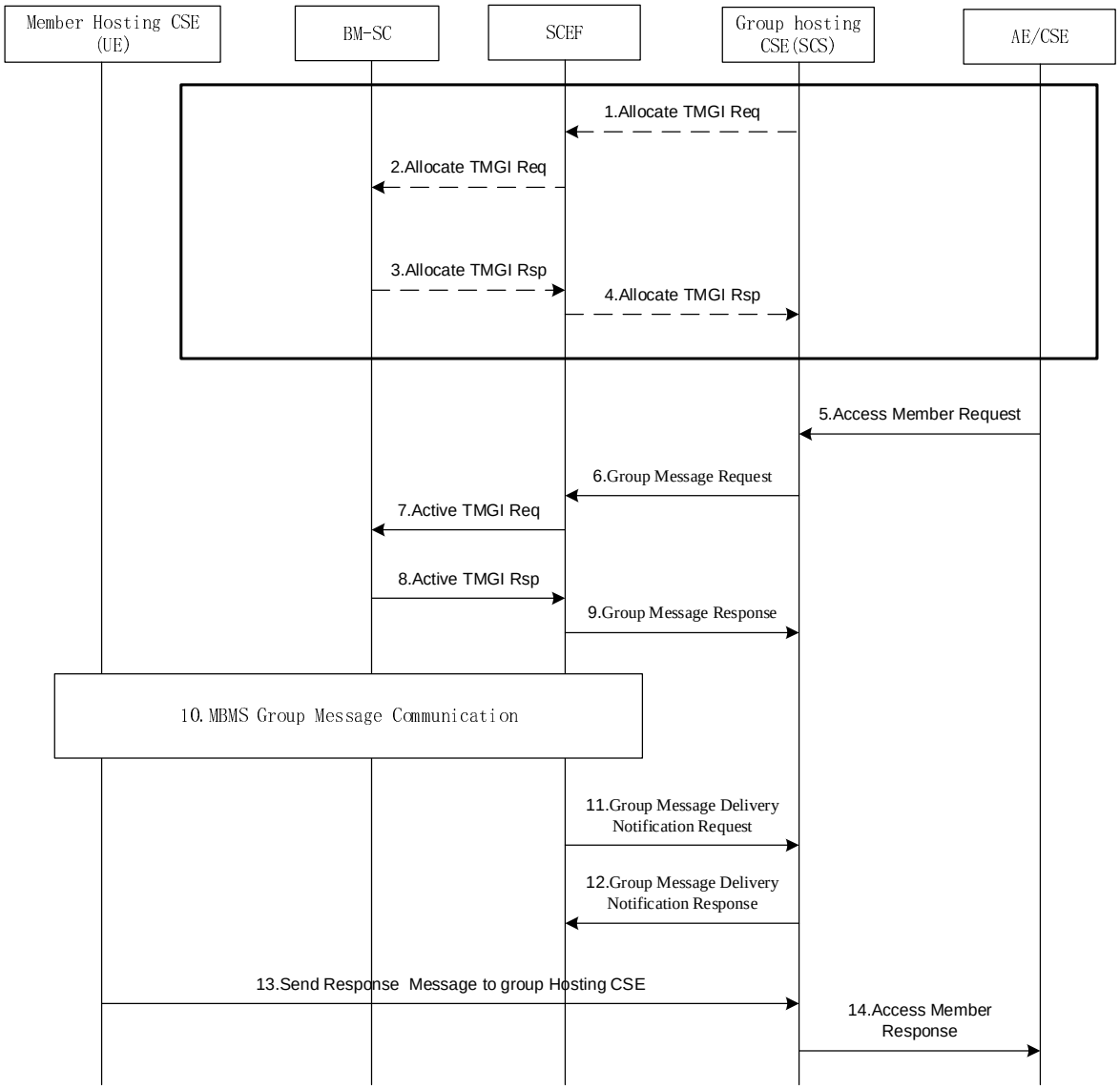

Figure 7.7.3.2-1: Service Flow of MBMS Group Message Delivery

Step 1: Before the *tmgiExpiration* of the multicast group, the Group Hosting CSE may send an Allocate TMGI Request to renew the expiration time for already allocated TMGIs. The request shall contain the following information as specified in ETSI TS 129 122 [4]:

- An HTTP PUT method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-group-message-delivery-mb2 /v1/{scsAsId}/*tmgi-allocation/*{tmgi}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{tmgi}* segment is configured by the SCEF in the response to the initial TMGI Allocation request.
- The request payload shall include a *TMGIAllocation* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalGroupId* shall be set to the *externalGroupID* of Member Hosting CSEs.
  - *mbmsLocArea* may be set to location information of Member Hosting CSEs per the accuracy policy.
  - *supportedFeatures* shall be set to a string value of "0" indicating no support for notifications over Websockets or notification test events.

General Exceptions

The SCEF is not reachable when Hosting CSE (i.e. IN-CSE) tries to send Allocate TMGI Request. In this case the IN-CSE will not be able to renew the TMGI with the underlying 3GPP network. Hence the IN-CSE will not be able to use multicast functionality for this group. The IN-CSE may service requests for the group using unicast functionality if applicable.

Steps 2 and 3: The Allocate TMGI is processed by the underlying 3GPP network based on the procedure defined in ETSI TS 123 682 [2].

Step 4: The SCEF sends the Allocate TMGI Response to the Group Hosting CSE. The response will contain the following information as specified in ETSI TS 129 122 [4]:

- A response code of 200 OK.
- The response payload will include an updated *TMGIAllocation* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a link to the {*apiRoot*}/3gpp-group-message-delivery-mb2 /v1/{*scsAsId*}/tmgi-allocation/{*tmgi*} resource created by the SCEF for the request.
  - *tmgi* is configured with the identity of a particular MBMS bearer service.
  - *tmgiExpiration* is configured with absolute time at which the TMGI is considered to expire.

The Group Hosting CSE shall replace the new *tmgiExpiration* in the Multicast Group Information locally.

NOTE 1: Steps 1 to 4 are optional (e.g. if the *tmgiExpiration* is not going to expire any time soon).

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 5: The IN-AE/CSE sends a request carrying the group resource identifier for accessing member resources to the Group Hosting CSE.

Step 6: If the *multicastType* is 3GPP_MBMS_group, the Group Hosting CSE checks the existing <*schedule*> child resources for all the Member Hosting CSE <*node*> resources. If there is no time intersection of the existing <*schedule*>s, then the Group Hosting CSE returns an error response to the IN-AE/CSE after which the procedure is terminated. If there is a time intersection, the Group Hosting CSE shall check if the ***Operation Execution Time and Request Expiration Timestamp*** are in the scope of the intersection when ***Operation Execution Time*** or ***Request Expiration Timestamp*** is included in the request. If not, the Group Hosting CSE shall return an error to the IN-AE/CSE after which the procedure is terminated.

NOTE 2: 3GPP supports the SCS/AS to set the *Message Delivery Start Time* for the UEs of a group which can impact the power saving mode of the UE, but oneM2M does not support it in Release 4.

Then the group Hosting CSE shall send the Group Message Delivery Request to the SCEF to activate the MBMS bearer to provide MBMS communication network resources for MBMS members from the next start time of the time intersection. The request shall contain the following information as specified in ETSI TS 129 122 [4]:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-group-message-delivery-mb2 /v1/{scsAsId}/*tmgi-allocation{*tmgi*}/delivery-via-mbms. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{tmgi}* segment is configured by the SCEF in the response to the initial TMGI Allocation request.
- The request payload shall include a *GMDViaMBMSByMb2* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalGroupId* shall be set to the same value as the *externalGroupID* of Member Hosting CSEs.
  - *groupMessagePayload* shall be set to the value specified in the request of access member resources from the IN-AE/CSE.
  - *mbmsLocArea* shall be set to location information of Member Hosting CSEs per the accuracy policy.

- *messageDeliveryStartTime* shall be set to the next start time of the time intersection.
- *notificationDestination* shall be configured with a URI that the SCEF can target Group Message Delivery notifications towards. The value of this URI shall be based on internal IN-CSE policies.
- *requestTestNotification* and *websockNotifConfig* are not supported by the present document and shall not be included.

General Exceptions

The SCEF is not reachable when Hosting CSE (i.e. IN-CSE) tries to send Group Message Delivery Request. In this case the IN-CSE will not be able to use multicast functionality to send the request to the group members. The IN-CSE may send the request to the group members using unicast functionality if applicable.

Steps 7 and 8: The Activate MBMS Bearer Procedure is processed by the underlying 3GPP network based on the procedure defined in ETSI TS 123 682 [2].

Step 9: The SCEF sends the Group Message Response to the Group Hosting CSE. The response shall contain the following information as specified in ETSI TS 129 122 [4].

- A response code of 201 CREATED.
- The *URI* of the Group Message Delivery resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-group-message-delivery-mb2 /v1/{scsAsId}/*tmgi-allocation{*tmgi*}/delivery-via-mbms*/{transactionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*tmgi*} and *{transactionId}* segments are configured by the SCEF.
- The response payload will include an updated *GMDViaMBMSByMb2* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a link to the *{apiRoot}/3gpp-group-message-delivery-mb2 /v1/{scsAsId}/*tmgi-allocation{*tmgi*}/delivery-via-mbms/*{transactionId}* resource created by the SCEF for the request.
  - *acceptanceStatus* indicating whether the activation of MBMS bearer corresponding to the TMGI was accepted or rejected.
  - *scefMessageDeliveryIPv4* indicates the Ipv4 address where the SCEF supports receiving group message payloads separate from the Group Message Delivery Request. In the present document, the IN-CSE includes the group message payload in the Group Message Delivery Request and hence the IN-CSE ignores this information in the response.
  - *scefMessageDeliveryIPv6* indicates the Ipv6 address where the SCEF supports receiving group message payloads separate from the Group Message Delivery Request. In the present document, the IN-CSE includes the group message payload in the Group Message Delivery Request and hence the IN-CSE ignores this information in the response.
  - *scefMessageDeliveryPort* indicates the port number where the SCEF supports receiving group message payloads separate from the Group Message Delivery Request. In the present document, the IN-CSE includes the group message payload in the Group Message Delivery Request and hence the IN-CSE ignores this information in the response.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 10: The Group Message Delivery by MBMS Procedure is processed by the underlying 3GPP network based on the procedure defined in ETSI TS 123 682 [2].

Step 11: The SCEF sends a Group Message Delivery Notification to the Group Hosting CSE.

The notification message contains the following information as specified in ETSI TS 129 122 [4]:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Group Message Delivery Request.

- The request payload will include a *GMDByMb2Notification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *transaction* configured with a URI to the transaction resource for which this notification corresponds to.
  - *tmgi* identifies the TMGI that this notification is applicable to.
  - *deliveryTriggerStatus* indicates whether the delivery of the group message payload was successful or not and will have the value of TRUE or FALSE.

Step 12: After receiving a Group Message Delivery Notification, the Group Hosting CSE (i.e. IN-CSE) returns a response having a response code of 204 NO CONTENT.

Step 13: The Member Hosting CSE shall send the response message within the scope of *responseTimeWindow*. Details are specified in clause 10.2.7.13.2 of ETSI TS 118 101 [1].

Step 14: The Group Hosting CSE shall receive the response messages from Member Hosting CSEs until *responseTimeWindow* expires and return the aggregated group member responses to the IN-AE/CSE.

General Exceptions

If the SCEF sends a Group Message Delivery Notification to the Group Hosting CSE with a *deliveryTriggStatus* set to FALSE indicating that the delivery of the group message payload was not successful, then the Group Hosting CSE may choose to return a GROUP_MEMBERS_NOT_RESPONDED error response to the IN-AE/CSE before the *responseTimeWindow* expires.

7.8 Informing about Potential Network Issues

7.8.1 Throttling of requests based on Network Status Reports

The 3GPP SCEF Network Status Monitoring functionality described in ETSI TS 129 122 [4] supports an API to allow an IN-CSE to be informed when there are network congestion issues in a geographical area in the underlying 3GPP network.

An IN-CSE may request to receive notifications from an underlying 3GPP network when the network congestion level in a specified geographical area crosses defined threshold value(s). Based on these reports, the IN-CSE can start/stop throttling of requests initiated by or targeted towards its registree AEs and CSEs that are hosted on UEs residing in this geographical area to help manage the congestion levels in the underlying 3GPP network.

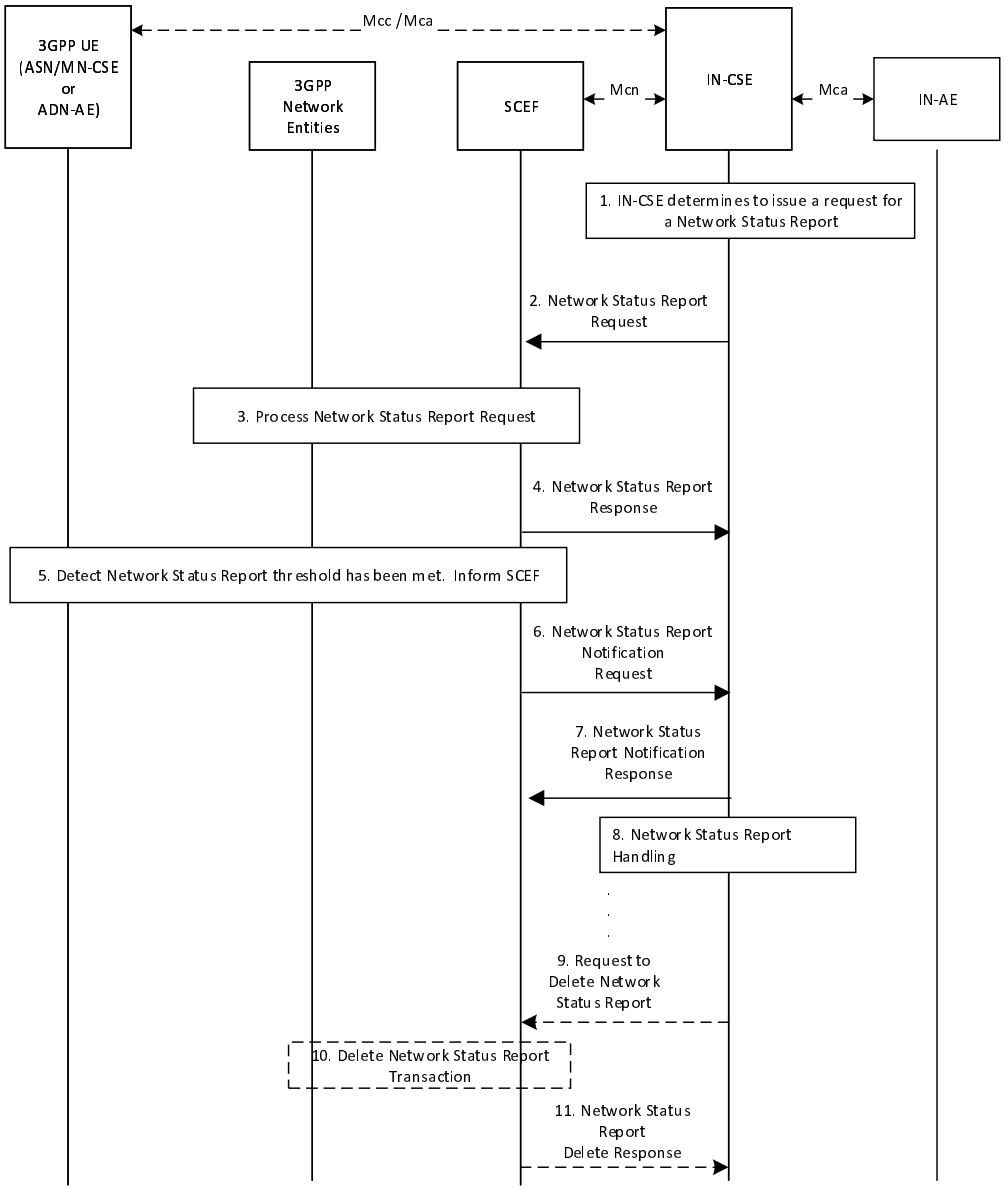

Figure 7.8.1-1: Request for Network Status Reports

Pre-conditions

There is a relationship in place between the IN-CSE and MNO allowing the IN-CSE to request Network Status Reports from the underlying 3GPP network. The method for establishing this relationship is outside the scope of the present document.

The IN-CSE is configured with system defaults for the following. The method for configuring these system defaults is outside the scope of the present document:

- The network congestion levels to receive reports.
- The severity of each specified congestion level.
- The specified actions to take based on the severity of each congestion level.

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

The IN-CSE is able to detect the location of its registree ASN/MN-CSEs and/or ADN-AEs. For example, a <*locationPolicy*> resource may be used by an IN-CSE to detect the location of each ASN/MN-CSE or ADN-AE.

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

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

Step 1: IN-CSE issues a Network Status Request

The IN-CSE issues a Network Status Report request to the SCEF via one or more of the following approaches:

- The IN-CSE may periodically check the location of its registree ASN/MN-CSEs and ADN-AEs. When the IN-CSE detects that a certain number of ASN/MN-CSEs and/or ADN-AEs are in the same geographical area, it may further check if the ASN/MN-CSEs and ADN-AEs are connected to the same network. The IN-CSE can detect if the ASN/MN-CSEs and ADN-AEs are connected to the same network by examining their *M2M-Ext-ID* attributes. For example, a 3GPP external identifier is composed of a local identifier and a domain identifier. If the ASN/MN-CSEs and ADN-AEs have the same domain identifier, they may be connected to the same network. When the IN-CSE detects that a number of ASN/MN-CSEs and/or ADN-AEs are in the same geographical area and attached to the same network, it may decide to request a Network Status Report in that geographical area.

- The IN-CSE may use [cmdhNwAccessRule] resources for corresponding registree CSEs that support CMDH functionality. The IN-CSE may check the *targetNetwork* attribute and use this attribute to identify a SCEF and issue a Network Status Request to this SCEF. When issuing the request for a Network Status Report, the IN-CSE shall provide a geographic area for which the report will apply. The IN-CSE may detect the geographic area for which the policy applies by checking the location that is associated with each CSE. For example, <*locationPolicy*> resources may be associated with a registree CSE for which the CMDH policies apply and used by an IN-CSE to detect locations for the CSEs.

How the IN-CSE determines which of the above approach(es) to use is implementation specific and outside the scope of the present document.

Step 2: Network Status Report Request

The IN-CSE requests network status reports for a geographical area. The Network Status Reporting Subscription request from the IN-CSE to the SCEF shall comply with ETSI TS 129 122 [4] as follows:

- An HTTP POST method shall be used.

- *URI* shall be set to *{apiRoot}/3gpp-net-stat-report/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.

- The request payload shall include a *NetworkStatusReportingSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:

  - *notificationDestination* shall be set to a URI that the SCEF can target Network Status Report notifications towards. The value of this URI shall be based on internal IN-CSE policies.

  - *thresholdValues* shall be a list of integer values in the range of 0 to 31 and specify what congestion threshold(s) the IN-CSE wants to receive a report for. Whenever the congestion in the geographical area goes above or below an indicated threshold, a report will be sent. The threshold(s) that are indicated by the IN-CSE are determined based on local IN-CSE policies. The definition of these policies is outside the scope of the present document.

  - *thresholdTypes* shall be a list of enumerated types with values HIGH, MEDIUM and LOW that specify the type of congestion status the IN-CSE would like to receive a report for. The threshold type(s) that are indicated by the IN-CSE are determined based on local IN-CSE policies. The definition of these policies is outside the scope of the present document. The IN-CSE shall not include thresholdValue and thresholdType in the same request. They shall be used mutually exclusive of one another.

  - *timeDuration* shall indicate the date and time that the SCEF will stop sending reports to the IN-CSE. The data and time value is determined based on local IN-CSE policies. The definition of these policies is outside the scope of the present document.

NOTE 1: If no duration is provided, then only one Network Status Report will be provided to the IN-CSE.

- *locationArea* shall be configured with location information specified by the IN-CSE. The IN-CSE may use location information that it collects from its registree's <*locationPolicy*> resources and/or *M2M-Ext-IDs* to configure this attribute. Shall be expressed as a list cell IDs, tracking areas, civic addresses or geographic area.
- *supportedFeatures* shall be set to a string value of "0" indicating no support for notifications via Websockets or notification test events.
- *requestTestNotification* and *websockNotifConfig* are not supported by the present document and shall not be included.

General Exceptions

The SCEF is not reachable when Hosting CSE (i.e. IN-CSE) tries to send Network Status Reporting Subscription request. In this case the IN-CSE will not be able to get receive network status reports from the underlying 3GPP network. Hence the IN-CSE will not be able to provide value-add services to the underlying 3GPP network such as throttling of requests targeted towards AEs and CSEs hosted on UEs residing in congested areas of the network.

Step 3: SCEF Processes Network Status Report Request

The SCEF and the underlying 3GPP network process the Network Status Report Request.

Step 4: Network Status Report Response

The SCEF sends a Network Status Report Response to the IN-CSE to acknowledge the request has been accepted. This response is defined in ETSI TS 129 122 [4] and includes the following information:

- A response code of 201 CREATED.
- The *URI* of the Group Message Delivery resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-net-stat-report/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.
- The response payload will include an updated *NetworkStatusReportingSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - self is configured with a link to the {apiRoot}/3gpp-net-stat-report/v1/{scsAsId}/subscriptions/{subscriptionId} resource created by the SCEF for the request.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 5: Detect Congestion

After receiving the initial Network Status Request or when the congestion level passes one of the indicated threshold(s), the SCEF will create a Network Status Report.

Step 6: Network Status Report

The SCEF sends a Network Status Report to the corresponding *notificationDestination* of the IN-CSE that was configured in Step 2. The report contains information as specified in ETSI TS 129 122 [4]. Such information includes:

- An HTTP POST method is used.
- *URI* is set to *{notification_uri}*. The *{notification_uri}* is configured by the IN-CSE in the Network Status Reporting Subscription Request.
- The request payload will include a *NetworkStatusReportingNotification* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *subscription* configured with a URI to the subscription resource for which this notification corresponds to.

- *nsiValue* configured with the network status indicator that is an integer in the range of 0 to 31 that indicates a congestion level as defined in ETSI TS 129 122 [4].

- *nsiType* configured with the network status indicator that is an enumerated value of HIGH, MEDIUM or LOW as defined in ETSI TS 129 122 [4].

NOTE 2: A response will not contain both nsiType and nsiValue. They are mutually exclusive.

Step 7: Network Status Report Acknowledgement

After receiving a Network Status Report Notification, the IN-CSE returns a response having a response code of 204 NO CONTENT.

Step 8: Process Network Status Report

In response to the Network Status Report, the IN-CSE may decide to throttle up/down traffic in the congested area of the network via one or more of the following approaches:

- An IN-CSE may reject requests that target nodes in congested areas of the network. If an IN-CSE rejects a request due to network congestion it shall return an EXTERNAL_OBJECT_NOT_REACHABLE response code. The IN-CSE may also inform the Originator to retry the request after some specified backoff delay. The method to inform the Originator is currently not specified in the present document however a message included in the payload of the response could be used.

- An IN-CSE may delay the processing (i.e. buffer) of requests that target nodes in congested areas of the network:

  - If the request is a blocking request, the IN-CSE should not delay the processing of the request and should instead reject this request with a corresponding response code informing the cause of rejection is due to network congestion.

  - If the request includes an Event Category that is set to immediate the IN-CSE should not delay the processing of the request and should instead reject the request with an EXTERNAL_OBJECT_NOT_REACHABLE response code. In this case, the IN-AE may decide to resubmit the request with the Event Category set to "bestEffort" or "latest" to indicate the IN-CSE may buffer the request.

- An IN-CSE may modify the <*schedule*> resource of its registree AEs or CSEs that are located in a congested area of the network such that they modify the times they send or receive requests:

  - A registree AE or CSE may retrieve or subscribe to its <*schedule*> resource such that it detects if the IN-CSE updates the *scheduleElement* attribute. Upon detecting an updated *scheduleElement* an AE or CSE shall modify the times which it sends requests and makes itself available to receive requests.

- An IN-CSE may modify the [cmdhNwAccessRule] resources for corresponding registree CSEs that support CMDH functionality.

How the IN-CSE determines which of the above approach(es) to use is outside the scope of the present document and may be based on agreements with the MNO.

Step 9 (Optional): Network Status Request Cancellation

Before the Duration expires, the IN-CSE may request that the SCEF stop sending status reports. The IN-CSE may make this decision, for example, when it detects that a number of devices are no longer in the geographical area applicable to the Network Status Request.

The IN-CSE shall send a Network Status Cancellation Request as follows:

- An HTTP DELETE method shall be used.

- *URI* shall be set to *{apiRoot}/3gpp-net-stat-report/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the Network Status Reporting Subscription was created.

- The request shall not contain a payload.

Step 10 (Optional): Process Network Status Cancellation Request

The SCEF processes the cancelation request.

Step 11 (Optional): Acknowledge Network Status Cancellation Request

The SCEF acknowledges the request to cancel Network Status Reports for the geographical area with a response code of 204 NO CONTENT.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

7.9 Setting up an AS session with required QoS procedure

7.9.1 Overview

3GPP supports setting up an IP flow to a UE with a specific QoS (e.g. low latency or jitter) and priority handling by 3rd party service providers (AS/SCS session) via the T8 API. The oneM2M system may use this functionality for the communication management between an IN-CSE and a UE. An AE may specify, for a set of target resources, a QoS level parameter which refers to the pre-defined QoS information between the oneM2M and the underlying 3GPP network. Based on this information, the oneM2M system shall map the operation addressing those resources from the IN-CSE to the target UE to the 3GPP IP flow, negotiate the QoS with the underlying 3GPP network, and request the underlying 3GPP network to deliver the operation with the negotiated QoS.

7.9.2 Resource Structure

Refer to the clause 9.6.63 Resource Type *<e2eQosSession>* of ETSI TS 118 101 [1].

7.9.3 Procedures

7.9.3.1 Create/Update E2E QoS procedure

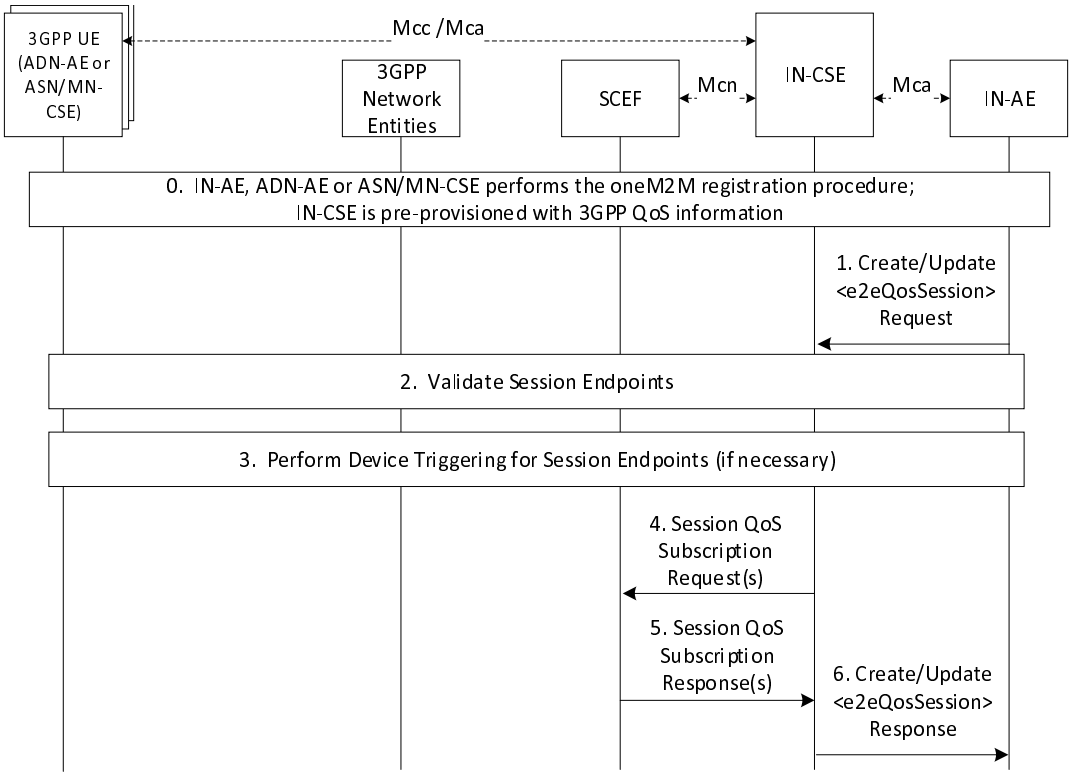

Figure 7.9.3.1-1: Create/Update E2E QoS procedure

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

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

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

Step 1: An AE or CSE sends a <*e2eQosSession*> CREATE/UPDATE request to the IN-CSE

The <*e2eQosSession*> CREATE/UPDATE request includes the following information:

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

NOTE 1: The Originator of the <*e2eQosSession*> CREATE/UPDATE request may be an entity specified in the *sessionEndpoints* attribute. Alternatively, it may be a different entity.

- *sessionEndpoints* attribute shall be set to a list consisting of one or more AE-IDs and/or CSE-IDs representing the endpoints of the E2E QoS session.
- *e2eQosRequirements* attribute shall be configured with a list of one or more tuples. Each tuple in the list has the following elements:
  - *qosLevel* element shall be set to a value between 0 and 100.
  - *resourceIDList* element shall beset to a list of resource identifiers the QoS requirement applies to.
  - *sessionSchedule* element may be set. If set, it consists of seven fields of second, minute, hour, day of month, month, day of week and year.
  - *numOfRequests* element may be set. If set, it consists of the minimum number of requests required to be transferred at the specified *qosLevel.*
  - *numOfBytes* element may be set. If set, it consists of the minimum number of bytes required to be transferred at the specified *qosLevel.*
- *e2eQosPolicies* attribute may be set. If set, it is configured with 1 or more tuples. Each tuple has the following elements:
  - *status* element shall be set with a value of FAILED, DISABLED or USAGE_EXHAUSTED.
  - *action* element shall be set with a value of RE-ENABLE or DISABLE.

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

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

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

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

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

NOTE 2: If the *sessionSchedule* element is configured, the IN-CSE uses the schedule information to determine whether to perform this step during the processing of the <*e2eQosSession*> CREATE/UPDATE request or sometime thereafter (e.g. closer to the time when scheduled communication via the session is required).

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

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

NOTE 3: If the *sessionSchedule* element is configured, the IN-CSE uses the schedule information to determine whether to perform this step during the processing of the <*e2eQosSession*> CREATE/UPDATE request or sometime thereafter (e.g. closer to the time when scheduled communication via the session is required).

Each AsSessionWithQoSSubscription Request from the IN-CSE to the SCEF contains information as specified in ETSI TS 129 122 [4]. Such information includes:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-as-session-with-qos/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload includes an *AsSessionWithQoSSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *supportedFeatures* shall be set to a string value of "0" indicating the IN-CSE does not support the QoS Session negotiable features specified in ETSI TS 129 122 [4].
  - *notificationDestination* shall be set to a URI that the SCEF should target QoS session related notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - *flowInfo* includes the following attributes:
    - *flowId* shall be set to an integer value that describes the IP flow. A value is assigned by the IN-CSE according to local policy. The value that is used is unique within the scope of the IN-CSE.
    - *flowDescriptions* shall be an array of strings configured with two entries. The first entry in the array is an IP flow description for oneM2M requests and responses flowing from the IN-CSE to the QoS session endpoint applicable to this request. The second entry in the array is an IP flow description for oneM2M requests and responses flowing in the reverse direction from the QoS session endpoint to the IN-CSE:
      - Entry #1 in the *flowDescriptions* array includes the following attributes:
        - *direction* shall be set to a value of "out".
        - *source IP address* shall be set to the IP address of the IN-CSE and *destination IP address* is set to the IP addresses configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

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

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

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

  - *direction* shall be set to a value of "in".

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

NOTE 4: The order is reversed from the order used in Entry #1.

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

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

NOTE 5: The order is reversed from the order used in Entry #1.

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

- *ueIpv4Addr* shall be set to the IPv4 address (if applicable) configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

- *ueIpv6Addr* shall be set to the IPv6 address (if applicable) configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

- *usageThreshold* includes the following attributes:

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

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

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

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

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

The SCEF handles the AsSessionWithQoSSubscription Request together with the 3GPP network entities. The SCEF sends an AsSessionWithQoSSubscription Response that contains information as specified in ETSI TS 129 122 [4] to the IN-CSE.

The message includes the following information:

- A response code of 201 CREATED.

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

- The response payload may include a *AsSessionWithQoSSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:

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

General Exceptions

If the SCEF responds with one of the error response codes defined in clause 8.3, the IN-CSE shall update the *e2eQosStatus* of the <*e2eQosSession*> resource to a value of FAILED.

Step 6: The IN-CSE returns response to Originator

7.9.3.2 QoS Session request processing procedure

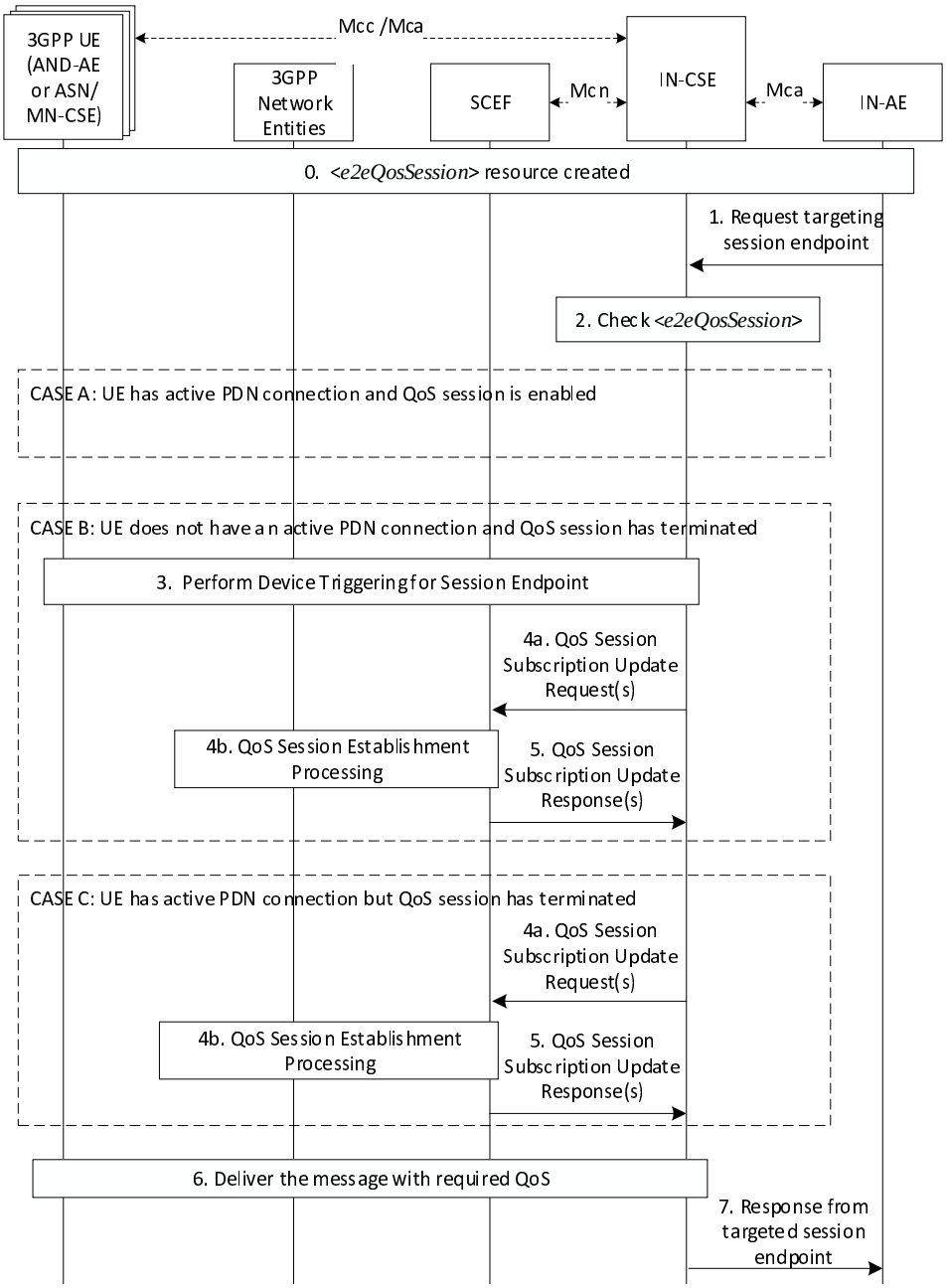

Figure 7.9.3.2-1: Setting up 3GPP session with required QoS

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

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

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

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

The IN-CSE processes the received request and obtains the targeted end point from the *To* parameter. Then IN-CSE checks the targeted end point and *From* parameters to see if they match with any *sessionEndpoints* configured within the <*e2eQosSession*> resources hosted by the IN-CSE. If a match is found, the IN-CSE then checks the *To* parameter in the request to see if the specified resource identifier matches any resource identifiers in the *resourceIDList* element of the *e2eQosRequirements* attribute configured within the same <*e2eQosSession*> resource. If the IN-CSE does not find a <*e2eQosSession*> resource with matching session endpoints or a matching resource identifier, the IN-CSE shall attempt to forward the request to the targeted endpoint without any negotiated 3GPP QoS and proceed to Step 7. If a match is found, the IN-CSE shall checks the *e2eQosStatus* attribute of the matching <*e2eQosSession*> resource to determine whether the QoS session is enabled or not.

The IN-CSE also checks whether the entity targeted by the request has an active 3GPP PDN connection and is reachable by the IN-CSE.

CASE A: The QoS session is enabled and the targeted entity has an active 3GPP PDN connection. The IN-CSE proceeds to Step 6.

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

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

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

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

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

If the configured *e2eQosRequirements* permit the IN-CSE to request that the QoS session be re-enabled when the *e2eQosStatus* attribute is set to DISABLED or USAGE_EXHAUSTED, the IN-CSE may execute this step. Otherwise, the IN-CSE shall either choose to continue processing the request in a best-effort fashion or go to Step 7 with a corresponding ***Response Status Code*** indicating "NETWORK_QOS_CONFIG_ERROR" by local policy.

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

The IN-CSE sends a request to update to AsSessionWithQoSSubscription Request from the IN-CSE to the SCEF contains information as specified in ETSI TS 129 122 [4]. Such information includes:

- An HTTP PUT method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-as-session-with-qos/v1/{scsAsId}/subscriptions/{subscriptionID}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.
- The request payload includes an *AsSessionWithQoSSubscription* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *supportedFeatures* shall be set to a string value of "0" indicating the IN-CSE does not support the QoS Session negotiable features specified in ETSI TS 129 122 [4].
  - *notificationDestination* shall be set to a URI that the SCEF should target QoS session related notifications towards. The value of this URI shall be based on internal IN-CSE policies.

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

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

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

NOTE 2: The order is reversed from the order used in Entry #1.

- *qosReference* shall be set to a pre-provisioned string value that maps to the *qosLevel*. This mapping is based on a SLA with the MNO. The *qosReference* serves as an identifier of the pre-defined QoS information pre-provisioned into the IN-CSE based on a SLA with the MNO.
- *ueIpv4Addr* shall be set to the IPv4 address (if applicable) configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.

- *ueIpv6Addr* shall be set to the IPv6 address (if applicable) configured in the *pointOfAccess* attribute of the <*AE*> or <*remoteCSE*> resource hosted on the IN-CSE and associated with the QoS session endpoint applicable to this request.
- *usageThreshold* includes the following attributes:
  - *duration* shall be set to the amount of time in seconds that the QoS session is requested to remain active. The IN-CSE computes this duration by inspecting all of the <*e2eQosSession*> resources that it hosts and that have a session endpoint that matches the session endpoint applicable to this request. For any matches found, the IN-CSE will aggregate the *sessionSchedule* elements (if any) configured within the list of *e2eQosRequirements* tuples of these <e2eQosSession> resources. Based on the aggregated *sessionSchedule* elements and local policies, the IN-CSE will determine a duration of time to request. If no *sessionSchedule* elements are configured, the IN-CSE will base its determination solely on local policies.
  - *totalVolume* shall be set to a total number of bytes of data that are required to be exchanged between the IN-CSE and the session endpoint applicable to this request. The IN-CSE shall compute this number of bytes by inspecting all of the <*e2eQosSession*> resources that it hosts and that have a session endpoint that matches the session endpoint applicable to this request. For any matches found, the IN-CSE will sum all of the *numOfBytes* elements (if any) configured within the list of *e2eQosRequirements* tuples of these <e2eQosSession> resources. Based on the *numOfBytes* elements and local policies, the IN-CSE will determine an amount to request. If no *numOfBytes* elements are configured, the IN-CSE will base its determination solely on local policies.
- *sponsorInfo* may be set. If set, the value is a string based on a SLA with the MNO.
- *ethFlowInfo, macAddr, requestTestNotification* and *websockNotifConfig* are not supported by the present document and are not included.

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

The SCEF handles the AsSessionWithQoSSubscription Request together with the 3GPP network entities. The SCEF sends an AsSessionWithQoSSubscription Response that contains information as specified in ETSI TS 129 122 [4] to the IN-CSE.

The message includes the following information:

- A response code of 200 OK.
- The response payload will include a *AsSessionWithQoSSubscription* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a URI to the resource created by the SCEF for the request.

General Exceptions

If the SCEF responds with one of the error response codes defined in clause 8.3, the IN-CSE shall update the *e2eQosStatus* attribute of the <*e2eQosSession*> resource to a value of FAILED.

Step 6: The IN-CSE delivers the message with the required QoS and updates the <*e2eQosSession*> resource

If the QoS session is enabled, the IN-CSE forwards the request to the targeted session endpoint entity. After receiving a response back from the targeted session endpoint, the IN-CSE updates the *e2eQosStatus* attribute of the <*e2eQosSession*> resource and prepares a response for the Originator (IN-AE).

If the QoS session is disabled and the IN-CSE is un-successful in re-enabling it, then the IN-CSE shall either choose to continue processing the request in a best-effort fashion or go to Step 7 with a corresponding *Response Status Code* indicating "NETWORK_QOS_CONFIG_ERROR" by local policy.

Step 7: The IN-CSE returns response to Originator

IN-CSE sends response to the IN-AE.

7.9.3.3 3GPP QoS status monitoring and report procedure

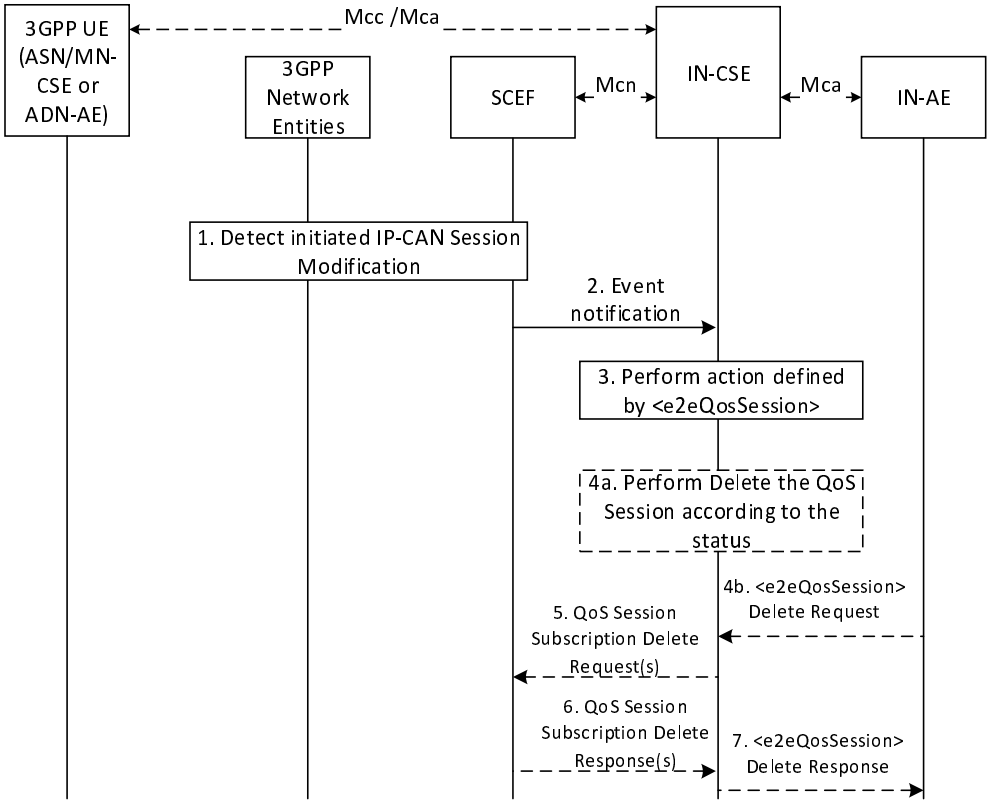

Figure 7.9.3.3-1: 3GPP QoS status report procedure

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

The 3GPP entities may notify the SCEF about bearer level events for the Rx session (e.g. transmission resources are released/lost) with an IP-CAN Session Modification as described in ETSI TS 123 203 [11].

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

When the SCEF receives information of a status change in step 1, the SCEF creates and sends an Event Notification message to the IN-CSE as specified in ETSI TS 129 122 [4].

The Event Notification request includes the following:

- *event* indicates the event reported by the SCEF and is configured with one of the following enumerated values as specified in ETSI TS 129 122 [4]:

  - SESSION_TERMINATION, LOSS_OF_BEARER, RECOVERY_OF_BEARER, RELEASE_OF_BEARER, USAGE_REPORT.

- *accumulatedUsage* indicates the amount of time in seconds that the QoS session was used and the amount of data bytes transferred via the QoS session when *event* is USAGE_REPORT. This notification is sent when the usage exceeds the values defined in the *usageThreshold* configured in the AsSessionWithQoSSubscription.

- *flowIds* is configured with the same value of *flowId* in the AsSessionWithQoSSubscription.

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

When the IN-CSE receives the Event Notification, the IN-CSE will map the *event* and *accumulatedUsage* to the *e2eQosStatus* of <*e2eQosSession*> resource and performs the action according to the status.

Table 7.9.3.3-1

3GPP event	oneM2M QoS session status(*e2eQosStatus*)
SESSION_TERMINATION	DISABLED
LOSS_OF_BEARER	DISABLED
RELEASE_OF_BEARER	DISABLED
RECOVERY_OF_BEARER	ENABLED
USAGE_REPORT	ENABLED (if *accumulatedUsage* indicates duration/volume has not been exhausted) USAGE_EXHAUSTED (if *accumulatedUsage* indicates duration/volume has been exhausted)

The IN-CSE may update the *e2eQosStatus* of the resource <*e2eQosSession*> resource if there is no Step 4.

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

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

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

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

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

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

For each QoS session subscription associated with the <*e2eQosSession*> resource being deleted, the IN-CSE sends a AsSessionWithQoSSubscription DELETE Request to the SCEF. The request to delete a AsSessionWithQoSSubscription contains information as specified in ETSI TS 129 122 [4]. Such information includes:

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

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

The SCEF handles the AsSessionWithQoSSubscription DELETE Request together with the 3GPP network entities. The SCEF sends an AsSessionWithQoSSubscription DELETE Response that contains information as specified in ETSI TS 129 122 [4] to the IN-CSE.

The message includes the following information:

- A response code of 204 No Content.

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

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

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

7.10 Background Data Transfer

7.10.1 Overview

For the oneM2M system, Background Data Transfer (BDT) allows the IN-AE/CSE to have some control over its transmissions to field domain nodes that use an underlying 3GPP network that provides transfer of data in the background. Namely, the IN-AE/CSE is provided with a list of potential transfer policies (time windows, with associated maximum bit rate) and charging condition so that the IN-AE/CSE may use a time window that is more favourable in terms of tariff/cost and/or overall throughput.

For the underlying 3GPP network, management of the background data traffic for UEs (such as M2M devices) may result in significant gains for the network. For example, it is expected that for some use cases, 3rd party entities will select the more underutilized time windows to take advantage of the more favourable tariff and/or cost for the charging conditions. This effectively allows the MNO to spread the network utilization over time.

The purpose of this feature is to provide a means for the oneM2M System to inform the underlying 3GPP network of parameters that can be used for optimizing the background data traffic over the underlying 3GPP network for a set of Field Domain Nodes (UEs). Such parameters may include the expected number of UEs in the set and amount of data to be transferred a desired/preferred time window for the data transfer to these UEs, and network area information. In response, the underlying 3GPP network may inform the oneM2M system about policies that may be used to meet the given background data transfer request.

Background Data Transfer takes place in 3 steps:

- Policy Request and Selection:
  - An initiating entity (AE or CSE) will provide information on the requested BDT (e.g. expected data volume per UE) for a set of Field Domain Nodes (ADN/ASN /MN) to the IN-CSE. The information will include a group or list of Field Domain Nodes that will use the policy, as well as some guidance to the IN-CSE so that it can better select from a set of potential transfer policies offered by the underlying 3GPP network.
  - The IN-CSE will use the Mcn interface to provide the SCEF of the selected underlying 3GPP network with the BDT information and to ask for the Policy.
  - The SCEF may provide the IN-CSE with a set of possible transfer policies for BDT and collect for charging. Using the guidance provided by the initiating Application Entity (AE) or Common Service Entity (CSE), the IN-CSE selects the transfer policy based on its own local policies, and notifies the initiating entity about the selected transfer policy.
  - The IN-CSE indicates to the SCEF which policy was selected and the SCEF records the selection for charging.
- Policy Enablement:
  - The IN-CSE contacts the PCRF via SCEF and enables the policy for each UE.
- Background Data Transfer:
  - During the policy time window, the IN-CSE transfers the data to the UE through the 3GPP network, and based on the chosen policy.

7.10.2 Resource Structure

The <*backgroundDataTransfer*> resource is a child of <*CSEBase*>, <*AE*>, or <*remoteCSE*> and is used to request that the IN-CSE negotiates a background data transfer for a set of field nodes, with the underlying 3GPP Network. The resource attributes provide the characteristics of the background data transfer (volume per node, number of nodes), optionally a preferred time window for the transfer and geographic information, as well as the nodes that will be involved with the data transfer. Additionally, the resource also includes guidance to the IN-CSE so that it may select a transfer policy, if the underlying 3GPP network provides multiple potential transfer policies (*transferSelectionGuidance*).

The *groupLink*(s) or *memberIDs* attributes are used to identify the target nodes for the background data transfer request. It is assumed that the *memberIDs* list only includes field nodes that are UE's. If the IN-AE wishes to send the same message to a group of field domain nodes, it is assumed that the IN-AE has already created a <*group*> resource in the IN-CSE, with a *memberIDs* list that includes all field domain nodes that need to be reached through the background data transfer.

NOTE: The *memberIDs* are known when the <*backgroundDataTransfer*> resource is created so that the IN-CSE can determine the proper underlying 3GPP network to contact.

7.10.3 Procedures

7.10.3.1 Requesting and Selecting a Background Data Transfer Policy

Figure 7.10.3.1-1 depicts a general procedure for the request and configuration of traffic policies for BDT initiated by a request from an IN-AE. The procedure may also be initiated by a request from an MN/ASN-CSE or from the IN-CSE itself.

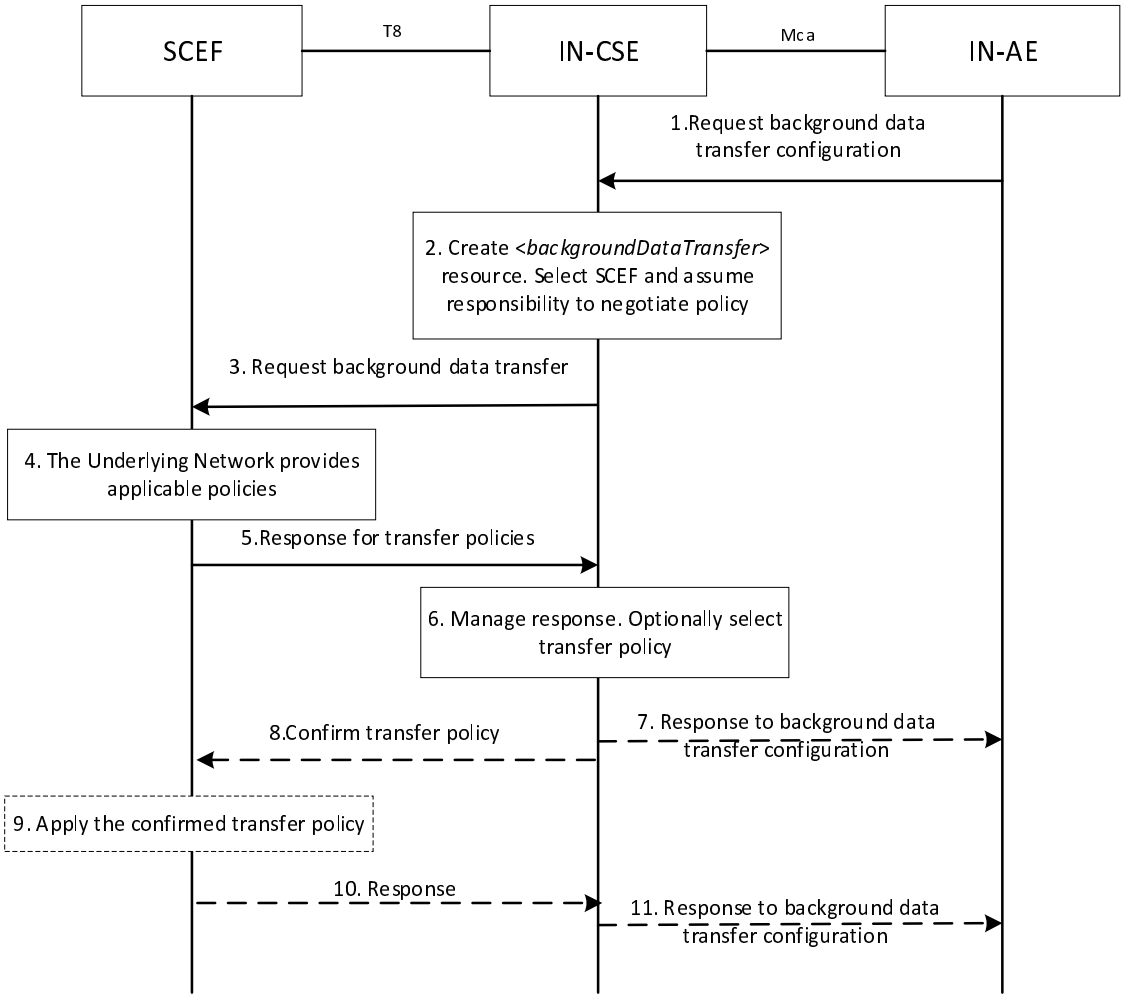

Figure 7.10.3.1-1: General Procedure for configuration of Background Data Transfer

Step 1: Request background data transfer configuration

An IN-AE requests IN-CSE to negotiate with SCEF in the underlying 3GPP network, to configure background data transfer, by creating a <*backgroundDataTransfer*> resource.

The request includes:

- The originator AE-ID of the requesting AE.

- A target identifier: i.e. the <*backgroundDataTransfer*> child resource of <*AE*>, <*CSEBase*> or <*remoteCSE*> resource.
- A set of Background Data Transfer Parameters as indicated in clause 9.6.60 of ETSI TS 118 101 [1].

If the IN-CSE has received a request from an IN-AE or another Originator to create <*backgroundDataTransfer*> resource, it checks if the request is valid.

Step 2: IN-CSE prepares for background data transfer negotiation

IN-CSE selects the SCEF and assumes the responsibility of negotiating with the underlying 3GPP network for the background data transfer. The IN-CSE selects the SCEF based on the candidate nodes that were identified in the *groupLink(s)* or *memberIDs* list of the background data transfer request. The exact selection methods are outside the scope of the present document; however, it is expected that the external identifiers of the group members can be resolved to a SCEF.

Step 3: Request background data transfer

The IN-CSE selects the SCEF and issues a BDT request, providing Background Data Transfer parameters, to the selected SCEF for negotiating background data transfer. The fields of the API are populated as follows:

- An HTTP POST method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-bdt/v1/{scsAsId}/subscriptions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *Bdt* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - supportedFeatures shall be set to a string value of "0".
  - volumePerUE shall be set to the volume of data expected to be transferred per node, based on <backgroundDataTransfer> information.
  - numberOfUEs shall be set to the expected number of nodes, based on <backgroundDataTransfer> information.
  - desiredTimeWindow shall be set to the desired time window.
  - locationArea shall be set to the optional geographic information.
  - referenceId, selectedPolicy and transferPolicies shall be absent in a BDT Request POST message.

Based on this request, if the IN-CSE is authorized, the SCEF shall negotiate the transfer policy with PCRF using the Background-data-Transfer-Request (BTR) command over the Nt reference point as defined in ETSI TS 129 154 [7].

Step 4: The underlying 3GPP network provides applicable policies for Background Data Transfer

The underlying 3GPP network determines one or more applicable transfer policies based on the requesting Background Data Transfer parameters. The SCEF receives the Background-data-Transfer-Answer (BTA) on the Nt reference point as defined in ETSI TS 129 154 [7]).

Step 5: Response for transfer policies

The SCEF responds to the IN-CSE indicating the request was accepted and sends The response message as follows:

- A response code of 201 CREATED.
- The *URI* of the Background Data resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of *{apiRoot}/3gpp-bdt/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{subscriptionId}* segment is configured by the SCEF.

- The response payload will include a *Bdt* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes:
  - *self* is configured with a URI to the Background Data resource created by the SCEF for the request.
  - *transferPolicies* containing a list of offered transfer policies, each policy including the mandatory attributes *bdtPolicyId*, *ratingGroup* and *timeWindow*, and the optional attributes *maxUplinkBandwidth* and *maxDownlinkBandwidth*.
  - *referenceId* may be present in the response.

The IN-CSE stores locally the response *referenceID* and policy information received in the SCEF response, namely the *transferPolicies* list. See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 6: Process response with transfer policies provided by the underlying 3GPP network

The IN-CSE manages the SCEF response. If only one transfer policy was received from the underlying 3GPP network, the IN-CSE updates the *desiredTimeWindow* attribute of the <*backgroundDataTransfer*> resource, with the start and end time of the *timeWindow* attribute of the received policy. The IN-CSE also stores locally the response *referenceID*.

If more than one transfer policy was received from the underlying 3GPP network, the IN-CSE uses the *transferSelectionGuidance* and its own selection policies to select one of them. If *transferSelectionGuidance* is not provided, then the IN-CSE uses internal policies to select a policy. The definition of these internal policies is outside the scope of the present document.

Step 7 (Optional): Issue response to Entity initiating the background data transfer

If only one transfer policy has been received, IN-CSE responds to the original background data transfer request from the initiating entity.

Step 8: Confirm the transfer policy

If more than one transfer policy was offered in step 4, for the transfer policy selected in Step 6, the IN-CSE informs the SCEF of the selected transfer policy identifier. For this purpose, the IN-CSE shall use the PATCH request to modify the existing resource at the SCEF.

The message includes the following information:

- An HTTP PATCH method shall be used.
- *URI* shall be set to {*apiRoot*}/3gpp-bdt/v1/{*scsAsId*}/subscriptions/{*subscriptionId*}. The {*apiRoot*} and {*scsAsId*} segments are configured based on Service Provider and MNO policies. The {*subscriptionId}* segment is configured by the SCEF.
- The request payload shall include a *BdtPatch* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *selectedPolicy* shall be set to the *bdtPolicyId* of the selected background data transfer policy among those contained in *transferPolicies* list.

Step 9: Apply the confirmed transfer policy

The transfer policy confirmed by the IN-CSE is used by SCEF to apply the configuration by notifying the underlying 3GPP network of the selected transfer policy. The SCEF includes the *referenceID* and *bdtPolicyId* of the selected policy in the Background-Data-Transfer-Request (BTR) command to PCRF over the Nt reference point as defined in ETSI TS 129 154 [7].

As response, the SCEF receives the Background-Data-Transfer-Answer (BTA) on the Nt reference point as defined in ETSI TS 129 154 [7]).

Step 10: Response to IN-CSE

Once the underlying 3GPP network has recorded/ applied the confirmed transfer policy, the SCEF returns a response to the IN-CSE.

The message includes the following information:

- A response code of 200 OK.
- The response payload will include the updated *Bdt* data structure as specified in ETSI TS 129 122 [4] which includes updated *selectedPolicy*.

Upon receipt, the IN-CSE updates the *desiredTimeWindow* attribute of the <*backgroundDataTransfer*> resource, with the start and end time of the *timeWindow* attributes of the negotiated policy.

Step 11 (Optional): Issue response to Entity initiating the background data transfer

If more than one transfer policy has been received in step 5, and step 7 has not been performed, the IN-CSE responds to the original background data transfer request from the initiating entity.

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

7.10.3.2 Enabling a Background Data Transfer Policy

Figure 7.10.3.2-1 depicts a general procedure for configuring the negotiated policy in the underlying 3GPP network for the specific field domain nodes (UEs) for which the data transfer will be initiated. This is necessary as the underlying 3GPP network needs to configure its internal nodes so that these may monitor the traffic for these UEs against the negotiated policy. The procedure starts after the procedure of clause 7.10.3.1. This procedure may occur immediately after the procedure of clause 7.10.3.1 or during the time window of the selected policy.

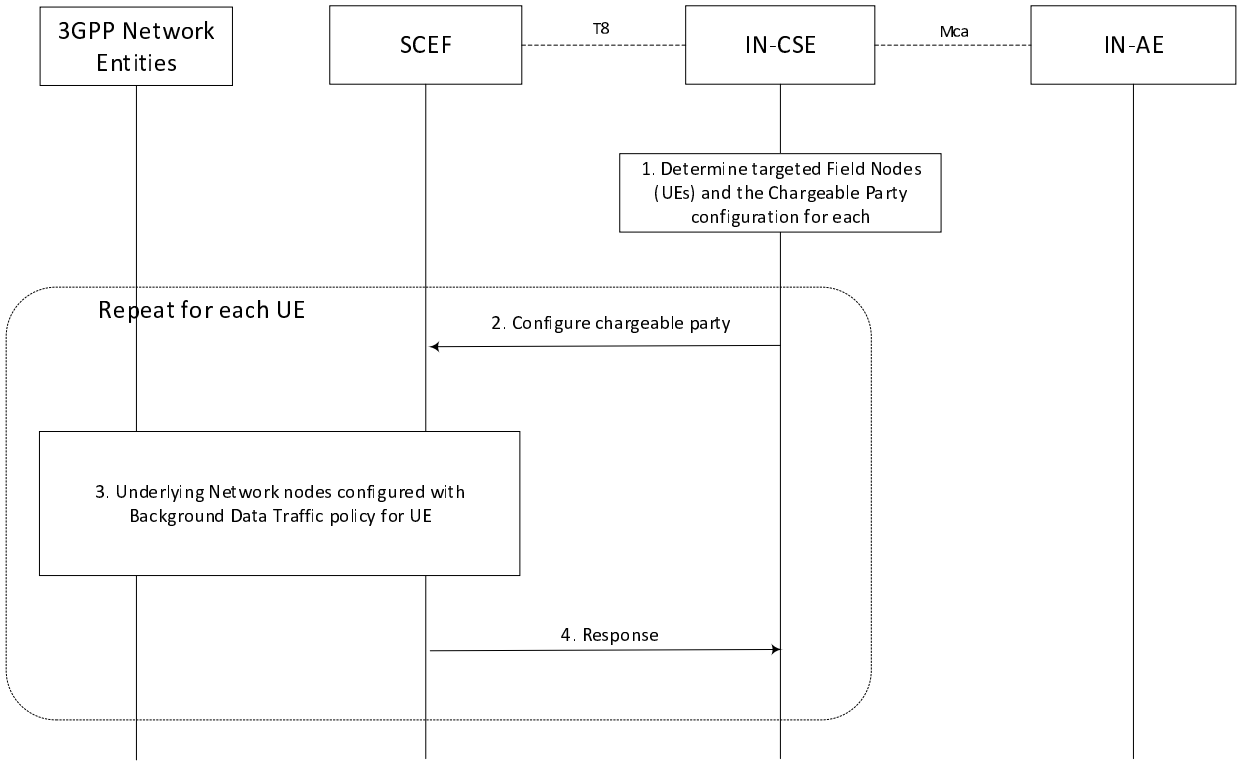

Figure 7.10.3.2-1: General Procedure for Policy Enablement

Step 1: IN-CSE determines the impacted UEs

It is assumed that prior to this procedure the IN-AE a Background Data Transfer has been requested and selected.

The <*backgroundDataTransfer*> resource either with a list of *memberIDs*, or with a link to the <*group*> resource that includes a list of *memberIDs* has been created. During the negotiation, the member list has been used by the IN-CSE to select the SCEF and a single background data transfer policy has been negotiated, for which the IN-CSE received relevant policy information e.g. the start and end time of the policy time window, the maximum aggregated authorized bandwidth for downlink transmission (in bps), and the maximum aggregated authorized bandwidth for uplink transmission (in bps).

Based on this information the IN-CSE or the initiating IN-AE may update the member list with the specific UEs for which the traffic policy enablement is to be performed (e.g. if the negotiated policy time window is different than the one requested, only a subset of the initial member list is used for performing the data transfer).

The IN-CSE uses the *pointOfAccess* for the entities on the member list, to obtain the IP address of the field domain nodes.

Step 2: For each UE, IN-CSE activates the selected transfer policy via the SCEF

For each UE involved in the Background Data Transfer, the IN-CSE triggers the "Change the chargeable party during the session" procedure via SCEF. The IN-CSE identifies each target UE by the IP address of the UE and provides the *referenceID* for the selected policy transfer to the SCEF. The request is configured as follows.

The body of the HTTP POST message shall include SCS/AS Identifier, UE IP address, Flow description, Sponsor ID, ASP ID, Sponsoring Status, time period and/or traffic volume used for sponsoring. The SCS/AS may also request to activate a previously selected policy of background data transfer by including Reference ID in the body of the HTTP POST message:

- An HTTP POST method shall be used.
- *URI* shall be set to {*apiRoot}/3gpp chargeable-party /v1/{scsAsId}/transactions/*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *ChargeableParty* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *supportedFeatures* shall be set to a string value of "0" indicating no support for notifications via Websockets or notification test events.
  - *referenceId* shall be set to *referenceID* of the applicable background data transfer to be applied.
  - *ipv4Addr* shall be set to the IPv4 address (if applicable) configured in the *pointOfAccess* attribute of the target UE hosted ADN-AE or ASN/MN-CSE.
  - *ipv6Addr* shall be set to the IPv6 address (if applicable) configured in the *pointOfAccess* attribute of the target UE hosted ADN-AE or ASN/MN-CSE.
  - *flowInfo* shall be set to provide description of the application flows. Each flow shall include a direction (uplink or downlink), source and destination IP address, protocol, and source and destination ports. Depending on the direction of the flow, the IN-CSE shall configure a source/destination with the IP address and port and of the IN-AE initiating the background data transfer. The IN-CSE shall configure the other destination/source with the IP address and port numbers and of the UE hosted ADN-AE or ASN/MN-CSE. The IN-CSE shall configure the protocol based on the corresponding protocol binding used between the IN-AE and ADN-AE or ASN/MN-CSE.

NOTE 1: To meet 3GPP requirements, the IP Address of the ADN-AE or ASN/MN-CSE is a non NAT'd IP Address and Port Number.

  - *sponsorInformation, sponsoringEnabled* shall be configured by IN-CSE as prearranged between the Service Provider and MNO.
  - *notificationDestination, requestTestNotification, websockNotifConfig* are not supported by the present document.

NOTE 2: How to address the case in which *referenceID* is not provided in the response to the background data transfer request, is outside the scope of the present document and left to implementation.

Step 3: The network is configured by SCEF for the background data transfer

For each UE involved in the Background Data Transfer, the SCEF executes the Change the chargeable party Procedure as described in ETSI TS 129 154 [7].

Via this procedure, the underlying 3GPP network is configured with the traffic policy information and the SCEF is informed for each UE that it has been enabled for background data transfer.

NOTE 3: The MNO will not enforce the maximum aggregated bitrate of a selected transfer policy. However, the MNO can apply offline CDRs processing to determine whether the maximum aggregated bitrate was reached.

Step 4: SCEF acknowledges policy enablement for each UE

The SCEF informs the IN-CSE that the UE has been enabled for background data transfer. If there is more than one UE listed in *memberIDs*, the IN-CSE then moves onto the next UE to enable, and repeats steps 2 to 4.

7.10.3.3 Using Background Data Transfer Policy

Once the transfer policy has been enabled and the time window has arrived, the initiating entity may:

1) use the fanout and group communication procedure to send the same request to each of the field domain nodes configured for background data transfer; or

2) send individual (and potentially different) requests to each of the field domain nodes configured for background data transfer.

NOTE: The data transfers corresponding to this step uses the Sgi interface.

7.10.3.4 Deleting a Background Data Transfer Policy

Figure 7.10.3.4.1-1 depicts a general procedure for deletion of a Background Data Transfer initiated by a request from an IN-AE. The procedure may also be initiated by a request from an MN/ASN-CSE or from the IN-CSE itself.

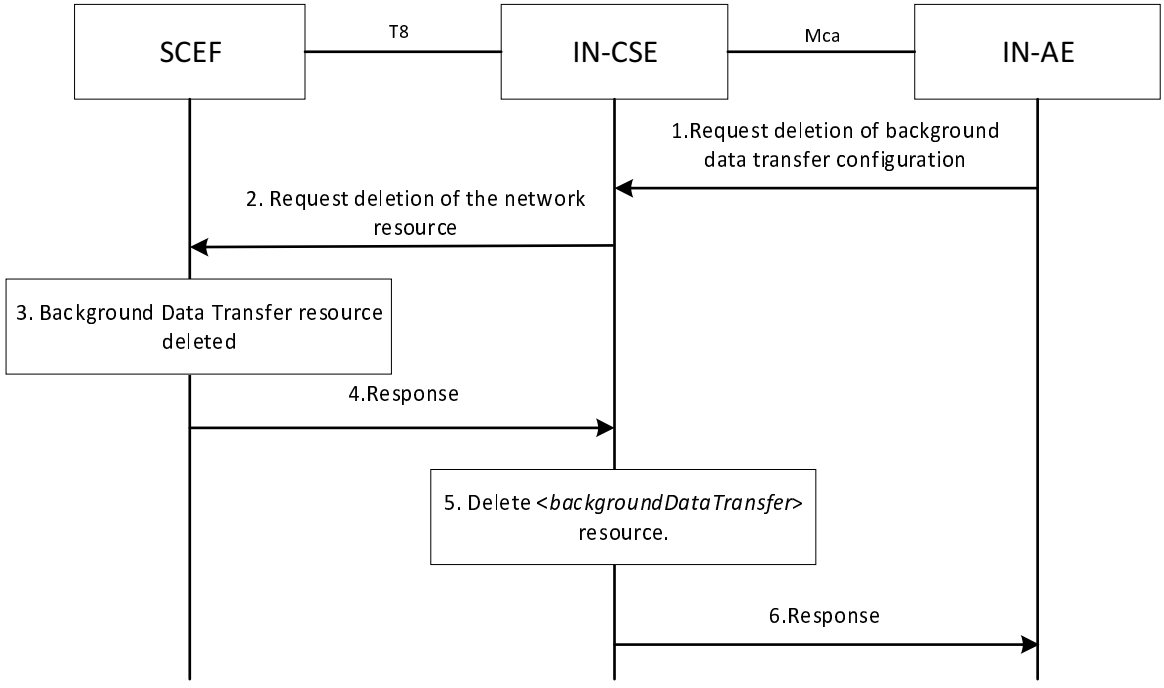

Figure 7.10.3.4-1: General Procedure for deletion of Background Data Transfer

Step 1: Request background data transfer configuration

An IN-AE requests IN-CSE to delete a <*backgroundDataTransfer*> resource.

The request includes:

- The originator AE-ID of the requesting AE.
- A target identifier: i.e. the <*backgroundDataTransfer*> child resource of <*AE*>, <*CSEBase*> or <*remoteCSE*> resource.

Step 2: Request deletion of the Background Data Transfer resource

The IN-CSE selects the SCEF and issues request to delete a Background Data Transfer resource at the SCEF as follows:

- An HTTP DELETE method shall be used.
- *URI* shall be set to *{apiRoot}/3gpp-bdt/v1/{scsAsId}/subscriptions/{subscriptionId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The {*subscriptionId*} corresponds to the one configured by the SCEF and returned to the IN-CSE when the Bdt resource was created at the SCEF.
- The request shall not contain a payload.

Step 3: The SCEF deletes the Background Data Transfer resource

The underlying 3GPP network removes the applicable Background Data Transfer configuration.

Step 4: SCEF Background Data Transfer deletion

The SCEF responds with a 204 NO CONTENT indicating the request was accepted.

Step 5: The IN-CSE deletes the <*backgroundDataTransfer*> resource

The IN-CSE deletes the <*backgroundDataTransfer*> resource based on the procedure specified in clause 10.2.20.5 of ETSI TS 118 101 [1].

Step 6: The IN-CSE responds to Originator

If an AE (e.g. IN-AE) was the Originator of the delete request, the IN-CSE shall return the oneM2M response primitive to the AE.

7.11 Change the chargeable party at session set-up or during the session procedure

Not supported in oneM2M Release 4.

7.12 Network Parameter Configuration

The 3GPP SCEF functionality described in ETSI TS 129 122 [4]. supports an API for Network Parameter Configuration which may be used by the IN-CSE to suggest to the 3GPP Mobile Network specific configuration parameters. The procedure may be used by the IN-CSE to influence certain aspects of UE/network behaviour such as the UE's PSM and extended idle mode DRX. For this purpose, parameter values may be suggested for Maximum Latency and Maximum Response Time for a UE. The Mobile Core Network may choose to accept, reject or modify (via the SCEF) the suggested configuration parameter value.

NOTE: Once the network provides the SCEF with the configured values, the MME could later change the values. For example, the UE can be roaming and the visited network might not allow certain values. In this scenario, the SCEF can request a reachability notification with the Idle Status Indication set to indicate that it wants to be notified of the UE's active timer and periodic TAU/RAU timer when the UE enters the idle state.

In the 3GPP interworking architecture of oneM2M, the UE can host an ADN-AE or an ASN/MN-CSE. The Network Parameter Configuration flow in Figure 7.12-1 takes place after the UE has attached to the underlying 3GPP Network and the ADN-AE or ASN/MN-CSE is registered with the IN-CSE.

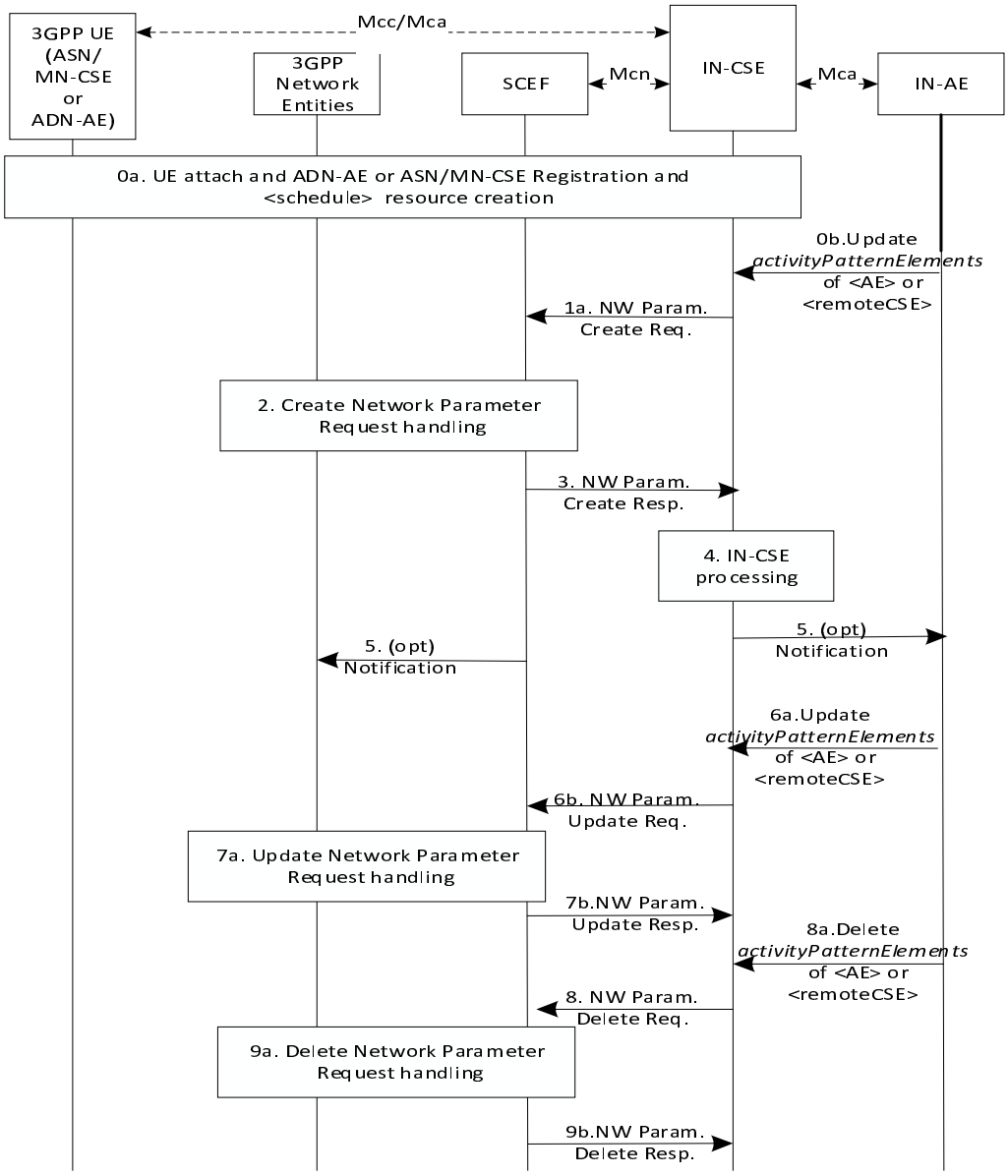

Figure 7.12-1: Network Parameter Configuration flow

Step 0: UE Attach and oneM2M Registration Procedures

The UE attaches to the underlying 3GPP network and the ADN-AE(s) or ASN/MN-CSE hosted on the UE perform the oneM2M registration procedure, as detailed in clause 6.3. The IN-CSE hosts the corresponding <*AE*> or <*remoteCSE*> resources and an associated <*node*> resource for the registree. During this procedure, a <*schedule*> resource is created as child of the <*node*> resource. The UE hosted ADN-AE(s) or ASN/MN may subscribe to the node <*schedule*> resource. If an IN-AE is interested in the reachability status of the UE, it may also subscribe to the <*schedule*> resource.

An ADN-AE, ASN/MN-CSE or IN-AE may configure the *activityPatternElements* attribute of a <*AE*> or <*remoteCSE*> resource with one or more anticipated windows of availability for the corresponding ADN-AE, ASN/MN-CSE. The information contained within the *activityPatternElements* attribute(s) of all ADN-AE(s) and ASN/MN-CSE hosted on the same UE are used by the IN-CSE to configure a network parameter configuration request that is sent to the SCEF.

Step 1: IN-CSE sends to the SCEF a Network Parameter Configuration request

This step is triggered by the creation of one or more <*AE*> or <*remoteCSE*> resources with the *activityPatternElements* attribute set (step 0a) or the modification of one or more of the *activityPatternElements* attributes during an update of the <*AE*> or <*remoteCSE*> resources (step 0b).

The IN-CSE determines the SCEF based on the *M2M-Ext-ID*'s of the registree ASN/MN-CSE or ADN-AEs (e.g. either a DNS lookup on the *M2M-Ext-ID* or the based on the domain portion of the *M2M-Ext-ID*'s.). The IN-CSE provides the network pattern to the SCEF, the fields of the API are populated as follows:

- An HTTP POST method shall be used.
- *URI* shall be set to {*apiRoot*}/3gpp-network-parameter-configuration/v1/{*scsAsId*}/configurations/. The {*apiRoot*} and {*scsAsId*} segments are configured based on Service Provider and MNO policies.
- The request payload shall include a *NpConfiguration* data structure as specified in ETSI TS 129 122 [4] with the following attributes:
  - *externalId* shall be set to M2M-Ext-ID.
  - *supportedFeatures* - shall be set to a string value of "0" indicating no support for notifications over Websockets or notification test events.
  - *maximumLatency* - This value tells the network how long the UE is allowed to sleep. Setting it to 0 will disable PSM, extended idle mode DRX, and S-GW buffering. The IN-CSE shall extract the active periodicity defined in the scheduleElement(s) of all the applicable activityPatternElements attributes of the <AE> resource(s) of the ADN-AE(s) and <remoteCSE> resource of the ASN/MN-CSE hosted by the UE, if configured. The IN-CSE shall set Maximum Latency to be approximately the periodicity of the active periods defined in the scheduleElement(s) of all the applicable activityPatternElements attributes of the <AE> resource(s) of the ADN-AE(s) and <remoteCSE> resource of the ASN/MN-CSE hosted by the UE, if configured. If there is no periodicity it is recommended not to utilize this parameter.
  - *maximumResponseTime* - When the UE uses PSM, Maximum Response Time tells the network how long the UE should stay reachable after a TAU. When the UE uses eDRX, Maximum Response Time is used by the network to determine when to send a reachability notification before a UE's paging occasion. The IN-CSE extracts a duration of activity from the scheduleElement of all the applicable activityPatternElements attributes of the <AE> resource(s) of the ADN-AE(s) and <remoteCSE> resource of the ASN/MN-CSE hosted by the UE, if configured.. The IN-CSE shall set Maximum Response Time to reflect this duration of activity, indicating how long the UE should stay reachable for downlink communications.
  - *notificationDestination* shall be set to a URI that the SCEF can target Network Parameter notifications towards. The value of this URI shall be based on internal IN-CSE policies.
  - *msisdn, externalGroupId, requestTestNotification, groupReportingGuardTime, websockNotifConfig and suggestedNumberOfDlPackets* are not supported by the present document and shall not be included.

General exceptions and error handling

If the SCEF is not reachable when the IN-CSE tries to send Network Parameter Configuration request then the IN-CSE may attempt to retry Network Parameter Configuration requests sometime in the future in case the SCEF does become reachable. The conditions for when the IN-CSE should retry a Network Parameter Configuration request are not defined in the present document.

Steps 2 and 3: Network Parameter Configuration Handling in the underlying 3GPP network

The SCEF processes the request and sends a response to the IN-CSE to acknowledge the request has been accepted. This message is defined in ETSI TS 129 122 [4] and includes the following information:

- A response code of 201 CREATED.
- The *URI* of the Network Parameter Configuration resource created by the SCEF. The *URI* is returned in the HTTP Location header with a format of {*apiRoot*}/3gpp-network-parameter-configuration/v1/{*scsAsId*}/configurations/*{configurationId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{configurationId}* segment is configured by the SCEF.

- The response payload will include a *NpConfiguration* data structure as specified in ETSI TS 129 122 [4] that includes the attributes present in the request along with the following additional attributes. The response may include updated values of *maximumLatency* and *maximumResponseTime* if the network chose to use values that were different than the values that were suggested by the IN-CSE:

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

- If the SCEF does not respond to the IN-CSE or responds with an error response code, the IN-CSE shall assume that the Network Parameter Configuration resource has not been created by the SCEF. Any further creates or updates of *activityPatternElements* attributes for ADN-AE(s) or ASN/MN-CSE hosted on this same UE shall result in a Network Parameter Configuration POST request by the IN-CSE until the SCEF responds with a successful response (201 CREATED).

See clause 8.3 for a list of possible error scenarios and error handling options for the IN-CSE.

Step 4: Network Parameter Configuration Handling at the IN-CSE

The IN-CSE processes information received in the response which may include updated values of *maximumLatency* and *maximumResponseTime* if the network chose to use values that were different than the values that were suggested by the IN-CSE.

Note that IN-CSE shall not update the *activityPatternElements* attribute based on the response received from SCEF. Any further updates to the UE reachability shall be reflected in the <*schedule*> resource.

Step 5 (Optional): If IN-AEs have subscribed to changes in the <*schedule*> resources, a notification will be sent to the subscribers when UE changes it reachability status such as transitioning to connected mode or idle mode. Notifications will also be sent to the UE hosted ADN-AE or ASN-CSE/MN-CSE, if subscriptions to their respective <*schedule*> resources have been created.

Step 6: IN-CSE sends to the SCEF a Network Parameter Configuration update request

Once a Network Parameter Configuration resource has been created by the SCEF for a given UE, the IN-CSE shall keep it updated if any *activityPatternElements* of the ADN-AE(s) or ASN/MN-CSE hosted on the UE are modified or deleted. To perform the update, the IN-CSE shall generate a Network Parameter Configuration update request that contains the following information as specified in ETSI TS 129 122 [4]:

- An HTTP PATCH method shall be used.

- URI shall be set to {*apiRoot*}/3gpp-network-parameter-configuration/v1/{*scsAsId*}/configurations/*{configurationId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{configurationId}* segment is configured by the SCEF and provided to the IN-CSE in the Network Parameter Configuration create response.

- The request payload may include the following parameters:

  - *maximumResponseTime, maximumLatency and suggestedNumberOfDlPackets.*

  - *groupReportGuardTime* is not supported currently and is out of the scope of the present document.

Step 7: SCEF processes the Network Parameter Configuration update request and sends response

SCEF checks whether the maximum latency, maximum response time and suggested number of downlink packets are within the range defined by the MNO policies. SCEF processes the request and sends a response to the IN-CSE to acknowledge that the request has been accepted. The message structure is defined in ETSI TS 129 122 [4]. The SCEF:

- either rejects the request message by sending HTTP response code 403 FORBIDDEN and indicates which parameters are out of range in the problemDetails attribute; or

- accepts the suggested network parameters by sending HTTP response code "200 OK".

The IN-CSE shall not update the *activityPatternElements* attribute based on the response received from the SCEF.

Step 8: IN-CSE sends Network Parameter Configuration Delete request to SCEF

If/when all the *activityPatternElements* for the ADN-AE(s) or ASN/MN-CSE hosted on a given UE are deleted, the IN-CSE shall send a Network Parameter Configuration DELETE request that contains the following information as specified in ETSI TS 129 122 [4]:

- An HTTP DELETE method shall be used.
- URI shall be set to {*apiRoot*}/3gpp-network-parameter-configuration/v1/{*scsAsId*}/configurations//*{configurationId}*. The *{apiRoot}* and *{scsAsId}* segments are configured based on Service Provider and MNO policies. The *{configurationId}* segment is configured by the SCEF and provided to the IN-CSE in the Network Parameter Configuration create response.

Once the Network Parameter Configuration resource for a given UE has been deleted, the IN-CSE shall create a new Network Parameter Configuration create request, using the same procedure described above, if/when an *activityPatternElements* for an ADN-AE or ASN/MN-CSE hosted on the UE is configured.

Step 9: SCEF processes Network Parameter Delete request and sends a response to IN-CSE

The SCEF processes the Network Parameter Delete Request and returns a 204 NO CONTENT response to the IN-CSE.

7.13 Node Schedule Management

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

- A child <*schedule*> resource of the <*node*> resource shall indicate the time periods when the node can communicate via the underlying 3GPP network. If multiple underlying 3GPP networks are supported, for each there can be a maximum of one <*schedule*> resource. One <*schedule*> resource may be used for multiple underlying 3GPP networks.

The *mgmtLink* attribute of the <*cmdhNwAccessRule*> child resource of a <*node*> resource shall link to a <*schedule*> resource that is also a child of the same <*node*> resource.

In the context of 3GPP connectivity technologies, per ETSI TS 123 682 [2], the network reachability and UE reachability are both indications that the UE becomes reachable for receiving either an SMS or downlink data. The SCEF supports the capability to notify the IN-CSE of the network reachable status or the UE reachable status. The IN-CSE shall maintain a <*schedule*> resource of a UE and if the *networkCoordinated* attribute of the <*schedule*> is set to TRUE, then the IN-CSE shall coordinate the schedule based on the UE's reachability. For example, the IN-CSE shall support synchronizing the start time of the *scheduleElement* attribute to be the same as the start time of the targeted UE idle status which the IN-CSE receives from the underlying 3GPP network.

Refer to the clause 9.6.9 Resource Type <*schedule*> of ETSI TS 118 101 [1].

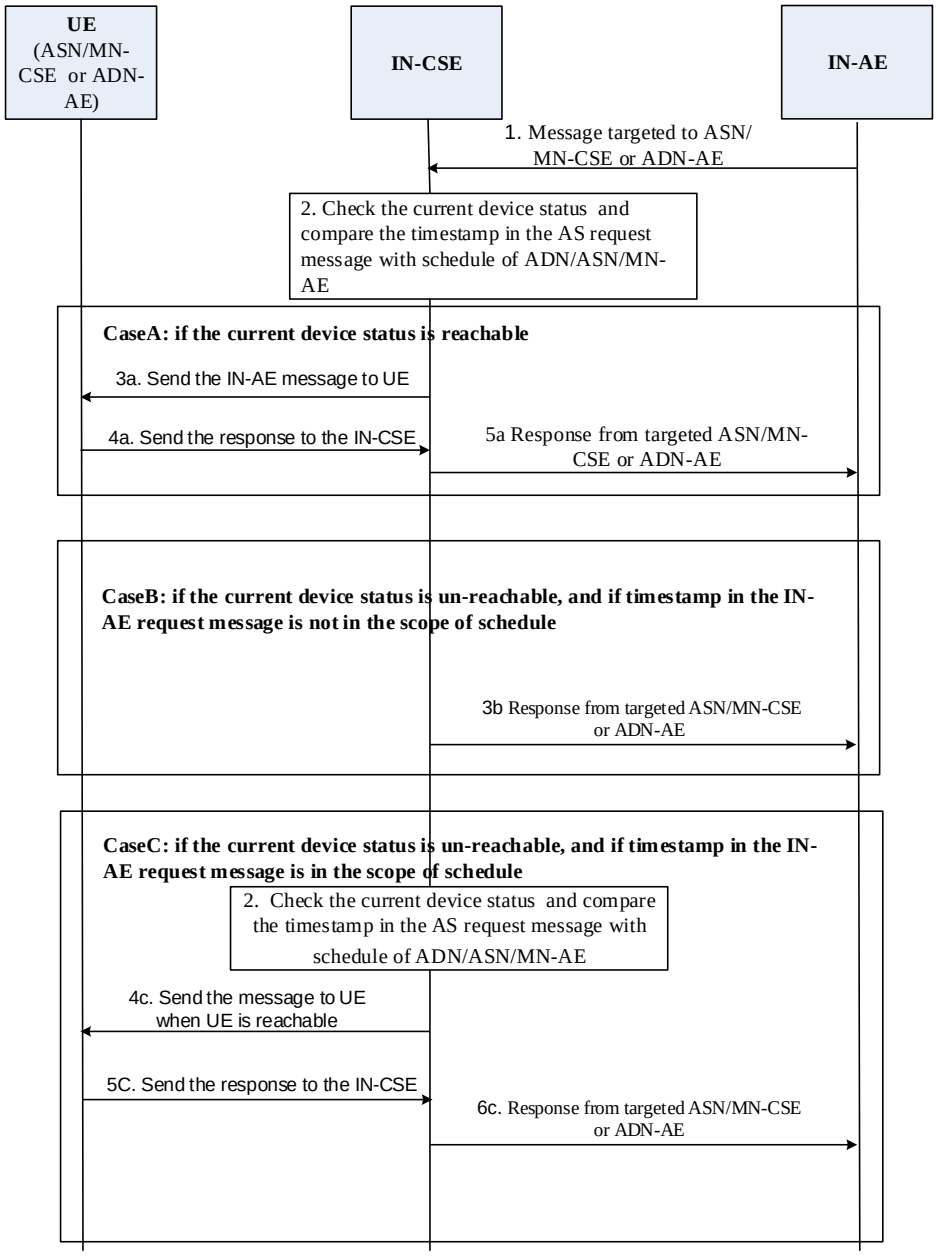

Figure 7.13-1: Targeting UE based on the <*schedule*> of <*node*> resource

Pre-requisites:

- The *M2M-Ext-ID* attribute of <*remoteCSE*> or <*AE*> resource of the targeted UE is pre-configured.
- For the targeted UE, the <*schedule*> resource is a child resource of a <*node*> resource, and the *networkCoordinated* attribute of <*schedule*> is 'True'.

Step 1: The IN-AE sends message to the IN-CSE that targets an ASN/MN-CSE or ADN-AE hosted on a UE. When the message is a request, it shall include the targeted resource identity.

Step 2: IN-CSE checks the local <*schedule*> of the targeted ASN/MN-CSE or ADN-AE node which indicates the pre-defined reachability schedule information of the targeted node according to the target resource identity. The IN-CSE also checks if the *networkCoordinated* attribute of the <*schedule*> resource is TRUE, to determine whether the schedule is coordinated with the UE's underlying 3GPP network schedule. Based on this information, the IN-CSE determines whether the UE is available to receive a request or response message at the current time.

Case A: if the current time is within the period of <*schedule*>, then this indicates the target ASN/MN-CSE's or ADN-AE's current status is reachable and the following steps are applicable:

- **Step 3a:** IN-CSE sends the message to ASN/MN-CSE or ADN-AE directly after CMDH message processing is successful as specified in Annex H in ETSI TS 118 104 [3]; and then continues with the step 4a). Otherwise continues with the step 5a) as specified as in Annex H in ETSI TS 118 104 [3].

- **Step 4a:** The ASN/MN-CSE or ADN-AE sends the response message to the IN-CSE if the message in Step 1 is a request.

- **Step 5a:** IN-CSE sends response message to the IN-AE if the message in Step 1 is a request.

Case B: if the current time is not in the period of <*schedule*>, then this indicates the target ASN/MN-CSE's or ADN-AE's current status is unreachable. The IN-CSE calculates the next reachable start time based on the <*schedule*>, and checks if the ***Operation Execution Time*** or the ***Request Expiration Timestamp*** in the IN-AE request message is earlier than the next reachable start time, or if the ***Operation Execution Time*** or ***Request Expiration Timestamp*** is not configured in the request. If this is the case, then go to Step 3b:

- **Step 3b:** IN-CSE sends error response message to the IN-AE which indicates that the request cannot be delivered to the target ASN/MN-CSE or ADN-AE:

  - If the ***Operation Execution Time*** and ***Request Expiration Timestamp*** are not configured, the ***Response Status Code*** shall be 6003 in Table 6.6.3.7-1 of ETSI TS 118 104 [3].

  - If the ***Request Expiration Timestamp*** is configured, and ***Request Expiration Timestamp*** is earlier than the next reachable start time, the ***Response Status Code*** shall be 6030 in Table 6.6.3.7-1 of ETSI TS 118 104 [3].

  - If the ***Operation Execution Time*** are configured, the ***Operation Execution Time*** is earlier than the next reachable start time, the error information should be the request cannot be delivered to the target resource before ***Operation Execution Time*** expires.

Case C: if the current time is not in the period of <*schedule*>, then this indicates the target ASN/MN-CSE's or ADN-AE's current status is unreachable. The IN-CSE calculates the next reachable start time based on the <*schedule*>, and checks if the ***Operation Execution Time*** and ***Request Expiration Timestamp*** in the IN-AE message are both in the period of <*schedule*>. For example, later than the next reachable start time and earlier than the next end time. If this is the case, then go to Step 3c:

- **Step 3c:** IN-CSE buffers the message until the ASN/MN-CSE or ADN-AE is reachable again.

- **Step 4c:** IN-CSE forwards the message to the target ASN/MN-CSE or ADN-AE before the ***Operation Execution Time*** and ***Request Expiration Timestamp*** expire during the next reachable time after CMDH message processing is successful as specified in Annex H in ETSI TS 118 104 [3]; and then continues with the step 5c). Otherwise continues with the step 6c) as specified as in Annex H in ETSI TS 118 104 [3].

- **Step 5c:** the ASN/MN-CSE or ADN-AE sends the response message to the IN-CSE if the message in Step 1 is a request.

- **Step 6c:** IN-CSE sends the response message to the IN-AE if the message in Step 1 is a request.

7.14 Supported features

7.14.1 General Concepts

The supported features are negotiated separately for each API. For each of the APIs, the applicable list of features is contained in the related API definition defined in ETSI TS 129 122 [4]. The procedure to negotiate applicable features is defined in ETSI TS 129 500 [9]. Each resource for a SCEF API will contain a "*supportedFeatures*" attribute of the SupportedFeatures data type defined in ETSI TS 129 571 [10] containing a bitmask to indicate supported features. The features and their positions in that bitmask are defined separately for each API.

The SCEF/3GPP Network Entities will determine the supported features for the corresponding resource by comparing the supported features indicated by an IN-CSE with the supported features the SCEF/3GPP Network Entities support. The SCEF will include the "*supportedFeatures*" attribute indicating those features in the representation of the resource it returns to the IN-CSE in the response confirming the creation of the resource.

7.14.2 Normal Procedures

This clause introduces normal procedures for a *supportedFeatures*. If a SCEF receives a Monitoring Event Subscription Request for a Monitoring Event with the corresponding *supportedFeatures*, the SCEF sends an HTTP POST response to the IN-CSE with a "201 CREATED" status code as described in ETSI TS 129 122 [4].

Figure 7.14.2.-1 shows an example of the normal procedure for a *supportedFeatures*. A SCEF supports Location Reporting of Monitoring Event API. If an IN-CSE sends a Monitoring Event Subscription Request (*monitoringType* attribute is set to *LOCATION_REPORTING*), the *supportedFeatures* needs to be set to the value of *Location_Notifications* and the SCEF will response the request by sending the above status code.

If the IN-CSE receives the Monitoring Event Subscription Response, the IN-CSE will identify it as a successful response and continue the procedure for the Monitoring Event.

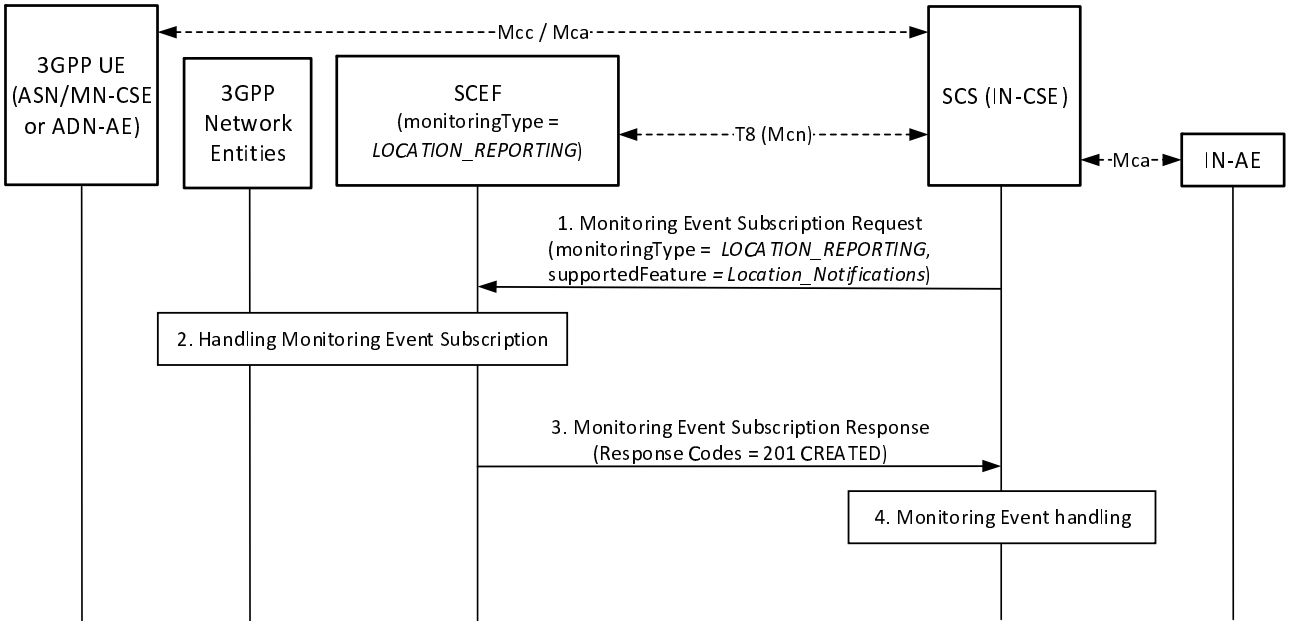

Figure 7.14.2-1: Normal procedures for a *supportedFeatures*

7.15 Network Monitoring Request

7.15.1 Overview

This clause provides details on how an AE (Originator) exchanges with underlying 3GPP network parameters to be used for optimizing the data traffic over the underlying 3GPP network for a set of Field Domain Nodes hosted on UEs. If the AE (Originator) sets the type of network request with the associated attributes such as a geographic area, congestion threshold and External Group ID, the Hosting CSE determines the corresponding T8 API(s) based on the type of network request, maps the attributes to the T8 API(s), and communicates with the SCEF. When the SCEF returns a response to the Hosting CSE, the Hosting CSE maps the response to the specified oneM2M resource and sends a response to the AE (Originator). Based on the information, the AE (Originator) may adjust data processing/transfer for the Field Domain Nodes (ASN/MN/ADN).

7.15.2 Resource Structure

Refer to clause 9.6.64 Resource Type <*nwMonitoringReq*> of ETSI TS 118 101 [1].

7.15.3 Procedures

7.15.3.0 Introduction

This clause describes procedures to retrieve an underlying 3GPP network information in a particular geographic area initiated by a request from an AE. The following T8 APIs are applicable for this procedure:

- Network Status Reports API.
- Monitoring Event API (Monitoring Type: Number of UEs in an Area).

7.15.3.1 Procedure for Network Status Reports API

Figure 7.15.3.1-1 depicts a procedure to retrieve an underlying 3GPP network information in a particular geographic area with Network Status Reports API.

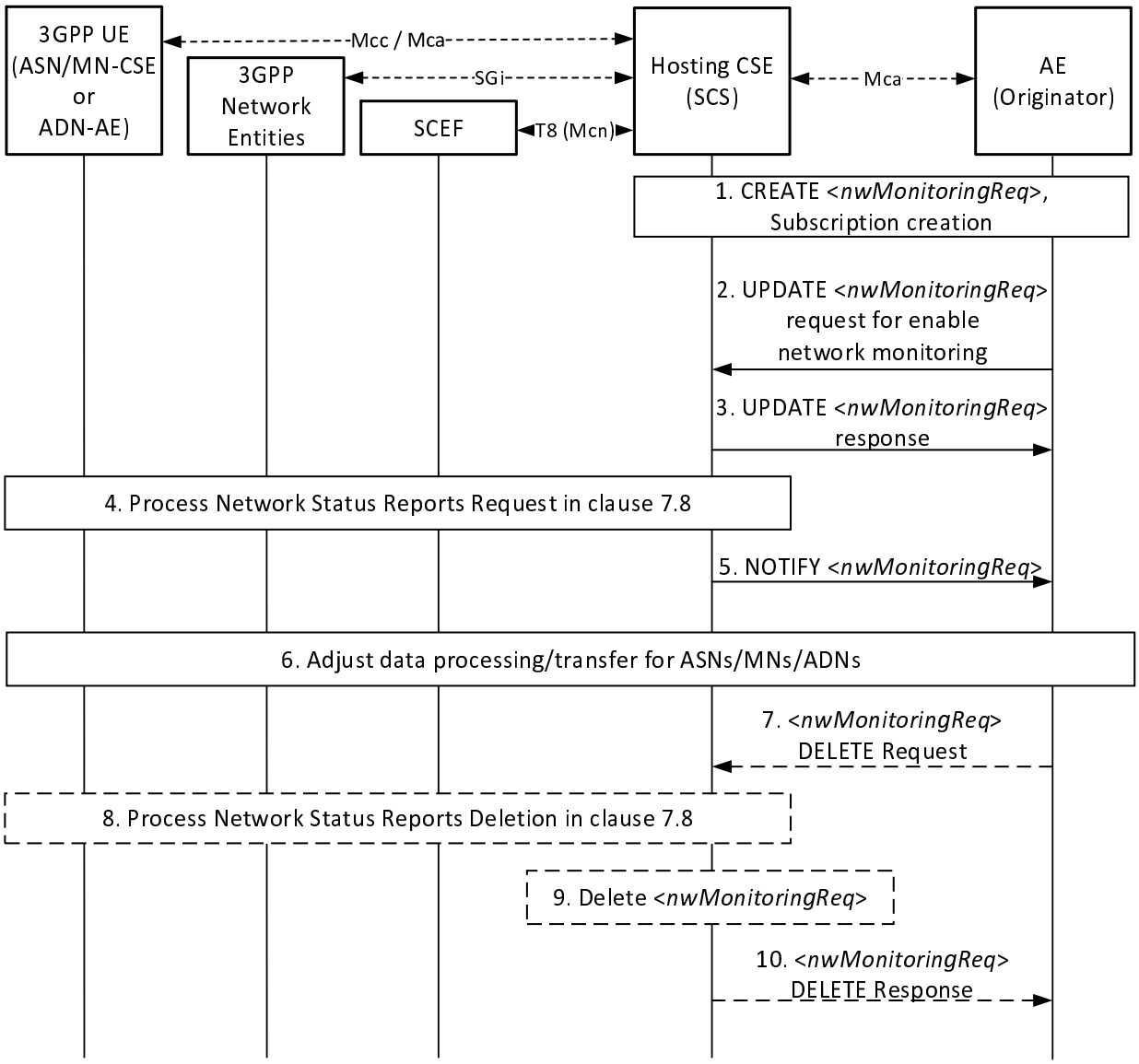

Figure 7.15.3.1-1: Procedure for Network Status Reports API

Pre-conditions:

There is a relationship in place between the Service Provider and MNO allowing the AE (Originator) to request 3GPP T8 API information from the underlying 3GPP network. The method for establishing this relationship is outside the scope of the present document.

The Hosting CSE is configured with system defaults as described in clause 7.8 and/or clause 7.4.8.

Step 1: CREATE <*nwMonitoringReq*> Request & Response, Subscription creation

An Originator (AE) requests the creation of a <*nwMonitoringReq*> resource at the Hosting CSE. The request shall include the following parameter as specified in clause 9.6.64 of ETSI TS 118 101 [1]:

- *monitorStatus* shall be set to DISABLED.

If the operation is successful, the Originator receives a response message. And the Originator shall subsequently create the <*subscription*> resource as the child of the <*nwMonitoringReq*> resource to get notified of network monitoring status.

Step 2: UPDATE <*nwMonitoringReq*> Request for enable network monitoring

In order to initiate a monitoring request**,** the Originator sends a request to update the *monitorEnable* attribute of the <*nwMonitoringReq*> resource:

- *monitorEnable* shall be set to MonitorCongestion.
- *geographicArea* shall be set to the geographic area where the Originator wants to retrieve an underlying 3GPP network information.
- *congestionLevel* shall be set to one of following values:
  - The list of congestion level(s) with exact value and specify what congestion threshold(s) the Originator wants to receive a report for.
  - The list of enumerated types with values HIGH, MEDIUM and LOW that specify the type of congestion status the Originator would like to receive a report for.

If the value of *monitorStatus* is set to ENABLED, the Originator shall not send an UPDATE request.

Step 3: UPDATE <*nwMonitoringReq*> Response

The Hosting CSE shall update the <*nwMonitoringReq*> resource and return a response to the Originator.

If the value of *monitorEnable* is MonitorCongestion, the Hosting CSE shall check if *congestionLevel* attribute and *geographicArea* attribute are included in the request:

- If the attributes are present, the Hosting CSE shall set the value of *monitorStatus* to ENABLED, and the subsequent Update procedures of the Hosting CSE shall be performed for the resource.
- If the attributes are not present, the Hosting CSE shall not process the request and shall return a response primitive with a ***Response Status Code*** indicating "BAD_REQUEST" error.

If the value of *monitorStatus* is ENABLED, the Hosting CSE shall reject the request with a ***Response Status Code*** indicating "CONFLICT" error.

If the Hosting CSE receives a request for deletion of *monitorEnable* attribute, the Hosting CSE shall set the value of *monitorStatus* to DISABLED.

Step 4: Process Network Status Reports Request

The Hosting CSE shall map the attributes of the <*nwMonitoringReq*> resource to the following attributes of Network Status Reports API as described in clause 7.8:

- The Hosting CSE shall set the fixed parameters with the corresponding attributes of the API (e.g. *URI, monitorExpireTime, supportedFeatures*).
- *geographicArea* of the <*nwMonitoringReq*> resource shall be set to *locationArea*.
- If the *congestionLevel* of the <*nwMonitoringReq*> resource indicates an abstracted value for congestion level(s) (e.g. HIGH, MEDIUM or LOW), *thresholdTypes* shall be set to the abstracted value of the *congestionLevel*. If *congestionLevel* indicates an exact value for congestion level(s) (e.g. between 0 and 31), *thresholdValues* shall be set to the exact value of the *congestionLevel.*

Then the Hosting CSE shall send a Network Status Report request to the SCEF, and the SCEF sends a Network Status Report response to the Hosting CSE as described in clause 7.8.

Step 5: NOTIFY<*nwMonitoringReq*>

The Hosting CSE sends a notification request of <*nwMonitoringReq*> resource to the Originator. The notification is configured as follows:

- After receiving a Network Status Report Notification request from the SCEF, the Hosting CSE shall map the following attributes of the Network Status Reports API described in clause 7.8 to the attribute of the <*nwMonitoringReq*> resource:
  - nsiValue or nsiType shall be set to the congestionStatus of the <nwMonitoringReq> resource.

If the Hosting CSE receives an error response from the SCEF, the Hosting CSE shall set the value of *monitorStatus* to FAILED, and shall map the error response code to the corresponding value of *failureReason*. Then, the Hosting CSE shall send a notification request of <*nwMonitoringReq*> resource to the Originator. Each error response code is configured as follows:

- 400 Bad Request shall be set to BAD_REQUEST.
- 401 Unauthorized shall be set to UNAUTHORIZED.
- 403 Forbidden shall be set to FORBIDDEN.
- 404 Not Found shall be set to NOT_FOUND.
- 411 Length Required shall be set to LENGTH_REQUIRED.
- 413 Payload Too Large shall be set to PAYLOAD_TOO_LARGE.
- 415 Unsupported Media Type shall be set to UNSUPPORTED_MEDIA_TYPE.
- 429 Too Many Requests shall be set to TOO_MANY_REQUESTS.
- 500 Internal Server Error shall be set to INTERNAL_SERVER_ERROR.
- 503 Service Unavailable shall be set to SERVICE_UNAVAILABLE.

Step 6: The Originator adjusts data processing/transfer for Field Domain Nodes (ASN/MN/ADN)

The Originator may use the information provided in step 4 in order to adjusts data processing/transfer for Field Domain Nodes (ASN/MN/ADN).

If the value of *failureReason* is set to FORBIDDEN, the Originator may be configured with the values (e.g. *congestionLevel*,*geographicArea*) within the range defined by MNO policies.

If the value of *failureReason* is set to PAYLOAD_TOO_LARGE, the Originator may retry the request without optional attribute(s).

If the value of *failureReason* is set to TOO_MANY_REQUESTS, the Originator may reduce the frequency of requests or avoid immediate retries.

Step 7 (Optional): DELETE <*nwMonitoringReq*> Request

The Originator sends a request to delete the <*nwMonitoringReq*> resource.

Step 8 (Optional): Process deletion of Network Status Reports

The Hosting CSE shall send a DELETE request of the Network Status Reports API to the SCEF as described in clause 7.8.

Step 9 (Optional): The Hosting CSE deletes the <*nwMonitoringReq*> resource

If in step 8 the Hosting CSE receives a 204 No Content response code from the SCEF, the Hosting CSE shall delete the <*nwMonitoringReq*> resource. Otherwise, the Hosting CSE shall not delete the <*nwMonitoringReq*> resource.

Step 10 (Optional): The Hosting CSE returns response to the Originator

The Hosting CSE shall send a DELETE response back to the Originator.

7.15.3.2 Procedure for Monitoring Event API (Monitoring Type: Number of UEs in an Area)

Figure 7.15.3.2-1 depicts a procedure to retrieve an underlying 3GPP network information in a particular geographic area with Monitoring Event API (Monitoring Type: Number of UEs in an Area).

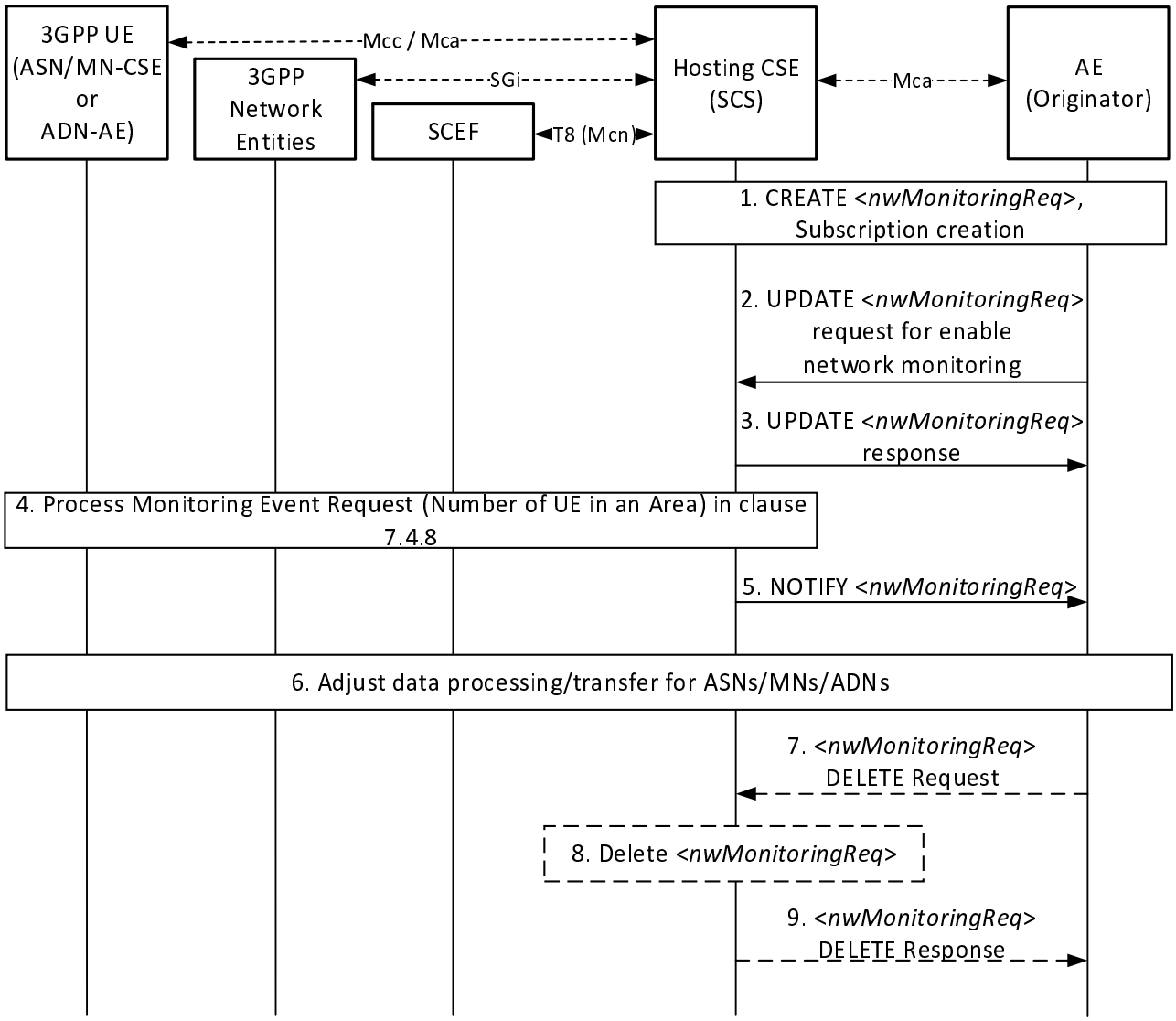

Figure 7.15.3.2-1: Procedure for Monitoring Event API (Monitoring Type: Number of UEs in an Area)

Pre-conditions

There is a relationship in place between the Service Provider and MNO allowing the AE (Originator) to request 3GPP T8 API information from the underlying 3GPP network. The method for establishing this relationship is outside the scope of the present document.

If the deployment uses External Group Identifier (*externalGroupId*) as described in ETSI TS 129 122 [4], when ASN/MN-CSEs or ADN-AEs register with the Hosting CSE (SCS), then they use *externalGroupId* information to configure the *externalGroupID* of the corresponding <*remoteCSE*> or <*AE*> resources (see clause 6.3 when *externalGroupID* is configured).

The Hosting CSE is configured with system defaults as described in clause 7.4.8.

Step 1: CREATE <*nwMonitoringReq*> Request & Response, Subscription creation

An Originator (AE) requests the creation of a <*nwMonitoringReq*> resource at the Hosting CSE. The request shall include the following parameter as specified in clause 9.6.64 of ETSI TS 118 101 [1]:

- *monitorStatus* shall be set to DISABLED.

If the operation is successful, the Originator receives a response message. And the Originator shall subsequently create the <*subscription*> resource as the child of the <*nwMonitoringReq*> resource to get notified of network monitoring status.

Step 2: UPDATE <*nwMonitoringReq*> Request for enable network monitoring

In order to initiate a monitoring request**,** the Originator sends a request to update the *monitorEnable* attribute of the <*nwMonitoringReq*> resource:

- *monitorEnable* shall be set to MonitorDeviceNumber.
- *geographicArea* shall be set to the geographic area where the Originator wants to retrieve an underlying 3GPP network information.
- *externalGroupID* shall be set to the group of interest in the request, in which case the Monitoring Event Request is for the number of group-member UEs present in the area of interest.

If the value of *monitorStatus* is set to ENABLED, the Originator shall not send an UPDATE request.

Step 3: UPDATE <*nwMonitoringReq*> Response

The Hosting CSE shall update the <*nwMonitoringReq*> resource and return a response to the Originator.

If the value of *monitorEnable* is MonitorDeviceNumber, the Hosting CSE shall check if *geographicArea* attribute is included in the request:

- If the attribute is present, the Hosting CSE shall set the value of *monitorStatus* to ENABLED, and the subsequent Update procedures of the Receiver shall be performed for the resource.
- If the attribute is not present, the Hosting CSE shall not process the request and shall return a response primitive with a ***Response Status Code*** indicating "BAD_REQUEST" error.

If the value of *monitorStatus* is ENABLED, the Hosting CSE shall reject the request with a ***Response Status Code*** indicating "CONFLICT" error.

If the Hosting CSE receives a request for deletion of *monitorEnable* attribute, the Hosting CSE shall set the value of *monitorStatus* to DISABLED.

Step 4: Process Monitoring Event (Number of UEs in an area) Request

The Hosting CSE shall map the attributes of the <*nwMonitoringReq*> resource to the following attributes of Monitoring Event API (Number of UEs in an area) as described in clause 7.4.8:

- The Hosting CSE shall set the fixed parameters with the corresponding attributes of the API (e.g. *URI, supportedFeatures*).
- *geographicArea* of the <*nwMonitoringReq*> resource shall be set to *locationArea*.
- *externalGroupID* of the <*nwMonitoringReq*> resource shall be set to *externalGroupId* if in step 2 the Hosting CSE monitoring request targets identifying the number of UEs from a specific group in the area and the Hosting CSE determined an *externalGroupID* to be monitored.

Then the Hosting CSE shall send a Monitoring Event request to the SCEF as described in clause 7.4.8.

Step 5: NOTIFY <*nwMonitoringReq*>

The Hosting CSE sends a notification request of <*nwMonitoringReq*> resource to the Originator. The notification is configured as follows:

- After receiving a Monitoring Event response from the SCEF, the Hosting CSE shall map the following attributes of the Monitoring Event API described in clause 7.4.8 to the attributes of the <*nwMonitoringReq*> resource:
  - *ueCount* shall be set to the *numberOfDevices* of the <*nwMonitoringReq*> resource. If an *externalGroupId* has been provided in the request, the count indicates the number of UEs from the given group which are found at the location.
  - *externalIds* shall be set to *M2M-Ext-ID* attribute of the <*nwMonitoringReq*> resource, if an *externalGroupId* has been provided in the request.

If the Hosting CSE receives an error response from the SCEF, the Hosting CSE shall set the value of *monitorStatus* to FAILED, and shall map the error response code to the corresponding value of *failureReason*. Then, the Hosting CSE shall send a notification request of <*nwMonitoringReq*> resource to the Originator. Each error response code is configured as follows:

- 400 Bad Request shall be set to BAD_REQUEST.
- 401 Unauthorized shall be set to UNAUTHORIZED.
- 403 Forbidden shall be set to FORBIDDEN.
- 404 Not Found shall be set to NOT_FOUND.
- 411 Length Required shall be set to LENGTH_REQUIRED.
- 413 Payload Too Large shall be set to PAYLOAD_TOO_LARGE.
- 415 Unsupported Media Type shall be set to UNSUPPORTED_MEDIA_TYPE.
- 429 Too Many Requests shall be set to TOO_MANY_REQUESTS.
- 500 Internal Server Error shall be set to INTERNAL_SERVER_ERROR.
- 503 Service Unavailable shall be set to SERVICE_UNAVAILABLE.

Step 6: The Originator adjusts data processing/transfer for Field Domain Nodes (ASN/MN/ADN)

The Originator may use the information provided in Step 5 in order to adjusts data processing/transfer for Field Domain Nodes (ASN/MN/ADN).

If the value of *failureReason* is set to FORBIDDEN, the Originator may be configured with the values (e.g. *geographicArea*) within the range defined by MNO policies.

If the value of *failureReason* is set to PAYLOAD_TOO_LARGE, the Originator may retry the request without optional attribute(s).

If the value of *failureReason* is set to TOO_MANY_REQUESTS, the Originator may reduce the frequency of requests or avoid immediate retries.

Step 7 (Optional): DELETE <*nwMonitoringReq*> Request

The Originator sends a request to delete the <*nwMonitoringReq*> resource.

Step 8 (Optional): The Hosting CSE deletes the <*nwMonitoringReq*> resource

The Hosting CSE shall delete the <*nwMonitoringReq*> resource.

Step 9 (Optional): The Hosting CSE returns response to the Originator.

The Hosting CSE shall send a DELETE response back to the Originator.

7.16 Interworking with ASN/MN-CSE(SCS)

7.16.1 Overview

The clause introduces the interworking procedures between an ASN/MN-CSE (SCS) and an SCEF via T8 APIs.

7.16.2 Procedures

7.16.2.1 Cellular IoT non-IP data delivery (NIDD)

N/A.

7.16.2.2 UE Reachability monitoring of Monitoring events

The procedure with IN-CSE is depicted in clause 7.4.1. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.3 UE Availability after DDN Failure of Monitoring events

The procedure with IN-CSE is depicted in clause 7.4.2. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.4 UE Communication Failure of Monitoring events

The procedure with IN-CSE is depicted in clause 7.4.3. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.5 UE Loss of Connectivity of Monitoring events

The procedure with IN-CSE is depicted in clause 7.4.4. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.6 Roaming Status of Monitoring events

The procedure is depicted in clause 7.4.5. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.7 Detecting Change of IMSI-IMEI(SV) Association of Monitoring events

The procedure with IN-CSE is depicted in clause 7.4.6. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.8 Location Reporting of Monitoring events

The procedure with IN-CSE is depicted in clause 7.4.7. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.9 Number of UEs in an Area of Monitoring events

The procedure with IN-CSE is depicted in clause 7.4.8. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.10 3GPP Based Device triggering

The procedure with IN-CSE is depicted in clause 7.5. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.11 Configuration of Traffic Patterns

The procedure with IN-CSE is depicted in clause 7.6. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.12 Group message delivery using MBMS

N/A.

7.16.2.13 Informing about Potential Network Issues

The procedure with IN-CSE is depicted in clause 7.8. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.14 Setting up an AS session with required QoS procedure

The procedure with IN-CSE is depicted in clause 7.9. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.15 Background Data Transfer

The procedure with IN-CSE is depicted in clause 7.10. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

7.16.2.16 Network Parameter Configuration

The procedure with IN-CSE is depicted in clause 7.12. In this procedure, the ASN/MN-CSE functions as a SCS and the procedure related to IN-CSE is replaced by the ASN/MN-CSE (SCS).

8 3GPP T8 Protocol Binding Details

8.1 Transport Protocol Binding

An IN-CSE that interworks to a 3GPP SCEF via the T8 reference point shall support sending and receiving of requests and responses that are compliant with the HTPP-based T8 protocol specified by ETSI TS 129 122 [4]. Where needed, the present document specifies the binding of the informational elements defined by the T8 protocol and the oneM2M protocol. The present document also specifies the additional actions (i.e. procedures) that the IN-CSE performs with respect to each of the T8 supported features. These actions further complement and provide additional value-added services over top of the 3GPP T8 capabilities.

8.2 Schemas

ETSI TS 129 122 [4] defines JSON-based schemas based on the OpenAPI 3.0.0. specification [6] for each type of request and response that flows over the T8 reference point. An IN-CSE that complies with the present document and interworks to the 3GPP SCEF T8 reference point shall support encoding and decoding of T8 messages per the ETSI TS 129 122 [4] defined JSON schemas.

For the cases where a oneM2M defined primitives is encapsulated within a T8 request or response, the encapsulated oneM2M primitive shall comply with the corresponding oneM2M defined schema. For example, a oneM2M request or response primitive that is encapsulated within the *data* attribute of a *NiddDownlinkDataTransfer* or *NiddUplinkDataNotification* request element.

8.3 Error Handling

8.3.1 Overview

An IN-CSE that interworks to a 3GPP SCEF via the T8 reference point shall support handling the following types of error conditions:

1) Unavailable SCEF - If the IN-CSE sends a request to the SCEF, but the SCEF does not respond back, the IN-CSE shall be robust to this scenario. At a minimum, the IN-CSE shall support timing out the request. The IN-CSE may support retrying requests but these details are out of scope of the present document.

2) Errors returned by the SCEF to the IN-CSE within T8 responses - Table 8.3.1-1 provides a list of the supported T8 mandatory error response codes applicable to all T8 APIs defined by ETSI TS 129 122 [4]. -40x response codes indicate a problem due to malformed requests from the IN-CSE that need to be addressed. -50x response codes typically indicate a problem with the SCEF that needs to be addressed.

Table 8.3.1-1: T8 Error response codes

Response Codes	Remarks
400 Bad Request	Incorrect parameters were passed in the request issued by the IN-CSE.
401 Unauthorized	The IN-CSE is not authorized to issue request to SCEF.
403 Forbidden	This represents the case when the SCEF is able to understand the request but unable to fulfil the request due to errors (e.g. the requested parameters are out of range).
404 Not Found	The resource URI was incorrect, for instance because of a wrong "scsAsId" field.
411 Length Required	The code indicates that the SCEF refuses to accept the request without a Content-Length header field.
413 Payload Too Large	The request contains a payload larger than the SCEF is able to process.
415 Unsupported Media Type	The code indicates that the resource is in a format which is not supported by the SCEF for the method.
429 Too Many Requests	The code indicates that due to excessive traffic which, if continued over time, may lead to (or may increase) an overload situation. The HTTP header field "Retry-After" may be added in the response to indicate how long the IN-CSE has to wait before making a new request.
500 Internal Server Error	The SCEF encountered an unexpected condition that prevented it from fulfilling the request.
503 Service Unavailable	The SCEF is unable to handle the request.

NOTE: Depending on the specific procedure, the IN-CSE performs different error handling actions. These procedure specific error-handling actions are defined in the respective clauses of the present document.

8.3.2 Error handling for Monitoring events

8.3.2.1 Internal Server Error

If a SCEF receives a Monitoring event request to create a subscription resource for a monitoring event that it does not support, the SCEF will reject the request by sending a "500 Internal Server Error" HTTP error response with the application error "EVENT_UNSUPPORTED".

Figure 8.3.2.1-1 shows an example of the error handling procedure for the case where the SCEF doesn't support the event requested by the SCS (IN-CSE). The SCEF supports the monitoring type of UE Reachability and does not support the monitoring type of Location Reporting. If an IN-CSE sends a Monitoring Event Subscription Request with the monitoring type of Location Reporting, the SCEF will reject the request by sending the above error response with the application error.

If the IN-CSE receives the error response from the SCEF, the IN-CSE may obtain the location information of an ASN/MN-CSE or ADN-AE by using Device-based method or Sharing-based method configured with *locationSource* attributes of <*locationPolicy*> resource based on the IN-CSE local policy.

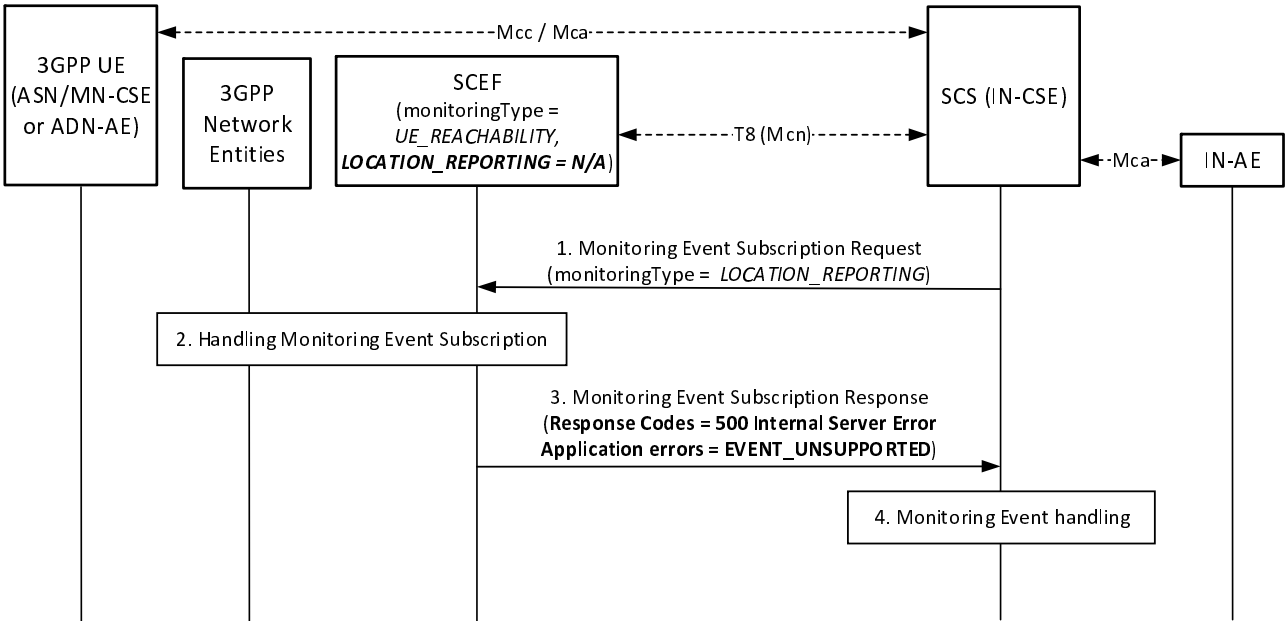

Figure 8.3.2.1-1: Error handling procedures for Location Reporting of Monitoring events

Figure 8.3.2.1-2 shows another example of the error handling procedure. The SCEF supports the monitoring type of UE Reachability and does not support the monitoring type of UE Loss of Connectivity. If an IN-CSE sends a Monitoring Event Subscription Request with the monitoring type of UE Loss of Connectivity, the SCEF will reject the request by sending the above error response with the application error.

If the IN-CSE receives the error response from the SCEF, the IN-CSE may retry the request with the monitoring type of UE Reachability for managing unreachable devices, based on the IN-CSE local policy.

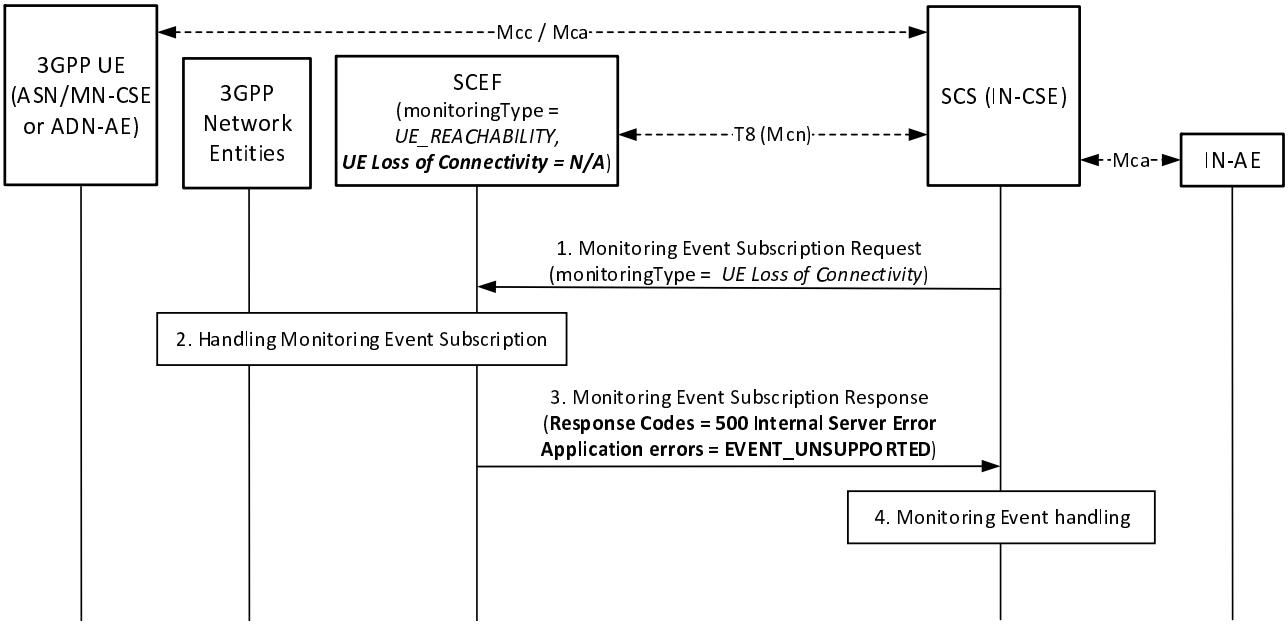

Figure 8.3.2.1-2: Error handling procedures for UE Loss of Connectivity of Monitoring events

8.3.2.2 Forbidden

If a SCEF receives a Monitoring event request to create a subscription resource, the SCEF will check whether the parameters (e.g. Maximum Number of Reports) in the request body are within the range defined by MNO policies. If one or more of these parameters are not within the range, the SCEF may reject the request by sending a "403 Forbidden" HTTP error response with the application error "PARAMETER_OUT_OF_RANGE".

Figure 8.3.2.2-1 shows an example of the error handling procedure. The SCEF supports the monitoring type of Communication Failure and *maximumNumberOfReports* parameter is set to "10" defined by MNO policies. If an IN-CSE sends a Monitoring Event Subscription Request for Communication Failure with *maximumNumberOfReports* parameter set to "20", the SCEF will reject the request by sending the above error response with the application error.

If the IN-CSE receives the error response from the SCEF, the IN-CSE may retry the request with the parameters set within the range (e.g. 8), based on the IN-CSE local policy.

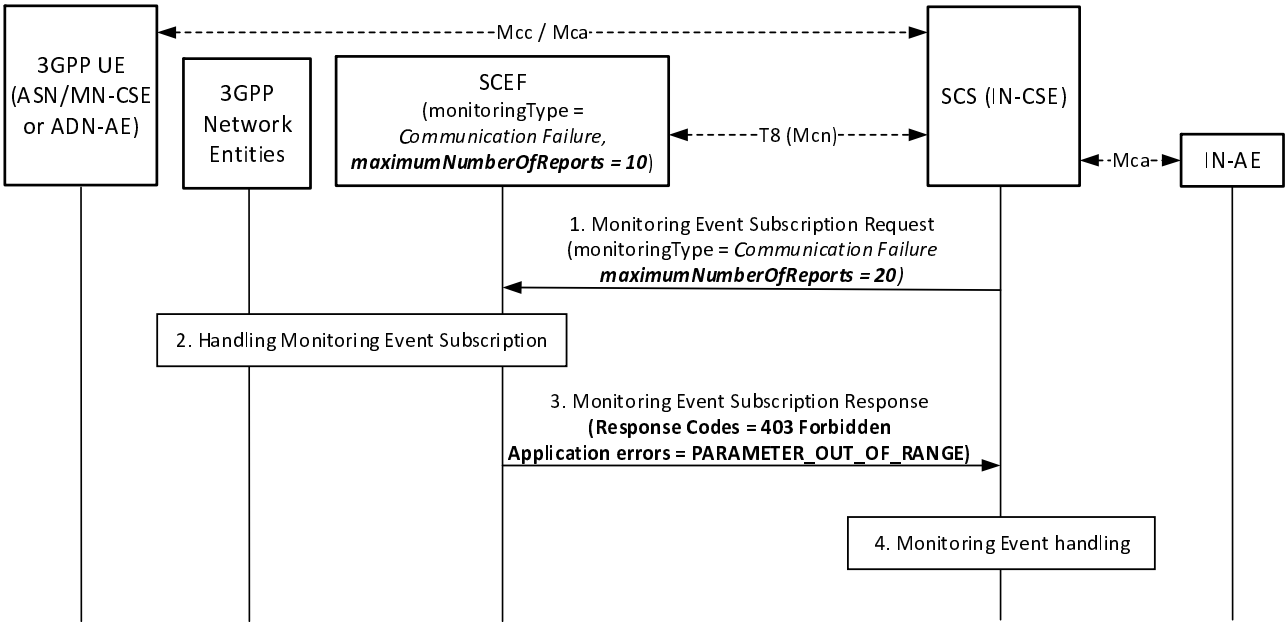

Figure 8.3.2.2-1: Error handling procedures for Communication Failure of Monitoring events

If the SCEF receives a Monitoring event request to create a subscription resource, the SCEF will check whether the Idle Status Indication is included for UE reachability event. If the Idle Status Indication is received in the request but not supported by the network, the SCEF may reject the request by sending a "403 Forbidden" HTTP error response with the application error "IDLE_STATUS_UNSUPPORTED" in the "cause" attribute of the "ProblemDetails" structure.

Figure 8.3.2.2-2 shows an example of the error handling procedure. The SCEF supports the monitoring type of UE Reachability and does not support to send notifications to an IN-CSE when the UE transitions into PSM idle mode, connected mode or receives an eDRX paging occasion. If the IN-CSE sends a Monitoring Event Subscription Request for UE Reachability with *idleStatusIndication* parameter set to "TRUE", the SCEF will reject the request by sending the above error response with the application error.

If the IN-CSE receives the error response from the SCEF, the IN-CSE may retry the request with *idleStatusIndication* parameter set to "FALSE" for one-time monitoring request, based on the IN-CSE local policy.

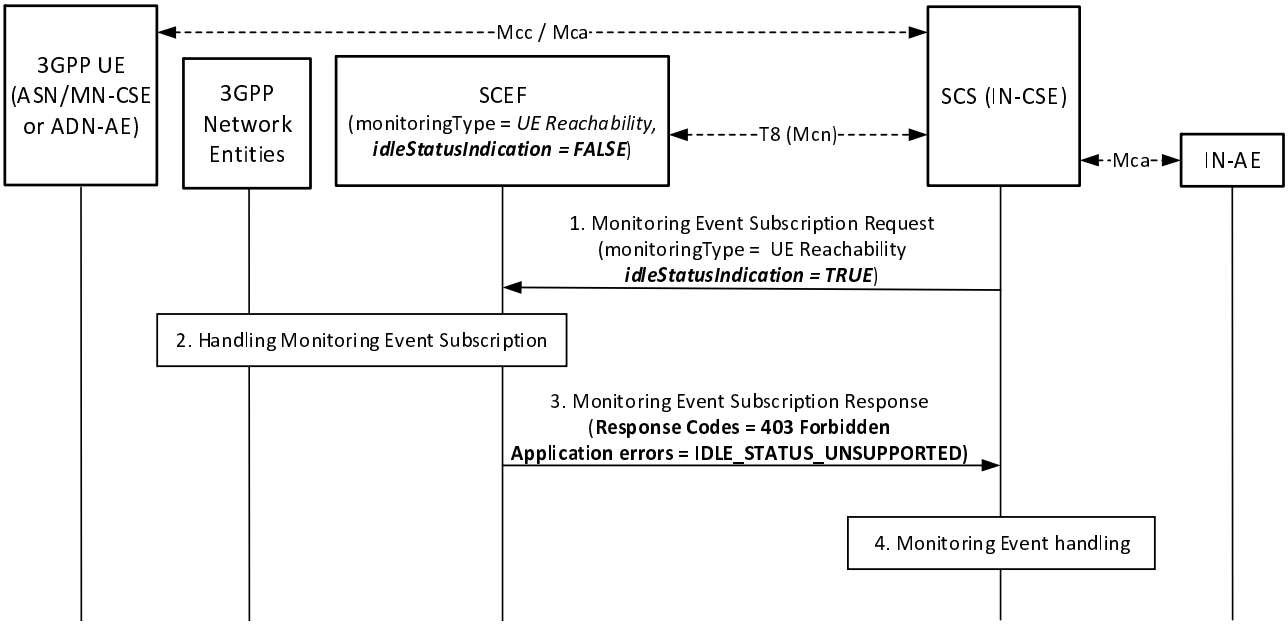

Figure 8.3.2.2-2: Error handling procedures for UE Reachability of Monitoring events

8.3.2.3 Bad Request

If a SCEF receives a request from an IN-CSE, but without an indication of the support for the feature, the SCEF will ignore the feature or reject the request by sending an error response. The response from the SCEF is different depending on the type of *supportedFeatures.*

This clause introduces error handling procedures for a mandatory *supportedFeatures*. If a SCEF receives a Monitoring Event Subscription Request for a Monitoring Event, but without an indication of the support for the feature corresponding to the Monitoring Event, the SCEF will reject the request by sending a 400 "Bad Request" HTTP error response with the application error "EVENT_FEATURE_MISMATCH".

Figure 8.3.2.3-1 shows an example of the error handling procedure for a mandatory *supportedFeatures*. A SCEF supports Location Reporting of Monitoring Event API. If an IN-CSE sends a Monitoring Event Subscription Request (*monitoringType* is set to *LOCATION_REPORTING*, *supportedFeature* is set to a value of *Roaming Status Notification*), the SCEF will reject the request by sending the above error response with the application error. Because the feature corresponding to the event type of Monitoring Event needs to be set to the value of *Location Notifications*.

If the IN-CSE receives the error response from the SCEF, the IN-CSE may retry the request with the value of *Location _Notifications*.

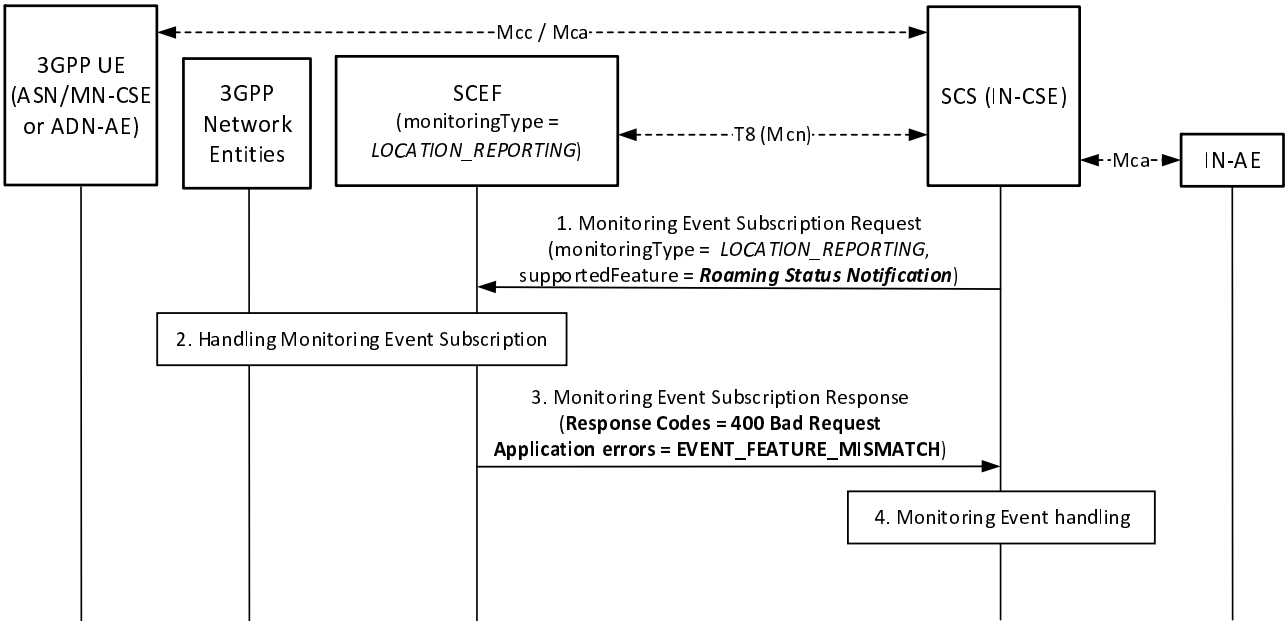

Figure 8.3.2.3-1: Error handling procedures for a mandatory *supportedFeatures*

8.4 Parameter checking for Monitoring Events

8.4.1 General Concepts

A monitoring events provides functions that monitors for the following notifications:

- LOSS_OF_CONNECTIVITY
- UE_REACHABILITY
- LOCATION_REPORTING
- CHANGE_OF_IMSI_IMEI_ASSOCIATION
- ROAMING_STATUS
- COMMUNICATION_FAILURE
- AVAILABILITY_AFTER_DDN_FAILURE

The procedures for each monitoring event are similar to use API which is *MonitoringEventSubscription* and *MonitoringNotification*. The basic procedures are:

- An IN-CSE, as a 3GPP SCS, sends a *MonitoringEventSubscription* requests to a SCEF.
- The SCEF responds to the *MonitoringEventSubscription* request.
- The 3GPP core network detects monitoring events and reports the detected information to the SCEF.
- The SCEF sends *MonitoringNotification* reports to IN-CSE.

The received *MonitoringNotification* depends on *monitoringType*.

8.4.2 General Parameter checking for Monitoring Events

When IN-CSE receives a *MonitoringNotification* report, the IN-CSE shall verify the request using the following procedures.

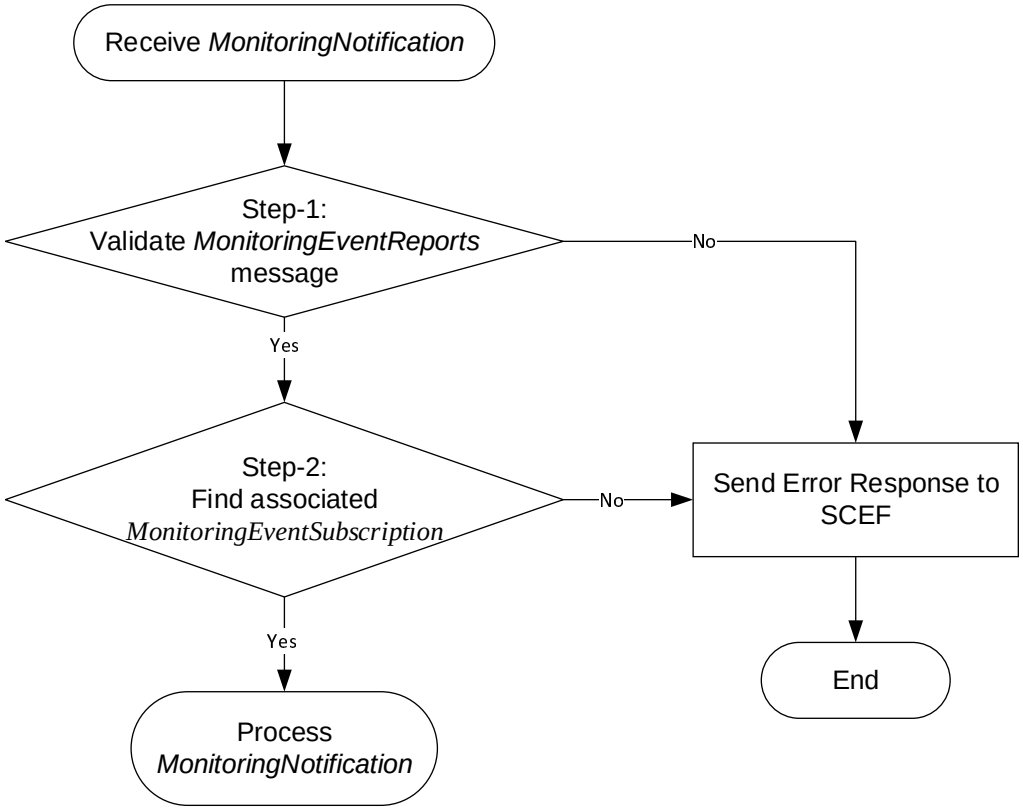

Figure 8.4.2-1: General procedure for parameter checking on monitoring event

When IN-CSE receives a *MonitoringNotification* from SCEF, the IN-CSE may check the parameters for validation.

Step 1: The IN-CSE validates received attributes of *MonitoringEventReports* based on *MonitoringType*. If the received message is not valid then the IN-CSE responds with the 400 Bad Request.

The mandatory attributes for Monitoring Type are:

- *lossOfConnectReason* for LOSS_OF_CONNECTIVITY
- *idleStatusInfo*, *eachabilityType* for UE_REACHABILITY
- *locationInfo* for LOCATION_REPORTING
- *imeiChange* for CHANGE_OF_IMSI_IMEI_ASSOCIATION
- *roamingStatus* for ROAMING_STATUS
- *failureCause* for COMMUNICATION_FAILURE
- *idleStatusInfo* for AVAILABILITY_AFTER_DDN_FAILURE

Step 2: Find the *MonitoringEventSubscription* that the received *MonitoringNotification* refers to based on the *subscription*, *monitoringType* and the *externalIDs* attributes. If a matching *MonitoringEventSubscription* is not found, then the IN-CSE responds with the 400 Bad Request.

History

Version	Date	Status
V4.7.1	February 2026	Publication