ETSI TS 129 336 V14.4.0 (2018-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications
(3GPP TS 29.336 version 14.4.0 Release 14)

Reference
RTS/TSGC-0429336ve40

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

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

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

Trademarks

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

Foreword

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

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

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

Modal verbs terminology

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

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

Contents

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 Diameter-based interfaces between the HSS and other network elements involved in the architecture for interworking with packet data networks and applications, such as Machine-Type Communications (MTC).

In particular, this document specifies the S6m interface between the Home Subscriber Server (HSS) and the MTC Interworking Function (MTC-IWF), the S6n interface between the HSS and the MTC-AAA and the S6t interface between the HSS and the Service Capability Exposure Function (SCEF). The procedures over those interfaces are defined in 3GPP TS 23.682 [2].

2 References

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

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

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[3] Void.

[4] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[5] IETF RFC 4960: "Stream Control Transport Protocol".

[6] 3GPP TS 29.228: "IP multimedia (IM) Subsystem Cx Interface; Signalling flows and Message Elements".

[7] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; protocol details ".

[8] 3GPP TS 29.173: "Diameter-based SLh interface for Control Plane LCS".

[9] IETF RFC 5234: "Augmented BNF for Syntax Specifications: ABNF".

[10] 3GPP TS 29.329: "Sh Interface based on the Diameter protocol".

[11] 3GPP TS 23.003: "Numbering, addressing and identification".

[12] 3GPP TS 29.338: "Diameter based protocols to support SMS capable MMEs".

[13] 3GPP TS 29.368: "Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS)".

[14] 3GPP TS 29.272: "Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

[15] IETF RFC 7683 : "Diameter Overload Indication Conveyance".

[16] 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications".

[17] 3GPP TS 29.217: "Congestion Reporting Over Np Reference Point".

[18] IETF RFC 5777: "Traffic Classification and Quality of Service (QoS) Attributes for Diameter".

[19] 3GPP TS 23.007: "Restoration procedures".

[20] IETF RFC 7944: "Diameter Routing Message Priority".

[21] IETF RFC 5778: "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction".

[22] IETF draft-ietf-dime-load-03: "Diameter Load Information Conveyance".

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

[23] IETF RFC 6733: "Diameter Base Protocol".

3 Definitions, symbols and abbreviations

3.1 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].

AAA	Authentication, Authorization and Accounting
ABNF	Augmented Backus-Naur Form
AVP	Attribute-Value Pair
DRMP	Diameter Routing Message Priority
DSCP	Differentiated Services Code Point
IANA	Internet Assigned Numbers Authority
MTC	Machine-Type Communications
MTC-IWF	MTC Interworking Function
NIDD	Non-IP Data Delivery
SCS	Services Capability Server
SCEF	Service Capability Exposure Function

4 General Description

4.1 Introduction

The S6m reference point between the MTC-IWF and the HSS, the S6n reference point between the MTC-AAA and the HSS, and the S6t reference point between the SCEF and the HSS, are defined in the 3GPP TS 23.682 [2].

This document describes the Diameter-based S6m, S6n and S6t related procedures, message parameters and protocol specification.

An excerpt of the architecture for Machine-Type Communication, as defined in 3GPP TS 23.682 [2] is shown in Figure 4.1-1, where the relevant interfaces towards the HSS are highlighted.

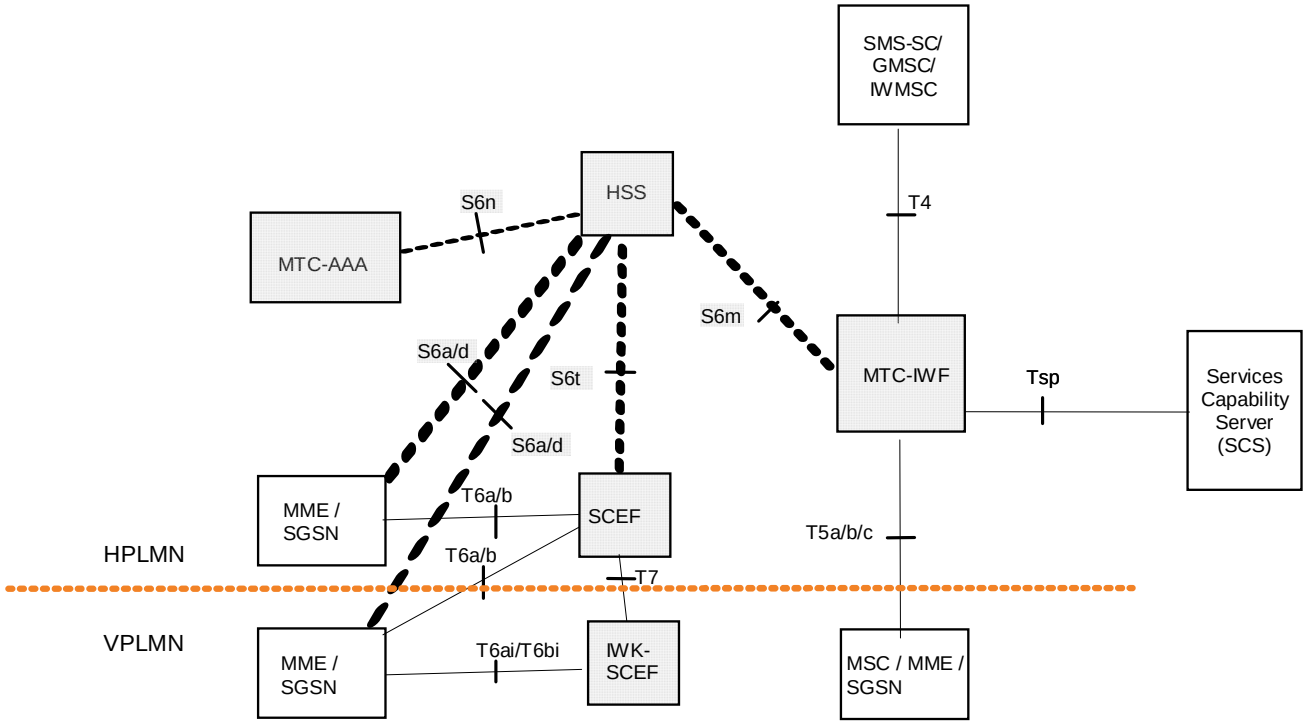

Figure 4.1-1: 3GPP Architecture for Machine-Type Communication

In this architecture, the S6m reference point connects the MTC-IWF with the HSS, where the subscription information of the UE (e.g., an MTC device) is stored. This reference points allows the MTC-IWF to retrieve subscription data and to do any necessary mapping between different identities associated to the UE.

The S6m interface shall allow the MTC-IWF to:

- retrieve subscription information of the UE from the HSS,
- request routing information from the HSS, i.e. the address of the UE's serving nodes supporting SMS for the UE ; in this context serving nodes of the UE are the MSC or MME but not both, the SGSN, and the IP-SM-GW,
- retrieve the IMSI of the UE,
- retrieve the External Identifier of the UE associated to an Application Port Identifier,
- perform authorization of the Service Capability Server that is requesting to send a device trigger to the UE.

Additionally, the S6n reference point connects the MTC-AAA with the HSS, and it allows the MTC-AAA to do the mapping of the UE IMSI to the external identifier(s) of the UE.

The S6t reference point connects the SCEF with the HSS to perform configuration and reporting of Monitoring events, and configuration of AESE Communication Pattern.

The S6t interface shall allow the SCEF to:

- configure UE related Monitoring events
- receive reporting of the configured Monitoring events from the HSS
- configure UE related AESE Communication Pattern
- Authorize the UE for NIDD.

5 Diameter-based S6m/S6n Interface

5.1 Introduction

This section describes the Diameter-based S6m and S6n interface related procedures and Information elements exchanged between functional entities.

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

5.2 Procedure Descriptions

5.2.1 Subscriber Information Retrieval

5.2.1.1 General

This procedure is used between the MTC-IWF and the HSS and between the MTC-AAA and the HSS.

When the procedure is invoked by the MTC-IWF, it is used:

- To translate an external identifier, or MSISDN, to the IMSI of the user,
- To retrieve information about the serving entities currently serving a certain user,
- To authorize a certain SCS to request a specific service (e.g. device triggering),
- To retrieve subscription data of the user, associated to the specific service requested by the SCS,
- To retrieve an External Identifier based on IMSI and application port identifier.

When the procedure is invoked by the MTC-AAA, it is used:

- To translate an IMSI to one or more external identifiers of the user.

This procedure is mapped to the commands Subscriber-Information-Request/Answer in the Diameter application specified in chapter 6. Tables 5.2.1.1/1 and 5.2.1.1/2 detail the involved information elements.

Table 5.2.1.1/1: Subscriber Information Retrieval (Request)

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User Identity (see 6.4.2)	User-Identifier	M	This Information Element shall contain the identity of the UE. This is a grouped AVP containing either an External Identifier, an MSISDN or an IMSI (exactly one, and only one, of those identifiers shall be included in the request).
Requested Service (see 6.4.3)	Service-ID	O	This Information Element shall contain the service requested by the SCS. In this release, only the Device Triggering and SMS_MO services are supported.
SCS Identity (see 6.4.4)	SCS-Identity	O	This Information Element shall contain the identity of the Service Capability Server that is requesting a service to be applied to a certain UE. When the Service-ID indicates DEVICE_TRIGGER (0) or SMS_MO (1), the SCS-Identity shall be formatted as an E.164 address as described in section 6.4.4.
Service Parameters (see 6.4.5)	Service-Parameters	O	This Information Element shall contain the parameters associated to the requested service by the SCS (identified by the Service-ID AVP). In this release, only parameters associated to Device Triggering via SMS-MT (T4) and parameters associated to SMS_MO are supported. For Device Triggering via SMS-MT, this AVP may contain: Priority-Indication, SM-RP-SMEA… For SMS_MO, this parameter may contain: Application-Port Identifier.
SIR Flags (see 6.4.10)	SIR-Flags	M	This Information Element shall contain a bit mask. See section 6.4.10 for the meaning of the bits.
Supported Features (See 3GPP TS 29.229 [7])	Supported-Features	O	If present, this Information Element shall contain the list of features supported by the origin host.

Table 5.2.1.1/2: Subscriber Information Retrieval (Response)

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result (See 6.3)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [23]). Experimental-Result AVP shall be used for S6m/S6n errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Identity (see 6.4.2)	User-Identifier	C	This information element shall contain the User Identity of the UE. This is a grouped AVP containing an External Identifier, an MSISDN, an IMSI, or other service-specific identities (such as an LMSI…). There may be multiple instances of this IE in the response provided by the HSS. This IE shall be present only when the Result- Code is DIAMETER_SUCCESS.
Service Data (see 6.4.7)	Service-Data	C	This information element shall contain data related to the requested service and additional data specific to each triggering method. In this release, only data associated to trigger delivery via SMS-MT (T4) is supported. This IE shall be present only when the Requested Service IE was included in the request, and the Result- Code is DIAMETER_SUCCESS.
Supported Features (See 3GPP TS 29.229 [7])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

5.2.1.2 Detailed Behaviour of the HSS

When the Subscriber Information Retrieval request is received from the MTC-IWF, indicated by the S6m/S6n indicator, which shall be set, the HSS shall, in the following order:

1. Check that the User Identity for whom data is asked exists in HSS. If not, Experimental-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Subscriber Information Retrieval Response.

2. Check whether the requesting/receiving SCS is authorized to request/receive the specified service for the UE. If not, Experimental-Result shall be set to DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY (5510) in the Subscriber Information Retrieval Response.

3. Check that the requested service (e.g., device trigger) is present and authorized. If not, Experimental-Result shall be set to DIAMETER_ERROR_UNAUTHORIZED_SERVICE (5511) in the Subscriber Information Retrieval Response.

4. If the requested service is DEVICE_TRIGGER, check whether the UE is currently registered in any serving node supporting SMS for the UE (MSC or MME which has registered as MSC but not both, SGSN, IP-SM-GW). If the user is not registered in any serving node, the HSS shall answer successfully, but it shall not include any Serving Node or Additional Serving Node(s) in the response; also, it shall indicate to the MTC-IWF that the user is absent, in the Subscriber Information Retrieval Response, by setting the relevant bit in the HSS-Cause IE.

   The HSS shall also check if the UE is known to be not reachable in the registered serving nodes (i.e. check MNRF, MNRG, and UNRI) and if the trigger delivery is requested with "non-priority"; if both are true, the HSS shall answer successfully, but it shall not include any Serving Node or Additional Serving Node(s) in the response, and it shall set the "Absent Subscriber" flag in the HSS-Cause IE.

5. If the requested service is DEVICE_TRIGGER, check whether the requested service cannot be delivered according to the user's provisioned teleservices and the user's active barring conditions. If so, the HSS shall answer successfully, but it should not include any Serving Node or Additional Serving Node(s) in the response, and it shall set accordingly the corresponding bits in the HSS-Cause IE (see clause 6.4.9).

6. If the requested service is SMS_MO, check whether IMSI and Application Port Identifier are present in the request within User-Identifier and Service- Parameters AVPs. If not, Experimental-Result shall be set to DIAMETER_ERROR_MISSING_APPLICATION_DATA (5598) in the Subscriber Information Retrieval Response.

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

If the HSS cannot fulfil the received request for reasons not stated in the above steps (e.g. due to a database error), it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

Otherwise, the requested operation shall take place and the HSS shall return the Result-Code AVP set to DIAMETER_SUCCESS. If the requested service is DEVICE_TRIGGER, the HSS returns the network addresses of the registered serving nodes supporting SMS for the UE (MSC or MME that has registered as MSC but not both and/or SGSN and/or IP-SM-GW), if available (and not marked "not reachable" by MNRF, MNRG, or UNRI, unless priority was indicated) in the HSS, and the IMSI of the subscriber, and the corresponding data needed by the service requested by the SCS; if available, the MSISDN of the user shall also be returned by the HSS, along with the user's IMSI. If the requested service is SMS_MO, the HSS returns the External-Identifier associated to the Application Port Identifier.

When the Subscriber Information Retrieval request is received from the MTC-AAA, indicated by the S6m/S6n indicator, which shall be cleared, the HSS shall check:

- That the User Identity IE is included in the request, and that it contains an IMSI; if other IEs are included in the request, they may be ignored by the HSS.

- Whether the user identified by that IMSI is known in the HSS. If it is known, the HSS shall answer successfully and return in the response one or several instances of the User Identity IE, each one containing either an External-Identifier or an MSISDN. If it is not known, Experimental-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Subscriber Information Retrieval Response.

5.2.1.3 Detailed Behaviour of the MTC-IWF

When the MTC-IWF sends a Subscriber Information Retrieval request to the HSS, it shall set the S6m/S6n indicator bit in the SIR Flags IE.

Upon receipt of a successful Subscriber Information Retrieval response for the DEVICE_TRIGGER service, when multiple serving nodes are returned from HSS, the MTC-IWF should give a higher preference to the serving node included in the "Serving Node" IE, than to those serving nodes included in the list of "Additional Serving Node" IEs.

Upon receipt of a successful Subscriber Information Retrieval response for the SMS_MO service, the MTC-IWF shall use the retrieved External-Identifier for communication with the SCS via Tsp.

5.2.1.4 Detailed Behaviour of the MTC-AAA

When the MTC-AAA sends a Subscriber Information Retrieval request to the HSS, it shall clear the S6m/S6n indicator bit in the SIR Flags IE.

The MTC-AAA shall only include the User Identifier IE in the request, and it shall contain only the IMSI of the UE.

6 Protocol Specification

6.1 Introduction

6.1.1 Use of Diameter Base Protocol

The Diameter base protocol as specified in IETF RFC 6733 [23] shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and error codes as specified in this specification. Unless otherwise specified, the procedures (including error handling and unrecognised information handling) shall be used unmodified.

6.1.2 Securing Diameter Messages

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

6.1.3 Accounting Functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) shall not be used on the S6m interface.

6.1.4 Use of Sessions

Between the MTC-IWF and the HSS, 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 as specified in IETF RFC 6733 [23] 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 6733 [23]. As a consequence, the server shall not maintain any state information about this session and the client shall not send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

6.1.5 Transport Protocol

Diameter messages over the S6m interface shall make use of SCTP IETF RFC 4960 [5] as transport protocol.

6.1.6 Routing Considerations

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

The S6m reference point is defined as an intra-operator interface so, both MTC-IWF and HSS shall be located in the same network domain/realm.

If the MTC-IWF knows the address/name of the HSS for a certain user, both the Destination-Realm AVP and the Destination-Host AVP shall be present in the request. Otherwise, only the Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node. Consequently, the Destination-Host AVP is declared as optional in the ABNF for all requests initiated by the MTC-IWF.

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

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

6.1.7 Advertising Application Support

The HSS and the MTC-IWF shall advertise support of the Diameter S6m 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 IETF RFC 6733 [23].

6.1.8 Diameter Application Identifier

The S6m/S6n 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 S6m interface application is 16777310 (allocated by IANA).

6.1.9 Use of the Supported-Features AVP

When new functionality is introduced on the S6m application, it should be defined as optional. If backwards incompatible changes can not be avoided, the new functionality shall be introduced as a new feature and support advertised with the Supported-Features AVP. The usage of the Supported-Features AVP on the S6m application is consistent with the procedures for the dynamic discovery of supported features as defined in clause 7.2 of 3GPP TS 29.229 [7].

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

As defined in 3GPP TS 29.229 [7], the Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the all reference points as specified in this specification, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, for features defined in this document, the Vendor-Id AVP shall contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the reference point, the Feature-List-ID AVP shall differentiate those lists from one another.

6.1.10 User Identity to HSS resolution

The User identity to HSS resolution mechanism enables the MTC-IWF to find the identity of the HSS that holds the subscription data for the target user when multiple and separately addressable HSSs have been deployed in the home network. The resolution mechanism is not required in networks that utilise a single HSS.

This User identity to HSS resolution mechanism may rely on routing capabilities provided by Diameter and be implemented in the home operator network within dedicated Diameter Agents (Redirect Agents or Proxy Agents) responsible for determining the HSS identity based on the provided user identity (e.g., external identifiers provided by the MTC-IWF).

When the Diameter Load Control mechanism is supported (see IETF draft-ietf-dime-load-03 [22]), load values from previously received Load AVPs of type HOST may be taken into account when determining the HSS identity.

NOTE: Alternatives to the user identity to HSS resolution Diameter based implementation are outside the scope of this specification.

6.2 Commands

6.2.1 Introduction

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

6.2.2 Command-Code values

This section defines Command-Code values for the S6m/S6n interface application as allocated by IANA.

Every command is defined by means of the ABNF syntax IETF RFC 5234 [9], according to the Command Code Format (CCF) specification defined in IETF RFC 6733 [23]. When the definition and use of an AVP is not specified in this document, the guidelines in IETF RFC 6733 [23] shall apply.

The Vendor-Specific-Application-Id AVP shall not be included in any command sent by Diameter nodes supporting applications defined in this specification. If the Vendor-Specific-Application-Id AVP is received in any of the commands defined in this specification, it shall be ignored by the receiving node.

NOTE: The Vendor-Specific-Application-Id is included as an optional AVP in all Command Code Format specifications defined in this specification in order to overcome potential interoperability issues with intermediate Diameter agents non-compliant with the IETF RFC 6733 [23].

The following Command Codes are defined in this specification:

Table 6.2.2/1: Command-Code values for S6m/S6n

Command-Name	Abbreviation	Code	Section
Subscriber-Information-Request	SIR	8388641	6.2.3
Subscriber-Information-Answer	SIA	8388641	6.2.4

For these commands, the Application-ID field shall be set to 16777310 (application identifier of the S6m/S6n interface application, allocated by IANA).

6.2.3 Subscriber-Information-Request (SIR) Command

The Subscriber-Information-Request (SIR) command, indicated by the Command-Code field set to 8388641 and the "R" bit set in the Command Flags field, is sent from the MTC-IWF to the HSS or from the MTC-AAA to the HSS.

Message Format:

```
< Subscriber-Information-Request> ::=     < Diameter Header: 8388641, REQ, PXY, 16777310 >
                                          < Session-Id >
                                          [ DRMP ]
                                          { Auth-Session-State }
                                          { Origin-Host }
                                          { Origin-Realm }
                                          [ Destination-Host ]
                                          { Destination-Realm }
                                          { User-Identifier }
                                          [ Service-ID ]
                                          [ SCS-Identity ]
                                          [ Service-Parameters ]
                                          { SIR-Flags }
                                          [ OC-Supported-Features ]
                                          *[ Supported-Features ]
                                          *[ Proxy-Info ]
                                          *[ Route-Record ]
                                          *[ AVP ]
```

6.2.4 Subscriber-Information-Answer (SIA) Command

The Subscriber-Information-Answer (SIA) command, indicated by the Command-Code field set to 8388641 and the "R" bit cleared in the Command Flags field, is sent from the HSS to the MTC-IWF or from the HSS to the MTC-AAA.

Message Format:

< Subscriber-Information-Answer> ::=< Diameter Header: 8388641, PXY, 16777310 >
< Session-Id >
[DRMP]
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[OC-Supported-Features]
[OC-OLR]
*[Load]
*[Supported-Features]
*[User-Identifier]
[Service-Data]
[Failed-AVP]
*[Proxy-Info]
*[Route-Record]
*[AVP]

6.3 Result-Code AVP and Experimental-Result AVP Values

6.3.1 General

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

6.3.2 Success

Result codes that fall within the Success category shall be used to inform a peer that a request has been successfully completed. The Result-Code AVP values defined in Diameter base protocol as specified in IETF RFC 6733 [23] shall be applied.

6.3.3 Permanent Failures

Errors that fall within the Permanent Failures category shall be used to inform the peer that the request has failed, and should not be attempted again. The Result-Code AVP values defined in Diameter base protocol as specified in IETF RFC 6733 [23] shall be applied. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and the Result-Code AVP shall be absent.

6.3.3.1 DIAMETER_ERROR_USER_UNKNOWN (5001)

This result code shall be sent by the HSS to indicate that the user identified by the IMSI, MSISDN, or External-Identifier is unknown. This error code is defined in 3GPP TS 29.229 [7].

6.3.3.2 DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY (5510)

This result code shall be sent by the HSS to indicate that the SCS is not allowed to request control plane services for an UE, to the MTC-IWF.

6.3.3.3 DIAMETER_ERROR_UNAUTHORIZED_SERVICE (5511)

This result code shall be sent by the HSS to indicate that the specific service requested by the SCS is not allowed for an UE, or that it cannot be delivered according to the current subscribed services of the UE.

6.4 AVPs

6.4.1 General

The following table specifies the Diameter AVPs defined for the S6m/S6n 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).

For all AVPs which contain bit masks and are of the type Unsigned32, bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x00000001 should be used.

Table 6.4.1/1: S6m/S6n specific Diameter AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
IP-SM-GW-Number	3100	6.4.14	OctetString	M,V				No
IP-SM-GW-Name	3101	6.4.15	DiameterIdentity	M,V				No
User-Identifier	3102	6.4.2	Grouped	M,V				No
Service-ID	3103	6.4.3	Enumerated	M,V				No
SCS-Identity	3104	6.4.4	OctetString	M,V				No
Service-Parameters	3105	6.4.5	Grouped	M,V				No
T4-Parameters	3106	6.4.6	Grouped	M,V				No
Service-Data	3107	6.4.7	Grouped	M,V				No
T4-Data	3108	6.4.8	Grouped	M,V				No
HSS-Cause	3109	6.4.9	Unsigned32	M,V				No
SIR-Flags	3110	6.4.10	Unsigned32	M,V				No
External-Identifier	3111	6.4.11	UTF8String	M,V				No
IP-SM-GW-Realm	3112	6.4.18	DiameterIdentity	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 6733 [23].

NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.

The following table specifies the Diameter AVPs re-used by the S6m/S6n interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within S6m/S6n.

Any other AVPs from existing Diameter Applications, except for the AVPs from Diameter base protocol as specified in IETF RFC 6733 [23], do not need to be supported. The AVPs from Diameter base protocol as specified in IETF RFC 6733 [23] are not included in table 6.4.1/2, but they may be re-used for the S6m/S6n protocol.

Table 6.4.1/2: S6m/S6n re-used Diameter AVPs

Attribute Name	Reference	Comments
User-Name	IETF RFC 6733 [23]	This AVP shall contain the IMSI of the UE, in the User-Identifier AVP.
MSISDN	3GPP TS 29.329 [10]	
LMSI	3GPP TS 29.173 [8]	
Serving-Node	3GPP TS 29.173 [8]	see 6.4.12
Additional-Serving-Node	3GPP TS 29.173 [8]	see 6.4.13
Supported-Features	3GPP TS 29.229 [7]	
Feature-List-ID	3GPP TS 29.229 [7]	
Feature-List	3GPP TS 29.229 [7]	
SM-RP-SMEA	3GPP TS 29.338 [12]	
Priority-Indication	3GPP TS 29.368 [13]	
MME-Number-for-MT-SMS	3GPP TS 29.272 [14]	
OC-Supported-Features	IETF RFC 7683 [15]	See 6.4.16
OC-OLR	IETF RFC 7683 [15]	See 6.4.17
DRMP	IETF RFC 7944 [20]	see section 6.4.19
Application-Port-Identifier	3GPP TS 29.368 [13]	
Load	IETF draft-ietf-dime-load-03 [22]	See 6.4.20

6.4.2 User-Identifier

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

AVP format:

User-Identifier ::= <AVP header: 3102 10415>

[User-Name]

[MSISDN]

[External-Identifier]

[LMSI]

*[AVP]

This AVP shall contain at least one of the identifiers used by the UE, i.e., it shall not be empty. The IMSI of the UE shall be included (when applicable) in the User-Name AVP.

6.4.3 Service-ID

The Service-ID AVP is of type Enumerated and it shall identify the service requested by the SCS. The following values are defined:

DEVICE_TRIGGER (0)

The SCS requests a control plane device triggering to the UE. .

SMS_MO (1)

The UE (identified by IMSI and application port identifier) requests SMS_MO to be delivered to the SCS.

6.4.4 SCS-Identity

The SCS-Identity AVP is of type OctetString and it shall contain the identity of the SCS or UE which originated the service request towards the MTC-IWF, over the Tsp reference point.

The encoding of the SCS-Identity AVP is defined per SCS service.

For the device triggering service, the SCS-Identity AVP shall contain the ISDN number of the SCS in international ISDN number format as described in ITU-T Rec E.164 [41]. It shall be encoded as a TBCD-string. See 3GPP TS 29.002 [24] for encoding of TBCD-strings. This AVP shall not include leading indicators for the nature of address and the numbering plan.

6.4.5 Service-Parameters

The Service-Parameters AVP is of type Grouped, and it contains the service-specific parameters related to the requested service.

AVP format:

Service-Parameters ::= <AVP header: 3105 10415>

[T4-Parameters]

[Application-Port-Identifier]

*[AVP]

6.4.6 T4-Parameters

The T4-Parameters AVP is of type Grouped.

AVP format:

T4-Parameters ::= <AVP header: 3106 10415>

[Priority-Indication]

[SM-RP-SMEA]

*[AVP]

6.4.7 Service-Data

The Service-Data AVP is of type Grouped, and it contains the service-specific data related to the device triggering request handled by the MTC-IWF.

Service-Data ::= <AVP header: 3107 10415>

[T4-Data]

*[AVP]

6.4.8 T4-Data

The T4-Data AVP is of type Grouped and it shall contain information about the network node(s) serving the targeted user for SMS, i.e. the names/numbers of the serving nodes (MSC or MME, SGSN, IP-SM-GW) which allow the trigger delivery. AVP format:

T4-Data ::= <AVP header: 3108 10415>

[HSS-Cause]

[Serving-Node]

*[Additional-Serving-Node]

*[AVP]

When the HSS-Cause indicates Absent Subscriber, via the corresponding flag in the bit mask, the Serving-Node and Additional-Serving-Node AVPs shall not be present. When the HSS-Cause indicates Teleservice Not Provisioned or Call Barred, via the corresponding flag in the bit mask, the Serving-Node and Additional-Serving-Node AVPs should not be present. Additional-Serving-Node AVP shall be absent if Serving-Node AVP is absent.

6.4.9 HSS-Cause

The HSS-Cause AVP is of type Unsigned32 and it contains a bit mask. The meaning of the bits is defined in table 6.4.9/1:

Table 6.4.9/1: HSS-Cause

Bit	Name	Description
0	Absent Subscriber	This bit, when set, indicates that there is no serving node registered in the HSS over which the corresponding triggering method should be immediately attempted for the user. NOTE 1.
1	Teleservice Not Provisioned	This bit, when set, indicates that the required teleservice(s) for the corresponding triggering method are not provisioned in the HSS/HLR for the user.
2	Call Barred	This bit, when set, indicates that the user has an active barring condition which makes it impossible to deliver the corresponding triggering method.
NOTE 1: This may be caused because there is not any serving node currently registered in HSS for the user, or because the user is known to be absent in all suitable registered serving nodes (based on MNRF, MNRG and UNRI flags) and the trigger delivery is requested with "non-priority". NOTE 2: Bits not defined in this table shall be cleared by the HSS and discarded by the receiving node, MTC-IWF.		

6.4.10 SIR-Flags

The SIR-Flags AVP is of type Unsigned32 and it contains a bit mask. The meaning of the bits is defined in table 6.4.10/1:

Table 6.4.10/1: SIR-Flags

bit	name	Description
0	S6m/S6n Indicator	This bit, when set, indicates that the SIR message is sent on the S6m interface, i.e. the source node is an MTC-IWF. This bit, when cleared, indicates that the SIR message is sent on the S6n interface, i.e. the source node is an MTC-AAA.
Note: Bits not defined in this table shall be cleared by the sending node, MTC-IWF or MTC-AAA, and discarded by the receiving HSS.		

6.4.11 External-Identifier

The External-Identifier AVP is of type UTF8String, and it shall contain an external identifier of the UE. See 3GPP TS 23.003 [11] for the definition and formatting of the external identifier.

6.4.12 Serving-Node

The Serving-Node AVP is of type Grouped and it shall contain the name/number of the serving node to be used for T4-triggering. It is originally defined in 3GPP TS 29.173 [8].

Serving-Node ::=<AVP header: 2401 10415>

[SGSN-Name]

[SGSN-Realm]

[SGSN-Number]

[MME-Name]

[MME-Realm]

[MME-Number-for-MT-SMS]

[MSC-Number]

[IP-SM-GW-Number]

[IP-SM-GW-Name]

[IP-SM-GW-Realm]

*[AVP]

The following combinations are allowed:

a) SGSN-Number

b) SGSN-Name & SGSN-Realm & SGSN-Number if the HSS supports the "Gdd in SGSN" feature and has received the "Gdd in SGSN" indication over S6a or Gr interface from the SGSN (cf. 3GPP TS 29.272 [4] and 3GPP TS 29.002 [9])

c) MME-Name & MME-Realm & MME-Number-for-MT-SMS

d) MSC-Number

e) MSC-Number & MME-Name & MME-Realm

f) IP-SM-GW-Number

g) IP-SM-GW-Number & IP-SM-GW-Name & IP-SM-GW-Realm

6.4.13 Additional-Serving-Node

The Additional-Serving-Node AVP is of type Grouped and when present it shall contain the name/number of an additional serving node to be used for T4-triggering. It is originally defined in 3GPP TS 29.173 [8],

Additional-Serving-Node ::= <AVP header: 2406 10415>

[SGSN-Name]

[SGSN-Realm]

[SGSN-Number]

[MME-Name]

[MME-Realm]

[MME-Number-for-MT-SMS]

[MSC-Number]

*[AVP]

The following combinations are allowed:

a) SGSN-Number

b) SGSN-Name & SGSN-Realm & SGSN-Number if the HSS supports the "Gdd in SGSN" feature and has received the "Gdd in SGSN" indication over S6a or Gr interface from the SGSN (cf. 3GPP TS 29.272 [4] and 3GPP TS 29.002 [9])

c) MME-Name & MME-Realm & MME-Number-for-MT-SMS

d) MSC-Number

e) MSC-Number & MME-Name & MME-Realm

6.4.14 IP-SM-GW-Number

The IP-SM-GW-Number AVP is of type OctetString and it shall contain the ISDN number of the IP-SM-GW in international number format as described in ITU-T Rec E.164 [41]. It shall be encoded as a TBCD-string. See 3GPP TS 29.002 [24] for encoding of TBCD-strings. This AVP shall not include leading indicators for the nature of address and the numbering plan.

6.4.15 IP-SM-GW-Name

The IP-SM-GW-Name AVP is of type DiameterIdentity and it shall contain the Diameter identity of the registered IP-SM-GW. For further details on the encoding of this AVP, see IETF RFC 3588 [5].

6.4.16 OC-Supported-Features

The OC-Supported-Features AVP is of type Grouped and it is defined in IETF RFC 7683 [15]. This AVP is used to support Diameter overload control mechanism, see Annex A for more information.

6.4.17 OC-OLR

The OC-OLR AVP is of type Grouped and it is defined in IETF RFC 7683 [15]. This AVP is used to support Diameter overload control mechanism, see Annex A for more information.

6.4.18 IP-SM-GW-Realm

The IP-SM-GW-Realm AVP is of type DiameterIdentity and it shall contain the Diameter identity of the registered IP-SM-GW's realm. For further details on the encoding of this AVP, see IETF RFC 3588 [5].

6.4.19 DRMP

The DRMP AVP is of type Enumerated and it is defined in IETF RFC 7944 [20]. This AVP allows the HSS and the MTC-IWF over the S6m interface and the HSS and the MTC-AAA over the S6n interface to indicate the relative priority of Diameter messages. The DRMP AVP may be used to set the DSCP marking for transport of the associated Diameter message.

6.4.20 Load

The Load AVP is of type Grouped and it is defined in IETF draft-ietf-dime-load-03 [22]. This AVP is used to support the Diameter load control mechanism.

7 Diameter-based S6t Interface

7.1 Introduction

This section describes the Diameter-based S6t interface related procedures and Information elements exchanged between functional entities.

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

7.2 Procedure Descriptions

7.2.1 Configuration Information on S6t

7.2.1.1 General

This procedure is used between the SCEF and the HSS for:

- the configuration/deletion of Monitoring events for a UE or a Group of UEs;
- the configuration/deletion of Communication Patterns;
- the configuration/query of Enhanced Coverage Restrictions.

The following events may be configured for monitoring:

- the association of the UE and UICC and/or new IMSI-IMEI-SV association;
- the UE reachability;
- location of the UE, and change in location of the UE;
- loss of connectivity;
- Communication failure;
- Roaming status (i.e. Roaming or No Roaming, VPLMN-ID) of the UE, and change in roaming status of the UE.
- Availability after DDN failure.

This procedure is mapped to the commands Configuration-Information-Request/Answer in the Diameter application specified in clause 8. The tables 7.2.1.1-1 and 7.2.1.1-2 detail the involved information elements.

Table 7.2.1.1-1: Configuration Information Request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User Identity (see 6.4.2)	User-Identifier	M	This Information Element shall contain the identity of the UE or the identity of a group of UEs. This is a grouped AVP containing either an External Identifier or an MSISDN (exactly one, and only one, of those identifiers shall be included in the request). When requesting event monitoring configuration for a group of UEs, the SCEF shall include the External Group Identifier (see 3GPP TS 23.003 [11]) in the External-Identifier AVP.
Group Reporting Guard Timer (See 8.4.59)	Group-Reporting-Guard-Timer	C	If present, this Information Element indicates that the collected Status Indications and/or reports for UEs belonging to a group shall be reported no later than at the interval indicated by the Group Reporting Guard Timer. Shall be present if the User-Identifier contains an External Group Identifier.
Supported Features (See 3GPP TS 29.229 [7])	Supported-Features	O	If present, this Information Element shall contain the list of features supported by the origin host.
Monitoring Event Configuration (see 8.4.2)	Monitoring-Event-Configuration	O	If present, this Information Element shall contain the details of Monitoring event(s). Multiples instances covering different monitoring events may be present.
AESE Communication Pattern (see 8.4.25)	AESE-Communication-Pattern	O	If present, this Information Element shall contain the details of Communication Pattern(s). Multiples instances covering different communication patterns may be present.
CIR-Flags (see 8.4.39)	CIR-Flags	O	If present, this Information Element shall contain a bit mask. See 8.4.39 for the meaning of the bits.
Enhanced Coverage Restriction (see 8.4.51)	Enhanced-Coverage-Restriction	O	If present, this Information Element shall contain the updates of the Enhanced Coverage Restriction.

Table 7.2.1.1-2: Configuration Information Answer

Information Element Name	Mapping to Diameter AVP	Cat	Description
Result (See 6.3)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [23]). Experimental-Result AVP shall be used for S6t errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. This AVP reflects the outcome of the procedure on Diameter level.
User Identity (see 6.4.2)	User-Identifier	C	This information element shall contain the User Identity of the UE. This is a grouped AVP containing an External Identifier or an MSISDN for a UE. This IE shall not be present if the External-Identifier of User-Identifier in CIR message contains the identity of a Group of UEs (i.e. External Group Identifier). This IE shall be present only when the Result-Code is DIAMETER_SUCCESS.
Supported Features (See 3GPP TS 29.229 [7])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Monitoring Event Report (see 8.4.3)	Monitoring-Event-Report	O	If an immediate report is available this information element shall contain the requested data available in the HSS.
AESE Communication Pattern Config Status (see 8.4.32)	AESE-Communication-Pattern-Config-Status	O	If present, this Information Element shall contain the details of Communication Pattern-Config-Status (s). Multiples instances covering different communication patterns configuration statuses may be present.
Monitoring Event-Config Status (see 8.4.24)	Monitoring-Event-Config-Status	O	If present, this information element shall contain the result of an individual Monitoring event request identified by its SCEF reference ID.
Supported Services (see 8.4.40)	Supported-Services	O	If present, this Information Element shall contain AVPs indicating details of the services supported by the HSS.
S6t-HSS Cause (see 8.4.50)	S6t-HSS-Cause	C	This information element shall contain an indication of Absent Subscriber. It shall be present if the user is not registered in any serving node.
Enhanced Coverage Restriction Data (see 8.4.52)	Enhanced-Coverage-Restriction-Data	C	This information element shall contain the result of a status query for Enhanced Coverage restriction control. It shall be present if the request contained a CIR-Flag AVP with the bit for Enhanced-Coverage-Query set.
CIA-Flags (see 8.4.60)	CIA-Flags	O	If present, this Information Element shall contain a bit mask. See 8.4.60 for the meaning of the bits.

7.2.1.2 Detailed Behaviour of the HSS

When the Configuration Information Request is received from the SCEF, the HSS shall, in the following order:

1. Check that the User Identity for whom data is asked exists in HSS. If not, Experimental-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Configuration Information Answer.

2. Check whether the requesting SCEF is authorized to request the specified service (e.g. presence of Monitoring Event Configuration AVP indicates the service). If not, Experimental-Result shall be set to DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY (5510) in the Configuration Information Answer.

3. Check that the requested service (e.g. Monitoring Event Configuration AVP) is authorized for the UE or the group of UEs. If not, Experimental-Result shall be set to DIAMETER_ERROR_UNAUTHORIZED_SERVICE (5511) in the Configuration Information Answer.

4. Check whether the limits on number of monitoring events that can be requested per monitoring type and SCEF-ID is reached. If so, Result-Code shall be set to DIAMETER_RESOURCES_EXCEEDED (5006).

5. When the request is for a group, i.e. because the External-Identifier AVP of the User-Identifier AVP contain an External Group Identifier, the HSS applies the Monitoring-Event-Configurtion AVP to each UE of the Group and includes the CIA-Flags AVP with the Group-Configuration-In-Progress bit set in the Configuration Information Answer. The Result-Code shall be set to DIAMETER_SUCCESS.

6. If a serving node is registered and is involved in the reporting of the configured monitoring event, the HSS shall forward the monitoring event configuration to the serving node and wait for the answer before sending the Configuration Information Answer to the SCEF. The monitoring event configuration status from the serving node for each event shall be conveyed by the HSS to the SCEF.

7. If the user is not registered in any serving node, the HSS shall answer successfully and stores the configuration data related to the service; also, it shall indicate to the SCEF that the user is absent, in the Configuration Information Answer, by setting the relevant bit in the S6t-HSS-Cause IE.

8. For Monitoring if the data related to an immediate reporting is available in the HSS, the HSS (e.g. as being received from the MME/SGSN in the Insert Subscriber Data answer) shall include this data in the Configuration Information Answer.

If the HSS is aware that the UE is registered in an MME and an SGSN and the services supported by the MME and SGSN are different, the HSS shall report the capabililities of the different nodes with Node-Type indication to the SCEF. If the capabilities are the same reported from the MME, the SGSN and the HSS, the HSS shall report the service capabilities without Node-Type to the SCEF. If the Supported-Services of the SGSN and MME were reported differently to the SCEF and the UE is purged in SGSN or MME the HSS shall report the Supported-Service to the SCEF excluding the Supported-Service from the purged node.

If the HSS receives CIR commad from SCEF and has forwarded it to an MME and an SGSN, the HSS check if the Result-Codes in Monitoring-Event-Config-Status AVPs reported by the MME and the SGSN are different

- the HSS includes Service-Report AVPs with Node-Type in the Monitoring-Event-Config-Status AVP to the SCEF in the CIA command;

- otherwise the HSS includes one Service-Report AVP without Node-Type in the Monitoring-Event-Config-Status AVP to the SCEF in the CIA command.

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

If the configuration data in the CIR command are out of the allowed range, the HSS shall set the Experimental-Result-Code to DIAMETER_ERROR_REQUESTED_RANGE_IS_NOT ALLOWED.

If the received SCEF Reference ID for Deletion does not exist, the HSS shall set the Experimental-Result-Code to DIAMETER_ERROR_CONFIGURATION_EVENT_NON_EXISTANT.

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

If the HSS cannot fulfil the received request for reasons not stated in the above steps (e.g. due to a database error), it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

If the HSS needs to report loss of connectivity it shall include the Monitoring-Type AVP set to "LOSS_OF_CONNECTIVITY" in the Monitoring Event Report. In addition the HSS may also include the Loss-Of-Connectivity-Reason AVP in the Monitoring Event Report.

If the SCEF indicates the support of Monitoring event feature to the HSS and the HSS supports Monitoring. The HSS shall include the Supported-Services AVP with the Supported-Monitoring-Events AVP in the CIA command.

If CIR message includes multiple SCEF Reference ID and for a SCEF Reference ID Monitoring events cannot be handled, the HSS shall report the failed SCEF-Reference-ID to the SCEF with an appropriate Experimental-Result-Code or Result-Code.

If a CIR message includes multiple SCEF Reference ID and for a SCEF Reference ID at least one CP parameter set cannot be handled, the HSS shall reply within the AESE-Communication-Pattern-Config-Status the failed SCEF Reference ID to the SCEF with an appropriate Experimental-Result-Code or Result-Code.

If an SCEF Reference ID received in a CIR command match with an SCEF Reference ID stored in the HSS and both SCEF Reference ID are provided by the same SCEF ID, the HSS shall delete the stored CP sets associated with the SCEF reference Id and store the new CP set(s).

If CIR message contains combinations of monitoring events and CP parameter set it shall handle each set belonging to an SCEF Reference ID separately and shall send a combined answer to the SCEF.

If the SCEF-Reference-ID-for-Deletion is present, the receiving node shall delete the corresponding monitoring event configuration, if stored.

If the SCEF-Reference-ID is present, the receiving node shall store the configuration event.

IF CIR message contains the CIR-Flags with delete all monitoring events, the HSS shall delete all Monitoring events configured by the SCEF for the subscriber. This includes forwarding the deletion to involved serving nodes.

If the CIR command contains the CIR-Flags AVP with the bit for Enhanced Coverage Query set, the HSS shall return the current settings of Enhanced Coverage together with the current Serving PLMN-ID (if any) in the CIA command.

If the CIR command contains Enhanced-Coverage-Restriction AVP, the HSS shall update the subscription data for Enhanced Coverage; the update shall be a complete replacement of any stored information with the received information. This may result in the need to update the MME/SGSN via S6a/d/MAP-Gr with the new value for access restriction; there is however no need for the HSS to delay sending of CIA until updates of serving nodes are confirmed.

7.2.1.3 Detailed Behaviour of the SCEF

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

When the SCEF receives an AESE-Communication-Pattern-Config-Status AVP from the HSS in a CIA command, it shall handle it according to the procedures defined in 3GPP TS 23.682 [2]. If the SCEF has included a number of CP pattern sets with several SCEF reference IDs in the request, it shall handle each AESE-Communication-Pattern-Config-Status AVP separately according to the procedures defined in 3GPP TS 23.682 [2].

If the SCEF receives a Supported-Services AVP it shall only trigger those services which are supported by the HSS and/or the MME/SGSN.

The SCEF shall store the Supported-Services received from the HSS and modify them, if the HSS reports change of capabililities.

NOTE: It depends on SCEF implementation, if the SCEF triggers only those services which are supported in both nodes when the UE is registered in both the MME and the SGSN.

When the SCEF needs to query the current settings of Enhanced Coverage Restriction, it shall send a CIR command to the HSS with the corresponding bit in the CIR-Flags AVP set, unless the SCEF knows that Enhanced Coverage Restriction Control is not supported by the HSS.

When the SCEF needs to update the current settings of Enhanced Coverage Restriction, it shall send a CIR command to the HSS with the new values for Enhanced Coverage Restriction within the Enhanced-Coverage-Restriction AVP.

The SCEF shall not query and update the current settings of Enhanced Coverage Restriction by means of a single CIR command.

7.2.2 Reporting on S6t

7.2.2.1 General

This procedure is used between the HSS and the SCEF.

When the procedure is invoked by the HSS, it is used for reporting:

- The change of association of the UE and UICC and/or new IMSI-IMEI-SV;
- The UE reachability for SMS;
- The Roaming status (Roaming or No Roaming) of the UE, and change in roaming status of the UE.

It is also used:

- To update the SCEF with the suspend/resume/cancel status of an ongoing monitoring.
- To convey reports and/or status indications for all or some UEs belonging to a group.

This procedure is mapped to the commands Reporting-Information-Request/Answer in the Diameter application specified in clause 8. The tables 7.2.2.1-1 and 7.2.2.1-2 detail the involved information elements.

Table 7.2.2.1-1: Reporting Information Request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User Identity (see 8.4.36)	User-Identifier	C	This information element shall contain the User Identity of the UE. This is a grouped AVP containing an External Identifier and/or an MSISDN. This AVP shall not carry the IMSI towards the SCEF. For group based configuration processing, the External-Identifier shall contain an External Group Identifier (see 3GPP TS 23.003 [11]).
Supported Features (See 3GPP TS 29.229 [7])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Monitoring Event Report (see 8.4.3)	Monitoring-Event-Report	O	If a report is available in the HSS this information element shall contain the requested data available in the HSS.
Group-Monitoring Event Report (see 8.4.61)	Group-Monitoring-Event-Report	C	If present, this information element shall contain reports and/or status indications for all UEs or a subset of UEs belonging to a group. Shall be present if User-Identifier contains an External Group Identifier
RIR-Flags (see 8.4.63)	RIR-Flags	O	If present, this Information Element shall contain a bit mask. See 8.4.63 for the meaning of the bits.
Supported Services (see 8.4.40)	Supported-Services	O	If present, this Information Element shall contain AVPs indicating details of the services supported by the HSS.

Table 7.2.2.1-2: Reporting Information Answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result (See 6.3)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [23]). Experimental-Result AVP shall be used for S6t errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [7])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

7.2.2.2 Detailed Behaviour of the HSS

For group based configuration processing, if the Group Guard Timer was included in the CIR command, the HSS shall send the RIR command before the Group Guard Timer expires and shall include several reports and/or status indications in one or more Group-Monitoring Event Report AVPs.

NOTE: The HSS may divide the accumulated Monitoring Configuration Indications/immediate reports into multiple messages.

The HSS shall send immediate reports and configuration indications for group based configuration processing using the Group-Monitoring-Event-Report.

If the HSS knows that it has additional RIR commands to send for the same group, the HSS shall include the RIR-Flags AVP with the Group-Configuration-In-Progress bit set and restart the Group Guard Timer to the value it originally received in the CIR.

For group based configuration processing, if the MME/SGSN previously indicated that it does not support the External-Identifier in the ULR command and the UE does not have an MSISDN configured as part of its subscription data, the HSS shall indicate that the UE is absent by setting the relevant bit in the S6t-HSS-Cause IE of the Group-Monitoring Event Report-Item AVP.If UE Reachability is reported, a Maximum-UE-Availability-Time AVP may also be present in the report.

If the HSS detects that the serving node does not support or does not activate a Monitoring event, or if the UE is part of a group and requires the External-Identifier to be supported by the serving node when it does not, it shall send to the SCEF, an RIR command with the Event-Handling AVP with the value SUSPEND.

If an HSS detects that in the new serving node an event to be activated is supported which was not supported in the old serving node or if the HSS detects that the new serving node supports the External-Identifier for a UE that is part of a group and requires the External-Identifier which was not supported in the old serving node, it shall send an RIR command with the Event-handling AVP with the value RESUME to the SCEF.

If the HSS receives a Notify Request from the MME/SGSN to inform the Monitoring-Event-Config-Status at the IWK-SCEF, the HSS shall send an RIR command to the SCEF, for the monitoring event configurations not accepted by the IWK-SCEF, with the Event-Handling AVP set to the value CANCEL.

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

If the Supported-Services of the SGSN and MME have been previously reported to the SCEF, an the HSS detects that they have changed from a previous report, the HSS shall report all the Supported-Service to the SCEF.

When a subscriber is barred/un-barred for services relevant to an active monitoring, the HSS shall send an RIR command to the SCEF with the Event-Handling AVP set to the value SUSPEND/RESUME.

When a subscriber is deleted from the HSS while monitoring is active or the authorization for monitoring is revoked, the HSS shall send an RIR command to the SCEF with the Event-Handling AVP set to the value CANCEL.

7.2.2.3 Detailed Behaviour of the SCEF

When the SCEF receives a Monitoring Event Report AVP from the HSS with an SCEF-Reference-ID not known by the SCEF, it shall reply with DIAMETER_ERROR_SCEF_REFERENCE_ID_UNKNOWN see 3GPP TS 23.007 [19].

Otherwise when the SCEF receives a Reporting Information Request from the HSS, the SCEF shall set Experimental-Result to DIAMETER_SUCCESS in the Reporting Information Answer and shall handle it according to the procedures defined in 3GPP TS 23.682 [2].

If the SCEF receives RIR command with the Event-Handling AVP set to SUSPEND it shall either notify the SCS/AS that the event is not active or initiate deletion of the event depending on operator configuration.

If the SCEF receives an RIR command with the Event-Handling AVP set to CANCEL it shall delete the event.

Editor's Note: The usage of Retry-After timer is FFS.

If the SCEF receives RIR command with the Event-Handling AVP set to RESUME it shall notify the SCS/AS that the event is activated in serving node.

If the SCEF receives a Reporting Information Request from the HSS with the Monitoring-Type AVP set to LOSS_OF_CONNECTIVITY, it shall interpret this as the reporting of loss of connectivity of the UE.

On receiving Monitoring event reports, the SCEF shall check whether the number of reports for this Monitoring event type reaches the configured maximum number of reports. When the reports reach the configured maximum number, the SCEF shall send CIR message to the HSS to delete the corresponding Monitoring Event Configuration, with the SCEF-Reference-ID-for-Deletion AVP set to the related SCEF Reference ID.

If the HSS reports change of Supported-Services, the SCEF shall replace the stored Supported-Service by the received ones.

If the SCEF receives the RIR command with the Group-Configuration-In-Progress bit of the RIR-Flags AVP set, the SCEF shall restart the associated Group Reporting Guard Timer.

NOTE: The SCEF needs to be prepared to receive RIR for Group based configuration processing before the Group Reporting Group Timer expires.

7.2.3 NIDD Information on S6t

7.2.3.1 General

This procedure is used between the SCEF and the HSS for:

- the authorization of the UE for NIDD.

This procedure is used between the HSS and the SCEF for:

- the update/revocation of a UE’s authorization for NIDD.

This procedure is mapped to the commands NIDD-Information-Request/Answer in the Diameter application specified in clause 8. The tables 7.2.3.1-1 and 7.2.3.1-2 detail the involved information elements.

Table 7.2.3.1-1: NIDD Information Request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User Identity (see 8.4.36)	User-Identifier	M	This Information Element shall contain the identity of the UE. This is a grouped AVP containing either an IMSI, External Identifier or an MSISDN (exactly one, and only one, of those identifiers shall be included in the request).
Supported Features (See 3GPP TS 29.229 [7])	Supported-Features	O	If present, this Information Element shall contain the list of features supported by the origin host.
NIDD Authorization Request (see 8.4.44)	NIDD-Authorization-Request	O	If present, this Information Element shall contain the details of Authorization for NIDD. Shall be absent when sent by the HSS.
NIDD Authorization Update (see 8.4.57)	NIDD-Authorization-Update	O	If present, this Information Element shall contain the details of the updated NIDD Authorization. Shall be absent when sent by the SCEF.

Table 7.2.3.1-2: NIDD Information Answer

Information Element Name	Mapping to Diameter AVP	Cat	Description
Result (See 6.3)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [23]). Experimental-Result AVP shall be used for S6t errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. This AVP reflects the outcome of the procedure on Diameter level.
Supported Features (See 3GPP TS 29.229 [7])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
NIDD-Authorization-Response (see 8.4.45)	NIDD-Authorization-Response	C	If present, this Information Element shall contain the details of NIDD Authorization. When sent by the HSS the IE shall only be present when the Result Code is DIAMETER_SUCCESS. Shall be absent when sent by the SCEF.

7.2.3.2 Detailed Behaviour of the HSS

When the NIDD Information Request is received from the SCEF, the HSS shall, in the following order:

1. Check that the User Identity for whom data is asked exists in HSS. If not, Experimental-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN in the NIDD Information Answer.

2. Check that the requested service is authorized for the UE. If not, Experimental-Result shall be set to DIAMETER_ERROR_UNAUTHORIZED_SERVICE (5511) in the NIDD Information Answer.

3. Check that the APN sent in the Service-Selection AVP of the NIDD-Authorization-Request AVP is subscribed for the subscriber identified by the given MSISDN or the External Identifier. If it is not subscribed, then the Experimental-Result shall be set to DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION (5451) in the NIDD Information Answer.

4. If the User-Identifier contains an External Identifier, the HSS shall include the IMSI and if available the MSISDN associated with the appropriate External Identifier in the NIDD-Authorization-Response.

5. If the User-Identifier contains an MSISDN, the HSS shall include the IMSI and if available, the appropriate External Identifier associated with the MSISDN in the NIDD-Authorization-Response.

6 If the User-Identifier contains an IMSI the HSS shall include the MSISDN and the appropriate External Identifier assigned to the IMSI in the NIDD-Authorization-Response.

7 If the requested service is NIDD Authorization request and the feature "NIDD Authorization Update" is commonly supported by HSS and SCEF, the HSS shall store the granted NIDD Authorization in order to being able to update/revoke the Authorization towards the SCEF when so needed. The HSS may indicate within the NIDD-Authorization-Response AVP a granted validity time which shall not be later than the requested validity time as received within the NIDD-Authorization-Request AVP (if any). If so the HSS shall delete the stored Authorization at the indicated point in time.

NOTE 1: If several External Identifiers are mapped to one IMSI, some functions might not work in this release of the specification.

NOTE 2: Step 6 above is applicable for the case where the SCEF receives a T6a/b-CMR command while a valid NIDD configuration does not exist for the UE at the SCEF.

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

If the HSS cannot fulfil the received request for reasons not stated in the above steps (e.g. due to a database error), it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY. Otherwise the Result-Code shall be set to DIAMETER_SUCCESS.

When the need to update/revoke one or several stored granted NIDD Authorizations for a user is detected in the HSS, and the feature "NIDD Authorization Update" is commonly supported by the HSS and the SCEF, the HSS shall issue an NIDD-Information Request command containing a NIDD-Authorization-Update AVP towards the SCEF. The NIDD-Authorization-Update AVP may identify several granted NIDD Authorizations for the user to be updated.

7.2.3.3 Detailed Behaviour of the SCEF

When the SCEF receives an NIDD-Authorization-Response AVP from the HSS in a NIA command, it shall handle it according to the procedures defined in 3GPP TS 23.682 [2]. If the feature "NIDD Authorization Update" is commonly supported by the HSS and the SCEF, and a granted validity time was received within the NIDD-Authorization-Response, the SCEF shall consider the authorization being implicitly revoked at the indicated time, and may issue a new NIDD Authorization request towards the HSS.

8 Protocol Specification for S6t

8.1 Introduction

8.1.1 Use of Diameter Base Protocol

The Diameter base protocol as specified in IETF RFC 6733 [23] 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.

8.1.2 Securing Diameter Messages

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

8.1.3 Accounting Functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) shall not be used on the S6t interface.

8.1.4 Use of 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 6733 [23]. 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.

8.1.5 Transport Protocol

Diameter messages over the S6t interface shall make use of SCTP IETF RFC 4960 [5] as transport protocol.

8.1.6 Routing Considerations

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

If the SCEF knows the address/name of the HSS for a certain user, both the Destination-Realm AVP and the Destination-Host AVP shall be present in the request. Otherwise, only the Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node. Consequently, the Destination-Host AVP is declared as optional in the ABNF for all requests initiated by the SCEF.

As the HSS knows the address/name and the associated home network domain name of the SCEF to which it sends RIR and NIR commands from a previously received CIR command, both the Destination-Realm and Destination-Host AVPs shall be present in request commands sent by the HSS to the SCEF.

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

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

8.1.7 Advertising Application Support

The HSS and the SCEF shall advertise support of the Diameter S6t 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 IETF RFC 6733 [23].

8.1.8 Diameter Application Identifier

The S6t 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 S6t interface application is 16777345 (allocated by IANA).

8.1.9 Use of the Supported-Features AVP

When new functionality is introduced on the S6t application, it should be defined as optional. If backwards incompatible changes cannot be avoided, the new functionality shall be introduced as a new feature and support

advertised with the Supported-Features AVP. The usage of the Supported-Features AVP on the S6t application is consistent with the procedures for the dynamic discovery of supported features as defined in clause 7.2 of 3GPP TS 29.229 [7].

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

As defined in 3GPP TS 29.229 [7], the Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the all reference points as specified in this specification, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, for features defined in this document, the Vendor-Id AVP shall contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the reference point, the Feature-List-ID AVP shall differentiate those lists from one another.

8.1.10 User Identity to HSS resolution

The User identity to HSS resolution mechanism enables the SCEF to find the identity of the HSS that holds the subscription data for the target user when multiple and separately addressable HSSs have been deployed in the home network. The resolution mechanism is not required in networks that utilise a single HSS.

This User identity to HSS resolution mechanism may rely on routing capabilities provided by Diameter and be implemented in the home operator network within dedicated Diameter Agents (Redirect Agents or Proxy Agents) responsible for determining the HSS identity based on the provided user identity (e.g. external identifiers provided by the SCEF).

When the Diameter Load Control mechanism is supported (see IETF draft-ietf-dime-load-03 [22]), load values from previously received Load AVPs of type HOST may be taken into account when determining the HSS identity.

NOTE: Alternatives to the user identity to HSS resolution Diameter based implementation are outside the scope of this specification.

8.2 Commands

8.2.1 Introduction

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

8.2.2 Command-Code values

This section defines Command-Code values for the S6t interface application as allocated by IANA.

Every command is defined by means of the ABNF syntax IETF RFC 5234 [9], according to the Command Code Format (CCF) specification defined in IETF RFC 6733 [23]. When the definition and use of an AVP is not specified in this document, the guidelines in IETF RFC 6733 [23] shall apply.

The Vendor-Specific-Application-Id AVP shall not be included in any command sent by Diameter nodes supporting applications defined in this specification. If the Vendor-Specific-Application-Id AVP is received in any of the commands defined in this specification, it shall be ignored by the receiving node.

NOTE: The Vendor-Specific-Application-Id is included as an optional AVP in all Command Code Format specifications defined in this specification in order to overcome potential interoperability issues with intermediate Diameter agents non-compliant with the IETF RFC 6733 [23].

The following Command Codes are defined in this specification for S6t:

Table 8.2.2-1: Command-Code values for S6t

Command-Name	Abbreviation	Code	Section
Configuration-Information-Request	CIR	8388718	8.2.3
Configuration-Information-Answer	CIA	8388718	8.2.4
Reporting-Information-Request	RIR	8388719	8.2.5
Reporting-Information-Answer	RIA	8388719	8.2.6
NIDD-Information-Request	NIR	8388726	8.2.7
NIDD-Information-Answer	NIA	8388726	8.2.8

For these commands, the Application-ID field shall be set to 16777345 (application identifier of the S6t interface application, allocated by IANA).

8.2.3 Configuration Information Request (CIR) Command

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

Message Format:

```
< Configuration-Information-Request > ::=   < Diameter Header: 8388718, REQ, PXY, 16777345 >
                                            < Session-Id >
                                            [ DRMP ]
                                            { Auth-Session-State }
                                            { Origin-Host }
                                            { Origin-Realm }
                                            [ Destination-Host ]
                                            { Destination-Realm }
                                            { User-Identifier }
                                            [ OC-Supported-Features ]
                                            *[ Supported-Features ]
                                            *[ Monitoring-Event-Configuration ]
                                            [ CIR-Flags ]
                                            *[ AESE-Communication-Pattern ]
                                            [ Enhanced-Coverage-Restriction ]
                                            [ Group-Reporting-Guard-Timer ]
                                            *[ Proxy-Info ]
                                            *[ Route-Record ]
                                            *[AVP]
```

8.2.4 Configuration-Information-Answer (CIA) Command

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

Message Format:

```
< Configuration-Information-Answer > ::=    < Diameter Header: 8388718, PXY, 16777345 >
                                            < Session-Id >
                                            [ DRMP ]
                                            [ Result-Code ]
                                            [ Experimental-Result ]
                                            { Auth-Session-State }
                                            { Origin-Host }
                                            { Origin-Realm }
                                            [ OC-Supported-Features ]
                                            [ OC-OLR ]
                                            *[ Load ]
                                            *[ Supported-Features ]
                                            [ User-Identifier ]
                                            *[ Monitoring-Event-Report ]
```

*[Monitoring-Event-Config-Status]
*[AESE-Communication-Pattern-Config-Status]
*[Supported-Services]
[S6t-HSS-Cause]
[Enhanced-Coverage-Restriction-Data]
[CIA-Flags]
[Failed-AVP]
*[Proxy-Info]
*[Route-Record]
*[AVP]

8.2.5 Reporting-Information-Request (RIR) Command

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

Message Format:

< Reporting-Information-Request > ::= < Diameter Header: 8388719, PXY, 16777345 >
< Session-Id >
[DRMP]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
*[Supported-Features]
[User-Identifier]
*[Monitoring-Event-Report]
*[Group-Monitoring-Event-Report]
[RIR-Flags]
*[Supported-Services]
*[Proxy-Info]
*[Route-Record]
*[AVP]

8.2.6 Reporting-Information-Answer (RIA) Command

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

Message Format:

< Reporting-Information-Answer > ::=< Diameter Header: 8388719, PXY, 16777345 >
< Session-Id >
[DRMP]
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[Supported-Features]
[Failed-AVP]
*[Proxy-Info]
*[Route-Record]
*[AVP]

8.2.7 NIDD Information Request (NIR) Command

The NIDD Information Request (NIR) command, indicated by the Command-Code field set to 8388726 and the "R" bit set in the Command Flags field, is sent from the SCEF to the HSS. It may also be sent from the HSS to the SCEF when the feature "NIDD Authorization Update" is commonly supported by the HSS and the SCEF.

Message Format:

```
< NIDD-Information-Request > ::=< Diameter Header: 8388726, REQ, PXY, 16777345 >
                                < Session-Id >
                                [ DRMP ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                { User-Identifier }
                                [ OC-Supported-Features ]
                                *[ Supported-Features ]
                                [ NIDD-Authorization-Request ]
                                [ NIDD-Authorization-Update ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
                                *[AVP]
```

8.2.8 NIDD-Information-Answer (NIA) Command

The NIDD-Information-Answer (NIA) command, indicated by the Command-Code field set to 8388726 and the "R" bit cleared in the Command Flags field, is sent from the HSS to the SCEF. It may also be sent from the SCEF to the HSS when the feature "NIDD Authorization Update" is commonly supported by the HSS and the SCEF.

Message Format:

```
< NIDD-Information-Answer > ::= < Diameter Header: 8388726, PXY, 16777345 >
                                < Session-Id >
                                [ DRMP ]
                                [ Result-Code ]
                                [ Experimental-Result ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ OC-Supported-Features ]
                                [ OC-OLR ]
                                *[ Load ]
                                *[ Supported-Features ]
                                [ NIDD-Authorization-Response ]
                                [ Failed-AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
                                *[AVP]
```

8.3 Result-Code AVP and Experimental-Result AVP Values

8.3.1 General

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

8.3.2 Success

Result codes that fall within the Success category shall be used to inform a peer that a request has been successfully completed. The Result-Code AVP values defined in Diameter base protocol specified in IETF RFC 6733 [23] shall be applied.

8.3.3 Permanent Failures

Errors that fall within the Permanent Failures category shall be used to inform the peer that the request has failed, and should not be attempted again. The Result-Code AVP values defined in Diameter base protocol specified in IETF RFC 6733 [23] 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.

8.3.3.1 DIAMETER_ERROR_USER_UNKNOWN (5001)

This result code shall be sent by the HSS to indicate that the user identified by the IMSI, MSISDN, or External-Identifier is unknown. This error code is defined in 3GPP TS 29.229 [7].

8.3.3.2 DIAMETER_ERROR_UNAUTHORIZED_REQUESTING_ENTITY (5510)

This result code shall be sent by the HSS to indicate that the SCEF is not allowed to request the service.

8.3.3.3 DIAMETER_ERROR_UNAUTHORIZED_SERVICE (5511)

This result code shall be sent by the HSS to indicate that the specific service requested by the SCEF is not allowed for an UE, or that it cannot be delivered according to the current subscribed services of the UE.

8.3.3.4 DIAMETER_ERROR_REQUESTED_RANGE_IS_NOT ALLOWED (5512)

This result code shall be sent by the HSS to indicate that the specific service requested by the SCEF is not allowed for an UE, or that it cannot be delivered according to the current subscribed services of the UE.

8.3.3.5 DIAMETER_ERROR_CONFIGURATION_EVENT_STORAGE_NOT_ SUCCESSFUL (5513)

This result code shall be sent by the HSS to indicate that the specific service requested by the SCEF could not be stored for an UE.

8.3.3.6 DIAMETER_ERROR_CONFIGURATION_EVENT_NON_EXISTANT (5514)

This result code shall be sent by the HSS to indicate that the requested deletion by the SCEF could not be performed for an UE because the event does not exist.

8.3.3.7 DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION (5451)

This result code shall be sent by the HSS to indicate that the APN is not authorized for an UE.

8.4 AVPs

8.4.1 General

The following table specifies the Diameter AVPs defined for the S6t 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).

For all AVPs which contain bit masks and are of the type Unsigned32, bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x00000001 should be used.

Table 8.4.1-1: S6t specific Diameter AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
AESE-Communication-Pattern	3113	8.4.25	Grouped	M,V				No
Communication-Pattern-Set	3114	8.4.26	Grouped	M,V				No
Periodic-Communication-Indicator	3115	8.4.27	Unsigned32	M,V				No
Communication-Duration-Time	3116	8.4.28	Unsigned32	M,V				No
Periodic-time	3117	8.4.29	Unsigned32	M,V				No
Scheduled-Communication-Time	3118	8.4.30	Grouped	M,V				No
Stationary-Indication	3119	8.4.31	Unsigned32	M,V				No
AESE-Communication-Pattern-Config-Status	3120	8.4.32	Grouped	M,V				No
AESE-Error-Report	3121	8.4.33	Grouped	M,V				No
Monitoring-Event-Configuration	3122	8.4.2	Grouped	M,V				No
Monitoring-Event-Report	3123	8.4.3	Grouped	M,V				No
SCEF-Reference-ID	3124	8.4.4	Unsigned32	M,V				No
SCEF-ID	3125	8.4.5	DiameterIdentity	M,V				No
SCEF-Reference-ID-for-Deletion	3126	8.4.6	Unsigned32	M,V				No
Monitoring-Type	3127	8.4.7	Unsigned32	M,V				No
Maximum-Number-of-Reports	3128	8.4.8	Unsigned32	M,V				No
UE-Reachability-Configuration	3129	8.4.9	Grouped	M,V				No
Monitoring-Duration	3130	8.4.10	Time	M,V				No
Maximum-Detection-Time	3131	8.4.11	Unsigned32	M,V				No
Reachability-Type	3132	8.4.12	Unsigned32	M,V				No
Maximum Latency	3133	8.4.13	Unsigned32	M,V				No
Maximum Response Time	3134	8.4.14	Unsigned32	M,V				No
Location-Information-Configuration	3135	8.4.15	Grouped	M,V				No
MONTE-Location-Type	3136	8.4.16	Unsigned32	M,V				No
Accuracy	3137	8.4.17	Unsigned32	M,V				No
Association-Type	3138	8.4.18	Unsigned32	M,V				No
Roaming-Information	3139	8.4.19	Unsigned32	M,V				No
Reachability-Information	3140	8.4.20	Unsigned32	M,V				No
IMEI-Change	3141	8.4.22	Unsigned32	M,V				No
Monitoring-Event-Config-Status	3142	8.4.24	Grouped	M,V				No
Supported-Services	3143	8.4.40	Grouped	M,V				No
Supported-Monitoring-Events	3144	8.4.41	Unsigned64	M,V				No
CIR-Flags	3145	8.4.39	Unsigned32	M,V				No
Service-Result	3146	8.4.37	Grouped	M,V				No
Service-Result-Code	3147	8.4.38	Unsigned32	M,V				No
Reference-ID-Validity-Time	3148	8.4.42	Time	M,V				No
Event-Handling	3149	8.4.43	Unsigned32	M,V				No
NIDD-Authorization-Request	3150	8.4.44	Grouped	M,V				No
NIDD-Authorization-Response	3151	8.4.45	Grouped	M,V				No
Service-Report	3152	8.4.47	Grouped	M,V				No
Node-Type	3153	8.4.48	Unsigned32	M,V				No
S6t-HSS-Cause	3154	8.4.50	Unsigned32	M,V				No
Enhanced-Coverage-Restriction	3155	8.4.51	Grouped	V			M	No
Enhanced-Coverage-Restriction-Data	3156	8.4.52	Grouped	V			M	No
Restricted-PLMN-List	3157	8.4.53	Grouped	V			M	No
Allowed-PLMN-List	3158	8.4.54	Grouped	V			M	No
Requested-Validity-Time	3159	8.4.55	Time	V			M	No
Granted-Validity-Time	3160	8.4.56	Time	V			M	No
NIDD-Authorization-Update	3161	8.4.57	Grouped	V			M	No
Loss-Of-Connectivity-Reason	3162	8.4.58	Unsigned32	V			M	No

Group-Reporting-Guard-Timer	3163	8.4.59	Unsigned32	V			M	No
CIA-Flags	3164	8.4.60	Unsigned32	V			M	No
Group-Monitoring-Event-Report	3165	8.4.61	Grouped	V			M	No
Group-Monitoring-Event-Report-Item	3166	8.4.62	Grouped	V			M	No
RIR-Flags	3167	8.4.63	Unsigned32	V			M	No
Type-Of-External-Identifier	3168	8.4.64	Unsigned32	V			M	No
APN-Validity-Time	3169	8.4.65	Grouped	V			M	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 6733 [23]. NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.								

The following table specifies the Diameter AVPs re-used by the S6t interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within S6t.

Any other AVPs from existing Diameter Applications, except for the AVPs from Diameter base protocol specified in IETF RFC 6733 [23], do not need to be supported. The AVPs from Diameter base protocol specified in IETF RFC 6733 [23] are not included in table 8.4.1-2, but they may be re-used for the S6t protocol.

Table 8.4.1-2: S6t re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
User-Identifier	6.4.2	see 8.4.36	
External-Identifier	6.4.11		
MSISDN	3GPP TS 29.329 [10]		
User-Name	IETF RFC 6733 [23]	This AVP shall contain the IMSI of the UE	
Supported-Features	3GPP TS 29.229 [7]	see 8.4.23	
Feature-List-ID	3GPP TS 29.229 [7]		
Feature-List	3GPP TS 29.229 [7]		
OC-Supported-Features	IETF RFC 7683 [15]	See 6.4.16	Must not set
OC-OLR	IETF RFC 7683 [15]	See 6.4.17	Must not set
Visited PLMN Id	3GPP TS 29.272 [14]		
Charged-Party	3GPP TS 32.299 [16]		
EPS-Location-Information	3GPP TS 29.272 [14]	see 8.4.21	
MME-Location-Information	3GPP TS 29.272 [14]	see 8.4.34	
SGSN-Location-Information	3GPP TS 29.272 [14]	see 8.4.35	
E-UTRAN-Cell-Global-Identity	3GPP TS 29.272 [14]		
Tracking-Area-Identity	3GPP TS 29.272 [14]		
Geographical-Information	3GPP TS 29.272 [14]		
Geodetic-Information	3GPP TS 29.272 [14]		
Current-Location-Retrieved	3GPP TS 29.272 [14]		
Age-Of-Location-Information	3GPP TS 29.272 [14]		
User-CSG-Information	3GPP TS 29.272 [14]		
Cell-Global-Identity	3GPP TS 29.272 [14]		
Service-Area-Identity	3GPP TS 29.272 [14]		
Routing-Area-Identity	3GPP TS 29.272 [14]		
eNodeB-ID	3GPP TS 29.217 [17]		
Day-Of-Week-Mask	IETF RFC 5777 [18]		
Time-Of-Day-Start	IETF RFC 5777 [18]		
Time-Of-Day-End	IETF RFC 5777 [18]		
DRMP	IETF RFC 7944 [20]	see 8.4.46	Must not set
Service-Selection	IETF RFC 5778 [21]	See 8.4.49	
Load	IETF draft-ietf-dime-load-03 [22]	See 6.4.20	Must not set
DL-Buffering-Suggested-Packet-Count	3GPP TS 29.272 [14]		
Extended-eNodeB-ID	3GPP TS 29.217 [17]		Must not set
Maximum-UE-Availability-Time	3GPP TS 29.338 [12]		

8.4.2 Monitoring-Event-Configuration

The Monitoring-Event-Configuration AVP is of type Grouped, and it contains the details of the monitoring event from the SCEF. At least SCEF-Reference-ID or one SCEF-Reference-ID-for-Deletion shall be present.

AVP format:

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

[SCEF-Reference-ID]

{ SCEF-ID }

{ Monitoring-Type }

*[SCEF-Reference-ID-for-Deletion]

[Maximum-Number-of-Reports]

[Monitoring-Duration]

[Charged-Party]

[Maximum-Detection-Time]

[UE-Reachability-Configuration]

[Location-Information-Configuration]

[Association-Type]

[DL-Buffering-Suggested-Packet-Count]

*[AVP]

At least one of the SCEF-Reference-ID or SCEF-Reference–ID-for-Deletion shall be present.

8.4.3 Monitoring-Event-Report

The Monitoring-Event-Report AVP is of type Grouped, and it contains the information to be reported as requested by Monitoring-Event-Configuration.

AVP format:

Monitoring-Event-Report::= <AVP header: 3123 10415>

{ SCEF-Reference-ID }

[SCEF-ID]

[Visited-PLMN-Id]

[Roaming-Information]

[IMEI-Change]

[Reachability-Information]

[Maximum-UE-Availability-Time]

[EPS-Location-Information]

[Monitoring-Type]

[Event-Handling]

*[Service-Report]

[Loss-Of-Connectivity-Reason]

*[AVP]

8.4.4 SCEF-Reference-ID

The SCEF-Reference-ID AVP is of type Unsigned32 and it shall contain the identifier provided by the SCEF.

8.4.5 SCEF-ID

The SCEF- ID AVP is of type DiameterIdentity and it shall contain the identity of the SCEF which has originated the service request towards the HSS.

8.4.6 SCEF-Reference-ID-for-Deletion

The SCEF-Reference-ID-for-Deletion AVP is of type Unsigned32 and it shall contain the SCEF-Reference-ID (in combination with the SCEF identified by the SCEF-ID) for the event to be deleted.

8.4.7 Monitoring-Type

The Monitoring-Type AVP is of type Unsigned32 and shall identify the type of event to be monitored. The following values are defined:

LOSS_OF_CONNECTIVITY (0)

UE_REACHABILITY (1)

LOCATION_REPORTING (2)

CHANGE_OF_IMSI_IMEI(SV)_ASSOCIATION (3)

ROAMING_STATUS (4)

COMMUNICATION_FAILURE (5)

AVAILABILITY_AFTER_DDN_FAILURE (6)

NUMBER_OF_UES_PRESENT_IN_A_GEOGRAPHICAL_AREA (7)

8.4.8 Maximum-Number-of-Reports

The Maximum-Number-of-Reports AVP is of type Unsigned32. It shall contain the number of reports to be generated and sent to the SCEF.

8.4.9 UE-Reachability-Configuration

The UE-Reachability-Configuration AVP is of type Grouped, and it shall contain the details for configuration for UE reachability.

AVP format:

```
UE-Reachability-Configuration::= <AVP header: 3129 10415>
                                 [ Reachability-Type ]
                                 [ Maximum-Latency ]
                                 [ Maximum-Response-Time ]
                                 *[AVP]
```

8.4.10 Monitoring-Duration

The Monitoring-Duration AVP is of typeTime. It shall contain the absolute time at which the related monitoring event request is considered to expire.

8.4.11 Maximum-Detection-Time

The Maximum-Detection-Time AVP is of type Unsigned32. It shall contain the maximum number of seconds without any communication with the UE after which the SCEF is to be informed that the UE is considered to be unreachable.

8.4.12 Reachability-Type

The Reachability-Type AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.4.12-1:

Table 8.4.12-1: Reachability-Type

Bit	Name	Description
0	Reachability for SMS	This bit, when set, indicates that the monitoring for reachability for SMS of the UE is to be configured
1	Reachability for Data	This bit, when set, indicates that the monitoring for reachability for data of the UE is to be configured
NOTE 1: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command. NOTE 2: Bits 0 and 1 shall not both be set simultaneously.		

8.4.13 Maximum-Latency

The Maximum-Latency AVP is of type Unsigned32. It shall contain the maximum acceptable delay time for downlink data transfer in seconds.

8.4.14 Maximum-Response-Time

The Maximum-Response-Time AVP is of type Unsigned32. It shall contain the maximum time in seconds for which the UE stays reachable.

8.4.15 Location-Information-Configuration

The Location-Information-Configuration AVP is of type Grouped, and it contains the details for location reporting.

AVP format:

Location-Information-Configuration::= <AVP header: 3135 10415>

[MONTE-Location-Type]

[Accuracy]

*[AVP]

8.4.16 MONTE-Location-Type

The MONTE-Location-Type AVP is of type Unsigned32. It indicates actually of the location information to be provided. The following values are defined:

CURRENT_LOCATION (0)

LAST_KNOWN_LOCATION (1)

8.4.17 Accuracy

The Accuracy AVP is of type Unsigned32. It shall indicate the requested accuracy. The following values are defined:

CGI-ECGI (0)

eNB (1)

LA-TA-RA (2)

PRA(3)

8.4.18 Association-Type

The Association-Type AVP is of type Unsigned32. It shall indicate the details of the reporting related to the IMEI-IMSI association. The following values are defined:

IMEI-CHANGE (0)

IMEISV-CHANGE (1)

8.4.19 Roaming-Information

The Roaming-Information AVP is of type Unsigned32. It shall indicate the roaming status of the subscriber. The following values are defined:

SUBSCRIBER_ROAMING (0)

SUBSCRIBER_NOT_ROAMING (1)

8.4.20 Reachability-Information

The Reachability-Information AVP is of type Unsigned32. It shall indicate the reachability of the subscriber. The following values are defined:

REACHABLE_FOR_SMS (0)

REACHABLE_FOR_DATA (1)

8.4.21 EPS-Location-Information

The EPS-Location-Information AVP is of type Grouped. It shall contain the information related to the user location relevant for EPS. It was originally defined in 3GPP TS 29.272 [49].

AVP format:

EPS-Location-Information ::= <AVP header: 1496 10415>

[MME-Location-Information]

[SGSN-Location-Information]

*[AVP]

8.4.22 IMEI-Change

The IMEI-Change AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.4.22-1:

Table 8.4.22-1: IMEI-Change

Bit	Name	Description
0	IMEI	This bit, when set, indicates that the IMEI has changed
1	IMEISV	This bit, when set, indicates that only the IMEI software version has changed but the IMEI has not changed.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

8.4.23 Feature-List AVP

8.4.23.1 Feature-List AVP for the S6t application

The syntax of this AVP is defined in 3GPP TS 29.229 [7].

For the S6t application, the meaning of the bits shall be as defined in table 8.4.23-1 for the Feature-List-ID.

Table 8.4.23-1: Features of Feature-List-ID used in S6t

Feature bit	Feature	M/O	Description
0	MONTE	O	Configuration and reporting of monitoring events This feature is applicable to from an SCEF with CIR/CIA command pair and the reporting of events to the SCEF with RIR/RIA command pair. If the HSS does not support this feature, the SCEF shall not send monitoring event configurations to the HSS within CIR.
1	AESE-Communication-Pattern	O	Configuration of CP parameter sets This feature is applicable to from an SCEF with CIR/CIA command pair. If the HSS does not support this feature, the SCEF shall not send CP parameter set to the HSS within CIR.
2	NIDD-Authorization	O	Authorization of NIDD This feature is applicable to from an SCEF with NIR/NIA command pair. If the HSS indicates in the NIA command that it does not support Authorization of NIDD, the SCEF shall not send NIDD Authorizations requests to the HSS in subsequent NIR commands towards that HSS.
3	Enhanced-Coverage-Restriction-Control	O	Control Of Enhanced Coverage Restriction This feature is applicable for the CIR/CIA command pair. If the SCEF detects that the HSS does not support this feature, it may refrain from sending further CIR commands containing an Enhanced-Coverage-Restriction AVP or a CIR-Flags AVP with the bit for Enhanced-Coverage-Query set.
4	NIDD Authorization Update	O	Update/Revocation of NIDD Authorization This feature is applicable for the NIR/NIA command pair. It shall not be supported when NIDD-Authorization is not supported. If the SCEF indicates in the NIR command that it does not support NIDD Authorization Update, the HSS shall not send subsequent NIR commands to update or revoke a granted NIDD Authorization. The HSS may decide not to grant NIDD Authorization when Update/Revocation is not supported by the SCEF.

Feature bit: The order number of the bit within the Supported-Features AVP, e.g. "1".
Feature: A short name that can be used to refer to the bit and to the feature, e.g. "MONTE".
M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O").
Description: A clear textual description of the feature.

8.4.24 Monitoring-Event-Config-Status

The Monitoring-Event-Config-Status AVP is of type Grouped, and it contains the details of the Error occurred during handling of the Requested action for the Monitoring event.

AVP format:

```
Monitoring-Event-Config-Status::=   <AVP header: 3142 10415>
                                    *[ Service-Report ]
                                    { SCEF-Reference-ID }
```

[SCEF-ID]

*[AVP]

8.4.25 AESE-Communication-Pattern

The AESE-Communication-Pattern AVP is of type Grouped, and it shall contain the details of the Communication-Pattern from the SCEF.

AVP format

AESE-Communication-Pattern ::= <AVP header: 3113 10415>

[SCEF-Reference-ID]

{ SCEF-ID }

*[SCEF-Reference-ID-for-Deletion]

*[Communication-Pattern-Set]

*[AVP]

At least one SCEF-Reference-ID or SCEF-Reference-ID-for-deletion shall be present.

8.4.26 Communication-Pattern-Set

The Communication-Pattern-Set AVP is of type Grouped, and it shall contain a set of Communication-Pattern.

AVP format

Communication-Pattern-Set ::= <AVP header: 3114 10415>

[Periodic-Communication-Indicator]

[Communication-Duration-Time]

[Periodic-Time]

*[Scheduled-Communication-Time]

[Stationary-Indication]

[Reference-ID-Validity-Time]

*[AVP]

Communication-duration-time and Periodic-Time shall be only provided when the Periodic-Communication-Indicator is set to PERIODICALLY.

If the Reference-ID-Validity-Time AVP is absent, it indicates that there is no expiration time defined for the Communication-Pattern-Set.

8.4.27 Periodic-Communication-Indicator

The Periodic-communication-indicator AVP is of type Unsigend32. The following values are defined:

PERIODICALLY (0)

ON_DEMAND (1)

8.4.28 Communication-duration-time

The Communication-duration-time AVP is of type Unsigned32 and shall provide the time in seconds of the duration of the periodic communication.

8.4.29 Periodic-time

Periodic-time AVP is of type Unsigned32 and shall provide the time in seconds of the interval for periodic communication.

8.4.30 Scheduled-communication-time

The Scheduled-communication-time AVP is of type Grouped.

AVP format

Scheduled-communication-time ::= <AVP header: 3118 10415>

[Day-Of-Week-Mask]

[Time-Of-Day-Start]

[Time-Of-Day-End]

*[AVP]

If Day-Of-Week-Mask is not provided this shall be interpreted as every day of the week.

If Time-Of-Day-Start is not provided, starting time shall be set to start of the day(s) indicated by Day-Of-Week-Mask.

If Time-Of-Day-End is not provided, ending time is end of the day(s) indicated by Day-Of-Week-Mask.

8.4.31 Stationary indication

The Stationary-indication AVP are of type Unsigned32.

STATIONARY_UE (0)

MOBILE_UE (1)

8.4.32 AESE-Communication-Pattern-Config-Status

The AESE-Communication-Pattern-Config-Status AVP is of type Grouped, and it shall contain the details of the outcome of Communication-Pattern handling from the HSS.

AVP format

AESE-Communication-Pattern-Config-Status ::= <AVP header: 3120 10415>

{ SCEF-Reference-ID }

[SCEF-ID]

[AESE-Error-Report]

*[AVP]

8.4.33 AESE-Error-Report

The AESE-Error-Report AVP is of type Grouped, and it contains the details of the Error occurred during handling of the Requested action for the Communication-Pattern-Set.

AVP format

AESE-Error-Report ::= <AVP header: 3121 10415>

[Service-Result]

*[AVP]

8.4.34 MME-Location-Information

The MME-Location-Information AVP is of type Grouped. It shall contain the information related to the user location relevant for the MME. It was originally defined in 3GPP TS 29.272 [49].

AVP format

MME-Location-Information ::= <AVP header: 1600 10415>

[E-UTRAN-Cell-Global-Identity]

[Tracking-Area-Identity]

[Geographical-Information]

[Geodetic-Information]

[Current-Location-Retrieved]

[Age-Of-Location-Information]

[User-CSG-Information]

[eNodeB-ID]

[Extended-eNodeB-ID]

*[AVP]

8.4.35 SGSN-Location-Information

The SGSN-Location-Information AVP is of type Grouped. It shall contain the information related to the user location relevant for the SGSN. It was originally defined in 3GPP TS 29.272 [49].

AVP format

SGSN-Location-Information ::= <AVP header: 1601 10415>

[Cell-Global-Identity]

[Service-Area-Identity]

[Routing-Area-Identity]

[Geographical-Information]

[Geodetic-Information]

[Current-Location-Retrieved]

[Age-Of-Location-Information]

[User-CSG-Information]

*[AVP]

8.4.36 User-Identifier

The User-Identifier AVP is of type Grouped and it contains the different identifiers used by the UE. This AVP is defined in sub-clause 6.4.2. The AVP format for the S6t interface shall be as given below.

AVP format:

User-Identifier ::= <AVP header: 3102 10415>

[User-Name]

[MSISDN]

[External-Identifier]

[Type-Of-External-Identifier]

*[AVP]

This AVP shall contain one of the identifiers (IMSI, MSISDN or External-Identifier). The IMSI of the UE shall be included (when applicable) in the User-Name AVP.

The External-Identifier AVP may either contain the identity of an individual UE or the identity of a Group of UEs. The Type-Of-External-Identifier is used to indicate which type of identity is carried in the External-Identifier. When the Type-Of-External-Identifier is not present, it means the External-Identifier AVP contains the identity of an individual UE.

8.4.37 Service-Result

The Service-Result AVP is of type Grouped, and it contains the Error code identified during the handling of the Requested action for the Monitoring event.

AVP format:

Service-Result ::= <AVP header: 3146 10415>

[Vendor-Id]

[Service-Result-Code]

*[AVP]

If the Service-Result-Code contains an Experimental-Result-Code value defined by 3GPP, then the Vendor-Id shall be set to the value 10415. If the Service-Result-Code contains a Result-Code value defined in the Diameter base protocol by IETF (see IETF RFC 6733 [23]), then the Vendor-Id shall be absent or set to the value 0.

8.4.38 Service-Result-Code

The Service-Result-Code AVP is of type Unsigned32. This AVP shall contain either the value of an Experimental-Result-Code defined by 3GPP or the value of a Result-Code defined in Diameter base protocol by IETF (see IETF RFC 6733 [23]).

8.4.39 CIR-Flags

The CIR-Flags AVP is of type AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.4.39-1:

Table 8.4.39-1: CIR-Flags

Bit	Name	Description
0	Delete all Monitoring events	This bit shall be set if the SCEF wants to delete all Monitoring events for a subscriber stored in the HSS.
1	Enhanced Coverage Query	This bit shall be set if the SCEF wants to query the current settings of the Enhanced-Coverage-Restriction.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

8.4.40 Supported-Services

The Supported-Services AVP is of type Grouped and it shall contain the different bit masks representing the services supported by the HSS:

AVP format

Supported-Services ::= <AVP header: 3143 10415>

[Supported-Monitoring-Events]

[Node-Type]

*[AVP]

8.4.41 Supported-Monitoring-Events

The Supported-Monitoring-Events AVP is of type Unsigned64 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.4.41-1:

Table 8.4.41-1: Supported-Monitoring-Events

Bit	Name	Description
0	UE and UICC and/or new IMSI-IMEI-SV association	This bit shall be set if Monitoring the association of the UE and UICC and/or new IMSI-IMEI-SV association Monitoring event is supported in the HSS
1	UE-reachability	This bit shall be set if UE reachability Monitoring event is supported in the HSS
2	Location-of-the-UE	This bit shall be set if Location of the UE and change in location of the UE Monitoring event is supported in the HSS
3	Loss-of-connectivity	This bit shall be set if Loss of connectivity Monitoring event is supported in the HSS
4	Communication-failure	This bit shall be set if Communication failure Monitoring event is supported in the HSS
5	Roaming-status	This bit shall be set if Roaming status (i.e. Roaming or No Roaming) of the UE, and change in roaming status of the UE Monitoring event is supported in the HSS
6	Availability after DDN failure	This bit shall be set if Availability after DDN failure Monitoring event is supported in the HSS
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

8.4.42 Reference-ID-Validity-Time

The Reference-ID-Validity-Time AVP is of type Time (see IETF RFC 6733 [23]), and contains the point of time when the CP sets associated to an SCEF-Reference-ID (in combination with an SCEF-ID) becoming invalid and shall be deleted.

8.4.43 Event-Handling

The Event-handling AVP is of type Unsigned32. The following Values are defined:

SUSPEND (0)

RESUME (1)

CANCEL (2)

8.4.44 NIDD-Authorization-Request

The NIDD-Authorization-Request AVP is of type Grouped, and it contains the details for the Authorisation of NIDD via the SCEF.

AVP format:

NIDD-Authorization-Request ::= <AVP header: 3150 10415>

[Service-Selection]

[Requested-Validity-Time]

*[AVP]

8.4.45 NIDD-Authorization-Response

The NIDD-Authorization-Response AVP is of type Grouped, and it contains the information to be provided triggered by NIDD-Authorization-Request.

AVP format:

NIDD-Authorization-Response::= <AVP header: 3151 10415>

[MSISDN]

[User-Name]

[External-Identifier]

[Granted-Validity-Time]

*[AVP]

The User-Name AVP, when present, shall contain the IMSI.

8.4.46 DRMP

The DRMP AVP is of type Enumerated and it is defined in IETF RFC 7944 [20]. This AVP allows the HSS and the SCEF over the S6t interface to indicate the relative priority of Diameter messages. The DRMP AVP may be used to set the DSCP marking for transport of the associated Diameter message.

8.4.47 Service-Report

The Service-Report AVP is of type Grouped, and it contains the Error code identified during the handling of the Requested action for the Monitoring event, the type of node and the services it supports.

AVP format:

Service-Report ::= <AVP header: 3152 10415>

[Service-Result]

[Node-Type]

*[AVP]

8.4.48 Node-Type

The Node-Type AVP is of type Unsigned32 and shall identify the type of node sending the information. The following values are defined:

HSS (0)

MME (1)

SGSN (2)

8.4.49 Service-Selection

The Service-Selection AVP is of type of UTF8String. This AVP shall contain the APN Network Identifier (i.e. an APN without the Operator Identifier) per 3GPP TS 23.003 [11], clauses 9.1 & 9.1.1,).

The contents of the Service-Selection AVP shall be formatted as a character string composed of one or more labels separated by dots (".").

This AVP is defined in IETF RFC 5778 [21].

8.4.50 S6t-HSS-Cause

The S6t-HSS-Cause AVP is of type Unsigned32 and it contains a bitmask. The meaning of the bits is defined in table 8.4.50-1:

Table 8.4.50-1: S6t-HSS-Cause

Bit	Name	Description
0	Absent Subscriber	This bit, when set, indicates that there is no serving node registered in the HSS to which the configuration could be forwarded.
NOTE:	Bits not defined in this table shall be cleared by the sending node and discarded by the receiving node.	

8.4.51 Enhanced-Coverage-Restriction

The Enhanced-Coverage-Restriction AVP is of type Grouped and shall identify either a complete (and possibly empty) list of serving PLMNs where Enhanced Coverage shall be restricted or a complete (and possibly empty) list of serving PLMNs where Enhanced Coverage shall not be restricted.

AVP format:

Enhanced-Coverage-Restriction ::= <AVP header: 3155 10415>

[Restricted-PLMN-List]

[Allowed-PLMN-List]

*[AVP]

8.4.52 Enhanced-Coverage-Restriction-Data

The Enhanced-Coverage-Restriction-Data AVP is of type Grouped and shall identify the current visited PLMN (if any) and the current settings of Enhanced-Coverage-Restriction.

AVP format:

Enhanced-Coverage-Restriction-Data ::= <AVP header: 3156 10415>

{ Enhanced-Coverage-Restriction }

[Visited-PLMN-Id]

*[AVP]

8.4.53 Restricted-PLMN-List

The Restricted-PLMN-List AVP is of type Grouped and shall identify the complete set of serving PLMNs where Enhanced Coverage is restricted.

AVP format:

Restricted-PLMN-List ::= <AVP header: 3157 10415>

*[Visited-PLMN-Id]

*[AVP]

Absence of Visited-PLMN-Id AVPs indicates that Enhanced Coverage is allowed in all serving PLMNs.

8.4.54 Allowed-PLMN-List

The Allowed-PLMN-List AVP is of type Grouped and shall identify the complete set of serving PLMNs where Enhanced Coverage is allowed.

AVP format:

Allowed-PLMN-List ::= <AVP header: 3158 10415>

*[Visited-PLMN-Id]

*[AVP]

Absence of Visited-PLMN-Id AVPs indicates that Enhanced Coverage is restricted in all serving PLMNs.

8.4.55 Requested-Validity-Time

The Requested-Validity-Time AVP is of type Time (see IETF RFC 6733 [23]), and contains the point of time after which the SCEF is willing to consider a granted NIDD authorization as being implicitly revoked.

8.4.56 Granted-Validity-Time

The Granted-Validity-Time AVP is of type Time (see IETF RFC 6733 [23]), and contains the point of time after which the HSS removes a stored NIDD Authorization and after which the SCEF shall consider a granted NIDD authorization as being implicitly revoked.

A value in the past indicates that the NIDD Authorization is explicitly revoked.

8.4.57 NIDD-Authorization-Update

The NIDD-Authorization-Update AVP is of type Grouped, and it contains the information to be provided triggered by an update or revocation of the NIDD-Authorization.

AVP format:

NIDD-Authorization-Update::=<AVP header: 3161 10415>

*[APN-Validity-Time]

*[AVP]

The User-Name AVP, when present, shall contain the IMSI.

8.4.58 Loss-Of-Connectivity-Reason

The Loss-Of Connectivity-Reason AVP is of type Unsigned32 and shall identify the reason why loss of connectivity is reported. The following values are defined:

UE_DETACHED_MME (0)

UE_DETACHED_SGSN (1)

MAX_DETECTION_TIME_EXPIRED_MME (2)

MAX_DETECTION_TIME_EXPIRED_SGSN (3)

UE_PURGED_MME (4)

UE_PURGED_SGSN (5)

8.4.59 Group-Reporting-Guard-Timer

The Group-Reporting-Guard-Timer AVP is of type Unsigned32. The Group Reporting Guard Timer indicates an interval in seconds after which time the HSS (at the latest) shall send aggregated Status Indications and/or event report(s) which have been detected for UEs that are part of a group.

8.4.60 CIA-Flags

The CIA-Flags AVP is of type AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.4.60-1:

Table 8.4.60-1: CIA-Flags

Bit	Name	Description
0	Group-Configuration-In-Progress	This bit is set when the HSS indicates that the HSS is processing the Group Monitoring Event configuration(s) and will report further status using the RIR command.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

8.4.61 Group-Monitoring-Event-Report

The Group-Monitoring-Event-Report AVP is of type Grouped, and it contains the information to be reported as requested by Monitoring-Event-Configuration for a group.

AVP format:

Group-Monitoring-Event-Report::= <AVP header: 3165 10415>

{ SCEF-Reference-ID }

[SCEF-ID]

*[Group-Monitoring-Event-Report-Item]

*[AVP]

8.4.62 Group-Monitoring-Event-Report-Item

The Group-Monitoring-Event-Report-Item AVP is of type Grouped, and it contains the information to be reported as requested by Monitoring-Event-Configuration for a specific UE as part of group processing.

AVP format:

Group-Monitoring-Event-Report-Item::= <AVP header: 3166 10415>

{ User-Identifier }

[Visited-PLMN-Id]

[Roaming-Information]

[Reachability-Information]

[Maximum-UE-Availability-Time]

[EPS-Location-Information]

[Monitoring-Type]

*[Service-Report]

[S6t-HSS-Cause]

*[AVP]

8.4.63 RIR-Flags

The RIR-Flags AVP is of type AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.4.63-1:

Table 8.4.63-1: RIR-Flags

Bit	Name	Description
0	Group-Configuration-In-Progress	This bit is set when the HSS indicates that the HSS is processing the Group Monitoring Event configuration and will report further status/reports for the group using additional RIR command(s).
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

8.4.64 Type-Of-External-Identifier

The Type-Of-External-Identifier AVP is of type Unsigned32 and it shall indicate which type of identity is carried in the External-Identifier AVP. The following values are defined:

EXTERNAL-UE-IDENTIFIER-TYPE (0)

The value 0 indicates the External-Identifier AVP carries the identity of an individual UE.

EXTERNAL-GROUP-IDENTIFIER-TYPE (1)

The value 1 indicates the External-Identifier AVP carries the identity of a Group of UEs.

8.4.65 APN-Validity-Time

The APN-Validity-Time AVP is of type Grouped, and it contains the APN (within the Service-Selection AVP) and the updated validity time for the granted NIDD authorization associated to the APN.

AVP format:

APN-Validity-Time::= <AVP header:3169 10415>

{ Granted-Validity-Time }

[Service-Selection]

*[AVP]

Absence of Service-Selection AVP indicates that the Granted-Validity-Time applies to all granted NIDD Authorizations for the user. In this case only one APN-Validity-Time AVP shall be present within the NIDD-Authorization-Update AVP.

Annex A (normative): Diameter overload control mechanism

A.1 General

IETF RFC 7683 [15] specifies a Diameter overload control mechanism which includes the definition and the transfer of related AVPs between Diameter nodes.

A.2 S6m interface

A.2.1 General

The Diameter overload control mechanism is an optional feature over the S6m interface.

It is recommended to make use of the IETF RFC 7683 [15] on the S6m interface where, when applied, the MTC-IWF shall behave as a reacting node and the HSS as a reporting node.

NOTE: There is no need to support this mechanism in the other way (overload of the MTC-IWF) as no Diameter request commands are sent by the HSS to the MTC-IWF.

A.2.2 HSS behaviour

The HSS requests traffic reduction from the MTC-IWF when it is in an overload situation, by including OC-OLR AVP in answer commands as described in IETF RFC 7683 [15].

The HSS identifies that it is in an overload situation by implementation specific means. For example, the HSS may take into account the traffic over the S6m interfaces or other interfaces, the level of usage of internal resources (CPU, memory), the access to external resources etc.

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

A.2.3 MTC-IWF behaviour

The MTC-IWF applies required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [15].

Requested traffic reduction is achieved by the MTC-IWF by implementation specific means. For example, it may implement message throttling with prioritization.

Annex B gives guidance on message prioritisation over the S6m interface.

A.3 S6t interface

A.3.1 General

The Diameter overload control mechanism is an optional feature over the S6t interface.

It is recommended to make use of the IETF RFC 7683 [15] on the S6t interface where, when applied, the SCEF shall behave as a reacting node and the HSS as a reporting node.

NOTE: With the current services used on this interface there is no need to support this mechanism in the other direction (overload of the SCEF) as the number of Diameter request commands sent by the HSS to the SCEF is determined by the SCEF in one earlier command of the SCEF and they corresponds to non-frequent events.

A.3.2 HSS behaviour

The HSS requests traffic reduction from the SCEF when it is in an overload situation, by including OC-OLR AVP in answer commands as described in IETF RFC 7683 [15].

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

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

A.3.3 SCEF behaviour

The SCEF applies required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [15].

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

Annex B (Informative): Diameter overload control node behaviour

B.1 Introduction

Annex B gives guidance on the Diameter overload control node behaviours regarding message prioritisation over the S6m and S6t interface.

B.2 Message prioritisation over S6m

This clause gives an analysis of possible behaviours of the MTC-IWF regarding message prioritisation as guidance and for an informative purpose.

When the HSS is overloaded, the MTC-IWF will receive overload reports from the HSS requesting a reduction of requests sent by the MTC-IWF. This will apply to the SIR request commands.

The MTC-IWF can consider some messages with a lower or a higher priority; lower priority messages will be candidates for throttling before higher priority messages.

Following considerations can be taken into account:

- SIR messages for a given SCS can have a lower priority according to operator policies;
- If a SCS node generates a peak signalling over the Tsp interface, SIR messages over S6m related to this SCS can have a lower priority;
- The SIR messages over S6m related to a recall procedure or a replace procedure over the Tsp interface (see 3GPP TS 29.368 [13]) may have a lower priority according to operator policies.

B.3 Message prioritisation over S6t

This clause gives an analysis of possible behaviours of the SCEF regarding message prioritisation as guidance and for an informative purpose.

When the HSS is overloaded, the SCEF will receive overload reports from the HSS requesting a reduction of requests sent by the SCEF. This will apply to the CIR request commands.

The SCEF can consider some messages with a lower or a higher priority; lower priority messages will be candidates for throttling before higher priority messages.

Following considerations can be taken into account:

- CIR messages for a given SCEF can have a lower priority according to operator policies;
- If a SCEF node generates a peak signalling over the S6t interface, CIR messages from this SCEF can have a lower priority;

Annex C (normative): Diameter message priority mechanism

C.1 General

IETF 7944 [20] specifies a Diameter routing message priority mechanism that allows Diameter nodes to indicate the relative priority of Diameter messages. With this information, other Diameter nodes may leverage the relative priority of Diameter messages into routing, resource allocation, set the DSCP marking for transport of the associated Diameter message, and also abatement decisions when overload control is applied.

It is recommended to make use of IETF 7944 [20] over the S6m, S6n and S6t interfaces of an operator network when the overload control defined in Annex A is applied on these interfaces.

C.2 S6m, S6n, S6t interfaces

The Diameter message priority mechanism is an optional feature which may apply on one or several of the S6m, S6n, S6t interfaces.

A 3GPP functional entity supporting the Diameter message priority mechanism over one or several of the S6m, S6n, S6t interfaces shall comply with IETF RFC 7944 [20].

A 3GPP functional entity sending a request shall determine the required priority according to its policies. When priority is required, it shall include the DRMP AVP indicating the required priority level in the request it sends, and shall prioritise the request according to the required priority level.

When the 3GPP functional entity receives the corresponding response, it shall prioritise received response according to the priority level received within the DRMP AVP if present in the response, otherwise according to the priority level of the corresponding request.

When a 3GPP functional entity receives a request, it shall handle the request according to the received DRMP AVP priority level. For the response, it may modify the priority level received in the DRMP AVP according to its policies and shall handle the response according to the required priority level. If the required priority level is different from the priority level received in the request, it shall include the DRMP AVP in the response.

The decisions of the 3GPP functional entity for a required priority and for the priority level value are implementation specific.

If:

- a 3GPP functional entity supports using the Diameter message priority mechanism for DSCP marking purposes,
- the transport network utilizes DSCP marking, and
- message-dependant DSCP marking is possible for the protocol stack transporting Diameter,

then the 3GPP functional entity shall set the DSCP marking for transport of the request or response according to the required priority level.

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

Annex D (normative): Diameter load control mechanism

D.1 General

IETF draft-ietf-dime-load-03 [22] specifies a mechanism for sharing of Diameter load information. It includes the definition and the transfer of related AVPs between Diameter nodes.

D.2 S6m interface

D.2.1 General

The Diameter load control mechanism is an optional feature over the S6m interface.

It is recommended to make use of IETF draft-ietf-dime-load-03 [22] on the S6m interface where, when applied, the MTC-IWF shall behave as reacting nodes and the HSS as a reporting node.

D.2.2 HSS behaviour

The HSS may report its current load by including a Load AVP of type HOST in answer commands as described in IETF draft-ietf-dime-load-03 [22].

The HSS calculates its current load by implementation specific means. For example, the HSS may take into account the traffic over the S6m interface or other interfaces, the level of usage of internal resources (e.g. CPU, memory), the access to external resources, etc.

The HSS determines when to send Load AVPs of type HOST by implementation specific means.

D.2.3 MTC-IWF behaviour

When performing next hop Diameter Agent selection for requests that are routed based on realm, the MTC-IWF may take into account load values from Load AVPs of type PEER received from candidate next hop Diameter nodes, as per IETF draft-ietf-dime-load-03 [22].

D.3 S6t interface

D.3.1 General

The Diameter load control mechanism is an optional feature over the S6t interface.

It is recommended to make use of IETF draft-ietf-dime-load-03 [22] on the S6t interface where, when applied, the SCEF shall behave as reacting nodes and the HSS as a reporting node.

D.3.2 HSS behaviour

The HSS may report its current load by including a Load AVP of type HOST in answer commands as described in IETF draft-ietf-dime-load-03 [22].

The HSS calculates its current load by implementation specific means. For example, the HSS may take into account the traffic over the S6t interface or other interfaces, the level of usage of internal resources (e.g. CPU, memory), the access to external resources, etc.

The HSS determines when to send Load AVPs of type HOST by implementation specific means.

D.3.3 SCEF behaviour

When performing next hop Diameter Agent selection for requests that are routed based on realm, the SCEF may take into account load values from Load AVPs of type PEER received from candidate next hop Diameter nodes, as per IETF draft-ietf-dime-load-03 [22].

Annex E (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2012-09	CT#57	CP-120485			V.1.0.0 presented for information and approval	1.0.0	11.0.0
2012-12	CT#58	CP-120731	0001	3	T4 device triggering via IMS	11.0.0	11.1.0
2012-12	CT#58	CP-120731	0002	1	MWD and SMS-SC address		
2012-12	CT#58	CP-120731	0003	-	Application ID and Command Codes		
2013-06	CT#60	CP-130300	0004	2	S6m complements related to Diameter for SMS with SGSN	11.1.0	12.0.0
2013-09	CT#61	CP-130456	0005	2	SGSN Diameter address with Gdd support	12.0.0	12.1.0
2014-06	CT#64	CP-140243	0007	3	Diameter overload over S6m	12.1.0	12.2.0
2014-12	CT#66	CP-140775	0008	1	Absent Subscriber detection	12.2.0	12.3.0
2015-06	CT#68	CP-150248	0012	1	IP-SM-GW-Realm	12.3.0	12.4.0
2015-06	CT#68	CP-150265	0009	1	Unsuccessful Triggering due to MT-SMS barring	12.4.0	13.0.0
2015-06	CT#68	CP-150271	0013	3	Introducing S6t reference point	12.4.0	13.0.0
2015-09	CT#69	CP-150456	0019	3	New Monitoring configuration commands on S6t	13.0.0	13.1.0
2015-09	CT#69	CP-150456	0020	2	Update S6t description to support AESE Communication Pattern provision	13.0.0	13.1.0
2015-09	CT#69	CP-150456	0022	3	Introducing CP parameter to commands on S6t	13.0.0	13.1.0
2015-12	CT#70	CP-150778	0023	-	S6t Application ID and Command Codes	13.1.0	13.2.0
2015-12	CT#70	CP-150778	0024	3	Enhancements to St6 on MONTE	13.1.0	13.2.0
2015-12	CT#70	CP-150778	0026	1	Diameter Overload on S6t	13.1.0	13.2.0
2015-12	CT#70	CP-150778	0028	1	Corrections to some MONTE AVPs, references and procedures	13.1.0	13.2.0
2015-12	CT#70	CP-150778	0030	3	Multiple instances in a configuration request command	13.1.0	13.2.0
2015-12	CT#70	CP-150778	0031	2	Enhancements and clarification on MONTE	13.1.0	13.2.0
2015-12	CT#70	CP-150778	0033	3	Deletion of all Monitoring events assigned to a subscriber (UE)	13.1.0	13.2.0
2015-12	CT#70	CP-150785	0025	3	Introducing a Bitmask to inform the SCEF of the Monitoring capabilities of the HSS	13.1.0	13.2.0
2015-12	CT#70	CP-150771	0027	3	Introducing CP parameter to CIR/CIA commands on S6t	13.1.0	13.2.0
2015-12	CT#70	CP-150759	0032	1	Reference to DOIC updated with IETF RFC 7683	13.1.0	13.2.0
2016-03	CT#71	CP-160029	0037	2	Clarification on LOSS_OF_CONNECTIVITY reporting	13.2.0	13.3.0
2016-03	CT#71	CP-160029	0039	2	SCEF Restart	13.2.0	13.3.0
2016-03	CT#71	CP-160029	0040	2	Reporting of the start and stop of the reporting of monitoring events	13.2.0	13.3.0
2016-03	CT#71	CP-160029	0044	1	Count and Stop Monitoring Event Reports at SCEF	13.2.0	13.3.0
2016-03	CT#71	CP-160029	0045	1	Change of type of Monitoring-Duration AVP to represent an absolute time	13.2.0	13.3.0
2016-03	CT#71	CP-160033	0046	4	Authorization for NIDD procedure over S6t	13.2.0	13.3.0
2016-03	CT#71	CP-160023	0047	1	Diameter message priority over S6m, S6n, S6t	13.2.0	13.3.0
2016-03	CT#71	CP-160129	0048	4	Definition of Monitoring-Type and clarifications on UE in MME and SGSN for MONTE	13.2.0	13.3.0
2016-06	CT#72	CP-160225	0049	1	Cleanup on MONTE	13.3.0	13.4.0
2016-06	CT#72	CP-160225	0056	-	Address editor's note on retry-after when sending cancel monitoring event to the SCEF	13.3.0	13.4.0
2016-06	CT#72	CP-160228	0050	7	NIDD authorisation update	13.3.0	13.4.0
2016-06	CT#72	CP-160228	0051	-	IANA Command Code Registration	13.3.0	13.4.0
2016-06	CT#72	CP-160228	0052	-	Type of SCEF-ID AVP	13.3.0	13.4.0
2016-06	CT#72	CP-160233	0053	-	Renaming of Validity-Time AVP	13.3.0	13.4.0
2016-06	CT#72	CP-160233	0057	1	Missing reference to SIR-flags	13.3.0	13.4.0
2016-09	CT#73	CP-160416	0043	2	SCS identity format	13.4.0	13.5.0
2016-12	CT#74	CP-160650	0059	1	AVP code alignment with 29.230	13.5.0	13.6.0
2016-12	CT#74	CP-160657	0060	1	User Identity correction on NIDD configuration procedure	13.5.0	13.6.0
2016-12	CT#74	CP-160657	0061	1	IMSI in NIR	13.5.0	13.6.0
2016-12	CT#74	CP-160657	0063	2	External-Identifier Retrieval when no NIDD configuration exists	13.5.0	13.6.0
2016-12	CT#74	CP-160664	0065	-	Correction to change IETF drmp draft version to official RFC 7944	13.5.0	13.6.0
2016-12	CT#74	CP-160660	0066	2	HSS-Cause in CIA	13.5.0	13.6.0
2016-12	CT#74	CP-160660	0067	1	Maximum Detection Time	13.5.0	13.6.0
2016-12	CT#74	CP-160673	0062	1	MO SMS over T4	13.6.0	14.0.0
2016-12	CT#74	CP-160681	0064	1	Load Control	13.6.0	14.0.0

2017-03	CT#75	CP-170031	0081	1	S6t Update to Provide the Suggested Buffering Packet Count to the HSS	14.0.0	14.1.0
2017-03	CT#75	CP-170039	0068	2	Enhanced Coverage	14.0.0	14.1.0
2017-03	CT#75	CP-170039	0070	2	NIDD Authorization revocation	14.0.0	14.1.0
2017-03	CT#75	CP-170036	0069	2	Loss Of Connectivity Reason	14.0.0	14.1.0
2017-03	CT#75	CP-170036	0072	1	Monitoring Status Update	14.0.0	14.1.0
2017-03	CT#75	CP-170036	0073	1	Recources Exceeded	14.0.0	14.1.0
2017-03	CT#75	CP-170036	0076	-	Failed-AVP AVP in Request Commands	14.0.0	14.1.0
2017-03	CT#75	CP-170036	0077	1	Bit ordering in Diameter AVPs used as bit-masks	14.0.0	14.1.0
2017-03	CT#75	CP-170036	0078	-	Support of long and short Macro eNodeB IDs	14.0.0	14.1.0
2017-03	CT#75	CP-170036	0079	-	Service-ID in SIR	14.0.0	14.1.0
2017-03	CT#75	CP-170029	0083	1	Maximum UE Availability Time	14.0.0	14.1.0
2017-03	CT#75	CP-170048	0084	-	Update of reference for the Diameter base protocol	14.0.0	14.1.0
2017-03	CT#75	CP-170048	0085	-	Handling of the Vendor-Specific-Application-Id AVP	14.0.0	14.1.0
2017-03	CT#75	CP-170048	0086		Cardinality of the Failed-AVP AVP in answer	14.0.0	14.1.0
2017-06	CT#76	CP-171029	0087	3	Support for group based reporting and status indication for MONTE	14.1.0	14.2.0
2017-06	CT#76	CP-171030	0088	-	NIDD Authorization revocation	14.1.0	14.2.0
2017-06	CT#76	CP-171030	0089	1	NIDD Authorization update per APN	14.1.0	14.2.0
2017-06	CT#76	CP-171038	0090	1	MO-SMS	14.1.0	14.2.0
2017-06	CT#76	CP-171184	0092	1	Communication Patterns without Expiry Time	14.1.0	14.2.0
2017-06	CT#76	CP-171021	0094	1	Remove User-Identifier from NIA	14.1.0	14.2.0
2017-06	CT#76	CP-171029	0095	1	Unauthorized Requesting Entity on S6t	14.1.0	14.2.0
2017-06	CT#76	CP-171018	0097	1	Support for signaling transport level packet marking	14.1.0	14.2.0
2017-09	CT#77	CP-172013	0104	-	Correction of DRMP Procedures	14.2.0	14.3.0
2017-12	CT#78	CP-173029	0115	-	Reachability Type	14.3.0	14.4.0

History

Document history		
V14.1.0	May 2017	Publication
V14.2.0	July 2017	Publication
V14.3.0	October 2017	Publication
V14.4.0	January 2018	Publication