ICS 33.040.01
M 19

YD

中华人民共和国通信行业标准

YD/T 2624-2013

演进的移动分组核心网络（EPC）接口技术要求 S6a/S6d/S13/S13' /STa/SWd/SWx/SWa/SWm/S6b

Technical requirements for
evolved mobile packet core network interfaces
- S6a/S6d/S13/S13' /STa/SWd/SWx/SWa/SWm/S6b

2013-10-17 发布　　2014-01-01 实施

中华人民共和国工业和信息化部 发布

目　次

前　言

YD/T 2624-2013《演进的移动分组核心网络(EPC)接口技术要求 S6a/S6d/S13/S13'/STa/SWd/SWx/SWa/SWm/S6b》是演进的移动分组核心网系列标准之一。该系列标准的结构和名称预计如下：

a）YD/T 2620-2013《演进的移动分组核心网络(EPC)总体技术要求》

— 第1部分：支持E-UTRAN接入；

— 第2部分：支持CDMA接入。

b）YD/T 2628-2013《演进的移动分组核心网络(EPC)设备技术要求》

— 第1部分：支持E-UTRAN接入；

— 第2部分：支持CDMA接入。

c）YD/T 2629-2013《演进的移动分组核心网络(EPC)设备测试方法》

— 第1部分：支持E-UTRAN接入；

— 第2部分：支持CDMA接入。

d）YD/T 2622-2013《演进的移动分组核心网络(EPC)接口技术要求 S3/S4/S5/S8/S10/S11/S16》；

e）YD/T 2625-2013《演进的移动分组核心网络(EPC)接口测试方法 S3/S4/S5/S8/S10/S11/S16》；

f）YD/T 2623-2013《演进的移动分组核心网络(EPC)接口技术要求 S2a/S101/S102/S103》；

g）YD/T 2626-2013《演进的移动分组核心网络(EPC)接口测试方法 S2a/S101/S102/S103》；

h）YD/T 2624-2013《演进的移动分组核心网络(EPC)接口技术要求 S6a/S6d/S13/S13'/STa/SWd/SWx/SWa/SWm/S6b》；

i）YD/T 2627-2013《演进的移动分组核心网络(EPC)接口测试方法 S6a/S6d/S13/S13'/STa/SWd/SWx/SWa/SWm/S6b》。

随着技术的发展，还将制定后续相关标准。

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、中国电信集团公司、中国移动通信集团公司、华为技术有限公司、中兴通讯股份有限公司、上海贝尔股份有限公司、诺基亚西门子通信（上海）有限公司、南京爱立信熊猫通信有限公司、大唐电信科技产业集团、新邮通信设备有限公司、中国普天信息产业股份有限公司。

本标准主要起草人：刘荣朵、李文苡、闫学霞、丁兆明、游世林、金曙光、徐　鹏、谢晓棠、夏　琪、习建德、徐　晖、蔡杰、姜怡华。

演进的移动分组核心网络（EPC）接口技术要求 S6a/S6d/S13/S13' /STa/SWd/SWx/SWa/SWm/S6b

1 范围

本标准规定了 EPC 系统中基于 Diameter 的接口协议，包括协议的概述、各接口消息描述、消息参数配置等。本标准规定的协议涉及到的接口包括 S6a/S6d/S13/S13' /STa/SWd/SWx/ /SWm/S6b。本标准不包括语音、LCS、紧急呼叫、家庭基站等场景。

本标准适用于EPC系统中采用Diameter协议进行通信的设备。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3GPP TS 22.016 IMEI（International Mobile station Equipment Identities）

3GPP TS 23.003 编号，寻址和标识（Numbering, addressing and identification）

3GPP TS 23.011 补充业务的实现(Technical realization of Supplementary Services)

3GPP TS 23.060 GPRS业务描述（General Packet Radio Service (GPRS); Service description; Stage 2）

3GPP TS 23.401 EUTRAN的接入的GPRS增强 （General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access）

3GPP TS 23.402 非3GPP接入的架构增强（Architecture enhancements for non-3GPP accesses）

3GPP TS 24.302 通过非3GPP接入3GPP网络演进分组核心网（EPC）；第3阶段 (Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3)

3GPP TS 29.002 MAP应用部分规格(Mobile Application Part (MAP) specification)

3GPP TS 29.061 支持数据业务的PLMN与数据网络的互操作(Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN))

3GPP TS 29.212 Gx参考点的策略和计费控制(Policy and Charging Control (PCC); Reference points)

3GPP TS 29.229 基于Diameter协议的Cx和Dx接口；协议明细(Cx and Dx interfaces based on the Diameter protocol; Protocol details)

3GPP TS 29.272 基于Diameter协议的移动性管理实体(MME)和服务GPRS支持节点(SGSN)相关接口（Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol）

3GPP TS 32.422 电信管理；用户和设备跟踪；跟踪控制和配置管理(Telecommunication management; Subscriber and equipment trace; Trace control and configuration management)

3GPP TS 33.102 3G安全；安全结构（3G security; Security architecture）

3GPP TS 33.203 3G安全；基于IP业务的接入安全性（3G security; Access security for IP-based services）

3GPP TS 33.234 无线局域网(WLAN)互通安全（3G security; Wireless Local Area Network (WLAN) interworking security）

3GPP TS 33.401 3GPP系统架构演进(SAE)：安全架构（3GPP System Architecture Evolution (SAE); Security architecture）

3GPP TS 33.402 3GPP 架构演进（SAE）；非3GPP接入的安全方面（3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses）

IETF RFC 3588 Diameter基础协议 (Diameter Base Protocol)

IETF RFC 3748 可扩展认证协议 (Extensible Authentication Protocol (EAP))

IETF RFC 4005 Diameter网络接入服务应用 (Diameter Network Access Server Application)

IETF RFC 4006 Diameter信用控制应用 (Diameter Credit-Control Application)

IETF RFC 4072 Diameter 可扩展鉴权协议应用 (Diameter Extensible Authentication Protocol (EAP) Application)

IETF RFC 4282 网络接入标识(The Network Access Identifier)

IETF RFC 5447 Diameter移动IPv6:支持网络接入服务与Diameter服务的交互 (Diameter Mobile IPv6:Support for Network Access Server to Diameter Server Interaction)

IETF RFC 5448 第三代鉴权和密钥协商协议定义的“增强的可扩展鉴权协议”(Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'))

IETF RFC 5777 用于Diameter的业务分类和QoS属性(Traffic Classification and Quality of Service (QoS)Attributes for Diameter)

IETF RFC 5778 Diameter移动IPv6:家乡代理和Diameter服务器的交互 (Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction)

IETF RFC 5779 Diameter代理移动IP：移动性接入网关和本地移动性锚点与Diameter服务器交互(Diameter Proxy·Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

必选 Mandatory

命令消息中应该携带被标记为必选的信息单元。如果消息中缺少必选的信息单元，则接受方的应用层会报错，并将设置了结果值为DIAMETER_MISSING_AVP的响应返回给发送方，响应消息还应该同时在Failed-AVP中携带所缺失的必选信息单元。

条件可选 Conditional optional

条件具备的情况下，命令消息中应该携带被标记为条件可选的信息单元。如果接收方发现条件具备但信息单元缺失，则应用层会报错，并将携带有值为DIAMETER_MISSING_AVP的Result-Code返回给发送方。响应消息中还应该同时在Failed-AVP中携带所缺失的必选信息单元。

条件不具备的情况下，不应该携带被标记为条件可选的信息单元。如果该信息单元出现在消息中，在没有明确将这种状况定义为一种错误的情况下，接收方忽略该消息；在明确定义出现该信息单元为错误的情况下，接收方应该将携带有值为DIAMETER_AVP_NOT_ALLOWED的Result-Code返回给发送方，响应消息中还应该同时在Failed-AVP中携带这个多余的信息单元。

可选 Optional

命令消息中可以携带可选的信息单元，也可以不带，具体的判断由发送方进行。消息中出现该信息单元或者缺少该信息单元都都不会引起接收方应用层报错，接收方可能会忽略该信息单元。

3.2 缩略语

下列缩略语适用于本文件。

AVP	Attribute Value Pair	属性值对
EIR	Equipment Identity Register	设备标识寄存器
EPC	Evolved Packet Core	演进的分组核心网
ePDG	evolved Packet Data Gateway	演进的分组数据网关
FACoA	Foreign Agent Care-of-Address	外地代理转交地址
HSS	Home Subscriber Server	归属位置服务器
IE	Information Element	信息单元
LMA	Local Mobility Anchor	本地移动性锚点
MAG	Mobile Access Gateway	移动接入网关
MIPv4	Mobile IP version 4	移动IPv4
MME	Mobility Management Entity	移动性管理实体
NAS	Network Access Server	网络接入服务器
ODB	Operator Determined Barring	运营商禁止业务
PBU	Proxy Binding Update	代理绑定更新
PMIP/PMIPv6	Proxy Mobile IP version 6	代理移动IPv6
RRP	MIPv4 Registration Reply	MIPv4注册响应
RRQ	MIPv4 Registration Request	MIPv4注册请求
SCTP	Stream Control Transmission ProtocolL	流媒体控制传输协议
SGW	Serving Gateway	服务网关
UE	User Equipment	用户设备
URRP-MME	User Reachability Request Parameter for MME	MME的用户可达性请求信息单元
URPP-SGSN	User Reachability Request Parameter for SGSN	SGSN的用户可达性请求信息单元

4 概述

支持 3GPP 接入和非 3GPP 接入的 EPC 系统中有多个接口使用 Diameter 协议进行通信，图 1 所示为 3GPP 接入 EPC 网络的参考模型，其中接口 S6a、S6d、S13 和 S13`采用 Diameter 协议进行通信。S6a 是 MME 与 HSS 的接口，S6d 是 SGSN 与 HSS 的接口，S6a 接口与 S6d 接口的信令、消息以及信息单元类似。S13 是 MME 与 EIR 的接口，S13`是 SGSN 与 EIR 的接口、S13 接口与 S13`接口的信令、消息以及信息单元类似。

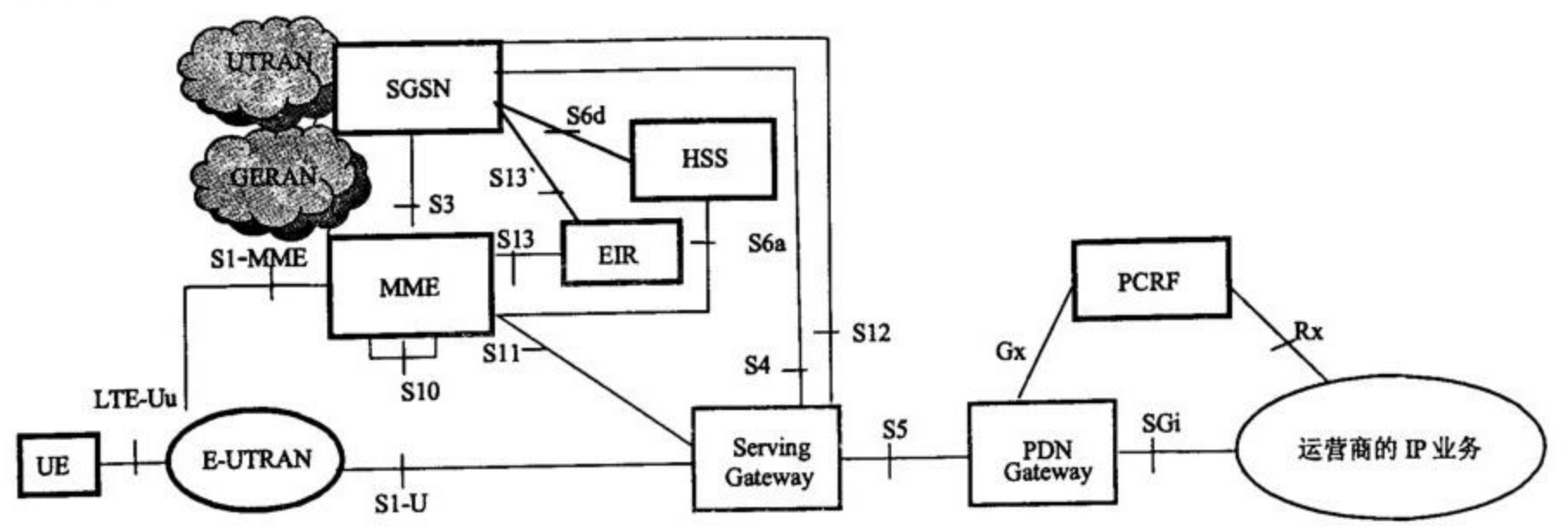

图1 3GPP 接入 EPC 网络参考模型

图 2 所示为非 3GPP 接入 EPC 的网络参考模型，其中接口 STa、SWd、SWx、SWa、SWm 和 S6b 采用 Diameter 协议。STa 是信任域的非 3GPP 接入与 3GPP AAA 服务器（或 3GPP AAA 代理服务器）之间的接口。SWd 是 3GPP AAA 代理服务器与 3GPP AAA 服务器之间的接口。SWx 是 3GPP AAA 服务器与 HSS 之间的接口。S6b 是 3GPP AAA 服务器（或 3GPP AAA 代理服务器）与 PDN GW 之间的接口。SWa 是非信任域的非 3GPP 接入与 3GPP AAA 服务器（或 3GPP AAA 代理服务器）之间的接口。SWm 是 ePDG 与 3GPF AAA Server（或者 3GPP AAA 代理服务器）之间的接口。本标准中可信任的非 3GPP 接入特指 CDMA 接入。

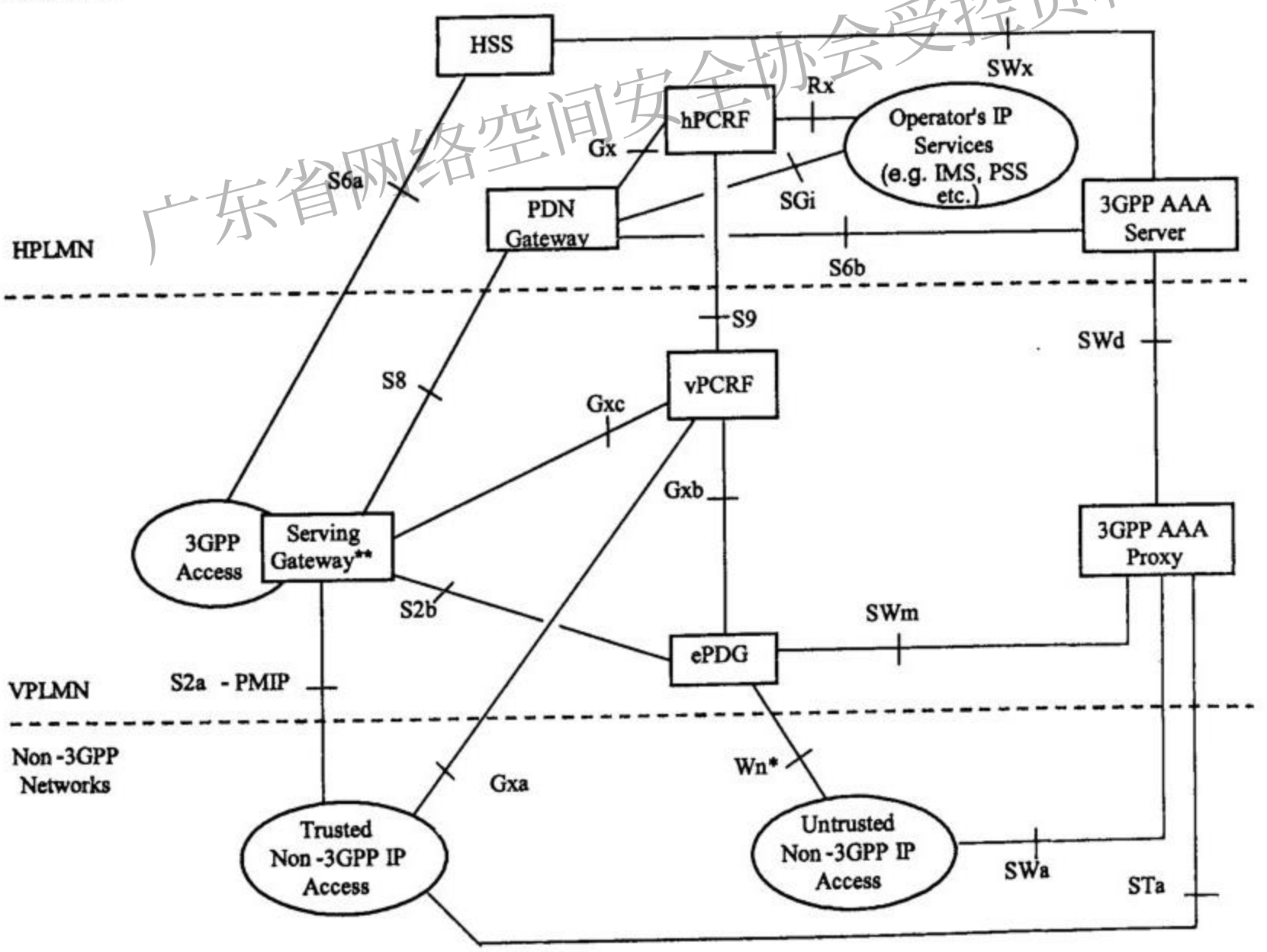

图2 非 3GPP 接入 EPC 网络参考模型

5 S6a/S6d 接口

5.1 概述

S6a接口位于MME与HSS之间，S6d接口位于SGSN与HSS之间，这两个接口支持位置更新、用户数据管理以及鉴权等消息。

5.2 消息

5.2.1 位置更新消息 (ULR/ULA)

5.2.1.1 消息内容

位置更新消息是MME/SGSN和HSS之间的消息，用于更新用户的位置信息，由MME/SGSN向HSS发起请求。位置更新消息的主要功能包括：

a）通知 HSS 当前服务用户 MME 或 SGSN 的标识；

b）更新 MME 或 SGSN 中的用户签约数据；

c）提供给 HSS 其他类型的用户数据，例如：终端信息（IMEI、IMEISV）。

表 1 和表 2 分别为位置更新请求消息和位置更新响应消息的信息单元列表。

表1 位置更新请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户身份标识，主要是指IMSI
Supported Features	Supported-Features	可选	这个IE如果出现，包含源主机支持的特性列表
Terminal Information	Terminal-Information	可选	这个参数包含用户移动终端的设备信息。在S6a/S6d接口中，只有IMEI和Software-Version这两个AVP包含在这个信元中
ULR Flags	ULR-Flags	必选	这个参数含有比特掩码
Visited PLMN Id	Visited-PLMN-Id	必选	这个参数包含MCC和MNC，详细定义依据GPP TS23.003，一般用于漫游特性
RAT Type	RAT-Type	必选	这个参数包含UE正在使用的无线接入类型
SGSN number	SGSN-Number	条件可选	这个参数包含SGSN的ISDN号码，依据3GPP TS 23.003. 当S6d接口上发送短信或者SGSN支持LCS或者SMS功能时，这个必选出现。 当S6a接口发送短信并且请求节点包含MME/SGSN (MME/SGSN为合一设备)时，这个可能也出现
Homogeneous Support of IMS Voice Over PS Sessions	Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions	可选	这个参数如果出现，指示当前服务节点（MME或SGSN或者MME/SGSN合一设备）所服务下的所有的TA或者RA是否都支持“IMS Voice over PS Sessions”。 SUPPORTED：表示所有的TA或者RA都支持"IMS Voice over PS Sessions"； NOT_SUPPORTED：表示不是所有TA或者RA支持"IMS Voice over PS Sessions"
V-GMLC address	GMLC-Address	条件可选	这个参数包含和当前服务节点相关联的可用的V-GMLC的IPv4或IPv6的地址

表1（续）

信息单元名称	映射到Diameter AVP	类别	描述
Active APN	Active-APN	可选	这个参数如果出现，包含MME或SGSN上所激活的APN列表，其中包含了为每一个APN分配的PDN GW的身份标识。同时也应该包含下面的信息： - Context-Identifier: 正在使用的签约的APN的上下文索引。 - Service-Selection: 正在使用的签约的APN的名字 - MIP6-Agent-Info: 正在使用的签约的APN关联的PDN GW的标识 - Visited-Network-Identifier: 被分配的PDN GW所处PLMN的标识 - Specific-APN-Info: 因签约通配APN而授权激活的PDN-GW的身份列表 当HSS发起一个重启(RSR)过程后，MME或SGSN使用此信元为HSS恢复(当前激活的APN的)PDN-GW身份信息

表2 位置更新响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示S6a/S6d的错误，包括： - User Unknown 用户不存在 - Unknown EPS Subscription 用户没有EPS签约数据 - RAT Not Allowed：不允许当前无线接入类型 - Roaming Not Allowed：不允许漫游
ULA-Flags	ULA-Flags	条件可选	这个参数包含比特掩码，当Result-Code为DIAMETER_SUCCESS时，这个参数才会出现
Subscription Data	Subscription-Data	条件可选	这个参数包含用户的所有签约数据。 如果(向对端)报告成功，这个参数应该出现，除非请求消息中明确包含了"skip subscriber data"指示

5.2.1.2 HSS 行为

HSS收到该消息，先检查是否存在与请该求消息中的IMSI匹配的用户。如果没有匹配的用户，则HSS返回DIAMETER_ERROR_USER_UNKNOWN。然后HSS查检该IMSI用户是否有签约数据，如果该IMSI用户没有任何类型的签约（EPS、GPRS、CS），则返回DIAMETER_ERROR_USER_UNKNOWN。

HSS检查用户是否有APN配置数据或者GPRS签约数据，如果没有任何APN配置数据或者GPRS签约数据，且该请求消息是来自S6d接口，HSS在响应消息返回DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION。

HSS检查用户是否有APN配置数据，如果没有任何APN配置数据 且该请求消息是来自S6a接口，HSS在响应消息返回DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION。

HSS根据UE的签约检查当前UE所用的RAT类型是否允许，如果不允许，返回DIAMETER_ERROR_RAT_NOT_ALLOWED。

HSS检查UE是否因为签约了ODB而不允许在VPLMN漫游，如果不允许漫游则返回DIAMETER_ERROR_ROAMING_NOT_ALLOWED。

如果消息来自S6a接口，HSS发送CLR给前一个MME，Cancellation-Type取值为MME_UPDATE_PROCEDURE，同时HSS保存当前服务的MME标识代替原来的MME标识，并且将“UE purged in MME”标志位清除。如果该消息中包含了"Single-Registration-Indication"指示，HSS则发送一个CLR（Cancellation-Type SGSN_UPDATE_PROCEDURE）给HSS中的SGSN，并删除其存储的SGSN地址和SGSN 点码。如果MME指示了“Initial-Attach-Indicator”且HSS内存储了SGSN信息，则无论消息中是否携带了"Single-Registration-Indication",HSS都会发送CLR给当前注册的SGSN，并删除其存贮的SGSN 地址和SGSN点码。Cancellation-Type取值为INITIAL_ATTACH_PROCEDURE。

如果消息从S6d接口上来，HSS应该发送CLR给前一个SGSN，Cancellation-Type 取值为SGSN_UPDATE_PROCEDURE。同时保存当前服务SGSN-Identity的标识代替原来的SGSN信息，并且将“UE purged in SGSN”标志位清除。如果SGSN指示了“Initial-Attach-Indicator”，且HSS存在MME注册信息，则应该也给当前注册的MME发送一个CLR，Cancellation-Type 取值为INITIAL_ATTACH_PROCEDURE。

注：如果CLR消息通过S6d接口发送，则该消息通过DIAMETER消息发送给旧的SGSN；如果CLR消息通过Gr接口发送，则这些信息需要封装在MAP消息中发送给旧的SGSN。

如果在该消息中收到的IMEI有15位，则HSS可以丢弃第15位，保留前14位。

如果在该消息中包含一系列激活的APN，则HSS删除原来保存的动态PDN GW信息，并保存新的PGW信息。

如果从s6a接口收到ULR，并且HSS中设置了URRP-MME参数，则HSS应该清除原来存储的URRP-MME参数，并发送指示给相应的业务实体。

如果从s6d接口收到ULR，并且HSS中设置了URRP-SGSN参数，则HSS应该清除原来存储的URRP-SGSN参数，并发送指示给相应的业务实体。

如果前面的步骤都已成功，且"skip subscriber data" 标志位没有设置，则HSS应该在ULA中携带签约数据给MME/SGSN，携带哪些数据具体要看ULR-Flags和MME以及SGSN的特性支持情况。并返回DIAMETER_SUCCESS。

HSS发送给MME/SGSN的响应消息中的签约数据APN-Configuration-Profile中应该包含默认APN的APN配置和上下文标识，默认APN不能是通配APN。以下三种情况下，该响应消息中应该包含GPRS签约：

——请求消息中，业务节点通过 ULR-Flags 指示要求携带 GPRS 签约数据；

——对于只支持 3GPP R8 之前消息的 SGSN，HSS 通过 IWF 返回用户的签约数据；

——消息来自 S6d 接口，但是 HSS 中没有 APN 配置。

如果HSS在响应消息中携带了GPRS签约，HSS应该保存ULR-Flags中的GPRS-Subscription-Data-Indicator 标志，以便于后续签约数据更新流程。

在响应消息中，对于UE的Call-Barring-Infor-List data的签约数据，HSS根据服务节点是否支持这些能力决定是否下发。由于只有SGSN支持SMS，所以如果HSS发现这个服务节点是一个独立的MME，则不下发SMS相关信息。

HSS保存请求消息中ULR-Flags中的Node-Type-Indicator标志，以便于后续签约数据更新流程。

Subscription-Data信元中应包含Subscriber-Status子信元。如果Subscriber-Status子信元的值为"OPERATOR_DETERMINED_BARRING"，则还应包含Operator-Determined-Barring信元和HPLMN-ODB信元。

如果UE的签约数据Access-Restriction-Data中至少有一个被限制项，则HSS在响应消息中应该带上Access-Restriction-Data信元。

在响应消息的Subscription-Data信元中应包含AMBR 子信元。APN-Configuration信元中应包含EPS-Subscribed-QoS-Profile和AMBR子信元。

在Specific-APN-Info信元中需要包含因为签约通配APN而授权访问的APN动态信息。这样做的目的是通知MME。

如果HSS给对方返回DIAMETER_SUCCESS，则响应消息中ULA-Flags信元中的Separation Indication应该置位。

5.2.2 删除位置消息(CLR/CLA)

5.2.2.1 消息内容

由HSS发起请求消息到MME/SGSN，用于删除MME/SGSN上的订阅信息。触发场景为HSS中动态数据改变（MME/SGSN地址切换）或者此用户在HSS被销户、IMSI被修改，MME/SGSN收到此消息后删除该用户所有数据，此用户在MME中不再是有效用户。如果MME/SGSN收到的消息中取消类型是“初始附着过程”，则不应删除签约数据。表3和表4分别是删除位置请求消息和删除位置响应消息的信息单元列表。

表3 删除位置请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户身份标识，主要是指IMSI
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
Cancellation Type	Cancellation-Type	必选	删除类型定义: - MME-Update Procedure：MME更新流程 - SGSN-Update Procedure：SGSN更新流程 - Subscription Withdrawal：取消签约数据 - Update Procedure_IWF.：有IWF参与的更新流程 - Initial Attach Procedure：初始附着流程
注：IWF用于在Gr接口和S6a/S6d接口之间进行MAP到DIAMETER进行转换的功能实体			

表4 删除位置响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码
注：IWF用于在Gr接口和S6a/S6d接口之间进行MAP到DIAMETER进行转换的功能实体			

5.2.2.2 HSS 行为

该消息主要用于HSS发现该UE被销户或者该UE移动到一个新的MME或者SGSN，通知旧的MME/SGSN。

如果用户是销户处理，则HSS将该消息的Cancellation Type设置为"Subscription Withdrawal"。

如果UE移动到新的MME，则HSS将该消息的Cancellation Type设置为"MME Update Procedure"。

如果UE移动到新的SGSN，则HSS将该消息的Cancellation Type设置为"SGSN Update Procedure"。

如果UE发起的注册是一个初始的注册流程，则HSS将该消息的Cancellation Type设置为"Initial Attach Procedure"。

5.2.3 清除用户消息(PUR/PUA)

5.2.3.1 消息内容

PUR消息由MME/SGSN发送给HSS指示去附着用户的签约数据和MM上下文已经删除。在显式或隐式去附着UE以后，MME可以立刻删除用户的签约数据，并发起PUR消息；MME也可以将用户的数据保留一段时间，然后再删除并发起PUR消息。

表5和表6分别是清除用户请求消息和清除用户响应消息的信息单元列表。

表5 清除用户请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户身份标识，主要是指IMSI.
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

表6 清除用户响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表。
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。Experimental-Result用于指示S6a/S6d的错误，包括： - User Unknown 用户不存在
PUA-Flags	PUA-Flags	条件可选	这个参数包含比特掩码。只有Result-Code为DIAMETER_SUCCESS时，这个参数才会出现

5.2.3.2 HSS 行为

收到 Purge UE 的请求后，HSS 检查 IMSI，如果无法识别，则返回 DIAMETER_ERROR_USER_UNKNOWN；如果 IMSI 可以识别，则设置返回码 DIAMETER_SUCCESS，并将 Original-Host 和存贮的 MME-Identity 以及 SGSN-Identity 比较。

——如果与 MME-identity 和 SGSN-Identity 两个都匹配，则在响应结果中对"freeze M-TMSI"和"freeze P-TMSI" 进行置位，并在数据库中设置"UE purged in MME"和"UE purged in SGSN"标志位。

——如果只与 MME-identity 匹配，则在响应结果中设置"freeze M-TMSI"标志位，并在数据库中设置"UE purged in MME"。

——如果只与 SGSN-identity 匹配，则在响应结果中设置"freeze P-TMSI"标志位，并在数据库中设置"UE purged in SGSN"。

——如果都不匹配，则在响应结果中清除"freeze M-TMSI"和"freeze P-TMSI"的置位。

5.2.4 插入用户数据(IDR/IDA)

5.2.5 消息内容

由HSS发起请求到MME/SGSN，用于向MME/SGSN增加用户数据，或者更新MME/SGSN上的用户数据。

触发场景如下：

a） 用户签约了新的数据，或者签约数据发生变化；

b） 运营商给用户启用、改变或者删除了 ODB；

c） 激活 MME 或 SGSN 的跟踪业务（可选）；

d） HSS 向 MME/SGSN 订阅 UE 可达性通知；

e） 通知 MME 或 SGSN 报告用户当前位置信息或状态信息。

表 7 和表 8 分别是插入用户数据请求消息和插入用户数据响应消息的信息单元列表。

表7 插入用户数据请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户身份标识，主要是指IMSI
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
Subscription Data	Subscription-Data	必选	这个参数包含要么向MME/SGSN增加的，要么更换现有MME/ SGSN存储的部分用户签约数据
IDR-Flags	IDR-Flags	条件可选	这个参数包含比特掩码

表8 插入用户数据响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示S6a/S6d的错误，包括： - User Unknown 用户不存在
IDA-Flags	IDA-Flags	条件可选	这个参数包含比特掩码。
EPS-User-State	EPS-User-State	条件可选	这个参数包含EPS用户的状态。 在IDR消息中，如果请求的是EPS用户，这个参数将出现

5.2.5.1 HSS 行为

HSS利用IDR消息来更新MME/SGSN中的部分特定用户数据，或者增加特定的用户数据。

如果HSS中Subscriber-Status的值发生变化，需要通过该消息通知给MME/SGSN。如果Subscriber-Status设置为"SERVICE_GRANTED"，则表示要删除所有的ODB；如果Subscriber-Status AVP设置为OPERATOR_DETERMINED_BARRING，则the Operator-Determined-Barring AVP或者HPLMN-ODB AVP应该包含在Subscription-Data AVP中。

如果HSS中ARD发生变化，则该消息中应该包含ARD，并通知MME/SGSN。

如果HSS中增加或者修改了UE级别的APN-OI-Replacement，则该消息中应该包含该信息，并通知给MME/SGSN。

当 HSS 中发生以下情况发生时，该消息中的 Subscription-Data AVP 中应该包含 APN-Configuration-Profile 子信元：

——至少增加或者修改了一个 APN。此时签约数据中应该包含具体的 APN 配置，或者

——默认 APN 被修改，此时应该包含默认 APN 的上下文标识和其对应的 APN 配置，默认 APN 不能是通配 APN。

EPS-Subscribed-QoS-Profile和AMBR是APN配置中的必选参数。

如果之前的ULR中携带了GPRS-Subscription-Data-Indicator，则HSS利用IDR来更新SGSN或者MME/SGSN联合体中的GPRS签约数据，或者为它们增加PDP上下文数据。

如果HSS收到相关业务实体（如IP-SM-GW）的订阅消息（如MAP ATM或者Sh-Subs-Notif）通知HSS UE的可达性：

——HSS 应该将用户可达性相关的签约数据和 URRP-MME 和 URRP-SGSN 参数关联起来。

——并且，如果 URRP-MME 和/或 URRP-SGSN 参数没有设置（即至少要有一个），则 HSS 设置 URRP-MME 和/或 URRP-SGSN 参数，

——并且发送一个 IDR 给注册的 MME 或者 SGSN，并设置"UE Reachability Request flag"标志位，以便 UE 可达时由 MME/SGSN 通知 HSS。

如果IDR被用作UE可达性管理或者用于向MME/SGSN请求EPS用户状态，则消息中应该包含Subscription-Data信元并设置为空（无子信元）。

如果HSS中更改了通配APN中的信息，则需要消息中携带当前存储的通配APN对应的特定动态APN信息。

HSS收到了带 "SGSN Area Restricted"的IDA消息，需要在数据库记录"SGSN area restricted"。

5.2.6 删除用户数据(DSR/DSA)

5.2.6.1 消息内容

由HSS发起请求到MME/SGSN，用于删除在MME中存储的HSS用户签约清单。这些业务清单包括：

a）在 MME 中用户的 ESP 签约数据（APN 配置签约数据）的子集或者全部；

b）区域漫游签约信息；

c）用户计费特征；

d）SRVCC 的会话传输号码；

e）跟踪业务数据（可选）。

触发场景为HSS中的签约数据改变，MME收到此消息后只是删除部分用户数据，此用户在MME仍然是有效用户。

表9和表10分别是删除用户数据请求消息和删除用户响应消息的信息单元列表。

表9 删除用户数据请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户身份标识，主要是指IMSI
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
DSR Flags	DSR-Flags	必选	这个参数包含比特掩码
Trace Reference	Trace- Reference	条件可选	这个参数包含的值用于激活跟踪会话。 只有当DSR-Flags的设置"Trace Data Withdrawal"位时，此参数才出现
Context Identifier	Context-Identifier	条件可选	这个参数用于指示被删除的PDN签约的上下文索引或者GPRS-PDP上下文索引。 只有在DSR-Flag的"PDN subscription contexts Withdrawal"比特位被置，或者"PDP context withdrawal"比特位被置时，这个参数才出现。 在"PDN subscription contexts Withdrawal"比特位被置的情况下，Context-Identifier取值不应该为默认APN的取值。 为了和3GPP TS 29.002[24]定义的MAP协议兼容，这个参数取值不能为0
TS Code List	TS-Code	条件可选	这个参数包含用户被删除的TS码。 只有DSR-Flag中的"SMS Withdrawal"比特位被置，并且SMS关联的TS码被删除时，这个参数才出现
SS Code List	SS-Code	条件可选	这个参数包含需要删除的该用户的补充业务码。 只有DSR-Flag中的"SMS Withdrawal"比特位被置，或者"LCS Withdrawal"比特位被置时，这个参数才出现

表10 删除用户数据响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表。
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示S6a/S6d的错误，包括： - User Unknown 用户不出现
DSA Flags	DSA-Flags	条件可选	这个参数包含比特掩码。

5.2.6.2 HSS 行为

HSS利用此过程删除MME或者SGSN上的签约数据。

如果HSS在通过MME发的ULR消息中收到了GPRS-Subscription-Data-Indicator，并在ULA中下发了GPRS签约数据，HSS也要删除SGSN或者MME/SGSN联合体上的GPRS签约数据。

由于MME至少要有一个默认APN，故HSS给MME发送DSR时不允许设置"Complete APN Configuration Profile Withdrawal" 标志位。

收到DSA后，如果携带了"SGSN Area Restricted"，则设置数据库的"SGSN area restricted"标志位。

5.2.7 鉴权信息消息(AIR/AIA)

5.2.7.1 消息内容

由MME/SGSN发起请求到HSS，用于从HSS上获取鉴权信息。表11和表12分别是鉴权信息请求消息和鉴权信息响应消息的信息单元。

表11 鉴权信息请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户标识，主要是指IMSI
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
Requested E-UTRAN Authentication Info	Requested-EUTRAN-Authentication-Info	条件可选	这个参数包含E-UTRAN鉴权请求相关的信息
Requested UTRAN/GERAN Authentication Info	Requested-UTRAN-GERAN Authentication-Info	条件可选	这个参数包含UTRAN或者GERAN鉴权请求相关的信息
Visited PLMN ID	Visited-PLMN-ID	必选	这个参数包含拜访域PLMN的MCC和MNC，详细定义依据3GPP TS23.003[3]

表12 鉴权信息响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示S6a/S6d的错误，包括： - User Unknown 用户不出现 - Unknown EPS Subscription: 用户没有签约的EPS
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
Authentication Info	Authentication-Info	条件可选	这个参数包含鉴权向量

5.2.7.2 HSS 行为

HSS收到该消息，先检查是否存在与请该求消息中的IMSI匹配的用户。如果没有匹配的用户，则HSS返回DIAMETER_ERROR_USER_UNKNOWN。然后HSS查检该IMSI用户是否有签约数据，如果该IMSI用户没有任何类型的签约（EPS、GPRS、CS），则返回DIAMETER_ERROR_USER_UNKNOWN。

HSS检查用户是否有APN配置数据或者GPRS签约数据，如果没有任何APN配置数据或者GPRS签约数据，且该请求消息是来自S6d接口，HSS在响应消息返回DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION。

HSS检查用户是否有APN配置数据，如果没有任何APN配置数据 且该请求消息是来自S6a接口，HSS在响应消息返回DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION。

HSS到AuC中请求鉴权矢量。如果在该消息中有Immediate-Response-Preferred AVP，根据负载状态或者其他考虑，可以产生少于MME/SGSN请求的鉴权矢量数。

如果请求消息中请求的是EUTRAN-Authentication-Info，HSS根据AuC产生的鉴权矢量生成KASME，并在响应消息中发给MME或者合设的MME/SGSN。

在请求消息中有Immediate-Response-Preferred AVP时，由于这个UE不允许附着而导致的AuC不能计算鉴权矢量（比如用户签约的是SIM卡，而UE通过E-UTRAN接入到网络），HSS则发DIAMETER_AUTHORIZATION_REJECTED给MME/SGSN，在响应消息不携带鉴权矢量。否则，如果是由于目前没有可用的鉴权矢量，且AuC不能计算鉴权矢量的情况下，HSS发DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE。

KASME计算方法依据3GPP TS 33.401。如果请求的是EUTRAN-Authentication-Info AVP，则HSS下载E-UTRAN鉴权矢量给MME，如果请求的是UTRAN-GERAN-Authentication-Info AVP，则HSS下载UTRAN或者GERAN鉴权矢量给SGSN。

如果HSS在该消息中收到Immediate-Response-Preferred AVP，HSS在返回给MME/SGSN的鉴权矢量的数量可能会少于请求的数量；如果在请求消息中有E-UTRAN和UTRAN/GERAN鉴权矢量，并且其中有一个带有Immediate-Response-Preferred信元，则HSS可能只返回带有Immediate-Response-Preferred信元的矢量；对于E-UTRAN的鉴权矢量，HSS一定计算出KASME。

如果请求消息中有Re-Synchronization-Info AVP，HSS要检查AUTS，具体的方法依据3GPP TS 33.102；如果请求消息中同时存在E-UTRAN和UTRAN-GERAN鉴权矢量请求，且两个鉴权矢量中都有Re-Synchronization-Info AVP，则HSS不应检查AUTS,直接返回DIAMETER_UNABLE_TO_COMPLY，响应消息中不携带任何鉴权矢量。

5.2.8 重启消息(RSR/RSA)

5.2.8.1 消息内容

由HSS发起请求到MME/SGSN,用于通知MME/SGSN，HSS发生了重启，可能丢失了部分用户的漫游信息。表13和表14分别是重启请求消息和重启响应消息的信息单元列表。

表13 重启请求消息

信息单元名称	映射到Diameter AVP	类别	描述
User Id List	User-Id	可选	这个参数包含一个用户标识列表，一个用户标识一般为IMSI前缀，用来标识包含该IMSI前缀的一类用户。当HSS发生故障的时候，如果受影响用户局限于一个或者多个IMSI号段，则此参数应该出现
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

表14 重启响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示S6a/S6d的错误,在这个消息中没有Experimental-Result返回码

5.2.8.2 HSS 行为

HSS重启后，可能会丢失部分给用户提供服务的MME/SGSN信息，后续HSS可能不能正常的给这些网元下发CLR、IDR、DSR等操作。所以当HSS重启后，采用该消息通知与其相关的MME、SGSN、或者合设的MME/SGSN。如果HSS发现HSS自身的故障只是引起了一部分IMSI号段的用户有问题，则在该消息中携带这部分有问题的IMSI信元，以便控制影响范围。

如果HSS知道与其关联的MME/SGSN是一个合设的MME/SGSN，则HSS只通知一次。

5.2.9 通知消息 (NOR/NOA)

5.2.9.1 消息内容

由MME/SGSN发起请求消息到HSS，用于通知HSS更改终端的信息，通知的内容包括：

a）用户终端信息的更新（IMEI，IMEISV）；

b）APN 的 PDN GW 的指派变化或者删除；

c）向当前服务的 SGSN 发送删除位置消息。

表 15 和表 16 分布是通知请求消息和通知响应消息的信息单元列表。

表15 通知请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户标识，主要是指IMSI
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
Terminal Information	Terminal-Information	条件可选	这个参数包含用户移动终端的设备信息。 当需要通知HSS任何终端信息变化时，MME/SGSN将在请求消息中携带新的终端信息 在S6a/S6d接口中，只有IMEI和Software-Version这两个AVP包含在这个信元中
PDN GW Identity	MIP6-Agent-Info	条件可选	这个参数包含了为APN选择或者动态分配的PDN-GW标识。 如果用户允许通过非3GPP网络接入且选择了一个新的PDN-GW时，该参数应携带。 如果需要通知HSS重新选择了一个新的PDN-GW，MME/SGSN需要在通知请求消息中携带此参数。 如果需要通知HSS移除APN的PDN-GW，MME/SGSN在通知请求消息中则不携带该参数
PGW PLMN ID	Visited-Network-Identifier	条件可选	这个参数包含了被分配的PDN GW所处的PLMN标识。如果PDN GW标识参数存在，则这个参数也应该出现。 当通知HSS删除某个APN的PDN GW时，这个参数不应该存在

表15（续）

信息单元名称	映射到Diameter AVP	类别	描述
Context Identifier	Context-Identifier	可选	这个参数用来标识当前被指派或者删除的PDN-GW相关的APN配置。 如果需要操作的PDN-GW存在且关联某一具体的APN而不是所有APN，那么该参数需要携带。 当通知HSS移除已经分配给APN的PDN-GW时，该参数需要携带。 如果通知请求标识设为“删除所有APN以及相关的PDN-GW”，该参数不携带。 为了与3GPP TS 29.002 [24]定义的MAP协议相兼容，该参数的值不能为0
APN	Service-Selection (See IETF RFC 5778 [20])	条件可选	这个参数包含了为APN选择或者动态分配的PDN-GW标识，如果所操作的PDN-GW存在且关联某一具体的APN而不是所有APN，那么该参数需要携带。 当通知HSS移除已经分配给APN的PDN-GW时，该参数需要携带。 如果通知请求标识设为“删除所有APN以及相关的PDN-GW”，该参数不携带
Alert Reason	Alert-Reason	条件可选	该参数指示移动用户在网或者MS内存可用。 在通知HSS目标用户在网或者UE内存可用而可以接收一条或者多条短消息时，该参数需要携带
NOR Flags	NOR-Flags	条件可选	该信元为一串比特标识，如果该信元未携带则认为所有的比特位取值为“0”。 当通知HSS需要向当前的SGSN下发“取消位置”消息时，MME需要在NOR-Flags中设置“Single-Registration-Indication”标识。 当通知HSS当前的SGSN区域为受限状态时，SGSN需要在NOR-Flags中设置“SGSN area restricted”标识。 当通知HSS用户在网或者UE内存可用而可以接收一条或多条短消息时，SGSN需要在NOR-Flags中设置“Ready for SM”标识。 当通知HSS用户重新可及时，MME需要在NOR-Flags中设置“UE Reachable”标识。 当通知HSS需要删除动态存储的所有的APN以及相关的PDN-GW相关数据时，MME需要在NOR-Flags中设置“Delete all APN and PDN GW identity pairs”标识

表16 通知响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示S6a/S6d的错误，包括： - User Unknown 用户不存在
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

5.2.9.2 HSS 行为

HSS 检查请求消息中的 IMSI 是否有签约，如果 IMSI 没有签约，HSS 则返回 DIAMETER_ERROR_USER_UNKNOWN。如果该 IMSI 在 HSS 有签约，HSS 进一步检查该请求消息中的 MME/SGSN 是否是给该 UE 提供服务的 MME/SGSN；如果不是，HSS 则返回 DIAMETER_ERROR_UNKNOWN_SERVING_NODE。如果该 IMSI 是签约的，且 MME/SGSN 是给该 UE 提供服务的 MME/SGSN，则 HSS 进行下面的处理：

—— 如果该消息中包含了终端信息，HSS 则保存该信息。

—— 如果该消息中包含了 APN 和其对应的 PDN GW 信息：

- HSS 检查这个 APN 是不是签约的 APN，其对应 PDN GW 是否为动态分配的，如果是，HSS 保存 PDN GW 和 PLMN ID；
- 如果这个 APN 不是签约的 APN，HSS 检查 UE 是否有签约的通配 APN，如果有，则 HSS 保存 PDN GW 和 PLMN ID 以及请求消息中的 APN 到 APN 的签约配置中；
- 如果以上条件均不满足，则 HSS 返回 DIAMETER_ERROR_UNABLE_TO_COMPLY。

—— 如果在该消息中有“restricted”指示，HSS 则在该位置区域标识为 "restricted"[注]。

——如果该消息中包含了 Single-Registration-Indication 指示，HSS 则给 SGSN 发送 CLR 消息。

—— 当 UE 可达后，HSS 收到 MME 通过 S6a 接口的消息，指示 UE 从 MME 可达，并且 HSS 中设置了 URRP-MME 参数，则 HSS 应该清除 URRP-MME 参数，并发送指示给相应的业务实体。

—— 当 UE 可达后，HSS 收到 SGSN 通过 S6d 接口的消息，指示 UE 从 SGSN 可达，并且 HSS 中设置了 URRP-SGSN 参数，则 HSS 应该清除 URRP-SGSN 参数，并发送指示给相应的业务实体。

——如果 HSS 通过 S6d 收到 SGSN 发来的 Alert Reason 信息，则 HSS 重置 MNRG 标志位并发送 MAP-Alert-Service-Centre 消息。

注：“restricted”标识适用于 SGSN，不适用于 MME。

5.3 信息单元

5.3.1 Subscription-Data

用户签约数据结构为 Grouped 类型，包含了与 EPS 和 GERAN/UTRAN 相关的用户特征信息。

AVP 格式如下:

```
Subscription-Data ::= <AVP header: 1400 10415>
                      [ Subscriber-Status ]
                      [ MSISDN ]
                      [ STN-SR ]
                      [ ICS-Indicator ]
                      [ Network-Access-Mode ]
                      [ Operator-Determined-Barring ]
                      [ HPLMN-ODB ]
                      *10[ Regional-Subscription-Zone-Code]
                      [ Access-Restriction-Data ]
                      [ APN-OI-Replacement ]
                      [ LCS-Info ]
```

[Teleservice-List]
[Call-Barring-Infor-List]
[3GPP-Charging-Characteristics]
[AMBR]
[APN-Configuration-Profile]
[RAT-Frequency-Selection-Priority-ID]
[Trace-Data]
[GPRS-Subscription-Data]
*[CSG-Subscription-Data]
[Roaming-Restricted-Due-To-Unsupported-Feature]
*[AVP]

AMBR 参数包含用户签约的 UE-AMBR 数据信息，APN-OI-Replacement 参数包含用户签约的终端级别的 APN-OI-Replacement。

5.3.2 Terminal-Information

终端信息结构为 Grouped 类型，包含了用户终端的信息。

AVP 格式如下：

Terminal Information ::= <AVP header: 1401 10415>
[IMEI]
[3GPP2-MEID]
[Software-Version]
*[AVP]

5.3.3 IMEI

国际移动台识别码(IMEI)用于唯一地识别一个移动台设备，UTF8String 格式，为一个 14 位的十进制数字，其构成为：TAC(8 个数字) +SNR(6 个数字)。

也有可能包含第 15 个十进制数字，第 15 个数字作为校验位。

5.3.4 Software-Version

软件版本号格式为 UTF8String。SVN 为 2 个数字，SVN 由生产厂商自行分配，其中 99 不用。

5.3.5 3GPP2-MEID

3GPP2-MEID 是 OctetString 类型。这个参数包含用户终端的移动设备标识。

5.3.6 ULR-Flags

位置更新请求标识是 Unsigned32 的比特掩码，其中各比特位代表的含义如表 17 所示。

表17 ULR-Flags

Bit	名称	描述
0	Single-Registration-Indication	该比特位置位时，指示HSS向SGSN下发位置取消消息，当SGSN发起位置更新请求时不设置该指示
1	S6a/S6d-Indicator	该比特位置位时，指示ULR消息通过S6a接口过来，对端节点为MME(或者为MME/SGSN，但通过E-UTRAN附着) 该比特位清除时，指示ULR消息通过S6d接口过来，对端节点为SGSN(或者为MME/SGSN，但通过UTRAN或者GERAN附着)

表17（续）

Bit	名称	描述
2	Skip Subscriber Data	该比特位置位时，HSS在位置更新流程中不进行用户数据插入，如果该用户在上一次位置更新成功之后，其在HSS中的签约数据发生了改变，则HSS将忽略该指示对MME/SGSN进行数据更新。如果HSS对忽略用户数据指示生效，则GPRS签约数据指示将被忽略
3	GPRS-Subscription-Data-Indicator	该比特位置位时，表示HSS会在ULA响应消息中返回GPRS定义数据，GPRS-Subscription—Data参数将包含在Subscription-Data参数中。 否则，当位置更新请求消息从S6a接口过来，并且HSS没有存储用户的EPS订阅数据，或者当用户数据是从Pre-Rel-8 HSS(通过IWF)返回的时候，HSS不会在ULA响应消息中携带GPRS-Subscription-Data参数。 独立的MME发送ULR时，不会设置该比特
4	Node-Type-Indicator	该比特位置位时，指示请求节点类型为MME/SGSN的合一类型，该比特位清除时，指示请求节点类型为单一的MME或者SGSN类型，此时，如果S6a/S6d指示也为1，HSS将忽略对仅在SGSN上应用的特性的检测，从而跳过将SMS相关的签约数据下载到单独的MME
5	Initial-Attach-Indicator	该比特位置位时，指示HSS需要向当前已经登记的MME/SGSN下发取消位置登记消息
6	PS-LCS-Not-Supported-By-UE	该比特位置位时，指示HSS该用户设备不能支持基于任何PS域的LCS业务方式，MME/SGSN根据用户设备的能力信息和其自身的接入技术设置该比特位
注：以上未定义的其他比特位，MME/SGSN在发送时将全部清除，HSS收到后不需对其进行处		

5.3.7 ULA-Flags

位置更新应答标识是 Unsigned32 的比特掩码，其中各比特位代表的含义如表 18 所示。

表18 ULA-Flags

Bit	名称	描述
0	Separation Indication	该比特位置位时，指示HSS将SGSN号码和MME号码分离存储，HSS在R8版本之后支持设置该指示值，R8版本之前该值为0
注：以上未定义的其他比特位，HSS在发送时将全部清除，MME/SGSN收到后不需对其进行处理		

5.3.8 Visited-PLMN-Id

拜访网络标识格式为 OctetString.，包含了移动国家码（MCC）和移动网络号码（MNC），其编码后的格式如表 19 所示。

当 MCC 或者 MNC 的长度少于 3 个数字时，未使用部分填充“1111”。

表19 Visited-PLMN-Id AVP 编码格式

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

5.3.9 Feature-List AVP

特性列表参数定义依据 3GPP TS 29.229。在 S6a/S6d 应用中，每个比特位的含义见表 20。

表20 S6a/S6d 中 Feature-List-ID 的特性

特性比特	特性	类别	描述
0	ODB-all-APN	可选	运营商闭锁全部PS域业务 该特性在位置更新请求/响应和插入用户数据请求/响应流程中应用。 如果MME/SGSN不支持该特性，HSS则不在位置更新响应中发送该类型的ODB，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该ODB数据，如果MME/SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息
1	ODB-HPLMN-APN	可选	当用户在拜访网络漫游时，运营商闭锁其归属网络的全部PS域业务 该特性在位置更新请求/响应和插入用户数据请求/响应流程中应用。 如果MME/SGSN不支持该特性，HSS则不在位置更新响应中发送该类型的ODB，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该ODB数据，如果MME/SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息
2	ODB-VPLMN-APN	可选	当用户在拜访网络漫游时，运营商闭锁其拜访网络的全部PS域业务 该特性在位置更新请求/响应和插入用户数据请求/响应流程中应用。 如果MME/SGSN不支持该特性，HSS则不在位置更新响应中发送该类型的ODB，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该ODB数据，如果MME/SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息
3	ODB-all-OG	可选	运营商闭锁用户的全部出呼业务 该特性只在SGSN的位置更新请求/响应和插入用户数据请求/响应流程中应用，对于MME不发送该ODB类型。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送该类型的ODB，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该ODB数据，如果SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息
4	ODB-all- International OG	可选	运营商闭锁用户的全部国际出呼业务 该特性只在SGSN的位置更新请求/响应和插入用户数据请求/响应流程中应用，对于MME不发送该ODB类型。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送该类型的ODB，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该ODB数据，如果SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息
5	ODB-all-International OGNotToHPLMN-Country	可选	运营商闭锁用户除归属网络国家之外的全部国际出呼业务 该特性只在SGSN的位置更新请求/响应和插入用户数据请求/响应流程中应用，对于MME不发送该ODB类型。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送该类型的ODB，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该ODB数据，如果SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息

表20（续）

特性比特	特性	类别	描述
6	ODB-all-Interzonal OG	可选	运营商闭锁用户的全部跨地区出呼业务 该特性只在SGSN的位置更新请求/响应和插入用户数据请求/响应流程中应用，对于MME不发送该ODB类型。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送该类型的ODB，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该ODB数据，如果SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息
7	ODB-all-Interzonal OGNotToHPLMN-Country	可选	运营商闭锁用户除归属网络国家之外的全部跨地区出呼业务 该特性只在SGSN的位置更新请求/响应和插入用户数据请求/响应流程中应用，对于MME不发送该ODB类型。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送该类型的ODB，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该ODB数据，如果SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息
8	ODB-all-Interzonal OGAndInternational OGNotToHPLMN-Country	可选	运营商闭锁用户除归属网络国家之外的全部国际出呼业务，同时闭锁所有跨地区出呼业务。 该特性只在SGSN的位置更新请求/响应和插入用户数据请求/响应流程中应用，对于MME不发送该ODB类型。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送该类型的ODB，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该ODB数据，如果SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息
9	RegSub	可选	地域性签约业务 该特性在位置更新请求/响应、插入用户数据请求/响应以及删除用户数据请求/应答流程中应用。 如果MME/SGSN不支持该特性，HSS则不在位置更新响应中发送该地域签约区号，而直接拒绝该次位置更新。 HSS在插入用户数据请求中发送了该地域签约区号数据，如果MME/SGSN在响应消息中未指示支持该特性，HSS则将禁止该用户漫游同时下发取消位置消息
10	Trace	可选	跟踪功能 该特性在位置更新请求/响应、插入用户数据请求/响应以及删除用户数据请求/应答流程中应用。 如果MME/SGSN不支持该特性，HSS则不在位置更新响应中发送跟踪数据信息。 HSS在插入用户数据请求中发送了跟踪数据，如果MME/SGSN在响应消息中未指示支持该特性，HSS将保存该指示，不再发送跟踪数据到该MME/SGSN。 HSS在删除用户数据请求中发送了跟踪数据，如果MME/SGSN在响应消息中未指示支持该特性，HSS将保存该指示，不再发送跟踪数据到该MME/SGSN

表20（续）

特性比特	特性	类别	描述
21	SM-MO-PP	可选	短消息MO-PP 这个特性 一般用于ULR/ULA和IDR/IDA消息对中。 如果MME或者SGSN不支持这个特性，HSS不会在ULA响应消息中返回SMS相关的信息给MME或者SGSN。 如果MME或者SGSN在IDA中不支持这个 特性，并且HSS已经在IDR中下发了SMS相关信息，那么HSS要存在这个表示，在以后的消息中不再下发SMS相关信息给MME或者SGSN
22	Barring-OutgoingCalls	可选	出呼闭锁业务 该特性通过S6d接口在位置更新请求/响应和插入用户数据请求/响应答流程中应用。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送短消息数据信息。 HSS在插入用户数据请求中发送了短消息数据，如果SGSN在响应消息中未指示支持该特性，HSS将保存该指示，不再发送跟踪数据到该SGSN
23	BAOC	可选	出呼闭锁业务 该特性通过S6d接口在位置更新请求/响应和插入用户数据请求/响应答流程中应用。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送短消息数据信息。 HSS在插入用户数据请求中发送了短消息数据，如果SGSN在响应消息中未指示支持该特性，HSS将保存该指示，不再发送跟踪数据到该SGSN
24	BOIC	可选	国际出呼闭锁业务 该特性通过S6d接口在位置更新请求/响应和插入用户数据请求/响应答流程中应用。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送短消息数据信息。 HSS在插入用户数据请求中发送了短消息数据，如果SGSN在响应消息中未指示支持该特性，HSS将保存该指示，不再发送跟踪数据到该SGSN
25	BOICExHC	可选	除归属网络国家的出呼闭锁业务 该特性通过S6d接口在位置更新请求/响应和插入用户数据请求/响应答流程中应用。 如果SGSN不支持该特性，HSS则不在位置更新响应中发送短消息数据信息。 HSS在插入用户数据请求中发送了短消息数据，如果SGSN在响应消息中未指示支持该特性，HSS将保存该指示，不再发送跟踪数据到该SGSN

5.3.10 Requested-EUTRAN-Authentication-Info

EUTRAN 鉴权信息请求是 Grouped 类型，包含对 E-UTRAN 进行鉴权请求的一些信息。参数格式如下：

Requested- EUTRAN-Authentication-Info ::= <AVP header: 1408 10415>
[Number-Of-Requested-Vectors]
[Immediate-Response-Preferred]

[Re-synchronization-Info]

*[AVP]

5.3.11 Requested-UTRAN- GERAN-Authentication-Info

UTRAN/GERAN鉴权信息请求是Grouped类型，包含对UTRAN/GERAN进行鉴权请求的一些信息。参数格式如下：

Requested-UTRAN-GERAN-Authentication-Info ::= <AVP header: 1408 10415>

[Number-Of-Requested-Vectors]

[Immediate-Response-Preferred]

[Re-synchronization-Info]

*[AVP]

5.3.12 RAT-Type

无线接入类型参数是Enumerated类型，用来标识提供服务的无线接入技术，详细请依据3GPP TS 29.212。

5.3.13 Number-Of-Requested-Vectors

鉴权向量请求数是Unsigned32类型，指MME/SGSN准备接收的鉴权向量个数。

5.3.14 Re-Synchronization-Info

重同步信息是OctetString类型，包含了RAND和AUTS信息。

5.3.15 Immediate-Response-Preferred

优先立即响应是Unsigned32类型，该可选标识存在则指示需要优先立即响应，如果不存在则无需优先。

当请求EUTRAN/ UTRAN/ GERAN鉴权向量时，在相应的鉴权向量请求消息中携带该标识指示该鉴权向量需要在MME/SGSN立即使用，HSS将通过该标识来确定向AuC获取鉴权向量的组数和向MME/SGSN下发鉴权向量的组数。

5.3.16 Authentication-Info

鉴权信息是Grouped类型，包含了鉴权向量信息。参数格式如下:

Authentication-Info ::= <AVP header: 1413 10415>

*[E-UTRAN-Vector]

*[UTRAN-Vector]

*[GERAN-Vector]

*[AVP]

5.3.17 E-UTRAN-Vector

E-UTRAN鉴权向量是Grouped类型，包含了E-UTRAN鉴权向量信息。参数格式如下：

E-UTRAN-Vector ::= <AVP header: 1414 10415>

[Item-Number]

{ RAND }

{ XRES }

{ AUTN }

{ KASME }

*[AVP]

5.3.18 UTRAN-Vector

UTRAN鉴权向量是Grouped类型，包含了UTRAN鉴权向量信息。参数格式如下：

UTRAN-Vector ::= <AVP header: 1415 10415>

[Item-Number]

{ RAND }

{ XRES }

{ AUTN }

{ Confidentiality-Key }

{ Integrity-Key }

*[AVP]

5.3.19 GERAN-Vector

GERAN鉴权向量是Grouped类型，包含了GERAN鉴权向量信息。参数格式如下：

GERAN-Vector ::= <AVP header: 1416 10415>

[Item-Number]

{ RAND }

{ SRES }

{ Kc }

*[AVP]

5.3.20 Network-Access-Mode

网络接入模式是Enumerated类型，其取值如下：

a）PACKET_AND_CIRCUIT (0)

b）Reserved (1)

c）ONLY_PACKET (2)

5.3.21 HPLMN-ODB

运营商自定义ODB是Unsigned32类型，其每个比特位包含了运营商对用户签约的一些特殊业务的闭锁操作，详细定义见表21。

表21 HPLMN-ODB

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

如果在用户签约数据中该参数存在，则该签约数据将被置为OPERATOR_DETERMINED_BARRING。如果MME/SGSN收到该参数，则将该信息存储，如果不支持该类型ODB则不进行存储。

5.3.22 Item-Number

项目序号为Unsigned32类型值，如果在一个鉴权信息中包含多组EPS/UTRAN/GERAN鉴权向量，则每组鉴权向量会包含该项目序号，项目序号小的鉴权向量将先被MME/SGSN使用。一次请求中的项目序号是排序的。当前一次请求的鉴权向量使用完后再进行下一次鉴权向量请求。

5.3.23 Cancellation-Type

取消类型为Enumerated类型，其取值如下：

a）MME_UPDATE_PROCEDURE (0)

该取值是在收到一个新的 MME 发起的位置更新消息后向旧的 MME 发起取消位置流程时使用。

b）SGSN_UPDATE_PROCEDURE (1)

该取值是在收到一个新的 SGSN 发起的位置更新消息后向旧的 SGSN 发起取消位置流程时使用。

c）SUBSCRIPTION_WITHDRAWAL (2)

该取值是运营商在 HSS 中注销一个用户向其当前所在的 MME/SGSN 发起取消位置流程时使用。

d）UPDATE_PROCEDURE_IWF (3)

e）INITIAL_ATTACH_PROCEDURE (4)

该取值是在各个 MME/SGSN 启动附着初始化期间收到一个位置更新消息后向 MME/SGSN 发起取消位置流程时使用。

5.3.24 DSR-Flags

删除用户数据请求标识是 Unsigned32 类型，其每个比特位所代表的含义详细描述见表 22。

表22 DSR-Flags

Bit	名称	描述
0	Regional Subscription Withdrawal	当bit0被置位时，指示用户签约的区域签约业务将被删除
1	Complete APN Configuration Profile Withdrawal	当bit1被置位时，指示用户签约的所有EPS APN配置数据将被删除，该bit位仅在S6d接口应用
2	Subscribed Charging Characteristics Withdrawal	当bit2被置位时，指示用户签约的计费特征数据已经被删除
3	PDN subscription contexts Withdrawal	当bit3被置位时，指示上下文标识合法的PDN订阅上下文数据将被删除（注1）
4	STN-SR	当bit3被置位时，表示从用户签约数据中删除SRVCC的会话转换号码
5	Complete PDP context list Withdrawal	当bit5被置位时，指示用户签约的所有PDP上下文数据将被删除
6	PDP contexts Withdrawal	当bit6被置位时，指示上下文标识合法的PDP上下文数据将被删除（注2）
7	Roaming Restricted due to unsupported feature	当bit7被置位时，指示MME/SGSN将从用户签约数据中删除漫游限制数据
8	Trace Data Withdrawal	当bit8被置位时，指示跟踪数据将被删除
9	CSG Deleted	当bit9被置位时，指示MME/SGSN将从用户签约数据中删除CSG签约数据
10	APN-OI-Replacement	当bit10被置位时，指示从用户签约数据中删除终端级别的APN-OI-Replacement。
11	GMLC List Withdrawal	当bit11被置位时，指示MME/SGSN删除用户的GMLC列表信息

表22（续）

Bit	名称	描述
12	LCS Withdrawal	当bit12被置位时，指示MME/SGSN删除用户签约的LCS补充业务数据
13	SMS Withdrawal	当bit13被置位时，指示SGSN删除用户签约的SMS业务以及相关补充业务数据
注1：如果取消全部APN配置数据比特位被置位，则该比特不允许置位。 注2：如果取消全部PDP上下文列表比特位被置位，则该比特不允许置位。 注3：HSS发送DSR消息中，以上定义之外的比特位将全部清除，MME/SGSN无需对其进行处理。 注4：比特3和比特6存在互斥关系，二者不能同时被置位		

5.3.25 DSA-Flags

删除用户数据响应标识是 Unsigned32 类型，其每个比特位所代表的含义详细描述见表 23。

表23 DSA-Flags

Bit	名称	描述
0	Network Node area restricted	当该比特位被置位时，指示由于区域签约业务导致整个网络节点区域被限制
注：SGSN发送DSA消息中，以上定义之外的比特位将全部清除，HSS无需对其进行处理		

5.3.26 Context-Identifier

上下文标识是 Unsigned32 类型。

5.3.27 Subscriber-Status

3GPP 用户状态是 Enumerated 类型值，用来指示业务是否可用，其取值如下：

a）SERVICE_GRANTED (0)　业务可用

d）OPERATOR_DETERMINED_BARRING (1)　运营商闭锁

5.3.28 Operator-Determined-Barring

运营商决定闭锁结构是 Unsigned32 类型，其由一串指示运营商针对用户签约业务进行闭锁的比特位组成，其每个比特代表的含义如表 24 所示。

表24 Operator-Determined-Barring

Bit	描述
0	闭锁所有PS域业务
1	闭锁漫游用户的归属网络接入
2	闭锁漫游用户的拜访网络接入
3	闭锁所有出呼
4	闭锁所有国际出呼
5	闭锁除归属国之外的国际出呼
6	闭锁所有的长途出呼
7	闭锁除归属国之外的长途出呼
8	闭锁除归属国之外的所有国际出呼以及所有长途出呼

如果在用户签约数据中该参数存在，则该签约数据将被置为 OPERATOR_DETERMINED_BARRING；如果 MME/SGSN 收到该参数，则将该信息存储，如果不支持该类型 ODB 则不进行存储。

5.3.29 Access-Restriction-Data

接入限制数据结构是 Unsigned32 类型，其由一串指示是否进行接入限制的比特位组成，其每个比特代表的含义如表 25 所示。

表25 Access-Restriction-Data

Bit	描述
0	UTRAN不允许
1	GERAN不允许
2	GAN不允许
3	I-HSPA-Evolution不允许
4	E-UTRAN不允许
5	HO-To-Non-3GPP-Access不允许

5.3.30 APN-OI-Replacement

APN-OI-Replacement 是 UTF8String 类型。这个参数指示用来替换当依赖 DNS 解决方案创立 PDN GW FQDN 时，非漫游和归属路由漫游情况下的 APN OI 的域名。

APN-OI-Replacement 参数内容被格式化成由多个圆点“.”分隔成特征字符串。

5.3.31 All-APN-Configurations-Inciuded-Indicator

APN 配置内部指示是 Enumerated 类型，其取值如下所示：

a）All_APN_CONFIGURATIONS_INCLUDED (0)

b）MODIFIED/ADDED_APN_CONFIGURATIONS_INCLUDED (1)

5.3.32 APN-Configuration-Profile

APN-Configuration-Profile 是 Grouped 类型。这个参数包含用户关于 EPS 签约的 APN 配置信息。这个参数中的 Context-Identifier 指示每个用户默认的 APN 配置。参数格式如下：

```
APN-Configuration-Profile ::= <AVP header: 1429 10415>
                              { Context-Identifier }
                              { All-APN-Configurations-Included-Indicator }
                              1*{APN-Configuration}
                              *[AVP]
```

一个 IMSI 关联的 Subscription-Data 只有一个 APN-Configuration-Profile。每一个 APN-Configuration-Profile 有一个或者多个 APN-Configuration，每个 APN-Configuration 参数只描述一个 APN 的配置。所以，IMSI 和 APN 之间的关系是 1 对多。

5.3.33 APN-Configuration

APN-Configuration 参数是 Grouped 类型。这个参数包含用户签约的 APN 配置相关信息。这个参数中的 Context-Identifier 指示每个 APN 配置，不能取值为 0。所以，APN-Configuration 参数中的 Context-Identifier 用来唯一指示每个用户的 EPS APN 标识。对于一个有多个 APN 配置的特别的 EPS 用户，Service-Selection 在多个 APN-Configuration 参数中应该是唯一的。参数格式如下：

```
APN-Configuration ::= <AVP header: 1430 10415>
                      { Context-Identifier }
                      * 2 [ Served-Party-IP-Address ]
                      { PDN-Type }
```

{ Service-Selection}
{ EPS-Subscribed-QoS Profile }（可选）
[VPLMN-Dynamic-Address-Allowed]
[MIP6-Agent-Info]
[Visited-Network-Identifier]
[PDN-GW-Allocation-Type]
[3GPP-Charging-Characteristics]
{ AMBR }
*[Specific-APN-Info]
[APN-OI-Replacement]
*[AVP]

AMBR 包含和 AMBR 相关的特别的 APN 配置（APN-AMBR）。

Served-Party-IP-Address 这个参数可能会出现 0、1 或者 2 次。如果是用静态分配 IP 地址，这个参数包含 IPv4 地址，IPv6 地址或者 IPv6 用户前缀。对于 IPv6 的前缀，地址的低 64 位都被设成 0。

参数 EPS-Subscribed-QoS Profile 为可选。

APN-OI-Replacement 参数包含 APN-OI-Replacement 关联的 APN 配置。这里的 APN-OI-Replacement 优先级比用户级别的 APN-OI-Replacement 高。

如果 PGW 是动态分配的，Visited-Network-Identifier 参数指示分配 PGW 的 PLMN 标识。

注：如果内部使用 MAP 通讯，上下文索引取值范围是 1~50。

5.3.34 Service-Selection

Service-Selection 是 UTF8String 类型。这个参数要么包含 APN 网络标识（比如没有运营商标识的 APN），要么包含通配值。这个参数内容会被多个圆点分隔符格式成特征字符串，或者通配 APN。比如只包含一个 ASCII 码“*”。

5.3.35 EPS-Subscribed-QoS-Profile

EPS-Subscribed-QoS-Profile 是 Grouped 类型。这个参数包含承和默认承载的 APN 相关的载网级别的 QoS 参数（QoS 类标识和保持分配优先级）。参数格式如下：

EPS-Subscribed-QoS-Profile ::= <AVP header: 1431 10415>
{ QoS-Class-Identifier }
{ Allocation-Retention-Priority }
*[AVP]

5.3.36 VPLMN-Dynamic-Address-Allowed

VPLMN Dynamic Address Allowed 是 Enumerated 类型，用来指示对于这个 APN，终端是否只能允许使用 HPLMV 这个域的 PDN GW,或者 VPLMN 域里的 PDN GW。如果这个参数不存在，标识终端不允许使用 VPLMN 域的 PDN GW。参数取值定义如下：

a）NOTALLOWED (0)

b）ALLOWED (1)

5.3.37 STN-SR

STN-SR 是 OctetString 类型，包含 SRVCC 的会话转换号码。

5.3.38 Allocation-Retention-Priority

Allocation-Retention-Priority 是 Grouped 类型，用来指示相应 APN 配置的分配和保持的优先级。

参数格式如下：

```
Allocation-Retention-Priority ::= <AVP header: 1034 10415>
                                  { Priority-Level }
                                  [ Pre-emption-Capability ]
                                  [ Pre-emption-Vulnerability ]
```

如果 Allocation-Retention-Priority AVP,中没有包含 Pre-emption-Capability AVP，则缺省的取值应该是 PRE-EMPTION_CAPABILITY_DISABLED (1)。

如果 Allocation-Retention-Priority AVP 中没有包含 Pre-emption-Vulnerability AVP，则缺省的取值应该是 PRE-EMPTION_VULNERABILITY_ENABLED (0)。

5.3.39 AMBR

AMBR 是个 Grouped 类型参数。参数格式如下：

```
AMBR::= <AVP header: 1435 10415>
        { Max-Requested-Bandwidth-UL }
        { Max-Requested-Bandwidth-DL }
        *[AVP]
```

5.3.40 MIP-Home-Agent-Address

MIP-Home-Agent-Address 是 Address 类型，要么是一个 IPv4 地址，要么是 PDN-GW 的 IPv6 地址。

5.3.41 MIP-Home-Agent-Host

MIP-Home-Agent-Host 是 Grouped 类型，这个参数包含用 DNS 功能解决 PDN-GW IP 地址的 PDN-GW FQDN。

5.3.42 PDN-GW-Allocation-Type

PDN-GW-Allocation-Type 是 Enumerated 类型，用来指示在其他节点上 PDN GW 的地址是动态分配的还是静态分配的。如果这个参数不存在，表示是静态分配的。参数取值定义如下：

a）STATIC (0)；

b）DYNAMIC (1)。

5.3.43 MIP6-Agent-Info

MIP6 代理信息为 Grouped 类型（依据 IETF RFC 5447），包含了 PDN-GW 标识。用来在 MME/SGSN 与 HSS 之间传递 PDN-GW 标识且忽略了使用的移动协议类型（GTP 或者 PMIPv6），该标识既可以是基于 MIP-Home-Agent-Address 传输的 IP 地址，也可以是基于 MIP-Home-Agent-Host 传出的 FQDN。参数格式如下：

```
MIP6-Agent-Info ::= < AVP Header: 486 >
                    *2[ MIP-Home-Agent-Address ]
                    [ MIP-Home-Agent-Host ]
                    [ MIP6-Home-Link-Prefix ]
```

*[AVP]

在 MIP6 代理信息中，如果使用静态地址分配，有以下可能：

—— 一个 MIP-Home-Agent-Address 包含 PGW 的一个 IPv4 或者 IPv6 地址。

—— 两个 MIP-Home-Agent-Address 中同时包含 PGW 的一个 IPv4 和 IPv6 地址。

S6a/S6d 接口上不适用 MIP6-Home-Link-Prefix 结构。

5.3.44 RAT-Frequency-Selection-Priority-ID

RAT-Frequency-Selection-Priority-ID 是 Unsigned32 类型值，它是用户签约数据 ID 的 RAT/周期优先级的值。取值范围是 1～256。

5.3.45 IDA-Flags

插入用户数据响应标识是 Unsigned32 类型，由一系列比特位组成，各比特位代表的含义见表 26。

表26 IDA-Flags

Bit	名称	描述
0	Network Node area restricted	该比特位置位，指示由于区域签约导致整个网络节点区域受限
注：SGSN发送IDA消息中，以上定义之外的比特位将全部清除，HSS无需对其进行处理		

5.3.46 PUA-Flags

Purge 用户响应标识是 Unsigned32 类型，由一系列比特位组成，各比特位代表的含义见表 27。

表27 PUA-Flags

bit	name	描述
0	Freeze M-TMSI	该比特位置位，指示MME该M-TMSI需要被冻结
1	Freeze P-TMSI	该比特位置位，指示SGSN该P-TMSI需要被冻结
注意：HSS发送PUA消息中，以上定义之外的比特位将全部清除，MME/SGSN无需对其进行处理		

5.3.47 NOR-Flags

通知请求标识是 Unsigned32 类型，由一系列比特位组成，各比特位代表的含义见表 28。

表28 NOR-Flags

bit	name	描述
0	Single-Registration-Indication	该比特位置位，指示HSS发送位置取消消息到SGSN。SGSN在发送通知请求时不设置该比特位
1	SGSN area restricted	该比特位置位，指示由于区域签约导致整个SGSN区域受限
2	Ready for SM	该比特位置位，指示该用户呈现或者内存可用，可以接收一条或者多条短消息
3	UE Reachable from MME	该比特位置位，指示MME某UE重新可用
4	Delete all APN and PDN GW identity pairs	该比特位置位，指示动态存储在HSS中的所有的APN和PDN GW标识将被删除
5	UE Reachable from SGSN	该比特位置位，指示SGSN某用户重新可用
注：MME/SGSN发送NOR消息中，以上定义之外的比特位将全部清除，HSS无需对其进行处理		

5.3.48 User-Id

用户标识是 UTF8String 类型，包含 IMSI 号码的前缀，在 HSS 中，每一个用户标识确定一组用户。

5.3.49 Regional-Subscription-Zone-Code

Regional-Subscription-Zone-Code 是 OctetString 类型。用户被允许漫游的跟踪和路由区域都应该在该参数中定义，最多不能超过 10 个区域码。依据 3GPP TS 23.003。

注：这个参数中，MME/SGSN 生成的任何漫游限制内部区域码列表信息均取决于运营商的部署。

5.3.50 RAND

随机数为 OctetString.类型，包含随机数信息，依据 3GPP TS 33.401。

5.3.51 XRES

期望响应为 OctetString.类型，包含期望响应信息，依据 3GPP TS 33.401。

5.3.52 AUTN

认证令牌为 OctetString 类型，包含认证令牌信息，依据 3GPP TS 33.401。

5.3.53 Confidentiality-Key AVP

CK 为 OctetString.类型，包含机密性检查密钥信息。

5.3.54 Integrity-Key AVP

IK 为 OctetString.类型，包含完整性检查密钥信息。

5.3.55 Kc AVP

加密密钥为 OctetString 类型，包含加密密钥信息。

5.3.56 SRES

SRES 为 OctetString 类型，详细描述依据 3GPP TS 33.102。

5.3.57 PDN-Type

PDN 类型为 Enumerated 类型，指示 PDN 地址的类型，其取值如下：

a）IPv4 (0)

指示 PDN 只能够通过 IPv4 地址模式接入。

b）IPv6 (1)

指示 PDN 只能够通过 IPv6 地址模式接入。

c）IPv4v6 (2)

指示 PDN 能够同时通过 IPv4 和 IPv6 两种地址模式接入，同时 UE 能够同时支持 IPv4 和 IPv6。

d）IPv4_OR_IPv6 (3)

指示 PDN 既能够支持 IPv4 地址接入模式，又能够支持 IPv6 地址接入模式，但是 UE 不能同时支持 IPv4 和 IPv6。这里需要注意是这个枚举值不能在 UE 的请求中使用，因为 UE 能够支持的类型只能为 IPv4、IPv6 以及 IPv4v6。该值只能作为 APN 签约上下文一部分，作为 HSS 和 MME 之间的一种鉴权机制。

5.3.58 Trace-Data AVP

跟踪数据结构是 Grouped 类型，包含了跟踪功能相关的信息。参数格式如下：

```
Trace-Data ::= <AVP header: 1458 10415>
                {Trace-Reference}
                {Trace-Depth-List}
                {Trace-NE-Type-List}
                [Trace-Interface-List]
                {Trace-Event-List}
                [OMC-Id]
                {Trace-Collection-Entity}
```

*[AVP]

5.3.59 Trace-Reference AVP

Trace-Reference 是 OctetString 类型。这个参数由 MCC,MNC 和 TraceID 串联组成，其中 TraceID 由 3 个字节的 8 位字符串，依据 3GPP TS 32.422。这个参数的按照 8 位字符串编码遵从表 29。当 MCC 或者 MNC 少于 3 个数字时，用“1111”来补齐。

表29 Trace-Reference AVP 的编码格式

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

5.3.60 Trace-Depth AVP

Trace-Depth 是 Enumerated 类型。参数取值依据 3GPP TS 32.422 中的 Trace Depth。

5.3.61 Trace-NE-Type-List AVP

Trace-NE-Type-List AVP 是 OctetString 类型，8 字节编码遵从 3GPP TS 32.422。

5.3.62 Trace-Interface-List AVP

Trace-Interface-List 是 OctetString 类型，8 字节编码遵从 3GPP TS 32.422。

5.3.63 Trace-Event-List AVP

Trace-Event-Type-List 是 OctetString 类型，8 字节编码遵从 3GPP TS 32.422。

5.3.64 OMC-Id AVP

OMC-Id AVP 是 OctetString，8 字节编码遵从 3GPP TS 29.002。

5.3.65 GPRS-Subscription-Data

GPRS-Subscription-Data 是 Grouped 类型的参数，包含用户 GPRS 相关的签约数据信息。参数格式:

GPRS-Subscription-Data ::= <AVP header: 1467 10415>
{ Complete-Data-List-Included-Indicator }
1*50{PDP-Context}
*[AVP]

注：PDP 上下文的最大个数以及最大个数的值依据 3GPP TS 29.002。

5.3.66 Complete-Data-List-Included-Indicator

Complete-Data-List-Included-Indicator 是 Enumerated 类型，参数取值如下：

All_PDP_CONTEXTS_INCLUDED (0)

MODIFIED/ADDED_PDP CONTEXTS_INCLUDED (1)

5.3.67 PDP-Context

PDP-Context 是 Grouped 类型。对于一个有多个 PDP-Context 配置的 GPRS 用户，对于不同的 PDP-Context Service-Selection 都相同。参数格式如下：

PDP-Context ::= <AVP header: 1469 10415>
{ Context-Identifier }
{ PDP-Type }
[PDP-Address]
{ QoS-Subscribed }
[VPLMN-Dynamic-Address-Allowed]
{ Service-Selection }
[3GPP-Charging-Characteristics]
*[AVP]

5.3.68 PDP-Type

PDP-Type 是 OctetString，8 字节编码遵从 3GPP TS 29.002。

5.3.69 QoS-Subscribed

QoS-Subscribed 是 OctetString，8 字节编码遵从 3GPP TS 29.002。（8 字节由 QoS-Subscribed, Ext-QoS-Subscribed, Ext2-QoS-Subscribed 和 Ext3-QoS-Subscribed 连接而成。）

5.3.70 CSG-Subscription-Data

CSG-Subscription-Data 是 Grouped 类型，这个参数包含 CSG-Id 和可选的超期日期。参数格式如下：

CSG-Subscription-Data ::= <AVP header: 1436 10415>
{ CSG-Id }
[Expiration-Date]
*[AVP]

5.3.71 CSG-Id

CSG-Id-Data 是 Unsigned32，定义遵从 3GPP TS 23.003。没有使用的（或没有意义的）比特位都用 0 来填补。

5.3.72 Expiration-Date

Expiration-Date 是 Time 类型（依据 IETF RFC 3588），包含定义 CSG-ID 到期的时间点。

5.3.73 Roaming-Restricted-Due-To-Unsupported-Feature

Roaming-Restricted-Due-To-Unsupported-Feature 是 Enumerated 类型，用来指示由于不支持的特性导致漫游受限。参数取值如下：

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

5.3.74 Specific-APN-Info AVP

Specific-APN-Info 是 Grouped 类型，只有 APN 是一个通配的 APN 时，这个参数才会在 APN 配置中出现。

这个参数包含虽然不在用户的上下文中的，但是终端可以连接的 APN，也包含注册过的 PND-GW 标识。参数格式如下：

Specific-APN-Info ::= <AVP header: 1472 10415>

{ Service-Selection }

{ MIP6-Agent-Info }

[Visited-Network-Identifier]

*[AVP]

5.3.75 Alert-Reason AVP

Alert-Reason 是 Enumerated 类型，参数取值如下：

a）UE_PRESENT (0)

b）UE_MEMORY_AVAILABLE (1)

5.3.76 SS-Code

SS-Code 是 OctetString 类型，8 字节编码遵从 3GPP TS 29.002。

5.3.77 SS-Status

SS-Status 是 OctetString 类型，8 字节编码遵从 3GPP TS 29.002，详细定义依据 3GPP TS 23.011。

5.3.78 Notification-To-UE-User

Privacy-Notification-UE-User AVP 是一个 Enumerated 类型，参数取值如下：

a）NOTIFY_LOCATION_ALLOWED (0)

b）NOTIFYANDVERIFY_LOCATION_ALLOWED_IF_NO_RESPONSE (1)

c）NOTIFYANDVERIFY_LOCATION_NOT_ALLOWED_IF_NO_RESPONSE (2)

d）LOCATION_NOT_ALLOWED (3)

5.3.79 External-Client

External-Client 是 Gouped 类型，这个参数包含允许为 MT-LR 定位一个目标中的外部客户端标识。参数格式如下：

External-Client ::= <AVP header: 1479 10415>

{ Client-Identity }

[GMLC-Restriction]

[Notification-To-UE-User]

*[AVP]

5.3.80 Client-Identity

Client-Identity 是 OctetString 类型，包含外部客户端中的的 ISDN 号码，更详细的说明依据 3GPP TS 23.003。

5.3.81 PLMN-Client

PLMN-Client 是 Enumerated 类型，参数取值如下：

a）BROADCAST_SERVICE (0)

b）O_AND_M_HPLMN (1)

c）O_AND_M_VPLMN (2)

d）ANONYMOUS_LOCATION (3)

e）TARGET_UE_SUBSCRIBED_SERVICE (4)

5.3.82 Service-Type

Service-Type 是 Gouped 类型，包含允许为 MT-LR 定位一个目标终端的客户端服务类型标识。参数格式如下：

Service-Type ::= <AVP header: 1483 10415>
{ ServiceTypeIdentity }
[GMLC-Restriction]
[Notification-To-UE-User]
*[AVP]

5.3.83 ServiceTypeIdentity

ServiceTypeIdentity 是 Unsigned32 类型，更详细的说明依据 3GPP TS 29.002。

5.3.84 MO-LR

MO-LR 是 Gouped 类型，这个参数包含因为一个特殊终端而存在的用户的 MO-LR 分类。参数格式如下：

· MO-LR ::= <AVP header: 1485 10415>
{ SS-Code }
{ SS-Status }
*[AVP]

5.3.85 Trace-Collection-Entity AVP

Trace-collection-Entity 是 Address 类型，包含包含跟踪收集网元的 IPv4 或者 IPv6 地址，定义依据 3GPP TS 32.422。

5.3.86 Teleservice-List

Teleservice-List 是 Grouped 类型，这个参数包含用户和电视服务相关的短信服务码，参数格式如下：

Teleservice-List ::= <AVP header: 1486 10415>
1 * { TS-Code }* [AVP]

5.3.87 TS-Code

TS-Code 是 OctetString 类型。8 字节编码遵从 3GPP TS 29.002.

5.3.88 Call-Barring-Infor-List

Call-Barring-Infor-List 是 Grouped 类型，这个参数包含一个用户和呼叫闭锁服务关联的短信服务码。参数格式如下：

Call-Barring-Infor-List ::= <AVP header: 1488 10415>
1 * { SS-Code }
* [AVP]

5.3.89 SGSN-Number AVP

SGSN-Number 是 OctetString 类型，包含 SGSN 中的 ISDN 的号码。详细定义依据 3GPP TS 23.003。

5.3.90 IDR-Flags

IDR-Flags 是 Unsigned32，包含比特掩码。每一个比特位的定义见表 30。

表30 IDR-Flags

位	名称	描述
0	UE Reachability Request	设置这个比特位，是为了告诉MME/SGSN：HSS正在等待终端可到达性的通知
1	T-ADS Data Request	设置这个比特位，是为了告诉MME/SGSN：HSS要求“IMS Voice over PS Sessions”的支持状态，RAT类型以及终端最后一次和无线通讯的时间戳
2	EPS User State Request	设置这个比特位，是为了告诉MME/SGSN：HSS需要MME或者SGSN的用户状态
3	EPS Location Information Request	设置这个比特位是为了告诉MME/SGSN：HSS需要MME/SGSN的位置信息
4	Current Location Request	设置这个比特是说明需要的是MME/SGSN当前的位置信息
注：这张表中没有定义的比特位会被发送的HSS清除和收到的MME忽略		

5.3.91 Visited-Network-Identifier

Visited-Network-Identifier 是在 PDN-GW 动态分配的情况下，包含分配的 PDN-GW 对应的网络标识。这个参数按照下面的要求编码。

mnc<MNC>.mcc<MCC>.3gppnetwork.org

5.3.92 Last-UE-Activity-Time

Last-UE-Activity-Time 是 Time 类型（依据 IETF RFC 3588），包含 UE 最后一次和服务节点（MME/SGSN）无线通讯的时间点。

5.3.93 EPS-User-State

EPS-User-State 是 Grouped 类型，包含在 MME/SGSN 里用户状态相关的信息。参数格式如下：

EPS-User-State ::= <AVP header:1495 10415>
[MME-User-State]
[SGSN-User-State]
*[AVP]

5.3.94 EPS-Location-Information

EPS-LocationInformation 是 Grouped 类型，包含用户跟 EPS 相关的位置信息。参数格式如下：

EPS-Location-Information ::= <AVP header: 1496 10415>
[MME-Location-Information]
[SGSN-Location-Information]
*[AVP]

5.3.95 MME-User-State

MME-User-State 是 Grouped 类型，包含在 MME 中用户状态相关的信息。参数格式：

MME-User-State ::= <AVP header: 1497 10415>
[User-State]
*[AVP]

5.3.96 SGSN-User-State

SGSN-User-State AVP 是 Grouped 类型，包含在 SGSN 中的用户注册状态相关的信息。参数格式如下：

SGSN-User-State ::= <AVP header: 1498 10415>
[User-State]

*[AVP]

5.3.97 User-State

User-State 是 Enumerated 类型，指示用户在 EPS 中的状态，参数取值如下：

a）DETACHED (0)

b）ATTACHED_NOT_REACHABLE_FOR_PAGING (1)

c）ATTACHED_REACHABLE_FOR_PAGING (2)

d）CONNECTED_NOT_REACHABLE_FOR_PAGING (3)

e）CONNECTED_REACHABLE_FOR_PAGING (4)

f）NETWORK_DETERMINED_NOT_REACHABLE (5)

5.3.98 E-UTRAN-Cell-Global-Identity

E-UTRAN-Cell-Global-Identity 是 OctetString 类型，用户标识单元格中的用户设备登记的 E-UTRAN Cell 全球统一标识，详细定义依据 3GPP TS 23.003，8 字节编码遵从 3GPP TS 29.002。

5.3.99 Tracking-Area-Identity

Tracking-Area-Identity 是 OctetString 类型，包含定位用户的跟踪域标识，详细定义依据 3GPP TS 23.003，8 字节编码遵从 3GPP TS 29.002。

5.3.100 Cell-Global-Identity

Cell-Global-Identity 是 OctetString 类型，并应包含用户标识单元格中的用户设备登记的 Cell 全球统一标识，详细定义依据 3GPP TS 23.003，8 字节编码遵从 3GPP TS 29.002。

5.3.101 Routing-Area-Identity

Routing-Area-Identity 是 OctetString 类型，包含定位用户的路由域索引，详细定义依据 3GPP TS 23.003，8 字节编码遵从 3GPP TS 29.002。

5.3.102 Location-Area-Identity

Location-Area-Identity 是 OctetString 类型，包含用来定位用户的位置域索引，详细定义依据 3GPP TS 23.003，8 字节编码遵从 3GPP TS 29.002。

5.3.103 Service-Area-Identity

Service-Area-Identity 是 OctetString 类型，含定位用户位置的用户的服务域标识，详细说明依据 3GPP TS 23.003，8 字节编码遵从 3GPP TS 29.002。

5.3.104 Geographical-Information

Geographical-Information 是 OctetString 类型，包含定位用户位置的用户地理位置信息，8 字节编码遵从 3GPP TS 29.002。

5.3.105 Geodetic-Information

Geodetic-Information 是 OctetString 类型，包含用户的测量位置信息，8 字节编码遵从 3GPP TS 29.002。

5.3.106 Current-Location-Retrieved

Current-Location-Retrieved 是 Enumerated 类型，枚举值定义如下：

a）ACTIVE-LOCATION-RETRIEVAL (0)

b）这个枚举表示重新激活位置成功页面调度之后，位置信息的重新获得。

5.3.107 Active-APN

Active-APN 是 Grouped 类型参数，它包含一个服务节点上动态连接的 APN 相关信息。所以 HSS 保存这个信息，方式节点重启导致信息丢失。参数格式如下：

Active-APN ::= <AVP header: 1612 10415>
{ Context-Identifier }
{ Service-Selection }
{ MIP6-Agent-Info }
{ Visited-Network-Identifier }
*[Specific-APN-Info]
*[AVP]

5.4 返回代码

5.4.1 DIAMETER_SUCCESS

处理成功。

5.4.2 DIAMETER_ERROR_USER_UNKNOWN

消息中的IMSI不存在。

5.4.3 DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION

消息中的IMSI没有关联的EPS订阅信息。

5.4.4 DIAMETER_ERROR_RAT_NOT_ALLOWED

消息中的IMSI的RAT type不正确。

5.4.5 DIAMETER_ERROR_ROAMING_NOT_ALLOWED

用户不允许在当前的MME/SGSN中漫游。

5.4.6 DIAMETER_ERROR_EQUIPMENT_UNKNOWN

移动设备在EIR中不存在。

5.4.7 DIAMETER_ERROR_UNKOWN_SERVING_NODE

通知消息中的用户在HSS中没有注册。

5.4.8 DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE

HSS返回未知的暂时的失败，对端能够尝试再发一次请求。

6 S13/S13`接口

6.1 概述

S13接口位于MME和EIR之间，支持ME标识验证流程，依据3GPP TS 23.401协议；S13`接口位于SGSN和EIR之间，支持ME标识验证流程，依据3GPP TS 23.060协议。

6.2 消息

6.2.1 ME 标识验证

6.2.1.1 概述

ME标识验证流程应用于MME和EIR之间，SGSN和EIR之间，用于检查移动设备的标识状态，例如：移动设备是否被盗，是否异常等。

ME标识验证流程包含一个Diameter应用命令对，即ME标识验证请求（ECR，ME-Identity-Check-Request）和ME标识验证应答（ECA，ME-Identity-Check-Answer）。

6.2.1.2 MME 和 SGSN 行为的详细处理

如果MME或SGSN的配置要求验证IMEI，MME或SGSN需要向EIR发送ME标识验证请求消息检查ME标识当前的状态，消息中需要携带终端信息，同时也可以携带IMSI，用于ODB的目的。

当接收到EIR返回的ME标识验证响应消息后，MME或SGSN检查返回代码和设备状态。根据返回结果，MME或SGSN决定后续的处理，例如：EIR指示移动设备未知或列入黑名单，附着请求将被MME或SGSN直接拒绝。

6.2.1.3 EIR 行为的详细处理

当接收到ME标识验证请求消息后，EIR基于IMEI AVP的头14个数字检查移动设备是否已知。如果移动设备未知，EIR在ME标识验证应答消息中返回DIAMETER_ERROR_ EQUIPMENT_UNKNOWN的返回代码。

如果移动设备已知，EIR在ME标识验证应答消息中返回DIAMETER_SUCCESS的返回代码，同时携带设备状态信息。

表31描述了ME设备验证请求消息所携带的参数信息，表32描述了ME设备验证应答消息所携带的参数信息。

表31 ME 标识验证请求

信息单元名称	映射到Diameter AVP	类型	描述
Terminal Information	Terminal-Information	必选	所述信息元应包含当前正在使用的移动设备的信息，即IMEI
IMSI	User-Name （依据IETF RFC 3588）	可选	所述信息元应包含用户IMSI，格式依据3GPP TS 23.003，2.2

表32 ME 标识验证应答

信息单元名称	映射到Diameter AVP	类型	描述
Result	Result-Code / Experimental-Result	必选	所述信息元包含了操作的结果。 结果代码属性值对指示操作结果是否成功，其成功或错误代码由Diameter基础协议定义。 实验结果属性值对是一组属性值对，包含了设备生产商标识属性值对和实验结果代码属性值对，其中设备生产商标识属性值对携带3GPP定义的设备生产商标识，实验结果代码属性值对携带S13/S13'接口定义的错误代码，如下： - 未知设备
Equipment Status	Equipment-Status	条件必选	所述信息元包含请求移动台的状态，移动台的状态定义依据3GPP TS 22.016。 所述信息元只有在ME标识验证消息操作结果为DIAMETER_SUCCESS时携带

6.3 信息单元

Equipment-Status 是一个 Enumerated 类型，并且应保护移动设备的身份，取值定义如下：

WHITELISTED (0)

BLACKLISTED (1)

GREYLISTED (2)

其他信息单元的定义参见 5.3 节。

6.4 返回代码

参见5.4节。

7 STa 接口

7.1 概述

STa接口是在非3GPP IP接入网络和3GPP AAA 服务器或者是在非3GPP接入网络和3GPP AAA Proxy之间的接口。

一个非3GPP接入网络是可信任或者是不可信任，不是接入网络的属性，而是在非3GPP接入网络和3GPP AAA 服务器进行接入鉴权和授权过程中决定的。这个是由STa和SWa接口通过共享Diameter应用以及部分共享鉴权和授权过程实现的。STa和SWa接口在交换完第一条鉴权和授权消息后，3GPP AAA server就可以确定网络是否可信任，并通知给非3GPP IP接入网络。剩余的交互过程对于STa和SWa来说都是不一样的。

STa接口应该用于对UE进行鉴权和授权。

在UE使用S2a接口附着到EPC的情况下，STa接口可以传输PMIPv6，MIPv4 FA-CoA 模式相关的移动性参数。

这个接口应该用来传送计费相关的信息，可选的传送IP移动性模式选择。

7.2 消息

7.2.1 STa 接入鉴权和授权

7.2.1.1 概述

这些过程使用Diameter传输，接入（重）鉴权和授权是在可信任的非3GPP接入网络和3GPP AAA(代理)服务器之间进行的。STa接口和Diameter应用被用来鉴权和授权PMIPv6和MIPv4 FA-CoA模式的可信任非3GPP接入的UE，还有在鉴权和授权过程中决定非3GPP接入是否是不信任的。

当在STa接入鉴权中使用EAP-AKA'，并且使用了PMIPv6，非3GPP接入网络的实体作为MAG，同时也要充当NAS(网络接入服务器)的角色。在STa接入鉴权中，NAS节点应该执行传递EPA鉴权者功能，传递EPA鉴权者功能包括在UE和鉴权实体之间进行消息传递，同时验证鉴权返回的结果从而决定是否允许UE接入网络。

在STa接口上的Diameter：

——当使用 EAP 时，可信任的非 3GPP 接入鉴权和授权过程应该映射到 Diameter-EAP-Request 和 Diameter-EAP-Answer，根据 IETF RFC 4072 中定义的命令码。

——对于（重）鉴权过程，下面描述的消息过程应该被重用。

在STa接入的鉴权和授权过程中，非3GPP接入可以提供PMIPv6能力信息给3GPP AAA Server。

对于可信任的非3GPP接入，3GPP AAA Server可以执行IP移动性模式选择。3GPP AAA Server可以给可信任的非3GPP GW一个指示，或者使用PMIPv6或者使用本地的IP地址分配。

在STa接入鉴权和授权过程中，可信任非3GPP GW应该提供Access Network Identity信息到3GPP AAA Server。

在STa接入鉴权和授权过程中，AAA Server可以提供Home Agent IPv6 address或者FQDN到可信任非3GPP的GW。如果Home Agent的地址发现选择用DHCPv6，就需要这个功能。如果Home Agent IPv6 address

或者FQDN没有包含在AAA server最后的Authentication and Authorization Answer消息中，可信任的非3GPP GW不应该通过DHCPv6分配Home Agent。

User-Name AVP可以在漫游场景下包含decorated NAI。在这种情况下，3GPP AAA Proxy应该处理decorated NAI，并根据decorated NAI支持路由Diameter请求消息。

当UE没有IMSI时，鉴权和授权过程不能在STa接口上进行。

对于支持PMIPv6和MIPv4 FA-CoA 模式的非3GPP接入，基于3GPP和非3GPP接入之间的移动性，对于UE已经连接的PDN，每个PDN GW所分配的PDN GW 标识和对应的PDN信息会提供给可信任的非3GPP网络。PDN GW 标识是一个PDN GW的FQDN和/或IP地址。如果提供FQDN，可信任的非3GPP网络应该根据所选择的移动性管理协议中衍生出IP地址。

表33 STa 接入鉴权和授权请求

信息单元名称	映射到Diameter AVP	类别	描述
User Identity	User-Name	必选	这个IE包含用户的标识，用IETF RFC4282定义的NAI表示，格式依据3GPP TS 23.003
EAP payload	EAP-payload	必选	封装用户-3GPP AAA Server共同鉴权使用的EAP负载
Authentication Request Type	Auth-Request-Type	必选	定义了用户是只被鉴权，或者只被授权，或者两者同时。AUTHORIZE_AUTHENTICATE在这个场景下需要使用
UE Layer-2 address	Calling-Station-ID	必选	传递UE的层2地址。
Supported 3GPP QoS profile	QoS-Capability	可选	如果非3GPP接入网络支持QoS机制，可以包含这个IE，按照IETF RFC 5777定义接入网络的QoS能力
Mobility Capabilities	MIP6-Feature-Vector	条件	这个IE应该包含非3GPP接入网络的移动性能力。如果执行了动态的移动性模式选择，需要使用这个IE。 如果非3GPP接入网络支持PMIPv6（IETF RFC 5779），应该设置成PMIP6_SUPPORTED 标志。如果支持基于DHCPv6的Home Agent地址发现，应该设置成MIP6_INTEGRATED标志
Access Type	RAT-Type	必选	包含了服务于该用户的非3GPP接入网络的网络类型。
Access Network Identity	ANID	必选	包含了在HSS中用于密钥衍生的接入网络标识。
Visited Network Identifier	Visited-Network-Identifier	可选	用于归属网络识别拜访网络。这个AVP可以由非3GPP接入网络中插入，取决于本地策略，并且只当用户没有连接到归属网络的时候才用
APN Id	Service-Selection	可选	包含了用户希望连接的APN，如果有的话
Terminal Information	Terminal-Information	可选	这个IE应该包含用户的移动终端信息。标识的类型取决于接入网络的类型。对于HRPD接入网络来说，3GPP2-MEID AVP应该包含在这个组AVP中
Supported Features (3GPP TS 29.229)	Supported-Features	可选	如果有这个AVP，它包含了在Diameter会话生命期中发起端所支持的特性列表

表34 可信任非 3GPP 接入鉴权和授权响应

信息单元名称	映射到Diameter AVP	类别	描述
User Identity	User-Name	必选	这个IE包含用户的标识，用IETF RFC4282定义的NAI表示，格式依据3GPP TS 23.003
EAP payload	EAP payload	必选	封装用户-3GPP AAA Server共同鉴权使用的EAP负载

表34（续）

信息单元名称	映射到Diameter AVP	类别	描述
Result code	Result-Code / Experimental Result Code	必选	操作的结果。结果代码在Diameter Base Protocol(IETF RFC 3588)中定义。STa错误码使用Experimental-Result AVP。这是一个组AVP，在Vendor-Id AVP中包含了3GPP Vendor ID，在Experimental-Result-Code AVP中包含错误代码
Session Alive Time	Session-Timeout	可选	如果Result-Code AVP是DIAMETER _SUCCESS，可以带这个AVP。它包含了会话允许激活的最大秒数
Accounting Interim Interval	Accounting Interim-Interval	可选	计费时长
Pairwise Master Key	EAP-Master-Session-Key	条件可选	如果Result-Code AVP 值是DIAMETER_SUCCESS，需要设置该AVP
Default APN	Context-Identifier	条件可选	指示用户的默认APN，这个只是在使用PMIPv6的情况下，非3GPP接入网络被认为是可信任的，而且Result-Code AVP的值是DIAMETER_SUCCESS
APN and PGW Data	APN-Configuration	条件可选	只有在Result-Code AVP 值为DIAMETER_SUCCESS时，才需要发送该IE。 如果使用PMIPv6，这个AVP应该包含默认的APN，授权的APN列表，用户的profile，以及PDN GW信息。 如果使用本地IP地址分配，当如果支持基于DHCP的Home Agent地址发现被使用时，才需要这个AVP。 AGW根据MIP6-Feature-Vector里的标识知道使用PMIPv6或者本地IP地址分配。 APN-Configuration是一个组AVP,在3GPP TS 29.272定义。 当PMIP使用时，每个APN中可以包含的信息如下： - APN - Authorized 3GPP QoS profile - Statically allocated User IP Address (IPv4 and/or IPv6) - Allowed PDN types (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed - APN-AMBR 当使用DSMIPv6，基于DHCPv6的Home Agent地址发现，每个Home Agent中可以包含的信息如下： - HA-APN - Authorized 3GPP QoS profile - PDN GW identity
APN-OI replacement	APN-OI-Replacement	条件可选	在非漫游场景或者漫游时回到归属网络的场景下，当构造PDN GW FQDN去执行DNS解析，这个AVP用于指示用域名来代替，APN-OI。 只有在使用PMIPv6并且Result-Code AVP值为DIAMETER_SUCCESS

表34（续）

信息单元名称	映射到Diameter AVP	类别	描述
Serving GW Address	MIP6-Agent-Info	可选	这个AVP只有在chained S2a-S8场景下，并且Result-Code AVP的值为DIAMETER_SUCCESS，才需要使用
Mobility Capabilities	MIP6-Feature-Vector	条件可选	这个AVP只有在Result-Code AVP的值为DIAMETER_SUCCESS，才需要使用。 如果执行了动态移动性模式选择，它应该包含AAA/HSS授权给可信任的非3GPP接入网络的移动性能力集。 3GPP AAA server需要设置PMIP6_SUPPORTED或者ASSIGN_LOCAL_IP标志，强制使用的移动性协议。 如果Home Agent 地址是由基于DHCPv6的Home Agent地址发现提供的，应该设置MIP6_INTEGRATED标志。 后一种情况，用于DHCPv6发现的HA信息是在APN-Configuration AVP中提供的
Permanent User Identity	Mobile-Node-Identifier	条件可选	只有在PMIPv6或者PMIPv4使用时，并且Result-Code AVP的值是DIAMETER_SUCCESS时，才需要这个AVP。它包含了AAA/HSS分配的ID（如EPC中的IMSI），用于MAG在后续的PBU消息中作为MN-ID，或者是MIPv4 RRQs中作为MN-NAI，来标识EPS的用户
3GPP AAA Server Name	Redirect-Host	条件可选	如果Result-Code值为DIAMETER_REDIRECT_INDICATION，需要使用该AVP。如果用户在之前被另外一个3GPP AAA Server鉴权过，它应该包含当前服务于该用户的3GPP AAA Server的Diameter ID。接收到该IE的节点按照Diameter Base Protocol (IETF RFC 3588)中规定的进行操作。这个命令应该包含0个或多个当前正在发生的IE。当从多个Redirect-Host AVP中为重定向选择一个目的，接收者应该发送Diameter请求到接收到的Diameter响应消息中的要求列表的第一个3GPP AAA Server。如果没有成功响应，接受者应该发送到列表中的下一个3GPP AAA Server。这个过程重复进行知道从3GPP AAA Server收到成功响应
UE Charging Data	3GPP-Charging-Characteristics	可选	包含了用户的计费方法类型（依据TS 29.061）
UE AMBR	AMBR	条件可选	包含了用户的UE AMBR。只有在非3GPP接入网络是可信任的，并且Result-Code AVP是DIAMETER_SUCCESS，ANID是"HRPD"的时候，才使用该AVP
Trust Relationship Indicator	AN-Trusted	条件可选	这个AVP是适用与第一次鉴权和授权过程。它包含3GPP AAA Server的决定，即非3GPP接入网络是否是可信任的
Supported Features (3GPP TS 29.229)	Supported-Features	可选	如果有这个AVP，它包含了在Diameter会话生命期中发起端所支持的特性列表

7.2.1.2 3GPP AAA Server 具体行为

当接收到第一个DER消息，3GPP AAA Server需要检查ANID AVP的有效性，以及非3GPP GW是否允许适用该值。3GPP AAA Server对于ANID的语法检查处理如下：

——在漫游场景下，如果消息没有经过 3GPP AAA Proxy，3GPP AAA Server 直接接收到请求，则应检查 ANID。

——在漫游场景下，如果请求是经过 3GPP AAA Proxy 的，则可以检查 ANID 也可以不检查 ANID。3GPP AAA Server 可以决定基于本地配置来检查 ANID，如根据接收到拜访地网络标识。

——如果检查结果显示包含的 ANID 值为无效（不在 3GPP 定义范围内）或者发送请求的实体不允许使用接收到的 ANID 值，则 Result-Code 应该设置为 DIAMETER_UNABLE_TO_COMPLY。

3GPP AAA Server应该检查用户数据是否存在于3GPP AAA Server中（对于当前接入网络ID：实体，包含了有效的鉴权信息）。如果不存在，3GPP AAA Server应该使用SWx接口来获取接入鉴权和授权数据。

如果SWx鉴权响应指示：

——用户不存在，3GPP AAA Server 应该响应 non-3GPP GW，Experimental-Result-Code 的值为 DIAMETER_ERROR_USER_UNKNOWN。

——用户没有非 3GPP 接入订阅，3GPP AAA Server 应该响应 non-3GPP GW，Experimental-Result-Code 的值为 DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION。

——用户不允许漫游到拜访地，3GPP AAA Server 应该响应 non-3GPP GW，Experimental-Result-Code 的值为 DIAMETER_ERROR_ROAMING_NOT_ALLOWED。

——用户当前由另外的 3GPP AAA Server 提供服务，这个 3GPP AAA Server 应该响应 non-3GPP GW，Result-Code 的值为 DIAMETER_REDIRECT_INDICATION，Redirect-Host 设置成当前提供服务的 3GPP AAA Server 的 Diameter 标识（从 HSS 返回的 SWx 鉴权响应中带的 3GPP-AAA-Server-Name AVP）。

——如果还有其他错误发生，错误码应设置成 DIAMETER_UNABLE_TO_COMPLY 返回给 Non-3GPP GW。

当SWx鉴权响应包含请求了的鉴权信息，3GPP AAA Server应该继续鉴权和授权过程。3GPP AAA Server应该使用SWx接口中定义的流程从HSS获得用户订阅数据。

在发送鉴权challenge前，3GPP AAA Server应该决定接入网络是否是可信任的。3GPP AAA Server应该基于接入网络标识和拜访网络标识信息，根据本来策略来做判断。3GPP AAA Server的本地策略应该基于3GPP TS 33.402规定的安全标准。

在漫游场景下，3GPP AAA Server从VPLMN(AN-Trusted AVP)获得了信任关系指示，3GPP AAA Server可以使用该信息，作为信任/非信任评估的输入参数。

VPLMN信任关系指示只有在下面的情况下使用：

——用户的某些 APN 连接可以使用本地疏导，并且

——在 HPLMN 和 VPLMN 运营商之间有适当的信任关系。

3GPP AAA Server应该基于用户订阅profile中的VPLMN-Dynamic-Address-Allowed AVPs，来确认本地疏导的可能性；如果VPLMN分配的PDN GW可以用于任何订阅的APN，那本地疏导被认为是有可能的。

如果3GPP AAA Server决定考虑接收到的信任关系，它应该综合它自己的决定（按上所述）和接收到的信任指示，只有两个都表示为可信任的，才能最后决定为可信任；若是其他情况，则最后的决定应该是不可信任。

基于信任/不信任决定，3GPP AAA Server可以发送信任关系指示给UE，按照3GPP TS 24.302的描述。

3GPP AAA Server应该在AT_TRUST_IND属性中指示给UE，关于对非3GPP接入网络可信任关系的评估，按照3GPP TS 24.302的定义。3GPP AAA Server还应该在DEA (EAP-Request/AKA-Challenge) 命令的AN-Trusted AVP指示给非3GPP接入网络关于其可信任关系的评估。

如果决定是可信任的，STa鉴权和授权过程将按本章节描述的执行，否则按照SWa的过程执行。

3GPP AAA Server应该按3GPP TS 33.402规定，允许EAP-AKA'鉴权。例外情况应该被当作错误处理，结果代码应该设置成DIAMETER_UNABLE_TO_COMPLY。一旦鉴权成功完成，3GPP AAA Server应该执行下面的授权判断（注：如果在这过程中有任何一步出错，3GPP AAA Server需要停止处理并返回相应的错误）：

a）判断用户是否被禁止使用非 3GPP 接入。如果是，Result-Code 应该设置为 DIAMETER_AUTHORIZATION_REJECTED。

b）判断用户是否被禁止使用订阅的 APN。如果是，Result-Code 应该设置为 DIAMETER_AUTHORIZATION_REJECTED。

c）判断 RAT-Type AVP。如果

——接入类型指示的值不在 3GPP TS 29.212 定义范围内，或者

——接收到的 RAT-Type 是在用户不允许的 RAT-Types 列表中

这应该被作为错误处理，Result-Code 应该设置为 DIAMETER_UNABLE_TO_COMPLY。

下面的步骤只有在非3GPP接入网络被认为可信任的情况下才执行。

e）判断用户请求的 APN 是否有订阅。如果不是，Result-Code 应该设置为 DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION。

f）如果有 MIP6-Feature-Vector 这个 AVP，判断接收到的值：

——如果值为 MIP6-INTEGRATED，并且 3GPP AAA server 授权了 DHCP Home Agent 分配，3GPP AAA server 应该在响应的 APN-Configuration AVP 中包含 Home Agent 的地址，同时 MIP6-Feature-Vector AVP 的值设为 MIP6-INTEGRATED。如果没有使用基于 DHCPv6 的 HA 分配，就不需要发送带有 MIP6-INTEGRATED 值的 MIP6-Feature-Vector AVP。

——PMIP6_SUPPORTED 标识指示给 3GPP AAA server，可信任的 non-3GPP GW 是否支持 PMIPv6。根据 3GPP TS 23.402，综合 UE，本地/归属地网络能力，以及本地/归属地网络策略，3GPP AAA server 可以执行移动性模式选择。如果 3GPP AAA server 决定使用 PMIPv6，发送给可信任 non 3GPP GW 的响应中应该包含 PMIP6_SUPPORTED 标识，表示 UE 支持 PMIPv6。如果 3GPP AAA server 决定使用本地 IP 地址分配，发送给可信任 non 3GPP GW 的响应中应该包含 ASSIGN_LOCAL_IP 标识，表示 IP 地址需要本地分配。3GPP AAA server 不可以在同一个响应消息中同时包含 PMIP6_SUPPORTED 和 ASSIGN_LOCAL_IP 标识。

一旦鉴权和授权过程成功结束，3GPP AAA Server应该从HSS的鉴权和授权响应中下载鉴权数据，授权的APN列表，授权的移动性协议。这些情况的例外都应该被3GPP AAA Server当作错误处理，Result-Code应设置DIAMETER_UNABLE_TO_COMPLY，而且，不会返回任何授权信息。

7.2.1.3 3GPP AAA Proxy 具体行为

当非3GPP接入网络连接到VPLMN时，需要3GPP AAA Proxy处理漫游场景。3GPP AAA Proxy应当作为一个有状态的proxy，还有下面功能的增强。

当接收到一个鉴权和授权请求时，3GPP AAA Proxy应该检查Visited-Network-Identifier AVP,

——如果这个AVP不存在，3GPP AAA Proxy应该在转发请求到3GPP AAA Server之前，插入该AVP。

——如果这个 AVP 存在，3GPP AAA Proxy 可根据本来策略检查并重写该 AVP 的值，如可信任非3GPP 接入网络由 VPLMN 运营或者第三方运营。

• 应该检查 ANID AVP。如果检查的结果显示包含的 ANID 值无效（不是 3GPP 定义的）或者请求方没有授权使用该值，Result-Code 应该设置成 DIAMETER_UNABLE_TO_COMPLY，并且鉴权响应该发送给可信任 non-3GPP GW。

• 可以从 VPLMN 的角度来决定非 3GPP 接入网络的信任度。如果执行该决策，应该根据 3GPP AAA Proxy 的本地策略，基于 ANI 和可选的关于非 3GPP 接入网络的信息来判断。本地策略应该基于 3GPP TS 33.402 规定的安全标准，并假设 VPLMN 分配 PDN GW。

对非3GPP接入网络的信任度决策编码到VPLMN 信任关系指示中，并插入到鉴权和授权请求中

当接收到第一个鉴权和授权请求，3GPP AAA Proxy应该检查本地配置信息，判断从HPLMN来的用户是否允许激活从非3GPP接入网络通过VPLMN的PDN连接。如果不可以，Experimental-Result-Code应该设置成DIAMETER_ERROR_ROAMING_NOT_ALLOWED，并且鉴权和授权响应该发送给非3GPP接入网络。

当接收到已成功鉴权的鉴权和授权回复，3GPP AAA Proxy需要进行以下的动作：

——可以根据本地配置判断是否使用 S8-S2a 到 HPLMN。如果使用 chaining，3GPP AAA Proxy 应该从网络配置数据库中选择一个 Serving GW，并在回复中包含该 Serving GW 的地址。

——应该检查配置信息中设置的特定 HPLMN 来的用户所允许的最大静态 QoS 参数，并根据从 3GPP AAA Server 接收到的 QoS 参数进行修改，执行策略限制功能。

——应该记录连接的状态（如鉴权和授权的成功）。

7.2.1.4 可信任的 non-3GPP GW 具体行为

当用户附着到接入网络时，可信任的non-3GPP GW应该发起可信任非3GPP接入鉴权和授权过程。在鉴权中，它应作为传递EAP的认证者。

如果使用PMIPv6，在成功完成鉴权过程后，可信任的non-3GPP GW 需要存储从3GPP AAA Server 接收到的非3GPP用户数据。可信任的non-3GPP GW 应该使用这个数据进行如下动作：

——授权用户请求的创建 PDN 连接中的 APN；

——授权请求中 home address 类型：IPv4 home address 和/或 IPv6 home network prefix。

7.2.2 HSS/AAA 发起的 STa 去附着

7.2.2.1 概述

这个过程是在3GPP AAA/HSS和可信任的非3GPP接入网络之间，用于表示3GPP AAA/HSS决定某个特定的UE应该从EPC中去附着。这个过程基于Diameter会话终止消息。

Diameter 在STa接口上的应用如下：

——参照 RFC 3588，这个过程映射到 Diameter 命令码 Diameter-Abort-Session-Request (ASR), Diameter-Abort-Session-Answer (ASA),Diameter-Session-Termination-Request (STR) 和 Diameter-Session-Termination-Answer (STA)。

——STa 的 Application Id 值 16777250 应该被作为 ASR/ASA/STR/STA 命令中的 Application Id 值使用。

表35 ASR 消息中传递的参数

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	这个IE包含用户的标识，（如IMSI在EPC root NAI的格式，依据3GPP TS 23.003）
Auth-Session-State	Auth-Session-State	可选	这个IE指示给Non-3GPP GW，表示3GPP AAA Server 是否需要STR消息

表36 ASA 消息中传递的参数

信息单元名称	映射到Diameter AVP	类别	描述
Result-Code	Result-Code	必选	运行结果

表37 STR 消息中传递的参数

信息单元名称	映射到Diameter AVP	类别	描述
Termination-Cause	Termination-Cause	必选	这个IE包含了会话被终止的理由。应该被设置成"DIAMETER_ADMINISTRATIVE"，表示会话终止是对于ASR消息的响应

表38 STA 消息中传递的参数

信息单元名称	映射到Diameter AVP	类别	描述
Result-Code	Result-Code	必选	运行结果

7.2.2.2 3GPP AAA Server 具体行为

3GPP AAA Server应该使用这个过程来指示非3GPP接入网络从接入网络中去附着一个特定的用户。

3GPP AAA Server 应该在ASR命令中包含Auth-Session-State AVP，如果不需要Non-3GPP GW的STR，值为NO_STATE_MAINTAINED。如果需要Non-3GPP GW的STR，3GPP AAA Server 应该或者忽略ASR中的Auth-Session-State AVP，或者ASR 命令的值为STATE_MAINTAINED的Auth-Session-State AVP。

当收到ASR命令，非3GPP接入网络应该判断这个用户在非3GPP接入网络中是否可知。如果不可知，Experimental-Result-Code 值为DIAMETER_ERROR_USER_UNKNOWN。

如果用户可知，非3GPP接入网络应该断开该用户的所有激活的PDN连接，并删除存贮的任何用户信息。

非3GPP接入网络应该设置Result-Code为DIAMETER_SUCCESS，并返回ASA 命令给3GPP AAA Server，去附着接入网络的用户状态需要更新。

如果3GPP AAA Server需要，Non-3GPP GW应该发送STR，Termination-Cause 设为DIAMETER_ADMINISTRATIVE。3GPP AAA Server 应该设Result-Code 为 DIAMETER_SUCCESS 并返回STA 命令给Non-3GPP GW。

7.2.2.3 3GPP AAA Proxy 具体行为

当3GPP AAA Proxy 从3GPP AAA Server 收到ASR，它应该路由该请求到非3GPP 接入网络。

如果3GPP AAA Proxy需要STR但是3GPP AAA Server不需要，3GPP AAA Proxy 可以重写ASR中Auth-Session-State AVP的值，设为STATE_MAINTAINED。在这种情况下，3GPP AAA Proxy 不应前转从non-3GPP GW收到的STR到3GPP AAA Server，应该给non-3GPP GW返回STA，其中的Result-Code 为DIAMETER_SUCCESS。其他情况下，3GPP AAA Proxy 不应该重写Auth-Session-State AVP的任何值。

当收到ASA消息，其中的Diameter Result Code 为DIAMETER_SUCCESS时，3GPP AAA Proxy不应该路由成功响应到3GPP AAA Server，而应该释放会话相关的资源。

当3GPP AAA Proxy从Non-3GPP GW收到STR时，应该路由请求到3GPP AAA Server。当收到STA消息时，3GPP AAA Proxy应路由响应到Non-3GPP GW。

7.2.3 STa 重鉴权和重授权过程

7.2.3.1 概述

STa重授权过程是在3GPP AAA Server和可信任的非3GPP接入之间进行，允许3GPP AAA Server 修改之前提供的授权参数。这个可能由于HSS中用户的profile被修改（例如，删除了用户相关的特定APN）。在这个情况下，这个过程按两个步骤执行：

——3GPP AAA server 应该发起 STa Re-Auth 请求到可信任的非 3GPP 接入。非 3GPP 接入接收到该请求后，应该响应，并指示请求的部署。这个过程映射到 Diameter 命令 Re-Auth-Request 和 Re-Auth-Answer（IETF RFC 3588）。接收到 STa Re-Auth 请求后，非 3GPP access 接入应该立即发起 STa 接入授权过程，重用 IETF RFC 4005 定义的 Diameter 命令码 AA-Request 和 AA-Answer。

——可信任的非3GPP接入从HSS中获取用户profile。这个过程可以在任何时间由可信任的non-3GPP GW 发起，用于检查 3GPP AAA Server 之前提供的用户授权参数是否有修改。在这个单步中，可信任的非 3GPP 接入应该发起 STa 接入授权过程，基于 IETF RFC 4005 定义的 Diameter 命令 AA-Request 和 AA-Answer。

可信任的non-3GPP GW接收到授权回复后，将会对撤回授权的那些激活的PDN连接进行释放。如果3GPP AAA server拒绝授权（如用户的非3GPP接入的订阅被终止），非3GPP接入网络应该把用户从非3GPP接入网络中去附着，并释放所有资源。

STa 重鉴权过程是在3GPP AAA Server和可信任的非3GPP接入之间进行，用于对用户重鉴权。3GPP AAA Server可以基于HPLMN运营商配置的策略在任何时候发起这个过程。这个过程按两个步骤执行：

——3GPP AAA server 发起 STa Re-Auth 请求到可信任的非 3GPP 接入。可信任的非 3GPP 接入接收到该请求，应该响应，并并指示请求的部署。这个过程映射到 Diameter 命令 Re-Auth-Request 和 Re-Auth-Answer （IETF RFC 3588）。

——当可信任的非 3GPP 接入接收到 STa Re-Auth 请求，应该根据 3GPP AAA server 提供的 Re-Auth 请求类型，立即发起 STa 接入鉴权和授权过程。这个过程映射到 Diameter 命令 Diameter-EAP-Request 和 Diameter-EAP-Answer（IETF RFC 4072）。

如果对用户的重鉴权不成功，可信任的非3GPP接入将释放所有与该用户相关的激活的PDN连接，除了紧急PDN连接。在成功完成鉴权和授权后，当授权被撤回时，3GPP GW应该释放所有的PDN连接。

表39 STa 重鉴权 请求

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	这个IE包含用户的标识，用IETF RFC4282定义的NAI表示，格式依据3GPP TS 23.003
Re-Auth Request Type	Re-Auth–Request-Type	必选	定义了用户是只被鉴权，或者只被授权，或者两者同时。有下面的参数 如果请求对用户重鉴权，使用AUTHORIZE_AUTHENTICATE； 如果需要更新之前提供的用户授权参数，使用AUTHORIZE_ONLY
Routing Information	Destination-Host	必选	这个IE从Origin-Host AVP中获得，包含在从可信任的非3GPP接入发送来的消息中

表40 STa 重鉴权响应

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	这个IE包含用户的标识，用IETF RFC4282定义的NAI表示，格式依据3GPP TS 23.003
Result	Result-Code / Experimental-Result	必选	操作的结果。结果代码在Diameter Base Protocol(IETF RFC 3588)中定义。STa错误码使用Experimental-Result AVP。这是一个组AVP，在Vendor-Id AVP中包含了3GPP Vendor ID，在Experimental-Result-Code AVP中包含错误代码

表41 STa 授权请求

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	这个IE包含用户的标识，用IETF RFC4282定义的NAI表示，格式依据3GPP TS 23.003
Request-Type	Auth-Request-Type	必选	定义了用户是只被鉴权，或者只被授权，或者两者同时。AUTHORIZE_ ONLY在这个场景下需要使用
Mobility Capabilities	MIP6-Feature-Vector	条件	这个IE应该包含非3GPP接入网络的移动性能力。 这个AVP只有在从E-UTRAN到HRPD 接入时支持优化的空闲态移动性时才需要包含。当包含时，应该设置MIP_SUPPORTED和OPTIMIZED_IDLE_MODE_MOBILITY 标志
Routing Information	Destination-Host	必选	3GPP AAA Server 名称从之前接收到的消息中的Origin-Host AVP获得

表42 STa 授权响应

信息单元名称	映射到Diameter AVP	类别	描述
Registration Result	Result Code/ Experimental Result Code	必选	操作的结果。结果代码在Diameter Base Protocol(IETF RFC 3588)中定义。STa错误码使用Experimental-Result AVP。这是一个组AVP，在Vendor-Id AVP中包含了3GPP Vendor ID，在Experimental-Result-Code AVP中包含错误代码
Session Alive Time	Session-Timeout	可选	如果Result-Code AVP是DIAMETER _SUCCESS，可以带这个AVP。它包含了会话允许激活的最大秒数
Accounting Interim Interval	Acct-Interim-Interval	可选	计费时长
APN-OI replacement	APN-OI-Replacement	条件	在非漫游场景或者漫游时回到归属网络的场景下，当构造PDN GW FQDN去执行DNS解析，这个AVP用于指示用域名来代替APN-OI。只有在使用PMIPv6并且Result-Code AVP值为DIAMETER_SUCCESS
UE Charging Data	3GPP-Charging-Characteristics	可选	包含了用户的计费方法类型（依据TS 29.061）
UE AMBR	AMBR	条件可选	包含了用户的UE AMBR。只有在非3GPP接入网络是可信任的，并且Result-Code AVP是DIAMETER_SUCCESS，ANID 是"HRPD"的时候，才使用该AVP
Mobility Capabilities	MIP6-Feature-Vector	条件可选	这个AVP只有在Result-Code AVP的值为DIAMETER_ SUCCESS，才需要使用。 当包含时，应该设置PMIP_SUPPORTED和OPTIMIZED_IDLE_MODE_MOBILITY 标志

表42 (续)

信息单元名称	映射到Diameter AVP	类别	描述
APN and PGW Data	APN-Configuration	条件可选	只有在Result-Code AVP 值为DIAMETER_SUCCESS时，才需要发送该IE。 如果使用PMIPv6，这个AVP应该包含默认的APN，授权的APN列表，用户的profile，以及PDN GW信息。 如果使用本地IP地址分配，当如果支持基于DHCP的Home Agent地址发现被使用时，才需要这个AVP。 可信任的Non-3GPP GW在STa接入鉴权和授权过程中，根据MIP6-Feature-Vector里的标识知道使用PMIPv6或者本地IP地址分配。 APN-Configuration是一个组AVP,在3GPP TS 29.272定义。 当PMIP使用时，每个APN中可以包含的信息如下： - APN - Authorized 3GPP QoS profile - Statically allocated User IP Address (IPv4 and/or IPv6) - Allowed PDN types (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed 当使用DSMIPv6，基于DHCPv6的Home Agent地址发现，每个Home Agent中可以包含的信息如下： - HA-APN - Authorized 3GPP QoS profile - PDN GW identity

表43 STa 接入鉴权和授权请求

信息单元名称	映射到Diameter AVP	类别	描述
User Identity	User-Name	必选	这个IE包含用户的标识，用IETF RFC4282定义的NAI表示，格式依据3GPP TS 23.003
EAP payload	EAP-payload	必选	封装用户-3GPP AAA Server共同鉴权使用的EAP负载
Authentication Request Type	Auth-Request-Type	必选	定义了用户是只被鉴权，或者只被授权，或者两者同时。AUTHORIZE_AUTHENTICATE在这个场景下需要使用

表44 STa 接入鉴权和授权响应

信息单元名称	映射到Diameter AVP	类别	描述
User Identity	User-Name	必选	这个IE包含用户的标识，用IETF RFC4282定义的NAI表示，格式依据3GPP TS 23.003
EAP payload	EAP payload	必选	封装用户-3GPP AAA Server共同鉴权使用的EAP负载
Result code	Result-Code / Experimental Result Code	必选	操作的结果。结果代码在Diameter Base Protocol(IETF RFC 3588)中定义。STa错误码使用Experimental-Result AVP。这是一个组AVP，在Vendor-Id AVP中包含了3GPP Vendor ID，在Experimental-Result-Code AVP中包含错误代码
Session Alive Time	Session-Timeout	可选	如果Result-Code AVP是DIAMETER _SUCCESS，可以带这个AVP。它包含了会话允许激活的最大秒数

表44（续）

信息单元名称	映射到Diameter AVP	类别	描述
Accounting Interim Interval	Accounting Interim-Interval	可选	计费时长。
Pairwise Master Key	EAP-Master-Session-Key	条件	Shall be sent if Result-Code AVP is set to DIAMETER_SUCCESS
Default APN	Context-Identifier	条件	指示用户的默认APN，这个只是在使用PMIPv6的情况下，非3GPP接入网络被认为是可信任的，而且Result-Code AVP的值是DIAMETER_SUCCESS
APN-OI replacement	APN-OI-Replacement	条件	在非漫游场景或者漫游时回到归属网络的场景下，当构造PDN GW FQDN去执行DNS解析，这个AVP用于指示用域名来代替APN-OI。 只有在使用PMIPv6并且Result-Code AVP值为DIAMETER_SUCCESS
UE Charging Data	3GPP-Charging-Characteristics	可选	包含了用户的计费方法类型（依据TS 29.061）
UE AMBR	AMBR	可选	包含了用户的UE AMBR。只有在非3GPP接入网络是可信任的，并且Result-Code AVP是DIAMETER_SUCCESS，ANID 是"HRPD"的时候，才使用该AVP
APN and PGW Data	APN-Configuration	条件	只有非3GPP接入网络被认为是可信任的，并且Result-Code AVP 值为DIAMETER_SUCCESS时，才需要发送该IE。 如果使用PMIPv6，这个AVP应该包含默认的APN，授权的APN列表，用户的profile，以及PDN GW信息。 如果使用本地IP地址分配，当如果支持基于DHCP的Home Agent地址发现被使用时，才需要这个AVP。 AGW根据MIP6-Feature-Vector里的标识知道使用PMIPv6或者本地IP地址分配。 APN-Configuration是一个组AVP,在3GPP TS 29.272定义。 当PMIPv6使用时，每个APN中可以包含的信息如下 ： - APN - Authorized 3GPP QoS profile - User IP Address (IPv4 and/or IPv6) - Allowed PDN types (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed - APN-AMBR 当使用DSMIPv6，基于DHCPv6的Home Agent地址发现，每个Home Agent中可以包含的信息如下: - HA-APN - Authorized 3GPP QoS profile - PDN GW identity

7.2.3.2 3GPP AAA Server 具体行为

a）处理 Re-Auth 请求

3GPP AAA server 应该利用这个过程来指示下面的参数

——如果可信任的 non-3GPP GW 需要更新相关的业务授权参数，Re-Auth-Request-Type 应该设成 AUTHORIZE_ONLY。这个过程可以由 HSS 发送订阅数据更新或者本地策略触发，本地策略如运营商配置的周期性重授权。对于 STa 接口，一个用户只能有一个 Diameter 授权会话，这个过程用于该用户的所有的 PDN 连接，即每个用户应该只有一个 Re-authorization 的请求实例。

——如果需要对用户进行重鉴权和授权，Re-Auth-Request-Type 应该设成 AUTHORIZE_AUTHENTICATE。这个过程可以根据配置在 3GPP AAA Server 内的本地策略来触发，如对用户最后一次（重）鉴权成功完成后启动的定时器到期后触发。

b）处理授权请求

3GPP AAA Server应该检查用户是否在3GPP AAA Server中存在，这个检查应该基于Diameter Session-Id。如果不存在，Experimental-Result-Code 应设为DIAMETER_ERROR_USER_UNKNOWN。如果存在，3GPP AAA Server应该按照7.2.1.2执行授权检查。

如果授权请求包含带有OPTIMIZED_IDLE_MODE_MOBILITY标志的MIP6-Feature-Vector，AAA server应该向HSS请求用户数据，为了获取最新的PDN GW信息。

3GPP AAA Server应该对用户执行重鉴权，按照3GPP TS 33.402中6.2节和6.3节定义的，使用完整的鉴权或者快速重鉴权过程。如果执行完整的鉴权，而且3GPP AAA Server中没有给定非3GPP接入网络有效的鉴权向量，3GPP AAA Server应该从HSS中获取鉴权向量。需要进行联合的鉴权和授权，QoS-Capability，Access Network Identity，Access Type, Visited Network Identifier，Terminal Information这些IE在初始的鉴权和授权过程中获得，同时还获得了非3GPP接入网络的可信任性，以及所选择的IP移动性模式。

如果用户的重鉴权失败，3GPP AAA Server 应该：

——终止所有的和该用户相关的 S6b 授权会话。

——删除 HSS 中的所有 APN-PDN GW 绑定关系，参考 SWx 接口。

——从 HSS 中去注册用户。根据重鉴权失败的原因，Server Assignment Type 应该设为 AUTHENTICATION_FAILURE 或者 AUTHENTICATION_TIMEOUT。

——释放所有和用户相关的资源。

7.2.3.3 3GPP AAA Proxy 具体行为

如果Non-3GPP GW在VPLMN中，3GPP AAA Proxy需要处理漫游场景。3GPP AAA Proxy应该作为有状态的代理，并有下面的增强。

当转发授权回复或者鉴权和授权回复时，3GPP AAA Proxy应该执行以下动作：

——检查配置信息中设置的特定 HPLMN 来的用户所允许的最大静态 QoS 参数，并根据从 3GPP AAA Server 接收到的 QoS 参数进行修改，执行策略限制功能。

——记录连接的状态 (如鉴权和授权的成功)。

7.2.3.4 可信任的非 3GPP 接入网络具体行为

当收到re-auth请求，可信任的non-3GPP GW应该执行下面的判断，如果有错误检测到，非3GPP接入网络应该停止处理请求并返回相应的错误码。

判断Re-Auth–Request-Type AVP:

a）如果指示 AUTHENTICATE_ONLY，Result-Code 应该设置成 DIAMETER_INVALID_AVP_VALUE。

b）如果指示 AUTHORIZE_AUTHENTICATE，按照 3GPP TS 33.402 发起对用户的鉴权和授权，Diameter 消息格式参照表 43 和表 44。

c）如果指示 AUTHORIZE_ONLY，non-3GPP GW 应该根据表 41 和表 42 定义的执行授权过程。

当授权或者鉴权和授权过程成功，对于请求和接收到的会话中指示的用户标识，可信任的non-3GPP GW应该重写当前的授权信息和从3GPP AAA Server接收到的信息。

如果用户订阅数据中的APN有一个激活的PDN连接被终止时，3GPP AAA Server应发起PDN连接的释放。

如果授权或者鉴权和授权过程失败，非3GPP接入网络应该把用户从非3GPP接入网络中去附着。

如不需要接收到来自AAA Server的重授权请求，可信任的Non-3GPP GW 应该用单步过程发起对用户的重授权，如果从E-UTRAN到HRPD接入，由于优化的空闲态模式移动性，需要更新PDN GW信息。

7.2.4 非 3GPP IP 接入网络发起的会话终结

7.2.4.1 通用

STa接口允许非3GPP接入网络通知3GPP AAA server，非3GPP接入网络分配给特定用户的会话资源将要释放。

这个过程由非3GPP接入网络发起，从3GPP AAA Server删除非3GPP接入信息。这些过程基于IETF RFC 3588的STR和STA命令。

表45 STa 会话终结请求

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	这个IE包含用户的标识，如IMSI在EPC root NAI格式，依据3GPP TS 23.003
Termination Cause	Termination-Cause	必选	包含断开连接的原因

表46 STa 会话终结响应

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code / Experimental-Result	必选	操作的结果。结果代码在Diameter Base Protocol(IETF RFC 3588)中定义。 Experimental-Result AVP 用于S6b错误

7.2.4.2 3GPP AAA Server 具体行为

当收到从非3GPP接入网络来的会话终止请求消息，3GPP AAA Server应检查与接收到的两个参数(Session-Id和User-Name)是否有相关的正在继续的会话。

如果找到由User-Name参数表示的用户相关的激活会话，因为3GPP AAA Server管理该用户，3GPP AAA Server将依据SWx接口的Location Management 流程，去注册这个用户。如果去注册成功，3GPP AAA Server应释放特定会话相关的会话资源，并且会话终止请求应发送给非3GPP接入网络，指示

DIAMETER_SUCCESS。如果HSS的去注册失败，3GPP AAA Server应该返回带有DIAMETER_UNABLE_TO_COMPLY错误码的Session-Termination响应。否则，3GPP AAA Server 应该返回带有DIAMETER_UNKNOWN_SESSION_ID 错误码的Session-Termination响应。

7.2.4.3 3GPP AAA Proxy 具体行为

如果Non-3GPP GW在VPLMN中，3GPP AAA Proxy需要处理漫游场景。3GPP AAA Proxy应该作为有状态的代理。

当接收从非3GPP接入网络来的会话终止请求，3GPP AAA Proxy应该路由该消息到3GPP AAA Server。

当接收从3GPP AAA Server来的会话终止回复，3GPP AAA Proxy应该路由该消息到非3GPP接入网络，如果返回码DIAMETER_SUCCESS，应该释放与特定会话关联的所有本地资源。

7.3 信息单元

7.3.1 概述

表47中定义的AVP适用于PMIP模式下的STa接口协议，定义了AVP码值、类型、可能的标识以及AVP是否被加密。

表47 Diameter STa AVPs

属性名称	AVP 码值	对应章节	值类型	AVP 标志规则				是否要加密
				Must	May	Should not	Must not	
APN-Configuration	1430	5.5.33	Grouped	M				No
MIP6-Feature-Vector	124	7.3.3	Unsigned64	M			V	
QoS-Capability	578	7.3.4	Grouped	M			V	No
RAT-Type	1032	7.3.6	Enumerated	M,V	P			Y
Visited-Network-Identifier	600	5.3.9.1	OctetString	M,V				No
ANID	1504	7.3.7	UTF8String	M, V				No
Service-Selection	493	7.3.5	UTF8String	M	P		V	No
Mobile-Node-Identifier	506	7.3.2	UTF8String	M	P		V	No
AN-Trusted	1503	7.3.9	Enumerated	M, V	P			No

下面的表格描述了STa接口协议重用现有的Diameter应用的AVP，包含它们对应的标准。其他现有Diameter应用的AVP，除了Diameter基本协议外的AVP，其他都不支持。

表48 STa 重用 Diameter AVPs

属性名称	参考文件	备注
Accounting-Interim-Interval	IETF RFC 3588	
Auth-Request-Type	IETF RFC 3588	
Calling-Station-Id	IETF RFC 4005	
EAP-Master-Session-Key	IETF RFC 4072	
EAP-Payload	IETF RFC 4072	
RAT-Type	3GPP TS 29.212	
Re-Auth-Request-Type	IETF RFC 3588	
Session-Timeout	IETF RFC 3588 [	
User-Name	IETF RFC 3588	

表48（续）

属性名称	参考文件	备注
Terminal-Information	3GPP TS 29.272	
MIP6-Agent-Info	IETF RFC 5447	
APN-OI-Replacement	3GPP TS 29.272	
Supported-Features	3GPP TS 29.229	
Feature-List-ID	3GPP TS 29.229	See section 7.3.10
Feature-List	3GPP TS 29.229	See section 7.3.11

7.3.2 Mobile-Node-Identifier

Mobile-Node-Identifier AVP (AVP Code 506)的类型是UTF8String。

Mobile-Node-Identifier AVP 是在响应消息中返回的，它成功地结束了AAA client和AAA server之间的鉴权（可能还有授权）。返回的Mobile Node Identifier可以被当作PMIPv6 MN-ID或者MIPv4 MN-NAI使用。

Mobile-Node-Identifier AVP在 IETF RFC 5779中定义。

7.3.3 MIP6-Feature-Vector

MIP6-Feature-Vector AVP (AVP Code 124)的类型是Unsigned64，并包含64bit的指示位支持非3GPP GW的移动IP能力（当这个AVP在请求中使用），也可以指示3GPP AAA Server授权的移动IP能力（当这个AVP在响应中使用）

STa 接口定义了下列能力:

——MIP6_INTEGRATED (0x0000000000000001)

这个标志是由 non-3GPP GW 和 3GPP AAA Server 设置的，它表示支持 Mobile IPv6 并带有 bootstrapping 功能。

——PMIP6_SUPPORTED (0x0000010000000000)

当这个标志是由 non-3GPP GW 设置时，告知 3GPP AAA Server，non-3GPP GW 支持 PMIPv6。当这个标志是由 3GPP AAA Server 设置时，告知 non-3GPP GW 应该使用 PMIPv6。

——ASSIGN_LOCAL_IP

这个标志是由 3GPP AAA server 设置的，它指示 non-3GPP GW 应该本地分配 IP 地址。

——MIP4_SUPPORTED

这个标志是由 PDN GW 设置的，意思是在 S2a 接口上使用 MIPv4。

——OPTMIMIZED_IDLE_MODE_MOBILITY

如果在空闲态，从 E-UTRAN 移动到 HRPD，需要更新 PDN GW 信息，这个标志由可信任的 Non-3GPP GW 来设置。

7.3.4 QoS Capability

该 AVP 还在研究中。

7.3.5 Service-Selection

Service-Selection AVP 的类型是 UTF8String。

Service-Selection AVP 在 IETF RFC 5778 中定义。

7.3.6 RAT-Type

RAT-Type AVP (AVP code 1032)的类型是Enumerated，它用来标识无线接入网络的类型，具体值依据TS 29.212。

7.3.7 ANID

ANID AVP的类型是 UTF8String; 该AVP包含Access Network Identity; 具体值的定义依据3GPP TS 24.302。

7.3.8 AMBR

请依据 3GPP TS 29.272。

7.3.9 AN-Trusted

AN-Trusted AVP (AVP Code 1503)的类型是Enumerated.

AN-Trusted AVP 是由3GPP AAA Server发送给Non-3GPP 接入网络的，包含了对接入网络是否可信任的判断，使用下面的值：

——TRUSTED (0)

——UNTRUSTED (1)

7.3.10 Feature-List-ID AVP

该AVP的语法依据3GPP TS 29.229。在目前的版本中，Feature-List-ID AVP在STa/SWa应用中应设为1。

7.3.11 Feature-List AVP

该AVP的语法依据 3GPP TS 29.229。空值表示STa/SWa 应用不使用任何特性。

注：目前版本没有定义任何 STa/SWa 的特性。

7.4 返回代码

7.4.1 概述

本节定义的返回代码同时适用于SWa、STa、SWd、SWm、SWx和S6b 接口。

7.4.2 成功(Success)类别

成功类别的返回代码用来通知对端其请求已经被成功完成。其Result-Code AVP应使用在 RFC3588中定义的成功(Success)类别的值。

7.4.3 永久失败(Permanent Failures)类别

7.4.3.1 概述

属于永久失败(Permanent Failures)的错误用来通知对端其请求不成功，并且不应该再重发。Result-Code AVP值使用定义在RFC3588中定义的值。当这里定义的返回值被包含在一个回应中时，它应被放在Experimental-Result AVP中，并且Result-Code AVP应不存在。

7.4.3.2 DIAMETER_ERROR_USER_UNKNOWN(5001)

该返回值应由HSS发送，表明用户标识IMSI不可知。

7.4.3.3 DIAMETER_ERROR_IDENTITY_NOT_REGISTERED(5003)

该返回值应由HSS发送，表明该用户当前没有登记任何3GPP AAA服务器。

7.4.3.4 DIAMETER_ERROR_ROAMING_NOT_ALLOWED(5004)

该返回值应由HSS发送，表明不允许该用户漫游到一个非3GPP的VPLMN。

7.4.3.5 DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED(5005)

该返回值应由HSS发送，表明试图注册到该3GPP AAA服务器上的网元标识已经被注册给一个特定用户。

7.4.3.6 DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION(5450)

该返回值应由HSS发送，表明IMSI正关联了一个非3GPP的签约信息。

7.4.3.7 DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION(5451)

该返回值应由3GPP AAA服务器发送，表明被请求的APN没有被包含在用户的概要(profile)中，因此该用户无权使用。

7.4.3.8 DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED(5452)

该返回值应由HSS发送，表明该IMSI不允许使用目前UE正使用的RAT类型。

7.4.4 临时失败(Transient Failures)类别

临时失败（Transient Failures）类别中的返回值应被用于通知对端，其请求在被收到的时刻并不被接受，但未来有可能被接受。Diameter 基础协议RFC 3588中定义的Result-Code AVP应被执行。当本节定义的返回值使用在响应消息里时，该返回值应该放在 Experimental-Result AVP中，并且 Result-Code AVP应不存在。

本标准中没有定义临时失败的返回值。

8 SWd 接口

8.1 概述

SWd接口是3GPP AAA Proxy经过中间网络连接到3GPP AAA Server的接口。其主要功能是以可靠安全方式传输认证、授权及相关信息。SWd接口应传输EAP认证消息。

SWd接口传输包含下面内容的AAA消息：

——3GPP AAA Server 与 3GPP AAA Proxy 之间用于认证信令的数据；

——3GPP AAA Server 与 3GPP AAA Proxy 之间用于授权信令的数据；

——每一个用户的计费信令；

——用于空口完整性保护和加密的密钥数据；

——用于隧道建立、隧道数据认证和加密目的的认证数据，其对应 ePDG 位于 VPLMN 的场景；

——ePDG 通过 3GPP AAA Server 向 3GPP AAA Proxy 发送的用户标识 ID 到隧道标识 ID 的映射信息；

——在立即业务终止情形下从接入网络清除用户；

——传输运营商网络标识，支持用户在不同运营商网络之间漫游；

——根据每个用户所授权的业务信息，向接入网络提供接入范围性质的限制信息（例如，IP 地址过滤器）；

——如果采用 QoS 机制，在 3GPP AAA Proxy 到 3GPP AAA Server 的认证请求消息中传输接入网络 QoS 能力及策略的数据（例如，所支持的 3GPP QoS 集）。

SWd接口是基于IETF RFC3588定义的Diameter协议，但是包含下面的扩展：

——IETF RFC4005，其定义了用于网络接入服务器中认证、授权和记账业务的 Diameter 协议应用；

——IETF RFC4072，其定义了在 Diameter 上支持传输 EAP（IETF RFC 3748）帧的 Diameter 应用；

——IETF RFC 5779，其定义了用于 PMIPv6 MAG 到 AAA 和 LMA 到 AAA 两个接口上的 Diameter 扩展和应用；

——IETF RFC5447，其定义了用于 Mobile IPv6 NAS 到 AAA 接口上的 Diameter 扩展。

Swd接口不定义单独的应用ID。3GPP AAA Proxy使用的应用ID依赖于SWd接口上发送的Diameter命令消息。尽管3GPP AAA Proxy可能会在所前转到或前转给3GPP AAA Server的Diameter命令消息中添加新的AVP，但是3GPP AAA Proxy在Swd接口上转发该消息时应能够使用原有的应用ID标识。

8.2 消息

8.2.1 可信 non-3GPP 接入认证和授权

在使用STa接口情形下，SWd接口应支持7.2.1章节中可信的non-3GPP接入认证和授权过程。3GPP AAA Proxy以有状态Diameter Proxy角色前转来自3GPP AAA Server和可信non-3GPP网关的Diameter命令消息。除此之外，3GPP AAA Proxy还具有下面的功能：

——如果不允许属于指定 HPLMN 网络的用户在 VPLMN 中漫游，则 3GPP AAA Proxy 可能拒绝认证和授权请求消息。

——如果前转了认证和授权请求消息，3GPP AAA Proxy 应检查消息中受访网络标识符 AVP 的存在性和值合法性。如果这个 AVP 不存在，3GPP AAA Proxy 应插入该 AVP；如果这个 AVP 存在，则在前转前可以覆盖这个 AVP 值。

——3GPP AAA Prxoy 可以修改 AAA 应答消息中业务授权信息，然后转发给可信的 non-3GPP 接入网关，其目的是能够根据本地策略和漫游协议执行 QoS 限制。

——3GPP AAA Proxy 可以从 VPLMN 的角度确定 non-3GPP 接入的信任程度，并在 AAA 请求消息中插入可信关系指示。

表49 SWd 接口用于于可信 Non-3GPP 接入认证授权请求消息

信息单元名称	映射到Diameter AVP	类型	描述
User Identity	User-Name	必选	这个IE应包含用户标识。按照RFC4282所指定的NAI形式和TS23.003所定义的格式表示这个用户标识
EAP payload	EAP-payload	必选	这个IE应包含封装EAP净荷，目的是用于UE与3GPP AAA服务器之间的互相认证
Authentication Request Type	Auth-Request-Type	必选	这个IE应定义用户是否只是认证、只是授权或者认证授权。在这种情形下应使用认证授权（AUTHORIZE_AUTHENTICATE）
UE Layer-2 address	Calling-Station-ID	必选	这个IE应包含UE的层2地址
Supported 3GPP QoS profile	QoS-Capability	可选	如果可信non-3GPP接入系统支持QoS机制，则这个IE包含了RFC5777所定义的接入网络QoS能力
Mobility Capabilities	MIP6-Feature-Vector	条件可选	如果采用动态移动性模式选择机制，则这个IE应包含可信non-3GPP接入网络的移动性能力。如果可信non-3GPP接入网络支持PMIPv6协议（RFC5779），则这个字段设置为PMIP6_SUPPORTED。如果按照RFC5447定义的支持基于DHCPv6de归属代理地址发现机制，则应设置为MIP6_INTEGRATED
Access Type	RAT-Type	必选	这个IE应包含服务UE的可信non-3GPP接入网络技术类型
Access Network Identity	ANID	必选	这个IE应包含接入网络标识符，其用于HSS中获取密钥。所有可能的值依据TS23.402的描述
Visited Network Identifier	Visited-Network-Identifier	必选	这个IE应包含拜访网络标识符，其允许归属网络识别拜访网络
APN Id	Service-Selection	可选	如果存在，则这个IE应包含用户想要连接的APN（如果有效）

表49（续）

信息单元名称	映射到Diameter AVP	类型	描述
Terminal Information	Terminal-Information	可选	如果存在，则这个IE应包含用户移动设备信息。所携带的标识类型依赖于接入网络技术类型。对于HRPD接入网络，这个组类型AVP中包含3GPP2-MEID AVP
Trust Relationship Indicator	AN-Trusted	可选	如果存在，则这个AVP应从VPLMN角度看表达了non-3GPP IP接入网络的可信或者不可信的决定指示

8.2.1.1 用于 STa PMIPv6 认证和授权过程的消息 DER/DEA

Diameter-EAP-Request命令，是从可信non-3GPP接入网络网关发送到3GPP AAA Server，其命令码字段设置为268，命令标志字段中"R"位设置为1。其他继续使用IETF RFC5779中的ABNF。

```
< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY, 16777250 >
                            < Session-Id >
                            { Auth-Application-Id }
                            { Origin-Host }
                            { Origin-Realm }
                            { Destination-Realm }
                            { Auth-Request-Type }
                            { EAP-Payload }
                            [ User-Name ]
                            [ Calling-Station-Id ]
                            ...
                            [ RAT-Type ]
                            [ ANID ]
                            [ QoS-Capability ]
                            [ MIP6-Feature-Vector ]
                            [ Visited-Network-Identifier ]
                            [ Service-Selection ]
                            [ Terminal-Information ]
                            [ AN-Trusted ]
                            *[ Supported-Features ]
                            ...
                            *[ AVP ]
```

Diameter-EAP-Answer(DEA)命令，是从3GPP AAA Server发送到3GPP AAA Proxy，其命令码字段设置为268，其命令标记字段中的"R"位清零。继续使用IETF RFC 5779和RFC 4072中所定义的ABNF。

```
< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY, 16777250 >
                            < Session-Id >
                            { Auth-Application-Id }
                            { Result-Code }
```

[Experimental-Result]
{ Origin-Host }
{ Origin-Realm }
{ Auth-Request-Type }
{ EAP-Payload }
[User-Name]
[Session-Timeout]
[Accounting-Interim-Interval]
[EAP-Master-Session-Key]
[Context-Identifier]
[APN-OI-Replacement]
*[APN-Configuration]
[MIP6-Feature-Vector]
[Mobile-Node-Identifier]
*[Redirect-Host]
*[Supported-Features]
...
*[AVP]

8.2.2 可信 non-3GPP 接入网络中 HSS/AAA 发起的去附着

在使用STa接口情形下，SWd接口应支持7.2.2节中所定义的HSS发起的去附着过程。在这种情形下，3GPP AAA Proxy应以有状态Diameter Proxy的角色前转从3GPP AAA Server和接入网络网关接收到的Diameter命令消息。

8.2.2.1 用于 STa 接口的 HSS/AAA 发起的去附着消息

与7.2.2节中HSS/AAA发起的去附着消息相同。

8.2.3 接入与业务授权信息更新

在使用STa接口情形下，SWd接口应支持7.2.3节中所定义的可信non-3GPP接入与业务授权信息更新过程（即STa重鉴权和重授权过程）。在这种情形下，3GPP AAA Proxy应以有状态Diameter Proxy的角色前转从3GPP AAA Server和可信non-3GPP网关接收到的Diameter命令消息，但还具有下面的功能：

——如果转发一个认证授权请求消息，3GPP AAA Proxy 应检查消息中的受访网络标识符存在和其值。如果不存在，应在消息中插入该值。如果存在，在前转该请求消息时可以覆盖该 AVP。

——3GPP AAA Proxy 可以修改认证授权应答消息中的业务授权信息，然后转发给可信 non-3GPP 接入网关，其目的是根据本地策略和漫游协议执行 QoS 限制。

表格50描述在SWd接口上所转发的可信non-3GPP接入授权请求消息。由于消息内容非常类似于STa接口上所接收到的请求消息的内容，仅仅列出了在两个接口上需要不同处理的AVP。

表50 SWd 接口用于可信 Non-3GPP 接入授权请求消息

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	这个IE包含用户ID。这个ID是按照TS23.003所定义的格式，以IETF RFC4282协议中NAI格式表示
Request-Type	Auth-Req-Type	必选	下面值只使用: AUTHORIZE_ONLY这个值应指示授权用户访问APN的初始请求
Visited Network Identifier	Visited-Network-Identifier	必选	允许归属网络识别受访网络的标识符
Routing Information	Destination-Host	必选	3GPP AAA Server名字从前面接收消息中的Origin-Host AVP中获取
Supported 3GPP QoS profile	QoS-Capability	可选	如果可信non-3GPP接入网络支持QoS机制，应在这个IE中包含这个接入网络QoS能力，其按照IETF RFC 5777所定义的要求
Access Type	RAT-Type	可选	如果存在，这个IE包含服务UE的可信non-3GPP接入网络技术类型

更为详细的 3GPP AAA Proxy 行为，依据 7.2.3.3 节描述。

8.2.3.1 用于 STa 接口的接入与业务授权更新请求消息

与7.2.3.1节中定义的用于STa接口的接入与业务授权更新请求消息与表39、表41和表43 中的定义相同。

8.2.3.2 用于 STa 接口的接入与业务授权更新响应消息

与7.2.3.1节中定义的用于STa接口的表40、表42和表44中定义的STa接入鉴权和授权响应消息相同。

8.2.4 可信 non-3GPP IP 接入网络发起的会话终止

在使用STa接口情形下，SWd接口应支持7.2. 4节中所定义的接入网络发起的会话终止过程。在这种情形下，3GPP AAA Proxy应已有状态Diameter Proxy角色前转来自3GPP AAA Server和接入网络网关的Diameter命令消息。

8.2.4.1 可信 non-3GPP IP 接入网络发起的会话终止消息

与7.2.4节中可信non-3GPP IP接入网络发起的会话终止消息相同。

8.2.5 非可信 non-3GPP 接入/ePDG 相关消息

在使用SWm接口情形下，SWd接口应支持下面的过程：

——附录 C.2.1 节中所定义的认证过程；

——附录 C.2.2 节中所定义的授权过程；

——附录 C.2.3 节中所定义的接入网络/ePDG 发起的会话终止过程；

——附录 C.2.4 节中所定义的 HSS/AAA 发起的去附着过程；

——附录 C.2.5 节中所定义的业务授权信息更新过程。

在上述过程中，3GPP AAA Proxy应已有状态Diameter Proxy角色前转来自3GPP AAA Server和ePDG的Diameter命令消息，还包含下面的功能：

——如果不允许属于指定 HPLMN 的用户漫游，3GPP AAA Proxy 可以拒绝认证请求消息或授权请求消息。

——3GPP AAA Proxy 可以修改授权应答消息中的业务授权信息，然后将其前转给 ePDG，其目的是根据本地策略和漫游协议执行 QoS 执行。

8.2.5.1 与 SWm 接口连接相关联的消息

与附录C.3节中所定义的Diameter命令消息相同。

8.2.6 PGW 相关的过程

在使用S6b接口情形下，SWd接口应支持下面的过程：

——使用 10.2.1 节中定义的 PMIPv6 协议时，授权过程；

——10.2.2 节所定义的 PGW 发起的会话终止过程；

——10.2.3 节所定义的 HSS/AAA 发起的去附着过程；

——10.2.4 节所定义的业务授权信息更新过程。

在上述情形下，3GPP AAA Proxy应已有状态Diameter Proxy角色前转来自3GPP AAA Server和PGW的Diameter命令消息，还包含下面的功能：

——如果不允许属于指定 HPLMN 的用户漫游，3GPP AAA Proxy 可以拒绝认证请求消息或者授权请求消息。

——3GPP AAA Proxy 可以在授权应答消息中修改业务授权信息，然后前转给 PGW，目的是根据本地策略和漫游协议执行 QoS 限制。

8.2.6.1 与 S6b 接口连接相关联的 Diameter 命令消息

与10.3节中所定义的Diameter命令消息相同。

8.3 信息单元

表51描述了PMIPv6模式下SWd接口上所定义的Diameter AVP参数。

表51 Diameter SWd AVPs

属性值对名称	AVP代码	值类型	AVP Flag规则					参考章节
			Must	May	Should not	Must not	May Encr	
APN-Configuration	1430	Grouped	M				No	5.3.3.
MIP6-Feature-Vector	124	Unsigned64	M			V		7.3.3
QoS-Capability	578	Grouped	M			V	No	7.3.4
RAT-Type	1032	Enumerated	M,V	P			Y	7.3.6
Visited-Network-Identifier	600	UTF8String	M,V				No	5.3.91
ANID	1504	UTF8String	M, V				No	7.3.7
Service-Selection	493	UTF8String	M	P		V	No	7.3.5
Mobile-Node-Identifier	506	UTF8String	M	P		V	No	7.3.2
AN-Trusted	1503	Enumerated	M,V	P			No	7.3.9

表52描述了SWd接口继续使用现有Diameter应用的Diameter AVP，其中包含各自的参考规范。除了Diameter 基础协议外，不需要支持现有Diameter应用所使用的其他Diameter AVP。

表52 SWd 继续使用的 Diameter AVPs

属性值名称	参考	备注
Accounting-Interim-Interval	IETF RFC 3588	
Auth-Request-Type	IETF RFC 3588	
Calling-Station-Id	IETF RFC 4005	
EAP-Master-Session-Key	IETF RFC 4072	
EAP-Payload	IETF RFC 4072	
RAT-Type	3GPP TS 29.212	

表52（续）

属性值名称	参考	备注
Re-Auth-Request-Type	IETF RFC 3588	
Session-Timeout	IETF RFC 3588	
User-Name	IETF RFC 3588	
Terminal-Information	3GPP TS 29.272	
APN-OI-Replacement	3GPP TS 29.272	
Supported-Features	3GPP TS 29.229	参见注
Feature-List-ID	3GPP TS 29.229	参见注
Feature-List	3GPP TS 29.229	参见注
注：SWd接口没有定义单独的Diameter应用ID，因此不需要单独的支持特性列表，所支持的特性依赖于Swd接口上代理的命令消息		

8.4 返回代码

同7.4节。

9 SWx 接口

9.1 概述

SWx是3GPP AAA Server和HSS之间的接口，主要用于对UE连接到EPC是做认证和鉴权，同时用来更新HSS上存储的PDN-GW的地址信息。

9.2 消息

9.2.1 鉴权消息(MAR/MAA)

如下场景需要 3GPP AAA Server 向 HSS 发起鉴权消息：

a）当一个新用户访问“可信的非 3GPP 接入网”或者“非可信的非 3GPP 接入网”时；

b）已经接入 3GPP AAA 服务器的用户需要申请一组新的鉴权向量时；

c）当 3GPP AAA 服务器检测到当前服务 PLMN 或者接入网发生变化时。

表 53 和表 56 分别是鉴权数据请求消息和鉴权数据响应消息的信息单元列表。表 54 和表 55 分别表示“正常鉴权”和“重同步鉴权”两种场景下鉴权请求消息（MAR）中 Authentication Data 信元的内容。

表53 鉴权数据请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户身份标识，主要指IMSI
Visited Network Identifier	Visited-Network-Identifier	条件可选	允许从归属域漫游的漫游域的漫游网络索引。如果3GPP AAA 服务器从SWd信令接口获得了这个信元，则在MAR消息中携带中这个参数
Number Authentication Items	SIP-Number-Auth-Items	必选	这个参数指示需要请求的鉴权向量的个数
Authentication Data	SIP-Auth-Data-Item	条件可选	此信元的内容请参考表54和表55，分别定义了“正常鉴权”和“重同步鉴权”两种场景下此信元的内容

表53（续）

信息单元名称	映射到Diameter AVP	类别	描述
Routing Information	Destination-Host	条件可选	如果3GPP AAA服务器已经知道HSS的地址，这个参数就会出现。 只有3GPP AAA服务器已经存储的HSS地址的情况下此信元才可用。 HSS地址来自于上次收到的HSS命令或SLF命令中的Origin-Host信元。 否则只应该携带Destination-Realm信元，以便通过SLF（或者类似功能实体）解析得到一个HSS的地址。一旦获取到合适的HSS地址，3GPP AAA服务器需要存储这个地址为以后备用
Access Network Identity	ANID	条件可选	这个参数包含接入网络标识（参见3GPP TS 24.302所有取值）供HSS进行密钥推导。 如果鉴权方式是EAP-AKA'，这个参数应存在
Access Type	RAT-Type	必选	这个参数包含无线接入类型（参见3GPP TS 29.212所有取值）
Terminal Information	Terminal-Information	可选	这个参数包含用户移动终端的设备信息。只有3GPP AAA服务器从非3GPP接入网关的鉴权或认证请求消息中收到此信息时，才会携带此信元。3GPP AAA服务器透传此信元给HSS
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

表54 MAR消息在正常鉴权场景下Authentication Data信元的内容

信息单元名称	映射到Diameter AVP	类别	描述
Authentication Method	SIP-Authentication-Scheme	必选	这个参数指示鉴权方式，可能取值EAP-AKA或者EAP-AKA,EAP-AKA'在IETF RFC 5448中定义

表55 MAR消息在重同步场景下Authentication Data信元的内容

信息单元名称	映射到Diameter AVP	类别	描述
Authentication Method	SIP-Authentication-Scheme	必选	这个参数指示鉴权方式，包括EAP-AKA,或者EAP-AKA'
Authorization Information	SIP-Authorization	必选	这个参数的取值由RAND的取值和Auts的取值串接而成。RAND是送给终端的数据，Auts是从来自终端的数据。rand和auts都是二进制加密的

表56 鉴权数据响应消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	应	用户身份标识，主要是指IMSI
Number Authentication Items	SIP-Number-Auth-Items	条件可选	这个参数指示鉴权数据消息中的鉴权向量的个数。当返回码为DIAMETER_SUCCESS时，这个参数会出现
Authentication Data	SIP-Auth-Data-Item	条件可选	当SIP-Number-Auth-Items为0，或者不存在的时候，这个参数不会出现。 此信元的内容请参考表57

表56（续）

信息单元名称	映射到Diameter AVP	类别	描述
3GPP AAA Server Name	3GPP-AAA- Server-名称	条件可选	这个参数包含3GPP AAA服务器的Diameter地址。 当用户已经被另一个3GPP AAA服务器鉴权通过，已经由另一个服务器为用户服务的时候，这个参数会出现
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示SWx的错误
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

表 57 表示 MAA 消息中 Authentication Data 信元的取值和内容。

表57　MAA 消息中 Authentication Data 信元内容

信息单元名称	映射到Diameter AVP	类别	描述
Item Number	SIP-Item-Number	条件可选	当出现多个SIP-Auth-Data-Item信元并且需要按顺序处理这些信元时，这个参数包含在SIP-Auth-Data-Item参数中 在这种情况下，包含SIP-Item-Number值小的SIP-Auth-Data-Item应该比包含SIP-Item-Number值大的SIP-Auth-Data-Item先处理
Authentication Method	SIP-Authentication Scheme	必选	这个参数指示鉴权方式，包括EAP-AKA,或者EAP-AKA'
Authentication Information AKA	SIP-Authenticate	必选	这个参数以二进制方式编码，取值由挑战随机数RAND和AUTN密串的取值串接而成。更多细节参见3GPP TS 33.203
Authorization Information AKA	SIP-Authorization	必选	这个参数以二进制方式编码，表示期望响应XRES。更多细节参见3GPP TS 33.203
Confidentiality Key AKA	Confidentiality-Key	必选	这个参数包含加密密钥CK或者CK',这个参数以二进制方式编码
Integrity Key AKA	Integrity-Key	必选	这个参数包含完整性密钥IK或者IK'。这个参数以二进制方式编码

9.2.2　非 3GPP IP 接入注册消息(SAR/SAA)

如下场景需要 3GPP AAA Server 主动发起 SAR 消息：

a）通知 HSS 记录当前服务某个非 3GPP 用户的 3GPP AAA 服务器地址。当一个新的用户的身份被 3GPP AAA 服务器鉴别通过之后，3GPP AAA 服务器发起这个消息。

b）通知 HSS 清除当前服务某个非 3GPP 用户的 3GPP AAA 服务器地址到。3GPP AAA Server 准备删除某个非 3GPP 用户的接入信息（例如：STa、SWm、S6b 会话被终结）或者 OCS（在线计费系统）发起断链请求，3GPP AAA 服务器向 HSS 通知这个断链事件，此时 HSS 清除该非 3GPP 用户的注册信息。

c）必要时下载用户签约数据到 3GPP AAA 服务器。如果因为某些原因导致某个用户的签约数据丢失，时 3GPP AAA 发起此消息。

d）由于 non-3GPP 接入时 PDN 连接建立或者 PDN 断链，需要更新 PGW 标识到 HSS 中，此时需要 3GPP AAA 服务器主动发起 SAR 消息。

表 58 和表 59 分别表示非 3GPP IP 接入注册请求消息和非 3GPP IP 接入注册响应消息的信息单元列表。

表58 非 3GPP IP 接入注册请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户身份标识，主要是指IMSI
Server Assignment Type	Server-Assignment-Type	必选	此信元指出3GPP AAA服务器要求HSS执行的处理过程。 如果此信元取值为REGISTRATION，HSS为非3GPP用户执行注册过程。 如果此信元取值为USER_DEREGISTRATION/ADMINISTRATIVE_DEREGISTRATION / REAUTHENTI CATION _FAILURE，HSS注销此非3GPP用户。 如果此信元取值为AAA_USER_DATA_REQUEST，HSS下发用户签约数据给3GPP AAA服务器，但是请注意此时HSS不允许执行注册过程。 如果此信元取值为PGW_UPDATE，HSS检查存储的3GPP AAA服务器名是否是用户当前注册的AAA服务器，并更新为此用户的存贮的PGW 身份标识。 如果这个参数为其他取值，则为异常处理
Routing Information	Destination-Host	条件可选	如果3GPP AAA服务器已经知道HSS的地址，这个参数就会出现。 HSS地址来自于上次收到的HSS命令或SLF命令中的Origin-Host信元。 否则只应该携带Destination-Realm信元以便通过SLF(或者类似功能实体) 解析得到一个HSS的地址。一旦获取到合适的HSS地址，3GPP AAA服务器存储这个信息为以后备用
PGW identity	MIP6-Agent-Info	条件可选	此信元包含动态分配的PDN GW的身份标识，当Server-Assignment-Type为PGW_UPDATE时，这个参数应该出现。 如果通知HSS删除一个APN的PDN GW时，这个参数不应该出现
PGW PLMN ID	Visited-Network-Identifier	条件可选	此信元包含当前动态分配的PDN GW所处的PLMN的标识
Context Identifier	Context-Identifier	可选	此信元用来标识当前被重新分配的或要被删除的PDN GW相关的APN的配置信息。 只有当Server-Assignment-Type为PGW_UPDATE，并且此参数可用的时候，这个信元才出现
APN Id	Service-Selection	条件可选	当Server-Assignment-Type为PGW_UPDATE时，这个参数包含APN信息
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表
IMSI	User-名称	必选	用户身份标识，主要是指IMSI.
Registration result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示SWx的错误，包括： - User Unknown 用户不存在

表59 非 3GPP IP 接入注册响应消息

信息单元名称	映射到Diameter AVP	类别	描述
User Profile	Non-3GPP-User-Data	条件可选	此信元包含当前指定用户的签约数据。当SAR消息中的Server-Assignment-Type信元取值为AAA_USER_DATA_REQUEST或者REGISTRATION，并且响应消息中的Result-Code信元取值为DIAMETER_SUCCESS时，这个参数才出现
3GPP AAA Server Name	3GPP-AAA- Server-名称	条件可选	这个参数包含3GPP AAA服务器的Diameter地址。 当用户已经被另一个3GPP AAA服务器鉴权通过，已经由另一个服务器为用户服务的时候，这个参数会出现
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

9.2.3 HSS 发起的用户去活消息(RTR/RTA)

这个消息用在3GPP AAA服务器与HSS之间，用来删除non-3GPP用户以前的登记和所有的关联状态。该消息由HSS发起，指示AAA用户应被删除。

表60和表61分别指示HSS发起的用户去活请求消息和用户去活响应消息的信息单元列表。

表60 HSS 发起的用户去活请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户身份标识，主要是指IMSI
Reason for de-registration	Deregistration-Reason	必选	此信元包含HSS给3GPP AAA服务器发起注销的原因。这个注销原因分为两部分：一部分是转发给被注销用户的文本信息；另一部分是用来决定3GPP AAA服务器行为的原因码（依据3GPP TS 29.229）
Routing Information	Destination-Host	必选	从3GPP AAA服务器发送的请求消息的Origin-Host信元中获取的3GPP AAA服务器地址
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

表61 HSS 发起的用户去活响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示SWx的错误
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

9.2.4 HSS 发起的用户签约数据更新消息 (PPR/PPA)

当用户签约数据被修改时，这个消息由HSS发起到3GPP AAA服务器。

表62和表63分别表示HSS发起的用户签约数据更新请求消息和用户签约数据更新响应消息的信息单元列表。

表62 用户签约数据更新请求消息

信息单元名称	映射到Diameter AVP	类别	描述
IMSI	User-Name	必选	用户身份标识，主要是指IMSI
User profile	Non-3GPP-User-Data	必选	此信元包含需要被更新的用户签约数据。在跟踪业务激活或者去激活时，此信元应该包含Trace-Info子信元，并且可能是此信元中唯一存在的子信元

表62（续）

信息单元名称	映射到Diameter AVP	类别	描述
Routing Information	Destination-Host	必选	从3GPP AAA服务器发送的请求消息的Origin-Host信元中获取的3GPP AAA服务器地址
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

表63 用户签约数据更新响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code / Experimental-Result	必选	这个参数包含操作结果。Result-Code用于指示Diameter基础协议所定义的成功或者错误码。 Experimental-Result用于指示SWx的错误
Supported Features	Supported-Features	可选	这个参数如果出现，将包含源主机支持的特性列表

10 S6b 接口

10.1 概述

S6b接口使用于3GPP AAA Server/Proxy和PDN GW之间。

S6b接口基于IETF RFC 3588定义Diameter以及如下的扩展：

——IETF RFC 4005所定义的在网络接入服务器(NAS)环境下用于AAA服务的Diameter协议应用。

——IETF RFC 5779所定义的用于PMIPv6 MAG与AAA接口和LMA和AAA接口的Diameter扩展和应用。

——IETF RFC 5777所定义的用于Dianmeter设备间的用来传达QoS信息的属性值对。

LMA 与 3GPP AAA Server 之间或 LMA 与 3GPP AAA Server proxy 之间的通信要使用 IETF RFC 5779 定义的 LMA 与 AAA 间的接口功能来更新 3GPP AAA Server 的 PDN GW 标识并且可选的获取移动性相关的参数和静态的 QoS 设置。

当 UE 用 S2a 或 S2b 参考点附着到 EPC 并使用 PMIPv6 时，PDN-GW 成为 LMA。当 UE 用 S2a 参考点附着到 EPC 并使用 MIPv4 时，PDN-GW 成为 HA。

当 UE 用 S2c 参考点附着到 EPC 时，PDN GW 和 HA 间的通信要执行 IETF RFC 5778。应用表示要在 S6b 参考点广播，并遵循 IETF RFC 5778 定义的 DSMIPv6 "Diameter Mobile IPv6 IKE (MIP6I)"应用标识。

基于 IKEv2 EAP 的主动身份验证用来身份认证及鉴全 UE 及更新 PDN-GW 标识。这种情形下，PDN GW 或 HA 成为基于 3GPP TS 33.234 的 NAS。

10.2 消息

10.2.1 S6b PMIPv6 身份认证过程的命令

10.2.1.1 AA-Request (AAR) 命令

AA-Request (AAR)命令标识为设成265的命令码域及命令标志域的“R”比特被设置，该命令从PDN GW发到一个3GPP AAA服务器。命令码域值和ABNF重用自IETF RFC 4005的AA-Request命令。在原有的ABNF基础上使用*[AVP]扩展机制扩展了新的AVP。

<AA-Request> ::= < Diameter Header: 265, REQ, PXY, 16777272 >
< Session-Id >
{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Auth-Request-Type }
[User-Name]
[MIP6-Agent-Info]
[MIP6-Feature-Vector]
[QoS-Capability]
[Service-Selection]
*[Supported-Features]
...
*[AVP]

10.2.1.2 AA-Answer (AAA) 命令

AA- Answer (AAR)命令标识为设成265的命令码域及命令标志域的“R”比特被清除，该命令从3GPP AAA服务器发到一个PDN GW。命令码域值和ABNF重用自IETF RFC 4005的AA- Answer命令。在原有的ABNF基础上使用*[AVP]扩展机制扩展了新的AVP。

<AA-Answer> ::= < Diameter Header: 265, PXY, 16777272 >
< Session-Id >
{ Auth-Application-Id }
{ Auth-Request-Type }
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
...
[MIP6-Feature-Vector]
[Session-Timeout]
[QoS-Resources]
*[Redirect-Host]
[Trace-Info]
*[Supported-Features]
...
*[AVP]

10.2.2 PDN GW 发起的会话终结流程及消息

通过S6b参考点，PDN GW通知3GPP AAA 服务器终端（UE）释放了和某一APN相关的PDN连接，因而会删除为此PDN连接建立的移动会话. STR由PDN GW发给3GPP AAA服务器。当和某一PDN GW相关的最后一个PDN连接删除时，3GPP AAA服务器将删除此PGW的信息。

表64 会话终结请求

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	用户标识.
Termination Cause	Termination-Cause	必选	会话释放原因

表65 S6b 会话终结应答

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code / Experimental-Result	必选	指示会话操作结果 Result-Code 用于 DBP的错误. Experimental-Result 用于S6b的错误

10.2.3 3GPP AAA 发起的会话终结流程及消息

通过S6b参考点，3GPP AAA请求PDN GW删除某一由UE激活的PDN连接。PDN 连接由Session-ID AVP和User-Name AVP 来标识。3GPP AAA发起的会话终结流程重用了由NASREQ IETF RFC 4005定义的STR，STA，ASR和ASA命令。

如果3GPP AAA不要求PDN GW发起STR，应在ASR命令的Auth-Session-State AVP中包括NO_STATE_MAINTAINED。如果3GPP AAA要求PDN GW发起STR，应该不包括Auth-Session-State AVP，或者在Auth-Session-State AVP中包括STATE_MAINTAINED。

表66 终结会话请求

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	用户标识.
Auth-Session-State	Auth-Session-State	可选	如果3GPP AAA 服务器包括此信元,告诉 PDN GW是否要求发起STR消息

10.3 信息单元

10.3.1 Non-3GPP-User-Data

Non-3GPP-User-Data 是Grouped类型，包含用户相关EPS业务信息。参数格式如下：

```
Non-3GPP-User-Data ::= < AVP Header: 1500 10415 >
                        [ Subscription-ID ]
                        [ Non-3GPP-IP-Access ]
                        [ Non-3GPP-IP-Access-APN ]
                        *[ RAT-Type ]
                        [ Session-Timeout ]
                        [ MIP6-Feature-Vector ]
                        [ AMBR ]
                        [ 3GPP-Charging-Characteristics ]
                        [ Context-Identifier ]
                        [ APN-OI-Replacement ]
```

*[APN-Configuration]

[Trace-Info]

*[AVP]

AMBR包含AMBR关联的用户订阅信息（UE-AMBR）。

APN-OI-Replacement包含终端级别APN-OI-Replacement关联的用户订阅信息。APN-OI-Replacement比APN-Configuration参数包含的APN级别的APN-OI-Replacement优先级低。

Non-3GPP-IP-Acess， Non-3GPP-IP-Access-APN， the Context-Identifier AVP 至少有一个在APN-Configuration中存在，除非当Non-3GPP-User-Data标识为一个已注册用户通过SWx接口下载跟踪激活或者去激活信息。在这种特殊情况下，Trace-Info参数应存在，其他参数可选。

10.3.2 Subscription-ID

Subscription-ID 是一个Grouped类型，指示用来计费的用户标识，它按照 RFC 4006的定义。EPC仅仅用IMSI和MSISDN作为用户标识。这个组类型的参数中的子参数Subscription-Id-Type设为“END_USER_E164”或者“END_USER_IMSI”，子参数Subscription-Id-Data设为MSISDN的值。参数格式如下：

Subscription-Id ::= < AVP Header: 443 >

[Subscription-Id-Type]

[Subscription-Id-Data]

10.3.3 Non-3GPP-IP-Access

Non-3GPP-IP-Access是个Enumerated类型的参数，允许运营商决定闭锁3GPP-非3GPP之间的用户。枚举值定义如下：

a） NON_3GPP_SUBSCRIPTION_ALLOWED (0)

该用户有非 3GPP 用户接入 EPC 网络的订阅。

b） NON_3GPP_SUBSCRIPTION_BARRED (1)

该用户没有非 3GPP 用户接入 EPC 网络的订阅。

10.3.4 Non-3GPP-IP-Access-APN

Non-3GPP-IP-Access-APN是一个Enumerated类型（AVP码是1502），允许运营商同一时间禁用一个用户所有的APN。参数取值定义如下：

a）Non_3GPP_APNS_ENABLE (0)

一个用户的所有 APN 可以用。

b）Non_3GPP_APNS_DISABLE (1)

一个用户的所有 APN 被禁用。

10.3.5 RAT-Type

RAT-Type（AVP 码是1032）是一个Enumerated类型的参数，用来识别为终端服务的无线继而技术。

10.3.6 Session-Timeout

Session-Timeout是一个Unsigned32类型，其定义依据IETF RFC 3588,用来指示一个会话的用秒计算的最大周期。这个参数用于重鉴权流程。如果这个字段没有用，非3GPP 接入节点将用默认时间间隔。

10.3.7 APN-Configuration

定义参见5.3.33节。

10.3.8 ANID

ANID是一个UTF8String类型，这个参数包含接入网络的标识。

10.3.9 SIP-Auth-Data-Item

SIP-Auth-Data-Item 格式如下：

```
SIP-Auth-Data-Item ::= < AVP Header: 612 10415 >
                       [ SIP-Item-Number ]
                       [ SIP-Authentication-Scheme ]
                       [ SIP-Authenticate ]
                       [ SIP-Authorization ]
                       [ Confidentiality-Key ]
                       [ Integrity-Key ]
                       *[ AVP ]
```

10.3.10 Confidentiality-Key

Confidentiality-Key是一个OctetString，包括机密性密钥，或使用后密钥派生接入网络标识符，保密密钥。3GPP AAA不管受到CK还是CK'，都是透传给终端。

10.3.11 Integrity-Key

Integrity-Key是一个OctetString，包含完整性密钥（IK）的，或使用后密钥派生接入网络标识符，完整性密钥(IK')。3GPP AAA不管收到IK还是IK'，都是透传给终端。

10.3.12 Server-Assignment-Type AVP

Server-Assignment-Type是一个Enumerated值，在SAR操作中用于指示服务器更新类型。作为SWx协议定义，增加下面两个枚举值：

a） AAA_USER_DATA_REQUEST (12)

这个枚举是 3GPP AAA 服务器从 HSS 获取非 3GPP 用户的业务数据。

b） PGW_UPDATE (13)

这个枚举是 3GPP AAA 服务器要求存储，更新或者删除 HSS 上的 PDN-GW 标识。

10.3.13 Trace-Info

Trace-Info是一个Grouped类型参数，这个参数包含有关用户和设备跟踪功能和必要的活动，比如激活去激活的信息。参数格式如下：

```
Trace-Info ::= < AVP header: 1505 10415>
               [Trace-Data]
               [Trace-Reference]
              *[AVP]
```

Trace-Info要么只包含Trace-Data，要么只包含Trace-Reference。当需要激活跟踪时，只包含Trace-Data。当需要去激活跟踪时，Trace-Info直接包含Trace-Reference。

10.3.14 Trace-Data

The Trace-Data 是一个Grouped类型。

10.3.15 Feature-List-ID AVP

SWx应用中，Feature-List-ID应该为1。

10.3.16 Feature-List AVP

SWx应用中，这个参数应该为空，标识没有特性。

注：该规范还未有特性标识定义。

10.4 返回代码

10.4.1 DIAMETER_SUCCESS

操作成功。

10.4.2 DIAMETER_ERROR_USER_UNKNOWN

用户不存在。

10.4.3 DIAMETER_ERROR_RAT_NOT_ALLOWED

消息中的IMSI对应的RAT类型不正确。

10.4.4 DIAMETER_ERROR_ROAMING_NOT_ALLOWED

用户不允许在当前的拜访网络中漫游。

10.4.5 DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTON

移动用户没有非3GPP订阅。

10.4.6 DIAMETER_ERROR_IDENTITY_NOT_REGISTERED

用户未注册。

10.4.7 DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

用户已经注册。

表67 终结会话应答

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code / Experimental-Result	必选	指示会话操作结果。 Result-Code 用于 DBP的错误。 Experimental-Result 用于S6b的错误，应在Vendor-Id AVP中包括3GPP Vendor ID，在Experimental-Result-Code AVP包括错误码

表68 S6b 会话终结请求

信息单元名称	映射到Diameter AVP	类别	描述
Termination Cause	Termination-Cause	必选	会话释放原因，应设为DIAMETER_ADMINISTRATIVE，表示这是回应ASR的会话终结

表69 S6b 会话终结应答

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code	必选	指示会话操作结果

10.4.8 业务授权信息更新流程

通过S6b 参考点，3GPP AAA可以修改以前提供给PDN GW的授权信息，也就是说，可以在以下情形下进行修改：在PMIPv6或MIPv4的业务授权时，或者在使用以前的业务授权更新流程提供的信息进行业务授权时，此流程可由修改UE的非3GPP profile时触发,或者由激活或去活HSS中用户和设备的追踪触发。

业务授权信息更新流程分为两步:

a）3GPP AAA 服务器向 PDN GW 发起没有请求的重鉴权和/或重授权请求。PGN GW 受到请求时，会回应此请求并表示对请求进行处理，此流程基于 IETF RFC 3588 的 RAR 和 RAA。

b）PDN GW 收到重授权的请求时，对指示的 APN 进行重授权。

表70 S6b 重授权请求

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	用户标识
Request Type	Re-Auth-Request-Type	必选	表示是否重鉴权或重授权。这里，应该用AUTHORIZE_ONLY

表71 S6b 重授权应答

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code / Experimental-Result	必选	指示会话操作结果。 Result-Code 用于 DBP的错误。 Experimental-Result 用于S6b的错误，应在Vendor-Id AVP中包括3GPP Vendor ID，在Experimental-Result-Code AVP包括错误码

表72 使用 DSMIPv6 时的授权请求

信息单元名称	映射到Diameter AVP	类别	描述
User identity	User-Name	必选	用户标识
Authentication Request Type	Auth-Request-Type	必选	表示是否要求只鉴权，或只授权或两者都要。这里，应该用AUTHORIZE_ONLY
PGW PLMN ID	Visited-Network-Identifier	条件可选	家乡网络通过此IE识别PGW所在网络的PLMN
Access Type	RAT-Type	必选	包括服务UE的非3GPP 接入网络技术
PDN GW Identity	MIP6 -Agent-Info	必选	包括用户连接的PDN GW的FQDN和/或IP address(es)
APN	Service-Selection	可选	包括从IKE_AUTH 消息中提取的APN 信息，应包括用户应连接到的APN，只有从UE收到时才包括。如果没有从UE收到，3GPP AAA服务器将缺省的APN指定给PDN GW
QoS capabilities	QoS-Capability	条件可选	如果请求消息包含此IE，告诉3GPP AAA 服务器PGW能下载此UE的静态QoS profile。PGW 应只在UE附着的时候包括
Supported Features	Supported-Features	可选	如果包括，应包括源主机Diameter会话中支持的功能列表，依据 3GPP TS 29.229

表73 使用授权应答

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code	必选	指示会话操作结果。 Result-Code 用于 DBP的错误，依据RFC 3588. 如果MAG 授权成功或PDN GW地址更新成功，应设为DIAMETER_SUCCESS。 如果新的MAG授权失败，或PDN GW地址更新失败，应设为DIAMETER_AUTHORIZATION_REJECTED
Authorized mobility features	MIP6-Feature-Vector	条件可选	The 3GPP AAA Server shall insert this AVP if the authorization was successful. The MIP4_SUPPORTED flag shall be set
Session Time	Session-Timeout	条件可选	如果成功鉴权和授权，此IE包括授权的时长

表73（续）

信息单元名称	映射到Diameter AVP	类别	描述
QoS resources	QoS-Resources	条件可选	如果成功鉴权和授权，并且PGW在请求消息中包括了QoS-Capabilities AVP并且用户已配置了静态的QoS，3GPP AAA 应在UE附着时包括静态。QoS profile template 应设为0。 此IE 应包括3GPP AAA 基于签约QoS参数授权的QoS Profile
3GPP AAA Server Name	Redirect-Host	条件可选	如果Result-Code为DIAMETER_REDIRECT_INDICATION，应包括此IE。当用户先前由另一个3GPP AAA授权后，此IE应包括当前服务用户的3GPP AAA Server的Diameter标识。 收到此IE的节点应遵循RFC 3588。 命令中应包含零个或一个IE
Supported Features	Supported-Features	可选	如果包括，应包括源主机Diameter会话中支持的功能列表.

10.5 信息单元

10.5.1 S6b PMIPv6 流程的信息单元

信息单元名称如下：

MIP6-Agent-Info

MIP6-Feature-Vector

QoS-Capability

QoS-Resources

Trace-Info

10.5.1.1 MIP6-Agent-Info

依据 IETF RFC 5447。

MIP6-Agent-Info AVP 包含了 PDN GW 标识或 chained S2 – 基于 PMIP 的 S8 时的 SGW 地址信息。PDN GW 标识可以是 MIP-Home-Agent-Address 中的 IP 地址，或是 MIP-Home-Agent-Host 中的 FQDN。如果单个 IP 地址可以用于 PDN GW 所有的接入网络和协议, PDN GW 可能使用这个 IP 地址；其他情况下，PDN GW 应是使用 FQDN。MAG/AAA/HSS 如果有 FQDN 的信息，应该用 FQDN。

MIP6-Agent-Info AVP 的格式如下:

```
MIP6-Agent-Info ::=
                    < AVP Header: 486 >
                    *2[ MIP-Home-Agent-Address ]
                    [ MIP-Home-Agent-Host ]
                    [ MIP6-Home-Link-Prefix ]
                    *[ AVP ]
```

10.5.1.2 MIP6-Feature-Vector

MIP6-Feature-Vector AVP包括一个64位的标志域，表征NAS支持的移动能力。NAS可能在请求消息中包含此AVP，告诉3GPP AAA server它的移动能力。同样，Diameter服务器可能在应答消息包含此AV，通知NAS哪些NAS的移动能力Diameter服务器能够支持或哪些得到3GPP AAA的授权。

PMIPv6 模式下，S6b参考点支持以下能力：

——PMIP6_SUPPORTED

——IP4_HOA_SUPPORTED

10.5.1.3 QoS-Capability

依据IETF RFC 5777。

QoS-Capability AVP 包含了支持的QoS profile 模板的列表。

10.5.1.4 QoS-Resources

依据IETF RFC 5777。

QoS-Resources AVP 包括了控制话务流的QoS资源的描述。

10.5.2 S6b 可以重用的 Diameter AVPs

信息单元名称如下：

Supported-Features

Feature-List-ID

Feature-List

10.5.2.1.1 Feature-List-ID AVP

依据3GPP TS 29.229。这个Release中，S6b application的Feature-List-ID AVP 应设为1。

10.5.2.1.2 Feature-List AVP

依据3GPP TS 29.229。6b应用,此AVP为空。

10.6 返回代码

同7.4节。

附 录 A
（规范性附录）
MME 中 S6a/S6d 和 NAS 原因值映射

MME在接收到附着消息后需要和HSS交互获取用户的签约数据。如果操作不成功，有几种可能的原因值需要映射到应用于UE的NAS原因值，映射关系参见表A.1和表A.2。

表A.1 S6a/S6d 和 NAS 原因值映射

基于S6a/S6d从HSS到MME的拒绝指示	应用于UE的NAS原因值
DIAMETER_ERROR_USER_UNKNOWN (5001)	#8 "EPS业务和非EPS业务不允许"
DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION (5420)	#15 "跟踪区域无合适小区"
DIAMETER_ERROR_RAT_NOT_ALLOWED(5421)	#15 "跟踪区域无合适小区"，或 #13 "跟踪区域漫游不允许"，或 #12 "跟踪区域不允许" （注1）
DIAMETER_ERROR_ROAMING_NOT_ALLOWED(5004)	#11 "PLMN不允许"
DIAMETER_ERROR_AUTHORIZATION_REJECTED(5003)	#15 "跟踪区域无合适小区"
DIAMETER_UNABLE_TO_COMPLY (5012), DIAMETER_INVALID_AVP_VALUE (5004)（注2）	#17 "网络失败"
注1：由运营商决定选择任意一种NAS原因值发送到UE。 注2：其他Diameter基础协议定义的永久性错误，未在此列出，也应映射为#17 "网络失败"的NAS原因值	

表A.2 NAS原因值网络条件映射

应用于UE的NAS原因值	条件
#2 "HSS中IMSI未知"	MME接收到来自VLR的SGsAP-LOCATION-UPDATE-REJECT的消息，其中拒绝原因值指示"HSS中IMSI未知"。仅应用于绑定TAU/LAU流程
#14 "此PLMN中EPS业务不允许"	- MME接收到ULA应答消息，并指示由于不支持的业务导致MME漫游限制，或 - 用户状态属性值对携带的值为OPERATOR_DETERMINED_BARRING
#12 "跟踪区域不允许"	HSS指示由于UE签约了“区域性限制业务”导致UE在跟踪区域操作不允许
#25 "此CSG未授权"	发送TAU请求消息的UE所在小区的CSG标识未在CSG许可列表内

附 录 B
（资料性附录）
SWa 接口

B.1 概述

SWa接口是用于不可信的非3GPP IP接入系统以及3GPP AAA服务器或代理之间的控制平面接口。

SWa接口可选地用于当UE接入演进分组系统（EPS）时的鉴权和授权，是否启用本章定义的接口或过程取决于非3GPP运营商的策略。

从EPS运营商的观点来看，当UE附着在不可信的非3GPP IP接入系统时，需要使用附录C（SWm接口）和第10章（S6b接口）描述的隧道鉴权和授权过程来确保对用户的鉴权和授权。

SWa接口的过程与STa接口上的过程相同，只是参数进行了简化。但其中一个特例是SWa接口上不支持业务授权信息更新过程。

SWa接口和STa接口采用相同的Diameter Application。SWa和STa接口上的第一次鉴权命令交互（DER/DEA）是相同的；在初次交互中，3GPP AAA服务器中定义了HPLMN和非3GPP 接入网的信任关系，并使用第7.2章的过程与非3GPP接入网和UE通信。后续命令的内容根据该信任关系的不同而分别定义在SWa接口或STa接口中。

B.2 消息

B.2.1 SWa 鉴权和授权过程

B.2.1.1 概述

该过程遵循了STa鉴权和授权过程，但有如下差异：

a）描述用户业务需求的参数或描述接入网信息的参数不包括在 authentication and authorization request 消息中，或仅作为可选项。

b）描述用户签约数据的参数不会被下载到非 3GPP 接入网。

B.2.1.2 SWa 鉴权和授权请求（AAR）消息

该消息采用Diameter 协议的 Diameter-EAP-Request (DER)命令实现。

Diameter-EAP-Request (DER) 命令的Command-Code域值为268，其Command Flags域中的'R' bit 置位，并且从可信的非3GPP接入网NAS层发往3GPP AAA服务器。

其命令定义如下：

```
< Diameter-EAP-Request > ::=< Diameter Header: 268, REQ, PXY >
                            < Session-Id >
                            { Auth-Application-Id }
                            { Origin-Host }
                            { Origin-Realm }
                            { Destination-Realm }
                            { Auth-Request-Type }
                            { EAP-Payload }
                            [ User-Name ]
```

[Calling-Station-Id]

[RAT-Type]

...

[ANID]

*[Supported-Features]

...

*[AVP]

表B.1 鉴权和授权请求消息

信息单元名称	映射到Diameter AVP	类别	描述
User Identity	User-Name	必选	该参数包含了用户标识。该标识用NAI表描述，依据IETF RFC 4282。该用户标识的格式定义在3GPP TS 23.003中
EAP payload	EAP-payload	必选	该参数包含了用于UE - 3GPP AAA 服务器互鉴权(mutual authentication)的EAP有效载荷
Authentication Request Type	Auth-Request-Type	必选	定义了该用户是否只需鉴权，或只需授权，或两者都需要。 此处定义为 AUTHORIZE_AUTHENTICATE
UE Layer-2 address	Calling-Station-ID	必选	用于存放UE 的二层地址信息
Access Type	RAT-Type	可选	包含了目前服务于UE的不可信的非3GPP接入网类型
Access Network Identity	ANID	可选	包含了接入网类型的标识，被HSS用于密钥的推导(关于所有可能取值，请依据 3GPP TS 24.302)。 当非3GPP 接入网选择 EAP-AKA' 鉴权方式时，消息中包含该AVP
Supported Features (见 3GPP TS 29.229)	Supported-Features	可选	如果该参数存在，它应包含始发主机在该DIAMETER会话周期内所支持的功能列表

B.2.1.3 SWa 鉴权和授权响应（AAA）消息

该消息采用Diameter 协议的 Diameter-EAP-Answer (DEA)命令实现。

Diameter-EAP-Answer (DEA) 命令的Command-Code域值为268，其Command Flags域中的'R' bit 被清除，并且从3GPP AAA服务器发往可信的非3GPP接入网NAS层。

其命令定义如下：

< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY >

< Session-Id >

{ Auth-Application-Id }

{ Result-Code }

[Experimental-Result]

{ Origin-Host }

{ Origin-Realm }

{ Auth-Request-Type }

{ EAP-Payload }

[User-Name]

[Session-Timeout]

[Accounting-Interim-Interval]

[EAP-Master-Session-Key]

*[Redirect-Host]

[AN-Trusted]

*[Supported-Features]

...

*[AVP]

表B.2 鉴权和授权响应消息

信息单元名称	映射到Diameter AVP	类别	描述
User Identity	User-Name	必选	该参数包含了用户标识。该标识用NAI表描述，依据IETF RFC 4282。该用户标识的格式定义在3GPP TS 23.003中
EAP payload	EAP payload	必选	该参数包含了用于UE - 3GPP AAA 服务器互鉴权(mutual authentication)的EAP有效载荷
Result code	Result-Code / Experimental- Result	必选	该参数包含了操作结果。返回代码定义在DIAMETER基础协议中（IETF RFC 3588）。 Experimental-Result AVP 应被用于传递SWa接口的错误，这是一个AVP组，包含Vendor-Id AVP用于标识3GPP 开发商标识，和Experimental-Result-Code AVP用于标识错误代码
Session Alive Time	Session-Timeout	可选	如果Result-Code AVP被置成DIAMETER_SUCCESS，则该AVP可能存在。如果存在，它应包含该用户会话允许存活的最大秒数
Accounting Interim Interval	Accounting Interim-Interval	可选	该参数包含了计费时长
Pairwise Master Key	EAP-Master-Session-Key	条件可选	当Result-Code AVP 被置成DIAMETER_SUCCESS时，该参数应被传送
3GPP AAA Server Name	Redirect-Host	条件可选	当 Result-CodeAVP 被 置 成 DIAMETER_REDIRECT_INDICATION时，该参数应被传送。当该用户之前曾被其他3GPP AAA服务器鉴权过时，该参数应包含当前为用户服务的3GPP AAA服务器的Diameter标识。收到该参数的网元应按照Diameter基础协议（IETF RFC 3588）定义的方式处理。一条命令只能包含0个或1个该参数
Trust Relationship Indicator	AN-Trusted	必选	该AVP包含了3GPP AAA 服务器的决定，即非3GPP接入网是否可信。对SWa接口来说， 应使用“UNTRUSTED”
Supported Features (见 3GPP TS 29.229)	Supported-Features	可选	如果该参数存在，它应包含始发主机在该DIAMETER会话周期内所支持的功能列表

B.2.1.4 3GPP AAA 服务器在该过程中的行为

3GPP AAA服务器的具体行为遵循在STa鉴权和授权过程中的行为，但有如下差别：

a）3GPP AAA 服务器认为非 3GPP 接入网是不可信的。

b）鉴权方式的选择应根据 Access Network Identity 来决定，如果该参数存在，那么使用 EAP-AKA' 模式；否则使用 EAP-AKA 模式。

B.2.2 SWa HSS/AAA 发起的去附着过程

该过程和STa HSS/AAA发起的去附着过程相同。具体过程和消息依据第8.2.2章。

B.2.3 SWa 非 3GPP 接入网发起的去附着过程

该过程和STa非3GPP 接入网发起的去附着过程相同，具体过程和消息依据第8.2.4章。

B.2.4 SWa 重鉴权和重授权过程

B.2.4.1 概述

该过程是可选的，如果运营商的策略需要在SWa接口上启用对用户的重鉴权并且非3GPP接入网支持重鉴权，那么3GPP AAA服务器可以激活该过程。

该过程分为两步执行：

—— 3GPP AAA 服务器应主动向可信的非 3GPP 接入系统发送一个重鉴权请求，表明需要对用户进行重鉴权和重授权。在收到请求后，可信的非 3GPP 接入系统应响应该请求并应指示对该请求的部署。这个过程通过 Diameter 命令 Re-Auth-Request 和 Re-Auth-Answer 实现，依据 IETF RFC 3588。消息的参数内容应符合下面章节的定义。

—— 在收到重鉴权的请求后，非 3GPP 接入系统应该立即激活 SWa 鉴权和授权过程，通过 EAP 并使用 DER/DEA 命令来请求得到用户标识。DER/DEA 命令采用相同的 session-ID 但命令内容应根据重鉴权的的需求作相应调整。这些消息的参数内容应符合下面的定义。

如果对用户的重鉴权不成功，不可信的非 3GPP 接入系统应该去附着该用户。

B.2.4.2 SWa 重鉴权请求消息

表B.3 SWa重鉴权请求消息

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	该参数包含了用户标识。该标识用NAI表描述，依据IETF RFC 4282。该用户标识的格式定义在3GPP TS 23.003中
Re-Auth Request Type	Re-Auth–Request-Type	必选	该参数定义了是否只需授权，或同时需要鉴权和授权。 此处定义为 AUTHORIZE_AUTHENTICATE
Routing Information	Destination-Host	必选	该参数应从上一条来自于可信的非3GPP接入网的消息的Origin-Host AVP处获得

该消息采用Diameter 协议的 Re-Auth-Request (RAR)命令实现。

Re-Auth-Request (RAR)命令的Command-Code域值为258，其Command Flags域中的‘R’ bit 被置位，并且从3GPP AAA服务器发往不可信的非3GPP接入网NAS层。

RAR命令的ABNF格式定义如下：

```
< Re-Auth-Request >   ::= < Diameter Header: 258, REQ, PXY, 16777250 >
                          < Session-Id >
                          { Origin-Host }
                          { Origin-Realm }
                          { Destination-Realm }
                          { Destination-Host }
                          { Auth-Application-Id }
```

{ Re-Auth-Request-Type }

[User-Name]

...

*[AVP]

B.2.4.3 SWa 重鉴权响应消息

表B.4 SWa重鉴权响应消息

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	该参数包含了用户标识。该标识用NAI表描述，依据IETF RFC 4282。该用户标识的格式定义在3GPP TS 23.003中
Result	Result-Code / Experimental-Result	必选	操作结果。返回代码定义在DIAMETER基础协议中（IETF RFC 3588）。Experimental-Result AVP 应被用于传递SWa接口的错误，这是一个AVP组，包含Vendor-Id AVP用于标识3GPP 开发商标识，以及Experimental-Result-Code AVP用于标识错误代码

该消息采用Diameter 协议的 Re-Auth-Answer (RAA)命令实现。

Re-Auth-Answer (RAA)命令的Command-Code域值为258，其Command Flags域中的'R' bit 被清除，并且从不可信的非3GPP接入网NAS层发往3GPP AAA服务器。

RAA命令的ABNF格式定义如下：

< Re-Auth-Answer > ::= < Diameter Header: 258, PXY, 16777250 >

< Session-Id >

{ Result-Code }

{ Origin-Host }

{ Origin-Realm }

...

*[AVP]

B.2.4.4 SWa 鉴权和授权请求（AAR）消息

该消息采用Diameter协议的 Diameter-EAP-Request (DER)命令实现。命令的ABNF格式定义见B.2.4.2节。

表B.5 SWa鉴权和授权请求消息

信息单元名称	映射到Diameter AVP	类别	描述
User Identity	User-Name	必选	该参数包含了用户标识。该标识用NAI表描述，依据IETF RFC 4282。该用户标识的格式定义在3GPP TS 23.003中
EAP payload	EAP-payload	必选	改参数包含了用于UE - 3GPP AAA 服务器互鉴权(mutual authentication)的EAP有效载荷
Authentication Request Type	Auth-Request-Type	必选	该参数定义了是否只需授权，或同时需要鉴权和授权。此处定义为AUTHORIZE_AUTHENTICATE

B.2.4.5 SWa 鉴权和授权响应消息

表B.6 SWa鉴权和授权响应消息

信息单元名称	映射到Diameter AVP	类别	描述
User Identity	User-Name	必选	该参数包含了用户标识。该标识用NAI表描述，依据IETF RFC 4282。该用户标识的格式定义在3GPP TS 23.003中

表B.6（续）

信息单元名称	映射到Diameter AVP	类别	描述
EAP payload	EAP payload	必选	该参数包含了用于UE - 3GPP AAA 服务器互鉴权(mutual authentication)的EAP有效载荷
Result code	Result-Code / Experimental- Result	必选	该参数包含了操作结果。返回代码定义在DIAMETER基础协议中（IETF RFC 3588）。Experimental-Result AVP 应被用于传递SWa接口的错误，这是一个AVP组，包含Vendor-Id AVP 用于标识3GPP 开发商标识，和Experimental-Result-Code AVP用于标识错误代码
Session Alive Time	Session-Timeout	可选	该参数包含了该用户会话允许存活的最大秒数
Accounting Interim Interval	Accounting Interim-Interval	可选	该参数包含了计费时长
Pairwise Master Key	EAP-Master-Session -Key	条件可选	当Result-Code AVP 被置成DIAMETER_SUCCESS时，该参数应被传送

该消息采用Diameter协议的Diameter-EAP-Answer (DEA)命令实现。命令的ABNF格式定义见B.2.4.3节。

B.2.4.6 3GPP AAA 服务器在该过程中的行为

3GPP AAA 服务器应能根据运营商配置的内部策略来启动该过程。

3GPP AAA 服务器在该过程中应使用和在 UE 附着过程中所使用的完全鉴权相同的鉴权方式。如果使用了 EAP-AKA'模式，3GPP AAA 服务器应使用在 UE 附着时的鉴权和授权过程中收到的 ANID 参数。

B.3 信息单元

SWa的消息信息单元的定义和STa接口上的信息单元定义相同，具体定义依据7.3节。

附 录 C
（资料性附录）
SWm 接口

C.1 概述

SWm接口定义了ePDG和3GPP AAA Server或者Proxy之间的接口会话功能。UE通过ePDG连接到EPC时，应通过SWm接口完成认证授权。同时，SWm接口也用于移动管理协议相关信息单元的传递：

- UE在通过SWn和S2b接口附着到EPC时，SWm接口用于传递PMIPv6相关的移动管理信息单元，即IP移动模式选择信息。
- UE在通过S2c接口附着到EPC时，SWm接口用于传递DSMIPv6相关的移动管理信息单元。特别的，在使用基于IKEv2的完成家乡代理发现时，SWm用于从3GPP AAA服务器向ePDG传递家乡代理的IP地址或者FQDN。

ePDG和3GPP AAA服务器之间的基于Diameter会话的流程包括认证授权流程，重授权流程，ePDG发起的会话终结流程，3GPP AAA服务器发起的会话终结流程和授权信息更新流程。

C.2 消息

C.2.1 认证授权消息

认证授权消息基于IETF RFC 4072定义的Diameter EAP应用的DER/DEA命令。当ePDG收到UE的“隧道建立请求”消息时就会向3GPP AAA服务器发起认证授权流程。整个流程是以转发IKEv2交换信息的形式执行的，该IKEv2交换是为了认证以建立UE和ePDG之间IKE安全关联。

对于每个新的IKE_SA，ePDG都应发起一个新的认证授权流程，即每个IKE_SA应在一个独立的会话流程中进行。认证授权请求消息内容见表C.1。

在收到Diameter-EAP-REQUEST消息后，3GPP AAA服务器检查本地是否存有用户数据信息，如果没有，那么3GPP AAA服务器将会向HSS获取用户信息。如果HSS返回未知用户信息，则3GPP AAA服务器应对ePDG返回相同的错误码。如果HSS指示3GPP AAA服务器用户当前已经在另外一个3GPP AAA服务器，那么3GPP AAA服务器将对ePDG进行重定向操作，具体见表C.2中对应的描述。认证成功后，3GPP AAA服务器会进行授权检查，授权响应消息内容见表C.2。

表C.1 认证和授权请求消息

信息单元名称	映射到Diameter AVP	类别	描述
User Identity	User-Name	必选	UE的用户标识信息，格式须按照IETF RFC 4282定义的NAI格式表示，具体格式定义见3GPP TS 23.003
EAP payload	EAP-Payload	必选	包含封装的UE和3GPP AAA服务器之间相互认证的EAP载荷信息
Authentication Request Type	Auth-Request- Type	必选	指示消息的目的是仅请求认证还是同时请求认证授权。在认证授权流程中，须设置的值为AUTHORIZE_AUTHENTICATE
APN	Service-Selection	条件可选	如果ePDG收到UE发来的IKEv2信令中包含请求授权的接入点名称，那么ePDG应在消息中携带包含请求授权的接入点名称的信息元素
Visited Network Identifier	Visited-Network-Identifier	条件可选	在漫游场景下，即ePDG不属于家乡网络时，ePDG应在消息中携带信息元素以标识被访问的网络，即VPLMN ID

表C.1（续）

信息单元名称	映射到Diameter AVP	类别	描述
Access Type	RAT-Type	条件可选	如果ePDG知道UE接入的非授信非3GPP接入网类型，那么ePDG应在消息中携带本信息元素用以指示接入网类型
Mobility features	MIP6-Feature-Vector	可选	当VPLMN的ePDG和HPLMN的3GPP AAA服务器之间的移动性管理相关的标识是动态处理的，ePDG应在消息中携带本信息元素，设置对应的标识值。 如果使用动态IP移动模式选择功能并且ePDG支持PMIPv6，本信息元素中须按照IETF RFC 5779中的定义设置PMIP6_SUPPORTED标识。 如果ePDG支持基于IKEv2的家乡代理地址发现功能，本信息元素中须设置MIP6_INTEGRATED标识
Supported Features	Supported-Features	可选	可选信息元素。如果ePDG在消息中携带本信息元素，那么应包含源主机在整个Diameter会话生命周期内支持的特性列表

表C.2　认证和授权应答消息

信息单元名称	映射到Diameter AVP	类别	描述
EAP payload	EAP-Payload	必选	包含封装的UE和3GPP AAA服务器之间相互认证的EAP载荷信息
Master-Session-Key	EAP-Master-Session-Key	条件可选	当Result Code设置为DIAMETER_SUCCESS时，消息中应携带本信息元素。元素包含用于保护用户和ePDG之间通信安全的密钥材料
Result code	Result-Code / Experimental-Result-Code	必选	指示请求消息的处理结果。本信息元素错误码的设置应基于Diameter基础协议或者NASREQ
3GPP AAA Server Name 3GPP	Redirect-Host	条件可选	如果Result Code的值设置为DIAMETER_REDIRECT_INDICATION（DIAMETER重定向指示），那么消息中应携带本信息元素。 如果用户在此之前已经被另外的3GPP AAA服务器认证过，本信息元素应包含当前正在服务于用户的3GPP AAA服务器的Diameter标识。 ePDG收到本信息元素后须按照IETF RFC 3588中要求的处理方式执行。消息中可以携带本信息元素的零个或多个实例。 当ePDG接收到本信息元素（列表）后会选择一个服务器标识作为消息目的服务器，此时ePDG应首先向列表中的第一个3GPP AAA服务器发送Diameter请求。如果ePDG没有收到成功的响应消息，ePDG须向列表中的下一个3GPP AAA服务器发送Diameter请求消息。以此类推，直至ePDG收到一个3GPP AAA服务器成功的响应消息
Mobility Capabilities	MIP6-Feature-Vector	可选	如果在请求消息中包含本信息元素，那么在认证授权成功的响应消息中也要对应的包含本信息元素。此时本信息元素应包含授权的移动特性。 如果3GPP AAA服务器决定使用PMIPv6，那么本信息元素须设置为PMIP6_SUPPORTED； 如果3GPP AAA服务器决定应该分配本地IP地址，那么本信息元素须设置为ASSIGN_LOCAL_IP。 如果家乡代理的地址是基于IKEv2家乡代理地址发现实现的，那么本信息元素须设置为MIP6_INTEGRATED。在下面的例子中可以看到，基于IKEv2发现的HA信息是通过APN-Configuration AVP下发提供的
APN-OI replacement	APN-OI-Replacement	条件可选	在非漫游或者家乡转发的漫游场景下，本信息元素用以指示替换APN-OI字段的域名用以对PDN GW的FQDN进行DNS解析。只有当使用PMIPv6并且Result-Code是DIAMETER_SUCCESS时消息中才能携带本信息元素

表C.2（续）

信息单元名称	映射到Diameter AVP	类别	描述
PN and PGW Data	APN-Configuration	条件可选	只有当Result-Code为DIAMETER_SUCCESS时，消息中应携带本信息元素。 APN-Configuration是一组AVP，具体定义见3GPP TS 29.272。当使用PMIPv6时，基于每个APN可能会包含如下信息元素： - APN接入点名称 - User home IP Address用户家乡IP地址 (如果静态IPv4 和/或 IPv6有分配给UE签约APN) - PDN GW identity PDN GW标识 (如果是在切换的已经激活的PDN连接，或者对于UE的签约APN有分配静态PDN GW) - PDN GW allocation type PDN GW分配类型 - VPLMN Dynamic Address Allowed 当3GPP决定用户设备应该进行本地地址分配时，本信息元素只有在使用基于IKEv2家乡代理地址发现时才在消息中携带，并且须符合下面其中一个条件： - 在切换的已经激活的PDN连接； - 对于UE的签约APN有分配静态PDN GW 此时本信息元素中应包含： - HA-APN - PDN GW identity
Session time	Session-Timeout	条件可选	如果授权成功，消息中应携带本信息元素包含本次认证的有效时间
Permanent User Identity	Mobile-Node-Identifier	条件可选	本信息元素在使用PMIPv6时用以为后续MAG(ePDG)发送的PBU消息中携带的MN-ID，即用户在EPS网络中的用户标识
Serving GW Address	MIP6-Agent-Info	可选	本信息元素当且仅当在S2b-S8连接场景下用以指示Serving GW的地址信息，并且此时消息中的Result-Code为DIAMETER_SUCCESS
Supported Features	Supported-Features	可选	可选信息元素。如果ePDG在消息中携带本信息元素，那么应包含源主机在整个Diameter会话生命周期内支持的特性列表

C.2.2 授权消息

当ePDG收到3GPP AAA服务器发起的有效重认证请求消息后（见C.2.5），ePDG会向3GPP AAA服务器发起授权请求消息以更新授权信息信息单元。授权请求消息内容见表C.3。

3GPP AAA服务器在收到授权请求消息后检查用户信息的合法有效性，返回授权应答消息。消息内容见表C.4。

表C.3 授权请求消息

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	UE的用户标识信息，格式须按照IETF RFC 4282定义的NAI格式表示，具体格式定义见3GPP TS 23.003
Diameter Session ID	Session-Id	必选	会话标识，唯一标识本Diameter会话
Request Type	Auth-Request -Type	必选	请求类型，在本消息中应设置为AUTHORIZATION_ONLY (0).

表C.4 授权应答消息

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	UE的用户标识信息，格式须按照IETF RFC 4282定义的NAI格式表示，具体格式定义见3GPP TS 23.003
Diameter Session ID	Session-Id	必选	会话标识，唯一标识本Diameter会话
Registration Result	Result-Code/ Experimental Result Code	必选	指示请求消息的处理结果。本信息元素错误码的设置应基于Diameter基础协议或者NASREQ
UE IPv4 Home Address	PMIP6-IPv4-Home-Address	可选	如果授权成功并且用户拥有一个静态IPv4家乡地址，消息中可能会携带本信息元素包含分配给UE的静态IPv4家乡地址
UE Charging Data	3GPP-Charging-Characteristics	可选	可选信息元素，包含应用于用户的计分方法类型，具体定义见3GPP TS 29.061
Session time	Session-Timeout	条件可选	如果授权成功，消息中应携带本信息元素包含本次认证的有效时间
APN and PGW Data	APN-Configuration	条件可选	只有当Result-Code为DIAMETER_SUCCESS时，消息中应携带本信息元素。 APN-Configuration是一组AVP，具体定义见3GPP TS 29.272。当使用PMIPv6时，基于每个APN可能会包含如下信息元素： - APN接入点名称 - 授权的3GPP QoS数据 - User home IP Address用户家乡IP地址（如果静态IPv4和/或 IPv6有分配给UE签约APN) - PDN GW标识 - PDN GW allocation type PDN GW分配类型 - VPLMN Dynamic Address Allowed 当3GPP决定用户设备应该进行本地地址分配时，本信息元素只有在使用基于IKEv2家乡代理地址发现时才在消息中携带，并且须符合下面其中一个条件： - 在切换的已经激活的PDN连接； - 对于UE的签约APN有分配静态PDN GW 此时本信息元素中应包含： - HA-APN - PDN GW identity

C.2.3 ePDG 发起的会话终结流程消息

当UE和ePDG之间的IKE_SA终结时，ePDG将向3GPP AAA服务器发起会话终结流程，删除相关的非3GPP接入信息。会话终结请求消息内容见表C.5。

在收到会话终结请求消息后，3GPP AAA对用户信息以及会话标识进行合法性检查，返回会话中间应答消息，消息内容见表C.6。

表C.5 会话终结请求消息

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	UE的用户标识信息，格式须按照IETF RFC 4282定义的NAI格式表示，具体格式定义见3GPP TS 23.003
Termination Cause	Termination-Cause	必选	本信息元素指示会话终结的原因值

表C.6 会话终结应答消息

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code	必选	指示会话操作结果

C.2.4 3GPP AAA服务器发起的会话终结流程消息

3GPP AAA服务器可以通过发起会话终结流程终结UE和ePDG之间的IKE_SA。该流程先由3GPP AAA服务器向ePDG发起中止会话请求消息（见表C.7），ePDG在返回中止会话应答消息（见表C.8）后即发起会话终结请求消息（见表C.9），3GPP AAA服务器再返回对应的会话终结应答消息（见表C.10）。

表C.7 中止会话请求消息

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	UE的用户标识信息，格式须按照IETF RFC 4282定义的NAI格式表示，具体格式定义见3GPP TS 23.003
Auth-Session-State	Auth-Session-State	可选	可选信息元素，用以告知ePDG 3GPP AAA服务器是否需要STR消息

表C.8 中止会话应答消息

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code	必选	指示会话操作结果

表C.9 会话终结请求消息

信息单元名称	映射到Diameter AVP	类别	描述
Termination Cause	Termination-Cause	必选	本信息元素指示会话终结的原因值。这里须设置为“DIAMETER_ADMINISTRATIVE”用以指示会话终结是响应的ASR（Abort-Session-Request）中止会话请求消息

表C.10 会话终结应答消息

信息单元名称	映射到Diameter AVP	类别	描述
Result	Result-Code	必选	指示会话操作结果

C.2.5 授权信息更新消息

当HSS上的用户数据信息发生变化时会引起授权信息更新流程。本流程分为两步：

3GPP AAA服务器首先向ePDG发送重认证请求，ePDG收到请求后发送处理结果的响应消息。消息内容分别见表C.11和表C.12。

ePDG在收到授权信息更新请求后立刻发起授权流程完成授权信息的更新，这里消息同C.2.2中的描述。

表C.11 授权信息更新请求消息

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	UE的用户标识信息，格式须按照IETF RFC 4282定义的NAI格式表示，具体格式定义见3GPP TS 23.003

表C.11（续）

信息单元名称	映射到Diameter AVP	类别	描述
Re-Auth Request Type	Re-Auth-Request-Type	必选	定义用户认证授权行为是仅认证，仅授权还是同时认证授权。这里须设置为仅授权“AUTHORIZE_ONLY”
Routing Information	Destination-Host	必选	包含在先前收到的ePDG发送的消息中指示的3GPP AAA服务器的标识信息

表C.12 授权信息更新应答消息

信息单元名称	映射到Diameter AVP	类别	描述
Permanent User Identity	User-Name	必选	UE的用户标识信息，格式须按照IETF RFC 4282定义的NAI格式表示，具体格式定义见3GPP TS 23.003
Result	Result-Code	必选	指示会话操作结果

C.3 信息单元

C.3.1 概述

表C.13描述了SWm接口协议用于非信任的非3GPP接入所定义的Diameter AVP、AVP代码值、可能的Flag值以及该AVP是否可能加密。

表C.13 SWm接口的DIAMETER AVP

				AVP Flag 规则				
名称	AVP码	定义所在章节	值类型	Must	May	Should not	Must not	可能加密
APN-Configuration	1430	9	Grouped	M			V	No
Mobile-Node-Identifier	506	7.	OctetString	M			V	
MIP6-Feature-Vector	124	7.	Unsigned64	M			V	
QoS-Capability	578	12	Grouped	M			V	No
RAT-Type	1032	7.	Enumerated	M,V	P			Y
Visited-Network-Identifier	600	10	UTF8String	M,V				No

表C.14中是SWm接口复用的现有Diameter应用中的Diameter AVP，包括对应AVP的参考规范。现有Diameter应用中的其他AVP，除了Diameter基本协议中的AVP之外，都无须支持。

表C.14 SWm接口复用的现有DIAMETER AVP

名称	参考	备注
Auth-Request-Type	IETF RFC 3588	
Called-Station-Id	IETF RFC 4005	
EAP-Master-Session-Key	IETF RFC 4072	
EAP-Payload	IETF RFC 4072	
Re-Auth-Request-Type	IETF RFC 3588	
Session-Timeout	IETF RFC 3588	
User-Name	IETF RFC 3588	
MIP6-Agent-Info	IETF RFC 5447	
APN-OI-Replacement	3GPP TS 29.272	
Supported-Features	3GPP TS 29.229	
Feature-List-ID	3GPP TS 29.229	见C.3.2
Feature-List	3GPP TS 29.229	见C.3.3

C.3.2 Feature-List-ID

该AVP的语法定义见3GPP TS 29.229。对于SWm应用，Feature-List-ID AVP的值应设为1。

C.3.3 Feature-List

该AVP的语法定义见3GPP TS 29.229。SWm应用不使用相关的feature，取值为空。

C.3.4 User-Name

该AVP类型为UTF8String，定义见IETF RFC 3588。

C.3.5 EAP-payload

该AVP类型为OctetString，用于封装归属Diameter服务器与EAP客户之间交换的EAP包。其定义见IETF RFC 4072。

C.3.6 Auth-Request-Type

该AVP类型为Enumerated，用于指示该用户是要仅鉴权、仅认证、或者同时需要鉴权和认证。其定义见IETF RFC 3588。

C.3.7 Visited-Network-Identifier

该AVP类型为UTF8String，定义见第10章。

C.3.8 Service-Selection

该AVP类型为UTF8String，定义见第7章。

C.3.9 RAT-Type

该AVP类型为Enumerated，定义见第7章。

C.3.10 MIP6-Feature-Vector

该AVP类型为Unsigned64，定义见第7章。

C.3.11 Supported-Features

该AVP的语法定义见3GPP TS 29.229。

C.3.12 EAP-Master-Session-Key

该AVP类型为OctetString，定义见IETF RFC 4072。

C.3.13 Result-Code

见10.4。

C.3.14 Experimental-Result-Code

见10.4。

C.3.15 Redirect-Host

见IETF RFC 3588。

C.3.16 APN-OI-Replacement

见3GPP TS 29.272。

C.3.17 APN-Configuration

该AVP类型为Grouped，定义见第9章。

C.3.18 Session-Timeout

该AVP类型为Unsigned32，指示在会话终止前向用户提供服务的最长秒数。其定义见IETF RFC 3588。

C.3.19 Mobile-Node-Identifier

该AVP类型为OctetString，定义见第7章。

C.3.20 MIP6-Agent-Info

见IETF RFC 5447。

C.3.21 Session-Id

该AVP类型为UTF8String，用于标识会话。该AVP的定义见IETF RFC 3588。

C.3.22 3GPP-Charging-Characteristics

见3GPP TS 29.061。

C.3.23 Termination-Cause

该AVP类型为Enumerated，用于指示会话终止的原因。其定义见IETF RFC 3588。

C.3.24 Auth-Session-State

该AVP类型为Enumerated，用于指示是否为指定的会话维持状态。其定义见IETF RFC 3588。

C.3.25 Re-Auth-Request-Type

该AVP类型为Enumerated，其定义见IETF RFC 3588。

C.3.26 Destination-Host

该AVP类型为DiameterIdentity，定义见IETF RFC 3588。

C.3.27 QoS-Capability

该AVP类型为Grouped，定义见第10章。

中华人民共和国
通信行业标准
演进的移动分组核心网络（EPC）接口技术要求
S6a/S6d/S13/S13'/STa/SWd/SWx/SWa/SWm/S6b
YD/T 2624-2013
*
人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100064
宝隆元（北京）印刷技术有限公司印刷

*
开本：880×1230　1/16　　2014年1月第1版
印张：6.25　　2014年1月北京第1次印刷
字数：169千字
15115·458
定价：70元
本书如有印装质量问题，请与本社联系　电话：(010)81055492