

ETSI TS 129 128 V13.0.0 (2016-05)



**LTE;**  
**Universal Mobile Telecommunications System (UMTS);**  
**Mobility Management Entity (MME)**  
**and Serving GPRS Support Node (SGSN)**  
**interfaces for interworking with packet data networks**  
**and applications**  
**(3GPP TS 29.128 version 13.0.0 Release 13)**



---

**Reference**

DTS/TSGC-0429128vd00

---

**Keywords**

LTE,UMTS

**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 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**The present document can be downloaded from:  
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at  
<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:  
<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.  
All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.  
**3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.  
**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (<https://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, 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.

---

## Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

---

## 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.

# Contents

Intellectual Property Rights .....	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	6
1 Scope .....	7
2 References .....	7
3 Definitions and abbreviations.....	8
3.1 Definitions .....	8
3.2 Abbreviations .....	8
4 General Description.....	8
4.1 Introduction .....	8
5 Procedures Description.....	10
5.1 Introduction .....	10
5.2 Report Procedures .....	10
5.2.1 General.....	10
5.2.2 Detailed Behaviour of the MME/SGSN .....	11
5.2.2.1 UE Loss of Connectivity .....	11
5.2.2.2 UE Reachability .....	11
5.2.2.3 Location Reporting.....	11
5.2.2.4 Communication Failure.....	11
5.2.3 Detailed Behaviour of the SCEF.....	11
5.2.4 Detailed Behaviour of the IWK-SCEF.....	12
5.3 Event Configuration Procedure .....	12
5.3.1 General .....	12
5.3.2 Detailed Behaviour of the MME/SGSN.....	13
5.3.3 Detailed Behaviour of the IWK-SCEF.....	13
5.3.4 Detailed Behaviour of the SCEF.....	14
5.4 Event Configuration Procedure for Roaming .....	14
5.4.1 General .....	14
5.4.2 Detailed Behaviour of the IWK-SCEF.....	15
5.4.3 Detailed Behaviour of the MME/SGSN.....	15
5.5 MO-Data Procedure .....	16
5.5.1 General .....	16
5.5.2 Detailed Behaviour of the MME.....	17
5.5.3 Detailed Behaviour of the SCEF.....	17
5.5.4 Detailed Behaviour of the IWK-SCEF.....	17
5.6 MT Data Procedure .....	17
5.6.1 General .....	17
5.6.2 Detailed Behaviour of the SCEF.....	18
5.6.3 Detailed Behaviour of the MME.....	18
5.6.4 Detailed Behaviour of the IWK-SCEF.....	19
5.7 Connection Management Procedure.....	19
5.7.1 General .....	19
5.7.2 Detailed Behaviour of the MME.....	20
5.7.3 Detailed Behaviour of the SCEF.....	20
5.7.4 Detailed Behaviour of the IWK-SCEF.....	21
6 Protocol Specification and Implementation .....	21
6.1 Introduction .....	21
6.1.1 Use of Diameter Base Protocol.....	21
6.1.2 Securing Diameter Messages .....	21
6.1.3 Accounting Functionality .....	21

6.1.4	Use of Sessions .....	21
6.1.5	Transport Protocol .....	21
6.1.6	Routing Considerations.....	22
6.1.7	Advertising Application Support .....	22
6.1.8	Diameter Application Identifier.....	23
6.1.9	Use of the Supported-Features AVP .....	23
6.2	Commands.....	23
6.2.1	Introduction.....	23
6.2.2	Command-Code values.....	23
6.2.3	Configuration Information Request (CIR) Command .....	24
6.2.4	Configuration-Information-Answer (CIA) Command .....	24
6.2.5	Reporting-Information-Request (RIR) Command .....	25
6.2.6	Reporting-Information-Answer (RIA) Command .....	26
6.2.7	Connection-Management-Request (CMR) Command.....	26
6.2.8	Connection-Management-Answer (CMA) Command.....	27
6.2.9	MO-Data-Request (ODR) Command .....	27
6.2.10	MO-Data-Answer (ODA) Command.....	28
6.2.11	MT-Data-Request (TDR) Command .....	28
6.2.12	MT-Data-Answer (TDA) Command .....	29
6.3	Result-Code AVP and Experimental-Result AVP Values .....	29
6.3.1	General.....	29
6.3.2	Success.....	29
6.3.3	Permanent Failures .....	29
6.3.3.1	DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY (5510).....	30
6.3.3.2	DIAMETER_ERROR_UNAUTHORIZED_SERVICE (5511) .....	30
6.3.3.3	DIAMETER_ERROR_CONFIGURATION_EVENT_STORAGE_NOT_SUCCESSFUL (5513).....	30
6.3.3.4	DIAMETER_ERROR_CONFIGURATION_EVENT_NON_EXISTANT (5514).....	30
6.3.3.5	DIAMETER_ERROR_REQUESTED_LOCATION_NOT_SERVED (5650) .....	30
6.3.3.6	DIAMETER_ERROR_USER_UNKNOWN (5001).....	30
6.3.3.7	DIAMETER_ERROR_OPERATION_NOT_ALLOWED (5101).....	30
6.3.3.8	DIAMETER_ERROR_INVALID_EPS_BEARER (5xxx) .....	30
6.3.3.9	DIAMETER_ERROR_NIDD_CONFIGURATION_NOT_AVAILABLE (5yyy).....	30
6.3.3.10	DIAMETER_ERROR_SCEF_REFERENCE_ID_UNKNOWN (5xxx).....	30
6.4	AVPs .....	30
6.4.1	General.....	30
6.4.2	Monitoring-Event-Configuration .....	32
6.4.3	Monitoring-Event-Report .....	33
6.4.4	Communication-Failure-Information.....	33
6.4.5	Cause-Type .....	33
6.4.6	S1AP-Cause.....	34
6.4.7	RANAP-Cause.....	34
6.4.8	BSSGP-Cause .....	34
6.4.9	GMM-Cause .....	34
6.4.10	SM-Cause .....	34
6.4.11	Number-Of-UE-Per-Location-Configuration .....	34
6.4.12	Number-Of-UE-Per-Location-Report.....	34
6.4.13	UE-Count.....	34
6.4.14	Feature-List AVP.....	35
6.4.14.1	Feature-List AVP for the T6a/T6b application .....	35
6.4.15	DRMP.....	35
6.4.16	User-Identifier.....	35
6.4.17	Bearer-Identifier .....	35
6.4.18	Connection-Action.....	36
6.4.19	Non-IP-Data.....	36
<b>Annex A (normative):</b>	<b>Diameter overload control mechanism .....</b>	<b>37</b>
A.1	T6a/b and T7 interfaces .....	37
A.1.1	General.....	37
A.1.2	SCEF behaviour.....	37
A.1.3	MME/SGSN behaviour.....	37
A.1.4	IWK-SCEF behaviour.....	37

**Annex B (normative): Diameter message priority mechanism.....38**  
B.1 General .....38  
B.2 T6a, T6ai, T6b, T6bi, T7 interfaces.....38

**Annex C (informative): Change history .....39**  
History .....40

---

# Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

---

# 1 Scope

The present document describes the Diameter-based interfaces between the SCEF/IWK-SCEF and other network entities such as MME/SGSN for the Architecture enhancements to facilitate communications with packet data networks and applications.

In particular, this document specifies the T6a interface between the MME and the SCEF, the T6ai interface between the MME and the IWK-SCEF, the T6b interface between the SGSN and the SCEF, the T6bi interface between the SGSN and the SCEF and the T7 interface between the SCEF and the IWK-SCEF. The procedures over those interfaces are defined in 3GPP TS 23.682 [2].

---

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".
- [3] IETF RFC 3588: "Diameter Base Protocol".
- [4] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; protocol details".
- [5] 3GPP TS 29.336: "Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications".
- [6] 3GPP TS 29.228: "IP multimedia (IM) Subsystem Cx Interface; Signalling flows and Message Elements".
- [7] IETF RFC 4960: "Stream Control Transport Protocol".
- [8] IETF RFC 5234: "Augmented BNF for Syntax Specifications: ABNF".
- [9] IETF RFC 7683: "Diameter Overload Indication Conveyance".
- [10] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".
- [11] 3GPP TS 25.413: "UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling".
- [12] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".
- [13] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".
- [14] 3GPP TS 48.018: "General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS protocol (BSSGP)".
- [15] IETF draft-ietf-dime-drmp-03: "Diameter Routing Message Priority".



Editor's note: The above document cannot be formally referenced until it is published as an RFC.

- [16] 3GPP TS 29.272: "Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".
- [17] 3GPP TS 29.329: "Sh Interface based on the Diameter protocol; Protocol details".
- [18] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".
- [19] 3GPP TS 23.007: "Restoration procedures".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply.

### 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

DRMP	Diameter Routing Message Priority
SCEF	Service Capability Exposure Function
IWK-SCEF	Interworking - SCEF

---

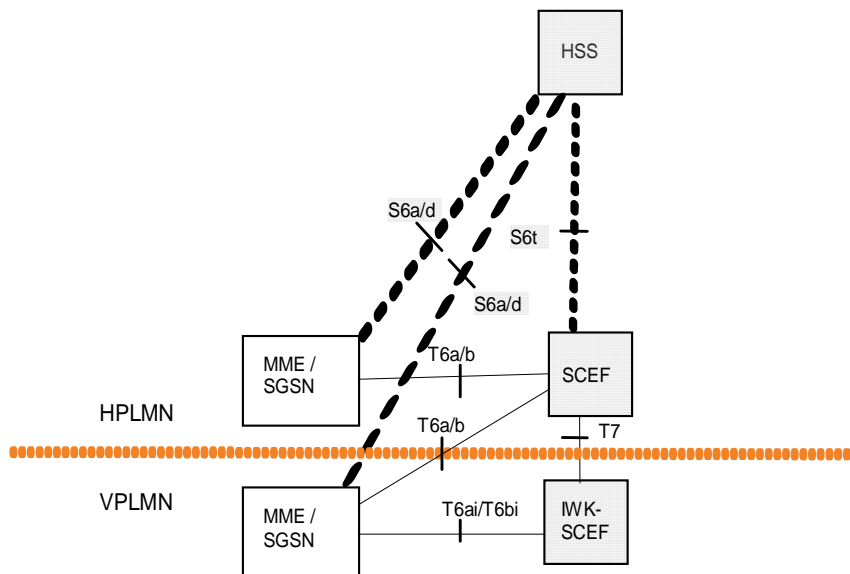
## 4 General Description

### 4.1 Introduction

The T6a/b reference point between the MME/SGSN and the SCEF, the T6ai/bi reference point between the MME/SGSN in the VPLMN and the IWK-SCEF and the T7 reference point between the IWK-SCEF and the SCEF are defined in the 3GPP TS 23.682 [2].

This document describes the Diameter-based T6a/b, T6ai/bi and T7 related procedures, message parameters and protocol specification.

An excerpt of the 3GPP Architecture for the enhancements to facilitate communications with packet data networks and applications, as defined in 3GPP TS 23.682 [2] is shown in Figure 4.1-1, where the relevant interfaces towards the SCEF/IWK-SCEF are highlighted.



**Figure 4.1-1: 3GPP Architecture for the enhancements to facilitate communications with packet data networks and applications**

In this architecture, the T6a/b reference point connects the MME/SGSN with the SCEF.

The T6a/b interface shall allow the SCEF to:

- receive reports of the monitoring events from the MME/SGSN configured via an HSS,
- to configure the monitoring events at an MME/SGSN which are not UE related.

The T6ai/bi reference point connects the MME/SGSN with the IWK-SCEF in the visited network, if the IWK-SCEF is deployed.

The T6ai/bi interface shall allow the IWK-SCEF to:

- receive configuration of the monitoring events from the MME or the SGSN and perform a filtering of the services which are allowed for this subscriber in this visited network based on roaming policies,
- receive reports of the monitoring events from the MME/SGSN that are configured via an HSS, perform a filtering and forward them to the SCEF (in the home network which has configured the event) via the T7 reference point.

The T7 reference point connects the IWK-SCEF in the visited network with the SCEF in the home network.

The T7 interface shall allow the IWK-SCEF to:

- forward reports received on T6ai/bi to the SCEF indicated in the event report received on T6ai/T6bi.
- receive configuration of monitoring events that are not UE related, from the SCEF, validate if those events are allowed as per roaming policies and then forward such monitoring event configurations to the MME/SGSN via the T6ai/T6bi reference points.

## 5 Procedures Description

### 5.1 Introduction

This section describes the Diameter-based T6a, T6b, T6ai, T6bi and T7 interface related procedures and the Information elements exchanged between the functional entities.

In the tables that describe the Information Elements transported by each Diameter command, each Information Element is marked as (M) Mandatory, (C) Conditional or (O) Optional in the "Cat." column. For the correct handling of the Information Element according to the category type, see the description detailed in section 6 of the 3GPP TS 29.228 [6].

### 5.2 Report Procedures

#### 5.2.1 General

This procedure is used between the MME/SGSN and the SCEF, between the MME/SGSN and the IWK-SCEF and between the IWK-SCEF and the SCEF.

When the procedure is invoked by the MME or the SGSN, it is used for reporting:

- the UE Loss of Connectivity;
- the UE Reachability;
- location of the UE and change in location of the UE;
- Communication Failure.

When the procedure is invoked by the IWK-SCEF, it is used for conveying the monitoring event reported by the MME or the SGSN to the SCEF, after applying the roaming policies configured at the IWK-SCEF.

This procedure is mapped to the commands Reporting-Information-Request/Answer in the Diameter application specified in clause 6. The tables 5.2.1-1 and 5.2.1-2 detail the involved information elements.

**Table 5.2.1-1: Reporting Information Request**

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Monitoring Event Report (see 3GPP TS 29.336 [5] subclause 8.4.3)	Monitoring-Event-Report	C	If the Reporting-Information-Request is sent for reporting the monitoring events, the MME/SGSN and the IWK-SCEF shall include the monitoring event(s) reported towards the SCEF.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 5.2.1-2: Reporting Information Answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result (See 6.3)	Result-Code / Experimental- Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for T6a/b errors. This is a grouped AVP, which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

## 5.2.2 Detailed Behaviour of the MME/SGSN

The MME/SGSN shall fill the Monitoring-Event-Report AVP according to the event reported as specified below. For all monitoring events, the SCEF-ID and the SCEF-Reference-ID AVPs shall be included. In addition, the event specific AVPs as listed below shall be included based on the type of event reported.

### 5.2.2.1 UE Loss of Connectivity

The following AVPs shall be present within the Monitoring-Event-Report AVP when the UE Loss of Connectivity event is reported:

- Monitoring-Type set to LOSS\_OF\_CONNECTIVITY (0)

### 5.2.2.2 UE Reachability

The following AVPs shall be present within the Monitoring-Event-Report AVP when the UE Reachability event is reported:

- Monitoring-Type set to UE\_REACHABILITY (1)
- Reachability-Information set to REACHABLE\_FOR\_DATA(1)

### 5.2.2.3 Location Reporting

The following AVPs shall be present within the Monitoring-Event-Report AVP when the location event is reported:

- Monitoring-Type set to LOCATION\_REPORTING (2)
- EPS-Location-Information

### 5.2.2.4 Communication Failure

The following AVPs shall be present within the Monitoring-Event-Report AVP when the Communication Failure event is reported

- Monitoring-Type set to COMMUNICATION\_FAILURE (5)
- Communication-Failure-Information (see subclause 6.4.3)

## 5.2.3 Detailed Behaviour of the SCEF

When the SCEF receives a Reporting-Information-Request command from the MME/SGSN or the IWK-SCEF, the SCEF shall set Experimental-Result to DIAMETER\_SUCCESS in the Reporting-Information-Answer and shall handle it according to the procedures defined in 3GPP TS 23.682 [2].

## 5.2.4 Detailed Behaviour of the IWK-SCEF

When the IWK-SCEF receives a Reporting-Information-Request command from the MME/SGSN it shall deliver the request to the SCEF after applying the roaming policies configured at the IWK-SCEF, as specified in 3GPP TS 23.682 [2].

## 5.3 Event Configuration Procedure

### 5.3.1 General

This procedure is used between the SCEF and the MME and between the SCEF and the SGSN to configure the monitoring events directly at the MME/SGSN through the T6a/b interface.

This procedure is also used between the SCEF and the IWK-SCEF through the T7 interface to configure the monitoring events directly at the MME/SGSN at the VPLMN in case of roaming scenarios, if the IWK-SCEF is deployed at the VPLMN. If the IWK-SCEF accepts the event configuration from the SCEF, this procedure is used between the IWK-SCEF and the MME/SGSN through the T6ai/T6bi interfaces.

When the procedure is invoked by the SCEF, it is used for configuring the event(s):

- the number of UEs at a given geographic location

This procedure is mapped to the commands Configuration-Information-Request/Answer in the Diameter application specified in clause 6. The tables 5.3.1-1 and 5.3.1-2 detail the involved information elements.

**Table 5.3.1-1: Configuration Information Request**

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Monitoring Event Configuration (see 3GPP TS 29.336 [5] subclause 8.4.2)	Monitoring-Event-Configuration	C	If present, this Information Element shall contain the details of the Monitoring event(s) configured.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this Information Element shall contain the list of features supported by the origin host.

**Table 5.3.1-2: Configuration Information Answer**

Information Element Name	Mapping to Diameter AVP	Cat	Description
Result (See 6.3)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for T6a/T6b, T6ai/T6bi and T7 errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Monitoring Event Report (see 3GPP TS 29.336 [5] subclause 8.4.3)	Monitoring-Event-Report	C	If an immediate report is available this information element shall contain the requested data available in the MME/SGSN.
Monitoring Event-Configuration Status (see 3GPP TS 29.336 [5] subclause 8.4.24)	Monitoring-Event-Config-Status	O	If present it shall contain the status of each monitoring event configuration identified by an SCEF-Reference-ID

### 5.3.2 Detailed Behaviour of the MME/SGSN

When the Configuration-Information-Request is received from the SCEF, the MME/SGSN shall, in the following order:

1. Check whether the requesting SCEF is authorized to request the specified service (e.g: number of UEs at a given geographic location). If not, Experimental-Result shall be set to `DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY` (5510) in the Configuration-Information-Answer.
2. If the TA / RA / ECGI location requested by the SCEF is not served by the MME/SGSN, then the MME/SGSN shall set the Experimental-Result AVP to `DIAMETER_ERROR_REQUESTED_LOCATION_NOT_SERVED` (5650) in the Configuration-Information-Answer.

When the Configuration-Information-Request is received from the IWK-SCEF, the MME/SGSN shall, in the following order:

1. If the TA / RA / ECGI location requested by the IWK-SCEF is not served by the MME/SGSN, then the MME/SGSN shall set the Experimental-Result AVP to `DIAMETER_ERROR_REQUESTED_LOCATION_NOT_SERVED` (5650) in the Configuration-Information-Answer.

If there is an error in any of the above steps then the MME/SGSN shall stop processing and shall return the error code specified in the respective step.

If the MME/SGSN cannot fulfil the received request for reasons not stated above, it shall stop processing the request and set Result-Code to `DIAMETER_UNABLE_TO_COMPLY`.

If CIR message includes multiple SCEF-Reference-ID and for a SCEF-Reference-ID the monitoring events cannot be handled, the MME/SGSN shall report the failed SCEF-Reference-ID to the SCEF or the IWK-SCEF with an appropriate status in the Monitoring-Event-Config-Status AVP.

For the number of UEs in a geographic location monitoring event, for each SCEF-Reference-ID that the MME/SGSN is able to successfully process, the MME/SGSN shall include in the Configuration-Information-Answer, the exact count of the number of UEs at the requested location. If the requested location type is current location, then the MME/SGSN may activate the paging and RAN location reporting procedures (if required) before providing the response in the Configuration-Information-Answer.

If the MME receives the `DIAMETER_ERROR_SCEF_REFERENCE_ID_UNKNOWN` within an RIA command, it shall delete the event stored for the indicated SCEF-Reference-ID (see 3GPP TS 23.007 [19]).

### 5.3.3 Detailed Behaviour of the IWK-SCEF

When the SCEF receives a Monitoring Event Report AVP from the MME/SGSN or the IWK-SCEF with a SCEF-Reference-ID not known by the SCEF, it shall reply with `DIAMETER_ERROR_SCEF_REFERENCE_ID_UNKNOWN` (see 3GPP TS 23.007 [19]).

Otherwise when the Configuration-Information-Request is received from the SCEF, the IWK-SCEF shall, in the following order:

1. Check whether the requesting SCEF is authorized, as per roaming policies, to request the specified service (e.g: number of UEs at a given geographic location). If not, Experimental-Result shall be set to `DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY` (5510) in the Configuration-Information-Answer.

If the IWK-SCEF cannot fulfil the received request for reasons not stated in the above, it shall stop processing the request and set Result-Code to `DIAMETER_UNABLE_TO_COMPLY`.

If the roaming policies permit the SCEF to configure the monitoring events at the VPLMN MME/SGSN and if the IWK-SCEF is able to successfully process the Configuration-Information-Request, then the IWK-SCEF shall deliver the Configuration-Information-Request to the MME/SGSN in the VPLMN.

If the VPLMN has pooled MME(s)/SGSN(s), then for event configurations that are not UE specific (e.g Number of UEs in a given geographic location):

- the IWK-SCEF shall generate the Configuration-Information-Request towards all the MME(s)/SGSN(s) in the pool. For the monitoring event, number of UEs for a given location, the IWK-SCEF shall identify the MME(s)/SGSN(s) to forward the Configuration-Information-Request based on the location (TA/RA/ECGI) served;
- the IWK-SCEF shall aggregate the Configuration-Information-Answer received from multiple MME(s)/SGSN(s) in the pool and shall send a single Configuration-Information-Answer towards the SCEF;
- if some of the MME(s)/SGSN(s) in the pool returned error for the monitoring event configuration, then the IWK-SCEF shall not include the response from such MME(s)/SGSN(s) in the aggregated report included in the Configuration-Information-Answer command towards the SCEF.

### 5.3.4 Detailed Behaviour of the SCEF

When the SCEF receives Monitoring Event Report AVP from the MME/SGSN or the IWK-SCEF in the CIA command, it shall handle it according to the procedures defined in 3GPP TS 23.682 [2].

## 5.4 Event Configuration Procedure for Roaming

### 5.4.1 General

The MME/SGSN shall send the monitoring event configuration information to the IWK-SCEF in roaming scenarios, when the MME/SGSN receives the monitoring event configuration from the HSS. The monitoring event configuration information shall be locally consumed at the IWK-SCEF and the IWK-SCEF shall not route such requests beyond it.

This procedure is mapped to the commands Configuration-Information-Request/Answer in the Diameter application specified in clause 6. The tables 5.4.1-1 and 5.4.1-2 detail the involved information elements.

**Table 5.4.1-1: Configuration-Information-Request**

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Monitoring Event Configuration (see 8.4.2)	Monitoring-Event-Configuration	C	If present, this Information Element shall contain the details of Monitoring event(s).
Monitoring Event Report (see 8.4.3)	Monitoring-Event-Report	C	If an immediate report is available this information element shall contain the event reported by the MME/SGSN. The IWK-SCEF may normalize the event report and return it in the Configuration-Information-Answer.
Supported Features (See 3GPP TS 29.229 [7])	Supported-Features	O	If present, this Information Element shall contain the list of features supported by the origin host.

Table 5.4.1-2: Configuration-Information-Answer

Information Element Name	Mapping to Diameter AVP	Cat	Description
Result (See 6.3)	Result-Code / Experimental- Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for S6t errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [7])	Supported- Features	O	If present, this information element shall contain the list of features supported by the origin host.
Monitoring Event- Configuration Status (see 3GPP TS 29.336 [5] subclause 8.4.24)	Monitoring-Event- Config-Status	O	If present it shall contain the status of each monitoring event configuration identified by an SCEF-Reference-ID

### 5.4.2 Detailed Behaviour of the IWK-SCEF

When the Configuration-Information-Request is received from the MME/SGSN, the IWK-SCEF shall, in the following order:

1. Check whether the requesting SCEF, identified by the SCEF-ID is authorized to request the specified service at the VPLMN. If not, Experimental-Result shall be set to `DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY` (5510) in the Configuration-Information-Answer.
2. Check whether the chargeable party for the monitoring event is authorized to be charged at the VPLMN. If not, Experimental-Result shall be set to `DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY` (5510) in the Configuration-Information-Answer.

If the monitoring event configuration also carries the monitoring event report, the IWK-SCEF checks if the immediate events reported by the MME/SGSN needs to be normalized. If yes, the IWK-SCEF shall normalize the event report as per local policies. The IWK-SCEF shall then send the normalized monitoring event report towards the SCEF as a separate Reporting-Information-Request message.

If the monitoring event configuration is for a continuous monitoring (i.e Monitoring-Duration and/or Maximum-Number-Of-Reports are set), then the IWK-SCEF shall temporarily store the monitoring event configuration until the deletion criteria for the monitoring event configuration is met. The stored monitoring event configuration information shall be used during subsequent monitoring event report procedure, to generate the charging records towards the right chargeable party.

If the received SCEF Reference ID for Deletion does not exist, the IWK-SCEF shall set the Experimental-Result-Code to `DIAMETER_ERROR_CONFIGURATION_EVENT_NON_EXISTANT` (5514).

If the SCEF-Reference-ID exists and the old configuration data could not be replaced by new Configuration event data, the HSS shall set the Experimental-Result-Code to `DIAMETER_ERROR_CONFIGURATION_EVENT_STORAGE_NOT_SUCCESSFUL` (5513).

If the IWK-SCEF cannot fulfil the received request for reasons not stated in the above, it shall stop processing the request and set Result-Code to `DIAMETER_UNABLE_TO_COMPLY`.

### 5.4.3 Detailed Behaviour of the MME/SGSN

When the MME/SGSN receives the Configuration-Information-Answer from the IWK-SCEF, it shall handle it as follows: For the monitoring event configurations for which the configuration status have changed since last informed to the HSS, the MME/SGSN shall report the status to the HSS through a Notify-Request command as specified in subclause 5.2.5 of 3GPP TS 29.272 [16].



## 5.5 MO-Data Procedure

### 5.5.1 General

This procedure shall be used between the MME and the SCEF, between the MME and the IWK-SCEF and between the IWK-SCEF and the SCEF.

When the procedure is invoked by the MME, it is used to forward mobile originated Non-IP data of a mobile user from the MME to the SCEF.

This procedure is used according to 3GPP TS 23.682 [2] subclause 5.5.4.

The IWK-SCEF may be in the path between the MME and the SCEF for roaming cases when the IWK-SCEF is deployed by the operator of the visited PLMN.

When the procedure is invoked by the IWK-SCEF, it is used to forward mobile originated Non-IP data received from the MME to the SCEF.

This procedure is mapped to the commands MO-Data-Request/Answer (ODR/ODA) in the Diameter application specified in clause 6.

The tables 5.5.1-1 and 5.5.1-2 detail the involved information elements.

**Table 5.5.1-1: MO Data Request**

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Identifier	M	This Information Element shall contain the identity of the UE. This is a grouped AVP containing the IMSI.
EPS Bearer Identity	Bearer-Identifier	M	This information element shall be present and shall contain the identity of the EPS-bearer identifying the T6a connection for the Non-IP data delivery.
Non IP data	Non-IP-Data	C	This information element shall contain the Non-IP data to be delivered to the SCEF. This Information Element shall be present when the request conveys Non-IP data.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

**Table 5.5.1-2: MO Data Answer**

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result (See 6.3)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for T6a/b errors. This is a grouped AVP, which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

## 5.5.2 Detailed Behaviour of the MME

The MME shall make use of this procedure over a T6a connection identified by its EPS bearer identity and previously established with the SCEF to forward the Non-IP data received from the UE to the SCEF or to an IWK-SCEF when deployed for a roaming case.

## 5.5.3 Detailed Behaviour of the SCEF

When the SCEF receives a MO Data Request from the MME or the IWK-SCEF, the SCEF shall, in the following order:

- Check that the User Identity exists in the SCEF. If not, Experimental-Result shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN in the MO Data Answer;
- Check, if, for this user, a valid EPS bearer context exists. If not, Experimental-Result shall be set to DIAMETER\_ERROR\_INVALID\_EPS\_BEARER in the MO Data Answer.
- Process the data delivery to the SCS/AS and if it is successful, return a Result code set to DIAMETER\_SUCCESS to the MME or IWK-SCEF; otherwise return an appropriate Diameter error code.

NOTE: The Diameter Result-Code / Experimental-Result returned by the SCEF can depend on the error returned by the SCS/AS to the SCEF. The interface between the SCEF and the SCS/AS is out of scope of 3GPP.

## 5.5.4 Detailed Behaviour of the IWK-SCEF

When the IWK-SCEF receives a MO Data Request from the MME, it shall forward the request to the SCEF after having addressed routing and charging aspects.

When the IWK-SCEF receives a MO Data Answer from the SCEF, it shall forward the answer to the MME after having addressed routing and charging aspects.

# 5.6 MT Data Procedure

## 5.6.1 General

This procedure shall be used between the SCEF and the MME, between the SCEF and the IWK-SCEF and between the IWK-SCEF and the MME.

When the procedure is invoked by the SCEF, it is used to forward mobile terminated Non-IP data of a mobile user from the SCEF to the MME.

This procedure is used according to 3GPP TS 23.682 [2] subclause 5.x.3.

The IWK-SCEF may be in the path between the SCEF and the MME for roaming cases when the IWK-SCEF is deployed by the operator of the visited PLMN.

When the procedure is invoked by the IWK-SCEF, it is used to forward mobile terminated Non-IP data received from the SCEF to the MME.

This procedure is mapped to the commands MT-Data-Request/Answer (TDR/TDA) in the Diameter application specified in clause 6.

The tables 5.6.1-1 and 5.6.1-2 detail the involved information elements.

NOTE: The corresponding message name in 3GPP TS 23.682 [2] is "NIDD Submit Request".

Table 5.6.1-1: MT Data Request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Identifier	M	This Information Element shall contain the identity of the UE. This is a grouped AVP containing the IMSI.
EPS Bearer Identity	Bearer-Identifier	M	This information element shall be present and shall contain the identity of the EPS-bearer identifying the T6a connection for the Non-IP data delivery.
Non-IP Data	Non-IP-Data	C	This information element shall contain the Non-IP data to be delivered to the MME. This Information Element shall be present when the request conveys Non-IP data.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 5.6.1-2: MT Data Answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result (See 6.3)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for T6a/b errors. This is a grouped AVP, which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

## 5.6.2 Detailed Behaviour of the SCEF

The SCEF shall make use of this procedure over a T6a connection identified by its EPS bearer identity and previously established with the MME to forward the Non-IP data received from the SCS/AS to the MME or to an IWK-SCEF when deployed for a roaming case.

The SCEF shall check if a valid EPS bearer context exists for the user before sending the request.

## 5.6.3 Detailed Behaviour of the MME

When the MME receives a MT Data Request from the MME or the IWK-SCEF, the SCEF shall, in the following order:

- Check that the User Identity exists in the MME. If not, Experimental-Result shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN in the MT Data Answer;
- Check whether, for this user, a valid EPS bearer context exists. If not, Experimental-Result shall be set to DIAMETER\_ERROR\_INVALID\_EPS\_BEARER in the MT Data Answer.
- Process the data delivery to the UE and if it is successful, return a Result code set to DIAMETER\_SUCCESS to the SCEF or IWK-SCEF; otherwise return an appropriate Diameter error code.

## 5.6.4 Detailed Behaviour of the IWK-SCEF

When the IWK-SCEF receives a MT Data Request from the SCEF, it shall forward the request to the MME after having addressed routing and charging aspects.

When the IWK-SCEF receives a MT Data Answer from the MME, it shall forward the answer to the SCEF after having addressed routing and charging aspects.

## 5.7 Connection Management Procedure.

### 5.7.1 General

This procedure shall be used between the MME and the SCEF, between the MME and the IWK-SCEF and between the IWK-SCEF and the SCEF.

When the procedure is invoked by the MME, it is used

- to establish a T6a connection between the MME and the SCEF.
- to release a T6a connection between the MME and the SCEF.

This procedure is used according to 3GPP TS 23.682 [2] subclause 5.x.1 and 5.x.5. The IWK-SCEF may be in the path between the MME and the SCEF for roaming cases when the IWK-SCEF is deployed by the operator of the visited PLMN.

When the procedure is invoked by the IWK-SCEF, it is used to forward the Connection Management Request received from the MME to the SCEF.

This procedure is mapped to the commands Connection-Management-Request/Answer (CMR/CMA) in the Diameter application specified in clause 6.

The tables 5.7.1-1 and 5.7.1-2 detail the involved information elements.

**Table 5.7.1-1: Connection Management Request**

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Identifier	M	This Information Element shall contain the identity of the UE. This is a grouped AVP containing the IMSI.
EPS Bearer Identity	Bearer-Identifier	M	This Information Element shall be present and shall contain the identity of the EPS bearer identifying the T6a connection to which the request applies.
T6a Connection Action	Connection-Action	M	This Information element shall be present and shall contain a T6a connection management action indicating a T6a connection establishment or a T6a connection release.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

**Editor's Note: Transfer of additional parameters on T6a to aid T6a connection to SCS/AS session binding at SCEF is FFS.**

Table 5.7.1-2: Connection Management Answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result (See 6.3)	Result-Code / Experimental- Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for T6a/b errors. This is a grouped AVP, which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [4])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

### 5.7.2 Detailed Behaviour of the MME

The MME shall make use of this procedure to request one of the following T6a connection management actions:

- for a T6a connection establishment, the MME shall:
  - fill the EPS-Bearer-Identity information element with the identity of the EPS bearer that MME allocated to the Non-IP PDN connection as described in 3GPP TS 23.682 [2];

Editor's Note: Which user identity (IMSI or MSISDN or another identity) shall be filled is FFS.

- for a T6a connection release, the MME shall:
  - fill the EPS Bearer Identity information element with the identity of the EPS bearer of the T6a connection which is released as described in 3GPP TS 23.682 [2];
  - upon getting the Connection Management Answer from the SCEF, delete the T6a connection context.

### 5.7.3 Detailed Behaviour of the SCEF

When the SCEF receives a Connection Management Request from the MME or the IWK-SCEF, the SCEF shall, in the following order:

- check that the User Identity exists in the SCEF. If not, Experimental-Result shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN in the Connection Management Answer;
- if the T6a connection action indicates a T6a connection establishment:
  - check whether a valid NIDD configuration exists for the UE at the SCEF. If not, Experimental-Result shall be set to DIAMETER\_ERROR\_NIDD\_CONFIGURATION\_NOT\_AVAILABLE in the Connection Management Answer;
  - create an EPS bearer context;
  - store the MME Address in the EPS bearer context. If successful, Result shall be set to DIAMETER\_SUCCESS in the Connection Management Answer;
- if the T6a connection action indicates a T6a connection release:
  - check whether, for this user and the received EPS bearer ID, a T6a connection context exists. If not, Experimental-Result shall be set to DIAMETER\_ERROR\_INVALID\_EPS\_BEARER in the Connection Management Answer.
  - Delete the T6a connection context at the SCEF. If successful, Result code shall be set to DIAMETER\_SUCCESS in the Connection Management Answer.

#### 5.7.4 Detailed Behaviour of the IWK-SCEF

When the IWK-SCEF receives a Connection Management Request from the MME, it shall forward the request to the SCEF after having addressed routing and charging aspects

When the IWK-SCEF receives a Connection Management Answer from the SCEF, it shall forward the answer to the MME after having addressed routing and charging aspects.

---

## 6 Protocol Specification and Implementation

### 6.1 Introduction

#### 6.1.1 Use of Diameter Base Protocol

The Diameter Base Protocol as specified in IETF RFC 3588 [3] shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and error codes as specified in this specification. Unless otherwise specified, the procedures (including error handling and unrecognised information handling) shall be used unmodified.

#### 6.1.2 Securing Diameter Messages

For secure transport of Diameter messages, see 3GPP TS 33.210 [4].

#### 6.1.3 Accounting Functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) shall not be used on the T6a/T6b interface, T6ai/T6bi interface and the T7 interface.

#### 6.1.4 Use of Sessions

Diameter sessions shall be implicitly terminated between:

- the MME/SGSN and the SCEF, for the T6a/T6b interface;
- the MME/SGSN and the IWK-SCEF, for the T6ai/T6bi interface and
- the IWK-SCEF and the SCEF for the T7 interface.

An implicitly terminated session is one for which the server does not maintain state information. The client shall not send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO\_STATE\_MAINTAINED (1), as described in IETF RFC 3588 [3]. As a consequence, the server shall not maintain any state information about this session and the client shall not send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

#### 6.1.5 Transport Protocol

Diameter messages over the T6a/T6b, T6ai/T6bi and T7 interface shall make use of SCTP IETF RFC 4960 [7] as transport protocol.

## 6.1.6 Routing Considerations

**Editor's Note:** It is to identify the routing impacts linked to Non-IP Data over T6a compared to the hereafter existing statements.

**Editor's Note:** Regarding routing aspects for Non-IP-Data, it is to be investigated if the IWK-SCEF can behave as Proxy Diameter Agent.

This clause specifies the use of the Diameter routing AVPs Destination-Realm and Destination-Host.

The MME/SGSN shall use the SCEF-ID it receives for a monitoring event configuration as the Destination-Host AVP in the Reporting-Information-Request for the monitoring event reports sent on the T6a/T6b interface.

The MME/SGSN shall use the pre-configured IWK-SCEF identifier as the Destination-Host AVP in the Reporting-Information-Request for the monitoring event reports and the Configuration-Information-Request for the monitoring event configuration sent on the T6ai/bi interface.

The IWK-SCEF shall use the SCEF-ID received from the MME/SGSN in the Monitoring-Event-Report AVP of the Reporting-Information-Request for deriving the Destination-Host AVP to be included in the Reporting-Information-Request from the IWK-SCEF to the SCEF on the T7 interface.

For monitoring events directly configured at the MME/SGSN by the SCEF, if the SCEF knows the address/name of the MME/SGSN or the IWK-SCEF, both the Destination-Realm AVP and the Destination-Host AVP shall be present in the request. Otherwise, only the Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node. Consequently, the Destination-Host AVP is declared as optional in the ABNF for all requests initiated by the SCEF.

Destination-Realm AVP is declared as mandatory in the ABNF for all requests.

If the Vendor-Specific-Application-ID AVP is received in any of the commands, it may be ignored by the receiving node, and it shall not be used for routing purposes.

**NOTE:** The Vendor-Specific-Application-ID can be included as an optional AVP in all commands in order to ensure interoperability with diameter agents following a strict implementation of IETF RFC 3588 [3], by which messages not including this AVP will be rejected. IETF RFC 3588 [3] indicates that the AVP shall be present in all proxiable commands, such as those defined in this specification, despite the fact that the contents of this AVP are redundant since the Application ID is already present in the command header. This AVP may be removed in subsequent revisions of this specification, once the diameter base protocol is updated accordingly.

## 6.1.7 Advertising Application Support

The SCEF, MME, SGSN and the IWK-SCEF shall advertise support of the Diameter T6a/T6b Application by including the value of the application identifier in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

**NOTE:** Even though the reference point between the MME/SGSN and the IWK-SCEF is called T6ai/T6bi respectively and the reference point between the IWK-SCEF and the SCEF is called T7, all these reference points use the same Diameter Application ID.

The vendor identifier value of 3GPP (10415) shall be included in the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and in the Vendor-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that is not included in the Vendor-Specific-Application-Id AVPs as described above shall indicate the manufacturer of the Diameter node as per IETF RFC 3588 [3].

## 6.1.8 Diameter Application Identifier

The T6a/T6b interface protocol shall be defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (<http://www.iana.org/assignments/enterprise-numbers>) is 10415.

The Diameter application identifier assigned to the T6a/T6b interface application is 16777346.

The T6ai/T6bi and the T7 interface protocol shall use the same Diameter application identifier as the T6a/T6b interface.

## 6.1.9 Use of the Supported-Features AVP

When new functionality is introduced on the T6a/T6b application, it should be defined as optional. If backwards incompatible changes cannot be avoided, the new functionality shall be introduced as a new feature and support advertised with the Supported-Features AVP. The usage of the Supported-Features AVP on the T6a/T6b application is consistent with the procedures for the dynamic discovery of supported features as defined in clause 7.2 of 3GPP TS 29.229 [4].

When extending the application by adding new AVPs for a feature, the new AVPs shall have the M bit cleared and the AVP shall not be defined mandatory in the command ABNF.

As defined in 3GPP TS 29.229 [4], the Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the all reference points as specified in this specification, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, for features defined in this document, the Vendor-Id AVP shall contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the reference point, the Feature-List-ID AVP shall differentiate those lists from one another.

## 6.2 Commands

### 6.2.1 Introduction

This section defines the Command code values and related ABNF for each command described in this specification. The ABNF for the commands on T6a/T6b, T6ai/T6bi and T7 are the same if not specified explicitly different.

### 6.2.2 Command-Code values

This section defines Command-Code values for the T6a/T6b interface application as allocated by IANA.

Every command is defined by means of the ABNF syntax IETF RFC 5234 [8], according to the rules in IETF RFC 3588 [3]. When the definition and use of an AVP is not specified in this document, the guidelines in IETF RFC 3588 [3] shall apply.

The following Command Codes are defined in this specification for T6a/T6b:



Table 6.2.2-1: Command-Code values for T6a/T6b

Command-Name	Abbreviation	Code	Section
Configuration-Information-Request	CIR	8388718	3GPP TS 29.336 [5] subclause 8.2.3 and subclause 6.2.3 below
Configuration-Information-Answer	CIA	8388718	3GPP TS 29.336 [5] subclause 8.2.4 and subclause 6.2.4 below
Reporting-Information-Request	RIR	8388719	3GPP TS 29.336 [5] subclause 8.2.5 and subclause 6.2.5 below
Reporting-Information-Answer	RIA	8388719	3GPP TS 29.336 [5] subclause 8.2.6 and subclause 6.2.6 below
Connection-Management-Request	CMR	xxxxxxx	6.2.7
Connection-Management-Answer	CMA	xxxxxxx	6.2.8
MO-Data-Request	ODR	xxxxxxx	6.2.9
MO-Data-Answer	ODA	xxxxxxx	6.2.10
MT-Data-Request	TDR	xxxxxxx	6.2.11
MT-Data-Answer	TDA	xxxxxxx	6.2.12

For these commands, the Application-ID field shall be set to 16777346 (application identifier of the T6a/T6b interface application, allocated by IANA).

### 6.2.3 Configuration Information Request (CIR) Command

The Configuration Information Request (CIR) command, indicated by the Command-Code field set to 8388718 and the "R" bit set in the Command Flags field, is sent from:

- the SCEF to the MME/SGSN;
- the SCEF to the IWK-SCEF and
- the MME/SGSN to the IWK-SCEF

This command is originally defined in 3GPP TS 29.336 [5].

For the T6a/T6b interface, the Configuration-Information-Request command format is specified as following:

Message Format:

```

< Configuration-Information-Request > ::=
  < Diameter Header: 8388718, REQ, PXY, 16777346 >
  < Session-Id >
  [ DRMP ]
  { Auth-Session-State }
  { Origin-Host }
  { Origin-Realm }
  [ Destination-Host ]
  { Destination-Realm }
  *[ Supported-Features ]
  *[ Monitoring-Event-Configuration ]
  *[ Proxy-Info ]
  *[ Route-Record ]
  *[AVP]

```

### 6.2.4 Configuration-Information-Answer (CIA) Command

The Configuration-Information-Answer (CIA) command, indicated by the Command-Code field set to 8388718 and the "R" bit cleared in the Command Flags field, is sent from:

- the MME/SGSN to the SCEF;
- the IWK-SCEF to the SCEF and
- the IWK-SCEF to the MME/SGSN

This command is originally defined in 3GPP TS 29.336 [5].

For the T6a/T6b interface, the Configuration-Information-Answer command format is specified as following:

Message Format:

```

< Configuration-Information-Answer > ::= < Diameter Header: 8388718, PXY, 16777346 >
    < Session-Id >
    [ DRMP ]
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    *[ Supported-Features ]
    *[ Monitoring-Event-Report ]
    *[ Monitoring-Event-Config-Status ]
    *[ Failed-AVP ]
    *[ Proxy-Info ]
    *[ Route-Record ]
    *[AVP]

```

## 6.2.5 Reporting-Information-Request (RIR) Command

The Reporting-Information-Request (RIR) command, indicated by the Command-Code field set to 8388719 and the "R" bit cleared in the Command Flags field, is sent from:

- the MME/SGSN to the SCEF;
- the MME/SGSN to the IWK-SCEF and
- the IWK-SCEF to the SCEF.

This command is originally defined in 3GPP TS 29.336 [5].

For the T6a/T6b interface, the Reporting-Information-Request command format is specified as following:

Message Format:

```

< Reporting-Information-Request > ::= < Diameter Header: 8388719, PXY, 16777346 >
    < Session-Id >
    [ DRMP ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Host }
    { Destination-Realm }
    [ OC-Supported-Features ]
    *[ Supported-Features ]
    *[ Monitoring-Event-Report ]
    *[ Failed-AVP ]
    *[ Proxy-Info ]
    *[ Route-Record ]
    *[AVP]

```

## 6.2.6 Reporting-Information-Answer (RIA) Command

The Reporting-Information-Answer (RIA) command, indicated by the Command-Code field set to 8388719 and the "R" bit cleared in the Command Flags field, is sent from:

- the SCEF to the MME/SGSN;
- the SCEF to the IWK-SCEF and
- the IWK-SCEF to the MME/SGSN.

This command is originally defined in 3GPP TS 29.336 [5].

For the T6a/T6b interface, the Reporting-Information-Answer command format is specified as following:

Message Format:

```
< Reporting-Information-Answer > ::= < Diameter Header: 8388719, PXY, 16777346 >
    < Session-Id >
    [ DRMP ]
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ OC-Supported-Features ]
    [ OC-OLR ]
    *[ Supported-Features ]
    *[ Failed-AVP ]
    *[ Proxy-Info ]
    *[ Route-Record ]
    *[AVP]
```

## 6.2.7 Connection-Management-Request (CMR) Command

The Connection-Management-Request (CMR) command, indicated by the Command-Code field set to **xxxx** and the "R" bit cleared in the Command Flags field, is sent from:

- the MME to the SCEF;
- the MME to the IWK-SCEF; and
- the IWK-SCEF to the SCEF.

For the T6a, T6ai, T7 interfaces, the Connection-Management-Request command format is specified as following:

Message Format:

```
< Connection-Management-Request > ::= < Diameter Header: xxxxx, PXY, 16777346 >
    < Session-Id >
    < User-Identifier >
    < Bearer-Identifier >
    [ DRMP ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Destination-Host ]
    { Destination-Realm }
    [ OC-Supported-Features ]
    *[ Supported-Features ]
    [ Connection-Action ]
    *[ Failed-AVP ]
    *[ Proxy-Info ]
```

\*[ Route-Record ]  
 \*[AVP]

## 6.2.8 Connection-Management-Answer (CMA) Command

The Connection-Management-Answer (CMA) command, indicated by the Command-Code field set to **xxxxxx** and the "R" bit cleared in the Command Flags field, is sent from:

- the SCEF to the MME;
- the SCEF to the IWK-SCEF and
- the IWK-SCEF to the MME.

For the T6a, T6ai and T7 interfaces, the Connection-Management-Answer command format is specified as following:

Message Format:

```
< Connection-Management-Answer > ::= < Diameter Header: xxxxxx, PXY, 16777346 >
    < Session-Id >
    [ DRMP ]
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ OC-Supported-Features ]
    [ OC-OLR ]
    *[ Supported-Features ]
    *[ Failed-AVP ]
    *[ Proxy-Info ]
    *[ Route-Record ]
    *[AVP]
```

## 6.2.9 MO-Data-Request (ODR) Command

The MO-Data-Request (DSR) command, indicated by the Command-Code field set to **xxxxx** and the "R" bit cleared in the Command Flags field, is sent from:

- the MME to the SCEF;
- the MME to the IWK-SCEF and
- the IWK-SCEF to the SCEF.

For the T6a, T6ai, T7 interfaces, the MO-Data-Request command format is specified as following:

Message Format:

```
< MO-Data-Request > ::= < Diameter Header: xxxxxx, PXY, 16777346 >
    < Session-Id >
    < User-Identifier >
    < Bearer-Identifier >
    [ DRMP ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Destination-Host ]
    { Destination-Realm }
    [ OC-Supported-Features ]
    *[ Supported-Features ]
    [ Non-IP-Data ]
```

```
*[ Failed-AVP ]
*[ Proxy-Info ]
*[ Route-Record ]
*[AVP]
```

## 6.2.10 MO-Data-Answer (ODA) Command

The MO-Data-Answer (ODA) command, indicated by the Command-Code field set to **xxxxxx** and the "R" bit cleared in the Command Flags field, is sent from:

- the SCEF to the MME;
- the SCEF to the IWK-SCEF and
- the IWK-SCEF to the MME.

For the T6a, T6ai and T7 interfaces, the MO-Data-Answer command format is specified as following:

Message Format:

```
< MO-Data-Answer > ::= < Diameter Header: xxxxxx, PXY, 16777346 >
    < Session-Id >
    [ DRMP ]
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ OC-Supported-Features ]
    [ OC-OLR ]
    *[ Supported-Features ]
    *[ Failed-AVP ]
    *[ Proxy-Info ]
    *[ Route-Record ]
    *[AVP]
```

## 6.2.11 MT-Data-Request (TDR) Command

The MT-Data-Request (TDR) command, indicated by the Command-Code field set to **xxxxx** and the "R" bit cleared in the Command Flags field, is sent from:

- the SCEF to the MME;
- the SCEF to the IWK-SCEF and
- the IWK-SCEF to the MME.

For the T6a, T6ai, T7 interfaces, the MT-Data-Request command format is specified as following:

Message Format:

```
< MT-Data-Request > ::= < Diameter Header: xxxxxx, PXY, 16777346 >
    < Session-Id >
    < User-Identifier >
    < Bearer-Identifier >
    [ DRMP ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Host }
    { Destination-Realm }
    [ OC-Supported-Features ]
```

```

*[ Supported-Features ]
[ Non-IP-Data ]
*[ Failed-AVP ]
*[ Proxy-Info ]
*[ Route-Record ]
*[AVP]

```

## 6.2.12 MT-Data-Answer (TDA) Command

The MT-Data-Answer (OSA) command, indicated by the Command-Code field set to **xxxxxx** and the "R" bit cleared in the Command Flags field, is sent from:

- the MME to the SCEF;
- the MME to the IWK-SCEF and
- the IWK-SCEF to the SCEF.

For the T6a, T6ai and T7 interfaces, the MT-Data-Answer command format is specified as following:

Message Format:

```

< MT-Data-Answer > ::= < Diameter Header: xxxxxx, PXY, 16777346 >
    < Session-Id >
    [ DRMP ]
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ OC-Supported-Features ]
    [ OC-OLR ]
    *[ Supported-Features ]
    *[ Failed-AVP ]
    *[ Proxy-Info ]
    *[ Route-Record ]
    *[AVP]

```

## 6.3 Result-Code AVP and Experimental-Result AVP Values

### 6.3.1 General

This section defines result code values that shall be supported by all Diameter implementations that conform to this specification.

### 6.3.2 Success

Result codes that fall within the Success category shall be used to inform a peer that a request has been successfully completed. The Result-Code AVP values defined in Diameter Base Protocol RFC 3588 [3] shall be applied.

### 6.3.3 Permanent Failures

Errors that fall within the Permanent Failures category shall be used to inform the peer that the request has failed, and should not be attempted again. The Result-Code AVP values defined in Diameter Base Protocol RFC 3588 [3] shall be applied. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and the Result-Code AVP shall be absent.

### 6.3.3.1 DIAMETER\_ERROR\_UNAUTHORIZED\_REQUESTING\_ENTITY (5510)

This result code shall be sent by the MME/SGSN or the IWK-SCEF to indicate that the SCEF is not allowed to request Monitoring services. This error code is defined in 3GPP TS 29.336 [5].

### 6.3.3.2 DIAMETER\_ERROR\_UNAUTHORIZED\_SERVICE (5511)

This result code shall be sent by the MME/SGSN or the IWK-SCEF to indicate that the specific service requested by the SCEF is not allowed as per local policies. This error code is defined in 3GPP TS 29.336 [5].

### 6.3.3.3 DIAMETER\_ERROR\_CONFIGURATION\_EVENT\_STORAGE\_NOT\_SUCCESSFUL (5513)

This result code shall be sent by the MME/SGSN to indicate that the specific service requested by the SCEF could not be stored. This error code is defined in 3GPP TS 29.336 [5].

### 6.3.3.4 DIAMETER\_ERROR\_CONFIGURATION\_EVENT\_NON\_EXISTANT (5514)

This result code shall be sent by the IWK-SCEF to indicate that the requested deletion by the MME/SGSN could not be performed because the event does not exist. This error code is defined in 3GPP TS 29.336 [5].

### 6.3.3.5 DIAMETER\_ERROR\_REQUESTED\_LOCATION\_NOT\_SERVED (5650)

This result code shall be sent by the MME/SGSN to indicate that the location for which a related monitoring event is configured (e.g. Number of UEs at a given geographical location) by the SCEF, is not served by the MME/SGSN.

### 6.3.3.6 DIAMETER\_ERROR\_USER\_UNKNOWN (5001)

This result code shall be sent by the SCEF to indicate that the user identified by the IMSI, MSISDN, or External-Identifier is unknown. This error code is defined in 3GPP TS 29.229 [4].

### 6.3.3.7 DIAMETER\_ERROR\_OPERATION\_NOT\_ALLOWED (5101)

This result code shall be sent by the SCEF to indicate that the operation is not allowed when an existing EPS bearer context for the user. This error code is defined in 3GPP TS 29.329 [17].

### 6.3.3.8 DIAMETER\_ERROR\_INVALID\_EPS\_BEARER (5xxx)

This result code shall be sent by the SCEF to indicate that there is no valid EPS bearer context for the user.

### 6.3.3.9 DIAMETER\_ERROR\_NIDD\_CONFIGURATION\_NOT\_AVAILABLE (5yyy)

This result code shall be sent by the SCEF to indicate that there is no valid NIDD configuration available.

### 6.3.3.10 DIAMETER\_ERROR\_SCEF\_REFERENCE\_ID\_UNKNOWN (5xxx)

This result code shall be sent by the SCEF to indicate that the SCEF reference ID is not known by the SCEF.

## 6.4 AVPs

### 6.4.1 General

The following table specifies the Diameter AVPs defined for the T6a/T6b interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-ID header of all AVPs defined in this specification shall be set to 3GPP (10415).

Table 6.4.1-1: T6a/T6b specific Diameter AVPs

Attribute Name	AVP Code	Section defined	Value Type	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
Communication-Failure-Information	4300	6.4.4	Grouped	M,V				No
Cause-Type	4301	6.4.5	Unsigned32	M,V				No
S1AP-Cause	4302	6.4.6	Unsigned32	M,V				No
RANAP-Cause	4303	6.4.7	Unsigned32	M,V				No
BSSGP-Cause	4309	6.4.8	Unsigned32	M,V				No
GMM-Cause	4304	6.4.9	Unsigned32	M,V				No
SM-Cause	4305	6.4.10	Unsigned32	M,V				No
Number-Of-UE-Per-Location-Configuration	4306	6.4.11	Grouped	M,V				No
Number-Of-UE-Per-Location-Report	4307	6.4.12	Grouped	M,V				No
UE-Count	4308	6.4.13	Unsigned32	M,V				No
Connection-Action	Xxxx	6.4.18	Unsigned32	M,V				No
Non-IP-Data	Xxx	6.4.19	Octetstring	M,V				No
NOTE 1: The AVP header bit denoted as "M" indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 3588 [3].								
NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.								

The following table specifies the Diameter AVPs re-used by the T6a/T6b interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within T6a/T6b.

Any other AVPs from existing Diameter Applications, except for the AVPs from Diameter Base Protocol, do not need to be supported. The AVPs from Diameter Base Protocol are not included in table 6.4.1-2, but they may be re-used for the T6a/T6b protocol.



Table 6.4.1-2: T6a/T6b re-used Diameter AVPs

Attribute Name	Reference	Comments
Monitoring-Event-Configuration	3GPP TS 29.336 [5]	This AVP shall contain the monitoring event to be configured at the MME/SGSN or the IWK-SCEF. See 6.4.2.
Monitoring-Event-Report	3GPP TS 29.336 [5]	This AVP shall contain the monitoring event reported by the MME/SGSN or the IWK-SCEF. See 6.4.3.
SCEF-Reference-ID	3GPP TS 29.336 [5]	
SCEF-ID	3GPP TS 29.336 [5]	
SCEF-Reference-ID-for-Deletion	3GPP TS 29.336 [5]	
Supported-Features	3GPP TS 29.229 [4]	
Feature-List-ID	3GPP TS 29.229 [4]	
Feature-List	3GPP TS 29.229 [4]	See 6.4.14
OC-Supported-Features	IETF RFC 7683 [9]	
OC-OLR	IETF RFC 7683 [9]	
Monitoring-Event-Config-Status	3GPP TS 29.336 [5]	This AVP shall contain the status of configuration of each monitoring event identified by an SCEF-ID and SCEF-Reference-ID.
DRMP	IETF draft-ietf-dime-drmp-03 [15]	see 6.4.15
User-Identifier	3GPP TS 29.336 [5]	See 6.4.16
Bearer-Identity	3GPP TS 29.212 [18]	See 6.4.17

## 6.4.2 Monitoring-Event-Configuration

The Monitoring-Event-Configuration AVP is of type Grouped. It shall contain the Monitoring event configuration related data. It is originally defined in 3GPP TS 29.336 [5].

For the T6a/T6b interface, the Monitoring-Event-Configuration AVP format is specified as following:

AVP format:

Monitoring-Event-Configuration ::= <AVP header: 3122 10415>

[ SCEF-Reference-ID ]  
 { SCEF-ID }  
 { Monitoring-Type }  
 \*[ SCEF-Reference-ID-for-Deletion ]  
 [ Maximum-Number-of-Reports ]  
 [ Monitoring-Duration ]  
 [ Charged-Party ]  
 [ UE-Reachability-Configuration ]  
 [ Location-Information-Configuration ]  
 \*[ Number-Of-UE-Per-Location-Configuration ]  
 \*[AVP]

### 6.4.3 Monitoring-Event-Report

The Monitoring-Event-Report AVP is of type Grouped. It shall contain the Monitoring event report data. It is originally defined in 3GPP TS 29.336 [5].

For the T6a/T6b interface, the Monitoring-Event-Report AVP format is specified as following:

AVP format:

```
Monitoring-Event-Report ::= <AVP header: 3123 10415>
    { SCEF-Reference-ID }
    [ SCEF-ID ]
    [ Monitoring-Type ]
    [ Reachability-Information ]
    [ EPS-Location-Information ]
    [ Communication-Failure-Information ]
    *[ Number-Of-UE-Per-Location-Report ]
    *[AVP]
```

The AVPs applicable for each Monitoring-Type reported by the MME/SGSN are specified under subclause 5.2.2.

### 6.4.4 Communication-Failure-Information

The Communication-Failure-Information AVP is of type Grouped. It shall contain the reason for communication failure.

AVP format:

```
Communication-Failure-Information ::= <AVP header: 4300 10415>
    [ Cause-Type ]
    [ S1AP-Cause ]
    [ RANAP-Cause ]
    [ BSSGP-Cause ]
    [ GMM-Cause ]
    [ SM-Cause ]
    *[AVP]
```

### 6.4.5 Cause-Type

The Cause-Type AVP is of type Unsigned32 and it shall identify the type of the S1AP-Cause. The following values are defined:

```
RADIO_NETWORK_LAYER (0)
TRANSPORT_LAYER (1)
NAS (2)
PROTOCOL (3)
MISCELLANEOUS (4)
```

## 6.4.6 S1AP-Cause

The S1AP-Cause AVP is of type Unsigned32. It shall contain a non-transparent copy of the S1AP cause code as specified subclause 9.2.1.3 of 3GPP TS 36.413 [13]. The RAN cause sub-category of the S1AP-Cause as specified in 3GPP TS 36.413 [13] shall be encoded in the Cause-Type AVP as specified in subclause 6.4.5 above.

## 6.4.7 RANAP-Cause

The RANAP-Cause AVP is of type Unsigned32. It shall contain the non-transparent copy of the cause value of the RANAP cause code as specified in subclause 9.2.1.4 of 3GPP TS 25.413 [11].

## 6.4.8 BSSGP-Cause

The BSSGP-Cause AVP is of type Unsigned32. It shall contain the non-transparent copy of the cause value of the BSSGP "Cause" as specified in subclause 11.3.8 in 3GPP TS 48.018 [14].

## 6.4.9 GMM-Cause

The GMM-Cause AVP is of type Unsigned32. It shall contain the GMM cause code as specified in subclause 10.5.5.14 of 3GPP TS 24.008 [12].

## 6.4.10 SM-Cause

The SM-Cause AVP is of type Unsigned32. It shall contain the SM cause code as specified in subclause 10.5.6.6 and 10.5.6.6A of 3GPP TS 24.008 [12].

## 6.4.11 Number-Of-UE-Per-Location-Configuration

The Number-Of-UE-Per-Location-Configuration AVP is of type Grouped. It shall contain the location information for which the number of UEs needs to be reported by the MME/SGSN.

AVP format:

```
Number-of-UE-Per-Location-Configuration ::= <AVP header: 4306 10415>
    { EPS-Location-Information }
    *[AVP]
```

## 6.4.12 Number-Of-UE-Per-Location-Report

The Number-Of-UE-Per-Location-Report AVP is of type Grouped. It shall contain the location information along with the number of UEs found at that location by the MME/SGSN.

AVP format:

```
Number-of-UE-Per-Location-Report ::= <AVP header: 4307 10415>
    { EPS-Location-Information }
    { UE-Count }
    *[AVP]
```

## 6.4.13 UE-Count

The UE-Count AVP is of type Unsigned32. It shall contain the number of UEs counted against a given criteria (say location information).

## 6.4.14 Feature-List AVP

### 6.4.14.1 Feature-List AVP for the T6a/T6b application

The syntax of this AVP is defined in 3GPP TS 29.229 [4].

For the S6t application, the meaning of the bits shall be as defined in table 6.4.14.1 -1 for the Feature-List-ID.

**Table 6.4.14.1-1: Features of Feature-List-ID used in S6t**

Feature bit	Feature	M/O	Description
0	MONTE	O	<p>Configuration and reporting of monitoring events</p> <p>This feature is applicable to from an SCEF with CIR/CIA command pair and the reporting of events to the SCEF with RIR/RIA command pair.</p> <p>If the MME/SGSN does not support this feature, the SCEF shall not send monitoring event configurations to the HSS within CIR.</p>
1	NIDD	O	<p>Support of Non-IP Data service over T6a</p> <p>This feature is applicable to OSR/OSA, ODR/ODA and TDR/TDA command pairs.</p> <p>If the SCEF does not indicate support of this feature in an OSA, the MME may store this information and not send any further OSR commands to that SCEF.</p>
<p>Feature bit: The order number of the bit within the Supported-Features AVP, e.g. "1".            Feature: A short name that can be used to refer to the bit and to the feature, e.g. "MONTE".            M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O").            Description: A clear textual description of the feature.</p>			

## 6.4.15 DRMP

The DRMP AVP is of type Enumerated and it is defined in IETF draft-ietf-dime-drmp-03 [15]. This AVP allows the MME, the SGSN, the SCEF and the IWK-SCEF to indicate the relative priority of Diameter messages.

## 6.4.16 User-Identifier

The User-Identifier AVP is of type Grouped and it contains the different identifiers used by the UE.

It is originally defined in 3GPP TS 29.336 [5]

AVP format:

```
User-Identifier ::= <AVP header: 3102 10415>
    [ User-Name ]
    *[AVP]
```

This AVP shall contain the User-Name AVP, i.e. it shall not be empty. The IMSI of the UE shall be included in the User-Name AVP.

## 6.4.17 Bearer-Identifier

The Bearer-Identifier AVP contains the identity of the EPS bearer used to identify the T6a connection between the MME and the SCEF. It is defined in 3GPP TS 29.212 [18].

## 6.4.18 Connection-Action

The Connection-Action AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 6.4.18-1:

**Table 6.4.18-1: Connection-Action**

Bit	Name	Description
0	Connection establishment	This bit shall be set if the request applies to a T6a Connection establishment.
1	Connection release	This bit shall be set if the request applies to a T6a Connection release.
NOTE:	Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.	

## 6.4.19 Non-IP-Data

The Non-IP-Data AVP is of type OctetString and it contains the Non-IP data conveyed between the MME and the SCEF.

---

## Annex A (normative): Diameter overload control mechanism

### A.1 T6a/b and T7 interfaces

#### A.1.1 General

The Diameter overload control mechanism is an optional feature over the T6a/b and T7 interface.

It is recommended to make use of the IETF RFC 7683 [9] on the T6a/b and T7 interface where, when applied, the MME/SGSN shall behave as a reacting node and the SCEF as a reporting node.

#### A.1.2 SCEF behaviour

The SCEF requests traffic reduction from the MME/SGSN and the IWK-SCEF when it is in an overload situation, by including OC-OLR AVP in answer commands as described in IETF RFC 7683 [9].

The SCEF identifies that it is in an overload situation by implementation specific means. For example, the SCEF may take into account the traffic over the S6t interfaces or other interfaces, the level of usage of internal resources (CPU, memory), the access to external resources etc.

The SCEF determines the specific contents of the OC-OLR AVP in overload reports and the SCEF decides when to send OC-OLR AVPs by implementation specific means.

The SCEF may decide to deactivate Monitoring events to reduce the number of Reporting-Information-Requests sent for reporting monitoring events.

#### A.1.3 MME/SGSN behaviour

The MME/SGSN and the IWK-SCEF apply required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [9].

Requested traffic reduction is achieved by the MME/SGSN by implementation specific means. It may implement throttling of monitoring event reports or stop reporting with prioritization (e.g. prioritisation on the type of events, or that one time reporting takes priority over continuous reporting, ...).

#### A.1.4 IWK-SCEF behaviour

The IWK-SCEF applies required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [9].

Requested traffic reduction is achieved by the IWK-SCEF by implementation specific means. For example, it may implement throttling of monitoring event report with prioritization.

---

## Annex B (normative): Diameter message priority mechanism

### B.1 General

IETF draft-ietf-dime-drmp-03 [15] specifies a Diameter routing message priority mechanism that allows Diameter nodes to indicate the relative priority of Diameter messages. With this information, other Diameter nodes may leverage the relative priority of Diameter messages into routing, resource allocation and also abatement decisions when overload control is applied.

### B.2 T6a, T6ai, T6b, T6bi, T7 interfaces

The Diameter message priority mechanism is an optional feature which may apply on one or several of the T6a, T6ai, T6b, T6bi, T7 interfaces.

It is recommended to make use of IETF draft-ietf-dime-drmp-03 [15] over the T6a, T6ai, T6b, T6bi, T7 interfaces of an operator network when the overload control defined in Annex A is applied on these interfaces.

A 3GPP functional entity supporting the Diameter message priority mechanism over one or several of the T6a, T6ai, T6b, T6bi, T7 interfaces shall comply with IETF draft-ietf-dime-drmp-03 [15]. In particular, when priority is required, it shall include the DRMP AVP indicating a priority level in the requests it sends, and prioritise received requests according to the priority level received within the DRMP AVP. It shall prioritise received answers according to the priority level received within the DRMP AVP if present, otherwise according to the priority level of the corresponding request. It shall include the DRMP AVP in the answer to a received request if the required priority of the answer is different from the one of the request. The decisions of the 3GPP functional entity for a required priority and for the priority level value are implementation specific.

Diameter requests related to high priority traffic should contain a DRMP AVP with a high priority of which the level value is operator dependent.

---

## Annex C (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2015-05					Skeleton of the TS after CT4#69	-	0.0.0
2015-11					TS after CT4#71	0.0.0	0.1.0
2015-12	CT#70	CP-150625			Presented for information	0.1.0	1.0.0
2016-02					TS after CT4#72	1.0.0	1.1.0
2016-03	CT#71	CP-160119			Presented for approval	1.1.0	2.0.0
2016-03	CT#71				Version 13.0.0. created after CT#71	2.0.0	13.0.0



---

# History

<b>Document history</b>		
V13.0.0	May 2016	Publication