



中华人民共和国通信行业标准

YD/T 1972.1-2009

800MHz/2GHz cdma2000 数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求 第 1 部分：会话控制类设备

Technical requirements for 800MHz/2GHz cdma2000 digital cellular
mobile telecommunication network multimedia domain equipment
Part 1: Call control equipments

2009-12-11 发布

2010-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 缩略语.....2

4 概述.....3

 4.1 网络架构.....3

 4.2 定义.....3

5 功能要求.....5

 5.1 P-CSCF 的功能.....5

 5.2 I-CSCF 的功能.....14

 5.3 S-CSCF 的功能.....17

6 性能及可靠性指标.....31

 6.1 会话处理能力.....31

 6.2 注册用户数.....31

 6.3 系统可靠性和可用性.....31

7 接口要求.....31

 7.1 物理接口.....31

 7.2 逻辑接口.....32

8 操作维护及网管要求.....32

 8.1 MML 和 GUI.....32

 8.2 本地维护和远程维护.....32

 8.3 日志.....32

 8.4 性能统计.....32

 8.5 故障诊断.....32

 8.6 加载.....33

 8.7 软件版本及补丁管理.....33

9 定时与同步要求.....33

10 电源及接地要求.....33

 10.1 电源要求.....33

 10.2 接地要求.....34

11 环境要求.....34

参考文献.....35

前 言

《800MHz/2GHz cdma2000 数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求》是根据我国CDMA网络的发展需要，参考3GPP2的系列规范，并根据我国国内的实际情况制定而成的。

YD/T 1972《800MHz/2GHz cdma2000 数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求》分为4部分。

- 第1部分：会话控制类设备；
- 第2部分：用户数据类设备；
- 第3部分：互通类设备；
- 第4部分：媒体资源类设备。

本部分是YD/T 1972的第1部分。

《800MHz/2GHz cdma2000 数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求》是“800MHz/2GHz cdma2000 数字蜂窝移动通信网多媒体域（MMD）系统”系列标准之一，该系列标准的结构及名称如下：

a) YD/T 1972《800MHz/2GHz cdma2000 数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求》

- 第1部分：会话控制类设备；
- 第2部分：用户数据类设备；
- 第3部分：互通类设备；
- 第4部分：媒体资源类设备。

b) YD/T 1973《800MHz/2GHz cdma2000 数字蜂窝移动通信网 多媒体域（MMD）系统设备测试方法》

- 第1部分：会话控制类设备；
- 第2部分：用户数据类设备；
- 第3部分：互通类设备；
- 第4部分：媒体资源类设备。

本部分与 YD/T 1973.1《800MHz/2GHz cdma2000 数字蜂窝移动通信网 多媒体域（MMD）系统设备测试方法 第1部分：会话控制类设备》配套使用。

本部分由中国通信标准化协会提出并归口。

本部分起草单位：工业和信息化部电信研究院、中国联合网络通信股份有限公司、中讯邮电咨询设计院。

本部分主要起草人：李侠宇、顾旻霞、王君珂、杨艳松。

800MHz/2GHz cdma2000 数字蜂窝移动通信网

多媒体域（MMD）系统设备技术要求

第 1 部分：会话控制类设备

1 范围

本部分规定了 800MHz/2GHz cdma2000 数字蜂窝移动通信网多媒体域的会话控制类设备 P-CSCF、I-CSCF、S-CSCF 的功能要求、安全要求、操作维护及网管，性能及可靠性指标等内容。

本部分适用于 800MHz/2GHz cdma2000 数字蜂窝移动通信网中 MMD 系统的会话控制类设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 2887-2000 电子计算机场地通用规范

GB 9254-1998 信息技术设备的无线电骚扰限值和测量方法

GB/T 17618-1998 信息技术设备抗扰度限值和测量方法

GB 50174-2000 电子计算机机房设计规范

3GPP2 X.S0013-003-A V1.0, 全 IP 核心网多媒体域：IP 多媒体会话处理；IP 多媒体呼叫模型；阶段 2

3GPP2 X.S0013-005-A V1.0, 全 IP 核心网多媒体域：IP 多媒体子系统 Cx 接口信令流程和消息内容

3GPP2 X.S0013-008-A V1.0, 全 IP 核心网多媒体域：IP 多媒体子系统——计费信息流程和协议

3GPP2 S.R0086-B V1.0, IMS 安全框架

IETF RFC 1305: 网络时间协议（版本 3）规范和执行

IETF RFC 2403: 在 ESP 和 AH 内的 HMAC-MD5-96 的使用

IETF RFC 2404: 在 ESP 和 AH 内的 HMAC-SHA-1-96 的使用

IETF RFC 2406: IP 压缩安全有效载荷

IETF RFC 3261 进程初始化协议

IETF RFC 3310: 使用证明与密钥协议的 HTTP 摘要证明

IETF RFC 3320: 信号压缩（SigComp）

IETF RFC 3321: 信号压缩（SigComp）——扩展操作

IETF RFC 3323: 对于进程初始化协议（SIP）的一个私密机制

IETF RFC 3325: 对于进程初始化协议（SIP）在可信任网络用于尚待证实的识别私自扩展

IETF RFC 3326: 对于进程初始化协议的（SIP）原因报头域

IETF RFC 3329: 对于进程初始化协议（SIP）安全机制协定

IETF RFC 3485: 信号压缩（SigComp）的会话初始协议（SIP）和会话描述协议（SDP）静态字母检

索表

IETF RFC 3486: 压缩会话初始协议（SIP）

- IETF RFC 3680: 会话初始协议 (SIP) 注册的事件包
- IETF RFC 3761: E.164 到统一资源标识符 (URI) 动态授权发现系统 (DDDS) 应用 (ENUM)
- IETF RFC 3841: 会话初始协议 (SIP) 的呼叫者优先选择
- IETF RFC 3861: 即时消息和出席的地址解析
- IETF RFC 3966: 电话号码的 tel URI
- IETF RFC 4028: 会话发起协议 (SIP) 中的会话定时器
- IEEE 802.3 信息技术、系统间的远程通信和信息交换, 局域网和城域网规范要求
- IEEE 802.3u 信息技术、电信和系统间的信息交换, 局域网和城域网特殊要求: 100Mbit/s 以太网
- IEEE 802.3ab 信息技术、电信和系统间的信息交换, 局域网和城域网特殊要求, CSMA/CD 及物理层规范的补充: 物理层参数和 1000Mbit/s 操作规范

3 缩略语

下列缩略语适用于本部分。

ACR	Accounting Request	计费请求
AS	Application Server	应用服务器
AAA	Authentication, Authorization and Accounting	鉴权、授权、计费
BGCF	Breakout Gateway Control Function	出口网关控制功能
CRF	Charging Rules Function	计费规则功能
CS	Circuit Switched	电路交换
CSCF	Call Session Control Function	呼叫会话控制功能
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name System	域名系统
ENUM	E.164 Number	E.164 号码
ECUR	Event Charging with Unit Reservation	计费单元预留的事件计费
HSS	Home Subscriber Server	归属用户服务器
ICID	IMS Charging ID	IMS 计费标识
I-CSCF	Interrogating-CSCF	查询 CSCF
IEC	Immediate Event Charging	即时事件计费
IMCN	IP Multimedia	IP 多媒体
IMS	IP Multimedia Network Subsystem	IP 多媒体网络子系统
IOI	Inter Operator Identifier	归属网络标识
ISC	IMS Service Control	IMS 业务控制接口
IP	Internet Protocol	互联网协议
MGCF	Media Gateway Control Function	媒体网关控制功能
MRFC	Multimedia Resource Function Controller	多媒体资源功能控制器
MRFP	Multimedia Resource Function Processing	多媒体资源功能处理器
OCS	Online Charging System	在线计费系统
OSA	Open Services Architecture	开放业务体系

P-CSCF	Proxy-CSCF	代理 CSCF
PCRF	Policy Decision Function	策略决策功能
PDSN	Packet Data Serving Node	分组数据服务节点
PSI	Public Service Identity	公共业务标识
PUI	Public User Identity	公共用户标识
PVI	Private User Identity	私有用户标识
QoS	Quality of Service	业务服务质量
SDP	Session Description Protocol	会话描述协议
SCUR	Session Charging with Unit Reservation	计费单元预留的会话计费
SIP	Session Initiated Protocol	会话初始协议
S-CSCF	Serving-CSCF	服务 CSCF
SBBC	Service Based Bearer Control	基于业务的承载控制
THIG	Topology Hiding Inter-network Gateway	拓扑隐藏网间网关
UE	User Equipment	用户设备
URI	Uniform Resource Identifier	统一资源标识

4 概述

4.1 网络架构

MMD 系统包括两个部分，分组数据子系统（PDS）和 IP 多媒体子系统（IMS），其中 IMS 提供多媒体会话能力，PDS 为 IMS 提供承载层的支撑，IMS 的多媒体会话能力建立在分组数据支撑能力的基础上。在实际的应用中，PDS 可以在没有 IMS 的情况下独立部署。图 1 所示为 MMD 系统的网络参考模型。

4.2 定义

会话控制设备功能定义如下。

呼叫会话控制功能CSCF分为代理CSCF（P-CSCF）、服务CSCF（S-CSCF）和查询CSCF（I-CSCF）。P-CSCF 在 IMS 中是 UE 的第一个接触点，可以位于用户的归属网络或者拜访网络中。P-CSCF 将 UE 接入 IMS 网络并负责在 UE 与 IMS 归属域间进行消息路由。P-CSCF 维护与 UE 之间的 SA，提供 SIP 消息的完整性保护和压缩。P-CSCF 还负责媒体检查，并能够与 QoS 策略功能实体交互进行承载 QoS 控制。

在某运营商的网络中，I-CSCF 是针对该网络中某用户或目前处于该网络中的某漫游用户的所有 IMS 连接的接触点。I-CSCF 在 UE 注册阶段为其分配 S-CSCF。I-CSCF 能够处理终呼，将会话请求正确路由到被叫的 S-CSCF。根据运营商的需求，I-CSCF 还能提供 THIG 的功能。

在网络中，S-CSCF位于用户归属网络，为UE提供注册，会话控制和业务触发等功能。这些功能包括：用户注册和重注册、注销、认证鉴权、第三方注册、会话管理、消息路由、漫游判断、业务触发、媒体授权。

会话控制设备相关的接口定义如下。

ISC接口：ISC接口位于S-CSCF与AS之间，是IMS核心网络CSCF提供给IMS应用网络的接口，基于SIP，ISC接口向业务引擎/OSA业务能力服务器提供SIP/SDP呼叫控制、SIP事件相关的订购与通知等功能。

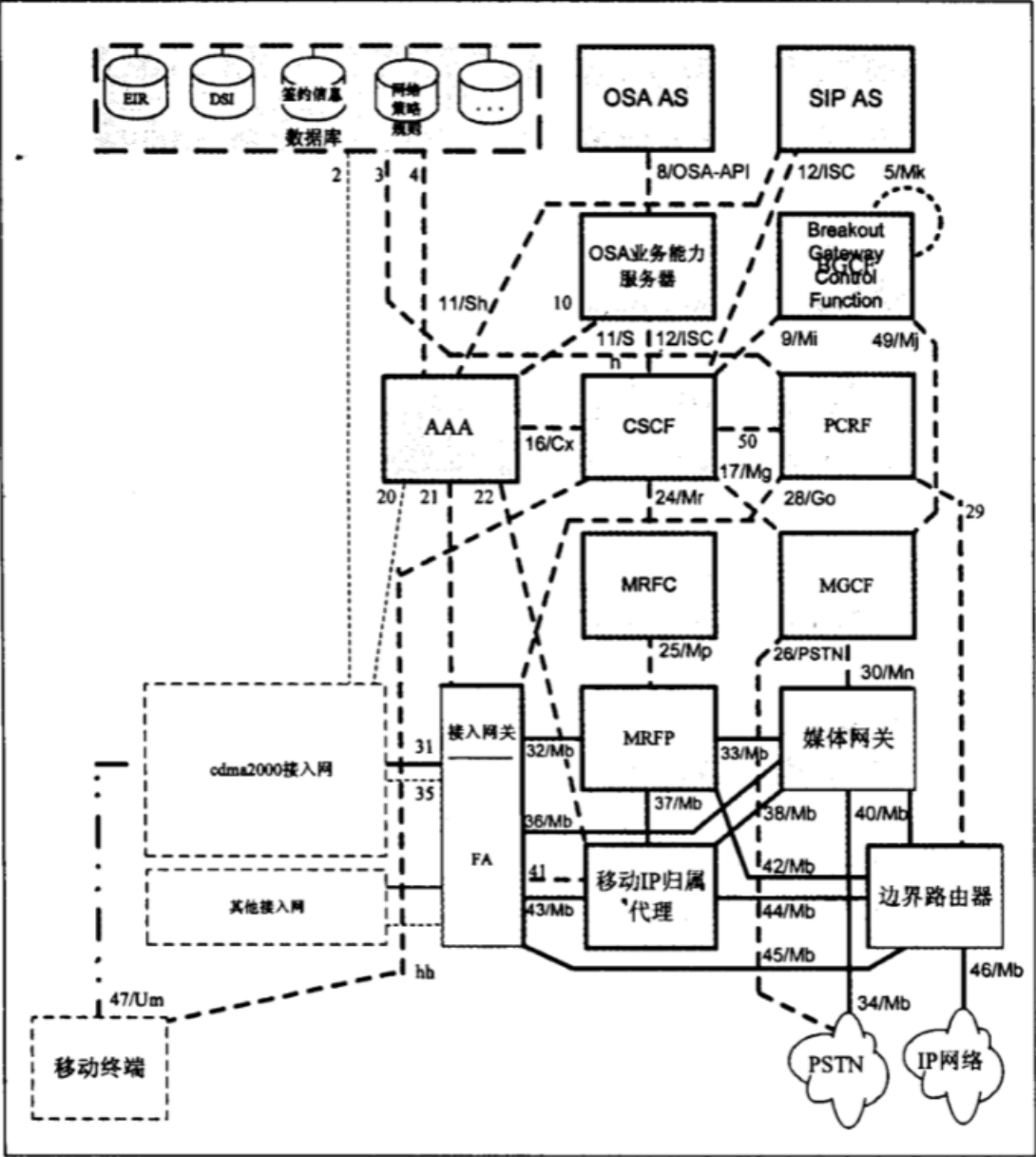


图 1 MMD 系统的网络参考模型

Gm接口：Gm接口位于IMS用户终端与IMS核心网P-CSCF之间，基于SIP，主要用于IMS用户的注册及会话控制。

Tx接口：Tx接口位于P-CSCF和PCRF之间，基于DIAMETER协议，完成会话的QoS策略控制功能。

Rf接口：Rf接口位于CSCF与离线计费实体之间，基于DIAMETER协议，实现会话相关离线计费功能。

Mw接口：Mw接口位于不同的CSCF之间，基于SIP，用于IMS登记及会话流程中CSCF之间的消息通信及代理前转。

Mg接口：Mg接口位于CSCF与MGCF之间，基于SIP，CSCF通过该接口间接控制与其他非IMS网络，包括PSTN、其他基于IP承载的移动3G网络、固定NGN网络等。

Cx 接口：Cx 接口用于 CSCF 与 HSS 之间的信息交互与传输，基于 DIAMETER 协议。

Mr接口：Mr接口位于S-CSCF与MRFC之间，基于SIP，CSCF通过该接口间接控制MRFP上的网络媒体资源（包括音频、视频多媒体等）。

Mi 接口：Mi 接口位于 S-CSCF 与 BGCF 之间，基于 SIP，S-CSCF 通过该接口将会话控制信令前转到 BGCF，由 BGCF 完成到传统窄带 PSTN、3G/2G CS 网络互通所需要的 MGCF 的选择。

5 功能要求

5.1 P-CSCF 的功能

5.1.1 注册和注销功能

5.1.1.1 注册

P-CSCF可以使用IETF RFC 3261中定义的SIP默认端口, 或者使用UE在P-CSCF发现过程中获得的端口来接收初始注册请求。

当P-CSCF接收到来自UE的注册请求时, 应进行以下操作。

a) 插入 Path 消息头, 包含标识 P-CSCF 的 SIP URI, MT 请求指示, 以便 S-CSCF 可以把到终端的请求转发到该 P-CSCF。

b) 插入 Require 消息头, 包含 path 标签。

c) 插入 P-Charging-Vector 消息头, 包含根据 3GPP2 X.S0013-008 产生的 icid 值。

d) 在 Authorization 消息头插入 integrity-protected 参数: 当该注册请求通过正在进行的认证过程产生的安全关联进行完整性保护(例如携带 RES 参数), 或者通过上一次成功认证所建立的安全关联(例如携带 RES 参数)接收时, integrity-protected 参数设为“yes”, 其他情况该参数设为“no”。

e) 如果接收到的注册请求没有进行完整性保护, 检查是否存在 Security-Client 消息头: 如果存在, 移除并保存该消息头; 如果不存在, P-CSCF 返回 4xx 响应。

f) 如果接收到的注册请求进行了完整性保护, P-CSCF 应注意以下 3 项内容。

1) 检查保护该请求的安全关联, 如果是一个临时的安全关联, 检查请求中是否包含 Security-Verify 和 Security-Client 消息头: 如果不存在这两个消息头, P-CSCF 将返回 4xx 响应; 如果存在这两个消息头, P-CSCF 将对比该 Security-Verify 消息头和早前发出(例如在 401 消息中)的 Security-Server 消息头以及 Security-Client 消息头和在初始注册请求中收到的 Security-Client 消息头, 如果这几者不匹配, 则可能存在人为的中间攻击, P-CSCF 应返回 4xx 响应来拒绝该请求。如果匹配, P-CSCF 将移除 Security-Verify 和 Security-Client 消息头。

2) 如果该安全关联是一个已经建立的安全关联, P-CSCF 应进行以下 3 项工作:

— 如果存在 Security-Verify, 则移除该消息头;

— Security-Client 消息头应包含新的参数, 如果没有该消息头或者没有携带需要的参数, P-CSCF 应返回 4xx 响应;

— P-CSCF 应移除并保存 Security-Client 消息头;

3) 检查 Authorization 消息头中的 PVI 和早前在初始注册请求中收到的 PVI, 如果不一致, P-CSCF 应返回 403 响应拒绝该请求。

g) 插入 P-Visited-Network-ID 消息头。

h) 将请求转发给归属网络的 I-CSCF: 如果为收到响应, 或是受到 3xx 或 480 响应, P-CSCF 应选择新的 I-CSCF 转发该注册请求; 如果到所有可能的 I-CSCF 的请求均未成功, P-CSCF 应根据 IETF RFC 3261 的规定返回 408 (请求超时) 或 504 (服务器超时); 如果收到其他响应, 在执行可能的相应操作后(如加入/删除相应消息头和/或参数), 转发至 IMS 终端。

当P-CSCF收到注册请求的401响应后, 应进行以下操作。

a) 删除与 IMS 终端之间存在的任何临时安全关联。

b) 移除 401 (Unauthorized) 响应中的 CK 和 IK 参数, 并将 CK 和 IK 参数与 PVI 以及即将建立的临时安全关联进行绑定, 将移除 CK 和 IK 参数后的 401 (Unauthorized) 响应转发给 UE。

c) 插入 Security-Server 消息头, 包括 P-CSCF 静态安全列表和 3GPP2 S.R0086 中定义的安全关联参数。P-CSCF 应支持 IETF RFC 3329 定义的“ipsec-3gpp”安全机制。P-CSCF 应支持 IETF RFC 2403 定义的 HMAC-MD5-96 和 IETF RFC 2404 定义的 HMAC-SHA-1-96 的 IPsec 层算法。

d) 在 UE 和 P-CSCF 之间建立一组 SIP 层生命周期的临时安全关联, 该生命周期应能保证认证过程的完成, 详细定义见 3GPP2 S.R0086 和 IETF RFC 3329。

e) 如果注册请求被保护, 通过相应的安全关联发送 401 响应到 IMS 终端; 如果注册请求未被保护, 则不对 401 响应进行保护。

当 P-CSCF 收到注册请求的 200 (OK) 响应后, P-CSCF 应检查 Expires 消息头和/或 Contact 消息头中的 Expires 参数, 如果值不为 0, P-CSCF 应进行以下操作:

a) 保存 Service-Route 消息头的列表, 如果是重注册则更新原先储存的列表。

b) 将 Service-Route 列表与注册的 PUI 相关联。

c) 保存在 P-Associated-URI 消息头中携带的 PUI, 并将第一个 PUI 为缺省 PUI。

d) 保存 P-Charging-Function-Address 消息头的值。

e) 如果存在一组已经建立好的安全关联, 将其生命周期设置为二者的最大值: 现有安全关联的生命周期, 刚结束的注册生命周期加上 30s。

f) 如果存在一组临时安全关联, 将其改为新的安全关联, 其生命周期设置为二者的最大值: 原有安全关联的生命周期, 刚结束的注册生命周期加上 30s。

g) 通过与注册请求相同的安全关联将 200 (OK) 响应转发给 IMS 终端。

当 P-CSCF 通过新的安全关联收到 UE 发出的 SIP 消息 (包括注册请求), P-CSCF 应缩短旧的安全关联的生命周期为 $64 \times T1$ (如果长于 $64 \times T1$); 使用新的安全关联向 UE 发送后续的消息。

在这种情况下, P-CSCF 将通过新的安全关联向 UE 发送请求。对于发往 UE 的响应, 如果通过 UDP 发送, 则使用新的安全关联; 如果通过 TCP 发送, 则使用和请求一致的安全关联。

当旧的安全关联将要超时, 例如其生命周期小于 $64 \times T1$, 并且新的安全关联尚未启用时, P-CSCF 将使用新的安全关联向 UE 发送后续消息。

当向 UE 发送的 200 (OK) 响应是一个重鉴权响应时, P-CSCF 应保持发送 re-authentication 的注册请求的安全关联; 保持重鉴权建立的新的安全关联; 删除其他所有存在的安全关联; 继续使用发送 re-authentication 注册请求时使用的安全关联向用户发送后续请求。

当向 UE 发送的 200 (OK) 响应是一个初始鉴权响应时, 例如接收的初始注册请求未进行保护, P-CSCF 应: 保持新建的安全关联; 删除其他所有存在的安全关联; 使用新建的安全关联向用户发送后续消息; 当生命周期过期时, P-CSCF 应删除该安全关联。

5.1.1.2 用户注册状态事件订阅功能

当收到对用户初始注册请求的 200 (OK) 响应后, P-CSCF 应向 S-CSCF 发起用户注册状态事件订阅来了解用户的注册状态信息 (订阅流程见 IETF RFC 3680), P-CSCF 应进行以下二项操作:

a) 产生 SUBSCRIBE 请求, 包含以下内容:

— Request-URI: P-CSCF 希望订阅的用户标识;

- From: 标识P-CSCF的SIP URI;
- To: 订阅用户的缺省SIP URI;
- Event: 设为reg;
- Expires: 订阅超时时间, 设置为大于200 (OK) 返回的注册超时时间;
- P-Asserted-Identity: 标识P-CSCF的SIP URI;
- P-Charging-Vector: 包含根据3GPP2 X.S0013-008产生的icid值。

b) 将订阅请求转发给I-CSCF

当收到订阅请求的200 (OK) 的响应后, P-CSCF应当存储相应的对话信息和在200 (OK) 中指明的订阅超时时间。

如果需要连续的订阅, P-CSCF应能在适当地时间自动更新注册事件订阅。

当收到注册事件NOTIFY请求后, P-CSCF将根据NOTIFY请求中的某一公用标识的属性进行相应处理, 如果是注册, 则设置该公用标识为已注册, 绑定相应的联系地址; 如果是注销, 则设置该公用标识从相应的终端或是所有的终端上注销, 并释放相关的信息。

如果与某一终端相关联的所有公用标识全部注销, P-CSCF将从S-CSCF收到NOTIFY请求并指示订阅终止; 如果NOTIFY请求未指明订阅终止, P-CSCF应取消该订阅或让该订阅过期, 即不发送更新订阅请求。

5.1.1.3 注销

P-CSCF应能支持来自终端或是网络的注销请求。

P-CSCF应能接收来自终端的注销请求, 并转发至P-CSCF所在网络的边界点 (如果P-CSCF所在网络是拜访地网络, 且采用网络拓扑隐藏), 或是转发至用户归属网络的入口点。

当P-CSCF接收到注册请求的200 (OK) 响应时, P-CSCF将检查其中的Expires消息头和/或Contact消息头中expires参数中的值, 如果该值为0, P-CSCF应从已注册PUI列表中删除To消息头中指定的PUI以及与其相关联的PUI, 并释放所有相关的信息; 并检查该终端是否还有其他已注册的PUI, 如果在该终端上所有的PUI均已注销, 则在SIP注销操作的事务处理结束后, 删除与该终端相关的安全关联。

当收到来自网络的NOTIFY请求指明用户注销, 则P-CSCF应将相应公用标识从所有终端或指定终端标记为注销, 并释放存储的相应信息; 如果该IMS终端上的所有公用标识均已注销, 则缩短到该用户安全关联的生命周期。

5.1.2 用户数据及业务数据管理

P-CSCF 保存基于会话的部分用户数据。P-CSCF 作为 UE 到 IMS 网络的第一个接触实体, 在 UE 注册完成后, P-CSCF 会存储与该会话相关的 UE 信息 (包括 UE 的地址, UE 的 PUI/PVI) 以及路由信息 (与归属网络相联的 I-CSCF 地址和 S-CSCF 地址)。

5.1.3 注册无关请求基本处理功能

当P-CSCF收到一个注册无关请求时, P-CSCF将首先检查该请求是UE发起的请求或UE终结的请求:

- 如果在Route消息头中包含MT指示 (如5.1.1节所示), 则为UE终结的请求;
- 如果没有该指示, 则为UE发起的请求。

5.1.3.1 UE 发起的请求

当 P-CSCF 接收到初始对话请求或者独立事务请求, P-CSCF 应检查请求消息中 P-Preferred-Identity,

如果该信息与 UE 注册的某个 PUI 相符时, P-CSCF 判断该请求是由此 PUI 发起的。如果不符, 或者没有包含 P-Preferred-Identity, 则应判断该请求是由默认的 PUI 发起的。如果有多个默认的 PUI, P-CSCF 可以随机的任选一个。

当 P-CSCF 收到 UE 发起的初始对话请求, P-CSCF 应进行以下操作。

- a) 校验 Service-Route 头域的 URI 列表是否与收到请求中的预加载的 Route 头部相匹配, 如果不匹配: P-CSCF 将不转发该请求, 并返回 400(Bad Request)响应, 该响应中可以包含带有 warn-code 399 的 Warning 头; 或者 P-CSCF 用注册或重注册时保存 Service-Route 头域来替换请求中预加载的 Route 消息头;
- b) 插入标识自身地址的 Via 消息头;
- c) 在 Record-Route 头域的最顶端增加 P-CSCF 的 SIP URI;
- d) 如果有 P-Preferred-Identity, 删除并插入 P-Asserted-Identity, 其中的值应标识为请求的发起者;
- e) 插入 P-Charging-Vector 消息头, 包含根据 3GPP2 X.S0013-008 产生的 icid 值;
- f) 如果该请求是 INVITE 请求, 保存请求中的 Contact、Cseq 和 Record-Route 等消息头的值, 以使 P-CSCF 必要时能释放会话。

当 P-CSCF 收到上述请求的 1xx 或 2xx 响应时, P-CSCF 应进行以下操作。

- a) 保存响应中 P-Charging-Function-Addresses 消息头的值;
- b) 保存 Record-Route 消息头中的列表;
- c) 保存 dialog ID, 并与会话中涉及的 PVI 和 PUI 相关联;
- d) 使用与 UE 协商的服务器端口号刷新 Record-Route 中自身的端口号, 同时根据协商的情况插入 SIP 压缩相关的参数 (详细定义见 IETF RFC 3486)
- e) 如果是 INVITE 请求的响应, 保存 Contact、From、To、Record-Route 消息头的值, 以使 P-CSCF 必要时能释放会话。

当 P-CSCF 收到 UE 发起的目标刷新请求时, P-CSCF 应进行以下操作。

- a) 检验该请求是否关联一个现存的对话, 如果没有与请求关联的对话, P-CSCF 将不转发该请求, 同时 P-CSCF 将返回 403 (Forbidden) 响应, 该响应中可以包含带有 warn-code 399 的 Warning 头; 如果存在与请求关联的对话, P-CSCF 将继续以下操作。
- b) 校验请求中的 Route 消息头和保存的关联对话的 Record-Route 消息头, 如果不一致, P-CSCF 将不转发该请求, 并返回 400 (Bad Request) 响应, 该响应中可以包含带有 warn-code 399 的 Warning 头; 或者 P-CSCF 用保存的关联对话的 Record-Route 消息头来替换请求中的 Route 消息头。
- c) 插入标识自身地址的 Via 消息头。
- d) 在 Record-Route 头域的最顶端增加 P-CSCF 的 SIP URI。
- e) 如果是 INVITE 对话, 刷新已保存的 Contact 和 Cseq, 只有收到 1xx 或 2xx 响应后刷新的 Contact 值才有效, 否则依然使用旧的值。

当 P-CSCF 收到上述目标刷新请求的 1xx 或 2xx 响应时, P-CSCF 应使用与 UE 协商的服务器端口号刷新 Record-Route 中自身的端口号, 同时根据协商的情况插入 SIP 压缩相关的参数 (详细定义见 IETF RFC 3486); 刷新保存的 Contact 消息头的值, 以使 P-CSCF 必要时能释放会话。

当 P-CSCF 收到 UE 发起独立事务请求, P-CSCF 应进行以下操作。

- a) 校验 Service-Route 头域的 URI 列表是否与收到请求中的预加载的 Route 头部相匹配, 如果不匹配,

P-CSCF 将不转发该请求,并返回 400(Bad Request)响应,该响应中可以包含带有 warn-code 399 的 Warning 头;或者 P-CSCF 用最近注册时保存 Service-Route 头域来替换请求中预加载的 Route 消息头。

- b) 如果有 P-Preferred-Identity,删除并插入 P-Asserted-Identity,其中的值应标识为请求的发起者。
- c) 插入 P-Charging-Vector 消息头,包含根据 3GPP2 X.S0013-008 产生的 icid 值。

当 P-CSCF 收到上述请求的任何响应时,P-CSCF 应保存响应中 P-Charging-Function-Addresses 消息头的值。

当 P-CSCF 收到 UE 发起的除目标刷新请求以外的后续请求(包括与当前对话相关的未知方法),P-CSCF 应进行以下操作。

- a) 检验该请求是否关联一个现存的对话:
 - 如果没有与请求关联的对话,P-CSCF 将不转发该请求,同时 P-CSCF 将返回 403 (Forbidden) 响应,该响应中可以包含带有 warn-code 399 的 Warning 头;
 - 如果存在与请求关联的对话,P-CSCF 将继续以下操作。
- b) 校验请求中的 Route 消息头和保存的关联对话的 Record-Route 消息头,如果不一致,P-CSCF 将不转发该请求,并返回 400 (Bad Request) 响应,该响应中可以包含带有 warn-code 399 的 Warning 头;或者 P-CSCF 用保存的关联对话的 Record-Route 消息头来替换请求中的 Route 消息头。
- c) 对于非 INVITE 的对话,插入 P-Charging-Vector 消息头,包含根据 3GPP2 X.S0013-008 产生的 icid 值。
- d) 对于 INVITE 对话,刷新保存的 Contact 消息头的值,以使 P-CSCF 必要时能释放会话。

当 P-CSCF 收到 UE 发起的未知方法请求时(与当前的对话无关),而且存在一个 Service-Route 列表与请求的发起者相对应,P-CSCF 应进行以下操作。

a) 校验 Service-Route 消息头中的 URI 列表是否以相同的顺序存在于收到的请求所带的预装载的 Route 消息头,如果不匹配,P-CSCF 将不转发该请求,并返回 400 (Bad Request) 响应,该响应中可以包含带有 warn-code 399 的 Warning 头;或者 P-CSCF 用最近注册时保存 Service-Route 头域来替换请求中预加载的 Route 消息头。

- b) 如果有 P-Preferred-Identity,删除并插入 P-Asserted-Identity,其中的值应标识为请求的发起者。

5.1.3.2 UE 终结的请求

当 P-CSCF 接收到发往 UE 的初始对话请求,在转发之前 P-CSCF 应进行以下操作。

- a) 转换 Record-Route 列表信息到 Route 列表信息中,并保存 Route 列表;
- b) 如果该请求为 INVITE,保存请求中的 Contact, CSeq 和 Record-Route 字段并备份,以使 P-CSCF 必要时能释放会话;
- c) 把 P-CSCF 的 SIP URI 加到 Record-Route 头域的最顶端并保存列表,其中 P-CSCF SIP URI 中包含有关 SIP 压缩的参数(详细定义见 IETF RFC 3486)以及与 UE 建立的安全关联中受保护的服务器端口号;
- d) 把 P-CSCF 的地址加到 Via 头域的最顶端并保存该列表,其中 P-CSCF SIP URI 中包含有关 SIP 压缩的参数(详细定义见 IETF RFC 3486)以及与 UE 建立的安全关联中受保护的服务器端口号;
- e) 保存 P-Charging-Function-Addresses 消息头的值;
- f) 移除并保存 P-Charging-Vector 消息头中的 icid;
- g) 备份“P-Called-Party-ID”消息头。

当 P-CSCF 收到上述请求的 1xx 或 2xx 响应时, P-CSCF 应进行以下操作。

a) 如果有 P-Preferred-Identity, 删除并插入 P-Asserted-Identity, 其中的值应为收到请求时保存下来的 P-Called-Party-ID 中的参数。

b) 校验 Via 列表是否与同一对话的请求消息中保存的 Via 列表匹配, 如果不匹配, P-CSCF 应丢弃该响应; 或者根据前面收到的请求替换 Via。

c) 校验请求中 Record-Route 的 URI 列表是否以相同的顺序存在于响应的 Record-Route 列表中, 如果不匹配, P-CSCF 应丢弃该响应; 或者根据前面收到的请求替换 Record-Route。

如果校验成功, P-CSCF 将重写 Record-Route 中自身的端口号, 用于接收来自主叫方的后续请求, 并删除 SIP 压缩参数。

d) 保存 dialog ID 和与会话相关的 PVI 及 PUI。

e) 如果响应对应于 INVITE 请求, 保存响应中的 Contact、To、From 和 Record-Route 头域的值, 以使 P-CSCF 必要时能释放会话。

当 P-CSCF 收到上述请求的其他响应时, P-CSCF 校验 Via 列表是否与同一对话的请求消息中保存的 Via 列表匹配, 如果不匹配, P-CSCF 将丢弃该响应, 或者根据前面收到的请求替换 Via。

当 P-CSCF 接收到发往 UE 的目标刷新请求, 在转发之前 P-CSCF 应进行以下操作:

a) 把 P-CSCF 的地址加到 Via 头域的最顶端并保存该列表, 其中 P-CSCF SIP URI 中包含有关 SIP 压缩的参数 (详细定义见 IETF RFC 3486) 以及与 UE 建立的安全关联中受保护的服务器端口号;

b) 把 P-CSCF 的 SIP URI 加到 Record-Route 头域的最顶端并保存列表, 其中 P-CSCF SIP URI 中包含有关 SIP 压缩的参数 (详细定义见 IETF RFC 3486) 以及与 UE 建立的安全关联中受保护的服务器端口号;

c) 对于 INVITE 对话, 更新保存的 Contact 和 Cseq 消息头, 以使 P-CSCF 必要时能释放会话。

只有收到 1xx 或 2xx 响应后更新的 Contact 值才有效, 否则依然使用旧的值。

当 P-CSCF 收到上述请求的 1xx 或 2xx 响应时, P-CSCF 应进行以下操作。

a) 校验 Via 列表是否与同一对话的请求消息中保存的 Via 列表匹配, 如果不匹配, P-CSCF 应丢弃该响应; 或者根据前面收到的请求替换 Via。

b) 重写 Record-Route 中自身的端口号, 用于接收来自主叫方的后续请求, 并删除 SIP 压缩参数。

c) 更新保存的 Contact 消息头, 以使 P-CSCF 必要时能释放会话。

当 P-CSCF 收到上述请求的其他响应时, P-CSCF 应进行以下操作。

a) 校验 Via 列表是否与同一对话的请求消息中保存的 Via 列表匹配, 如果不匹配, P-CSCF 应: 丢弃该响应; 或者根据前面收到的请求替换 Via。

b) 重写 Record-Route 中自身的端口号, 用于接收来自主叫方的后续请求, 并删除 SIP 压缩参数。

当 P-CSCF 接收到发往 UE 的独立事务请求或未知方法请求 (与当前的对话无关), 在转发之前 P-CSCF 应进行以下操作。

a) 把 P-CSCF 的地址加到 Via 头域的最顶端并保存该列表, 其中 P-CSCF SIP URI 中包含有关 SIP 压缩的参数 (详细定义见 IETF RFC 3486) 以及与 UE 建立的安全关联中受保护的服务器端口号;

b) 保存 P-Charging-Function-Addresses 消息头的值;

c) 移除并保存 P-Charging-Vector 消息头中的 icid;

d) 备份 “P-Called-Party-ID” 消息头。

当 P-CSCF 收到上述请求的任何响应时, P-CSCF 应进行以下操作。

a) 校验 Via 列表是否与同一对话的请求消息中保存的 Via 列表匹配, 如果不匹配, P-CSCF 应丢弃该响应; 或者根据前面收到的请求替换 Via。

b) 如果有 P-Preferred-Identity, 删除并插入 P-Asserted-Identity, 其中的值应为收到请求时保存下来的 P-Called-Party-ID 中的参数。

当 P-CSCF 接收到发往 UE 的独立事务请求或未知方法请求(与当前的对话无关), 在转发之前 P-CSCF 应进行以下操作。

a) 把 P-CSCF 的地址加到 Via 头域的最顶端并保存该列表, 其中 P-CSCF SIP URI 中包含有关 SIP 压缩的参数(详细定义见 IETF RFC 3486)以及与 UE 建立的安全关联中受保护的服务器端口号;

b) 移除并保存 P-Charging-Vector 消息头中的 icid;

c) 对于 INVITE 对话, 更新保存的 Cseq 消息头, 以使 P-CSCF 必要时能释放会话。

当收到上述请求的任何响应时, P-CSCF 应:

校验 Via 列表是否与同一对话的请求消息中保存的 Via 列表匹配, 如果不匹配, P-CSCF 应丢弃该响应; 或者根据前面收到的请求替换 Via。

5.1.4 会话管理功能

IMS 中的 SIP 信令的路由需要使用 SIP URI。E.164 格式的公共用户标识 PUI 不用于 IMS 路由, 基于 E.164 格式的 PUI 的会话请求需要进行转换成为 SIP URI 格式再进行路由。SIP URI 可以通过 DNS 完成解析。IMS 系统实体的路由信息的获取可以通过静态配置完成, 也可以通过 DNS/ENUM 服务的动态方式完成。

P-CSCF 在处理 SIP 请求时, 应能应用 IETF RFC 3261 中描述的松散路由策略。在 IMS 中所有的 SIP 消息都要通过用户归属域的 S-CSCF 进行路由。P-CSCF 应维护两组路由信息。第一组路由信息列表是在注册过程中建立的, 仅用来验证用户发起的起始请求中的路由信息, 此路由信息列表在用户相应的公共用户标识 PUI 的整个注册期间是有效的。第二组路由信息列表是根据起始 INVITE 请求及其应答消息中的 Record-Route 头域来建立的, 用于会话过程中的路由, 一旦会话结束, 此路由信息列表将被清除。

5.1.4.1 初始 INVITE

a) MO 会话请求处理

当 P-CSCF 收到 UE 的 INVITE 请求时, 可要求周期性的刷新, 以免 P-CSCF 的状态吊死。如果 P-CSCF 要求周期性刷新会话, 将采用在 IETF RFC 4028 clause8 中描述的流程。

注: 刷新请求会话要求至少一个 UE 支持。该功能不能自动获得, 例如, 至少有一个参与的 UE 支持。

P-CSCF 对所有 INVITE 请求响应返回 100 (Trying) 临时响应。

如果支持 SBBC, P-CSCF 应在 UE 发送到 P-CSCF 的第一个请求中的 P-Charging-Vector 头中增加 access-network-charging-info 参数(如果通过 Ty 和 Tx 接口从 PCRF 获得了计费信息)。典型情况下, 如果远端 UA 支持资源预留, 则第一个请求为 UPDATE; 如果远端 UA 不支持资源预留, 则第一个请求为 re-INVITE。

b) MT 会话请求处理

当 P-CSCF 接收到发往 UE 的 INVITE 请求时, 可能要求周期性的刷新, 以免 P-CSCF 的状态吊死。如果 P-CSCF 要求周期性刷新会话, 将采用在 IETF RFC 4028 clause8 中描述的流程。

注：刷新请求会话要求至少一个UE支持。该功能不能自动获得，例如，至少有一个参与的UE支持。

当P-CSCF收到发往UE的初始请求，其中在Request-URI中包含UE的URI，以及一个预加载的Route头。收到的初始INVITE请求也可以有Record-Route头列表。

另外，P-CSCF将给所有INVITE请求回100（Trying）临时响应。

如果支持SBBC，P-CSCF应在UE发送到P-CSCF的第一个请求中的P-Charging-Vector头中增加access-network-charging-info参数（如果通过Ty和Tx接口从PCRF获得了计费信息）。典型情况下，如果远端UA支持资源预留，则第一个请求为180（Ringing）或者200（OK）；如果远端UA不支持资源预留，则第一个请求为re-INVITE。

5.1.4.2 会话释放

对于正在建立的多媒体会话，当收到失去无线覆盖的指示时（如PCRF发起的异常中止会话请求），P-CSCF应该取消对话，根据IETF RFC 3261 和IETF RFC 3326的相关过程，向UE发送CANCEL消息。

对于已经存在的会话，P-CSCF收到无线接口资源无效的指示（如来自PCRF的异常中止会话的请求），应按照以下步骤释放会话。

a) 如果 P-CSCF 服务于会话的主叫用户，将产生 BYE 请求，该请求消息的内容将基于保存的对话相关的信息，包括以下几项：

- Request-URI，设置为保存的被叫提供的Contact头；
- To消息头，设置为初始INVITE请求对应的200OK中的To头；
- From消息头，设置为初始INVITE请求中的From头；
- Call-ID消息头，设置为初始INVITE请求中的Call-ID头；
- Cseq消息头，设置为当前从主叫到被叫的Cseq，增量加1；
- Route消息头，设置为保存的到被叫的路由信息；

其他消息头，基于本地策略设置或者根据请求会话释放的原因设置。

b) 如果 P-CSCF 服务会话的被叫用户，将产生 BYE 请求，该请求的内容基于保存的对话相关的信息，包括以下几项：

- Request-URI，设置为主叫提供的Contact头；
- To消息头，设置为初始INVITE请求的From头；
- From消息头，设置为初始请求INVITE对应的200（OK）响应中的To头；
- Call-ID消息头，设置为初始INVITE请求中的Call-ID头；
- Cseq消息头，设置为当前从被叫到主叫的Cseq，增量加1；
- Route消息头，设置为到主叫的路由信息；

其他消息头，基于本地策略设置或者根据请求会话释放的原因设置。

c) 发送 BYE 请求到被指示的用户。

d) 当 P-CSCF 收到对话 BYE 请求的 2xx 响应，P-CSCF 将删除保存的所有与该对话相关的信息。异常情况下，P-CSCF应该中止该请求，并回响应481（对话或者事务不存在）。

当用户的安全联系已经被删除，如果仍有和这个用户有关的对话处于活动状态，P-CSCF 应该丢弃所有与这些对话相关的信息。

如果支持SBBC，P-CSCF需要通过Tx接口告知该会话已经中止。

当其他实体发起会话释放时，P-CSCF收到对应当前对话BYE请求的2xx响应，应删除保存的所有与该对话相关的信息。

如果P-CSCF要求会话能定时刷新，而且P-CSCF得到了会话将被刷新的信号，那么会话定时器一旦超时，P-CSCF就应该删除和这个会话有关的信息。

如果支持SBBC，P-CSCF需要通过Tx接口通知IP-CAN，该会话已经被终止了。

5.1.4.3 后继请求

P-CSCF应对所有reINVITE请求回应100 (Trying) 临时响应。

如果支持SBBC，UE发起的reINVITE或者UPDATE请求，当P-CSCF发送该请求/后续请求到S-CSCF时，P-CSCF应在P-Charging-Vector头中包括更新过的access-network-charging-info参数。

如果支持SBBC，发往UE的reINVITE或者UPDATE请求，当P-CSCF发送200 (OK) 响应到S-CSCF时，P-CSCF应在P-Charging-Vector头中包括更新过的access-network-charging-info参数。

5.1.5 媒体授权检查

当P-SCSCF收到任何含有SDP offer的SIP请求，P-CSCF将检查收到的SDP中的媒体参数。根据本地的策略，如果P-CSCF发现任何网络上不允许的媒体参数，P-CSCF将返回含有SDP负载的488响应(Not Acceptable Here)。这个SDP负载可以包含所有的媒体类型，编解码方法和本地策略允许的其他SDP参数；或者依据P-CSCF所属运营商的配置，包含这些允许参数的子集。这个子集可能依赖于收到的SIP请求的内容。P-CSCF应根据编码优先次序对SDP负载进行排序。如果SDP offer被加密，P-CSCF可拒绝请求。

当P-CSCF收到含有SDP offer又不同于200 (OK) 响应的SIP响应，P-CSCF将不检查收到的SDP offer中的媒体参数，但P-CSCF将检查后续的含有对这个offer的SDP answer，如果需要（例如，UE产生的SDP answer违背了本地策略），P-CSCF将返回一个488响应，包含本地策略所允许的SDP负载。如果SDP answer被加密，P-CSCF将拒绝后续的请求。

当P-CSCF收到包含SDP offer的200 (OK) 响应，P-CSCF应检查SDP中的媒体参数。依据本地策略，如果P-CSCF发现不允许的媒体参数，P-CSCF将转发SDP offer，在收到含有SDP answer的ACK时，释放已存在的会话。

P-CSCF将监视“b=RS”和“b=RR”列，目的是发现RTCP所需要的带宽分配。

5.1.6 QoS 和承载控制要求

IMS网络与接入网络相互独立，IMS会话控制并不直接控制传输承载网络的资源分配，这需要在IMS会话层和传输承载层间建立一套交互机制，即基于业务的承载控制(Service Based Bearer Control, SBBC)。

SBBC解决会话控制层与承载层机制之间的控制机制。这种联系通过cdma2000 ALL-IP NAM中的两个接口来定义。第一个是连接PDSN/AGW（负责承载资源策略实施）和策略计费规则功能(Policy and Charging Rules Function, PCRF)的Ty接口。另一个是连接PCRF和应用功能(Application Function, AF, 负责应用层业务决策)的Tx接口。从策略控制的角度说，PCRF担当策略决策点(Policy Decision Point, PDP)。

P-CSCF应能作为AF，支持与PCRF的Tx接口，进而完成授权承载建立、授权承载修改、撤销授权、启用和禁用属于某个会话的媒体流、从PCRF接收承载资源不再可用的指示等功能。

5.1.7 信令压缩与解压缩

在 IMS 中, 主要采用 SIP 信令。由于 SIP 信令采用文本的编码方式, 使得信令的流量大大增加。为了节约链路带宽资源 (特别是无线链路带宽资源), 应该使用信令压缩技术对 SIP 信令进行压缩处理, 以便有效利用带宽, 减少传输时延。IMS 系统的 P-CSCF 要求支持 SIP 信令的压缩, IMS 内的 SIP 消息可以不需要压缩。

P-CSCF 应该能够支持 IETF RFC 3320 和 IETF RFC 3321 (可选) 所要求的信令压缩机制。当采用信令压缩时, P-CSCF 应根据 IETF RFC 3486 来决定是否发送压缩的 SIP 消息。

P-CSCF 应该能够根据 IETF RFC 3485 支持基于 SIP/SDP 字典的压缩。

P-CSCF 应该能够压缩发给 UE 的 SIP 请求和响应, 并能够解压从 UE 收到的压缩后的 SIP 请求和响应。

5.1.8 计费功能

P-CSCF 在收到特定的 SIP 后必须能够向 AAA 报告计费信息。

报告是通过发送 Diameter Accounting Requests (ACR) [start, interim, stop and event] 消息实现的。在与成功 SIP 会话相关的流程中, P-CSCF 使用 ACR Start、Interim 和 Stop 消息; 在不成功的 SIP 会话相关的流程和非会话的流程中, P-CSCF 使用 ACR Event 消息。

ACR消息的触发可以由运营商根据具体情况自行定义。

P-CSCF 必须支持基于流的计费功能, P-CSCF 起到了 AF 的作用。AF 提供给 CRF 相关信息用于 CRF 选择合适的计费规则。

5.1.9 安全要求

5.1.9.1 鉴权

P-CSCF 应支持 IMS AKA 鉴权、HTTP Digest 鉴权、基于 CAVE 的 2G RUIM 卡鉴权方式, 本部分中只给出 IMS AKA 的详细规定。

具体内容见 5.1.1 节。

5.1.9.2 完整性保护

P-CSCF 应支持 P-CSCF 与 UE 之间的 SIP 信令的完整性保护。

P-CSCF 可以采用 IPsec ESP (见参考文献 IETF RFC 2406) 协议来提供 UE 和 P-CSCF 间 SIP 信令的完整性保护, 保护 IP 层的所有 SIP 信令, 并且完整性保护应该采用传输模式。

P-CSCF 也可以支持网络部分, 对同一安全域内的 CSCF 间消息的完整性保护, 具体算法可以由运营商自己决定, 也可以对不同安全域内的 CSCF 间以及 CSCF 与 HSS 间的消息应进行完整性保护。

5.1.9.3 SIP 信令的加密

根据运营商的需要, UE 和 P-CSCF 之间的 SIP 信令消息可能会施加保密性保护。这里采用 IPsec ESP 来提供保护。运营商应该注意所配置的保密性保护方案和漫游协议能够满足本地私有性法规中提出的保密性需求。在 SIP 层提供以下机制:

P-CSCF 应该决定是否使用 IMS 特定加密机制。如果使用, UE 和 P-CSCF 应该协商安全联盟, 从而确定保密性保护中所使用的加密密钥;

在网络部分, P-CSCF 对同一安全域内/不同安全域内的 CSCF 间消息的机密性保护为可选。

5.2 I-CSCF 的功能

5.2.1 S-CSCF 指配

5.2.1.1 正常情况下 I-CSCF 的处理过程

I-CSCF支持在注册流程中充当SIP stateful proxy的功能。

当I-CSCF收到一个注册请求，I-CSCF会向HSS发起用户注册状态查询流程。用户注册状态查询消息包括PUI，PVI和Visited Network ID等AVP。

如果从HSS返回的用户注册状态查询响应中包括有效的SIP URI，那么I-CSCF用它来代替注册请求中的Request-URI；将注册请求转发给HSS指示的S-CSCF。

如果从HSS返回的用户注册状态查询响应中包括一张能力列表，那么I-CSCF将会进行以下操作。

a) 把注册请求转发给符合全部必选能力的那个S-CSCF。如果多个S-CSCF都具备这些必选能力，则哪个S-CSCF具备更多的可选能力，就选择哪个S-CSCF。

b) 用被选择S-CSCF的URI代替注册请求中的Request-URI。

c) 将注册请求转发给被选择的S-CSCF。

如果用户注册状态查询流程从HSS返回的既有能力列表又有效的SIP URI，则I-CSCF首先使用SIP URI选择S-CSCF，如果被选择的S-CSCF不可达，I-CSCF则根据异常情况下的处理流程选择新的S-CSCF。

当I-CSCF收到来自注册请求的2xx响应，I-CSCF会把它转发给P-CSCF。

5.2.1.2 异常情况下 I-CSCF 的处理过程

如果HSS对用户注册位置请求发送一个拒绝响应，I-CSCF将发送一个403（拒绝）响应，该响应可能包括一个带有warn-code为399的warning头。

如果用户注册状态查询流程无法完成，比如，由于超时或者HSS的消息不正确，I-CSCF会发回一个480响应给UE。

如果I-CSCF找不到一个具备HSS所要求的必选能力的S-CSCF，I-CSCF就发回一个600响应给用户。

如果被选择的S-CSCF不响应I-CSCF发出的注册请求以及后来的重发消息，同时注册请求中integrity-protected参数被设置为“yes”，I-CSCF会发回一个408或504响应给用户。

如果被选择的S-CSCF不响应I-CSCF发出的注册请求以及后来的重发消息，或者S-CSCF返回3xx或480响应，同时注册请求中没有完整性保护，或'完整性保护'设置为'yes'之外的其他值，I-CSCF会根据已收到的S-CSCF能力列表重选一个S-CSCF。如果之前I-CSCF没有S-CSCF能力列表，则I-CSCF需要从HSS请求一个能力列表，再进行重选。

5.2.2 初始请求处理

5.2.2.1 正常初始请求处理

对于初始请求，I-CSCF可以扮演一个有状态的Proxy角色。

I-CSCF将验证所有的请求是否来自一个可信的域，如果请求来自一个非可信域，I-CSCF应执行以下流程。

a) 如果该请求是注册请求，发送403（拒绝）响应；

b) 如果请求不是注册请求，删除请求中可能包含的所有的P-Asserted-Identity头、P-Access-Network-Info头、P-Charging-Vector头和P-Charging-Function-Addresses头，同时继续下面的流程。

如果请求来自可信域，I-CSCF应执行以下的流程。

当I-CSCF收到一个对话或者单独事务的初始请求，I-CSCF进行以下判断。

a) 如果Request-URI中包含一个pres: 或者一个im: URI, 那么将pres: 或者im: URI转换成用户公有标识, 并把收到的入呼请求中的Request-URI替换成用户的公有标识。

b) 如果请求中不包含一个Route头, 那么检查Request-URI的域名是否和I-CSCF中配置的PSI子域中的一个匹配。如果匹配, 通过内部的DNS机制将Request-URI转换成PSI归属的AS的IP地址, 无需启动用户位置查询过程。否则, I-CSCF将开始向HSS查询被叫用户(被叫用户在Request-URI中指明)位置。

当I-CSCF收到Invite请求, I-CSCF可以进行定期会话刷新, 避免I-CSCF处于吊死状态。如果I-CSCF要求进行会话刷新, 它将根据IETF RFC 4028 clause 8中描述的流程执行。

如果I-CSCF能将Request-URI转换成PSI归属的AS的IP地址, 它应该保存从P-Charging-Vector头中得到的icid参数值, 同时保留P-Charging-Vector头中的icid参数。如果P-Charging-Vector头中没有icid参数, 那么I-CSCF将生成一个新的、全局的、唯一的icid, 并把新生成的icid插入在P-Charging-Vector头中。如果需要拓扑隐藏, 进行拓扑隐藏, 同时将请求直接发给PSI归属的AS。

当成功地进行用户位置查询, 且响应中包含分配的S-CSCF的URI, I-CSCF应该把从HSS中获得的URI作为topmost Route头插入。保存从P-Charging-Vector头中得到的icid参数值, 同时保留P-Charging-Vector头中的icid参数。如果P-Charging-Vector头中没有icid参数, 那么I-CSCF将生成一个新的、全局的、唯一的icid, 并把新生成的icid插入在P-Charging-Vector头中。如果需要拓扑隐藏, 进行拓扑隐藏, 同时根据topmost Route头路由请求消息。

当成功地进行用户位置查询, 且响应中包含S-CSCF需要的能力, I-CSCF应该选择一个S-CSCF, 将被选的S-CSCF的URI作为topmost Route头插入。保存从P-Charging-Vector头中得到的icid参数值, 同时保留P-Charging-Vector头中的icid参数。如果P-Charging-Vector头中没有icid参数, 那么I-CSCF将生成一个新的、全局的、唯一的icid, 并把新生成的icid插入在P-Charging-Vector头中。如果需要拓扑隐藏, 进行拓扑隐藏, 同时将请求消息发给被选择的S-CSCF。

当查询用户位置不成功, 从HSS返回的响应指出用户不存在, I-CSCF将返回一个合适的表示查询失败的SIP响应。用户在归属网络不存在时, 这个响应可能是404(找不到)或者是604(任何地方都不存在)。

当查询用户位置失败, 从HSS返回的响应表明该用户没有注册或者没有服务提供给这个用户, I-CSCF将返回一个合适的表明查询失败的响应。如果用户被验证为一个合法用户, 但是此时该用户没有注册, 同时没有供给该未注册用户的业务, 这个响应可以是480(临时不可得)。

当I-CSCF收到一个对话或者单独事务的初始请求, 请求中包含一个指向自己的单独的路由头, I-CSCF将根据路由头的内容判断是否需要HSS查询或者隐藏。如果需要HSS查询, I-CSCF执行的过程和没有Router头时描述的流程一致。如果I-CSCF判断对于出呼请求需要信息隐藏, I-CSCF应该从Router头中移走自己的SIP URI; 执行信息隐藏过程, 同时依靠Request-URI头域路由请求。

当I-CSCF收到一个用于对话和单独事务的初始请求, 请求中包含多个Router头, I-CSCF应该从topmost Route头中移走自己的SIP URI; 执行信息隐藏过程, 同时按照topmost Route头路由请求。

注: 为了保持和SIP一致, 无论请求是否是初始请求或者是否需要执行拓扑隐藏, I-CSCF可以将自己可路由的SIP URI添加到任何请求的Record-Route头的顶部。P-CSCF将忽略任何一个不在对话初始请求中的Record-Route头。

当I-CSCF收到初始请求的响应(如183或者2xx响应), 如果存在, I-CSCF将保存P-Charging-Function-Addresses头中的值。如果下一跳不在当前网络中, I-CSCF在转发该请求消息前, 将移除P-Charging-Function-Addresses头。

5.2.2.2 异常情况的处理

在用户位置查询中，如果I-CSCF收到否定性响应，I-CSCF会发回404响应。

如果I-CSCF收到一个CANCEL请求，同时I-CSCF的内部状态显示和HSS的Cx流程正在进行过程中，I-CSCF会用200 OK回应CANCEL，用487响应原先的请求，接下来会丢弃所有来自HSS的Cx应答信息。

5.2.3 THIG 功能

I-CSCF (THIG) 必须向所有包含拓扑信息的信息头 (比如Via、Route、Record-Route、Service-Route) 实施拓扑隐藏。

收到含有path头的注册请求并且需要使用拓扑隐藏时，I-CSCF (THIG) 需要把一个路由可达的I-CSCF (THIG) 的SIP URI放在path头的最上面。I-CSCF (THIG) 将在SIP URI中插入标识符以指示I-CSCF收到的后续请求的方向，例如，指示从S-CSCF到P-CSCF以标识终呼的情况。I-CSCF将采用不同的方式对标识符编码，例如，URI中的唯一参数，URI用户名部分的字符串，或者URI中指明的端口号。

收到含有Record-Route头的初始请求并且需要使用拓扑隐藏时，I-CSCF (THIG) 需要把一个路由可达的I-CSCF (THIG) 的SIP URI放在Record-Route头的最上面。

在发出一个需要使用拓扑隐藏并且含有 P-Charging-Function-Addresses 头的初始请求之前，I-CSCF (THIG) 必须删除 P-Charging-Function-Addresses 头。

当接收到隐藏网络发出的请求/响应，I-CSCF (THIG) 应执行加密过程以实现拓扑隐藏的目的。

接收到发往隐藏网络的请求/回应时，I-CSCF (THIG) 会执行解密操作。

5.2.4 计费功能

I-CSCF应支持离线计费，I-CSCF在收到特定的SIP消息后必须能够通过Rf接口将计费信息发送给AAA，Rf接口使用Diameter协议，计费事件的报告是通过发送Diameter消息Accounting Requests (ACR) 消息实现的。

5.3 S-CSCF 的功能

5.3.1 注册和注销功能

5.3.1.1 用户发起的注册

S-CSCF 需要在注册流程中充当 SIP Registrar 的功能；

S-CSCF 需要支持用户发起的注册请求，包括从归属网络发起的注册请求以及从拜访网络发起的注册请求；

S-CSCF 需要根据运营商的要求能够灵活配置注册有效时长的一个范围；

S-CSCF 可以根据运营商的要求能够灵活配置重注册定时器时长；

S-CSCF 需要根据 Cx 接口返回的消息来判断注册用户信息是否正确 (包括 PUI 是否存在、PUI 和 PVI 是否属于同一签约用户等)，如果不正确，S-CSCF 将拒绝这个注册请求。

5.3.1.1.1 初始注册

在用户初始注册流程中，S-CSCF 对用户进行鉴权为必选功能；

S-CSCF 需要判断初始注册请求是否已经进行了完整性保护：

a) 当收到不带"integrity-protected"参数或者认证头中 "integrity-protected" 参数设为 "No" 的注册请求，SCSCF 应该执行以下流程。

1) 根据收到注册请求中 To 头域中的用户公有标识和 REGISTER 请求的认证头中的用户名中的用户

私有身份鉴别用户。

2) 检查注册请求中是否包含 P-Visited-Network 头, 如果包括, 用该头域值鉴别被访问的网络。

3) 为用户选择鉴权向量, 如果用户没有可用的鉴权向量, S-CSCF 应在与 HSS 执行完 Cx 接口的 MAR, MAA 消息流程后选择一个鉴权向量。

此时 S-CSCF 将自身的 SIP URI 传送给 HSS, 通知 HSS 当前用户通过该 S-CSCF 进行注册, HSS 将用此信息定位该用户后续初始对话请求或其他单独事务到该 S-CSCF。

4) 存储从 P-Charging-Vector 头域中收到的 icid 参数;

5) 通过生成对应于 Register 请求的 401(Unauthorized)响应挑战用户, 该响应包含 WWW-Authenticate 头域, 该头域传送以下内容:

- 在 realm 中包含归属网络标识;
- 在 nonce 中包含 RAND 和 AUTN 参数等;
- 在 algorithm 域中包含安全机制: AKA_{v1}-MD5;
- 在 ik 域中包含用于 P-CSCF 的 IK (完整密钥) 参数;
- 在 ck 域中包含 P-CSCF 使用的 Ck (加密密钥) 参数。

6) 存储 401 响应中的 RAND 参数为以后重同步所用, 如果 S-CSCF 中已经存储了 RAND, 则使用 401 响应中的 RAND 替换已有的 RAND 参数。

7) 将 401 响应转发给 UE。

8) 开启 reg-await-auth 定时器监视下一个注册请求。

b) 如果注册请求进行了完整性保护, 即 “integrity-protected” 参数设置为 “yes”, 如果 reg-await-auth 定时器正在运行, 则 S-CSCF 应该检查请求中的 Call-ID 是否与 401 响应中的 Call-ID 一致, 如果 Call-ID 匹配, 则停止 reg-await-auth 定时器。检查 Authorization 头域中是否包含以下内容:

- username 域中包括用户私有标识;
- Algorithm 域中包括 AKA_{v1}-MD5 算法;
- Response 域中包括认证过程需要的认证挑战应答。

如果包含了认证挑战应答, S-CSCF 应该执行以下步骤:

1) 检查收到的挑战应答认证和期望的认证挑战响应(按照 IETF RFC 3310 描述的 SCSCF 使用 XRES 和其他参数计算得到的)是否一致, 如果一致, 当执行完与 HSS 之间的 Cx Server Assignment 流程, S-CSCF 应该存储以下本地数据信息:

— 与注册的公有用户标识相关的 PUI 列表, 包括注册中使用的 PUI 和隐式注册的 PUI, 每个 PUI 被标识为被禁止或不被禁止。

— 被注册 PUI 的所有 service profile, 包括 iFC。

2) 将用户 Contact 地址和已注册的非被禁止的 PUI (包括关联 PUI, 即隐式注册的 PUI) 关联起来。

3) 利用 Path 消息头维护一个预加载的路由消息表, 并将这个列表与 Contact 地址关联起来。

4) 用户注册成功后, S-CSCF 需要返回 200 消息给 UE, 在 200 OK 响应中, S-CSCF 把所有未被 Barring 的 PUI 列表 P-Associated-URI 消息头返回给用户; S-CSCF 将自身 SIP URI 信息、以及在网络需要 THIG 的情况下 I-CSCF 的 SIP URI 信息通过 Service-Route 消息头返回给用户; S-CSCF 需要在将该注册 PUI 对应的所有地址信息通过 Contact 消息头中返回给用户 (如果其他 UE 使用同一 PUI 注册, 则有多个 contact

地址), 并在 Expires 参数中定义注册的有效时长; S-CSCF 还应启动重注册定时器。

5) S-CSCF 可以根据存储的用户数据中 iFC, 触发可能到 AS 的第三方注册。

5.3.1.1.2 重注册

为了刷新已经存在的注册, 或者响应UE注册状态的变化, 或者UE的能力发生变化, UE应该发起重注册。用户重注册遵循与“用户初始注册”相同的处理方式。UE必须保持一个比网络侧注册相关定时器短一点的定时器。在重注册过程中, 对于未进行完整性保护的重注册请求, S-CSCF应该对用户进行重新鉴权。对于已经进行完整性保护的重注册请求, S-CSCF需要根据运营商的鉴权配置来决定是否需要重新对用户进行鉴权。如果需要对用户进行鉴权, 采用的鉴权过程应和初始注册过程中鉴权流程一样。用户重注册成功后, S-CSCF需要更新相应的关联关系: 重新将用户Contact地址和已注册的PUI (包括关联PUI, 即隐式注册的PUI) 关联起来; 重新利用Path消息维护一个预加载的路由消息表, 并将这个列表与Contact地址关联起来。当此用户已经和原来的Contact地址信息 (该Contact的地址值不同于重注册Contact的地址值) 关联且原注册并未到期, S-CSCF需要强制执行网络注销流程来注销原来的Contact地址信息。用户注册成功后, S-CSCF还应重新启动重注册定时器。S-CSCF需要检查重注册请求消息中的Expire头域, 如果Expire头域值为0, 则S-CSCF应判断此流程为用户发起的注销流程, 将按照用户发起的注销流程处理。S-CSCF可以根据存储的用户数据中iFC信息, 触发可能到AS的第三方重注册。

5.3.1.2 隐式注册

a) 如前述注册功能需求, S-CSCF 应支持用户通过 HSS 返回的隐式注册集在一次注册过程中同时注册多个 PUI, 这些 PUI 可以是 SIP URI 格式或者 TEL URI 格式;

b) S-CSCF 需要保证隐式注册集内某个 PUI 不能被单独注册或注销, 隐式注册集内某个 PUI 只要被注册或注销, 隐式注册集内的所有其他 PUI 也必须同时被注册或注销;

c) S-CSCF 和 HSS 之间 Cx 参考点在注册隐式注册集中的任何一个 PUI 时, 应该支持下载所有与隐式注册相关的 PUI;

d) 在注册期内, S-CSCF 应该存储与注册相关的 PUI 的所有 Service Profile;

e) S-CSCF 需要将同一重注册定时器功能运用于隐式注册集内所有的 PUI 上。

5.3.1.3 第三方注册

a) S-CSCF 需要支持在 PUI 注册成功后, 根据 HSS 下载对应的用户签约数据触发可能到 AS 的第三方注册: S-CSCF 遍历所述签约数据的隐式注册集中所有关联 PUI 的业务描述数据, 将注册消息与注册初始过滤规则中的初始过滤规则进行匹配, 并且在匹配成功时向对应的应用服务器 (AS) 发送请求消息以进行第三方注册, 第三方注册消息中 Request URI 应该为 AS 的地址, From 头域应该填充为 S-CSCF URI 信息, To 头域应该填充为注册用户 PUI, Contact 头域应填充为 S-CSCF 地址信息;

b) 第三方注册中包含的 expiration time 与 S-CSCF 在对收到的 register 请求向 UE 发送的 200 OK 响应消息中的 expiration time 是一致的;

c) 如果从 HSS 下载的数据中包含业务信息 (Service information) 数据, S-CSCF 需要支持通过第三方注册将业务信息透明传送给 AS。

d) 如果 AS 成功接受注册请求, 那么会向 S-CSCF 返回 200 (OK) 响应;

e) 如果 AS 未成功接受注册请求, 那么会向 S-CSCF 返回 4xx、5xx 等状态码的响应, 此时 S-CSCF 的处理需要根据触发该第三方注册的 iFC 中以下的默认处理要求分别对待:

- 如果默认处理要求是 SESSION_CONTINUED, 那么继续检查其他更低优先级的 iFC;
- 如果默认处理要求是 SESSION_TERMINATED, 那么停止检查 iFC, 并向用户侧进行网络注销。

5.3.1.4 注册状态信息订阅

a) S-CSCF 支持用户所有未被禁止的 PUI、所有 Path 头域标识的实体 (例如: P-CSCF) 以及 iFC 列表中的 AS 发起的对 UE 注册状态的订阅。

b) S-CSCF 在收到新的订阅请求时, S-CSCF 需要鉴别收到的 SUBSCRIBE 请求中 P-Asserted-Identity 消息头中的标识, 如果该标识已经注册, S-CSCF 会返回 200 消息, 随后 S-CSCF 需要向该订阅者发送 NOTIFY 消息, 通知其用户注册状态信息。

c) 在用户注册状态信息发生变化的情况下, S-CSCF 需要向所有订阅者发送 NOTIFY 消息, 通知其用户注册状态信息的改变。

d) S-CSCF 需要支持以下用户注册状态改变事件:

- Registered (PUI的初始注册);
- Created (PUI被初始隐式注册);
- Refreshed (PUI的重注册);
- Shortened (网络发起的重鉴权);
- Deactivated (网络发起的注销, 并规定以后可以再进行注册);
- Probation (网络发起的注销, 并规定某个时间以后必须再进行注册);
- Unregistered (用户发起的注销);
- Rejected (网络发起的注销, 并规定以后不可以再进行注册)。

e) S-CSCF 可以支持注册过程中的隐式订阅功能: 如果 S-CSCF 收到的注册请求中包含了建立隐式订阅事件的信息, 那么 S-CSCF 在用户注册成功后, 假定同时收到订阅 (SUBSCRIBE) 请求, S-CSCF 需要根据假定收到的订阅 (SUBSCRIBE) 请求在用户与 S-CSCF 之间创建订阅用户事件包的订阅对话, 然后 S-CSCF 会向 UE 返回注册应答消息, 指示隐式对话已经建立。(可选)

5.3.1.5 用户发起的注销

当S-CSCF收到IMS AKA鉴权用户发起的Expires头域为0的注册请求时, S-CSCF应进行以下操作。

a) 检查 Authorization 头域中的 integrity-protected 是否为“yes”, 指示接收到的注册请求是否已进行完整性保护。如果 integrity-protected 为“no”, S-CSCF 应该丢弃该注销请求; 如果 integrity-protected 为“yes”, S-CSCF: 释放被注销的 PUI (包括关联 PUI) 所有会话。

b) S-CSCF 收到注销消息后, 如果被注销的 PUI (包括关联 PUI) 只和一个用户 Contact 地址关联, 那么 S-CSCF 需要把自身保存的此关联项删除; 否则, S-CSCF 只需要删除自身保存的该 Contact 地址。

c) S-CSCF 将注销消息与注册初始过滤规则中的初始过滤规则进行匹配, 并且在匹配成功时向对应的应用服务器 (AS) 发送请求消息以进行第三方注销。

d) S-CSCF 收到注销消息后, S-CSCF 需要通知 HSS 该 PUI 的注销, 并相应地将 HSS 中对应 PUI (包括关联 PUI) 的状态设置为非注册状态, 并且 S-CSCF 需要删除或更新 (在被注销的 PUI 和多个用户 Contact 地址关联的时候就是更新; 不是这种情况的时候就是删除) 该 PUI (包括关联 PUI)、PUI 的注册状态以及所对应的 service profile (包括所有的关联 PUI 以及关联 PUI 所对应的所有 service profile)。

当S-CSCF收到HTTP Digest或者基于CAVE的2G RUIM卡鉴权用户发起的Expires头域为0的注册请求时，S-CSCF不做完整性保护检查，其他处理过程同上。

5.3.1.6 网络发起的注销

a) S-CSCF 需要支持重注册定时器超时而触发的网络注销流程。

b) S-CSCF 需要支持 HSS 基于管理目的（如删除开户用户的签约信息）发起的网络注销流程。

c) S-CSCF 需要支持自身内部事件而发起的网络注销流程。

d) 网络发起注销流程时，S-CSCF 需要释放其对应的活动会话、删除其对应的用户数据并通知 HSS 该 PUI 的注销，并相应地将 HSS 中对应 PUI（包括关联 PUI）的状态设置为非注册状态，并且 S-CSCF 需要删除或更新（在被注销的 PUI 和多个用户 Contact 地址关联的时候就是更新；不是这种情况的时候就是删除）该 PUI（包括关联 PUI）、PUI 的注册状态以及所对应的 service profile（包括所有的关联 PUI 以及关联 PUI 所对应的所有 service profile）。

e) 网络发起注销流程时，S-CSCF 将注销消息与注册初始过滤规则中的初始过滤规则进行匹配，并且在匹配成功时向对应的应用服务器（AS）发送请求消息以进行第三方注销。

f) 网络注销流程的情况，S-CSCF 都需要发送 NOTIFY 通知消息给 UE 和 P-CSCF 来通知其注销事件；重注册定时器超时而发起的网络注销流程的情况下 S-CSCF 可以不发送。

5.3.2 鉴权

S-CSCF应支持IMS AKA鉴权、HTTP Digest鉴权、基于CAVE的2G RUIM卡鉴权等鉴权方式。

a) 在用户初始注册流程中，S-CSCF 对用户进行鉴权为必选功能；

b) 在用户重注册和注销流程中，S-CSCF 是否需要用户对用户进行鉴权应与 5.3.1 节中的描述相同；

c) 在重注册流程和注销流程中，S-CSCF 使用的鉴权流程必须与初始注册流程中使用的鉴权流程保持一致；

d) S-CSCF 需要从 HSS 获得用户对应的鉴权数据，鉴权功能是由 S-CSCF 和 HSS 配合完成；

e) S-CSCF 需要检查 UE 提供的鉴权响应，通过比较 UE 提供的鉴权响应参数和从 HSS 下载存储的鉴权响应来判断用户的鉴权是否通过；

f) S-CSCF 需要支持由运营商策略配置而发起的重鉴权请求，该重鉴权请求是通过 NOTIFY 通知消息发送给 UE，其中含有缩短注册的有效时长的事件（可选）。

5.3.3 用户和业务数据管理

用户和业务数据管理需求如下：

a) S-CSCF 需要支持某个 PUI 在多个 PVI 之间共享使用；

b) S-CSCF 需要在初始注册过程从 HSS 下载用户对应的用户数据（包括基本用户数据和业务订阅数据），并在初始注册成功后将下载的用户数据存储在 S-CSCF 中；

c) S-CSCF 需要支持 HSS 主动发起的用户数据修改操作；

d) S-CSCF 需要支持在第三方注册过程中将和 AS 相关的 Service information 透明地传递给相应的 AS（可选）；

e) S-CSCF 需要配合 HSS 来支持用户组的管理：用户注册时，HSS（在 HSS 中预先对用户进行分组管理，设定用户组相关信息）将同组用户注册到同一 S-CSCF，并向该 S-CSCF 下发用户组的相关信息，S-CSCF 根据系统处理能力和所述用户组相关信息对同组内其他用户的接入请求进行动态控制（可选）。

注册过程前后S-CSCF中的信息存储状态如下：

a) 注册前：无状态信息。

b) 注册期间：HSS 的地址、部分用户配置、P-CSCF 的地址/名称、P-CSCF 所在的拜访网络标识符（一般为 P-CSCF 所在拜访网的域名）、注册用户的 PVI、注册用户的 PUI、注册用户的 UE IP 地址。

c) 注册后：HSS 的地址、部分用户配置、P-CSCF 的地址/名称、P-CSCF 所在的拜访网络标识符（一般为 P-CSCF 所在拜访网的域名）、注册用户的 PVI、注册用户的 PUI、注册用户的 UE IP 地址、隐含注册的 PUI (s) 及注册用户的签约信息。

5.3.4 业务触发

MMD系统中，业务的触发在S-CSCF中完成，业务数据在注册阶段或收到对未注册用户进行呼叫的初始请求时被下载到 S-CSCF中，包括 Filter Criteria。

MMD用户配置中和服务相关的专用数据被表示成初始过滤规则。一个过滤规则包括了：业务的触发点，AS的标识，各初始过滤规则的优先级等信息。触发点用来决定是否去联系应用服务器，它包含了一个到多个的服务点触发器实例。

— 请求URI：标识该请求所指向的资源。

— SIP方法：表示该请求的类型。

— SIP消息头：包含与该请求相关的信息。

— 会话情形：有3个可能的值，即Originating、Terminating、或Terminating_Unregistered，指明过滤器是否应该被处理起始、终结或终结未注册的终端用户服务的S-CSCF所使用。起始情形是指当S-CSCF正在服务主叫用户时，终结情形是指当S-CSCF正在服务被叫用户时。

— 会话描述：定义针对SIP方法体内的任何SDP字段内容的服务点触发器。

当S-CSCF收到初始请求时，S-CSCF按以下条件进行过滤器准则的评估。

a) 检查公共用户身份是否被禁止，如果不是，则继续。

b) 检查该请求是一个起始请求还是一个终止请求。

c) 为会话情形选择初始过滤规则（Originating、Terminating、或Terminating_Unregistered）。

d) 通过将该请求的公共用户身份与服务配置相比较，检查该请求是否与该用户的最高优先级的初始过滤规则相匹配。

1) 如果该请求与初始过滤规则匹配，则 S-CSCF 将请求转发给相应的 AS。接下来，S-CSCF 还会检查请求是否与较低优先级的下一个过滤规则相匹配，如果匹配，则在 SIP 消息从前一个 AS 处返回时，将该过滤规则应用于该 SIP 方法。

2) 若该请求不能与最高优先级的初始过滤规则相匹配，则检查它是否与下一个优先级的过滤规则匹配，直至匹配上一个为止。

3) 若不再有初始过滤规则适用，则 S-CSCF 基于路由决策对该请求进行转发。

4) 如果所联系的 AS 没有响应，则 S-CSCF 遵从与初始过滤规则相关的缺省处理过程，即基于过滤规则中的信息，或者终止会话，或者让会话继续。如果初始过滤规则没有包含在联系 AS 失败后 S-CSCF 应如何操作的指示，S-CSCF 的缺省行为是让呼叫继续。

5.3.5 会话控制

5.3.5.1 MO 请求处理

当S-CSCF收到来自信任域的被服务用户或者PSI的对话初始请求或单独事务的请求,在前转这些请求前, S-CSCF应该进行以下操作。

a) 确定请求的P-Asserted-Identity头是否包含一个禁止公有用户标识。如果该头包含有禁止的公有用户标识, S-CSCF将产生403 (Forbidden) 响应拒绝请求。响应中可以包含带有warn-code 399的Warning头。否则, 继续以下步骤。

b) 从Route头的最顶端删除自己的SIP URI。

c) 检查入呼请求的Route头最顶端是否存在S-CSCF以前放置的初始Dialog ID。如果存在, 表示该请求与一个存在的对话关联, 是从AS发送过来的对以前发送到AS请求的响应。

d) 按照优先级的顺序, 检查初始请求是否匹配下一个未执行的基于P-Asserted-Identity中公有用户标识的初始过滤规则, 如果匹配, S-CSCF应该插入AS URI到Route头作为topmost entry, 后面紧跟自己的URI (S-CSCF); 如果AS在信任域以外, S-CSCF将删除请求中P-Access-Network-Info头以及它的值; 如果AS在信任域之内, S-CSCF在前转到AS的请求中保留P-Access-Network-Info头以及它的值。根据处理过滤规则的结果, S-CSCF可能在处理出呼 Request URI之前和一个或者多个AS通信。

e) 如果在入呼请求的最顶端 route头没有初始Dialog ID, 保存P-Charging-Vector头的icid参数的值, 并保留P-Charging-Vector头的icid参数的值。作为可选, 当前转该消息时, S-CSCF可以产生一个新的全局唯一的icid, 在P-Charging-Vector头插入该icid参数。如果S-CSCF产生新的icid, 它将负责维护后续消息中这两个icid值。

f) 如果在入呼请求的topmost route没有初始Dialog Id, 在P-Charging_Vector头插入一个orig-ioi参数。S-CSCF设置的orig-ioi参数值标识了发送消息的网络。S-CSCF不应该包含term-ioi参数。

g) 如果在入呼请求的topmost route没有初始Dialog Id, 且消息是前转到S-CSCF归属域(包括到归属域的AS), 则S-CSCF插入P-Charging-Function-Addresses头, 该头的值从HSS获得的。

h) 如果在入呼请求的topmost route没有初始Dialog Id, 并且S-CSCF知道和P-Asserted-Identity中SIP URI相关联的tel-URI, 则增加第二个P-Asserted-Identity头包含该tel-URI。

i) 如果请求没有前转到AS, 并且出呼Request-URI是tel URI, S-CSCF将使用ENUM/DNS翻译机制(见IETF RFC 3761)将E.164地址(见IETF RFC 3966)翻译成一个全局可路由的SIP URI。如果翻译失败, 该请求可以前转到BGCF或者发起者归属域的其他合适实体(如MRFC来放音), S-CSCF也可以发送一个合适的SIP响应给发起者。如果出呼Request-URI是pres URI或者im URI, S-CSCF将前转该请求(见IETF RFC 3861)。在这种情况下, S-CSCF不允许修改收到的Request-URI。

j) 如果topmost Route中存在地址, 则使用其中的URI决定目的地址(如DNS接入), 否则, 基于Request-URI进行路由。如果目的地址是IP地址类型, 但不是IM CN子系统使用的IP地址类型, 且IM CN子系统支持和不同地址类型网络的交互, S-CSCF将前转该请求到MMD-ALG。

k) 如果根据本地策略需要对网络隐藏, 将I-CSCF (THIG) 的地址放到topmost Route头。

l) 对来自一个被服务用户的对话初始请求: 如果请求路由到信任域的AS, S-CSCF可以决定是否记录Record-Route。如何决定由S-CSCF根据收到的请求消息中的信息来配置。这些信息也可以被用作初始过滤规则。如果请求消息有record-routed, S-CSCF将产生Record-Route头包含自己的SIP URI; 如果请求被路由到别处, 则产生一个Record-Route头, 包含自己SIP URI。

对于由PSI发起的请求，S-CSCF可以决定是否record-route。需要说明的是在处理PSI发起的请求时，S-CSCF如何决定是否将自己的地址填入Record-Route头，可能是运营商策略的一部分。

m) 根据目的用户 (Request-URI)，在前转消息前删除P-Access-Network-Info。

n) 基于SIP路由流程路由请求。

o) 如果请求是INVITE请求，则保存Contact、Cseq和Record-Route头，以便S-CSCF必要时能够释放会话。

如果S-CSCF没有收到响应，或者收到408 (Request TimeOut) 响应，或者来自AS的一个5xx响应，S-CSCF应该：

1) 如果在过滤规则中定义的缺省处理为“SESSION-CONTINUED” (见 X.S0013-005)，或者没有缺省处理指示，则从 step 4 开始执行流程；

2) 如果在过滤规则中定义的缺省处理为“SESSION-TERMINATED” (见 X.S0013-005)，要么前转收到的响应，要么发送 408 (Request Timeout) 响应或者 5xx 响应给被服务的 UE (不再验证更低优先级的过滤规则，并且不进行进一步的处理)。

如果S-CSCF收到来自AS的任何最终响应，它将前转该响应给被服务的UE (不验证更低优先级的过滤规则，并且不进行更多的处理)。

当S-CSCF接收到以上请求的任何响应，S-CSCF可以根据IETF RFC 3323和IETF RFC 3325对P-Asserted-Identity头采用隐藏。

正常情况下P-Asserted-Identity头出现在1xx或者2xx响应中。

以上可选流程是对IETF RFC 3325规范中描述的可信域边界私密隐藏的补充。

当S-CSCF收到对以上请求的任何包含term-ioi的响应，S-CSCF将保存收到的P-Charging-Vector头中的term-ioi参数值 (如果存在的话)。term-ioi参数标识响应消息的发送网络。如果下一跳是AS，term-ioi和orig-ioi参数仅可以保持在P-Charging-Vector头。

当S-CSCF收到对话初始请求的1xx或者2xx响应，如果该响应对应一个INVITE请求，S-CSCF将保存响应中的Contact和Record-Route头，以便必要时能释放会话。

当S-CSCF收到被服务用户一个对话目标刷新请求，在前转该请求之前，S-CSCF应该：

a) 从最顶端的Route头删除自己的URI；

b) 产生包一个包含自己SIP URI的Record-Route头；

c) 如果该请求是一个INVITE请求，保存请求中的Contact和Record-Route头，以便S-CSCF必要时能释放会话。

d) 如果请求将被路由到目的用户 (Request-URI)，或者请求被路由到信任域之外的AS，删除P-Access-Network-Info消息头；

e) 基于最顶端Route头进行路由。

当S-CSCF收到对话目标刷新请求的1xx或者2xx响应，如果响应对应一个INVITE请求，S-CSCF将保存响应中的Contact和Record-Route头，以便S-CSCF必要时能释放会话。

当S-CSCF收到被服务用户的后续请求而不是一个对话目标刷新请求，在前转该请求之前，S-CSCF应该从最顶端的Route头删除自己的URI。在这种情况下，请求被路由到目的用户 (Request-URI) 或者请求被路由到信任域之外的AS，删除P-Access-Network-Info头；并且基于最顶端Route头进行路由。

5.3.5.2 MT 请求处理

当S-CSCF接收一个对话的初始请求或者一个单独事务的请求,该请求的目的地址是静态预配置的PSI或者已经注册的被服务用户,在前转该请求之前,S-CSCF应该进行以下操作。

a) 确定请求的Request-URI中是否包含有一个被禁止的公有用户标识。如果Request URI包含有被禁止的公有用户标识,S-CSCF将通过产生404 (Not Found) 响应拒绝该请求。否则,继续下面的步骤;

b) 删除最顶端Route头中自己URI;

c) 检查入呼的topmost Route头是否存在S-CSCF以前放置的初始Dialog ID。如果存在,表示该请求与一个存在的对话关联,是从AS发送过来,以响应以前发送到AS的请求;如果不存在,表示该请求是第一次访问S-CSCF,在这种情况下,S-CSCF将保存请求中的Request-URI。

d) 如果在入呼请求的最顶端的Route头包含有初始Dialog Id,检查Request-URI和保存的Request-URI是否相等。如果不匹配,则分两种情况操作:

1) 如果是 INVITE 请求,保存 Contact、Cseq 以及 Record-Route 头,以便 S-CSCF 必要时能够释放该会话;

2) 按照最顶端 Route 头前转该请求,并跳过以下步骤。

如果匹配,按照优先级顺序检查初始请求与下一个未被执行的初始过滤规则是否匹配,并按照3GPP2 X.S0013-003 6.5节描述的规则对SIP 方法进行检查。如果存在匹配的过滤规则,将AS URI插入到最顶端的Route头,紧接着插入自己的URI到Route头。

根据处理过滤规则的结果,S-CSCF可能在处理出呼Request URI之前和一个或者更多AS通信。

e) 如果在入呼请求的最顶端route没有初始Dialog Id,且消息前转到S-CSCF归属域(包括到AS),则插入P-Charging-Function-Addresses头。该头的值如果没有,则从HSS获得;

f) 如果在入呼请求的最顶端route头没有初始Dialog ID,保存P-Charging-Vector头的icid参数的值,并且保持P-Charging-Vector头icid参数的值。

g) 如果在入呼请求的最顶端route没有初始Dialog Id,保存P-Charging_Vector头中orig-ioi参数(如果存在)。orig-ioi参数的值标识了请求消息的发送网络。orig-ioi参数仅在下一跳为AS时才在P-Charging-Vector中保留。

h) 如果有必要,按照IETF RFC 3841执行主叫和被叫能力的匹配;

i) 对于请求中没有Route头的情形,可以从目的公有用户标识,注册或者重注册过程中预加载的Route列表决定路由,另外,S-CSCF可根据以前步骤的值建立Route头;可以根据目的公用用户标识,注册或者重注册过程中保存的可达Contact URI决定路由。如果对于目的公有用户标识保存有一个以上的联系地址,S-CSCF应该进行以下操作:

— 如果Request Disposition头被设置“no-fork”,构建Request-URI时采用最高的qvalue参数。如果没有提供qvalue参数,S-CSCF将根据本地策略决定采用哪一个联系地址。

— fork该请求,或者根据初始REGISTER请求中的contact头的qvalue参数执行连续查找-(见IETF RFC 3261)。如果没有提供qvalue参数,S-CSCF将根据Request Disposition头指示决定采用哪一个联系地址(见IETF RFC 3841)。如果Request Disposition头也没有提供,S-CSCF将根据本地策略决定是否fork,或者执行对联系地址的连续查找。

按照以前步骤决定的Contact URI内容构建Request-URI。插入P-Called-Party-ID头，其中包含接收到的请求Request-URI。

j) 如果请求是INVITE请求，保存Contact、Cseq并且Record-Route头，以便S-CSCF必要时能够释放会话。

k) 作为可选，可以根据IETF RFC 3323和IETF RFC 3325对P-Asserted-Identity头采用私密隐藏。

以上可选流程是对IETF RFC 3325规范中描述的可信域边界私密隐藏的补充。

l) 对于一个对话的初始请求，如果请求路由到信任域的AS，S-CSCF可以决定是否记录Record-Route。如何决定是由S-CSCF根据收到的请求的信息来配置的。这些信息可以被初始过滤规则使用。如果请求消息被记录路由record-routed，S-CSCF将产生Record-Route头包含自己的SIP URI。如果请求被路由到别处，产生一个Record-Route头，包含自己SIP URI。

m) 根据最顶端Route头前转该请求。

如果S-CSCF没有收到响应，或者收到408 (Request TimeOut) 响应，或者收到来自AS的一个5xx响应，S-CSCF应进行以下操作：

1) 如果在过滤规则中定义的缺省处理为“SESSION-CONTINUED”（见3GPP2 X.S0013-005），或者没有缺省处理指示，则从step 4开始执行流程；

2) 如果在过滤规则中定义的缺省处理为“SESSION-TERMINATED”（见3GPP2 X.S0013-005），要么前转收到的响应，要么发送408 (Request Timeout) 响应或者5xx响应给被服务的UE（不再验证更低优先级的过滤规则并且不进行进一步的处理）。

当S-CSCF收到对话的初始请求，或者单独事务请求，该请求发往一个没注册的用户，S-CSCF应进行以下操作：

a) 如果S-CSCF没有用户数据，发起S-CSCF注册/注销通知，用来下载相关用户数据（例如，没注册的用户）以及通知HSS用户没有注册，并且该S-CSCF应检查未注册用户的业务触发（见3GPP2 X.S0013-005描述）。

b) 执行上一节的步骤a)，b)和c)（当S-CSCF收到一个对话的初始请求或者单独事务请求，该请求发往注册的被服务用户）；

c) 执行上一节的步骤d)，e)，f)，g)，h)，i)，j)和k)（当S-CSCF收到一个对话的初始请求或者单独事务请求，该请求发往注册的被服务的用户）。

如果不需要与AS联系，S-CSCF将返回适当的不成功SIP响应。该响应可能是480 (Temporarily unavailable) 并且终止这些流程。

当S-CSCF收到一个对话初始请求（无论该用户是否注册）的1xx或者2xx响应，S-CSCF应进行以下操作：

a) 如果是INVITE请求的响应，保存响应中Contact和Record-Route头，以便S-CSCF必要时能够释放会话；

b) 在出呼响应的P-Charging-Vector中插入term-ioi参数。S-CSCF设置term-ioi参数的值标识响应的发送网络，并且设置orig-ioi的值为接收的orig-ioi的值；

c) 如果S-CSCF知道和P-Asserted-Identity头中SIP URI相关联的tel URI，S-CSCF将增加第二个P-Asserted-Identity头，包含tel URI；

d) 如果响应是发送到起呼用户, S-CSCF可以根据本地策略和目的用户 (Request-URI) 删除 P-Access-Network-Info头。

当S-CSCF收到一个单独事务请求的响应 (无论用户是否注册) 时, 如果S-CSCF知道和 P-Asserted-Identity头中SIP URI相关联的tel URI, S-CSCF将增加第二个P-Asserted-Identity头, 包含tel URI。如果响应发送到信任域的AS, S-CSCF将保持P-Access-Network-Info头, 否则, S-CSCF将删除P-Access-Network-Info头。

当S-CSCF收到单独事务请求的200 (OK) 响应时, S-CSCF应该进行以下操作:

a) 如果消息发送到S-CSCF归属域 (包括AS) 则插入P-Charging-Function-Address头, 填写从HSS获得值。

b) 在出呼响应的P-Charging-Vector中插入term-ioi参数。S-CSCF设置term-ioi参数的值标识响应的发送网络, 并且设置orig-ioi的值为接收的orig-ioi的值。

当S-CSCF收到一个对话的目标刷新请求时, 该请求发往一个被服务的用户, 在前转该请求之前, S-CSCF应该进行以下操作:

a) 从最顶端Route头删除自己的URI;

b) 如果该请求为INVITE请求, 需要保存请求中的Contact、Cseq以及Record-Route头, 以便S-CSCF必要时能够释放该会话;

c) 产生包一个含自己的SIP URI的Record-Route头;

d) 根据最顶端Route头前转该请求。

当S-CSCF收到对话的目标刷新请求的1xx或者2xx响应 (无论该用户是否注册), S-CSCF应该应进行以下操作:

a) 如果是对INVITE请求的响应, 保存响应中的Record-Route头和Contact头, 以便S-CSCF必要时能够释放该会话;

b) 如果响应发送到信任域的AS, S-CSCF将保持P-Access-Network-Info头, 否则, 删除该消息头。

当S-CSCF收到是后续请求, 而不是目标刷新请求时, 该请求发往被服务的用户, 在前转该请求之前, S-CSCF应该: 删除最顶端Route头中自己的URI, 根据最顶端Route头前转该请求。

当S-CSCF收到对话的后续请求而不是目标刷新请求的响应时, 如果该响应发送到信任域的AS, S-CSCF将保持P-Access-Network-Info头, 否则, S-CSCF将删除该消息头。

5.3.5.3 初始对话标识

初始对话标识是一个特殊的标记, 在前转该请求到AS之前, S-CSCF将该标记编码到S-CSCF自己的URI中, 形成Route消息头。这也许因为S-CSCF是产生和使用该值的唯一实体。

该标记标识了请求的初始对话, 因此当B2BUA方式的AS改变对话后, 当请求返回到S-CSCF, S-CSCF能够标识初始对话。该标记可以按不同方式进行编码, 例如, 可以作为S-CSCF URI用户部分的一个字符串, 也可以是S-CSCF URI的一个参数, 或者是S-CSCF URI的一个端口号。

S-CSCF将确保选择的值是唯一的, 因此当收到后续消息时, S-CSCF可以确认该值并且相关的对话之间建立关联 (对话通过AS)。

5.3.5.4 初始 INVITE 请求

当S-CSCF收到一个INVITE请求，无论是来自被服务的用户还是发往被服务的用户，S-CSCF可以要求周期性会话刷新，以免S-CSCF状态吊死。如果S-CSCF要求会话被刷新，可以采用IETF RFC 4028 clause 8中描述的流程。

刷新会话的请求要求至少一个UE支持。这种功能不能自动获得，例如，参与的UE至少有一个需要支持该功能。

5.3.5.5 后续请求

1) 起呼情形

当S-CSCF收到1xx或者2xx响应，如果该消息前转到S-CSCF归属域（包含到AS），S-CSCF将插入P-Charging-Function-Addresses消息头，其中的值从HSS中获得。

当S-CSCF收到包含access-network-charging-info参数（在P-Charging-Vector头中）的请求，S-CSCF将保存该参数。当该请求前转到AS时，将保持该参数。然而，当请求前转到S-CSCF的归属域之外时，不包含该参数。

当S-CSCF收到任何与起呼对话或者单独事务相关的请求或者响应（除了ACK请求、CANCEL请求以及对应的响应），在前转该消息到S-CSCF归属域（包括到AS）时，S-CSCF可以插入以前保存的值到P-Charging-Vector头和P-Charging_Function-Addresses头。

2) 终呼情形

当S-CSCF收到1xx或者2xx响应，如果该消息前转到S-CSCF归属域（包括到AS），S-CSCF将插入P-Charging-Function-Address头，其中的值从HSS中获得。

当S-CSCF收到包含access-network-charging-info参数（在P-Charging-Vector头中）的180（Ringing）或者200（OK）（对INVITE）响应时，S-CSCF将保存该参数。当该响应前转到AS时，将保持该参数。然而，当该响应前转到S-CSCF的归属域之外，不能包含该参数。

当S-CSCF收到任何与起呼对话或者单独事务相关的请求或者响应（除了ACK请求和CANCEL请求和响应），在前转该消息到S-CSCF归属域（包括到AS）时，S-CSCF可以插入以前保存的值到P-Charging-Vector头和P-Charging_Function-Addresses头。

5.3.5.6 会话释放

S-CSCF应支持用户发起的会话释放及自身发起的会话释放；

1) 取消正在建立的会话

当收到网络内部释放当前正在建立的会话的指示时，S-CSCF将通过发送CANCEL请求取消相关的对话（见IETF RFC 3261）。

2) 释放已经存在的会话

当收到对已经存在的多媒体会话的释放的指示时，S-CSCF应该进行以下操作：

a) 根据保存的与对话相关的信息为被叫用户产生第一个BYE请求，信息包括以下几项：

- request-URI，设置为保存的被叫用户提供的Contact头；
- To消息头，设置为对应初始请求的200OK响应的To消息头值；
- From消息头，设置初始INVITE请求的From头值；
- Call-ID头，设置初始INVITE请求的Call-ID头值；
- CSeq头，设置为保存的从主叫到被叫方向的CSeq值，增量加1；

— Route头, 设置为保存的该对话到被叫的路由信息;

其他别的消息头, 根据本地策略或者释放会话的原因。

b) 根据保存的与对话相关的信息为主叫用户产生第二各BYE请求, 信息包括以下几项:

— 一个request-URI, 设置为保存的主叫用户提供的Contact头;

— To消息头, 设置为对应初始请求的From消息头值;

— From消息头, 设置对应初始INVITE请求的200OK响应的To消息头值;

— Call-ID头, 设置对应初始INVITE请求的200OK响应的Call-ID头值;

— CSeq头, 设置为保存的从被叫到主叫方向的CSeq值, 增量加1; 如果没有保存该对话的Cseq, 将产生并采用一个有效范围内的随机数, 作为Cseq;

— Route头, 设置为保存的该对话到主叫的路由信息;

— 其他的消息头, 根据本地策略或者释放会话的原因。

c) 如果S-CSCF服务主叫用户, 对于第一个BYE消息可以认为是直接从主叫用户接收到的, 例如, 发送它到内部的业务控制逻辑, 并且根据结果进一步发送到被叫用户;

d) 如果S-CSCF服务主叫用户, 直接向主叫用户发送第二个BYE请求;

e) 如果S-CSCF服务被叫用户, 直接向被叫用户发送第一个BYE请求;

f) 如果S-CSCF服务被叫用户, 对于第二个BYE消息可以认为是直接从被叫用户接收到的, 例如, 发送它到内部业务控制逻辑, 并且根据结果进一步发送到主叫用户;

收到以上两个BYE请求的2xx响应时, S-CSCF将释放对话相关和多媒体会话相关的所有信息。

3) 其他会话释放的需求

a) 由于注册超期释放存在的对话

当唯一注册的公有用户标识(有关联隐式注册集, 但是没有其他注册的公有用户标识)的生命周期到期时, 但仍有包含该用户的多媒体会话处于激活状态, 而且该会话由当前注册的用户或者隐式注册集中的一个发起, S-CSCF将释放每一个多媒体会话。

b) 异常情形

当会话被S-CSCF释放后, S-CSCF收到对话请求, S-CSCF将终止接收的请求, 并且返回481(Call/Transaction Does Not Exist)响应。

c) 被其他实体发起的会话释放

收到对应BYE请求的2xx响应, 且匹配已经存在的对话, S-CSCF将删除所有保存的对话相关的信息。

d) 会话超期

S-CSCF请求会话周期性刷新, 并且S-CSCF获得会话将被刷新的指示, 当会话定时器超时后, S-CSCF将删除所有保存的和对话相关的信息。

5.3.5.7 ReINVITE

a) 起呼情形

对于来自UE的reINVITE请求, 当S-CSCF接收了UPDATE请求, S-CSCF将保存被更新的P-Charging-Vector头的access-network-charging-info参数。当该请求前转到AS时, S-CSCF将保留该参数。然而, 当reINVITE请求前转到S-CSCF归属域之外的网络, S-CSCF在P-Charging-Vector头不包含该参数。

对于来自 UE 的 reINVITE 请求，如果请求前转到信任域之内的 AS，S-CSCF 将保留 P-Access-Network-Info 头，否则 S-CSCF 将删除该头。

b) 终呼情形

对于发往 UE 的 reINVITE 请求，当 S-CSCF 收到对应 reINVITE 的 200 (OK) 响应时，将保存更新的 P-Charging-Vector 头的 access-network-charging-info 参数。当该响应前转到 AS 时，S-CSCF 将保留该参数。当 200OK 响应前转到 S-CSCF 归属域之外的网络，S-CSCF 在 P-Charging-Vector 头包含该参数。

对于 INVITE 请求的任何响应，如果前转到信任域之内的 AS，S-CSCF 将保留 P-Access-Network-Info 头，否则 S-CSCF 将删除该头。

5.3.5.8 媒体授权检查

当 S-CSCF 收到任何含有 SDP offer 的 SIP 请求，S-CSCF 将检查收到的 SDP 中的媒体参数。如果根据本地策略或者签约情况，S-CSCF 发现任何不允许的媒体参数，S-CSCF 将返回一个 488 响应，响应中包含 SDP 载荷。根据本地策略和用户签约情况，或者运营商配置情况，这个 SDP 载荷包含所有允许的媒体类型、编解码方式和其他 SDP 参数，或者这些被允许参数的子集。这个子集可以根据收到的 SIP 请求的内容确定。在 488 响应中 S-CSCF 将建立一个 SDP 载荷，建立的过程和 IETF RFC 3261 中描述的 UAS 在 488 响应中建立 SDP 的过程一样。如果 SDP offer 加密，S-CSCF 将拒绝请求。

当 S-CSCF 收到一个包含 SDP offer 且不同于 200 (OK) 响应的 SIP 响应，S-CSCF 将不检查收到的 SDP offer 中的媒体参数，而是，S-CSCF 将检查后续包含对这个 offer 的响应。如果必要（例如 UE 简化的 SDP 响应仍然违反本地策略）S-CSCF 将返回 488 响应，响应中包含本地策略允许的 SDP 载荷。如果 SDP 响应被加密，S-CSCF 可以拒绝后续的请求。

当 S-CSCF 收到一个 200 (OK) 响应，响应中包含 SDP offer，S-CSCF 将检查收到的 SDP 中的媒体参数。如果根据本地策略或者签约情况，S-CSCF 发现任何不允许的媒体参数，S-CSCF 转发 SDP offer，当收到包含 SDP 响应的 ACK 请求，S-CSCF 将立即中止会话。如果 SDP offer 被加密，S-CSCF 转发 SDP offer，当收到包含 SDP 响应的 ACK 请求，S-CSCF 将立即中止会话。

5.3.6 公共业务标识

在 MMD 网络中支持 PSI（公共业务标识）功能需要 HSS、I-CSCF 和 S-CSCF 等网元共同完成。对 S-CSCF 来说，需要满足以下功能需求：

- a) S-CSCF 需要支持用户在某个 MMD 会话中使用 PSI 做为被叫呼叫号码；
 - b) S-CSCF 需要支持根据 iFC 签约信息将被叫为 PSI 的某个 MMD 会话来正确地触发路由到某个 AS；
- 如同处理普通 MMD 会话一样，S-CSCF 可以使用相同的处理方式（如：信令路由，业务触发等）来处理被叫号码为 PSI 的某个 MMD 会话。

5.3.7 计费功能

5.3.7.1 离线计费

S-CSCF 在收到特定的 SIP 消息后必须能够向 AAA 报告计费信息。报告是通过发送 Diameter Accounting Requests (ACR) [start, interim, stop and event] 消息实现的。在与成功 SIP 会话相关的流程中，S-CSCF 使用 ACR start、interim 和 stop 消息；在不成功的 SIP 会话相关的流程和非会话流程中，S-CSCF 使用 ACR Event 消息。ACR 消息的触发可以由运营商根据具体情况自行定义。

5.3.7.2 在线计费

S-CSCF应支持在线计费功能。

如果S-CSCF利用ISC接口作为在线计费接口，需要OCS提供额外的功能，或者由IMS-GW完成ISC接口到Ro接口的转换。

a) 即时事件计费 IEC

S-CSCF 必须支持即时事件计费功能 IEC。IEC 在 Ro 接口，通过 Debit Units 操作实现。Debit Units 操作可以在提供业务之前，过程中或者结束后进行。

b) 计费单元预留的事件计费 ECUR/计费单元预留的会话计费 SCUR

1) ECUR 和 SCUR: S-CSCF 必须支持计费单元预留的事件计费 ECUR/计费单元预留的会话计费 SCUR 功能。ECUR/SCUR 在 Ro 接口通过 Reserve Units 和 Debit Units 操作实现。这两种操作都可以重复进行。

2) 超过预留有效期的处理：如果没有被使用，预留的单元可以在一个合理的时间被返还。这种情况的出现有可能是因为单元预留和 SIP 会话都被取消了，或只有单元预留被取消。S-CSCF 能够同时支持以上 3 种计费类型，是否使用某种计费类型由业务类型或者运营商的策略决定。

6 性能及可靠性指标

6.1 会话处理能力

单系统最大配置时，P-CSCF 应能够支持单机 500 万及以上 BHSA 的处理能力；

单系统最大配置时，I-CSCF 应能够支持单机 1000 万及以上 BHSA 的处理能力；

单系统最大配置时，S-CSCF 应能够支持单机 300 万及以上 BHSA 的处理能力；

平均会话时长为 120s。

6.2 注册用户数

单系统最大配置时，P-CSCF 应该能支持单机 300 万及以上的用户同时注册。

单系统最大配置时，S-CSCF 应该能支持单机 300 万及以上的用户同时注册。

6.3 系统可靠性和可用性

a) 设备必须采用容错技术设计，必须不低于 99.999%的可用性，全系统中断服务时间应小于 3min/年。

b) 要求设备具有高可靠性和高稳定性。设备必须采用冗余设计，主处理板、业务处理板等核心单板必须采用备份机制，当其中某块业务板故障时，不影响业务的继续提供。支持热插拔功能。

c) P/I/S-CSCF 设备的 IP 出口设备应能够支持以主备用的方式同时与分组承载网的网络设备相连接，即要求支持 IP 接口单板间的热备份机制。

d) P/I/S-CSCF 设备要支持端口级的热备份机制。

e) 在满配置情况下，故障设备自动重启动应在 30min 之内完成。

7 接口要求

7.1 物理接口

P/I/S-CSCF设备相关的媒体与信令接口、本地维护接口及与网管中心接口，应遵循以下物理接口要求。

对于10Mbit/s 以太网接口，应符合标准IEEE802.3。

对于100Mbit/s 以太网接口，应符合标准IEEE802.3u。

对于1000Mbit/s以太网接口，应符合标准IEEE802.3ab。

7.2 逻辑接口

P/I/S-CSCF设备相关的逻辑协议接口，具体规定见本部分4.2节。

8 操作维护及网管要求

8.1 MML 和 GUI

CSCF的操作维护系统应当提供MML和GUI形式的人机接口。

8.2 本地维护和远程维护

CSCF的维护系统应当提供本地维护和远程维护两种方式。

8.3 日志

CSCF的操作维护系统应当提供如下日志功能：

- a) 操作日志的管理；
- b) 导出操作日志；
- c) 主机运行和调试日志管理；
- d) 导出主机运行和调试日志。

8.4 性能统计

CSCF的操作维护系统应提供如下的性能统计管理功能：

- a) 计数器管理和全指标上报；
- b) 增加、删除可配置测量对象；
- c) 恢复和暂停测量；
- d) 设置任务的采集周期和开关；
- e) 支持多网元的性能控制管理。

8.5 故障诊断

a) 一般要求

系统应备有自动诊断功能，应能检测软件、硬件的故障，对各种故障应具有记录的功能。硬件故障的检测应具有故障定位的功能，以便维护人员及时准确的处理故障。在发生硬件故障时，应能隔离有故障的硬件或自动倒换至无故障的备用硬件，保证系统继续正常运行。在发生软件故障时，系统应具有一定的自纠能力和自动恢复功能，其中包括再启动和再装入等。

当发生软件和硬件故障时，除应能打印输出故障记录报告外，对于重要故障还应发出可闻、可见信号，并应立即向本局操作维护中心送出报告。在无人值机时，本局的输出设备可以关闭，但相应的告警信号仍可送至操作维护中心。

b) 故障的容错性

当发生软件和硬件故障时，一般不应产生系统阻断。当发生的故障将不可避免地导致降低服务质量时，系统应能继续运行。系统中的重要设备可以具有备份或“n+x”的冗余。保证在发生故障时能自动脱离并进行倒换或进行系统再配置。

系统对某一硬件故障应经重复检测后进行确定，以防止偶发性故障造成系统的再配置或导致服务质量的下降。

c) 硬件故障的定位

系统对硬件故障应具有自动诊断定位的能力。

d) 故障的恢复

当发生一般性软件和硬件故障时，系统应具有自愈能力，例如硬件发生故障时能立即倒换至无故障的电路继续正常运行，软件发生故障时能进行局部再装入等。当系统发生的全系统中断或电源中断恢复后，应能迅速地自动再启动运行。

再启动

系统应提供不同等级的人工和自动再启动功能。系统再启动应具有记录，并打印输出相关资料。当系统产生自动再启动时，应有告警提示。

再装入

系统应提供不同等级的人工和自动再装入功能。系统的再装入应有记录，并能打印输出相关资料。通过人机命令进行的不同等级的自动再装入，包括部分或全部软件、数据和参数的再装入。

e) 故障记录

系统应将所发生的各种故障进行及时记录，每月按故障种类输出故障统计表，也可以用人机命令索取前一天或前一周的故障记录。因故障而阻塞的电路数量超过预定值时也应作记录并送出警报。故障记录信息可在本局也可在操作维护中心输出。

8.6 加载

CSCF设备的所有软件可通过操作维护系统进行加载。

软件加载时应不影响正在进行的业务。

软件加载时长应当小于一定时长。

8.7 软件版本及补丁管理

CSCF的操作维护系统应提供以下功能：

- 1) 软件版本管理，如查询和校验；
- 2) 软件补丁管理，如补丁查询、校验、加载、激活。

9 定时与同步要求

P-CSCF、I-CSCF、S-CSCF等网元应具有与骨干网的网络时间同步的功能，可以通过NTPv3(IETF RFC 1305) 协议等实现同步。

10 电源及接地要求

10.1 电源要求

10.1.1 直流电源要求

10.1.1.1 额定电压

采用额定电压为-48V 的直流电源。

10.1.1.2 电压波动范围

电源设备供给设备电压波动范围，在每一个机架的直流输入端子处测量-48V 电压，允许变动范围为-57V~-40V。应当能在该电压变动范围之内正常工作。

10.1.1.3 杂音电压指标

a) 电话衡重杂音电压

整流器直流输出端电话加权衡重杂音电压应小于等于2mV。

b) 宽频杂音电话

整流器直流输出端在3.4kHz~150kHz频带内的宽频杂音电压应小于等于50mV。

整流器直流输出端在0.15MHz~30MHz频带内的宽频杂音电压应小于等于20mV。

c) 离散频率杂音电压

整流器直流输出端在3.4kHz~150kHz频带内的离散频率杂音电压应小于等于5mV。

整流器直流输出端在150kHz~200kHz频带内的离散频率杂音电压应小于等于3mV。

整流器直流输出端在200kHz~500kHz频带内的离散频率杂音电压应小于等于2mV。

整流器直流输出端在0.3MHz~30MHz频带内的离散频率杂音电压应小于等于1mV。

d) 峰-峰值杂音电压

整流器直流输出端在0~20MHz频带内的峰-峰值杂音电压应小于等于200mV。

10.1.2 交流电压要求

单相, 额定电压 220V, 波动 $\pm 15\%$, 频率 $50\text{Hz} \pm 5\%$, 线电压波形畸变率小于 5%, 应当能在该电压变动范围之内正常工作。

10.2 接地要求

10.2.1 接地方式

设备所在机房应采取各类通信设备的工作地、保护地以及建筑防雷接地共同合用一组接地体的集中接地方式, 即为联合接地方式。

10.2.2 接地要求

a) 由联合接地体的垂直接地总汇集线上所接的水平接地分汇集线引入机房, 路由器的各个机架设备的接地线就近引入水平接地分汇集线上。

b) 机架上的直流电源工作地应从接地汇集线上引入。

c) 机架设备做工作接地, 机壳和机架应作保护接地。

10.2.3 接地线截面积

接地线(指各种需接地的机架、地线等设备与水平接地分汇集线之间的连线), 其截面积应根据可能通过的最大电流负荷确定。接地线应采用良导体(铜)导线, 并且不准使用裸导线布放。

10.2.4 接地电阻值

机房的联合接地的接地电阻值要求小于 1Ω 。

11 环境要求

系统的环境要求见GB50174-2000, GB/T 2887-2000。

网关设备抗电磁干扰能力要求见GB/T 17618-1998。

设备本身产生的电磁干扰要求见GB9254-1998。

设备安装应有抗地震措施, 机架及设备需进行抗震加固, 应能达到抗里氏7级(美氏9级)地震的能力。

参 考 文 献

- [1]3GPP2 X.S0013-003-A V1.0, 全 IP 核心网多媒体域: IP 多媒体会话处理; IP 多媒体呼叫模型; 阶段 2
- [2]3GPP2 X.S0013-005-A V1.0, 全 IP 核心网多媒体域: IP 多媒体子系统 Cx 接口信令流程和消息内容
- [3]3GPP2 X.S0013-008-A V1.0, 全 IP 核心网多媒体域: IP 多媒体子系统——计费信息流程和协议
- [4]3GPP2 S.R0086-B V1.0, IMS 安全框架
- [5]IETF RFC 1305: 网络时间协议 (版本 3) 规范和执行
- [6]IETF RFC 2403: 在 ESP 和 AH 内的 HMAC-MD5-96 的使用
- [7]IETF RFC 2404: 在 ESP 和 AH 内的 HMAC-SHA-1-96 的使用
- [8]IETF RFC 2406: IP 压缩安全有效载荷
- [9]IETF RFC 3310: 使用证明与密钥协议的 HTTP 摘要证明
- [10]IETF RFC 3320: 信号压缩 (SigComp)
- [11]IETF RFC 3321: 信号压缩 (SigComp) ——扩展操作
- [12]IETF RFC 3323: 对于进程初始化协议 (SIP) 的一个私密机制
- [13]IETF RFC 3325: 对于进程初始化协议 (SIP) 在可信任网络用于尚待证实的识别私自扩展
- [14]IETF RFC 3326: 对于进程初始化协议的 (SIP) 原因报头域
- [15]IETF RFC 3329: 对于进程初始化协议 (SIP) 安全机制协定
- [16]IETF RFC 3485: 信号压缩 (SigComp) 的会话初始协议 (SIP) 和会话描述协议 (SDP) 静态字母检索表
- [17]IETF RFC 3486: 压缩会话初始协议 (SIP)
- [18]IETF RFC 3680: 会话初始协议 (SIP) 注册的事件包
- [19]IETF RFC 3761: E.164 到统一资源标识符 (URI) 动态授权发现系统 (DDDS) 应用 (ENUM)
- [20]IETF RFC 3841: 会话初始协议 (SIP) 的呼叫者优先选择
- [21]IETF RFC 3861: 即时消息和出席的地址解析
- [22]IETF RFC 3966: 电话号码的 tel URI
- [23]IETF RFC 4028: 会话发起协议 (SIP) 中的会话定时器

中华人民共和国
通信行业标准

800MHz/2GHz cdma2000 数字蜂窝移动通信网
多媒体域（MMD）系统设备技术要求
第1部分：会话控制类设备

YD/T 1972.1-2009

*

人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061

*

版权所有 不得翻印

*

本书如有印装质量问题，请与本社联系 电话：(010)67114922