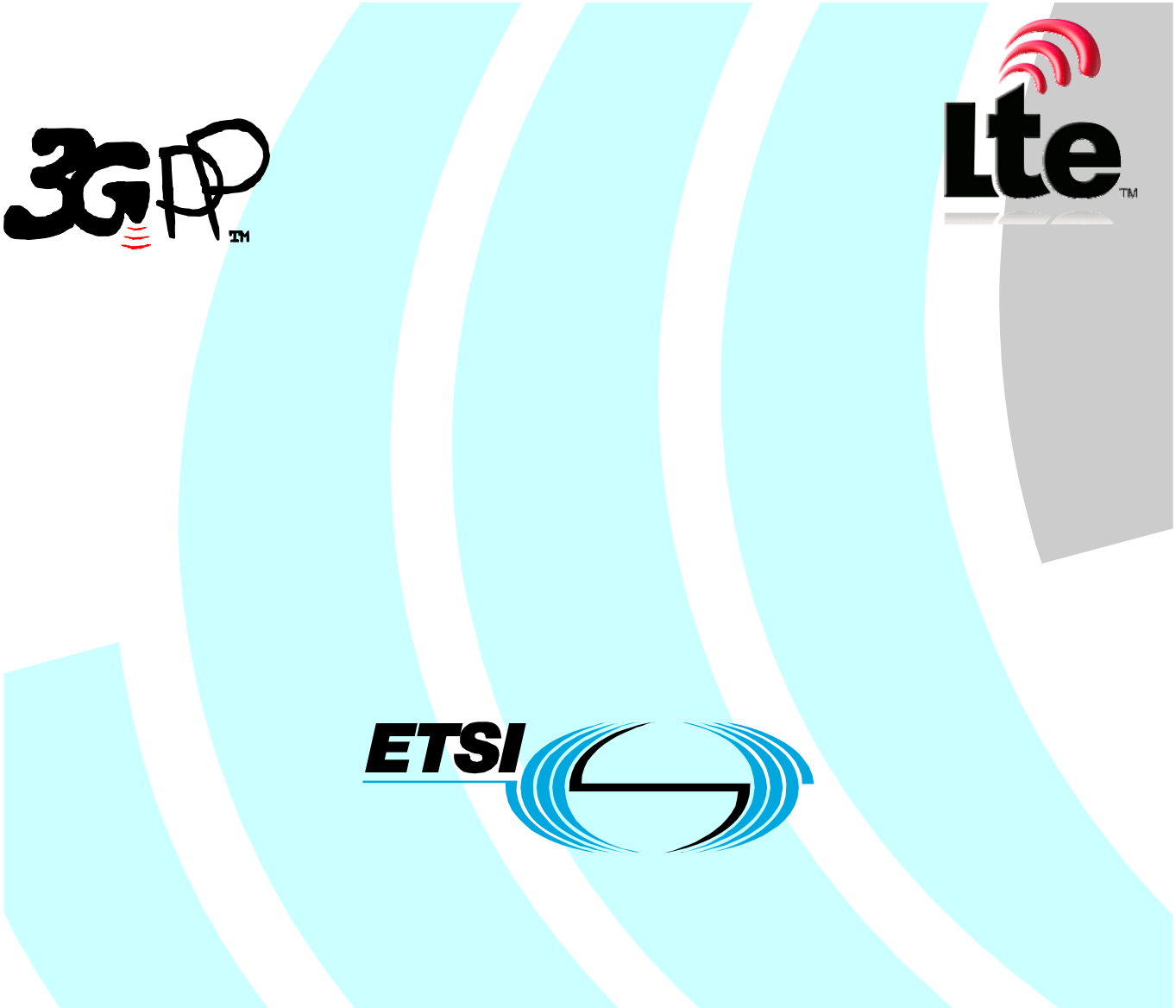
ETSI TS 129 272 V8.1.1 (2009-01)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
Evolved Packet System (EPS);
Mobility Management Entity (MME)
and Serving GPRS Support Node (SGSN)
related interfaces based on Diameter protocol
(3GPP TS 29.272 version 8.1.1 Release 8)



Reference
DTS/TSGC-0429272v811

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

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 (http://webapp.etsi.org/IPR/home.asp).

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.

Contents

Foreword

This Technical Specification has been produced by the 3rd 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 Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related diameter-based interfaces towards the Home Subscriber Server (HSS), and the MME and the SGSN related diameter-based interface towards the Equipment Identity Register (EIR).

This specification defines the Diameter application for the MME-HSS, S6a reference point, and for the SGSN-HSS, S6d reference point. The interactions between the HSS and the MME/SGSN are specified, including the signalling flows.

This specification defines the Diameter application for the MME-EIR, S13 reference point, and for the SGSN-EIR, S13' reference point. The interactions between the MME/SGSN and the EIR are specified, including the signalling flows.

If there is no specific indication, the SGSN in the specification refers to a S4-SGSN which supports S4 interface.

The Evolved Packet System stage 2 description (architecture and functional solutions) is specified in 3GPP TS 23.401 [2] and in 3GPP TS 23.060 [12].

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 23.401: "GPRS enhancements for E-UTRAN access ".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] IETF RFC 3588: "Diameter Base Protocol".

[5] 3GPP TS 33.401: "3GPP System Architecture Evolution: Security Architecture".

[6] IETF RFC 4005: "Diameter Network Access Server Application".

[7] IETF RFC 2234: "Augmented BNF for syntax specifications".

[8] 3GPP TS 32.299: "Charging management; Diameter charging applications".

[9] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol".

[10] 3GPP TS 29.212: "Policy and Charging Control over Gx reference point".

[11] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[12] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[13] 3GPP TS 22.016: "International Mobile station Equipment Identities (IMEI)".

[14] IETF RFC 2960: "Stream Control Transmission Protocol".

[15] IETF RFC 3309: "SCTP Checksum Change".

[16] 3GPP TS 33.210: "3G Security; Network Domain Security; IP Network Layer Security"..

[17] 3GPP TS 29.228: "IP multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and Message Elements".

[18] 3GPP TS 33.102: "3G Security; Security Architecture".

[19] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[20] IETF Draft draft-ietf-dime-mip6-split-12: "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction", work in progress.

[21] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[22] 3GPP TS 32.298: "Charging Management; CDR parameter description".

[23] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[24] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[25] 3GPP TS 29.329: "Sh Interface based on the Diameter protocol".

[26] IETF Draft draft-ietf-dime-mip6-integrated-10: "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", work in progress.

[27] IETF RFC 4004: "Diameter Mobile IPv4 Application".

[28] 3GPP2 A.S0022: "Interoperability Specification (IOS) for Evolved High Rate Packet Data (eHRPD) Radio Access Network Interfaces and Interworking with Enhanced Universal Terrestrial Radio Access Network (E-UTRAN)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Editor"s note: This section to be completed or removed later.

3.2 Symbols

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

Editor"s note: This section to be completed or removed later.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

AVP	Attribute Value Pair
C	Conditional
EIR	Equipment Identity Register
HSS	Home Subscriber Server
IE	Information Element
M	Mandatory
MME	Mobility Management Entity

O	Optional
ODB	Operator Determined Barring

4 General Description

This document describes the S6a/S6d and S13/S13' interfaces related procedures, message parameters and protocol specifications.

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 [17].

5 MME – HSS (S6a) and SGSN – HSS (S6d)

5.1 Introduction

The S6a interface enables the transfer of subscriber related data between the MME and the HSS as described in the 3GPP TS 23.401 [2].

The S6d interface enables the transfer of subscriber related data between the SGSN and the HSS as described in 3GPP TS 23.060 [12].

5.2 Mobility Services

5.2.1 Location Management Procedures

5.2.1.1 Update Location

5.2.1.1.1 General

The Update Location Procedure shall be used between the MME and the HSS and between the SGSN and the HSS to update location information in the HSS. The procedure shall be invoked by the MME or SGSN and is used:

- to inform the HSS about the identity of the MME or SGSN currently serving the user, and optionally in addition;
- to update MME or SGSN with user subscription data;
- to provide the HSS with other user data, such as Terminal Information.

This procedure is mapped to the commands Update-Location-Request/Answer (ULR/ULA) in the Diameter application specified in chapter 7.

Table 5.2.1.1.1/1 specifies the involved information elements for the request.

Table 5.2.1.1.1/2 specifies the involved information elements for the answer.

Table 5.2.1.1.1/1: Update Location Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Name (See IETF RFC 3588 [4])	User-Name	M	This information element shall contain the permanent identity of the user, i.e. the IMSI. See 3GPP TS 23.003 [3].
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Terminal Information (See 7.3.3)	Terminal-Information	O	This information element shall contain information about the user"s mobile equipment. Within this Information Element, only the IMEI and the Software-Version AVPs shall be used on the S6a/S6d interface.
ULR Flags (See 7.3.7)	ULR-Flags	M	This Information Element contains a bit mask. See 7.3.7 for the meaning of the bits.
Visited PLMN Id (See 7.3.9)	Visited-PLMN-Id	M	This IE shall contain the MCC and the MNC, see 3GPP TS 23.003[3]. It may be used to apply roaming based features.
RAT Type (See 7.3.13)	RAT-Type	M	This Information Element contains the radio access type the UE is using. See section 7.3.13 for details.

Table 5.2.1.1.1/2: Update Location Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Result (See 7.4)	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6a/S6d errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. The following errors are applicable: - User Unknown - Unknown EPS Subscription - RAT Not Allowed - Roaming Not Allowed
ULA-Flags (See 7.3.8)	ULA-Flags	C	This Information Element contains a bit mask. See 7.3.8 for the meaning of the bits. It shall be present only when the Result-Code AVP is DIAMETER_SUCCESS.
Subscription Data (See 7.3.2)	Subscription-Data	C	This Information Element contains the subscription profile of the user. It shall be present if success is reported, unless an explicit "skip subscriber data" indication was present in the request.

5.2.1.1.2 Detailed behaviour of the MME and the SGSN

The MME shall make use of this procedure to update the MME identity stored in the HSS (e.g. at initial attach, inter MME tracking area update or radio contact after HSS reset).

The SGSN shall make use of this procedure to update the SGSN identity stored in the HSS (e.g. at initial attach, inter SGSN routing area update or radio contact after HSS reset).

If the Update Location request is to be sent due to an inter node (SGSN to MME) update and the previous SGSN does not support Idle Mode Signalling Reduction, the MME shall set the "Single-Registration-Indication" flag in the ULR-Flags information element in the request.

A combined MME/SGSN shall set the "Skip Subscriber Data" flag in the ULR-Flags if subscriber data are already available due to a previous location update.

When receiving an Update Location response from the HSS the MME or SGSN shall check the result code. If it indicates success the MME or SGSN shall store the received subscription profile (if any).

If trace data are received in the subscriber data, the MME or SGSN shall start a Trace Session. For details, see 3GPP TS 32.422 [23].

5.2.1.1.3 Detailed behaviour of the HSS

When receiving an Update Location request the HSS shall check whether the IMSI is known.

If it is not known, a Result Code of DIAMETER_ERROR_USER_UNKNOWN is returned.

If it is known, but the subscriber has no EPS subscription, the HSS may (as an operator option) return a Result Code of DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION.

The HSS shall check whether the RAT type the UE is using is allowed. If it is not, a Result Code of DIAMETER_ERROR_RAT_NOT_ALLOWED is returned.

The HSS shall check whether roaming is not allowed in the VPLMN due to ODB. If so a Result Code of DIAMETER_ERROR_ROAMING_NOT_ALLOWED is returned.

If the Update Location Request is received over the S6a interface, the HSS shall send a Cancel Location Request (CLR; see chapter 7.2.7) to the previous MME (if any) and replace the stored MME-Identity with the received value (the MME-Identity is received within the Origin-Host-AVP). The HSS shall reset the "UE purged in MME" flag.

If the Update Location Request is received over the S6d interface, the HSS shall send a Cancel Location Request (CLR; see chapter 7.2.7, or MAP Cancel Location) to the previous SGSN (if any) and replace the stored SGSN-Identity with the received value (the SGSN-Identity is received within the Origin-Host-AVP). The HSS shall reset the "UE purged in SGSN" flag.

If the "Single-Registration-Indication" flag was set in the received request, the HSS shall send a MAP Cancel Location message to the SGSN, delete the stored SGSN address and SGSN number and set the "MS purged in SGSN" flag.

If no result code has been sent to the MME or SGSN so far, the HSS shall include the subscription data in the ULA command, unless an explicit "skip subscriber data" indication has been received in the request, taking into account the supported/unsupported features of the MME or SGSN and return a Result Code of DIAMETER_SUCCESS.

If a Result-Code of DIAMETER_SUCCESS is returned, the HSS shall set the Separation Indication in the response.

5.2.1.2 Cancel Location

5.2.1.2.1 General

The Cancel Location Procedure shall be used between the HSS and the MME and between the HSS and the SGSN to delete a subscriber record from the MME or SGSN. The procedure shall be invoked by the HSS and is used:

- to inform the MME or SGSN about the subscriber"s subscription withdrawal or
- to inform the MME or SGSN about an ongoing update procedure i.e. MME or SGSN change.

This procedure is mapped to the commands Cancel-Location-Request/Answer (CLR/CLA) in the Diameter application specified in chapter 7.

Table 5.2.1.2.1/1 specifies the involved information elements for the request.

Table 5.2.1.2.1/2 specifies the involved information elements for the answer.

Table 5.2.1.2.1/1: Cancel Location Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Name (See IETF RFC 3588 [4])	User-Name	M	This information element shall contain the permanent identity of the user, i.e. the IMSI. See 3GPP TS 23.003 [3].
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Cancellation Type (See 7.3.24)	Cancellation-Type	M	Defined values that can be used are: - MME-Update Procedure, - SGSN-Update Procedure, - Subscription Withdrawal, - Update Procedure_IWF.

Table 5.2.1.2.1/2: Cancel Location Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Result (See 7.4)	Result-Code / Experimental-Result	M	The result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol.

5.2.1.2.2 Detailed behaviour of the MME and the SGSN

When receiving a Cancel Location request the MME or SGSN shall check whether the IMSI is known.

If it is not known, a result code of DIAMETER_SUCCESS is returned.

If it is known, the MME or SGSN shall check the Cancellation Type and act accordingly. For details see 3GPP TS 23.401[2] and 3GPP TS 23.060[12]. Also in this case a result code of DIAMETER_SUCCESS is returned.

When a UE is served by a single combined MME/SGSN for both E-UTRAN and non-E-UTRAN access, the combined MME/SGSN shall check the Cancellation-Type. If it indicates Subscription Withdrawal or Update Procedure_IWF, the CLR is processed both in the MME part and in the SGSN part of the combined node. Otherwise, the CLR is processed only in the affected part of the combined node and subscription data are kept for the not affected part.

5.2.1.2.3 Detailed behaviour of the HSS

The HSS shall make use of this procedure when the subscriber"s subscription is withdrawn by the HSS operator and when the HSS detects that the UE has moved to a new MME or SGSN area.

The HSS shall include a cancellation type of "Subscription Withdrawal" if the subscriber"s subscription is withdrawn by the operator and shall include a cancellation type of "MME Update Procedure" if the UE moved to a new MME area and shall include a cancellation type of "SGSN Update Procedure" if the UE moved to a new SGSN area.

5.2.1.3 Purge UE

5.2.1.3.1 General

The Purge UE Procedure shall be used between the MME and the HSS and between the SGSN and the HSS to indicate that the subscriber"s profile has been deleted from the MME or SGSN either by an MMI interaction or automatically, e.g. because the UE has been inactive for several days.

This procedure is mapped to the commands Purge-UE-Request/Answer (PUR/PUA) in the Diameter application specified in chapter 7.

Table 5.2.1.3.1/1 specifies the involved information elements for the request.

Table 5.2.1.3.1/2 specifies the involved information elements for the answer.

Table 5.2.1.3.1/1: Purge UE Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Name (See IETF RFC 3588 [4])	User-Name	M	This information element shall contain the permanent identity of the user, i.e. the IMSI. See 3GPP TS 23.003 [3].
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 5.2.1.3.1/2: Purge UE Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Result (See 7.4)	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used to indication success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6a/S6d errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. The following errors are applicable: - User Unknown
PUA-Flags (See 7.3.48)	PUA-Flags	C	This Information Element shall contain a bit mask. See section 7.3.48 for the meaning of the bits. It shall be present only when the Result-Code AVP is DIAMETER_SUCCESS.

5.2.1.3.2 Detailed behaviour of the MME and the SGSN

The MME shall make use of this procedure to set the "UE Purged in the MME" flag in the HSS when the subscription profile is deleted from the MME database due to MMI interaction or after long UE inactivity.

The SGSN shall make use of this procedure to set the "UE Purged in SGSN" flag in the HSS when the subscription profile is deleted from the SGSN database due to MMI interaction or after long UE inactivity.

When receiving a Purge UE response from the HSS the MME shall check the Result Code. If it indicates success, the MME shall check the PUA flag "freeze M-TMSI", and if set freeze the M-TMSI i.e. block it for immediate re-use.

When receiving a Purge UE response from the HSS the SGSN shall check the Result Code. If it indicates success, the SGSN shall check the PUA flag "freeze P-TMSI", and if set freeze the P-TMSI i.e. block it for immediate re-use.

5.2.1.3.2 Detailed behaviour of HSS

When receiving a Purge UE request the HSS shall check whether the IMSI is known.

If it is not known, a result code of DIAMETER_ERROR_USER_UNKNOWN shall be returned.

If it is known, the HSS shall set the result code to DIAMETER_SUCCESS and compare the received identity in the Origin-Host with the stored MME-Identity and/or with the stored SGSN-Identity. If they are identical the HSS shall set the PUA flags "freeze M-TMSI" and/or "freeze P-TMSI" in the answer message and set the flag "UE purged in MME" and/or set the flag "UE purged in SGSN"; otherwise it shall clear the PUA flags "freeze M-TMSI" and "freeze P-TMSI..

5.2.2 Subscriber Data Handling Procedures

5.2.2.1 Insert Subscriber Data

5.2.2.1.1 General

The Insert Subscriber Data Procedure shall be used between the HSS and the MME and between the HSS and the SGSN for updating certain user data in the MME or SGSN in the following situations:

- due to administrative changes of the user data in the HSS and the user is now located in an MME or SGSN, i.e. if the user was given an subscription and the subscription has changed;
- the operator has applied, changed or removed Operator Determined Barring for this user.
- activate subscriber tracing in the MME or the SGSN

This procedure is mapped to the commands Insert Subscriber Data-Request/Answer (IDR/IDA) in the Diameter application specified in chapter 7.

Table 5.2.2.1.1/1 specifies the involved information elements for the request.

Table 5.2.2.1.1/2 specifies the involved information elements for the answer.

Table 5.2.2.1.1/1: Insert Subscriber Data Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Name (See IETF RFC 3588 [4])	User-Name	M	This information element shall contain the permanent identity of the user, i.e. the IMSI. See 3GPP TS 23.003 [3].
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Subscription Data (See 7.3.2)	Subscription-Data	M	This Information Element shall contain the part of the subscription profile that either is to be added to the subscription profile stored in the MME or SGSN or is replacing a part of the subscription profile stored in the MME or SGSN.

Table 5.2.2.1.1/2: Insert Subscriber Data Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Result (See 7.4)	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. Result-Code AVP shall be used to indicate success / errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6a/S6d errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. The following errors are applicable in this case: - User Unknown
IDA-Flags (See 7.3.47)	IDA-Flags	C	This Information Element shall contain a bit mask. See 7.3.47 for the meaning of the bits.

5.2.2.1.2 Detailed behaviour of the MME and the SGSN

When receiving an Insert Subscriber Data request the MME or SGSN shall check whether the IMSI is known.

If it is not known, a result code of DIAMETER_ERROR_USER_UNKNOWN shall be returned.

If it is known, the MME or SGSN shall replace the specific part of the stored subscription data with the received data, or shall add the received data to the stored data, and acknowledge the Insert Subscriber Data message by returning an Insert Subscriber Data Answer. If the addition or update of the subscription data succeeds in the MME or SGSN, the Result-Code shall be set to DIAMETER_SUCCESS.

In addition, if due to regional subscription restrictions or access restrictions the entire SGSN area is restricted, SGSN shall report it to the HSS by returning the "SGSN Area Restricted" indication within the IDA flags.

If the MME or SGSN cannot fulfil the received request due to other reasons, e.g. due to a database error, it shall set Result-Code to DIAMETER_UNABLE_TO_COMPLY. In this case the MME or SGSN shall mark the subscription record "Subscriber to be restored in HSS".

If trace data are received in the subscriber data, the MME or SGSN shall start a Trace Session. For details, see 3GPP TS 32.422 [23].

5.2.2.1.3 Detailed behaviour of HSS

The HSS shall make use of this procedure to replace a specific part of the user data stored in the MME or SGSN with the data sent, or to add a specific part of user data to the data stored in the MME or SGSN.

When receiving an Insert Subscriber Data answer with "SGSN Area Restricted" the HSS shall set the SGSN area restricted flag as "SGSN area restricted".

5.2.2.2 Delete Subscriber Data

5.2.2.2.1 General

This procedure shall be used between the MME and the HSS and between the SGSN and the HSS, to remove some or all data of the HSS user profile stored in the MME or SGSN. The procedure shall be invoked by the HSS and it corresponds to the functional level operation Delete Subscriber Data (see 3GPP TS 23.401[2]).

It shall be used to remove:

- all or a subset of the EPS subscription data (APN Configuration Profile) for the subscriber from the MME or SGSN;
- the regional subscription;
- the subscribed charging characteristics;
- Session Transfer Number for SRVCC;
- trace data.

This procedure is mapped to the commands Delete-Subscriber-Data-Request/Answer (DSR/DSA) in the Diameter application specified in chapter 7.

Table 5.2.2.2.1/1 specifies the involved information elements for the request.

Table 5.2.2.2.1/2 specifies the involved information elements for the answer.

Table 5.2.2.2.1/1: Delete Subscriber Data Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Name (See IETF RFC 3588 [4])	User-Name	M	This information element shall contain the permanent identity of the user, i.e. the IMSI. See 3GPP TS 23.003 [3].
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
DSR Flags (See 7.3.25)	DSR-Flags	M	This Information Element shall contain a bit mask. See 7.3.25 for the meaning of the bits.
Trace Reference (See 7.3.64)	Trace-Reference	C	This parameter shall contain the same value as used for the activation of the Trace Session. This element shall be present only if the "Trace Data Withdrawal" bit is set in the DSR-Flags.
Context Identifier (See 7.3.27)	Context-Identifier	C	This parameter shall identify the PDN subscription context or GPRS-PDP context that shall be deleted. This element shall be present only if the "PDN subscription contexts Withdrawal" bit or the "PDP context withdrawal" bit is set in the DSR-Flags.

Table 5.2.2.2.1/2: Delete Subscriber Data Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Result (See 7.4)	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6a/S6d errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
DSA Flags (See 7.3.26)	DSA-Flags	C	This Information Element shall contain a bit mask. See 7.3.26 for the meaning of the bits.

5.2.2.2.2 Detailed behaviour of the MME and the SGSN

When receiving a Delete Subscriber Data request, the MME or SGSN shall check whether the IMSI is known.

If it is not known, a result code of DIAMETER_ERROR_USER_UNKNOWN shall be returned.

If it is known, the MME or SGSN shall delete the corresponding data according to the indication as sent in the request, and acknowledge the Delete Subscriber Data message by returning a Delete Subscriber Data Answer.

If the deletion of the subscription data succeeds in the MME or SGSN, the Result-Code shall be set to DIAMETER_SUCCESS.

If the Regional Subscription is deleted from the subscription data, the SGSN shall check for its routing areas whether they are allowed or not. If the entire SGSN area is restricted, SGSN shall report it to the HSS by returning the "SGSN Area Restricted" indication within the DSA flags.

If the EPS Subscription Data is deleted from the subscription data, the MME shall check whether all EPS Subscription Data for the subscriber is deleted or if only a subset of the stored EPS Subscription Data for the subscriber is deleted, the MME or SGSN may then deactivate the associated affected active EPS bearers.

If the Subscribed Charging Characteristics are deleted from the subscription data, the MME or SGSN shall replace the Subscribed Charging Characteristics by a local default value or delete the Subscribed Charging Characteristics in the MME or SGSN.

If the MME or SGSN cannot fulfil the received request for other reasons, e.g. due to a database error, it shall set the Result-Code to DIAMETER_UNABLE_TO_COMPLY. In this case, the MME or SGSN shall mark the subscription record "Subscriber to be restored in HSS".

If trace data are deleted from the subscription data, the MME or SGSN shall deactivate the Trace Session identified by the trace reference. For details, see 3GPP TS 32.422 [23].

5.2.2.2.3 Detailed behaviour of the HSS

The HSS shall make use of this procedure to remove deleted subscription data from the MME or SGSN.

When receiving a Delete Subscriber Data Answer with "SGSN Area Restricted" the HSS shall set the SGSN area restricted flag as "SGSN area restricted".

5.2.3 Authentication Procedures

5.2.3.1 Authentication Information Retrieval

5.2.3.1.1 General

The Authentication Information Retrieval Procedure shall be used by the MME and by the SGSN to request Authentication Information from the HSS.

This procedure is mapped to the commands Authentication-Information-Request/Answer (AIR/AIA) in the Diameter application specified in chapter 7.

Table 5.2.3.1.1/1 specifies the involved information elements for the request.

Table 5.2.3.1.1/2 specifies the involved information elements for the answer.

Table 5.2.3.1.1/1: Authentication Information Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Name (See IETF RFC 3588 [4])	User-Name	M	This information element shall contain the permanent identity of the user, i.e. the IMSI. See 3GPP TS 23.003 [3].
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Requested E-UTRAN Authentication Info (See 7.3.11)	Requested-EUTRAN-Authentication-Info	C	This information element shall contain the information related to authentication requests for E-UTRAN.
Requested UTRAN/GERAN Authentication Info (See 7.3.12)	Requested-UTRAN-GERAN Authentication-Info	C	This information element shall contain the information related to authentication requests for UTRAN or GERAN.
Visited PLMN ID (See 7.3.9)	Visited-PLMN-ID	M	This IE shall contain the MCC and the MNC of the visited PLMN, see 3GPP TS 23.003 [3].
Requesting Node Type (See 7.3.61)	Requesting-Node-Type	O	This AVP shall indicate the type of node requesting authentication vectors from HSS, and it shall have 3 possible values: 1) MME (this shall indicate that the requesting node is a stand alone MME) 2) SGSN (this shall indicate that the requesting node is a stand alone SGSN) 3) MME/SGSN (this indicate that the requesting node is a combined MME/SGSN)

Table 5.2.3.1.1/2: Authentication Information Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.4)	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. This IE shall contain the Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6a/S6d errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. The following errors are applicable in this case: - User Unknown - Unknown EPS Subscription
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Authentication Info (See 7.3.17)	Authentication-Info	C	This IE shall contain the Authentication Vectors.

5.2.3.1.2 Detailed behaviour of the MME and the SGSN

The MME or SGSN shall make use of this procedure in order to retrieve the Authentication Vectors from the HSS.

If the request is triggered by a synchronization failure, the MME or SGSN shall include the Re-Synchronization Information in the request.

A stand alone MME shall include the Requested-EUTRAN-Authentication-Info AVP and shall not include the Requested-UTRAN-GERAN-Authentication-Info AVP in the request. The Immediate-Response-Preferred AVP should be present if a EUTRAN-Vector is needed for immediate use.

A stand alone SGSN shall not include the Requested-EUTRAN-Authentication-Info AVP and shall include the Requested-UTRAN-GERAN-Authentication-Info AVP in the request. The Immediate-Response-Preferred AVP should be present if a UTRAN/GERAN-Vector is needed for immediate use.

A combined MME/SGSN may include both the Requested-EUTRAN-Authentication-Info AVP and the Requested-UTRAN-GERAN-Authentication-Info AVP in the request. If so, not both AVPs shall have the Immediate-Response-Preferred AVP present. The presence of an Immediate-Response-Preferred AVP should indicate that a vector is needed for immediate use.

When receiving an Authentication Information response from the HSS, the MME or SGSN shall check the Result Code. If it indicates success and Authentication Information is present in the result, the MME or SGSN shall use the received vectors. For details see 3GPP TS 33.401 [5].

5.2.3.1.3 Detailed behaviour of the HSS

When receiving an Authentication Information request the HSS shall check whether the IMSI is known.

If it is not known, a result code of DIAMETER_ERROR_USER_UNKNOWN is returned. If it is known, but the subscriber has no EPS or GPRS subscription, the HSS may (as a configuration option) return a result code of DIAMETER_ERROR_UNKNOWN_ EPS_SUBSCRIPTION.

The HSS shall then request the AuC to generate the corresponding requested Authentication Vectors (AVs). Subject to load considerations and/or other implementation specific considerations which may be based on the presence of an Immediate-Response-Preferred AVP, less AVs than the requested number of AVs may be generated.

When receiving AVs from the AuC, the HSS shall generate the KASME before sending the response to the MME. For details see 3GPP TS 33.401 [5]. KASME generation is not performed before sending the response to the SGSN.

The HSS may use the value received in the Requesting-Node-Type AVP to indicate the AuC the type of node requesting authentication vectors, so the AuC can keep separate sequence number (SQN) in the generated vectors.

If the Requested-EUTRAN-Authentication-Info AVP is present in the request, the HSS shall download E-UTRAN authentication vectors to the MME. If the Requested-UTRAN-GERAN-Authentication-Info AVP is present in the request, the HSS shall download UTRAN or GERAN authentication vectors to the SGSN.

If the Immediate Response Preferred parameter has been received, the HSS may use it together with the number of requested vectors and the number of vectors stored in the HSS that are pre-computed to determine the number of vectors to be obtained from the AuC. The HSS may return less number of vectors than requested to the MME or SGSN. If both the Requested-EUTRAN-Authentication-Info AVP and the Requested-UTRAN-GERAN-Authentication-Info AVP are in the request, and one of them includes the Immediate Response Preferred parameter, the HSS may omit the vectors request that are not for immediate use. KASME is always computed for each E-UTRAN vector due to the PLMN-binding before sending the response to the MME independent of the presence of the Immediate Response Preferred parameter.

The HSS shall then return the result code DIAMETER_SUCCESS and the generated AVs (if any) to the MME or SGSN.

5.2.4 Fault Recovery Procedures

5.2.4.1 Reset

5.2.4.1.1 General

The Reset Procedure shall be used by the HSS, after a restart, to indicate to the MME and to the SGSN that a failure has occurred.

This procedure is mapped to the commands Reset-Request/Answer (RSR/RSA) in the Diameter application specified in chapter 7.

Table 5.2.4.1.1/1 specifies the involved information elements for the request.

Table 5.2.4.1.1/2 specifies the involved information elements for the answer.

Table 5.2.4.1.1/1: Reset Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Id List (See 7.3.50)	User-Id	O	This IE shall contain a list of User-Ids where a User-Id comprises the leading digits of a User Name (i.e. MCC, MNC, leading digits of MSIN) and it shall identify the set of subscribers whose user names begin with the User-Id. The HSS may include this information element if the occurred failure is limited to subscribers identified by one or more User-Ids.
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 5.2.4.1.1/2: Reset Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Result (See 7.4)	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6a/S6d errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

5.2.4.1.2 Detailed behaviour of the MME and the SGSN

When receiving a Reset message the MME or SGSN shall mark all impacted subscriber records "Subscriber to be restored in HSS". The MME or SGSN shall make use of the received HSS-Address and may make use of the received User-Id-List (if any) in order to determine which subscriber records are impacted.

At the next authenticated radio contact with the UE concerned, if the subscriber is marked as "subscriber to be restored in HSS", the restoration procedure shall be triggered.

5.2.4.1.3 Detailed behaviour of the HSS

The HSS shall make use of this procedure in order to indicate to the MME and SGSN that the HSS has restarted and may have lost the current MME-Identity and SGSN-Identity of some of its subscribers who may be currently roaming in the MME area and SGSN-Identity, and that the HSS, therefore, cannot send a Cancel Location messages or Insert Subscriber Data messages when needed.

The HSS optionally may include a list of Ids identifying a subset of subscribers served by the HSS, if the occurred failure is limited to those subscribers.

5.2.5 Notification Procedures

5.2.5.1 Notification

5.2.5.1.1 General

The Notification Procedure shall be used between the MME and the HSS and between the SGSN and the HSS when an inter MME or SGSN location update does not occur but the HSS needs to be notified about

- an update of terminal information;

The Notification Procedure shall also be used between the MME and the HSS and between the SGSN and the HSS to notify the HSS about:

- an assignment/change/removal of PDN GW for an APN;

The Notification Procedure shall be used between the MME and the HSS when an inter MME location update does not occur but the HSS needs to be notified about

- the need to send a Cancel Location to the current SGSN (which does not support ISR).

This procedure is mapped to the commands Notify-Request/Answer (NOR/NOA) in the Diameter application specified in chapter 7.

Table 5.2.5.1.1/1 specifies the involved information elements for the request.

Table 5.2.5.1.1/2 specifies the involved information elements for the answer.

Table 5.2.5.1.1/1: Notify Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Name (See IETF RFC 3588 [4])	User-Name	M	This information element shall contain the permanent identity of the user, i.e. the IMSI. See 3GPP TS 23.003 [3].
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Terminal Information (See 7.3.3)	Terminal-Information	C	This information element shall contain information about the user"s mobile equipment. When notifying the HSS about any change of Terminal Information, the MME or SGSN shall include the new Terminal Information in the request. Within this Information Element, only the IMEI and the Software-Version AVPs shall be used on the S6a/S6d interface.
PDN GW Identity (See 7.3.45)	PDN-GW-Identity	C	This IE shall contain the address of the selected PDN GW for an APN. It shall be present if a new PDN-GW has been selected and the subscriber is allowed handover to non 3GPP access. When notifying the HSS about a newly selected PDN GW, the MME or SGSN shall include the PDN-GW-Identity in the request. When notifying the HSS about removal of PDN GW for an APN, then this AVP shall not be included.
APN (See IETF Draft draft-ietf-dime-mip6-split-12 [20])	Service-Selection	C	This IE shall contain the APN for the selected PDN GW. It shall be present if the selected PDN-GW is present and is particular for one specific APN and not common to all the APNs. It shall be present when notifying the HSS about removal of the PDN GW associated with the indicated APN.
NOR Flags (See 7.3.49)	NOR-Flags	C	This Information Element shall contain a bit mask. See 7.3.49 for the meaning of the bits. Absence of this information element shall be interpreted as all bits set to 0. When notifying the HSS about the need to send cancel location to the current SGSN, the MME shall set the "Single-Registration-Indication" flag in the NOR-Flags. When notifying the HSS about the "restricted" status of the current SGSN area, the SGSN shall set the "SGSN area restricted" flag in the NOR-Flags.

Table 5.2.5.1.1/2: Notify Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.4)	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6a/S6d errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. The following errors are applicable in this case: - User Unknown
Supported Features (See 3GPP TS 29.229 [9])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

5.2.5.1.2 Detailed behaviour of the MME and the SGSN

The MME or SGSN shall include conditional AVPs in NOR according to the description given in table 5.2.5.1.1/1.

When receiving a Notify response from the HSS, no special action in the MME or SGSN is needed.

5.2.5.1.3 Detailed behaviour of the HSS

When receiving a Notify request the HSS shall check whether the IMSI is known.

If it is not known, a result code of DIAMETER_ERROR_USER_UNKNOWN is returned.

If it is known, the HSS shall set the result code to DIAMETER_SUCCESS and

- store the new terminal information if present in the request;
- store the new PDN GW for an APN if present in the request;
- delete the stored PDN GW for an APN, if the APN IE is present in the request and the PDN GW Identity IE is not present in the request;
- mark the location area as "restricted" if so indicated in the request;
- send Cancel Location to the current SGSN if so indicated in the request;

and then send the response to the MME or SGSN.

6 MME – EIR (S13) and SGSN – EIR (S13')

6.1 Introduction

The S13 interface shall enable the ME Identity check procedure between the MME and the EIR as described in the 3GPP TS 23.401 [2].

The S13' interface shall enable the ME Identity check procedure between the SGSN and the EIR as described in the 3GPP TS 23.060 [12].

6.2 ME Identity Check Procedures

6.2.1 ME Identity Check

6.2.1.1 General

This Mobile Equipment Identity Check Procedure shall be used between the MME and the EIR and between the SGSN and the EIR to check the Mobile Equipment's identity status (e.g. to check that it has not been stolen, or, to verify that it does not have faults).

This procedure is mapped to the commands ME-Identity-Check-Request/Answer (ECR/ECA) in the Diameter application specified in chapter 6.

Table 6.2.1.1/1 specifies the involved information elements for the request.

Table 6.2.1.1/2 specifies the involved information elements for the answer.

Table 6.2.1.1/1: ME Identity Check Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Terminal Information (See 7.3.3)	Terminal-Information	M	This information element shall contain the information about the used mobile equipment i.e. the IMEI.
User Name (See IETF RFC 3588 [4])	User-Name	O	This information element shall contain the permanent identity of the user, i.e. the IMSI. See 3GPP TS 23.003 [3].

Table 6.2.1.1/2: ME Identity Check Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.4)	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S13/S13' errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. The following errors are applicable in this case: - Unknown equipment
Equipment Status (See 7.3.51)	Equipment-Status	C	This information element shall contain the status of the requested mobile equipment as defined in 3GPP TS 22.016 [13]. It shall be present if the result of the ME Identity Check is DIAMETER_SUCCESS.

6.2.1.2 Detailed behaviour of the MME and the SGSN

The MME or the SGSN shall make use of this procedure to check the ME identity, if the MME or the SGSN is configured to check the IMEI with the EIR.

When receiving the ME Identity Check answer from the EIR, the MME or the SGSN shall check the result code and the equipment status. Dependent upon the result, the MME or the SGSN will decide its subsequent actions (e.g. sending an Attach Reject if the EIR indicates that the Mobile Equipment is unknown or blacklisted).

6.2.1.3 Detailed behaviour of the EIR

When receiving an ME Identity Check request, the EIR shall check whether the mobile equipment is known.

If it is not known, a result code of DIAMETER_ERROR_ EQUIPMENT_UNKNOWN is returned.

If it is known, the EIR shall return DIAMETER_SUCCESS with the equipment status.

IMSI may be sent together with Terminal Information to the EIR for operator-determined purposes.

7 Protocol Specification and Implementation

7.1 Introduction

7.1.1 Use of Diameter base protocol

The Diameter Base Protocol as specified in IETF RFC 3588 [4] 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.

7.1.2 Securing Diameter Messages

For secure transport of Diameter messages, see 3GPP TS 33.210 [16]

7.1.3 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) shall not be used on the S6a, S6d, S13 and S13' interfaces.

7.1.4 Use of sessions

Between the MME and the HSS and between the SGSN and the HSS and between the MME and the EIR, Diameter sessions shall be implicitly terminated. 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 [4]. 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.

7.1.5 Transport protocol

Diameter messages over the S6a, S6d, S13 and S13' interfaces shall make use of SCTP IETF RFC 2960 [14] and shall utilise the SCTP checksum method specified in RFC 3309 [15].

7.1.6 Routing considerations

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

If an MME or SGSN knows the address/name of the HSS for a certain user, both the Destination-Realm and Destination-Host AVPs 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 an MME or SGSN.

The address/name of the EIR shall be locally configured in the MME.

Requests initiated by the HSS towards an MME or SGSN shall include both Destination-Host and Destination-Realm AVPs. The HSS obtains the Destination-Host AVP to use in requests towards an MME or SGSN, from the Origin-Host AVP received in previous requests from the MME or SGSN. Consequently, the Destination-Host AVP is declared as mandatory in the ABNF for all requests initiated by the HSS.

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

7.1.7 Advertising Application Support

The HSS, MME, SGSN and EIR shall advertise support of the Diameter S6a/S6d and/or S13/S13' 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.

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 RFC 3588 [4].

7.1.8 Diameter Application Identifier

This clause specifies two Diameter applications: one is for the S6a/S6d interface application, and the other is for the S13/S13' interface application.

The S6a/S6d interface application allows a Diameter server and a Diameter client:

- to exchange location information;
- to authorize a user to access the EPS;
- to exchange authentication information;
- to download and handle changes in the subscriber data stored in the server.

The S6a/S6d 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 S6a/S6d interface application is 16777251 (allocated by IANA).

The S13/S13' interface application allows a Diameter server and a Diameter client:

- to check the validity of the ME Identity.

The S13/S13' 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 S13/S13' interface application is 16777252 (allocated by IANA).

7.2 Commands

7.2.1 Introduction

This section defines the Command code values and related ABNF for each command described in this specification.

7.2.2 Command-Code values

This section defines Command-Code values for the S6a/S6d interface application and S13/S13' interface application.

Every command is defined by means of the ABNF syntax IETF RFC 2234 [7], according to the rules in IETF RFC 3588 [4]. In the case, the definition and use of an AVP is not specified in this document, the guidelines in IETF RFC 3588 [4] shall apply.

The following Command Codes are defined in this specification:

Table 7.2.2/1: Command-Code values for S6a/S6d

Command-Name	Abbreviation	Code	Section
Update-Location-Request	ULR	tbd	7.2.3
Update-Location-Answer	ULA	tbd	7.2.4
Authentication-Information-Request	AIR	tbd	7.2.5
Authentication-Information-Answer	AIA	tbd	7.2.6
Cancel-Location-Request	CLR	tbd	7.2.7
Cancel-Location-Answer	CLA	tbd	7.2.8
Insert-Subscriber-Data-Request	IDR	tbd	7.2.9
Insert-Subscriber-Data-Answer	IDA	tbd	7.2.10
Delete-Subscriber-Data-Request	DSR	tbd	7.2.11
Delete-Subscriber-Data-Answer	DSA	tbd	7.2.12
Purge-UE-Request	PUR	tbd	7.2.13
Purge-UE-Answer	PUA	tbd	7.2.14
Reset-Request	RSR	tbd	7.2.15
Reset-Answer	RSA	tbd	7.2.16
Notify-Request	NOR	tbd	7.2.17
Notify-Answer	NOA	tbd	7.2.18

Editor"s note: the command codes for the S6a/S6d interface application are to be assigned by IANA.

For these commands, the Application-ID field shall be set to 16777251 (application identifier of the S6a/S6d interface application, allocated by IANA).

Table 7.2.2/2: Command-Code values for S13/S13'

Command-Name	Abbreviation	Code	Section
ME-Identity-Check-Request	ECR	tbd	7.2.19
ME-Identity-Check-Answer	ECA	tbd	7.2.20

Editor"s note: the command codes for the S13/S13' interface application are to be assigned by IANA.

For these commands, the Application-ID field shall be set to 16777252 (application identifier of the S13/S13' interface application, allocated by IANA).

7.2.3 Update-Location-Request (ULR) Command

The Update-Location-Request (ULR) command, indicated by the Command-Code field set to tbd and the 'R' bit set in the Command Flags field, is sent from MME or SGSN to HSS.

Message Format

```
< Update-Location-Request> ::=    < Diameter Header: tbd, REQ, PXY, tbd >
                                  < Session-Id >
                                  { Auth-Session-State }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  [ Destination-Host ]
                                  { Destination-Realm }
                                  { User-Name }
                                  *[ Supported-Features ]
                                  [ Terminal-Information ]
                                  { RAT-Type }
                                  { ULR-Flags }
                                  { Visited-PLMN-Id }
                                  *[ AVP ]
                                  *[ Proxy-Info ]
                                  *[ Route-Record ]
```

7.2.4 Update-Location-Answer (ULA) Command

The Update-Location-Answer (ULA) command, indicated by the Command-Code field set to tbd and the 'R' bit cleared in the Command Flags field, is sent from HSS to MME or SGSN.

Message Format

```
< Update-Location-Answer> ::=     < Diameter Header: tbd, PXY, tbd >
                                  < Session-Id >
                                  [ Result-Code ]
                                  [ Experimental-Result ]
                                  { Auth-Session-State }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  *[ Supported-Features ]
                                  [  ULA-Flags ]
                                  [ Subscription-Data ]
                                  *[ AVP ]
                                  *[ Failed-AVP ]
                                  *[ Proxy-Info ]
                                  *[ Route-Record ]
```

7.2.5 Authentication-Information-Request (AIR) Command

The Authentication-Information-Request (AIR) command, indicated by the Command-Code field set to tbd and the 'R' bit set in the Command Flags field, is sent from MME or SGSN to HSS.

Message Format

```
< Authentication-Information-Request> ::=    < Diameter Header: tbd, REQ, PXY, tbd >
                                             < Session-Id >
                                             { Auth-Session-State }
                                             { Origin-Host }
                                             { Origin-Realm }
                                             [ Destination-Host ]
                                             { Destination-Realm }
                                             { User-Name }
                                             *[Supported-Features]
                                             [ Requested-EUTRAN-Authentication-Info ]
                                             [ Requested-UTRAN-GERAN-Authentication-Info ]
                                             { Visited-PLMN-Id }
                                             { Requesting-Node-Type }
                                             *[ AVP ]
                                             *[ Proxy-Info ]
                                             *[ Route-Record ]
```

7.2.6 Authentication-Information-Answer (AIA) Command

The Authentication-Information-Answer (AIA) command, indicated by the Command-Code field set to tbd and the 'R' bit cleared in the Command Flags field, is sent from HSS to MME or SGSN.

Message Format

```
< Authentication-Information-Answer> ::=     < Diameter Header: tbd, PXY, tbd >
                                             < Session-Id >
                                             [ Result-Code ]
                                             [ Experimental-Result ]
                                             { Auth-Session-State }
                                             { Origin-Host }
                                             { Origin-Realm }
                                             * [Supported-Features]
                                             [ Authentication-Info ]
                                             *[ AVP ]
```

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

7.2.7 Cancel-Location-Request (CLR) Command

The Cancel-Location-Request (CLR) command, indicated by the Command-Code field set to tbd and the 'R' bit set in the Command Flags field, is sent from HSS to MME or SGSN.

Message Format

< Cancel-Location-Request> ::= < Diameter Header: tbd, REQ, PXY, tbd >
< Session-Id >
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
*[Supported-Features]
{ Cancellation-Type }
*[AVP]
*[Proxy-Info]
*[Route-Record]

7.2.8 Cancel-Location-Answer (CLA) Command

The Cancel-Location-Answer (CLA) command, indicated by the Command-Code field set to tbd and the 'R' bit cleared in the Command Flags field, is sent from MME or SGSN to HSS.

Message Format

< Cancel-Location-Answer> ::= < Diameter Header: tbd, PXY, tbd >
< Session-Id >
*[Supported-Features]
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

7.2.9 Insert-Subscriber-Data-Request (IDR) Command

The Insert-Subscriber-Data-Request (IDR) command, indicated by the Command-Code field set to tbd and the 'R' bit set in the Command Flags field, is sent from HSS to MME or SGSN.

Message Format

< Insert-Subscriber-Data-Request> ::= < Diameter Header: tbd, REQ, PXY, tbd >
< Session-Id >
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User Name }
*[Supported-Features]
{ Subscription Data}

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

7.2.10 Insert-Subscriber-Data-Answer (IDA) Command

The Insert-Subscriber-Data-Answer (IDA) command, indicated by the Command-Code field set to tbd and the 'R' bit cleared in the Command Flags field, is sent from MME or SGSN to HSS.

Message Format

< Insert-Subscriber-Data-Answer> ::= < Diameter Header: tbd, PXY, tbd >
< Session-Id >
*[Supported-Features]
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[IDA-Flags]
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

7.2.11 Delete-Subscriber-Data-Request (DSR) Command

The Delete-SubscriberData-Request (DSR) command, indicated by the Command-Code field set to tbd and the 'R' bit set in the Command Flags field, is sent from HSS to MME or SGSN.

Message Format

< Delete-Subscriber-Data-Request > ::= < Diameter Header: tbd, REQ, PXY, tbd >
< Session-Id >
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
*[Supported-Features]
{ DSR-Flags }
*[Context-Identifier]
*[AVP]
*[Proxy-Info]
*[Route-Record]

7.2.12 Delete-Subscriber-Data-Answer (DSA) Command

The Delete-SubscriberData-Answer (DSA) command, indicated by the Command-Code field set to tbd and the 'R' bit cleared in the Command Flags field, is sent from MME or SGSN to HSS.

Message Format

< Delete-Subscriber-Data-Answer> ::= < Diameter Header: tbd, PXY, tbd >
< Session-Id >
*[Supported-Features]
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[DSA-Flags]
*[AVP]

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

7.2.13 Purge-UE-Request (PUR) Command

The Purge-UE-Request (PUR) command, indicated by the Command-Code field set to tbd and the 'R' bit set in the Command Flags field, is sent from MME or SGSN to HSS.

Message Format

< Purge-UE-Request> ::= < Diameter Header: tbd, REQ, PXY, tbd >
< Session-Id >
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
{ User-Name }
*[Supported-Features]
*[AVP]
*[Proxy-Info]
*[Route-Record]

7.2.14 Purge-UE-Answer (PUA) Command

The Purge-UE-Answer (PUA) command, indicated by the Command-Code field set to tbd and the 'R' bit cleared in the Command Flags field, is sent from HSS to MME or SGSN.

Message Format

< Purge-UE-Answer> ::= < Diameter Header: tbd, PXY, tbd >
< Session-Id >
*[Supported-Features]
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[PUA-Flags]
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

7.2.15 Reset-Request (RSR) Command

The Reset-Request (RSR) command, indicated by the Command-Code field set to tbd and the 'R' bit set in the Command Flags field, is sent from HSS to MME or SGSN.

Message Format

< Reset-Request> ::= < Diameter Header: tbd, REQ, PXY, tbd >
< Session-Id >
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
[Supported-Features]
*[User-Id]
*[AVP]

*[Proxy-Info]
*[Route-Record]

7.2.16 Reset-Answer (RSA) Command

The Authentication-Information-Answer (RSA) command, indicated by the Command-Code field set to tbd and the 'R' bit cleared in the Command Flags field, is sent from MME or SGSN to HSS.

Message Format

< Reset-Answer> ::= < Diameter Header: tbd, PXY, tbd >
< Session-Id >
[Supported-Features]
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

7.2.17 Notify-Request (NOR) Command

The Notify-Request (NOR) command, indicated by the Command-Code field set to tbd and the 'R' bit set in the Command Flags field, is sent from MME or SGSN to HSS.

Message Format

< Notify-Request> ::= < Diameter Header: tbd, REQ, PXY, tbd >
< Session-Id >
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
{ User-Name }
* [Supported-Features]
[Terminal-Information]
[PDN-GW-Identity]
[Service-Selection]
[NOR-Flags]
*[AVP]
*[Proxy-Info]
*[Route-Record]

7.2.18 Notify-Answer (NOA) Command

The Notify-Answer (NOA) command, indicated by the Command-Code field set to tbd and the 'R' bit cleared in the Command Flags field, is sent from HSS to MME or SGSN.

Message Format

< Notify-Answer> ::= < Diameter Header: tbd, PXY, tbd >
< Session-Id >
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[Supported-Features]
*[AVP]

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

7.2.19 ME-Identity-Check-Request (ECR) Command

The ME-Identity-Check-Request (ECR) command, indicated by the Command-Code field set to tbd and the 'R' bit set in the Command Flags field, is sent from MME or SGSN to EIR.

Message Format

< ME-Identity-Check-Request > ::= < Diameter Header: tbd, REQ, PXY, tbd >
< Session-Id >
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
{ Terminal-Information }
[User-Name]
*[AVP]
*[Proxy-Info]
*[Route-Record]

7.2.20 ME-Identity-Check-Answer (ECA) Command

The ME-Identity-Check-Answer (ECA) command, indicated by the Command-Code field set to tbd and the 'R' bit cleared in the Command Flags field, is sent from EIR to MME or SGSN.

Message Format

< ME-Identity-Check-Answer> ::= < Diameter Header: tbd, PXY, tbd >
< Session-Id >
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Equipment-Status]
*[AVP]
*[Failed-AVP]
*[Proxy-Info]
*[Route-Record]

7.3 Information Elements

7.3.1 General

The following table specifies the Diameter AVPs defined for the S6a/S6d interface protocol and S13/S13' 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 7.3.1/1: S6a/S6d and S13/S13' specific Diameter AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
Subscription-Data	1400	7.3.2	Grouped	M, V				
Terminal-Information	1401	7.3.3	Grouped	M, V				No
IMEI	1402	7.3.4	UTF8String	M, V				No
Software-Version	1403	7.3.5	UTF8String	M, V				No
ULR-Flags	1405	7.3.7	Unsigned32	M, V				No
ULA-Flags	1406	7.3.8	Unsigned32	M, V				No
Visited PLMN Id	1407	7.3.9	OctetString	M, V				No
Requested-EUTRAN-Authentication-Info	1408	7.3.11	Grouped	M, V				No
Requested-UTRAN- GERAN-Authentication-Info	1409	7.3.12	Grouped	M, V				No
Number-Of-Requested-Vectors	1410	7.3.14	Unsigned32	M, V				No
Re-Synchronization-Info	1411	7.3.15	OctetString	M, V				No
Immediate-Response-Preferred	1412	7.3.16	Unsigned32	M, V				No
Authentication-Info	1413	7.3.17	Grouped	M, V				No
E-UTRAN-Vector	1414	7.3.18	Grouped	M, V				No
UMTS-Vector	1415	7.3.19	Grouped	M, V				No
GERAN-Vector	1416	7.3.20	Grouped	M, V				No
Network-Access-Mode	1417	7.3.21	Enumerated	M, V				No
HPLMN-ODB	1418	7.3.22	Enumerated	M, V				No
Item-Number	1419	7.3.23	Unsigned32	M, V				No
Cancellation-Type	1420	7.3.24	Enumerated	M, V				No
DSR-Flags	1421	7.3.25	Unsigned32	M, V				No
DSA-Flags	1422	7.3.26	Unsigned32	M, V				No
Context-Identifier	1423	7.3.27	Unsigned32	M, V				No
Subscriber-Status	1424	7.3.29	Enumerated	M, V				No
Operator-Determined-Barring	1425	7.3.30	Unsigned32	M, V				No
Access-Restriction-Data	1426	7.3.31	Unsigned32	M, V				No
APN-OI-Replacement	1427	7.3.32	UTF8String	M, V				No
All-APN-Configurations-Included-Indicator	1428	7.3.33	Enumerated	M, V				No
APN-Configuration-Profile	1429	7.3.34	Grouped	M, V				No
APN-Configuration	1430	7.3.35	Grouped	M, V				No
EPS-Subscribed-QoS-Profile	1431	7.3.37	Grouped	M, V				No
VPLMN-Dynamic-Address-Allowed	1432	7.3.38	Enumerated	M, V				No
STN-SR	1433	7.3.39	OctetString	M, V				No
ARP	1434	7.3.40	Unsigned32	M, V				No
AMBR	1435	7.3.41	Grouped	M, V				No
PDN-GW-Allocation-Type	1438	7.3.44	Enumerated	M, V				No
RAT-Frequency-Selection-Priority-ID	1440	7.3.46	Unsigned32	M, V				No
IDA-Flags	1441	7.3.47	Unsigned32	M, V				No
PUA-Flags	1442	7.3.48	Unsigned32	M, V				No
NOR-Flags	1443	7.3.49	Unsigned32	M, V				No
User-Id	1444	7.3.50	OctetString	V			M	No
Equipment-Status	1445	7.3.51	Enumerated	M, V				No
Regional-Subscription-Zone-Code	1446	7.3.52	OctetString	M, V				No
RAND	1447	7.3.53	OctetString	M, V				No
XRES	1448	7.3.54	OctetString	M, V				No
AUTN	1449	7.3.55	OctetString	M, V				No
KASME	1450	7.3.56	OctetString	M, V				No
CK	1451	7.3.57	OctetString	M, V				No
IK	1452	7.3.58	OctetString	M, V				No
Kc	1453	7.3.59	OctetString	M, V				No
SRES	1454	7.3.60	OctetString	M, V				No
Requesting-Node-Type	1455	7.3.61	Enumerated	M, V				No
PDN-Type	1456	7.3.62	Enumerated	M, V				No
Trace-Data	tbd	7.3.63	Grouped	M, V				No
Trace-Reference	tbd	7.3.64	OctetString	M, V				No
Trace-Depth-List	tbd	7.3.65	Grouped	M, V				No
Network-Element-Type	tbd	7.3.66	Enumerated	M, V				No

Trace-Depth	tbd	7.3.67	Enumerated	M, V				No
Trace-NE-Type-List	tbd	7.3.68	OctetString	M, V				No
Trace-Interface-List	tbd	7.3.69	OctetString	M, V				No
Trace-Event-List	tbd	7.3.70	OctetString	M, V				No
OMC-Id	tbd	7.3.71	OctetString	M, V				No
GPRS-Subscription-Data	tbd	7.3.72	Grouped	M, V				No
Complete-Data-List-Included-Indicator	tbd	7.3.73	Enumerated	M, V				No
PDP-Context	tbd	7.3.74	Grouped	M, V				No
PDP-Type	tbd	7.3.75	OctetString	M, V				No
PDP-Address	tbd	7.3.76	OctetString	M, V				No
QoS-Subscribed	tbd	7.3.77	OctetString	M, V				No
CSG-Subscription-Data	tbd	7.3.78	Grouped	M. V				No
CSG-Id	tbd	7.3.79	Unsigned32	M, V				No
Expiration-Data	tbd	7.3.80	time	M, V				No
Roaming-Restricted-Due-To-Unsupported-Feature	tbd	7.3.81	Enumerated	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 [4].								

The following table specifies the Diameter AVPs re-used by the S6a/S6d interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within S6a and S6d.

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 7.3.1/2, but they may be re-used for the S6a/S6d protocol and the S13/S13' protocol.

Table 7.3.1/2: S6a/S6d and S13/S13' re-used Diameter AVPs

Attribute Name	Reference	Comments
Service-Selection	IETF Darft draft-ietf-dime-mip6-split-12 [20]	See section 7.3.36
3GPP-Charging-Characteristics	3GPP TS 32.299 [8]	See 3GPP TS 29.061 [21], 3GPP TS 23.060 [12] Table 5 and 3GPP TS 32.298 [22] section 5.1.2.2.7
Supported-Features	3GPP TS 29.229 [9]	
Feature-List-ID	3GPP TS 29.229 [9]	
Feature-List	3GPP TS 29.229 [9]	See section 7.3.10
Served-Party-IP-Address	3GPP TS 32.299 [8]	holds the PDN IP Address of the user
QoS-Class-Identifier	3GPP TS 29.212 [10]	
Max-Requested-Bandwidth-DL	3GPP TS 29.214 [11]	
Max-Requested-Bandwidth-UL	3GPP TS 29.214 [11]	
RAT-Type	3GPP TS 29.212 [10]	See section 7.3.13
MSISDN	3GPP TS 29.329 [25]	
MIP6-Agent-Info	IETF Draft draft-ietf-dime-mip6-integrated [26]	
MIP-Home-Agent-Address	IETF RFC 4004 [27]	
MIP-Home-Agent-Host	IETF RFC 4004 [27]	

7.3.2 Subscription-Data

The Subscription-Data AVP is of type Grouped. It shall contain the information related to the user profile relevant for EPS and GERAN/UTRAN.

AVP format:

Subscription-Data ::= <AVP header: XXX XXXX>

[Subscriber-Status]

[MSISDN]

[STN-SR]

[Network-Access-Mode]

[Operator-Determined-Barring]

[HPLMN-ODB]

*[Regional-Subscription-Zone-Code]

[Access-Restriction-Data]

[APN-OI-Replacement]

[3GPP-Charging-Characteristics]

[AMBR]

[APN-Configuration-Profile]

[RAT-Frequency-Selection-Priority-ID]

[Trace-Data]

[GPRS-Subscription Data]

*[CSG-Subscription-Data]

[Roaming-Restricted-Due-To-Unsupported-Feature]

*[AVP]

The AMBR included in this grouped AVP shall include the AMBR associated to the user"s subscription (UE-AMBR).

7.3.3 Terminal-Information

The Terminal-Information AVP is of type Grouped. This AVP shall contain the information about the user"s terminal.

AVP format

Terminal Information ::= <AVP header: XXX XXXX>

[IMEI]

[3GPP2-MEID]

[Software-Version]

*[AVP]

7.3.4 IMEI

The IMEI AVP is of type UTF8String. This AVP shall contain the International Mobile Equipment Identity. See 3GPP TS 23.003 [3]

7.3.5 Software-Version

The Software-Version AVP is of type UTF8String. This AVP contains the Software Version of the International Mobile Equipment Identity. See 3GPP TS 23.003 [3]

7.3.6 3GPP2-MEID

This AVP is of type OctetString. This AVP contains the Mobile Equipment Identifier of the user's terminal. For further details on the encoding of this AVP, refer to 3GPP2 A.S0022 [28].

7.3.7 ULR-Flags

The ULR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 7.3.7/1:

Table 7.3.7/1: ULR-Flags

Bit	Name	Description
0	Single-Registration-Indication	This bit, when set, indicates that the HSS shall send Cancel Location to the SGSN. An SGSN shall not set this bit when sending ULR.
1	S6a/S6d-Indicator	This bit, when set, indicates that the ULR message is sent on the S6a interface, i.e. the source node is an MME (or a combined MME/SGSN to which the UE is attached via E-UTRAN). This bit, when cleared, indicates that the ULR message is sent on the S6d interface, i.e. the source node is an SGSN (or a combined MME/SGSN to which the UE is attached via UTRAN or GERAN).
2	Skip Subscriber Data	This bit, when set, indicates that the HSS may skip subscription data in ULA.
Bits not defined in this table shall be cleared by the sending MME or SGSN and discarded by the receiving HSS.		

7.3.8 ULA-Flags

The ULA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 7.3.8/1:

Table 7.3.8/1: ULA-Flags

Bit	Name	Description
0	Separation Indication	This bit, when set, indicates that the HSS stores SGSN number and MME number in separate memory. A Rel-8 HSS shall set the bit. An IWF interworking with a pre Rel-8 HSS/HLR shall clear the bit.
Bits not defined in this table shall be cleared by the sending HSS and discarded by the receiving MME or SGSN.		

7.3.9 Visited-PLMN-Id

The Visited-PLMN-Id AVP is of type OctetString. This AVP shall contain the concatenation of MCC and MNC. See 3GPP TS 23.003 [3]. The content of this AVP shall be encoded as an octet string according to table 7.3.9-1. Bits 1111 shall be used as filler when MCC or MNC have less than 3 digits.

Table 7.3.9/1: Encoding format for Visited-PLMN-Id AVP

8	7	6	5	4	3	2	1	
MCC digit 2				MCC digit 1				octet 1
MNC digit 3				MCC digit 3				octet 2
MNC digit 2				MNC digit 1				octet 3

7.3.10 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [9]. For the S6a/S6d application, the meaning of the bits shall be as defined in table 7.3.10/1.

Table 7.3.10/1: Features of Feature-List-ID 1 used in S6a/S6d

Feature bit	Feature	M/O	Description
0	ODB-all	O	Operator Determined Barring of all Packet Oriented Services This feature is applicable for the ULR and IDA commands. If the MME or SGSN does not support this feature, the HSS shall not send this ODB barring category to the MME or SGSN within ULA. Instead the HSS may reject location update. If the MME or SGSN does not indicate support of this feature in IDA and the HSS has sent this ODB category within IDR, the HSS may apply barring of roaming and send CLR.
1	ODB-HPLMN-APN	O	Operator Determined Barring of Packet Oriented Services from access points that are within the HPLMN whilst the subscriber is roaming in a VPLMN This feature is applicable for the ULR and IDA commands. If the MME or SGSN does not support this feature, the HSS shall not send this ODB barring category to the MME or SGSN within ULA. Instead the HSS may reject location update. If the MME or SGSN does not indicate support of this feature in IDA and the HSS has sent this ODB category within IDR, the HSS may apply barring of roaming and send CLR.
2	ODB-VPLMN-APN	O	Operator Determined Barring of Packet Oriented Services from access points that are within the roamed to VPLMN This feature is applicable for the ULR and IDA commands. If the MME or SGSN does not support this feature, the HSS shall not send this ODB barring category to the MME or SGSN within ULA. Instead the HSS may reject location update. If the MME or SGSN does not indicate support of this feature in IDA and the HSS has sent this ODB category within IDR, the HSS may apply barring of roaming and send CLR.
3	RegSub	O	Regional Subscription This feature is applicable for the ULR, IDA and DSA commands. If the MME or SGSN does not support this feature, the HSS shall not send Regional Subscription Zone Codes to the MME or SGSN within ULA. Instead the HSS may reject location update. If the MME or SGSN does not indicate support of this feature in IDA and the HSS has sent Regional Subscription Zone Codes within IDR, the HSS may apply barring of roaming and send CLR.
4	Trace	O	Trace Function This feature is applicable for the ULR, IDA and DSA commands. If the MME or SGSN does not indicate support of this feature in ULR, the HSS shall not send Trace Data to the MME or SGSN within ULA. If the MME or SGSN does not indicate support of this feature in IDA, and the HSS has sent Trace Data within IDR, the HSS may store this indication, and not send any further Trace Data to that MME or SGSN. If the MME or SGSN does not indicate support of this feature in DSA, and the HSS has sent Trace Data within DSR, the HSS may store this indication, and not send any further Trace Data to that MME or SGSN
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. "ODB-HPLMN-APN". M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O"). Description: A clear textual description of the feature.			

7.3.11 Requested-EUTRAN-Authentication-Info

The Requested-EUTRAN-Authentication-Info is of type Grouped. It shall contain the information related to the authentication requests for E-UTRAN.

AVP format

Requested- EUTRAN-Authentication-Info ::= <AVP header: XXX XXXX>

[Number-Of-Requested-Vectors]

[Immediate-Response-Preferred]

[Re-synchronization-Info]

*[AVP]

7.3.12 Requested-UTRAN- GERAN-Authentication-Info

The Requested-UTRAN-GERAN-Authentication-Info is of type Grouped. It shall contain the information related to the to authentication requests for UTRAN or GERAN.

AVP format

Requested-UTRAN-GERAN-Authentication-Info ::= <AVP header: XXX XXXX>

[Number-Of-Requested-Vectors]

[Immediate-Response-Preferred]

[Re-synchronization-Info]

*[AVP]

7.3.13 RAT-Type

The RAT-Type AVP is of type Enumerated and is used to identify the radio access technology that is serving the UE. See 3GPP TS 29.212 [10] for the defined values.

7.3.14 Number-Of-Requested-Vectors

The Number-Of-Requested-Vectors AVP is of type Unsigned32. This AVP shall contain the number of AVs the MME or SGSN is prepared to receive.

7.3.15 Re-Synchronization-Info

The Re-Synchronization-Info AVP is of type OctetString. It shall contain the concatenation of RAND and AUTS.

7.3.16 Immediate-Response-Preferred

The Immediate-Response-Preferred AVP is of type Unsigned32. When EUTRAN-AVs and UTRAN-AVs or GERAN AVs are requested, this parameter shall indicate which type of AV is requested for immediate use in the MME/SGSN. It may be used by the HSS to determine the number of vectors to be obtained from the AuC and the number of vectors downloaded to the MME or SGSN.

7.3.17 Authentication-Info

The Authentication-Info AVP is of type Grouped. This AVP contains Authentication Vectors.

AVP format:

Authentication-Info ::= <AVP header: tbd 10415>

*[E-UTRAN-Vector]

*[UTRAN-Vector]

*[GERAN-Vector]

*[AVP]

7.3.18 E-UTRAN-Vector

The E-UTRAN-Vector AVP is of type Grouped. This AVP shall contain an E-UTRAN Vector.

AVP format:

E-UTRAN-Vector ::= <AVP header: tbd 10415>

[Item-Number]

{ RAND }

{ XRES }

{ AUTN }

{ KASME }

*[AVP]

7.3.19 UTRAN-Vector

The UMTS-Vector AVP is of type Grouped. This AVP shall contain an UTRAN Vector.

AVP format:

UTRAN-Vector ::= <AVP header: tbd 10415>

[Item-Number]

{ RAND }

{ XRES }

{ AUTN }

{ Confidentiality-Key }

{ Integrity-Key }

*[AVP]

7.3.20 GERAN-Vector

The GERAN-Vector AVP is of type Grouped. This AVP shall contain a GERAN Vector.

AVP format:

GERAN-Vector ::= <AVP header: tbd 10415>

[Item-Number]

{ RAND }

{ SRES }

{ Kc }

*[AVP]

7.3.21 Network-Access-Mode

The Network-Access-Mode AVP is of type Enumerated. The following values are defined:

PACKET_AND_CIRCUIT (0)

ONLY_CIRCUIT (1)

ONLY_PACKET (2)

7.3.22 HPLMN-ODB

The HPLMN-ODB AVP is of type Unsigned32 and it shall contain a bit mask indicating the HPLMN specific services of a subscriber that are barred by the operator. The meaning of the bits is HPLMN specific:

Table 7.3.22/1: HPLMN-ODB

Bit	Description
0	HPLMN specific barring type 1
1	HPLMN specific barring type 2
2	HPLMN specific barring type 3
3	HPLMN specific barring type 4

If this AVP is present within the Subscription-Data AVP, then the Subscriber-Status AVP shall also be present and set to OPERATORDETERMINEDBARRING.

Upon receiving this AVP, the MME or SGSN shall replace stored HPLMN-ODB data (if any) with the received information rather than add the received information to the stored information. Unsupported Barring categories need not be stored.

7.3.23 Item-Number

The Item-Number AVP is of type Unsigned32. If more than one EPS or UTRAN or GERAN Vector is included within one Authentication-Info AVP, the Item-Number AVP shall be present within each Vector. Vectors with lower Item Number should be used before Vectors with higher Item Number are used in the MME or SGSN. The Item Number is used to order Vectors received within one request. For Vectors received within different requests those received by the earlier request should be used before those received by the later request.

7.3.24 Cancellation-Type

The Cancellation-Type AVP is of type Enumerated and indicates the type of cancellation. The following values are defined:

MME_UPDATE_PROCEDURE (0)

This value is used when the Cancel Location is sent to the previous MME due to a received Update Location message from a new MME.

SGSN_UPDATE_PROCEDURE (1)

This value is used when the Cancel Location is sent to the previous SGSN due to a received Update Location message from a new SGSN.

SUBSCRIPTION_WITHDRAWAL (2)

This value is used when the Cancel Location is sent to the current MME or SGSN due to withdrawal of the user"s subscription by the HSS operator.

UPDATE_PROCEDURE_IWF (3)

This value is used by an IWF when interworking with a pre-Rel-8 HSS.

7.3.25 DSR-Flags

The DSR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits is defined in table 7.3.25/1:

Table 7.3.25/1: DSR-Flags

Bit	Name	Description
0	Regional Subscription Withdrawal	This bit, when set, indicates that Regional Subscription shall be deleted from the subscriber data.
1	Complete APN Configuration Profile Withdrawal	This bit, when set, indicates that all EPS APN configuration data for the subscriber shall be deleted from the subscriber data.
2	Subscribed Charging Characteristics Withdrawal	This bit, when set, indicates that the Subscribed Charging Characteristics shall be replaced with a local default value or deleted in the MME or SGSN.
3	PDN subscription contexts Withdrawal	This bit, when set, indicates that the PDN subscription contexts whose identifier is included in the Context-Identifier AVP shall be deleted. (Note 1)
4	STN-SR	This bit, when set, indicates that the Session Transfer Number for SRVCC shall be deleted from the subscriber data.
5	Complete PDP context list Withdrawal	This bit, when set, indicates that all PDP contexts for the subscriber shall be deleted from the subscriber data.
6	PDP contexts Withdrawal	This bit, when set, indicates that the PDP contexts whose identifier is included in the Context-Identifier AVP shall be deleted. (Note 2)
7	Roaming Restricted in MME or SGSN due to unsupported feature	This bit, when set, indicates that the roaming restriction shall be deleted from the subscriber data.
8	Trace Data Withdrawal	This bit, when set, indicates that the Trace Data shall be deleted from the subscriber data.
9	CSG Deleted	This bit, when set, indicates that the CSG-Subscription-Data shall be deleted from the MME or SGSN.
10	APN-OI-Replacement	This bit, when set, indicates that the APN-OI-Replacement shall be deleted from the subscriber data.
11	Roaming Restricted due to unsupported feature	This bit, when set, indicates that Roaming is no longer restricted.
Note 1: If the Complete APN Configuration Profile Withdrawal bit is set, this bit should not be set. Note 2: If the Complete PDP context list Withdrawal bit is set, this bit should not be set. Note 3: Bits not defined in this table shall be cleared by the sending HSS and discarded by the receiving MME or SGSN. Note 4: Bits 3 and 6 are excluding alternatives and shall not both be set.		

7.3.26 DSA-Flags

The DSA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits is defined in table 7.3.26/1:

Table 7.3.26/1: DSA-Flags

Bit	Name	Description
0	Network Node area restricted	This bit, when set, shall indicate that the complete Network Node area (SGSN area) is restricted due to regional subscription.
Note: Bits not defined in this table shall be cleared by the sending SGSN and discarded by the receiving HSS.		

7.3.27 Context-Identifier

The Context-Identifier AVP is of type Unsigned32.

7.3.28 Void

7.3.29 Subscriber-Status

The 3GPP Subscriber Status AVP is of type Enumerated. It shall indicate if the service is barred or granted. The following values are defined:

SERVICE_GRANTED (0)

OPERATOR_DETERMINED_BARRING (1)

This AVP shall be present in the Subscription-Data AVP when sent within a ULA.

It shall also be present in the Subscription-Data AVP, sent within IDR, if the current value in the MME or SGSN needs to be changed.

If the value "OPERATOR_DETERMINED_BARRING" is sent, the Operator-Determined-Barring AVP shall also be present in the Subscription-Data AVP.

To remove all Operator Determined Barring Categories the Subscriber-Status shall be set to "SERVICE_GRANTED".

7.3.30 Operator-Determined-Barring

The Operator-Determined-Barring AVP is of type Unsigned32 and it shall contain a bit mask indicating the services of a subscriber that are barred by the operator. The meaning of the bits is the following:

Table 7.3.30/1: Operator-Determined-Barring

Bit	Description
0	All Packet Oriented Services Barred
1	Roamer Access HPLMN-AP Barred
2	Roamer Access to VPLMN-AP Barred

If this AVP is present within the Subscription-Data AVP, then the Subscriber-Status AVP shall also be present and set to OPERATORDETERMINEDBARRING.

When receiving this AVP the MME or SGSN shall replace stored ODB subscription information (if any) with the received information rather than add the received information to the stored information. Unsupported Barring categories need not be stored.

7.3.31 Access-Restriction-Data

The Access-Restriction-Data AVP is of type Unsigned32 and it shall contain a bit mask where each bit when set to 1 indicates a restriction.. The meaning of the bits is the following:

Table 7.3.31/1: Access-Restriction-Data

Bit	Description
0	UTRAN Not Allowed
1	GERAN Not Allowed
2	GAN Not Allowed
3	I-HSPA-Evolution Not Allowed
4	E-UTRAN Not Allowed
5	HO-To-Non-3GPP-Access Not Allowed

This AVP shall be present within the Subscription-Data AVP sent within a ULA if at least one of the defined restrictions applies.

This AVP shall be present within the Subscription-Data AVP send within an IDR if the information stored in the MME or SGSN needs to be modified.

When receiving this AVP within the Subscription-Data AVP the MME or SGSN shall replace stored information (if any) with received information rather than add received information to stored information

7.3.32 APN-OI-Replacement

The APN-OI-Replacement AVP is of type UTF8String. This AVP shall indicate the domain name to replace the APN OI when constructing the PDN GW FQDN upon which to perform a DNS resolution. See 3GPP TS 23.003 [3].

This AVP may be present in the Subscription-Data AVP sent within a ULA.

This AVP shall be present in the Subscription-Data AVP sent within an IDR, if the APN-OI-Replacement has been added or modified in the HSS.

When receiving this AVP, the MME or SGSN shall replace the stored information (if any) with the received information.

7.3.33 All-APN-Configurations-Included-Indicator

The All-APN-Configurations-Included-Indicator AVP is of type Enumerated. The following values are defined:

All_APN_CONFIGURATIONS_INCLUDED (0)

MODIFIED/ADDED_APN_CONFIGURATIONS_INCLUDED (1)

7.3.34 APN-Configuration-Profile

The APN-Configuration AVP is of type Grouped. It shall contain the information related to the user's subscribed APN configurations for EPS. It shall also contain a Context-Identifier AVP that identifies the per subscriber"s default APN configuration.

The AVP format shall conform to:

APN-Configuration-Profile ::= <AVP header: XXX XXXX>

{ Context-Identifier }

{ All-APN-Configurations-Included-Indicator }

1*{APN-Configuration}

*[AVP]

This AVP shall be present in the Subscription-Data AVP sent within a ULA.

This AVP shall be present in the Subscription-Data AVP sent within an IDR if at least one APN-Configuration is added or modified by the HSS.

The Subscription-Data AVP associated with an IMSI contains one APN-Configuration-Profile AVP.

Each APN-Configuration-Profile AVP contains one or more APN-Configuration AVPs.

Each APN-Configuration AVP describes the configuration for a single APN.

Therefore, the cardinality of the relationship between IMSI and APN is one-to-many.

When receiving this AVP, the MME or SGSN shall check the ALL-APN-Configurations-Included-Indicator value. If it indicates "All_APN_CONFIGURATIONS_INCLUDED", the MME or SGSN shall delete all stored APN-Configurations and then store all received APN-Configurations. Otherwise, the MME or SGSN shall check the Context-Identifier value of each received APN-Configuration. If the Context-Identifier of a received APN-Configuration matches a Context-Identifier of a stored APN-Configuration, the MME or SGSN shall replace the stored APN-Configuration with the received APN-Configuration. If the Context-Identifier of a received APN-Configuration does not match a Context-Identifier of a stored APN-Configuration, the MME or SGSN shall add the received APN-Configuration to the stored APN-Configurations.

7.3.35 APN-Configuration

The APN-Configuration AVP is of type Grouped. It shall contain the information related to the user"s subscribed APN configurations. The Context-Identifier in the APN-Configuration AVP shall identify that APN configuration. Furthermore, the Context-Identifier in the APN-Configuration AVP shall uniquely identify the EPS APN configuration per subscription.

The AVP format shall conform to:

APN-Configuration::= <AVP header: XXX XXXX>

{ Context-Identifier }

* 2 [Served-Party-IP-Address]

{ PDN-Type }

{ Service-Selection}

[EPS-Subscribed-QoS Profile]

[VPLMN-Dynamic-Address-Allowed]

[MIP6-Agent-Info]

[PDN-GW-Allocation-Type]

[3GPP-Charging-Characteristics]

[AMBR]

*[AVP]

The AMBR included in this grouped AVP shall include the AMBR associated to this specific APN configuration (APN-AMBR).

The Served-Party-IP-Address AVP may be present 0, 1 or 2 times. The AVP shall contain the IPv4 address, IPv6 address and/or the IPv6 prefix of the user, if static IP address allocation is used. For the IPv6 prefix, the lower 64 bits of the address shall be set to zero.

7.3.36 Service-Selection

The Service-Selection AVP is of type of UTF8String. This AVP shall contain an APN, formatted according to 3GPP TS 23.003 [3]. See IETF RFC Draft draft-ietf-dime-mip6-split [20] for the definition of Service-Selection.

7.3.37 EPS-Subscribed-QoS-Profile

The EPS-Subscribed-QoS-Profile AVP is of type Grouped. It shall contain the information related to the user profile relevant for EPS.

AVP format

EPS-Subscribed-QoS-Profile::= <AVP header: XXX XXXX>

{ QoS-Class-Identifier }

{ ARP }

*[AVP]

7.3.38 VPLMN-Dynamic-Address-Allowed

The VPLMN Dynamic Address Allowed AVP is of type Enumerated. It shall indicate whether for this APN, the UE is allowed to use the PDN GW in the domain of the HPLMN only, or additionally, the PDN GW in the domain of the VPLMN.. If this AVP is not present, this means that the UE is not allowed to use PDN GWs in the domain of the VPLMN. The following values are defined:

NOTALLOWED (0)

ALLOWED (1)

7.3.39 STN-SR

The STN-SR AVP is of type OctetString and shall contain the Session Transfer Number for SRVCC. See 3GPP TS 23.003 [3] for the structure of STN-SR.

7.3.40 ARP

The ARP AVP is of type Unsigned32. It shall indicate the Priority of Allocation and Retention for the corresponding APN configuration.

7.3.41 AMBR

The AMBR AVP is of type Grouped.

AVP format

AMBR::= <AVP header: XXX XXXX>

{ Max-Requested-Bandwidth-UL }

{ Max-Requested-Bandwidth-DL }

*[AVP]

7.3.42 MIP-Home-Agent-Address

The MIP-Home-Agent-Address AVP is of type Address and is defined in IETF RFC 4004 [27]. This AVP shall contain either IPv4 or IPv6 address of the PDN-GW and this IP address shall be used as the PDN-GW IP address.

7.3.43 MIP-Home-Agent-Host

The MIP-Home-Agent-Host is of type Grouped and is defined in IETF RFC 4004 [27]. This AVP shall contain a FQDN of the PDN-GW which shall be used to resolve the PDN-GW IP address using the Domain Name Service function.

7.3.44 PDN-GW-Allocation-Type

The PDN-GW-Allocation-Type AVP is of type Enumerated. It shall indicate whether the PDN GW address is statically allocated or dynamically selected by other nodes. If this AVP is not present, this means that the address is statically allocated. The following values are defined:

STATIC (0)

DYNAMIC (1)

7.3.45 MIP6-Agent-Info

The MIP6-Agent-InfoAVP is of type Grouped and is defined in IETF Draft draft-ietf-dime-mip6-integrated [26]. This AVP shall contain the identity of the PDN-GW.

AVP format

```
MIP6-Agent-Info ::= < AVP Header: TBD >
        *2[ MIP-Home-Agent-Address ]
        [ MIP-Home-Agent-Host ]
        *[ AVP ]
```

7.3.46 RAT-Frequency-Selection-Priority-ID

The RAT-Frequency-Selection-Priority-ID AVP is of type Unsigned32 and shall contain the Subscriber Profile ID for RAT/Frequency Priority. For details, see 3GPP TS 23.401 [2] and 3GPP TS 36.413 [19].

7.3.47 IDA-Flags

The IDA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meanings of the bits are defined in table 7.3.47/1:

Table 7.3.47/1: IDA-Flags

Bit	Name	Description
0	Network Node area restricted	This bit, when set, shall indicate that the complete Network Node area (SGSN area) is restricted due to regional subscription.
Note: Bits not defined in this table shall be cleared by the sending SGSN and discarded by the receiving HSS.		

7.3.48 PUA-Flags

The PUA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meanings of the bits are defined in table 7.3.48/1:

Table 7.3.48/1: PUA-Flags

bit	name	Description
0	Freeze M-TMSI	This bit, when set, shall indicate to the MME that the M-TMSI needs to be frozen, i.e. shall not be immediately re-used.
1	Freeze P-TMSI	This bit, when set, shall indicate to the SGSN that the P-TMSI needs to be frozen, i.e. shall not be immediately re-used.
Note: Bits not defined in this table shall be cleared by the sending HSS and discarded by the receiving MME or SGSN.		

7.3.49 NOR-Flags

The NOR-Flags AVP is of type Unsigned32 and it contains a bit mask. The meaning of the bits is defined in table 7.3.49/1:

Table 7.3.49/1: NOR-Flags

bit	name	Description
0	Single-Registration-Indication	This bit, when set, shall indicate that the HSS shall send a Cancel Location message to the current SGSN due to ISR. An SGSN shall not set this bit when sending NOR.
1	SGSN area restricted	This bit, when set, shall indicate that the complete SGSN area is restricted due to regional subscription.
Note: Bits not defined in this table shall be cleared by the sending MME or SGSN and discarded by the receiving HSS.		

7.3.50 User-Id

The leading digits of a User Name (i.e. MCC, MNC, leading digits of MSIN, see 3GPP TS 23.003 [3]). Within a HSS, a User-Id identifies a set of subscribers, each with identical leading User Name digits.

7.3.51 Equipment-Status

The Equipment-Status AVP is of type Enumerated, and shall contain the status of the mobile equipment. The following values are defined:

WHITELISTED (0)

BLACKLISTED (1)

GREYLISTED (2)

7.3.52 Regional-Subscription-Zone-Code

The Regional-Subscription-Zone-Code AVP is of type OctetString. Up to 10 zone codes may be defined of the tracking or routing areas into which the subscriber is allowed or not allowed to roam. See 3GPP TS 23.003 [3].

When receiving these AVPs within the Subscription-Data AVP the MME or SGSN shall replace stored Zone Codes (if any) with the received information rather than add the received information to the stored information. MMEs and SGSNs that do not support regional subscription need not store zone codes.

7.3.53 RAND

The RAND AVP is of type OctetString. This AVP shall contain the RAND. See 3GPP TS 33.401 [5].

7.3.54 XRES

The XRES AVP is of type OctetString. This AVP shall contain the XRES. See 3GPP TS 33.401 [5].

7.3.55 AUTN

The AUTN AVP is of type OctetString. This AVP shall contain the AUTN. See 3GPP TS 33.401 [5].

7.3.56 KASME

The KASME AVP is of type OctetString. This AVP shall contain the K_ASME. See 3GPP TS 33.401 [5].

7.3.57 Confidentiality-Key AVP

The Confidentiality-Key is of type OctetString, and shall contain the Confidentiality Key (CK).

7.3.58 Integrity-Key AVP

The Integrity-Key is of type OctetString, and shall contain the Integrity Key (IK).

7.3.59 Kc AVP

The Kc-Key is of type OctetString, and shall contain the Ciphering Key (Kc).

7.3.60 SRES

The SRES AVP is of type OctetString. This AVP shall contain the SRES. See 3GPP TS 33.102 [18].

7.3.61 Requesting-Node-Type AVP

The Requesting-Node-Type AVP is of type Enumerated and it shall contain the type of the node requesting for authentication vectors. The following values are defined:

MME (0)

SGSN (1)

MME/SGSN (2)

7.3.62 PDN-Type

The PDN-Type AVP is of type Enumerated and indicates the address type of PDN. The following values are defined:

IPv4 (0)

IPv6 (1)

IPv4v6 (2)

7.3.63 Trace-Data AVP

The Trace-Data AVP is of type Grouped. This AVP shall contain the information related to trace function.

AVP format

Trace-Data ::= <AVP header: XXX XXXX>

{Trace-Reference}

{Trace-Depth-List}

{Trace-NE-Type-List}

[Trace-Interface-List]

{Trace-Event-List}

[OMC-Id]

*[AVP]

7.3.64 Trace-Reference AVP

The Trace-Reference AVP is of type OctetString. This AVP shall contain the concatenation of MCC, MNC and Trace ID, where the Trace ID is a 2 byte Octet String. See 3GPP TS 32.422 [23]. The content of this AVP shall be encoded as octet strings according to table 7.3.64-1. Bits 1111 shall be used as filler when MCC or MNC have less than 3 digits.

Table 7.3.64/1: Encoding format for Trace-Reference AVP

8	7	6	5	4	3	2	1	
MCC digit 2				MCC digit 1				octet 1
MNC digit 3				MCC digit 3				octet 2
MNC digit 2				MNC digit 1				octet 3
Trace ID								octet 4 octet 5

7.3.65 Trace-Depth-List AVP

The Trace-Depth-List AVP is of type Grouped. It shall contain the list of depths of trace per network element.

AVP format

Trace-Depth-List ::= <AVP header: XXX XXXX>

[Network-Element-Type]

[Trace-Depth]

*[AVP]

7.3.66 Network-Element-Type AVP

The Network-Element-Type AVP is of type Enumerated. It shall contain the type of the network element. The following values are defined:

MME (0)

SGSN (1)

Serving GW (2)

PDN GW (3)

eNodeB (4)

RNC (5)

7.3.67 Trace-Depth AVP

The Trace-Depth AVP is of type Enumerated. The possible values are those defined in 3GPP TS 32.422 [23] for Trace Depth.

7.3.68 Trace-NE-Type-List AVP

The Trace-NE-Type-List AVP is of type OctetString. Octets are coded according to 3GPP TS 32.422 [23].

7.3.69 Trace-Interface-List AVP

The Trace-Interface-List AVP is of type OctetString. Octets are coded according to 3GPP TS 32.422 [23].

7.3.70 Trace-Event-List AVP

The Trace-NE-Type-List AVP is of type OctetString. Octets are coded according to 3GPP TS 32.422 [23].

7.3.71 OMC-Id AVP

The OMC-Id AVP is of type OctetString. Octets are coded according to 3GPP TS 29.002 [24].

7.3.72 GPRS-Subscription-Data

The GPRS-Subscription-Data AVP is of type Grouped. It shall contain the information related to the user profile relevant for GPRS.

AVP format:

GPRS-Subscription-Data ::= <AVP header: XXX XXXX>

{ Complete-Data-List-Included-Indicator }

*{PDP-Context}

*[AVP]

7.3.73 Complete-Data-List-Included-Indicator

The Complete-Data-List-Included-Indicator AVP is of type Enumerated. The following values are defined:

All_PDP_CONTEXTS_INCLUDED (0)

MODIFIED/ADDED_PDP CONTEXTS_INCLUDED (1)

7.3.74 PDP-Context

The PDP-Context AVP is of type Grouped.

AVP format

PDP-Context::= <AVP header: XXX XXXX>

{ Context-Identifier }

{ PDP-Type }

[PDP-Address]

{ QoS-Subscribed }

[VPLMN-Dynamic-Address-Allowed]

{ Service-Selection }

[3GPP-Charging-Characteristics]

*[AVP]

7.3.75 PDP-Type

The PDP-Type AVP is of type OctetString. Octets are coded according to 3GPP TS 29.002 [24].

7.3.76 PDP-Address

The PDP-Address AVP is of type OctetString. Octets are coded according to 3GPP TS 29.002 [24].

7.3.77 QoS-Subscribed

The QoS-Subscribed AVP is of type OctetString. Octets are coded according to 3GPP TS 29.002 [24] (octets of QoS-Subscribed, Ext-QoS-Subscribed, Ext2-QoS-Subscribed and Ext3-QoS-Subscribed values are concatenated).

7.3.78 CSG-Subscription-Data

The CSG-Subscription-Data AVP is of type Grouped. This AVP shall contain the CSG-Id and optionally an associated expiration date.

AVP format

CSG-Subscription-Data ::= <AVP header: XXX XXXX>

{ CSG-Id }

[Expiration-Date]

*[AVP]

7.3.79 CSG-Id

The CSG-Id-Data AVP is of type Unsigned32. Values are coded according to 3GPP TS 23.003 [3]. Unused bits (least significant) shall be padded with zeros.

7.3.80 Expiration-Date

The Expiration-Date AVP is of type Time (see IETF RFC 3588 [4]) and contains the point in time when subscription to the CSG-Id expires.

7.3.81 Roaming-Restricted-Due-To-Unsupported-Feature

The Roaming-Restricted-Due-To-Unsupported-Feature AVP is of type Enumerated and indicates that roaming is restricted due to unsupported feature. The following value is defined:

Roaming-Restricted-Due-To-Unsupported-Feature (0)

7.4 Result-Code and Experimental-Result Values

7.4.1 General

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

7.4.2 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 [4] shall be applied.

7.4.3 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 [4] 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.

7.4.3.1 DIAMETER_ERROR_USER_UNKNOWN (5001)

This result code shall be sent by the HSS to indicate that the user identified by the User Name is unknown

7.4.3.2 DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION (5420)

This result code shall be sent by the HSS to indicate that no EPS subscription is associated with the IMSI.

7.4.3.3 DIAMETER_ERROR_RAT_NOT_ALLOWED (5421)

This result code shall be sent by the HSS to indicate the RAT type the UE is using is not allowed for the IMSI.

7.4.3.4 DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)

This result code shall be sent by the HSS to indicate that the subscriber is not allowed to roam within the MME or SGSN area.

7.4.3.5 DIAMETER_ERROR_EQUIPMENT_UNKNOWN (5422)

This result code shall be sent by the EIR to indicate that the mobile equipment is not known in the EIR.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2008-09	CT#41	CP-080475			V2.0.0 approved in CT#41	2.0.0	8.0.0
2008-12	CT#42	CP-080691	0001	1	S6a Vendor-Specific-Application-Id AVP	8.0.0	8.1.0
		CP-080691	0002	1	RegSub feature		
		CP-080691	0005		Clarification on Immediate-Response-Preferred		
		CP-080691	0006	1	Correction of the Reference of Supported Features		
		CP-080691	0007		Definition of RAT-Frequency-Selection-Priority		
		CP-080691	0008	2	ME Identity Check		
		CP-080703	0009	2	Gr alignment		
		CP-080691	0010	3	Closed Subscriber Group		
		CP-080691	0011		AVP codes		
		CP-080691	0012	1	MSISDN AVP		
		CP-080691	0013		Result codes		
		CP-080691	0014		Removal of Editor's note in ULA Flag		
		CP-080691	0015	2	Duplicated AMBR AVP and Use of Called-Station-Id		
		CP-080691	0017		Change of AVP to carry the APN information		
		CP-080691	0018	1	Reference to 3GPP-Charging-Characteristics		
		CP-080691	0019		Access Restriction Data Definition		
		CP-080691	0020		AMBR Definition		
		CP-080691	0021	1	AVPs Encoding		
		CP-080691	0022	1	PDN-GW Delete		
		CP-080691	0023	1	Requesting Node Type Clarification		
		CP-080691	0024		Authn Session State AVP		
		CP-080691	0026	2	Trace Session Activation and Deactivation		
		CP-080691	0027	1	Context-Identifier in APN-Configuration-Profile		
		CP-080691	0029		APN-OIReplacement		
		CP-080703	0032		Access Restriction		
		CP-080691	0033	1	Context Identifier clarification		
		CP-080691	0034	1	APN-Configuration correction		
		CP-080691	0037		Removal of Supported RAT Types		
		CP-080691	0039	1	Extension of the Terminal-Information AVP for non-3GPP accesses		
		CP-080691	0040		Conditionality of ULA-Flags and PUA-Flags AVPs		
		CP-080691	0042		Wrong Description for Complete APN Configuration Profile Withdrawal		
		CP-080691	0043		Purge UE Detailed Behaviour		
		CP-080691	0044	1	MME/SGSN area restricted flag cleanup		
					TS number in cover page corrected	8.1.0	8.1.1

History

Document history		
V8.1.1	January 2009	Publication