ICS 33.030
M 21

YD

中华人民共和国通信行业标准

YD/T 1937-2009

移动网络中基于会话初始协议的推送业务技术要求

Technical Requirement for SIP Based Push

2009-06-15 发布　　2009-09-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本标准是移动网络中基于会话初始协议的推送业务技术要求，是参考开放移动联盟的《基于会话初始协议的推送业务标准》（OMA-SIP-Push-V1_0），以及SIP和Push技术相关标准而制定。

本标准的附录A和附录B是资料性附录。

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：华为技术有限公司、北京邮电大学

本标准主要起草人：范姝男、杨　健、陈国乔、王　雷、宋美娜、陈　辉、鄂海红

移动网络中基于会话初始协议的推送业务技术要求

1 范围

本标准规定了移动网络中基于会话初始协议的推送业务功能，体系架构、业务流程，并对安全性提出要求。

本标准适用于在移动网络中基于 SIP 来实现消息推送业务。

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。

IETF	draft-drage-sipping-service-identification 为会话初始协议业务识别的扩展 A Session Initiation Protocol (SIP) Extension for the Identification of Services
IETF	draft-ietf-sip-gruu 在会话初始协议（SIP）中获得和使用全球可路由用户代理 URI（GRUU） Obtaining and Using Globally Routable User Agent（UA）URIs（GRUU）in the Session Initiation Protocol
IETF	mmusic-file-transfer 实现文件传输的会话描述协议（SDP）发起/应答机制 A Session Description Protocol(SDP)Offer/Answer Mechanism to Enable File Transfer
IETF RFC2506	媒体特征标签注册流程 Media Feature Tag Registration Procedure
IETF RFC2616	超文本传输协议—HTTP/1.1 Hypertext Transfer Protocol -- HTTP/1.1
IETF RFC3261	SIP：会话初始协议 SIP: Session Initiation Protocol
IETF RFC3264	会话描述协议（SDP）一种提供/应答模式 An Offer/Answer Model with Session Description Protocol (SDP)
IETF RFC3325	会话初始协议的私有扩展 Private Extensions to the Session Initiation Protocol
IETF RFC3428	会话初始协议（SIP）即时消息的扩展 Session Initiation Protocol（SIP）Extension for Instant Messaging
IETF RFC3680	会话初始协议（SIP）注册的事件包 A Session Initiation Protocol（SIP）Event Package for Registrations”
IETF RFC3840	在会话初始协议（SIP）中指示用户代理能力 Indicating User Agent Capabilities in the Session Initiation Protocol（SIP）

IETF RFC3841	会话初始协议（SIP）的主叫优选方式 Caller Preferences for the Session Initiation Protocol（SIP）
IETF RFC4145	SDP 中基于 TCP 的媒体传输 TCP-Based Media Transport in Session Description Protocol（SDP）
IETF RFC4483	会话初始协议（SIP）的内容间接索引机制 A Mechanism for Content Indirection in Session Initiation Protocol（SIP） Messages
IETF RFC4566	会话描述协议（SDP） Session Description Protocol
IETF RFC4975	消息会话中继协议（MSRP） The Message Session Relay Protocol
IETF RFC4976	消息会话中继协议（MSRP）的中继扩展 Relay Extensions for the Message Session Relay Protocol (MSRP)
OMNA	OMA 命名机构 Open Mobile Naming Authority
OMA	SIP_UA_Prof 会话初始协议（SIP）用户代理档案传递框架 “A Framework for Session Initiation Protocol User Agent Profile Delivery”
OMA	Push OTA 推送业务空中接口协议 “Push Over The Air”
OMA	IMSArch IMS 能力系统的使用 “Utilization of IMS capabilities Architecture”
OMA	OMA-UAProf 用户代理档案 User Agent Profile
3GPP2 S.R0086-0	IMS 安全框架 IMS Security Framework
3GPP TS 23.228	IP 多媒体子系统 第二阶段 IP Multimedia Subsystem（MS）；Stage
3GPP TS 24.229	基于会话初始协议（SIP）和会话描述协议（SDP）的 IP 多媒体呼叫控制协议 第三阶段 Internet Protocol（IP）multimedia call control protocol based on Session Initiation Protocol（SIP）and Session Description Protocol（SDP）；Stage3
3GPP TS 26.141	IP 多媒体子系统消息和在线信息；多媒体格式和编码方式 IP Multimedia Subsystem（IMS）Messaging and Presence；Media formats and codecs
3GPP TS 33.203	基于 IP 业务的接入安全 Access Security for IP-based services
3GPP TS 33.210	网络域安全；IP 网络层安全 Network domain security；IP network layer security
3GPP2 X.S0013-002-A	全 IP 核心网络多媒体域；IP 多媒体子系统；第二阶段，修订本 A All-IP Core Network Multimedia Domain：IP Multimedia Subsystem - Stage 2
3GPP2 X.S0013-004-A	全 IP 核心网络多媒体域；基于会话初始协议（SIP）和会话描述协议（SDP）的 IP 多媒体呼叫控制协议第三阶段，修订本 A All-IP Core Network Multimedia Domain: IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3

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标准。

3.1.1

应用 Application

相关功能集合来完成有用工作，通常能实现一个或多个业务。它可以由软件和/或硬件元素构成。

3.1.2

应用级别寻址 Application-Level Addressing

在客户端上的特定用户代理和 Push 发起者间处理传递 Push 内容的能力。

3.1.3

Push 内容 Push Content

内容、元数据和应用层控制信息在Push发送者和Push代理之间有共同的释义。

3.1.4

Push 接收代理 Push Receiver Agent

Push 接收代理是一个使用 SIP Push 流程接收 Push 内容并对 Push 发送代理的请求，产生一个响应的逻辑实体。

3.1.5

Push 发送代理 Push Sender Agent

Push 发送代理是一个产生 Push 请求，应用 SIP Push 流程发送 Push 内容的逻辑实体。

3.1.6

客户端 Client

在 Push 上下文中，一个客户端是期望从服务器接收 Push 内容的一个设备（或业务）。在 Pull 上下文中，客户端是向服务器发起内容和数据请求的设备。

3.1.7

媒体类型 Media Type

一类由其表示形式和/或交换格式区分的信息。例如图片、纯文本、声音和视频。

3.1.8

设备 Device

设备是网络实体，它有发送或接收信息包的功能并且有单一的设备地址。一个设备既可以是用户也可以是服务器，在给定上下文或跨多个上下文中工作。例如，一个设备可以像服务器一样对一定数量的用户提供服务，同时也是另一个服务器的用户端。

3.1.9

推送 Push

由服务器发起内容传递到用户的一种传输方法。

3.1.10

Push 接入协议 Push Access Protocol

用于在 Push 发起者和 Push 网关间，向客户端推送传输内容和 Push 相关的控制信息的协议。

3.1.11

Push 框架

是整个 Push 系统。Push 框架包含协议、服务接口和提供推送数据到客户端用户代理方法的软件实体。

3.1.12

Push 发起者　Push Initiator

产生 Push 内容和提交到 Push 框架来传输到客户端用户代理的实体。

3.1.13

Push OTA 协议　Push Over Air Protocol

用于在Push代理网关和特定客户端用户代理间传输内容的协议。

3.1.14

Push 代理网关　Push Proxy Gateway

提供 Push 代理服务的代理网关。

3.1.15

Push 会话　Push Session

在 Push 发送和接收代理间共享的联合状态。

3.1.16

服务器　Server

在请求响应中为用户提供资源的实体。

3.1.17

会话标识　Session Identity

识别 Push 会话以及用于路由初始 SIP 请求的 SIP URI。

3.1.18

用户代理　User Agent

作为用户代表行为的软件或设备，与其他实体交互和处理资源。

3.1.19

用户面　User Plane

用户面包括在 Push 发送代理和 Push 接收代理间的媒体（MSRP）和媒体控制信令。

3.1.20

注册　Register

终端通过网络在服务器上进行登记。

3.1.21

去注册　de-register

通过网络在服务器上进行取消登记。

3.2　缩略语

下列缩略语适用于本标准。

AoR	Address of Record	登记的地址
HTTP	Hypertext Transfer Protocol	超文本传输协议

IANA	Internet Assigned Numbers Authority	互联网地址指派机构
IMS	Internet Multimedia System	IP 多媒体子系统
IP	Inetent Protocol	网际协议
MIME	Multipurpose Internet Mail Extensions	多用途网际邮件扩展
MM	Multimedia Message	多媒体消息
MMS	Multimedia Message Servie	多媒体消息业务
MMD	Multimedia Domain	多媒体域
MSISDN	Mobile Station International Subscriber Directory Number	移动台国际用户目录号
OTA	Over The Air	空中下载
OTA-HTTP	OTA over HTTP	基于 HTTP 的空中下载
OTA-SIP	OTA over Session Initiated Protocol	基于 SIP 的空中下载
OTA-WSP	OTA over Wireless Session Protocol	基于 WSP 的空中下载
PI	Push Initiator	Push 发起者
PPG	Push Proxy Gateway	Push 代理服务器网关
SDP	Session Description Protocol	会话描述协议
SIP	SIP Initiated Protocol	会话初始协议
SMS	Short Message Service	短消息服务
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
URI	Uniform Resource Indentifier	统一资源标识符
URL	Uniform Resource Locator	统一资源定位符
WSP	Wireless Session Protocol	无线会话协议

4 业务介绍

本标准定义了移动网络中基于 SIP 实现推送业务的协议，允许客户端接收服务器发起通信的内容，或 SIP/IP 核心网推送的内容。SIP Push 业务通过将 Push OTA 内容封装在 SIP 消息当中，利用现有的 SIP/IP 核心网络进行传送。SIP Push 与传统的 Push OTA 最大的区别在于 PPG 和 Client 之间的承载采用 SIP 技术实现；采用 SIP Push 技术实现 Push 的优势在于其维护的成本较小，有较高的互操作性，对现有资源可重用，并保证通信安全等优点。SIP Push 业务示意如图 1 所示。

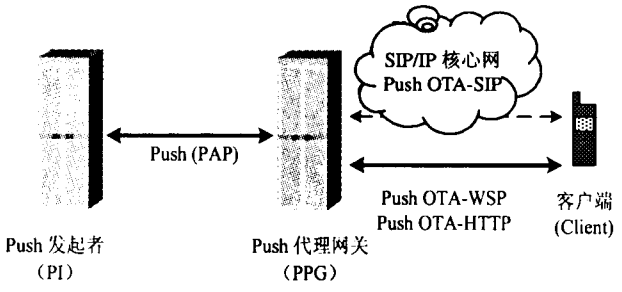

图 1 SIP Push 业务示意

5 SIP Push 业务应用场景

5.1 应用场景概述

本章节内容作为资料性介绍。

SIP PUSH 业务与 OTA PUSH 业务之间最大的差别主要是信息传送的承载方式不同，因此也造成业务流程方面的不同。除此之外，本标准规定在 SIP Push 的使用过程中，应给用户带来与 OTA Push 相同的用户体验。

SIP Push 可以用于 MMS 通知、Email 通知、Client Provisioning、DM 通知及传统推送业务。

5.2 MMS 通知

两个开通了 MMS 的用户，可以互相发送接收 MM。发送方可以激活其 MMS 客户端，输入接收方用户的地址，并编写或编辑将要发送的多媒体消息 MM。发送方客户端将消息发送到与之相关联的 MMS 网关中继服务器并返回传递报告，此多媒体消息将存储在接收方相关联的 MMS 服务器。

当 MM 在下发到用户之前，通常需要下发一个 MMS Notification 来通知用户，以确认用户是否对 MM 进行下载和接收，这一功能将可以通过 SIP Push 来完成的。

5.3 Email 通知

开通了 Email Notification 业务的用户，服务器在有新邮件到来时，将新邮件存储在接收方相关联的服务器上。

当 Email 在下发到用户之前，通常需要下发一个 Email Notification 来通知用户，以确认用户是否对 Email 进行下载和接收，这一功能将可以通过 SIP Push 来完成的。

5.4 Client Provisioning

Client Provisioning 是通过 OTA Push 通道自动配置用户终端一系列参数服务的业务。

用户从服务提供商订制新的业务的方法有很多，可以使用浏览器来激活业务，可以通过客户服务热线或者在零售商处进行开通。用户也可以通过发送短信请求参数配置，然后通过 OTA Push 发送一条短信到用户终端，用户根据提示选择更新，终端上的参数随之自动修改。

以用户需要订制的是一个现有的服务提供商提供的在线游戏服务为例。订制的方法是通过浏览器激活，即用户向服务提供商订制在线游戏服务，服务提供商接受了用户的请求，并请求 DM 服务器对在线游戏服务进行配置，DM 服务器担负 PI 的角色，采用 PAP 发送一个初始 DM 消息（Client Provisioning 消息）到 PPG。采用 Push OTA-SIP，PPG 经由 SIP/IP 核心网络将 DM 消息转发到终端。终端应用程序将所需要的服务设置都进行了正确有效的配置，最终，用户可以接入网络进行在线游戏。

5.5 DM 通知

DM 是一种通过 OTA Push 方式将管理指令从服务器下载到终端设备上，并由终端设备自动运行，进而完成终端软硬件升级、参数配置、诊断等的低成本远程管理解决方案，同时 DM 还可以将运营商需要的业务信息和终端设备的功能信息等从终端设备传递到服务器，以支持其他业务的开展。

在线服务之类的许多服务，在进行初始化的配置（Client Provisioning）过程之后还需要对后续服务过程中业务的设置进行管理，其中包括修改、更新等操作，整个设置信息的管理工作是通过 DM 服务器完成的。

在 DM 服务器需要对配置信息进行修改的时候，需要先将修改信息通知用户，并在用户确认的情况下进行修改，整个过程是 DM 服务器向 PPG 发送 DM 修改指令，通过 Push OTA-SIP 发送相关的 Notification

完成的。终端在收到 Notification 后，初始化设备管理会话，呈现或拒绝服务器配置修改选项。如果接受配置改变，用户的配置信息将会被更新并且被激活。

5.6 传统推送业务

5.6.1 无接收信息确认的推送业务

一些重要程度和价值较低的内容，如果希望通过Push的方式传送给用户，可采用无接收信息确认推送的形式与方法，其中比较广泛的一个应用就是广告内容的推送。出于对设备和网络条件的考虑，参与这类Push业务的用户在很多方面都存在一定的限制，也就意味着Push信道应该是单向的并且带宽有限，此外Push内容的对信道的消耗也应限制。所以，通知的接收者将不需要对消息的传递返回确认。PPG在接收到PI发来的PAP消息后，可以采用Push OTA-SIP方式传递不需要确认的Push内容。

5.6.2 需要接收信息确认的推送业务

对于一些比较重要，或有较高价值的内容需要通过 Push 的方式发送给用户。根据 Push 内容的特点，要求 Push 代理与移动设备之间需要建立公共的通信环境，并且 Push 内容的成功传送需要确认，且相应的通知需要返回给消息的发起者。这样，PPG 接收到 PAP 消息后，使用 Push OTA-SIP 方式向客户端转发特定内容，并明确要求传递确认消息。

6 安全需求

在安全方面，SIP Push 可依靠底层的安全机制，Push 代理处理 Push 消息时，应确保用户和消息发起者均经过授权和认证等安全设置相匹配过程后进行业务。同时，SIP Push 安全应符合 Push 提出的安全要求。

7 SIP Push 的系统要求

7.1 SIP Push 系统架构

如图 2 所示，为基于 SIP Push 业务的框架模型，其实体包括 Push 发送代理和 Push 接收代理。

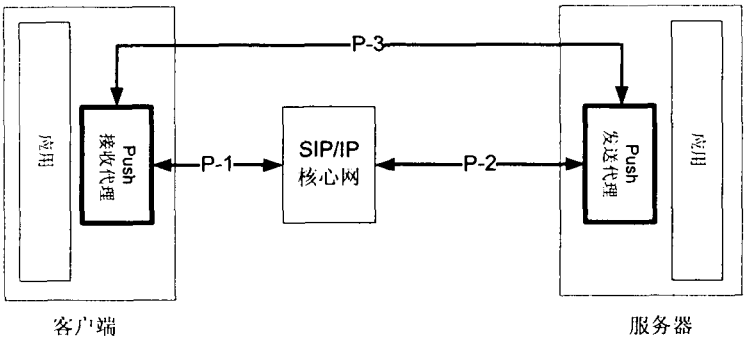

图 2 SIP Push 框架模型

SIP Push 网络实体通过 SIP/IP 核心网，使用 SIP 方式从 Push 发送代理传递 Push 内容到 Push 接收代理。SIP Push 协议使用 SIP 作为底层传输机制，能提供类似 Push OTA （见 OMA PushOTA）的功能。

Push 发送和接收代理是与 SIP/IP 核心网交互，完成基于 SIP Push 业务的逻辑实体。当 Push 消息使用 SIP Push 作为传递方式时,Push 代理网关 (PPG)作为 Push 发送代理发送 SIP Push 内容，客户端作为 Push 接收代理接收 SIP Push 内容。

7.2 SIP Push 网元要求

7.2.1 Push 发送代理

Push 发送代理是支持各种 SIP Push 特征的逻辑实体。Push 发送代理创建 Push 请求并使用 SIP Push 流程发送请求。Push 发送代理可以接收这些 Push 请求的响应并对响应进行处理。

发送的消息可由内容的订阅触发，也将依据从 UAProf 服务器取回的 Push 接收代理的能力判断、触发消息的发送。

Push 发送代理是一个推送内容到 Push 接收代理的实体。Push 发送代理支持接收注册功能，并支持接收、存储和共享 Push 接收代理能力信息，Push 发送代理依据此功能进行能力匹配以及供应用处理。Push 发送代理根据预设的处理方式，对 Push 消息进行处理。Push 发送代理创建 Push 请求，向 Push 接收代理传递内容，Push 发送代理接收重定向请求，并根据该请求发送 Push 消息。Push 发送代理选择发送 Push 消息的方法，依据 Push 接收代理支持的能力和应用，并向 Push 接收代理请求传递报告。Push 发送代理发送取消 Push 消息请求，该请求中携带此 Push 消息标识信息，Push 接收代理取消该 Push 消息。在多终端情况，即用户在 Push 发送代理上有多个注册的终端，Push 发送代理通过使用 GRUU 值来选择正确的终端发送消息。

Push 发送代理应支持 P-2 参考点。

7.2.2 Push 接收代理

Push 接收代理是支持各种 SIP Push 特征的逻辑实体。Push 接收代理接收 Push 内容，并可对 Push 发送代理的请求产生响应。

Push 接收代理是一个从 Push 发送代理接收 Push 内容的逻辑实体。Push 接收代理负责传递接收的 Push 内容并传递到适当的应用。Push 接收代理支持在 SIP/IP 核心网上注册，并发布 Push 接收代理 Push 能力信息，发送可用的 Push 资源列表。Push 接收代理接收 Push 请求消息或 Push 内容，支持发送“3xx”消息，并给出预设的地址信息，用于发送该 Push 请求或 Push 内容。Push 接收代理按 Push 发送代理要求，取消已接收消息，并可返回成功取消的响应，具体参见 IETF RFC3261。成功接收到 Push 消息后，Push 接收代理向应用层映射 SIP Push 传递状态（如 SIP 响应码），为 Push 发起者传达状态信息，并对 Push 发送代理的请求产生响应。

Push 接收代理应支持 P-1 参考点。

7.2.3 支持 SIP Push 业务的 SIP/IP 核心网要求

SIP/IP 核心网是一个由服务器组成的网络，例如用来完成一系列业务的代理或注册服务器等。

SIP Push 协议要求 SIP/IP 核心网至少支持接入层安全、基于应用和用户业务档案的 Push 发送和接收代理的鉴权和授权、SIP 信令的隐私保护、SIP 注册和路由功能。

SIP Push Enabler 框架中的 SIP/IP 核心网不局限于 3GPP IMS 和 3GPP2 MMD 网络，也对其他的 SIP/IP 核心网开放。在 IMS（见 OMA IMSArch 的上下文中，SIP Push 协议应遵循 3GPP TS 23.228 和 3GPP2 X.S0013-002-A 规范中定义的 3GPP IMS 和 3GPP2 MMD 功能。任何能够支持前面提出功能的其他 SIP/IP 核心网也可选择使用。

对于不支持 GRUU 的 SIP/IP 核心网的核心网，不在本标准范围内考虑。

在 IMS (3GPP IMS 和 3GPP2 MMD 网络) 的上下文中，使用本标准中定义的 SIP Push 应考虑作为基于 Push 业务的主要机制。

7.3 SIP Push 系统接口要求

7.3.1 P-1 接口：Push 接收代理-SIP/IP 核心网

P-1 参考点，如图 2 中描述，支持 Push 接收代理和 SIP/IP 核心网间的通信。SIP 协议是 P-1 参考点的协议。

P-1 参考点提供 Push 接收代理注册功能，使得 SIP/IP 核心网获知其支持的 Push 资源信息。在 Push 接收代理和 Push 发送代理间传递 Push 会话信令。对于传递消息时，应提供查询和地址解析功能，并对 Push 接收代理进行鉴权和授权，完成与 Push 发送代理的能力和资源的协商。

7.3.2 P-2 接口：Push 发送代理-SIP/IP 核心网

P-2 参考点支持 Push 发送代理和 SIP/IP 核心网间的通信，SIP 协议为 P-2 参考点的协议。

P-2 参考点提供 Push 接收代理注册功能，并发送表示 Push 事件的 Push 内容。接收 Push 接收代理的 Push 能力和注册信息，并在 Push 接收代理和 Push 发送代理之间传递 Push 会话信令。对于传递消息时，提供查询和地址解析功能，并对 Push 接收代理进行鉴权和授权。

当 SIP/IP 核心网相应于 3GPP/3GPP2 IMS 时，P-2 参考点需满足 3GPP TS 23.228 和 3GPP2 X.S0013-002-A 规范中定义的 ISC 参考点要求。

7.3.3 P-3 接口：Push 发送代理-Push 接收代理

P-3 参考点支持直接的 Push 发送代理和 Push 接收代理之间的通信。P-3 参考点的协议见 IETF RFC4975 规范。

P-3 参考点可以提供对任何非流式媒体的直接推送，对消息大小没有限制。其为客户端同时提供多个 Push 连接，并异步传递代表 Push 事件的消息或内容。

8 SIP PUSH 业务流程

8.1 SIP Push 的注册过程

8.1.1 注册概述

SIP/IP 核心网使用 SIP REGISTER 请求来完成注册过程，SIP REGISTER 允许用户通知 SIP/IP 核心网对特定业务的支持。SIP/IP 核心网也能使用注册流程完成用户接入网络前的鉴权和授权。

Push 接收代理完成在 SIP/IP 核心网的注册，为了让 Push 发送代理获知 Push 接收代理发送的 SIP REGISTER 请求，SIP/IP 核心网能基于 Push 接收代理发送的 SIP REGISTER 消息，通过第三方注册通知 Push 发送代理，此第三方注册请求能够基于为 SIP REGISTER 请求设置的过滤标准来触发，指示支持 SIP Push 业务，具体见 IETF RFC3261 规范。Push 发送代理可以订阅“reg”事件包，发送能力查询请求，具体见 IETF RFC3680 规范。

8.1.2 Push 接收代理注册流程

Push 接收代理应完成在 SIP/IP 核心网上注册、重新注册和去注册流程，具体见 IETF RFC3261 规则和流程及以下部分说明。注册流程示例如图 3 所示。

Push 接收代理应产生 SIP REGISTER 请求，并应在 Contact 头域中包含“Push Resource Identifier”作为特征标签“+g.oma.pusheventappp”，其值为所支持的 Push 资源 URI。Push 接收代理在 SIP REGISTER 请求中包含用户设置的控制策略，应在 SIP REGISTER 请求包含 Require 头域并携带一个可选“pref”标签，具体见 IETF RFC3840 规则和流程。

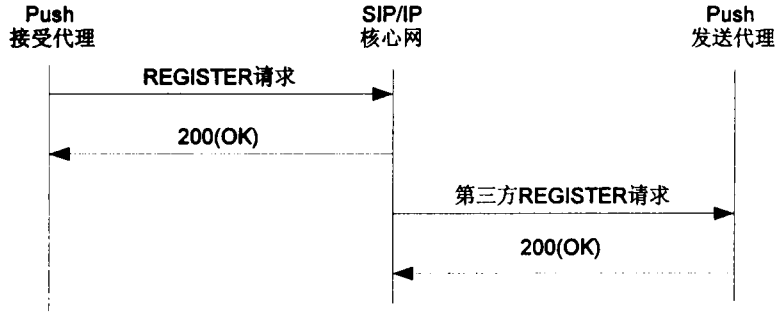

图 3 注册流程举例

Push 接收代理依靠全球可路由用户代理 URIs（GRUU），Push 接收代理应在注册过程中请求 GRUU 值，如果支持多终端情况下的能力传递和资源协商。如果不支持多终端情况下的能力传递和资源协商，可在注册过程中请求 GRUU 值。应在 Contact 头域参数中使用“+sip.instance ”参数，具体见 IETF draft-ietf-sip-gruu 规范。基于成功的注册后，SIP/IP 核心网返回 GRUU 值（临时或永久 GRUU 值）。这些 GRUU 值可以由 Push 接收代理在没有 SIP REGISTER 请求时使用。在 Supported 头域中应给出值为“gruu”，应向 SIP/IP 核心网发送 SIP REGISTER 请求。

当接收到的 SIP 200 OK 响应，并且 Contact 头域包含“pub-gruu”和“temp-gruu”值时，Push 接收代理应取回并存储“pub-gruu”和“temp-gruu”值。

在 IMS 网络情况下，当 SIP/IP 核心网接收到 Push 接收代理发送的注册请求并确认后，将应使用过滤标准产生一个第三方注册请求，发送给 Push 发送代理，此 Push 发送代理即为 iFC 配置中指定的应用服务器，见 3GPP TS 23.228 和 3GPP2 X.S0013-002-A 规范规则和流程。

当 Push 接收代理需要对某个 Push 资源进行去注册（de-register），但仍保留在 SIP/IP 核心网注册的情况下，Push 接收代理应根据 IETF RFC3261 产生一个 SIP REGSITER 请求，并在 Contact 头域中给出 Push 资源标识符特征标签“+g.oma.pusheventapp”，其值给出所有保留注册的 Push 资源标识。如果不需要保留任何 Push 资源，则在 Contact 头域不包含 Push 资源标识符特征标签“+g.oma.pusheventapp”。

Push 接收代理重新注册或去注册时，应产生一个 SIP REGISTER 请求。如果 Push 接收代理需要保留已在 SIP/IP 核心网注册，Push 接收代理在 SIP/IP 核心网上重注册时，不应携带每个 SIP Push 特性标签。如果客户端同时需要从 SIP/IP 核心网去注册，Push 接收代理应发送一个 SIP REGISTER 请求，将其 Expire 头域设为 0。

8.2 SIP Push 能力传递和资源协商

Push 接收代理可提供 SIP Push 的能力信息，例如可接收的内容类型。在 SIP Push 环境下，Push 接收代理请求 Push 发送代理支持的 Push 资源能力信息，并传递其设备参数给 Push 发送代理。这实现了当有新的 Push 接收代理可用和请求 Push 资源时，通知 Push 发送代理的功能。当 Push 发送代理不存在 Push 接收代理能力信息时，应向 Push 接收代理发送能力查询请求，Push 发送代理接收 Push 接收代理返回的能力信息或 UAProf。当 Push 接收代理能力发生变化时，宜通知 Push 发送代理，Push 发送代理应根据变更后能力信息进行更新。Push 发送代理可在 UAProf 服务器上取回此索引相关的能力，并应根据该能力信息进行终端能力管理，如图 4 所示。

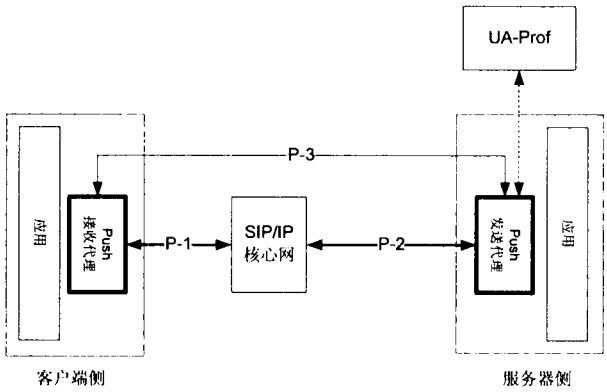

图 4　与 UAProf Enabler 的交互

Push 发送代理和 UAProf 服务器间的接口不在 SIP Push 标准范围内考虑。

在 SIP/IP 核心网注册后，Push 接收代理用 SIP OPTIONS 请求 Push 发送代理支持的 Push 资源。Push 发送代理接收到该能力信息请求，表示 Push 接收代理为可用状态，并同时请求 Push 发送代理支持的资源。能力传递和协商的流程示例如图 5 所示。

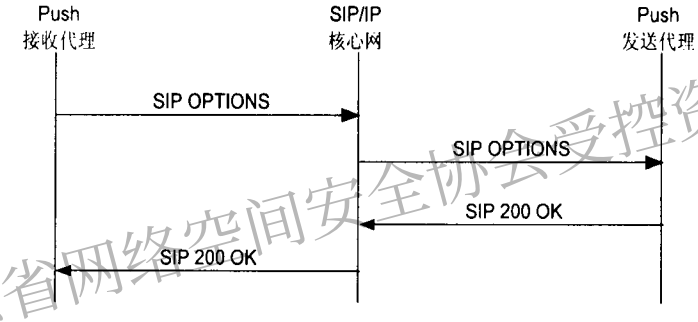

图 5　通过 SIP OPTIONS 的能力传递和资源协商流程举例

在 SIP/IP 核心网完成 SIP 注册，或如果支持的 Push 资源发生变化的情况下，已经注册的 Push 接收代理应遵循 IETF RFC3261 生成 SIP OPTIONS 请求，并应设置此 SIP OPTIONS 请求的 Request-URI 头域为 Push 发送代理的 URI 值。遵循 IETF RFC3325 规则和流程，在 OPTIONS 消息的 P-Preferred-Identity 头域可添加 Push 接收代理的 URI 值。如果 Push 接收代理在注册过程中，获得公共 GRUU，应根据 IETF draft-ietf-sip-gruu 规则和流程在 Contact 头域添加“GRUU”值。

在 Contact 头域中还应包含 Push 接收代理支持的 Push 资源标识特征标签，在值域部分给出所有 Push 资源相关的 URI 格式。在 Accept-Contact 头域中应包含 Push 资源标识符特征标签，在其值域给出所有 Push 发送代理应支持的 Push 资源。如果 Push 接收代理在注册过程中获得了公共 GRUU，那么此 OPTIONS 消息中应包含 Supported 头域，值域为“gruu”。在 Allow 头域应给出 Push 接收代理支持的 SIP 方法。建议包含 User-Agent 头域，根据 IETF RFC3261 规定在其值域给出 Push 接收代理的型号，生产厂商和版本信息。如果 Push 接收代理支持 User Agent Profile，在 Content-Type 头域中应包含 message/external-body 的 MIME 类型，ACCESS_TYPE 参数中给定一个“URL”，根据 IETF RFC4483 给出超时参数，在 URL 参数中包含 OMA-URProf 文档 HTTP URL 参数。如果 Push 接收代理支持 User Agent Profile，根据 IETF RFC4483 规则和流程消息体在 Content-type 中应包含“application/rdf+xml”，Content-Disposition 和 Content-ID 中应包含“attachment”。Push 接收代理将此 OPTIONS 消息发送到 SIP/IP 核心网。

Push 发送代理接收到该 OPTIONS 请求后，应验证是否出现 P-Asserted-Identity 头域，如果出现，验

证该 P-Asserted-Identity 的 URI 是否可信。如果授权验证失败，Push 发送代理应根据 IETF RFC3261 返回 SIP 403“Forbidden”响应。如果 Content-Type 头域定义为“message/external-body”，并且为 Content-Type Dev-Cap，如果没有缓存 OMA-UAProf 文档，则应通过 HTTP URI 取回文档。如果在 SIP OPTIONS 的 Contact 头域给出了“GRUU”，应存储该 Push 接收代理的 GRUU，并在所有发给此 Push 接收代理的 SIP 请求消息时，在 Request-URI 头域应添加此 GRUU 值。

Push 发送代理应遵循 IETF RFC3261 产生 200 OK 响应，在 Push 资源标识符特征标签中应给出支持的 Push 资源值，这个值应从 OPTIONS 请求中 Contact 头域中，Push 接收代理支持的 Push 资源标识符特征标签指示的 Push 资源值列表中选出。建议包含一个 Accept 头域，根据 IETF RFC3261 包含 Push 发送代理支持的 MIME 类型，包括“message/external-body”和“application/rdf+xml”，其他任何 Push 发送代理支持的 MIME 类型作为其提供的业务部分。Push 发送代理查询支持的相应方法，应在 Allow 头域中包含 Push 发送代理支持的相应 SIP 方法，并应发送此 200 OK 响应到 SIP/IP 核心网发送给终端。

Push 接收代理接收到返回的 200 OK 消息后，应根据 IETF RFC3841 规则和流程存储在 Accept-Contact 头域给出的 Push 发送代理的 Push 能力信息，以及在 Allow 头域给出的 Push 发送代理支持的 SIP 方法。

8.3 SIP MESSAGE 消息流程

SIP MESSAGE 方法是 SIP 的扩展，继承了所有 SIP 协议的请求路由和安全特点，允许消息传输到客户端。SIP MESSAGE 请求可以 MIME 主体部分形式携带内容，或可遵循 IETF RFC4483 直接索引内容。SIP MESSAGE 请求本身不发起 SIP 对话，在正常使用时每个 SIP MESSAGE 是独立的，在系统中不存储会话状态。Push 消息在 SIP MESSAGE 体中携带，遵循 IETF RFC3428 中定义其不应超过 1300 字节。SIP MESSAGE 消息流程示例如图 6 所示。

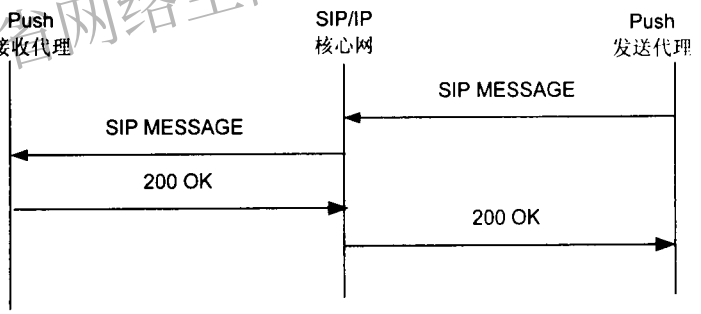

图 6 SIP MESSAGE 消息流程举例

Push 接收代理为 SIP Push 提供支持 SIP MESSAGE 方法的使用。Push 发送代理应产生一个 SIP MESSAGE 请求，遵循 IETF RFC3428 和 IETF RFC3841 规范规定。

Push 发送代理向 Push 接收代理发送消息，Push 发送代理在 Accept-Contact 头域中应包含一个 Push 资源标识符特征标签的名称和值，应检验目标接收代理是否设置重定向的公共 URI 标识或 GRUU 标识，如果该请求消息是发向所有 Push 接收代理时，应设置 SIP MESSAGE 请求的 Request-URI 为目标接收者的公共用户标识，或当该请求发送给目标接收者的特定终端时，应设置改 Request-URI 为指示特定终端的 GRUU 标识。Push 发送代理检查发送的内容，与用户能力指示的 Push 接收代理支持的内容类型，以及用户通过 Push 接收代理设置的 Push 消息安全设置进行比较。

如果内容包含在 Push 消息中，Push 发送代理应将 Push 内容封装在 SIP MESSAGE 请求的消息体中。如果使用内容间接索引方法，Push 发送代理应在 SIP MESSAGE 请求中间接索引内容部分，遵循 IETF

RFC4483 规定。

Push 发送代理应遵循 3GPP TS 24.229 和 IEFT RFC3325 规定，当消息发起者是 Push 发送代理可信任时，在 SIP MESSAGE 请求头域中应包含一个 P-Asserted-Identity。

用户在 Push 发送代理上有多个注册终端情况下，Push 发送代理应采用一种包含 GRUU 值的传递模型，用于判断发送消息的正确终端，具体流程见 IETF draft-ietf-sip-gruu。Push 接收代理的 GRUU 值可以通过 Push 接收代理发送的 SIP REGISTER 消息获得，或通过 Push 发送代理从 SIP/IP 核心网订阅注册事件包。

Push 发送代理应遵循 SIP/IP 核心网流程，向 SIP/IP 核心网发送 SIP MESSAGE 请求，SIP/IP 核心网转发 SIP MESSAGE 请求到 Push 接收代理。

Push 接收代理接收到该 SIP MESSAGE 消息，应能在响应中返回“3xx”响应码，并给出目标接收代理的公共 URI 标识或 GRUU 标识，遵循 IETF RFC 3261 规则和流程，以便 Push 发送代理根据此信息发送 SIP MESSAGE 消息。Push 接收代理检查 SIP MESSAGE 消息中携带的目的地址是否与当前 Push 接收代理的地址一致，以便能使应用正确进行 SIP MESSAGE 消息的处理。如果不一致则返回错误响应。应检查在 Accept-Contact 头域是否出现 Push 资源标识符，如果 Push 资源标识符特征标签没有出现或值域不可识别，Push 接收代理应返回 403“Forbidden”响应，应验证含有 P-Asserted-Identity 头域，并验证其给出的 URI 为可信任的。如果验证检查失败，Push 接收代理应返回 403“Forbidden”响应。如果 Push 内容在 SIP MESSAGE 请求的消息体中，Push 接收代理应传递已接收的 Push 内容到目标 Push 应用来执行；如果内容在 SIP MESSAGE 请求中是间接索引的，遵循 IETF RFC4483，Push 接收代理应在指定的位置取回 Push 内容，并传递内容到目标的 Push 应用。如果 Push 发送代理发送取消 SIP MESSAGE 消息请求，该请求中应携带 SIP MESSAGE 消息标识，Push 接收代理取消该 SIP MESSAGE 消息。Push 接收代理应遵循 IETF RFC3428 和 SIP/IP 核心网流程产生一个成功的响应。

Push 发送代理应识别成功的响应，遵循 IETF RFC342 和 SIP/IP 核心网流程。

8.4 SIP INVITE 和 MSRP 流程

当 Push 发送代理将发送一个较大的内容而不采用内容索引的方法时，Push 发送代理应发起一个 MSRP 会话。MSRP 会话建立后并且一旦消息传递完毕，Push 发送代理将自动关闭 MSRP 会话。推送 MSRP 消息流程示例如图 7 所示。

8.4.1 Push 接收代理要求

Push 接收代理为 SIP Push 支持 SIP INVITE 和 MSRP 方式的使用。

8.4.2 MSRP 会话建立——Push 发送代理和接收代理流程要求

当需要建立一个 MSRP 会话时，Push 发送代理应产生一个初始 SIP INVITE 请求，遵循 IETF RFC3261 规则和流程。如果 Push 接收代理发送重定向请求，根据其信息，将 SIP INVITE 请求的 Request-URI 应设置为目标 Push 接收代理的 URI 标识或 GRUU 标识，遵循 IETF RFC3261 规则和流程。如果该请求发送给目标用户的所有接收代理，Request-URI 应设置为目标用户的公共标识，如果发送给目标用户的特定终端，则应使用 GRUU 标识。SIP INVITE 请求的 Accept Contact 头域应包含一个 Push 资源标识符特征标签名称和值。在该 INVITE 消息中的 P-Asserted-Identity 头域可插入 Push 发送代理的 URI，应遵循 IETF RFC3325 规则和流程的定义。推荐包含一个 Allow 头域并携带所有支持的 SIP 方法。

当提供 SDP 时，SIP INVITE 请求中包含一个 MIME SDP 体，遵循 IETF RFC3264，IETF RFC4566

和 IETF RFC4975 流程，并应设置 SDP 方向的媒体属性为“a=sendonly”，并可在 SDP 设置中添加媒体属性。遵循 mmusic-file-transfer 规范给出的定义。当传送多个文档时，应遵循 IETF RFC4566 规范给出的定义，添加多个“m=”行。建议包含“a=setup”属性，并将值域设置为“passive”，应遵循 IETF RFC4145 规则和流程的定义。

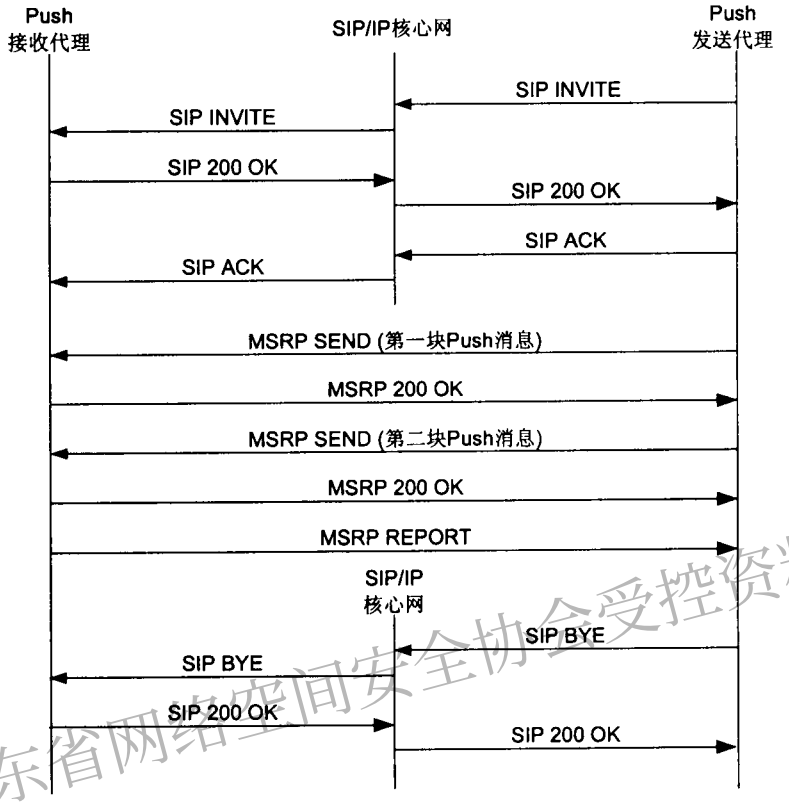

图 7　推送 MSRP 消息举例

用户在 Push 发送代理上有多个注册的终端情况下，Push 发送代理应采用一种包含 GRUU 值的传递模型，用于判断发送消息的正确终端，具体流程见 IETF draft-ietf-sip-gruu；应向 Push 接收代理发送 SIP INVITE 请求，遵循 SIP/IP 核心网规则和流程。

当 Push 接收代理接收到建立一个 MSRP 会话的 SIP INVITE 请求时，Push 接收代理应检查 SIP INVITE 的地址与当前接收代理地址的一致性，非一致的 SIP INVITE 消息进行丢弃，并返回失败响应；应检查 Push 接收代理是否支持 SIP INVITE 请求中 SDP “m=” 行的 Accept 类型属性，如果不支持，拒绝请求并返回“SIP 488 Not Acceptable Here”响应。响应可包含一个 SDP 体，在 SDP 体中有包括 Push 接收代理所支持 Accept 类型属性列表，遵循 IETF RFC3261 和 IETF RFC4975 规范中描述。可通过查找一个适当的拒绝码来拒绝 SIP INVITE 请求，例如 Push 接收代理确定没有足够的资源处理 MSRP 会话。应存储 Contact 头域的内容作为会话标识，参见 IETF RFC4975 规范中描述；应检查 Accept-Contact 头域是否出现 Push 资源标识符，如果 Push 资源标识符特征标签没有出现或值不可识别，Push 接收代理应返回 403“Forbidden”响应；应验证 P-Asserted-Identity 头域出现并且其 URI 为可信任的。如果授权检查失败，Push 接收代理应返回 403“Forbidden”响应。

当 Push 接收代理接收到一个 SIP INVITE 请求，并且包含根据 mmusic-file-transfer 指定的“file-selector”参数，Push 接收代理应只接受 Push 发送代理传递的相关的其要求接受的列表文档。

应在 SIP 200"OK"响应中包含 SDP 体作为 SDP 回应，遵循 IETF RFC3264，IETF RFC4975 和 IETF RFC4566，并应设置指示 SDP 方向的媒体属性为"a=recvonly"。可指示其要求接收的最大消息长度，采用最大消息长度行属性遵循 IETF RFC4975 规则和流程；应包含"a=setup"属性，并遵循 IETF RFC4145 规则和流程设置值为"active"。向 Push 发送代理发送此 200"OK"响应，并应准备接受 MSRP SEND 请求，遵循 IETF RFC4975 规则和流程。

8.4.3 MSRP 会话取消及释放——Push 发送代理和 Push 接收代理流程要求

Push 发送代理未接收到最终 SIP INVITE 请求的 SIP 响应，并且 Push 发送代理取消 SIP 会话发起，Push 发送代理应遵循 IETF RFC3261 规则和流程发送 SIP CANCEL 消息。

当最后 MSRP 会话被释放时，Push 发送代理应产生一个 SIP BYE 请求，遵循 IETF RFC3261 的规则和流程；应发送 SIP BYE 请求，遵循 SIP/IP 核心网规则和流程。

当接收到 SIP BYE 请求的 SIP 200 "OK" 响应后，Push 发送代理应根据 SIP/IP 核心网规则和流程发送此 200 "OK" 响应，并应释放相应的与 Push 接收代理的 SIP 会话的用户面资源。

8.4.4 MSRP 中继

Push 接收代理可以为 MSRP 会话支持中继的使用，遵循 IETF RFC4976 规范要求。

8.4.5 用户面

终端间的 MSRP 会话的媒体参数和媒体格式以 Offer 和 Answer 的模式协商，使用会话描述协议。这些协商参数由 SIP 信令携带。一些推荐媒体参数将在实时通信中使用，具体参见 IETF RFC3264 和 IETF RFC3261 规范中给出的定义。

8.4.5.1 MSRP 媒体会话-Push 发送代理和接收代理流程要求

Push 接收代理和 Push 发送代理应遵循 IETF RFC4975 和 mmusic-file-transfer 的规则和流程，并且 Push 接收代理应遵循 IETF RFC4566 解析出 Push 发送代理发送的 SIP INVITE 请求的 SDP 体，向 SDP connection"c="行给出的 IP 地址以及 SDP 媒体"m="行给出的 TCP 端口号，建立用于 MSRP 会话的 TCP 连接。

9 业务和应用的寻址

9.1 概述

之前规范中所描述的实体，将与其他 Enabler 所使用或单独使用，来构建基于 SIP Push 的业务和在这些 Enabler 上运行的应用。在 SIP PushEnabler 上运行的应用可以为其他 Enabler，例如 MMS。

SIP Push 制定了 Push 资源标识符的使用，Push 资源标识符应用来指示执行此 Push 消息的 Enabler 的资源，例如由 Enabler 指定的应用。资源可使用 SIP Push 作为内容或通知的传输机制。

SIP Push 的一般模型如图 8 所示。

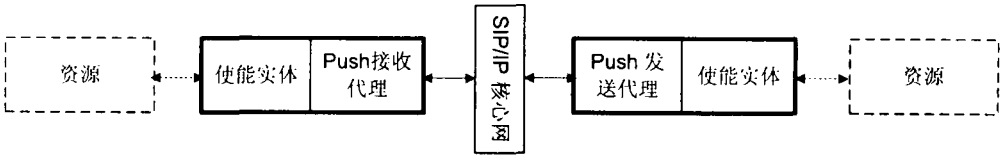

图 8 SIP Push 一般模型

9.1.1 特征标签格式

Push 资源标识符特征标签的语法是“名称=值域的语法格式”。

在下面情况下 Push 资源标识符应被编码成特称标签：

- 根据 IETF RFC3840 规定，媒体特征标签的名称应是“g.oma.pusheventapp”，由互联网地址指派机构（IANA）遵循 IETF RFC2506 规定分配的目标标识符。当特征标签包含在一个头域中时，加前缀“+”。
- 媒体特征标签的值是“event-app-id”的值，用引号表示，可用逗号分隔不同的资源，引用的字符串的语法为“event-app-id*（”，“event-app-id）”，event-app-id=1*(%x21/%x23-2B/%x2D-7E)。

9.2 应用资源标识符的使用

9.2.1 注册

在注册过程中，每个能够支持的 Push 应用的 Push 资源标识符可以包含在 SIP REGISTER 消息的 Contact 头域中，作为特征标签。

9.2.2 SIP MESSAGE 方法

通过 SIP MESSAGE 方式传递 Push 消息，Push 发送代理可在 Accept-Contact 头中添加 Push 资源标识符作为特征标签。

当接收到一个 SIP MESSAGE 请求时，Push 接收代理应检查 SIP MESSAGE 消息的地址与当前接收代理地址的一致性，非一致的 SIP MESSAGE 消息进行丢弃，否则使用 Push 资源标识符来路由转发 SIP MESSAGE 请求到目标应用。Push 接收代理将使用 Push 资源标识符来路由转发 SIP MESSAGE 请求到目标应用。

9.2.3 邀请

在发送 SIP INVITE 请求时，Push 发送代理可在 SIP INVITE 消息的 Accept-Contact 头域中，添加应用资源标识符作为特征标签，见 8.4 节的规则和流程。

10 SIP Push 业务安全模型及安全问题

10.1 概述

SIP Push Enabler 应依据和复用 SIP/IP 核心网底层提供的安全特性和机制，例如，保证业务环境安全和授权用户使用。这样的依据关系将会用作安全框架的基础。接入层安全机制由 SIP/IP 核心网提供。SIP/IP 核心网用来提供用户的鉴权和完整性，应能提供 SIP 信令加密保护，参见 IETF RFC3261 规范所定义。

对于在可信任或不可信任的网络上实现的 Push 接收代理，鉴权和安全的通信信道可以由 SIP/IP 核心网，使用内部网络安全流程来建立。在特定情况下，SIP 信令的机密性也是必要的，例如，像 SIP MSRP 或 SIP MESSAGE 等携带敏感的用户数据的 SIP 方法。Push 发送和 Push 接收代理应依据 SIP/IP 核心网底层提供的授权和加密性机制，完成用户身份认证。

用户面的安全并不在 SIP/IP 核心网安全保护范围内。实现 SIP Push 的 Enabler 的功能中，Push 发送代理根据预设的处理方式，对 Push 消息进行处理。同时应确保用户面安全是通过用户面传输协议提供的可用选项执行的，例如 MSRP 或 HTTP。

10.2 SIP/IP 核心网要求

SIP/IP 核心网提供 SIP Push 所需的功能。SIP Push Enabler 框架中的 SIP/IP 核心网不局限于 3GPP 和 3GPP2 IMS 网络，也对其他的 SIP/IP 核心网开放。本标准考虑了两种 SIP/IP 核心网框架来满足 SIP Push 的需求，这两种包括 3GPP IMS 网络和 3GPP2 MMD 网络。下面将介绍在这两种框架下实现 SIP Push 所

需的附加的需求和要求。

10.2.1 3GPP IMS 和 3GPP2 MMD 网络架构

在3GPP IMS和3GPP2 MMD网络上下文中，SIP Push应被看作是基于Push业务的主要机制。当SIP/IP核心网遵循3GPP IMS或3GPP2 MMD规范时，以下小节的附加需求和要求应被应用。

10.2.1.1 框架要求

Push发送代理和Push接收代理应遵循3GPP IMS或3GPP2 MMD的需求、机制和流程，例如会话建立，在以下情况应遵循3GPP TS 24.22和3GPP2 X.S0013-004-A规则和流程

- 当Push 接收代理在UE上实现时，为Push接收代理定义的P-1参考点应遵循Gm参考点，或当Push 接收代理在应用服务器上实现时，遵循 ISC 参考点规则，具体见 3GPP TS 23.228 和 3GPP2 X.S0013-002-A 规范定义。
- 为Push发送代理定义的P-2参考点应遵循3GPP TS 23.228和GPP2 X.S0013-002-A规范定义。

10.2.1.2 注册流程

为了让Push发送代理获知从Push接收代理发送的注册请求（SIP REGISTER），当UE实现时，SIP/IP核心网能按照Push接收代理发送的注册消息，发起第三方SIP REGISTER请求。此第三方注册请求能够基于为SIP REGISTER请求设置的过滤标准来触发，来指示支持SIP Push业务，具体见3GPP TS 23.228和3GPP2 X.S0013-002-A规范定义。同样，Push发送代理能够订阅"reg"事件包，具体见3GPP TS 24.229和3GPP2 X.S0013-004-A给出的定义。

10.2.1.3 安全要求

3GPP IMS和3GPP2 MMD网络架构提供了Push接收代理（在UE上实现）和Push发送代理（作为可信任网络元素实现的部分）间的互相鉴权、完整性保护以及 SIP 信令加密保护的功能。达到此功能的接入网络安全要求在3GPP IMS和3GPP MMD中有定义，具体见3GPP TS 33.20和3GPP2 S.R0086-0规则和流程。在域间和域内的可信任网络元素间完成安全通信的流程，3GPP IMS将遵循3GPP TS 33.210规范，3GPP2 MMD将遵循3GPP2 S.R0086-0给出的定义。

下面给出特定的需求：

- 在3GPP IMS网络中，Push发送代理（应用服务器）和Push接收代理（UE或应用服务器一部分）应遵循所有可用的安全需求，例如互相鉴权，对于3GPP IMS网络遵循3GPP TS 33.203、3GPP TS 33.210和3GPP TS 24.229规则和流程。对于3GPP2 MMD网络，遵循3GPP2 S.R0086-0和3GPP2 X.S0013-002-A规则和流程。
- 当Push发送代理，作为IMS应用服务器时，将不作为可信任网络元素的组成部分（域间安全不充分时），它应被鉴权，之后向网关或Push接收代理建立安全的通信，对于3GPP IMS网络，在3GPP TS 33.210给出定义，对于3GPP2 MMD，在3GPP2 S.R0086-0给出定义。
- 当Push发送代理作为发起业务的用户代理时，SIP/IP核心网应可以对其进行声明。对于3GPP IMS网络，具体见3GPP TS 24.229规范，对于3GPP2 MMD网络具体见3GPP2 X.S0013-002-A给出的定义。

10.3 可信任模型

SIP Push为SIP信令提供的可信任模型，是建立在SIP/IP核心网所提供的每一跳的安全，代理鉴权，和域内安全的可信任安全模型基础上的。当域内的安全不充分时，例如，Push 接收代理不是可信任网络中一部分，那么SIP/IP核心网应在SIP/IP核心网与Push接收代理之间，提供安全机制来鉴权和保证通信

的安全。SIP Push 消息接收的接收代理应检查 SIP Push 消息的地址与当前接收代理地址的一致性，否则，丢弃 SIP Push 消息来保证安全。

当 Push 发送代理作为发起方用户代理时，应可以由 SIP/IP 核心网遵循 IETF RFC3261，插入 Push 发送代理的用户标识。

10.4 SIP 信令安全

这里描述的 SIP 信令安全机制/特性涵盖 SIP 消息的信令和用户信息。

10.4.1 完整性和隐私保护

支持 SIP Push Enabler 的任何 SIP/IP 核心网应有能力提供必要的安全机制，在 Push 接收代理和 Push 发送代理间完成鉴权，完整性保护和保护 SIP 信令的机密性的功能。这包括机密性，鉴权机制和安全协议，不限于此。

10.4.2 对发起方鉴权

Push 接收代理和 Push 发送代理应采用 SIP/IP 核心网提供的安全机制来确保消息发起方鉴权。

当 SIP Push 发送代理在可信任网络中时，Push 发送代理可通过使用 P-Asserted-Identity 头域放入 Push 发送代理 URI 来完成鉴权，见 IETF RFC3325 规范。

10.5 用户面安全

执行 SIP Push 的 Enablers 应通过用户面安全的传输协议，来确保用户面安全，例如使用 MSRP 或 HTTP。

10.6 终端基于白名单的授权

为了保证从未授权的源端发起的业务被误认为攻击而拒绝接受，本标准引入了一种白名单机制。SIP Push 白名单是由一些可信任的 Push 发送代理或可信任的 PI 组成。如果 Push 接收代理配置了白名单，那么 Push 接收代理应用它来检查 Push 发送代理的源地址或 PI 的地址等信息。Push 发送代理的源地址或 PI 的源地址，与预设的白名单进行匹配，如果是可信任的，Push 接收代理应接收并处理接收到的消息；如果是不可信任的，Push 接收代理将丢弃接收到的消息。如果 Push 接收代理没有配置白名单，那么 Push 接收代理正常处理接收到的消息。

10.7 SIP/IP 核心网中最小化拥塞

Push 发送代理的错误行为，可导致在 SIP/IP 核心网的信令网络中，造成 Push 请求的拥塞。本标准认定 SIP/IP 核心网应遵循 IETF RFC3261 准则，使用拥塞控制方法。

Push 发送代理推荐减少尝试无效的 Push 请求，例如当 Push 接收代理不可用的情况下，避免发送 Push 请求。

附 录 A
（资料性附录）
响应码解析

当 Push 接收代理接收到一个 SIP 请求，将产生一个 SIP 响应。下表显示了在 SIP 响应码与 SIP Push 响应场景的对应关系，这些响应场景表示一个 SIP Push 码的解析和应用的指引。除了文档列出的，响应都应按照 SIP 规范 IETF RFC3261、IETF RFC3428 的规则解析。

表 A.1 响应码解析

情 景	SIP Push 方法	SIP 响应码	描 述
1	SIP MESSAGE	200 OK	接受 Push 请求
2	SIP MESSAGE	400 bad request- 500 server internal error - 503 server unavailable - 603 decline	拒绝 Push 请求，未指定原因，允许重新发送请求
3	SIP MESSAGE	- 403 Forbidden - 604 does not exist anywhere	拒绝 Push 请求，未指定原因，不允许重新发送请求
4	SIP MESSGE	- 408 request timeout	拒绝 Push 请求，原因为 Push 消息不能传递到目的地
5	SIP MESSAGE	- 500 Server internal error	拒绝 Push 请求，原因为 Push 消息不完整而丢弃
6	SIP MESSAGE	- 415 Unsupported media type	拒绝 Push 请求，原因为不能处理此内容类型

附 录 B
（资料性附录）
ICSI 和 IARI 的互操作性

B.1 介绍

本标准使用的 Enabler 可在 3GPP IMS 网络下开展 Push 业务。这种情况下，实现业务的 Enabler 需考虑 IMS 网络中通过 IMS 通信业务标识符（ICSI）来识别的通信业务。

多种同一类型的应用可能在相同通信业务上运行。IMS 应用索引标识符（IARI）用来寻址到应用实例上，例如可能在同一设备上使用两个 MMS 应用。

一个使用 SIP Push 的 Enabler 本身可能有多种不同资源需要路由寻址，Push 资源标识符可用来寻址。

图 B.1 所示为 ICSI、IARI 和 ARI 的使用。

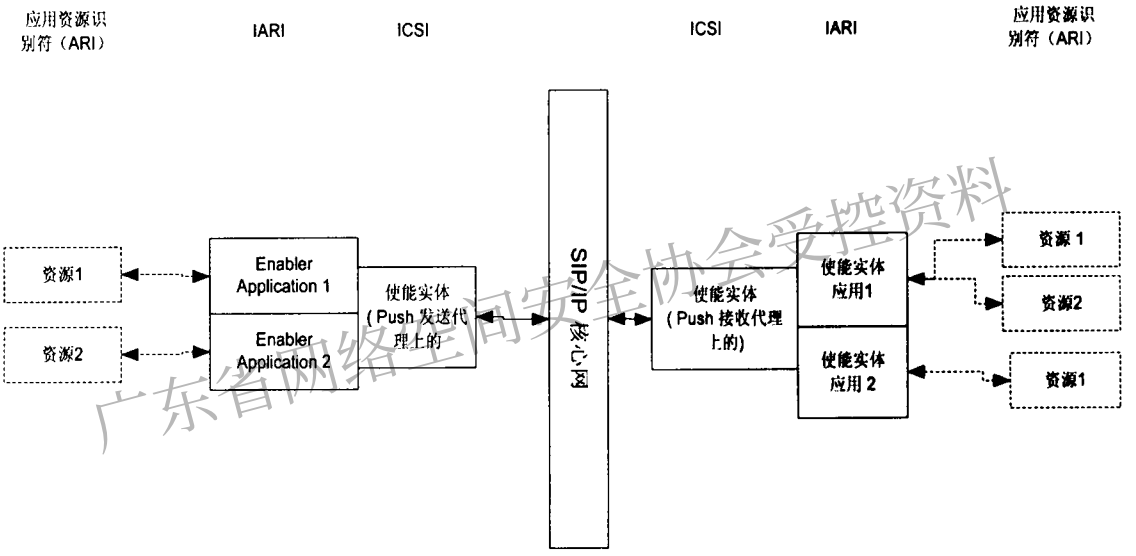

图 B.1 ICSI、IARI 和 ARI 的使用

本标准只规定 Push 资源标识的使用。如果 Enabler 在 IMS 环境下进行业务时，ICSI、IARI 以及 Push 资源标识符可同时使用。

B.2 举例

如下给出简单的举例，ICSI、IARI 和 Push 资源标识符同时在使用 SIP MESSAGE 方法的 Push 请求中出现的情形。IARI 和 Push Event Id 在 Accept-Contact 头域中作为特征标签出现。ICSI 在 P-Preferred-Service/P-Asserted-Service 头域中发送。

MESSAGE sip:user2@domain.com SIP/2.0

Via: SIP/2.0/TCP user1pc.domain.com;branch=z9hG4bK776sgdkse

Max-Forwards: 70

P-Preferred-Identity: "John Doe" <sip:john.doe@home1.net>

From: sip:user1@domain.com;tag=49583

To: sip:user2@domain.com

Accept-Contact;+g.ims.app_ref="<urn:urn-xxx:3gpp.application.mmsua>";+ g.oma.pusheventappp="mms.ua"

Call-ID: asd88asd77a@1.2.3.4

CSeq: 1 MESSAGE

Content-Type: text/plain

P-Preferred-Service: urn:urn-xxx.push

Content-Length: 18

SIP/2.0 200 OK

Via: SIP/2.0/TCP proxy.domain.com;branch=z9hG4bK123dsghds;received=192.0.2.1

Via: SIP/2.0/TCP user1pc.domain.com;;branch=z9hG4bK776sgdkse;received=1.2.3.4

P-Asserted-Identity: "John Doe" <sip:john.doe@home1.net>

From: sip:user1@domain.com;tag=49394

To: sip:user2@domain.com;tag=ab8asdasd9

Call-ID: asd88asd77a@1.2.3.4

CSeq: 1 MESSAGE

P-Asserted-Service: urn:urn-xxx.push

Content-Length: 0

参 考 文 献

[1] IETF RFC2119 Key words for use in RFCs to Indicate Requirement Levels

[2] IETF RFC2183 Communicating Presentation Information inInternet Messages: The Content-Disposition Header Field

[3] IETF RFC2234 Augmented BNF for Syntax Specifications: ABNF

中 华 人 民 共 和 国
通 信 行 业 标 准
移动网络中基于会话初始协议的推送业务技术要求
YD/T 1937-2008
*
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
北京新瑞铭印刷有限公司印刷

*
开本：880×1230　1/16　　2009年8月第1版
印张：1.75　　2009年8月北京第1次印刷
字数：46千字
ISBN 978-7-115-1894/09-136
定价：15元
本书如有印装质量问题，请与本社联系　电话：(010)67114922