ETSI TS 129 336 V12.5.0 (2016-01)

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 12.5.0 Release 12)

Reference
RTS/TSGC-0429336vc50

Keywords
LTE,UMTS

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

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

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

Foreword

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

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

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

Modal verbs terminology

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

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

Contents

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) and the S6n interface between the HSS and the MTC-AAA. The procedures over those interfaces are defined in 3GPP TS 23.682 [2].

2 References

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

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

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

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

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

[4] 3GPP TS 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".

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
IANA	Internet Assigned Numbers Authority
MTC	Machine-Type Communications
MTC-IWF	MTC Interworking Function
SCS	Services Capability Server

4 General Description

4.1 Introduction

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

This document describes the Diameter-based S6m and S6n 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.

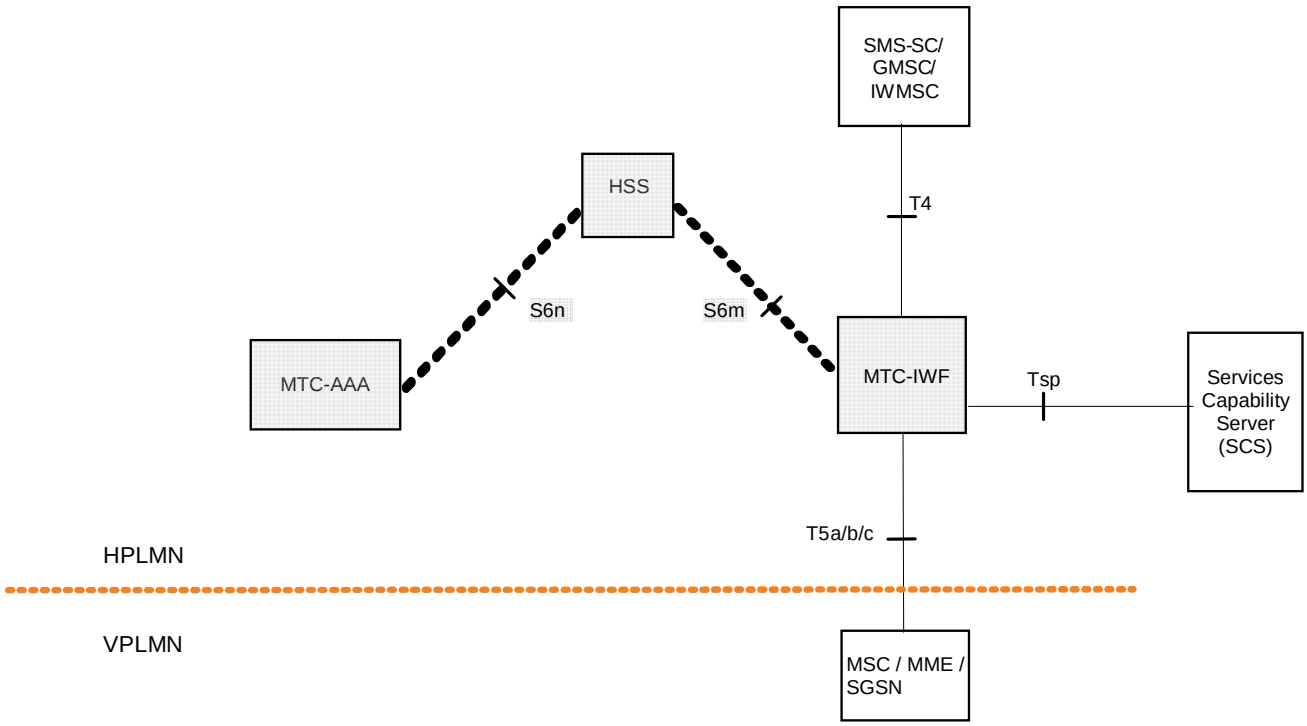

Figure 4.1-1: 3GPP Architecture for Machine-Type Communication

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,
- 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.

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.

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 service is 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.
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) is supported. For Device Triggering via SMS-MT, this AVP may contain: Priority-Indication, SM-RP-SMEA…
SIR Flags	SIR-Flags	M	This Information Element shall contain a bit mask. See section 6.4.7 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. 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 SCS is authorized to request 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 authorized. If not, Experimental-Result shall be set to DIAMETER_ERROR_UNAUTHORIZED_SERVICE (5511) in the Subscriber Information Retrieval Response.

4. 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. Check that the requested service can be delivered according to the user's provisioned teleservices and the user's active barring conditions. In the response, the HSS shall set accordingly the corresponding bits in the HSS-Cause IE (see clause 6.4.9).

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. 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.

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, 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.

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

6.1.2 Securing Diameter Messages

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

6.1.3 Accounting Functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) shall not be used on the 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 includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 3588 [3]. As a consequence, the server shall not maintain any state information about this session and the client shall not send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

6.1.5 Transport Protocol

Diameter messages over the 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.

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

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

6.1.7 Advertising Application Support

The 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 3588 [3].

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).

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 rules in IETF RFC 3588 [3]. When the definition and use of an AVP is not specified in this document, the guidelines in IETF RFC 3588 [3] shall apply.

The following Command Codes are defined in this specification:

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 >
                                          { 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 >
                                          [ Result-Code ]
                                          [ Experimental-Result ]
                                          { Auth-Session-State }
                                          { Origin-Host }
                                          { Origin-Realm }
                                          [ OC-Supported-Features ]
                                          [ OC-OLR ]
                                          *[ 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 RFC 3588 [3] shall be applied.

6.3.3 Permanent Failures

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

6.3.3.1 DIAMETER_ERROR_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).

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 3588 [3]. NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.								

The following table specifies the Diameter AVPs re-used by the 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, do not need to be supported. The AVPs from Diameter Base Protocol are not included in table 6.4.1/2, but they may be re-used for the S6m/S6n protocol.

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

Attribute Name	Reference	Comments
User-Name	IETF RFC 3588 [3]	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

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.

6.4.4 SCS-Identity

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

6.4.5 Service-Parameters

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

AVP format:

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

[T4-Parameters]

*[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. 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.

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].

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.

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 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 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 may 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.

Annex C (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
		CP-120731	0002	1	MWD and SMS-SC address		
		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
2015-12	CT#70	CP-150759	0036	-	Reference to DOIC updated with IETF RFC 7683	12.4.0	12.5.0

History

Document history		
V12.2.0	October 2014	Publication
V12.3.0	January 2015	Publication
V12.4.0	July 2015	Publication
V12.5.0	January 2016	Publication