ICS 33 070 01
M 37

YD

中华人民共和国通信行业标准

YD/T 1789-2008

移动多媒体广播业务 终端/卡设备技术要求

Mobile Multimedia Broadcast Service Technical Requirements for Equipment of Terminal and Card

2008-03-28 发布　　2008-06-01 实施

中华人民共和国工业和信息化部　发布

http://www.ptsn.net.cn

目　　次

http://www.ptsn.net.cn

前　言

本标准是移动多媒体广播业务系列规范之一，该系列标准的名称及结构如下：

（1）YD/T 1785-2008　移动多媒体广播业务：总体技术要求

（2）YD/T 1786-2008　移动多媒体广播业务 业务保护技术要求

（3）YD/T 1787-2008　移动多媒体广播业务 业务指南技术要求

（4）YD/T 1788-2008　移动多媒体广播业务 业务平台设备技术要求

（5）　移动多媒体广播业务 业务平台设备测试方法

（6）YD/T 1789-2008　移动多媒体广播业务 终端/卡设备技术要求

（7）　移动多媒体广播业务 终端/卡设备测试方法

（8）YD/T 1790-2008　移动多媒体广播业务 应用层接口技术要求

（9）YD/T 1791-2008　移动多媒体广播业务 交互应用技术要求

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：信息产业部电信研究院、中国移动通信集团公司、中国联合通信有限公司、华为技术有限公司、中兴通讯股份有限公司、诺基亚通信有限公司

本标准主要起草人：匡晓烜、袁　琦、吴　伟、张慧媛、常嘉岳、严斌峰、刘申健、陈国乔、彭宏利、王劲松、汪庆华

http://www.ptsn.net.cn

移动多媒体广播业务
终端/卡设备技术要求

1 范围

本标准规定了在提供移动多媒体广播业务时移动终端设备在基本功能、音视频功能、业务指南功能、业务交互功能、业务保护功能、协议、性能等方面的技术要求，以及智能卡设备在文件、命令、安全等方面的技术要求。

本标准适用于支持移动多媒体广播业务的数字蜂窝移动终端设备以及用户智能卡。

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 18287-2000	蜂窝电话用锂离子电池总规范
GB/T 18288-2000	蜂窝电话用金属氢化物镍电池总规范
GB/T 18289-2000	蜂窝电话用金属镉镍电池总规范
GB 19484.1-2004	800MHz CDMA 数字蜂窝移动通信系统 电磁兼容性要求和测量方法 第1部分：移动台及其辅助设备
YD/T 1268-2003	移动通信手持机锂电池及充电器的安全要求和试验方法
YD/T 1268-2003	移动通信手持机锂电池及充电器的安全要求和试验方法
YD/T 1032-2000	900/1800MHz TDMA数字蜂窝移动通信系统电磁兼容性限值和测量方法
YD/T 1592.1-2007	2GHz TD-SCDMA数字蜂窝移动通信系统电磁兼容性要求和测量方法 第1部分：用户设备及其辅助设备
YD/T 1595.1-2007	2GHz WCDMA数字蜂窝移动通信系统电磁兼容性要求和测量方法 第1部分：用户设备及其辅助设备
YD/T 1597.1-2007	cdma2000数字移动通信系统电磁兼容性要求和测量方法 第1部分：移动台及其辅助设备
YD/T 965-1998	电信终端设备的安全要求和试验方法
YD/T 1539-2006	移动通信手持机可靠性技术要求和测试方法
YD/T 1214-2006	900/1800MHz TDMA数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术要求：移动台
YD/T 1558-2007	2GHz cdma2000数字蜂窝移动通信网设备技术要求：移动台
YD/T 1562-2007	2GHz cdma2000数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第一阶段）接入终端（AT）
YD/T 1679-2007	2GHz cdma2000数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第二阶段）接入终端（AT）
YD/T 1367-2006	2GHz TD-SCDMA数字蜂窝移动通信网 终端设备技术要求

YD/T 1367-2006	2GHz TD-SCDMA数字蜂窝移动通信网 终端设备技术要求
YD/T 1547-2007	2GHz WCDMA数字蜂窝移动通信网终端设备技术要求（第二阶段）
YD/T 1168-2007	CDMA数字蜂窝移动通信网用户识别模块（UIM）技术要求
YD/T 1785-2008	移动多媒体广播业务 总体技术要求
YD/T 1787-2008	移动多媒体广播业务 业务指南技术要求
YD/T 1791-2008	移动多媒体广播业务 交互应用技术要求
YD/T 1786-2008	移动多媒体广播业务 业务保护技术要求
YD/T 1790-2008	移动多媒体广播业务 应用层接口技术要求
YDC 015-2006	800MHz CDMA 1X数字蜂窝移动通信网设备技术要求：移动台
YDC 068-2008	800MHz CDMA 1X数字蜂窝移动通信网高速分组数据（HRPD）设备技术要求：接入终端（第二阶段）
ISO/IEC 8825	信息技术ASN.1编码规则
3GPP TS 31.101	UICC终端卡接口：物理和逻辑特性
3GPP TS 31.102	USIM应用特性
3GPP TS 33.103	3G安全：综合指导方针
3GPP TS 33.220	通用鉴权架构，通用自举架构
3GPP TS 33.246	MBMS的安全
ETSI GSM 11.11	SIM卡接口的SIM应用工具箱标准
3GPP2 C.S0023-C_v1.0	扩频系统可移动用户识别模块一致性测试
3GPP2 S.S0083-A_v1.0	BCMCS业务安全框架
3GPP2 X.S0022-A	cdma2000无线IP网络中的广播和多播业务
3GPP2 S.S0055	增强密码算法
OMA-RD-BCAST-V1_0-20080226-C	移动广播业务需求
OMA-AD-BCAST-V1_0-20080226-C	移动广播业务架构

3 定义和缩略语

3.1 定义

下列定义适用于本标准。

3.1.1

广播承载

提供单向的、点对多点的信道，用于网络向移动终端传输数据。通常，这种广播传输机制允许多个接收者采用相同的协议同时接收同一数据源，如通过同一链接或基于同一无线频率。广播承载包括多种类型，可基于多种传输协议。典型的广播承载包括专用地面广播、移动网络广播以及卫星广播。

3.1.2

交互通道

提供双向、点对点的信道，用于网络与移动终端之间互相传递数据。交互通道有多种方式，包括IP承载流（如HTTP、流媒体等）、短消息、多媒体消息等。

3.2 缩略语

下列缩略语适用于本标准。

3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
3GPP2	3rd Generation Partnership Project 2	第三代合作伙伴计划2
AES	Advanced Encryption Standard	高级加密标准
BAK	Broadcast Access Key	128位广播访问密钥，这里统称为业务密钥
BCMCS	Broadcast Multicast Service	广播多播业务
BSF	Bootstrapping Server Function	引导服务功能
CDMA 1X	Code Division Multiple Access 1X	码分多址
cdma2000	Code Division Multiple Access 2000	第三代移动通信技术之一
DM	Device Management	设备管理
E-mail	Electronic Mail	电子邮件
GBA	Generic Bootstrapping Architecture	通用自举架构
GPRS	General Packet Radio Service	通用分组无线服务
GSM	Global System for Mobile Communications	全球移动通讯系统
GZIP	GNU zip	GNU自由软件的文件压缩程序
HTML	Hyper Text Markup Language	超文本标记语言
HTTP	Hyper Text Transfer Protocol	超文本传输协议
IP	Internet Protocol	互联网协议
LCD	Liquid Crystal Display	液晶显示屏
MBMS	Multimedia Broadcast/Multicast Service	多媒体广播/组播业务
MIKEY	Multimedia Internet KEYing	多媒体因特网密钥管理
MMS	Multimedia Messaging Service	多媒体消息业务
MO	Mobile Originated	终端发起
MPEG	Moving Pictures Experts Group	动态图像专家组
MRK	MBMS Request Key	MBMS请求密钥
MSK	MBMS Service Key	MBMS业务密钥
MTK	MBMS Traffic Key	MBMS传输密钥
OMA	Open Mobile Alliance	开放移动联盟
OTA	Over The Air	空中
QCIF	Quarter Common Intermediate Format	1/4通用中间格式
R-UIM	Removable User Identity Module	机卡分离用户识别模块
RTP	Real-time Transport Protocol	实时传输协议
RTCP	RTP Control Protocol	RTP控制协议
SG	Service Guide	业务指南
SG-C	Service Guide Client	业务指南客户端
SIM	Subscriber Identity Module	用户身份模块
SK	Short-term Key	128位节目密钥，用于加密BCMC节

		目内容的密钥
SMIL	Synchronized Multimedia Integration Languange	同步多媒体同步语言
SMS	Short Message Service	短消息业务
SQCIF	Sub-Quarter Common Intermediate Format	Sub-Quarter通用中间格式
SRTP	Security Real Traffic protocol	安全实时传输协议
TD-MBMS	TD-SCDMA Multimedia Broadcasting	TD-SCDMA多媒体广播业务
TD-SCDMA	Time Division Synchronous Code Division Multiple Access	时分同步码分多址接入
TK	Temporary Key	128位的临时密钥
UDP	User Datagram Protocol	用户数据报协议
USIM	Universal Subscriber Identity Module	通用用户识别模块
WAP	Wireless Application Protocol	无线应用协议
WCDMA	Wideband Code Division Multiple Access	宽带码分多址接入
XML	eXtensible Makeup Language	可扩展标记语言

4 总体要求

4.1 系统结构

图1所示描述了移动多媒体广播业务相关的功能实体。黄色功能实体和蓝线所代表的接口将是本系列标准所涉及的范围。

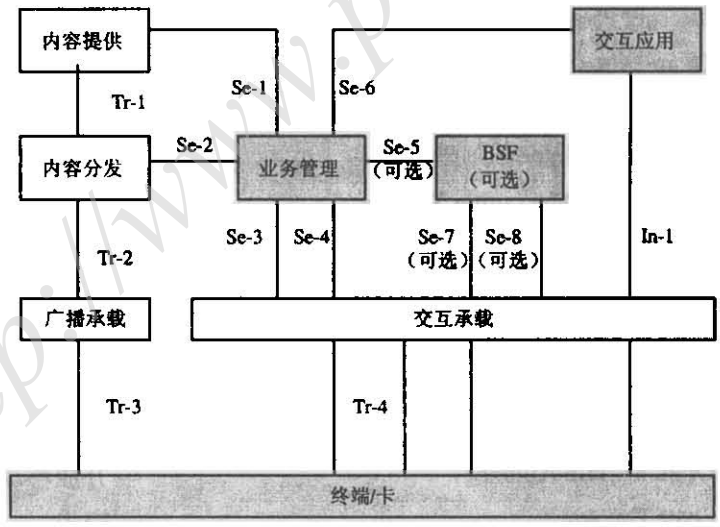

图1 移动多媒体广播业务系统功能结构

如图1所示，移动多媒体广播业务系统结构包含一系列逻辑实体及其之间的接口。移动多媒体广播业务功能的实现将基于这些广播功能模块实体；其中，终端和终端用户卡通过通信和广播承载模块分别与业务管理模块、内容分发模块接口。本标准主要规定图1中终端模块的技术要求。

4.2 基本要求

移动多媒体广播业务终端应能够正常接收移动多媒体广播业务。终端应能实现如下业务功能：

（1）业务订购、退订；

（2）根据业务指南信息接收数据或音视频流节目；

（3）必要的业务和内容保护；

（4）支持业务交互应用；

（5）支持业务平台所提供的漫游和移动性。

4.3 业务流程

移动多媒体广播业务终端应实现参考业务流程如图 2 所示。

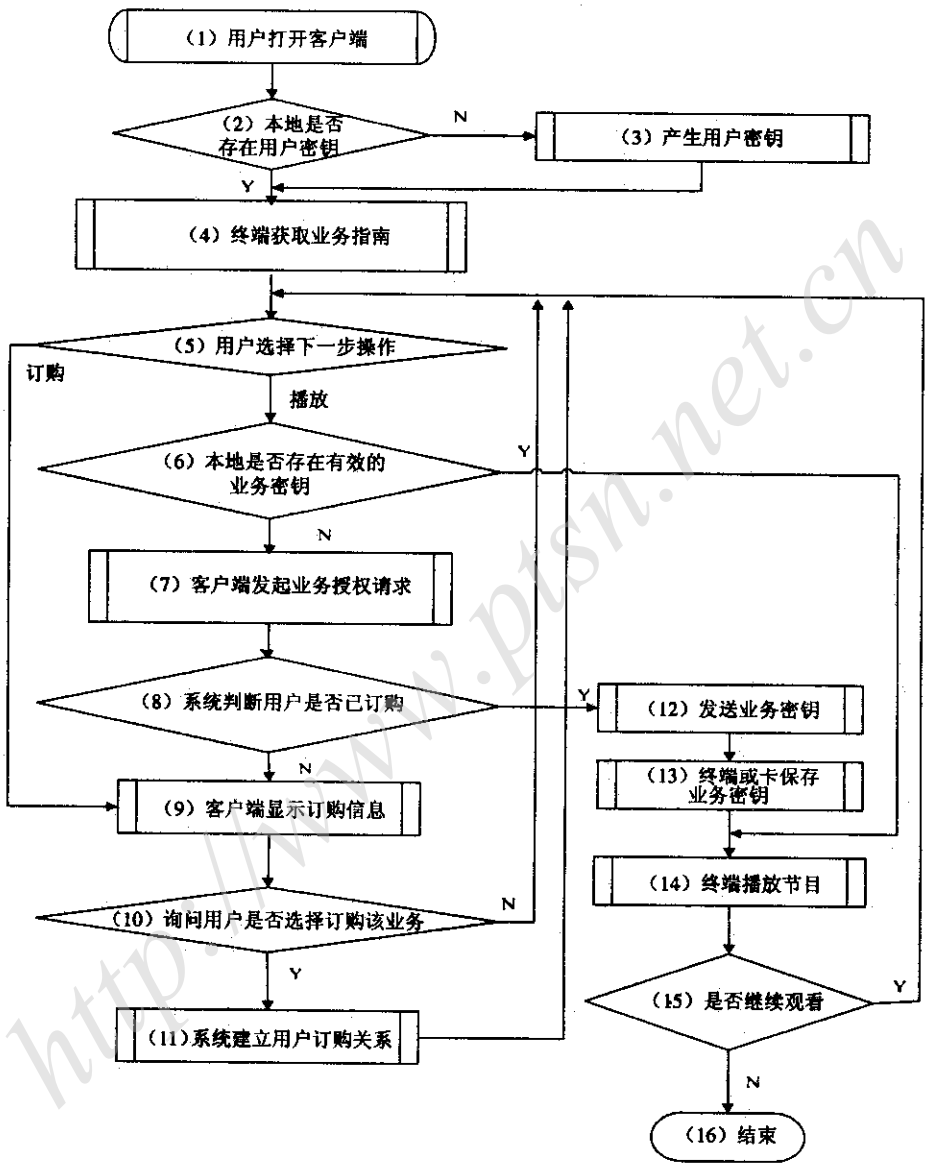

图2 移动多媒体广播业务流程图

业务流程描述如下：

步骤（1）：用户打开移动多媒体广播终端。

步骤（2）：终端判断本地是否存有共享密钥，如果是进入步骤（4），否则进入步骤（3）。

步骤（3）：业务管理系统对用户进行认证，认证通过后业务管理系统和终端侧的卡中各自生成用户的共享密钥。

步骤（4）：终端接收业务指南。

步骤（5）：用户浏览节目信息，选择希望收看的节目，如果用户选择订购业务，则进入步骤（9）；如果用户选择播放节目，则进入步骤（6）。

步骤（6）：终端判断是否存有将要播放的内容的业务密钥，如果有进入步骤（14），否则进入步骤（7）。

步骤（7）：终端向业务管理系统发起业务授权请求。

步骤（8）：业务管理系统判断用户是否已经订购了该业务，如果是进入步骤（12），否则进入步骤（9）。

步骤（9）：提示用户业务订购信息，进入步骤（10）。

步骤（10）：询问用户是否选择订购该业务，如果用户选择是，进入步骤（11），否则进入步骤（5）。

步骤（11）：业务管理系统建立用户订购关系，进入步骤（5）。

步骤（12）：业务管理系统发送业务密钥到终端。

步骤（13）：终端则将业务密钥存储在卡中。

步骤（14）：终端播放节目。

步骤（15）：用户在观看节目过程中可以选择调换内容继续观看还是结束业务，如果选择调换节目，则进入步骤5；否则进入步骤（16）。

步骤（16）：结束节目播放，关闭终端。

5 通信基本功能及性能要求

5.1 GSM（GPRS）

移动台应满足YD/T 1214-2006 《900/1800MHz TDMA数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术要求：移动台》的要求。

5.2 cdma 1X

移动台应满足YDC 015-2006 《800MHz CDMA 1X数字蜂窝移动通信网设备技术要求：移动台》的要求。

5.3 cdma 2000

移动台应满足下列标准的要求：

YD/T 1558-2007 2GHz cdma2000数字蜂窝移动通信网设备技术要求：移动台；

YD/T 1562-2007 2GHz cdma2000数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第一阶段）接入终端（AT）；

YD/T 1679-2007 2GHz cdma2000数字蜂窝移动通信网设备技术要求：高速分组数据（HRPD）（第二阶段）接入终端（AT）；

YDC 068-2008 800MHz CDMA 1X数字蜂窝移动通信网高速分组数据（HRPD）设备技术要求：接入终端（第二阶段）。

5.4 TD-SCDMA

移动台应满足YD/T 1367-2006 《2GHz TD-SCDMA数字蜂窝移动通信网 终端设备技术要求》的要求。

5.5 WCDMA

移动台应满足YD/T 1547-2007《2GHz WCDMA数字蜂窝移动通信网终端设备技术要求(第二阶段)》的要求。

6 功能与业务要求

6.1 基本功能要求

6.1.1 概述

用户应可以通过移动多媒体广播终端实时和非实时的播放多媒体节目，实现直播、广播文件下载、各种交互式广播节目等业务形式中的一种或多种。

主要业务描述如下：

（1）音视频节目直播：用户可以通过移动多媒体广播终端实时的观看各种频道的多媒体节目，并可以选择观看其他频道节目或退出观看，节目流是由业务平台以广播形式发送到终端的。当接收到直播紧急信息业务时，需要在不停止音视频节目播放的前提下及时进行显示紧急业务内容，并可以加入提示以提醒用户注意紧急信息。

（2）广播文件下载：用户可以通过移动多媒体广播终端定购并下载各种视音频文件、图片、文字文件、游戏等，这些文件是由业务平台以广播形式发送到终端的。

（3）其他交互式数据广播：用户能够接收交通、电子地图、天气等数据业务，并可以以Web等方式实现各种交互功能，比如在线投票、在线游戏等。

用户可以在业务指南信息引导下进行节目浏览和预览，在定购业务并取得业务密钥之后才可以在授权范围内播放节目。

6.1.2 终端硬件配置要求

（a）LCD显示屏规格要求

尺寸：对角线2.0英寸或以上；

分辨率：（220×176Pixels）或以上；

颜色：支持64k色或以上。

（b）耳机

支持立体声耳机，支持通话和收听移动多媒体广播业务的音频节目或视频节目伴音。

6.1.3 参数设置要求

终端应具备配置初始参数配置的能力，初始参数的设置可以是厂家事先预设、由用户手动修改或通过空中配置（OTA、DM等方式）或软件进行改写。

6.1.4 终端基本参数表

移动多媒体广播终端应支持如下基本参数的配置：

业务服务器地址、WAP网关地址、接入点等。

6.1.5 其他要求

（1）终端应支持用户直接输入频道号码的频道切换和用户连续按某一按键进行的连续频道切换；

（2）终端应支持在播放过程中调节音量，同时可以静音并可恢复。

（3）终端应支持纯音频节目的播放。

（4）从SG中每个节目都可以进入播放界面或相应广播信息界面；

（5）支持全屏切换、旋转（可选）、亮度调整等播放功能；

（6）可显示播放节目名称、类型、播出时间等信息；

（7）终端应能够提供菜单选项或其他方式查询、显示广播信号强度信息；在启动移动多媒体广播业务过程中，除全屏外，状态栏也可显示广播信号强度信息。

（8）播放过程中遭遇弱的电视信号时，要给出提示信息（文字、图标），尽可能避免显示马赛克情况。信号恢复后自动播放或提示用户是否继续播放。

6.2 音视频功能

用户应可以通过移动多媒体广播终端实时和非实时的收看多媒体节目广播和各种交互式节目等数据、音频、视频信息。

移动多媒体广播终端应能向用户显示电子节目单。

移动多媒体广播终端应根据内容源分辨率的不同调整视频输出分辨率，支持QCIF（176×144）、SQCIF（128×96）等分辨率。

移动多媒体广播终端应支持视频显示的亮度等关键参数的调节。

6.3 事件并发处理功能

在终端的移动多媒体广播业务激活时，并发其他功能或业务时终端应具备如下功能：

（1）播放过程中，闹钟到时，需要显示闹钟提示；

（2）播放过程中，当电量低时，要及时给出电量低的提示（图标或者提示信息），从而保证手机的通话、短信等基本功能实现的带电量；

（3）播放多媒体节目过程中，有消息（SMS，MMS，E-mail）到时，需要以文字（可选）、声音、振动方式提示接收消息，并在状态栏显示消息图标；

（4）搜索或播放过程中，并发来电，需要提供提示（文字/图标），并振铃；同时可提供询问接通或拒绝电话；

（5）接听电话时，显示通话界面；通话结束后，直接返回继续收看或终端给出提示：是否返回原节目收看界面，确认后可继续收看。

6.4 编解码

移动多媒体广播业务终端应支持的编解码功能见YD/T 1785-2008《移动多媒体广播业务 总体技术要求》。

6.5 业务指南

6.5.1 业务指南功能概述

业务指南功能提供给广播用户在本区域内有效的各种各样的广播内容的信息。根据广播传输系统的能力不同，广播内容信息发送的形式也不同，要么作为基于IP的业务指南信息，要么是广播传输系统特定的消息，或者两者皆是。业务指南信息可以根据广播传输系统来改变，例如增加一些广播传输系统特有的信息。这种改变可以在业务分发/适配模块中的Service Guide Generation/ Adaptation/Distribution实体中，或者在广播发送系统中。

移动多媒体广播终端应可以配置业务平台业务指南服务器地址，能以XML文件的形式由业务指南服务器接收并存储业务指南信息，终端应支持定期自动更新或手动更新指南信息。

移动多媒体广播终端应可以向用户显示业务指南信息，这些信息包括频道名称、节目名称、开始时间、结束时间、付费标准等，应支持支持节目列表显示和详情预览功能，用户根据这些业务指南信息可以进行节目预览、业务定购与退订、播放节目等操作。

终端应支持基于广播方式下发业务指南信息和基于交互信道下发指南信息。

终端应支持以下方式的节目选择：

（1）终端应支持用户直接通过点击频道编号方式选择播放节目；

（2）终端应支持用户通过连续点按某个键方式依次播放节目；

（3）终端支持用户通过SG指南到满意的节目；

（4）终端应支持业务指南信息的GZIP压缩。

6.5.2 终端中的业务指南模块

终端中的业务指南客户端模块（SG-C）负责从广播分发系统或交互网络中接收业务指南信息，使得业务指南在移动终端中得以实现。SG-C包括了特定的业务指南信息。更进一步的，SG-C能够根据特定的标准过滤业务指南信息，例如根据位置，用户设定或者终端能力。业务指南中包括的文件信息可以被转送到终端中的其他功能块中。通常用户可以通过菜单，目录或者列表的形式观看业务指南信息。SG-C可以通过SG-6发送一个请求到网络中来取得特定的业务指南信息或者完整的业务指南信息。

6.5.3 业务指南数据及封装

业务指南数据基于XML数据格式定义，业务指南的数据分片可以直接封装在XML文件中进行传输，也可以使用GZIP等方式压缩后再进行传输。终端应支持的业务指南数据和终端在处理业务指南数据封装时应符合的要求可见YD/T 1787-2008《移动多媒体广播业务 业务指南技术要求》。

6.5.4 业务指南的发现

终端发现交互式业务指南有两种方式。

（a）终端通过交互网络发现业务指南的入口信息

终端可以通过固化的业务指南门户地址，或者通过DM的MO的方式配置得到交互SG的发现地址，获取业务指南信息。

（b）终端通过广播网络发现交互式业务指南的信息

终端用户通过广播网络接收自举会话，假如业务指南提供商提供交互式业务指南，通过该自举会话终端用户可以获得交互式业务指南的入口信息，进而通过该入口对该业务指南进行访问和下载。

6.5.5 业务指南获取/更新流程

移动终端获取业务指南的流程如图3所示。终端向移动多媒体业务平台发送业务指南获取请求，而业务平台收到请求后通过HTTP响应在载荷（payload）中返回相应的业务指南数据。

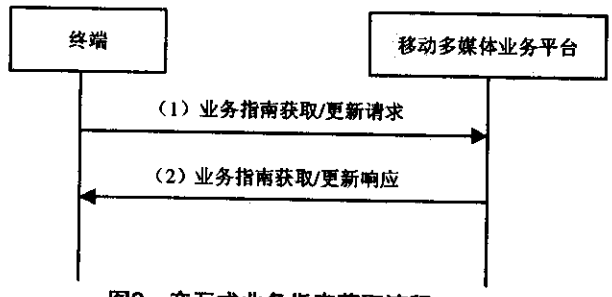

图3 交互式业务指南获取流程

移动终端更新业务指南的流程如图 3 所示，终端向移动多媒体业务平台发送业务指南更新请求，请求消息中可附带终端所要更新的业务指南标识信息，而业务平台收到请求后，通过 HTTP 响应在载荷（payload）中返回相应的业务指南数据。

6.6 业务交互

6.6.1 交互业务功能概述

业务交互功能提供了网络中的交互应用模块和终端之间的点对点的交互。业务交互功能需要交互网络的支持，例如蜂窝网或短消息系统。交互功能支持不同种类的交互，如访问，短消息，多媒体短消息，发送屏幕截图，下载，电子邮件，附加网址的链接等。

6.6.2 交互业务内容及数据定义

终端应支持的交互业务内容及数据定义可见YD/T 1791-2008《移动多媒体广播业务 交互应用技术要求》。

6.6.3 获取和更新交互业务数据

6.6.3.1 从广播通道获取交互业务数据

如果交互业务数据从广播通道下发，终端将通过如下结构中确定的Access分片获得对应的广播会话的接入信息：

6.6.3.2 从广播通道更新交互业务数据

从广播通道下发，服务器可以在不修改ID的情况下对InteractivityMediaDocument的version信息进行修改。终端收到id相同，但version发生改变的InteractivityMediaDocument，将会更新本地的交互业务数据。

6.6.3.3 从交互通道获取交互业务数据

如果交互业务数据从交互通道下发，终端通过向InteractivityData分片的InteractiveDelivery.interactivityMediaURL发起HTTP POST请求获取交互业务数据。终端可能首先获取InteractivityMediaDocument，再获取其中描述的某个媒体对象集；也可能直接获取InteractivityMediaDocument和所有的媒体对象。

6.6.3.4 从交互通道更新交互业务数据

从交互通道下发，当交互业务数据需要更新的时候，交互业务应用服务器会将交互业务更新数据通知业务管理交互业务服务器。

业务管理交互业务服务器在收到交互业务更新数据之后，会根据终端用户互动业务信息，利用Push消息通知终端进行交互业务的更新。终端在接受到通知消息之后，会主动发起交互业务数据更新请求。

6.6.4 终端业务交互流程

交互业务的获取和展现流程如图4所示。

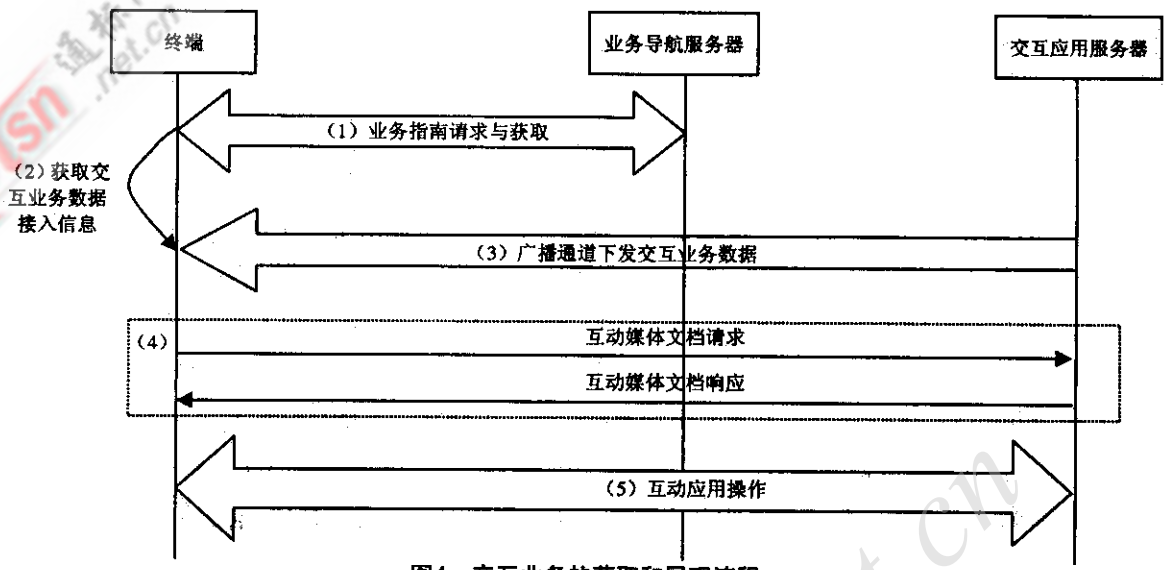

图4　交互业务的获取和展现流程

（1）终端向业务导航服务器发送业务指南获取请求，获取完整的业务指南信息；

（2）终端从业务指南中获得交互业务数据的接入信息；

（3）如果交互业务数据从广播通道下发，终端将根据 6.6.3.1 所述的方式获取 Access 分片，并根据其中的描述接入相应的广播会话；

（4）如果交互业务数据从交互通道下发，终端将根据 6.6.3.3 所述的方式获取请求交互业务数据的 URL，并根据消息体内容请求交互业务数据（见 YD/T 1791-2008《移动多媒体广播业务 交互应用技术要求》）；

（5）用户根据终端展现的交互业务向互动应用服务器反馈信息，实现交互。

6.7　业务保护

6.7.1　分层密钥管理体系

移动多媒体广播业务的业务保护基于分层密钥体系，如图 5 所示。

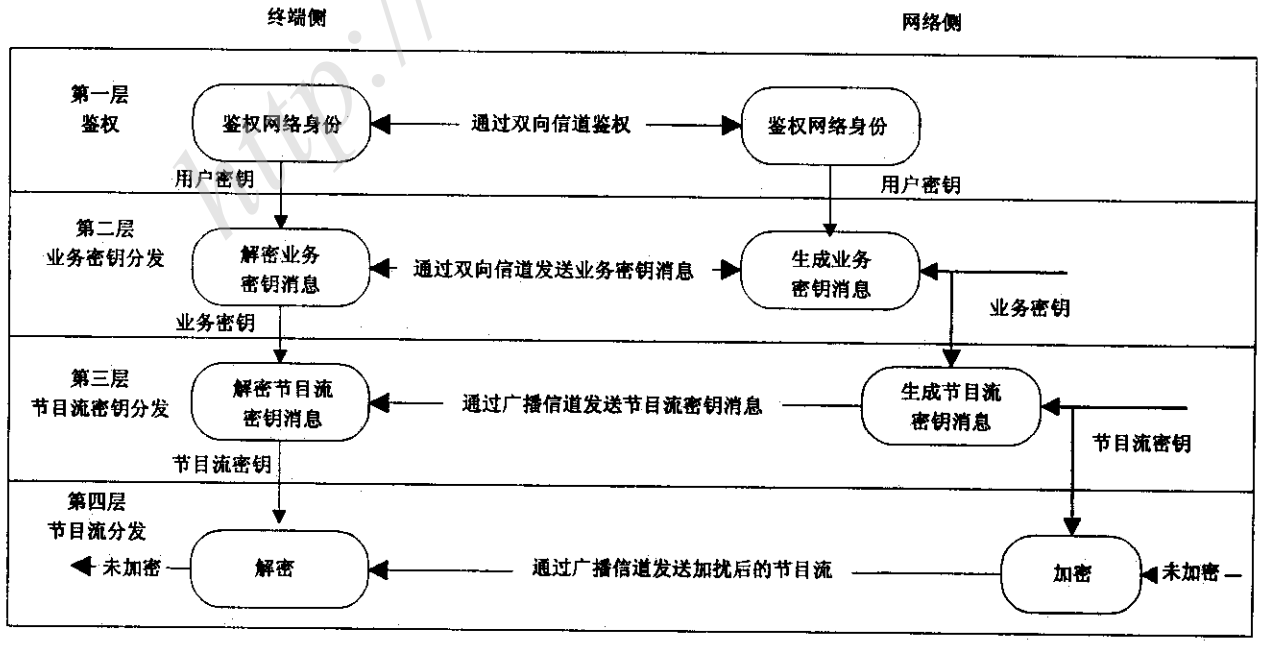

图5　分层密钥管理体系

第一层：认证管理。用户与网络之间进行相互认证，认证通过后获得共享密钥。由此共享密钥在终端和网络生成注册密钥和用户密钥。终端通过注册密钥向多媒体广播业务控制中心进行认证。认证通过后，用户密钥用于随后进行的业务密钥加密传输。

第二层：业务密钥管理。网络根据用户订购关系将业务密钥通过加密方式传送给用户。网络对业务密钥进行加密时将使用用户密钥，终端对业务密钥消息解密时将使用本地生成的用户密钥。对于 3GPP 体系，业务密钥消息采用 MIKEY 格式。对于 3GPP2 体系，业务密钥消息由 3GPP2 3GPP2 X.S0022-A[14] 定义。

第三层：节目流密钥管理。

（1）在 3GPP 体系下，使用节目流密钥加密节目流。将使用业务密钥加密后的节目流密钥在广播网络上传输。终端对节目流密钥解密时将使用业务密钥。节目流密钥消息采用 MIKEY 格式；

（2）在 3GPP2 体系下，节目流密钥分为两个子层：移动网络节目流密钥 SK 和广播网络节目流密钥 MBK。

— 广播网络节目流密钥：将使用 SK 加密后的广播网络节目流密钥 MBK 在广播网络上广播；终端将使用解密了的移动网络节目流密钥 SK 和使用 SK 加密后的广播网络节目流密钥 f（SK，MBK）生成广播网络节目流密钥 MBK。

— 移动网络节目流密钥：网络还需要将移动网络节目流密钥随机数 SK_RAND 和 BAK ID，以及 BCMCS_FLOW_ID（用于和 BAK_ID 一起惟一标识 BAK）在广播网络上广播，终端中的 RUIM 卡将使用解密了的业务密钥 BAK 和移动网络节目流密钥随机数 SK_RAND 生成移动网络节目流密钥 SK。

第四层：节目流管理。使用节目流密钥对节目流加密后通过广播网络进行分发，终端使用解密过的节目流密钥进行解密。

6.7.2 与终端相关的业务保护接口

业务保护体系结构如图 6 所示。

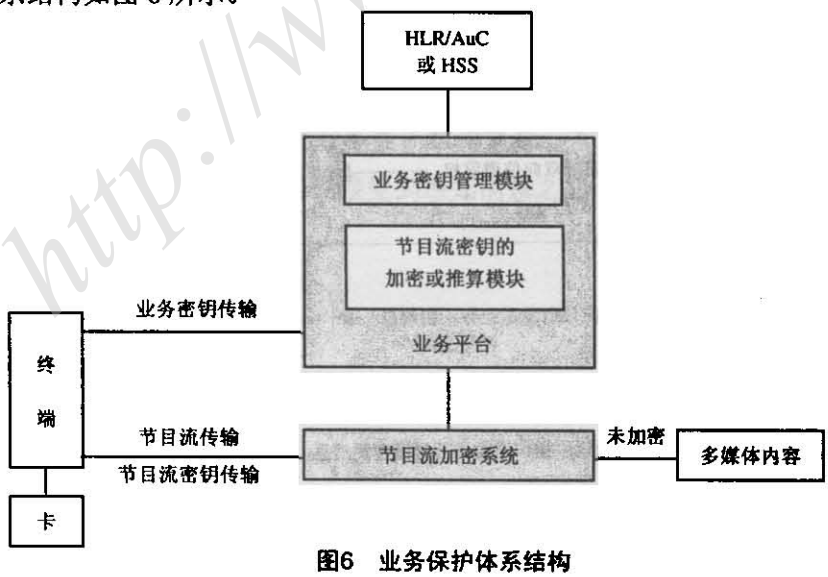

图6 业务保护体系结构

移动多媒体广播业务平台与终端之间的接口功能包括：

（1）完成业务密钥的分发；

（2）执行 GBA 初始化流程，生成 Ks（可选）。

节目流加密系统与终端之间的接口的安全功能包括：

（1）将加密后的节目流密钥广播发送给终端；

（2）将加密后的节目流广播发送给终端。

6.7.3 业务保护密钥分发流程

业务保护密钥分发流程及终端应符合的要求可见YD/T 1786-2008《移动多媒体广播业务 业务保护技术要求》。

6.7.4 其他要求

对于TD-MBMS终端，应支持SRTP协议和AES加密算法；应支持采用RTP/UDP/IP传输方式的节目流接收，支持采用流类方式传输的节目流密钥MIKEY消息的接收，该节目流MIKIEY消息作为UDP包的负荷，与节目流的目的IP地址相同，端口号为2269。

对于其他业务保护技术，本标准不做要求。

7 协议要求

7.1 协议栈

移动多媒体广播业务的协议框架如图 7 所示。

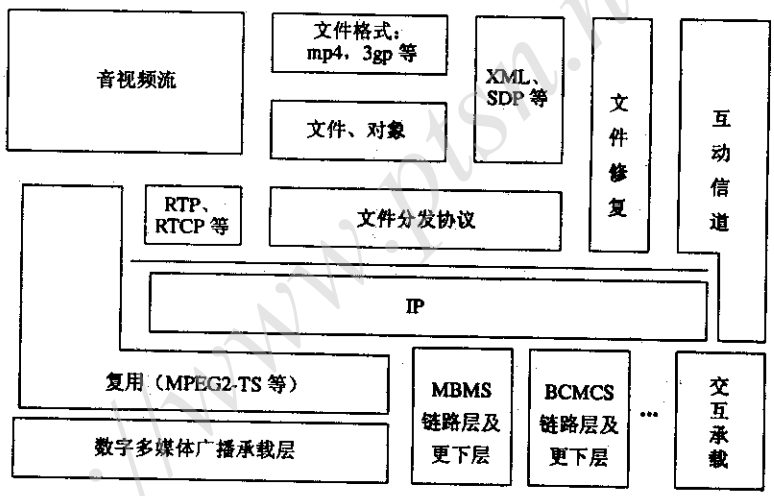

图7 移动多媒体广播业务协议体系结构

图 7 描述了移动多媒体广播业务的协议栈。

底层网络：包括单向广播和双向交互承载。通常，移动多媒体广播流通过单向广播网络发送，而文件（如业务指南）和用于交互的信息可选择采用单向或双向方式。从 IP 角度，底层网络又可分为 IP 网络和非 IP 网络，广播和交互应用均可基于 IP 或非 IP 网络。

从广播网络角度，广播网络又可分为基于移动网络的广播网络以及基于数据多媒体广播的广播网络。基于移动网络的广播网络包括基于 3GPP 的 MBMS 以及基于 3GPP2 的 BCMCS。数字多媒体广播包括了地面广播和卫星广播等多种广播技术。

业务保护一般在 IP、RTP 或 MEPG 传输层加以实现，它用于对业务接入进行保护。

流媒体分发可基于 RTP、MEPG-4 等系统，广播网络的文件（如业务指南 XML 文件、视频短片）分发一般基于文件分发协议（如 FLUTE）。而互动应用可基于 IP 之上的通信协议（如 HTTP）或非 IP 承载（如 SMS）。

移动多媒体广播终端应根据实际情况实现上述协议栈中部分协议，并保证所实现部分协议栈的完整性。

7.2 应用层接口协议

对于和终端/卡模块相关的接口的描述见表1。终端/卡模块需支持以下功能：

（1）支持MBMS安全或BCMCS安全。若采用MBMS业务保护机制，则要求支持GBA_U。

（2）业务指南信息的获取和解析。支持通过交互网络（HTTP）或广播网络获取业务指南信息。基于广播通道的业务指南要求不在本标准范围内。

（3）媒体流内容的获取和播放。支持通过广播网络或交互网络获取媒体流。内容获取不在本标准范围之内。

表1 终端/卡模块相关接口描述

与终端/卡模块相关的接口	接口描述
Se-4	业务指南信息获取、业务密钥获取、业务订购管理
Se-7	SIM/USIM卡与BSF之间的GBA认证。该接口对采用MBMS机制必选，但对BCMCS可选
In-1	交互应用服务器与终端之间的信息传递
Tr-3	提供多媒体广播信道
Tr-4	提供交互信道

表1中，Se-4、Se-7和In-1接口是应用层接口，终端/卡模块应符合YD/T 1790-2008《移动多媒体广播业务 应用层接口技术要求》中关于Se-4和Se-7接口的协议要求，并符合YD/T 1791-2008《移动多媒体广播业务 交互应用技术要求》中关于In-1接口的协议要求。

8 性能要求

8.1 音视频性能

移动多媒体广播终端应满足如下音视频性能要求：

（1）视频处理至少能够支持QCIF分辨率；

（2）视频处理至少能够支持15fps帧频；

（3）视频处理至少能够支持128kbit/s码率。

（4）在正常处理视频流的同时，应能处理相应的音频流同步播放。

8.2 续航能力

为保证移动多媒体广播业务的正常进行，在通常测试条件下终端续航能力应满足下列要求：

（1）视频节目的连续观看时间：≥2h；

（2）音频节目的连续收听时间：≥4h。

9 终端卡接口

9.1 基本要求

GSM（GPRS）移动台应满足YD/T 1214-2006 《900/1800MHz TDMA数字蜂窝移动通信网通用分组无线业务（GPRS）设备技术要求：移动台》的要求。

CDMA 1X移动台和cdma2000移动台应满足YD/T 1168-2007 《CDMA数字蜂窝移动通信网用户识别模块（UIM）技术要求》的要求。

TD-SCDMA终端和WCDMA终端应满足《TD-SCDMA/WCDMA UICC-终端（Cu）接口技术要求第一部分：物理、电气和逻辑》、《TD-SCDMA/WCDMA UICC-终端（Cu）接口技术要求第二部分：应用特性》和《TD-SCDMA/WCDMA UICC-终端（Cu）接口技术要求第二部分：USAT特性》的要求。

9.2 3GPP 体系的终端卡接口

9.2.1 终端与卡的交互流程

移动多媒体广播业务流程涉及到USIM卡、终端、移动网络和广播网络等各个组成部分。本章描述了移动多媒体广播业务中有关用户卡和终端之间的应用流程。

9.2.1.1 GBA 初始化

GBA初始化流程如图8所示。

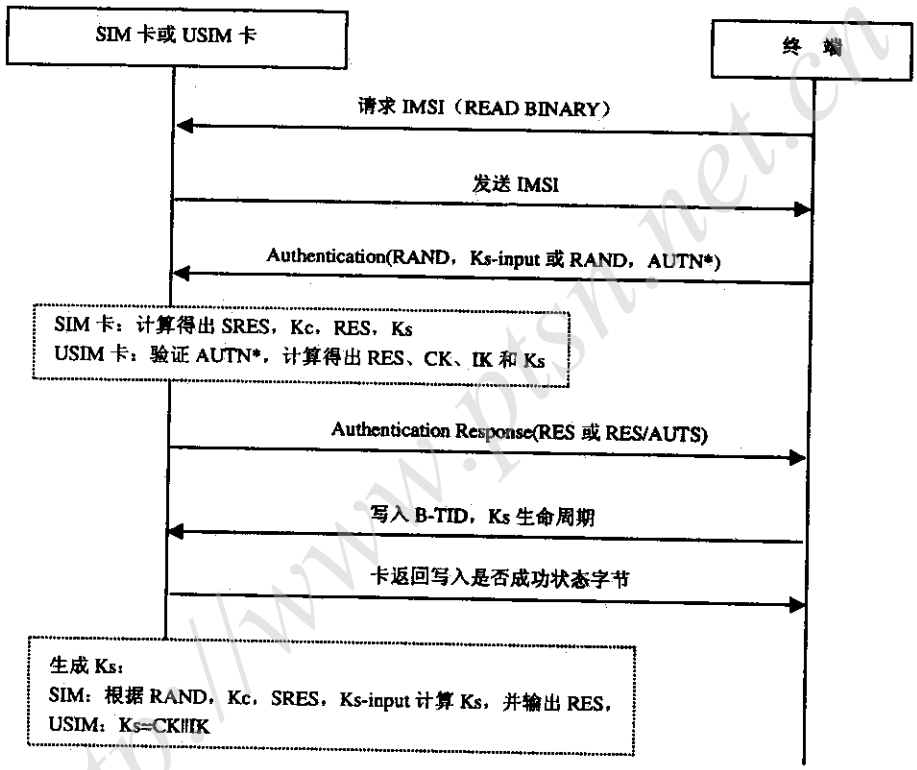

图8 GBA 初始化流程

流程说明：

（1）终端向卡发送读取EFimsi命令；

（2）卡向终端返回IMSI；

（3）终端向卡发送Authentication命令，数据域为RAND，Ks-input或RAND，AUTN；

（4）卡向终端返回如下响应数据，同时卡内保留Ks；

（5）SIM返回RES；

（6）USIM返回RES；

（7）终端向卡中写入B-TID，Ks生命周期；

（8）卡向终端返回写入是否成功状态字节。

9.2.1.2 MRK 请求过程

MRK请求过程如图9所示。

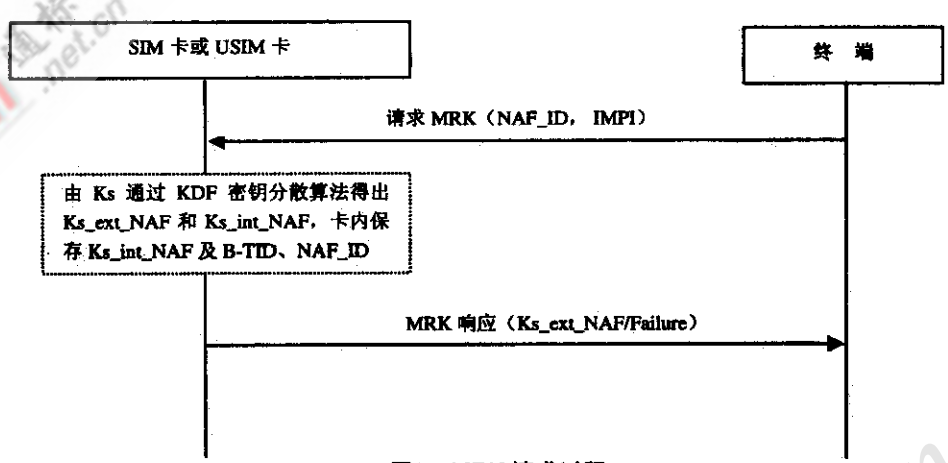

图9 MRK 请求过程

流程说明：

（1）终端向卡发送MRK命令，数据域为NAF_ID和IMPI；

（2）USIM利用Ks、分散因子NAF_ID、IMPI，并通过KDF分散算法计算出Ks_ext_NAF 和Ks_int_NAF，同时卡内存储Ks_int_NAF，并更新EFGBANL文件中的B-TID和 NAF_ID；

（3）卡向终端返回Ks_ext_NAF（MRK），用于网络对终端的认证。

9.2.1.3 MSK 更新过程

MSK更新过程如图10所示。

图10 MSK 更新过程

流程说明：

（1）终端从网络端接收到更新MSK的 MIKEY消息，并将MIKEY消息发送给USIM卡；

（2）USIM卡根据MIKEY消息中的MUK_ID找到对应的Ks_int_NAF，并使用Ks_int_NAF做为MUK解密得到MSK明文。之后卡内存储MSK，MSK Validity Time，同时更新EFmsk文件中的Domain ID、MSK ID；

（3）卡向终端返回消息处理状态字节。

9.2.1.4 MTK 生成过程

MTK生成过程如图11所示。

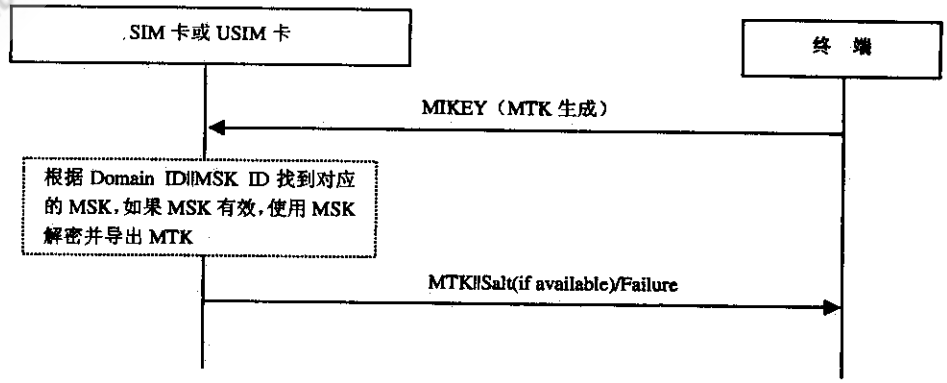

图11 MTK 生成过程

流程说明：

（1）终端从网络端接收到MTK MIKEY消息后，将MIKEY消息发送给USIM卡；

（2）USIM卡根据Domain ID||MSK ID找到对应的MSK，如果MSK有效，使用MSK解密并导出MTK；

（3）卡向终端返回MTK || Salt （可选）/ Failure。

9.2.2 终端对 MIKEY 消息的预处理

9.2.2.1 MSK MIKEY 消息

当终端接收到移动网络发送的MIKEY消息后，执行如下操作：

（1）检查扩展PAYLOAD（EXT），如果指示MSK更新过程，则从IDi和IDr中获取MUK ID；

（2）检查时间戳。终端读取EFMUK记录，并通过MUK ID索引到其对应的TS时间戳，如果MIKEY消息中的时间戳计数器小于或等于EFMUK文件中保存的TS，则终端认为是重发消息，丢弃该消息；

注：每次MSK更新成功时，USIM即更新EFMUK文件中对应MUK ID的时间戳。

（3）终端将MIKEY消息封装成APDU指令转发给USIM处理；

（4）USIM返回成功或失败状态字节。

9.2.2.2 MTK MIKEY 消息

当终端接收到广电网发送的MIKEY消息后，执行如下操作：

（1）检查扩展PAYLOAD（EXT），如果指示MTK更新过程，则从EXT中提取MSK ID；

（2）检查时间戳。终端读取EFMSK记录，并通过MSK ID索引到其对应的TS时间戳，如果MIKEY消息中的时间戳计数器小于或等于EFMSK文件中对应的TS，则ME认为是重发消息，丢弃该消息（可选项）；

（3）检查MTK ID是否有效。如果从EXT中提取的MTK ID小于或等于当前ME中保存的MTK ID值，则终端认为收到的是相同的MTK，丢弃该消息；（防止重发同样的MTK）

（4）终端将MIKEY消息封装成APDU指令转发给UICC处理；

（5）如果成功，UICC向终端返回MTK；否则返回错误信息。

9.3 3GPP2 体系的终端卡接口

9.3.1 终端与卡的交互流程

9.3.1.1 获取 SK（可选）

获取SK的流程如图12所示。

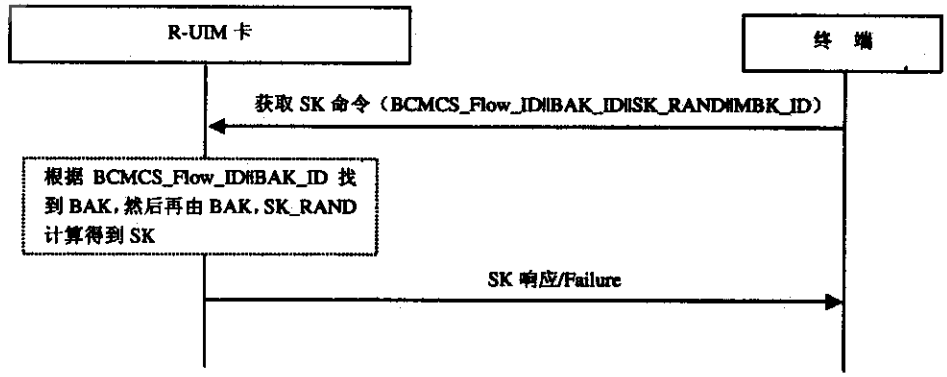

图12 获取 SK 流程

流程说明：

（1）当终端需要SK时，向UIM发送获取SK命令；

（2）R-UIM在指定文件中查找BCMCS_Flow_ID||BAK_ID记录，如果记录存在，且MBK_ID在BAK_Expire有效期范围内，则使用BCMCS_Flow_ID||BAK_ID对应的BAK计算SK；

（3）R-UIM向终端返回SK响应/失败消息。

9.3.1.2 更新 BAK

更新BAK的流程如图13所示。

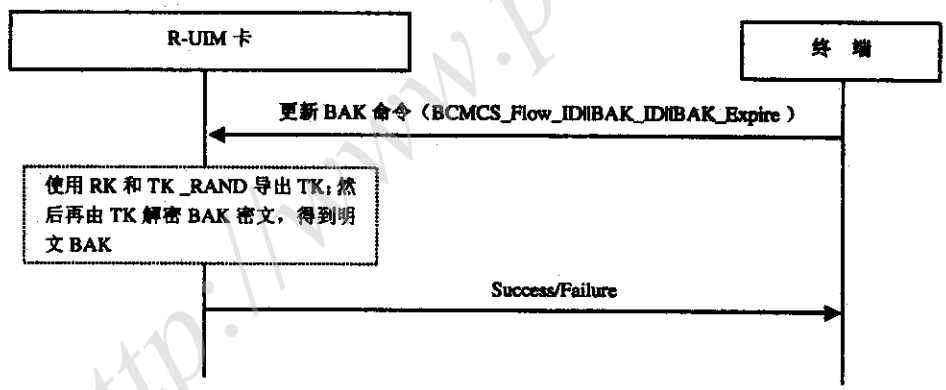

图13 更新 BAK 流程

注：在执行更新BAK之前，R-UIM和SM之间已共享RK密钥。

流程说明：

（1）终端从网络端接收到更新BAK命令后，将命令发送给R-UIM卡；

（2）R-UIM通过RK和给定TK_RAND导出TK；然后用TK对加密的BAK密文进行解密得到明文的BAK。最后在卡中保存该BAK及其三元组参数（BCMCS_Flow_ID，BAK_ID，BAK_Expire）；

（3）R-UIM向终端返回成功/失败消息。

9.3.1.3 删除 BAK

删除BAK的流程如图14所示。

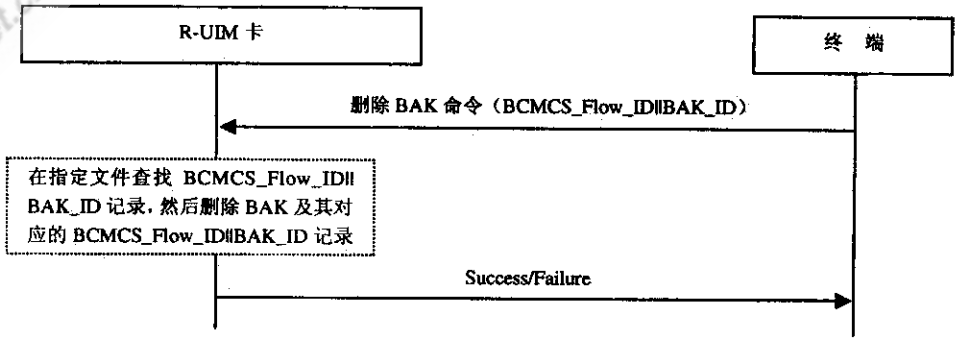

图14 删除 BAK 流程

流程说明：

（1）终端向R-UIM发送删除BAK命令；

（2）R-UIM在指定的文件中查找BCMCS_Flow_ID ||BAK_ID记录；然后删除BAK及其对应的BCMCS_Flow_ID||BAK_ID||BAK_Expire；

（3）R-UIM向终端返回成功/失败消息。

9.3.1.4 获取 SRTP SK

获取SRTP SK的流程如图15所示。

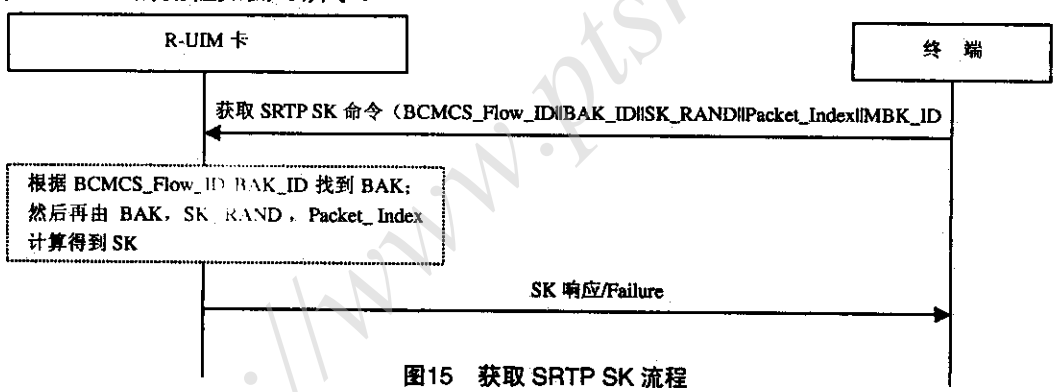

图15 获取 SRTP SK 流程

流程说明：

（1）当终端需要SRTP的SK时，向UIM发送获取SRTP SK命令；

（2）R-UIM 在指定文件中查找 BCMCS_Flow_ID||BAK_ID 记录，如果记录存在，且 MBK_ID 在 BAK_Expire 所指示的有效期范围内，则使用 BCMCS_Flow_ID||BAK_ID 对应的 BAK 及 SK_RAND，Packet_Index 计算得到 SK；

（3）R-UIM 向终端返回 SK 响应/失败消息。

9.3.1.5 生成认证签名（可选）

生成认证签名的流程如图16所示。

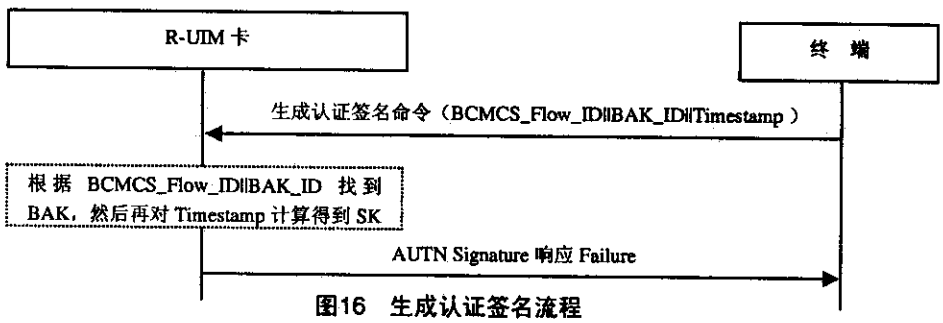

图16 生成认证签名流程

流程说明：

（1）终端向网络端发起BCMCS注册请求时，需要附上R-UIM生成的认证签名消息；

（2）R-UIM通过BCMCS_Flow_ID ||BAK_ID查找相应的BAK，然后通过EHMAC 算法对Timestamp计算得到认证签名；

（3）R-UIM向终端返回认证签名响应/失败消息。

9.3.1.6 BCMCS 认证

BCMCS认证的流程如图17所示。

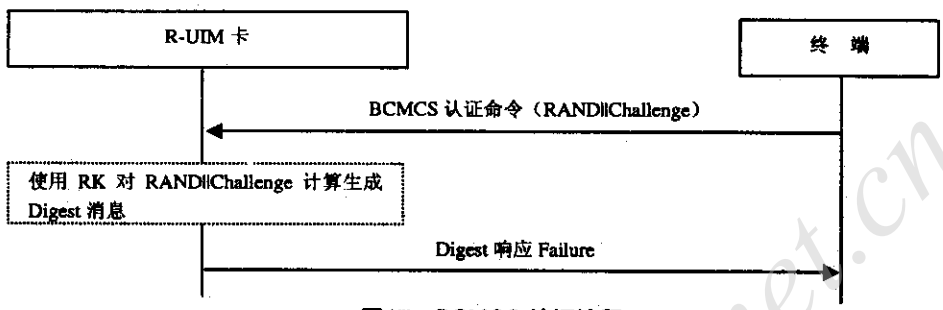

图17 BCMCS 认证流程

流程说明：

（1）终端向网络端发起BAK请求时，如果从网络侧接收到BCMCS认证质询（Challenge）后，终端将按照RAND = H（H（entity-body）| timestamp）算出一个RAND，并将其和网络侧发送的Challenge传给RUIM卡；

（2）R-UIM卡将按照3GPP2 3GPP2 S.S0055 中定义的f3算法使用RK和RAND算出一个密钥，这个密钥跟challege 一起作为输入算出Digest Response；

（3）R-UIM向终端返回Digest响应/失败消息。

10 用户卡

10.1 基本要求

移动多媒体广播终端用户卡应满足各制式SIM/USIM/R-UIM卡的基本要求，可见相应规范。本章主要分3GPP和3GPP2两个体系规定了相应的（U）SIM和R-UIM卡支持移动多媒体广播业务而应满足的要求。

10.2 SIM/USIM 卡

10.2.1 文件内容

本章将详细说明与移动多媒体广播相关的SIM/USIM卡基本文件，定义基本文件的访问条件、数据项及编码方式。SIM/USIM卡移动多媒体广播应用以外的其他文件内容，请参考相应行业标准或国际标准。

10.2.1.1 USIM ADF 应用下的文件

10.2.1.1.1 EF_{GBAPP}（GBA 引导参数）

EF_{GBAPP}包含GBA引导过程中AKA随机数（RAND）和引导业务标志（B-TID）。该文件是在支持GBA服务（服务68可用）条件下出现，服务在EF_{UST}（USIM服务列表）中分配。GBA引导参数EF_{GBAPP}描述见表2。

表2 GBA 引导参数 EF_{GBAPP}

文件标识符 '6FD6'	透明文件	必 须
记录长度 91 个字节	更新频率 低	
访问条件:		
READ	PIN	
UPDATE	PIN	
DEACTIVATE	ADM	
ACTIVATE	ADM	

字 节	描 述	M/O	长 度
1	RAND 长度	M	1 字节
2~(*X*+1)	RAND	M	16 字节
X+2	B-TID 长度	M	1 字节
(*X*+3) ~ (*X*+2+*L*)	B-TID	M	*L* 字节
X+*L*+3	Ks 生命周期的长度	M	1 字节
(*X*+*L*+4) ~ (*X*+*L*+*N*+3)	Ks 生命周期	M	8 字节

随机数长度:

— 随机数的字节数，不包括随机数长度字节。本规范定义随机数长度 16 字节。

随机数:

— 内容：在 GBA_U 引导过程中使用的随机数;

— 编码：见 3GPP TS 33.103。

B-TID长度:

— B-TID 的字节数，不包括长度本身，本规范定义 B-TID 长度不超过 64 字节。

B-TID:

— 内容：GBA_U 引导密钥的业务标识;

— 编码：见 3GPP TS 33.220。

密钥生命周期长度:

— 密钥生命周期字节数，不包括长度本身，本规范定义 Ks 生命周期不超过 8 字节。

密钥生命周期:

— 内容：GBA_U 引导密钥的生命周期;

— 编码：基于 1970 年 1 月 1 日 00：00：00 GMT 开始到该值为止的时间，单位为秒。

10.2.1.1.2 EF_{MSK}（业务密钥列表）

此文件每条记录中包含与移动多媒体广播服务相关的MSK密钥及参数，每一对Key Domain ID/Key Group ID 中至少存在两条MSK密钥。每条记录中两个4字节的MSK ID对应相同的2字节Key Group ID值。

该文件是在支持MBMS安全服务（服务69可用）条件下出现，服务在USIM服务列表文件EF_{UST}中分配，见表3。

表3 业务密钥列表 EF_{MSK}

文件标识符 '6FD7'	线性记录文件	必须
记录长度 20 个字节	更新频率 低	
访问条件： READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

字 节	描 述	M/O	长 度
1~3	密钥网络 ID	M	3 字节
4	MSK 密钥标识及其参数组数	M	1 字节
5~8	第一个 MSK ID	M	4 字节
9~12	第一个时间戳计数器（TS）	M	4 字节
13~16	第二个 MSK ID	M	4 字节
17 ~ 20	第二个时间戳计数器（TS）	M	4 字节

密钥网络ID：

— 内容：提供移动多媒体广播服务的 BM－SC 的网络标识；

— 编码：见 3GPP TS 33.246。

MSK密钥组数：

— 内容：一条记录中所包含的 MSK ID 和对应的 TS 的组数，3GPP TS 33.246 中有定义；

— 编码：二进制。

MSK ID：

— 内容：某一网络内的移动多媒体广播服务密钥标识；

— 编码：见 3GPP TS 33.246。

时间戳计数器（TS）：

— 内容：通过 MTK 传输过程更新，每个时间戳计数器与某一 MSK 相关；

— 编码：见 3GPP TS 33.246。

注： 本规范定义该文件为20条定长记录。当记录已满时，SIM卡或USIM将采用先进先出的原则覆盖原有的记录。

10.2.1.1.3 EF_{MUK} （用户密钥）

EF_{MUK}存放用户密钥（MUK）的标识，该MUK用于保护业务密钥的传输。EF_{MUK}同样含有与MUK相关的时间标识计数器，

该文件是在支持移动多媒体广播安全服务（服务69可用）条件下出现，该服务在EF_{UST}（USIM服务列表）中分配。用户密钥EF_{MUK}描述见表4。

表4 用户密钥 EF_{MUK}

文件标识符 '6FD8'	线性记录文件	必须
记录长度：103 个字节	更新频率 低	
访问条件： READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

描 述	值	M/O	长度（字节）
MUK ID Tag	'A0'	M	1
MUK ID 长度	X	M	1（注）
MUK IDr Tag	'80'	M	1
MUK IDr 长度	A	M	1（注）
MUK IDr 值	—	M	A
MUK IDi Tag	'82'	M	1
MUK IDi 长度	W	M	1（注）
MUK IDi 值	—	M	W
时间戳计数器 Tag	'81'	M	1
时间戳计数器长度	Y	M	1（注）
时间戳计数器值	—	M	4
注：长度编码可参考 ISO/IEC 8825			

MUK ID Tag 为 'A0'，它由IDr和 IDi组成：

— IDr Tag '80'：IDr 值编码见 3GPP TS 33.246，本规范定义其长度不超过 64 字节；

— IDi Tag '82'：IDi 值编码见 3GPP TS 33.246，本规范定义其长度不超过 27 字节。

时间戳计数器Tag '81'：

— 时间戳计数器，通过 MSK 传输过程更新，每个时间戳计数器与某一 MUK 相关，长度编码见 3GPP TS 33.246；

— 时间戳计数器值编码见 3GPP TS 33.246。

未使用的字节设置为 'FF'。

注：本规范定义该文件为20条定长记录。当记录已满时，SIM卡或USIM将采用先进先出的原则覆盖原有的记录。

10.2.1.1.4 EF_{GBANL}（GBA NAF 列表）

EF_{GBANL}包含与GBA NAF过程有关的NAF_ID和B-TID列表，见表5。该文件是在服务68可用条件下出现。

表5 GBA NAF 列表 EF_{GBANL}

文件标识符 '6FDA'	线性记录文件	必须
记录长度：100 个字节	更新频率 低	
访问条件：		
READ PIN		
UPDATE ADM		
DEACTIVATE ADM		
ACTIVATE ADM		

字 节	描 述	M/O	长 度
1~Z	NAF 密钥标识符 TLV 对象	M	Z 字节

NAF密钥标识符Tag的描述见表6。

表6 NAF 密钥标识符 Tag

描 述	Tag 值
NAF_ID Tag	80
B-TID Tag	81

NAF Key标识符信息见表7。

表7 NAF Key 标识符信息

描 述	值	M/O	长度（字节）
NAF_ID Tag	80	M	1
Length	X	M	1（注）
NAF_ID value	—	M	X
B-TID Tag	81	M	1
Length	Y	M	1（注）
B-TID value	—	M	Y
注：长度编码可参考 ISO/IEC 8825			

NAF-ID Tag '80'：

— 内容：网络应用功能标识，本规范定义其长度不超过 32 字节；

— 编码：见 3GPP TS 33.220。

B-TID Tag '81'：

— 内容：GBA_U 引导的密钥引导业务标识，本规范定义其长度不超过 64 字节；

— 编码：见 3GPP TS 33.220。

注：本规范定义该文件为20条定长记录。当记录已满时，SIM卡或USIM将采用先进先出的原则覆盖原有的记录。

10.2.1.2 文件映射关系

为支持2G终端移动多媒体广播功能，复合USIM卡中的SIM应用也应包含与移动多媒体广播业务相关的基本文件。即DFGSM目录下的 EFGBABP 、EFMSK、 EFMUK 和EFGBANL 4个文件应与USIM ADF应用下的对应文件互相映射。

10.2.2 命令

本节主要描述了与移动多媒体广播业务相关的命令和响应。其他命令及其响应的代码请见相应行业标准或国际标准。

10.2.2.1 鉴权命令（AUTHENTICATE）

10.2.3 命令描述

该命令被用于以下几种安全语境：

— 3G 安全语境：详细见相应行业标准或国际标准的 AUTHENTICATE 命令；

— GSM 安全环境：详细见《TD-SCDMA/WCDMA UICC——终端（Cu）接口技术要求第一部分：物理、电气和逻辑》定义的 AUTHENTICATE 命令；

— VGCS/VBS 安全语境：当获得 VGCS/VBS 鉴权数据时使用；

— GBA_U 安全语境：当请求 GBA 引导过程时使用；

— MBMS 安全语境：当请求 MBMS 安全过程时使用。

GBA_U安全语境支持两种模式：

— Bootstrapping 模式：USIM 和 BSF 之间相互认证，并且在 AKA 认证过程中获取引导密钥；

— NAF 分散模式：通过 Bootstrapping 模式生成的密钥，获得 NAF 专用密钥。

MBMS安全语境支持两种模式：

— MSK 更新模式：在此模式下更新 MBMS 服务密钥（MSK）；

— MTK 生成模式：在此模式下终端可获取 MBMS 传输密钥（MTK）解密媒体流。

10.2.3.1 3G 安全语境

详细见3GPP TS 31.102 章节7.1.1.1。

10.2.3.2 GSM 安全语境

详细见3GPP TS 31.102 章节7.1.1.2。

10.2.3.3 VGCS/VBS 安全语境

详细见3GPP TS 31.102 章节7.1.1.3。

10.2.3.4 GBA 安全语境（Bootstrapping 模式）

如果服务68可用，则USIM卡可支持GBA Bootstrapping模式。

USIM接收到RAND和AUTN（AUTN* = SQN ⊕ AK ‖ AMF ‖ MAC*）之后，首先计算匿名密钥AK = f5K （RAND），并获得SQN = （SQN ⊕ AK）⊕ AK。

USIM计算IK= f4K（RAND）和MAC（MAC= MAC* ⊕ Trunc（SHA-1（IK））见3GPP TS 33.220）。然后计算XMAC = f1K（SQN ‖ RAND ‖ AMF），并比较其是否与之前计算的MAC值相同。如果值不同，USIM返回9862，终止鉴权过程。

然后，USIM检查AUTH中的序列号SQN是否正确。如果序列号不正确，则同步失败，USIM终止鉴权过程。此时，命令返回AUTS，计算方法同UMTS安全语境。

如果序列号SQN在正确的范围内，USIM计算RES = f2K （RAND）和CK = f3K （RAND）。

Bootstrapping引导成功后，USIM内部保存CK和IK，同时在EFGBAPP文件中保存RAND值，并将RES最低位取反后发送给终端。

终端将接收到的RES发送给网络端进行认证，认证成功后，网络端返回B-TID、Ks生命周期，并由终端更新EFGBABP文件中的B-TID、Ks生命周期。

每次GBA引导过程之后，BSF和UICC共享Ks= CK‖IK。

Input：

— RAND、AUTN。

Output：

— RES/AUTS。

10.2.3.5 GBA 安全语境（NAF 分散模式）

如果服务68可用，则USIM卡可支持Bootstrapping模式。

USIM收到终端发送的NAF_ID 和 IMP之后，首先使用上一次GBA_U引导过程生成的共享密钥Ks，并通过KDF算法分散获得Ks_ext_NAF和 Ks_int_NAF，详细见3GPP TS 33.220。

如果USIM没有找到Ks，则认为上一次GBA_U引导失败，USIM终止鉴权过程，并返回6985。终端接收到此错误代码后，将重新发起GBA引导申请。

否则，USIM在卡内存储Ks_int_NAF密钥，更新EFGBANL 中的B-TID 和NAF_ID数据参数。并向终端返回Ks_ext_NAF（MRK）。

EFGBANL文件更新原则如下：

— 如果给定的 NAF_ID 记录已经存在，则 USIM 更新这条记录中相应的 B-TID；

— 如果给定的 NAF_ID 记录不存在，则 USIM 在一条空记录中保存 NAF_ID 及其 B-TID。

注： 根据3GPP TS 33.220，USIM可以同时包含几个Ks_int_NAF及其相对应的B-TID和NAF_ID。但每个NAF_ID仅对应一对Ks_int_NAF 和 B-TID。

Input：

— NAF_ID、IMPI。

Output：

— Ks_ext_NAF。

10.2.3.6 MBMS 安全语境 （MSK 更新模式）

USIM收到终端发来的MIKEY消息包后，首先判断是否为MSK更新消息，如果是则执行如下操作。

首先USIM从IDi和IDr中解析MUK ID，根据MUK ID来判断是否发生了一个新的NAF 分散过程（MRK）。如果是这样，USIM将使用最新生成的Ks_int_NAF做为MUK保存，同时按如下方式更新EFMUK文件内容：

如果IDi（包含在MUK ID中）对应的记录已经存在，则USIM将接收到MUK ID替代此记录中相应的数据域，并重置TS。另外，USIM内部保存上次成功使用过的MUK和MUK ID留做将来使用（检验密钥过期）。

如果IDi（包含在MUK ID中）对应的记录不存在，则USIM使用一条空记录保存MUK ID，并重置TS。

如果接收到的MUK ID与卡内上次产生的MUK不一致，则USIM执行如下操作：

如果接收到的MUK ID与上次成功使用过的MUK一致，则USIM使用此MUK校验消息的完整性。如果完整性校验失败，鉴权过程中止，USIM返回9862（MAC不正确）；如果完整性校验成功，鉴权过程也中止，USIM返回9865（密钥过期）。此时，USIM不会返回MIKEY校验包。

否则，USIM认为卡内保存的MUK不正确，鉴权过程中止，USIM返回6A88（密钥没找到）。

如果接收到的MUK ID与上次产生的MUK一致，USIM使用该MUK进行密钥分散并校验MSK MIKEY消息的完整性。如果完整性校验失败，鉴权过程中止，USIM返回9862（MAC不正确）。否则，USIM从KEMAC中解密获得MSK，并按如下方式保存MSK，更新EFMSK：

如果接收到的KEY Domain ID和KEY Group 在EFMSK记录中存在，则第2nd个MSK ID及其TS将被第1ST个MSK ID及其TS所替代。新的MSK ID被保存在第1ST个MSK ID的位置，其TS清零；

如果接收到的KEY Domain ID和KEY Group在EFMSK记录中不存在，则USIM使用一条空记录保存MSK ID。该MSK ID 保存在第1ST个MSK ID的位置，其TS被清零。

MSK更新以后，USIM从TS中解析出时间戳计数器，并更新EFMUK文件MUK ID对应的时间戳。

如果MIKEY包中不存在MSK密钥，则只更新MSK ID对应的KV值（Num=0x0除外）。

Input：

— MIKEY message（HDR，EXT，TS，RAND，IDi，IDr，KEMAC）。

Output：

— MIKEY message（HDR，TS，IDr，V）or None。

10.2.3.7 MBMS 安全语境 （MTK 生成模式）

USIM收到终端发来的MIKEY消息包后，首先判断是否为MTK消息，如果是则执行如下操作。

首先从EXT中解析出Key Domain ID||MSK ID，如果卡内没有找到对应的MSK，则USIM终止操作，并返回6A88（没有找到密钥）。如果EFMSK存在对应的Key Domain ID||MSK ID（可能存在两个），USIM以此查找对应的MSK和KV，并判断KV是否有效，如果SEQL>SEQU，则USIM终止操作，并返回6985（使用条件不满足）。

然后USIM从EXT中解析出MTK ID，判断MTK ID是否有效（当SEQL<MTK ID=<SEQU时有效）。当存在两个相同的MSK ID时，USIM须分别在两个KV区间判断MTK ID的有效性，且在一个KV 区间有效即认为MTK ID有效。如果MTK ID无效，则USIM终止操作，并返回9865（密钥过期）。

如果MTK ID有效，则USIM使用MSK进行密钥分散，验证MIKEY消息的完整性并解密得到MTK。如果完整性验证失败，则USIM终止操作，并返回9862（MAC错误）。

如果MIKEY完整性验证成功，则USIM使用MIKEY消息携带的MTK ID（SEQp）替代SEQL值。

然后，从TS中解析出时间戳计数器，并更新EFMSK文件MSK ID对应的时间戳（如存在两个相同的MSK ID，可根据KV值来确定更新哪一个TS）。

最后，USIM向终端输出MTK和Salt key（如果需要）。

Input：

— MIKEY message（HDR，EXT，TS KEMAC）。

Output：

— MTK and Salt （if available）。

10.2.4 命令参数和数据

CLA	在 3GPP TS 31.101 中规定
INS	88
P1	00
P2	见下表
LC	注 1
DATA	注 1
Le	响应数据的最大长度

P2参数说明如下：

编码 b8-b1	说　明
1--------	专用参数
------XXX	安全语境： 000 GSM 001 3G 010 VGCS/VBS 100 GBA 101 MBMS

注1：见3GPP TS 31.102的7.1.2。

10.2.4.1　GSM/3G 安全语境

详细见3GPP TS 31.102的7.1.2.1。

10.2.4.2　VGCS/VBS 安全语境

详细见3GPP TS 31.102的7.1.2.2。

10.2.4.3　GBA 安全语境　（Bootstrapping 模式）

字　节	描　述	长　度
1	‘GBA 安全语境引导模式’ 标签 ‘DD’	1
2	RAND 长度（*L*1）	1
3~（*L*1+2）	RAND	*L*1
（*L*1+3）	AUTN 长度（*L*2）	1
（*L*1+4）~（*L*1+*L*2+3）	AUTN	*L*2

GBA安全语境　（Bootstrapping模式）同步失败响应数据：

字　节	描　述	长　度
1	“同步失败” 标签 = ‘DC’	1
2	AUTS 长度（*L*1）	1
3 ~（*L*1+2）	AUTS	*L*1

GBA安全语境　（Bootstrapping模式）命令执行成功响应数据：

字　节	描　述	长　度
1	“GBA 操作成功” 标签 = ‘DB’	1
2	RES 长度（*L*）	1
3 ~（*L*+2）	RES	*L*

10.2.4.4　GBA 安全语境　（NAF 分散模式）

字　节	描　述	长　度
1	‘GBA 安全语境 NAF 分散模式’ 标签 ‘DE’	1
2	NAF_ID 长度（*L*1）	1
3~（*L*1+2）	NAF_ID	*L*1
（*L*1+3）	IMPI 长度（*L*2）	1
（*L*1+4）~ （*L*1+*L*2+3）	IMPI	*L*2

GBA安全语境（NAF分散模式）命令执行成功响应数据：

字 节	描 述	长 度
1	“成功执行 GBA 操作”标签 = ‘DB’	1
2	Ks_ext_NAF 长度（*L*）	1
3 ~（*L*+2）	Ks_ext_NAF	*L*

Ks_ext_NAF编码见3GPP TS 33.220。

10.2.4.5 MBMS 安全语境（适用于所有模式）

字 节	描 述	长 度
1	MBMS 安全语境，MSK 更新模式“01” MBMS 安全语境，MTK 生成模式“02”	1
2	MIKEY 消息长度（*L*1）	1
3~（*L*1+2）	MIKEY 消息	*L*1

MBMS安全语境（MSK更新模式）命令执行成功响应数据：

字节	描 述	长 度
1	“成功执行 MBMS 操作”标签 = ‘DB’ 见注释 1）	1
2	MIKEY 长度（*L*） （见注释 1）	1
3 ~（*L*+2）	MIKEY 消息 （见注释 1）	*L*
注释：如果返回 MIKEY 验证消息，此参数出现		

MBMS安全语境（MTK更新模式）命令执行成功响应数据：

字 节	描 述	长 度
1	“成功执行 MBMS 操作”标签 = ‘DB’	1
2	MTK 和 Salt 的长度（如果 Salt 密钥可获得）（*L*）	1
3 ~（*L*+2）	MTK‖Salt（如果 Salt 密钥可获得）	*L*

参数编码见3GPP TS 33.246。

10.2.4.6 USIM 返回状态条件

USIM返回SW1和SW2两个命令处理状态字节，除了在规范3GPP TS 31.101中定义的状态字以外，下表规定了状态字的编码。

10.2.5 安全管理

SW1	SW2	错误描述
‘98’	‘62’	鉴权错误，不正确的 MAC
‘98’	‘64’	鉴权错误，不支持 GSM 安全语境
‘98’	‘65’	密钥过期错误

10.2.6 命令状态字

Status Words	AUTHENTICATE
90 00	*
91 XX	*
93 00	
98 50	
98 62	*
98 64	*

表（续）

Status Words	AUTHENTICATE
98 65	*
62 00	*
62 81	
62 82	
62 83	
63 CX	
64 00	*
65 00	*
65 81	*
67 00	*
67 XX – （see note）	*
68 00	*
68 81	*
68 82	*
69 81	
69 82	*
69 83	
69 84	*
69 85	*
69 86	
6A 80	
6A 81	*
6A 82	
6A 83	
6A 86	*
6A 87	
6A 88	*
6B 00	*
6E 00	*
6F 00	*
6F XX – （see note）	*
NOTE：Except SW2 = ‘00’	

注：*表示AUTHENTICATE可能返回的状态字。

10.2.7 安全

10.2.7.1 密钥管理

基于UICC的密钥管理体系如图18如示。

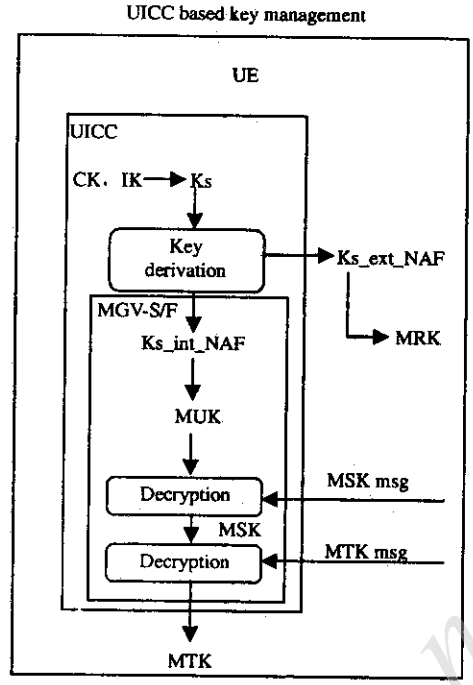

图18 基于UICC的密钥管理体系

终端通过运行GBA引导过程，可以在网络端和终端共享Ks_ext_NAF和Ks_int_NAF密钥。其中Ks_int_NAF做为MUK在卡内存储，用来解密由网络端发送过来的MSK密文消息；Ks_ext_NAF由终端发送给网络，用于网络对终端的身份认证。

网络端通过共享密钥MUK对MSK加密，然后以MIKEY Message消息格式发送给UICC，UICC解密得到MSK。

网络端通过共享密钥MSK对MTK加密，然后以MIKEY Message消息格式发送给UICC，UICC解密得到MTK。终端获得MTK后用来解密MBMS数据。

在上述密钥生成、存储过程中，MUK、MSK始终处于UICC专用的MGV-S/F安全存储区内；而网络和UE之间的密钥分发和更新都是采用密文方式传输的。

10.2.8 SIM 卡或 USIM 卡 2G 语境

10.2.8.1 适用范围

本章节定义的2G 移动多媒体广播业务适用于SIM卡或UICC平台的SIM应用。

10.2.8.2 2G 终端要求

支持移动多媒体广播业务的2G终端应满足以下要求：

（1）支持对SIM卡、UICC平台的USIM、ISIM和SIM应用的选择；

（2）支持两条扩展命令：AUTHENTICATE命令GBA模式和MBMS模式。

10.2.8.3 2G AUTHENTICATE 扩展命令

SIM卡或UICC SIM应用要求支持2G AUTHENTICATE扩展命令，该命令与3G AUTHENTICATE定义的GBA和MBMS两种安全语境和命令格式基本相同。所不同的是，2G AUTHENTICATE其命令类为A0。另外，2G GBA Bootstrapping机制不同于3G GBA下面具体进行描述。

10.2.8.3.1 2G_GBA 安全语境（Bootstrapping 模式）

当终端向网络侧发起2G_GBA请求时，HLR向BSF发送三元组的认证向量RAND，Kc，和SRES，BSF首先计算RES：

RES = KDF （key，“3gpp-gba-res”，SRES），结果取前128 bit

其中，key = Kc ‖ Kc ‖ RAND；

KDF是3GPP TS 33.220附录B定义的密钥分散函数。

然后，BSF产生128位的随机数Ks-input，并将RAND和Ks-input一起发送给终端。

当SIM卡或UICC SIM应用接收到终端发来的2G_GBA命令时（数据域为RAND‖Ks_input），SIM首先解析出RAND值，并计算SRES和 Kc（如果是SIM卡，其SRES 和Kc计算方法符合GSM11.11规范；如果是UICC SIM应用其SRES 和Kc计算方法同3G GSM语境）。然后按如下计算方法得出：

Ks = KDF（key，Ks-input，“3gpp-gba-ks”，SRES），长度为256 bit

RES= KDF（key，“3gpp-gba-res”，SRES），长度取前128 bit

其中：“3gpp-gba-ks”和“3gpp-gba-res”为字符串常数

key = Kc ‖ Kc ‖ RANDSIM卡或UICC SIM应用将Ks及RAND在卡内保存，并向终端回送RES。终端将RES发送给BSF，用于网络侧对终端的GBA鉴权认证。

如果BSF对RES认证成功，则网络侧向终端返回B-TID、Ks生命周期，并由终端更新EFGBABP文件中B-TID、Ks生命周期。

10.2.8.3.2 命令参数

Code	Value
CLA	A0
INS	‘88’
P1	‘00’
P2	见 P2 说明
Lc	注 1
Data	注 1
Le	‘00’，或数据返回的最大长度

P2参数说明如下：

编码 b8-b1	说　明
1--------	专用参数
------XXX	100 GBA 101 MBMS

注1：见 3GPP TS 31.102的7.1.2。

10.2.8.3.3 2G_GBA （Bootstrapping 模式）数据域

Byte（s）	Description	Length
1	“2G_GBA 安全语境引导模式” 标签 = ‘DD’	1
2	RAND 随机数长度	1
3 ~（*L*1+2）	RAND	*L*1
（*L*1+3）	BSF 产生的 Ks-input 长度 （*L*2）	1
（*L*1+4）~（*L*1+*L*2+3）	Ks-input	*L*2

注：这里 RAND 和 Ks-input 分别为 16 字节，与 3G GBA 数据域长度相同。

2G_GBA （Bootstrapping 模式）成功返回数据：

字 节	描 述	Length
1	“GBA 成功”标签 = ‘DB’	1
2	RES 长度 （*L*）	1
3 ~ （*L*+2）	RES	*L*

10.2.8.4 新增文件及定义

SIM卡：在DFGSM（7F20）目录下，增加EFGBABP 、EFMSK、 EFMUK 和EFGBANL四个基本文件，文件定义见本标准10.2.1.1。

UICC SIM应用：在DFGSM（7F20）目录下，增加EFGBABP 、EFMSK、 EFMUK和EFGBANL四个基本文件，文件定义见本标准10.2.1.1。这四个文件与USIM应用下的对应文件互相映射。

对DFGSM目录下的EFSST业务列表文件，新增定义如下：

业务No.50：GBA

业务No.51：MBMS

编码：

采用原有2bit编码方式，全部为1表示支持此业务。

注1：终端通过读取该文件，可获取SAM卡或复合USIM是否支持移动多媒体广播业务。

10.3 R-UIM 卡

10.3.1 文件内容

移动多媒体广播相关文件创建于 DF_{CDMA}目录，下面具体进行描述。

10.3.1.1 $EF_{BAKPARA}$（当前的 BAK 参数）

如果业务n°39可用，则要求创建此文件。

$EF_{BAKPARA}$中保存当前正在使用的BAK相关参数（BCMCS_Flow_ ID，BAK_ ID，BAK_Expire），可见3GPP2 3GPP2 C.S0023-C_v1.0。

文件标识符 ‘6F63’	定长记录文件	必选
记录长度 *X*+*Y*+*Z*+3 字节	更新频率 高	
访问条件：		
READ	CHV1	
UPDATE	ADM	
DEACTIVATE	ADM	
ACTIVATE	ADM	

字 节	描 述	M/O	长 度
1	BCMCS_Flow_ID 长度	M	1 字节
2~（*X*+1）	BCMCS_Flow_ID	M	*X* 字节
X+2	BAK_ID 长度	M	1 字节
（*X*+3）~（*X*+*Y*+2）	BAK_ID	M	*Y* 字节
X+Y+3	BAK 生命周期的长度	M	1 字节
（*X*+*Y*+4）~（*X*+*Y*+*Z*+3）	BAK 生命周期	M	*Z* 字节

说明：

BCMCS_Flow_ID长度：

— 内容：下述 BCMCS_Flow_ID 数据的字节数，不包括随机数长度字节。

— 编码：二进制。

BCMCS_Flow_ID：

— 内容：BCMCS 流标识。

— 编码：二进制。

BAK_ID长度：

— 内容：下述 BAK 标识的字节数，不包括长度字节。

— 编码：二进制。

BAK_ID：

— 内容：BAK 标识。

— 编码：二进制。

BAK密钥生命周期长度：

— 内容：密钥生命周期字节数，不包括长度本身。

— 编码：二进制。

BAK密钥生命周期：

— 内容：BAK 密钥生命周期。

— 编码：二进制。

10.3.1.2 $EF_{UpBAKPARA}$（最新的 BAK 参数）

如果业务n°39可用，则要求创建此文件。

$EF_{UpBAKPARA}$中包含最新写入到UIM中但当前还没有使用的BAK相关参数（BCMCS_Flow_ ID，BAK_ ID，BAK_Expire），可见3GPP2 3GPP2 C.S0023-C_v1.0。

文件标识符 '6F64'	循环记录文件	必选
记录长度 X+Y+Z+3 字节	更新频率 高	
访问条件： READ CHV1 UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

字 节	描 述	M/O	长度
1	BCMCS_Flow_ID 长度	M	1 字节
2~ （X+1）	BCMCS_Flow_ID	M	X 字节
X+2	BAK_ID 长度	M	1 字节
（X+3）~（X+Y+2）	BAK_ID	M	Y 字节
X+Y+3	BAK 生命周期的长度	M	1 字节
（X+Y+4）~（X+Y+Z+3）	BAK 生命周期	M	Z 字节

说明：

BCMCS_Flow_ID长度：

— 内容：下述 BCMCS_Flow_ID 数据的字节数，不包括随机数长度字节。

— 编码：二进制。

BCMCS_Flow_ID：

— 内容：BCMCS 流标识。

— 编码：二进制。

BAK_ID长度：

— 内容：BAK 标识的字节数，不包括长度字节。

— 编码：二进制。

BAK_ID：

— 内容：BAK 标识。

— 编码：二进制。

BAK密钥生命周期长度：

— 内容：密钥生命周期字节数，不包括长度本身。

— 编码：二进制。

BAK密钥生命周期：

— 内容：BAK 密钥生命周期。

— 编码：二进制。

10.3.2 命令

本节主要描述了在CDMA网络环境下，与移动多媒体广播业务相关的命令和响应。

10.3.2.1 BCMCS 命令描述

下述命令被用作BCMCS密钥管理，只有移动多媒体广播服务在CDMA服务列表中分配时，这些命令才可以使用。这里我们假定RK密钥已经安全地存储在R-UIM之中（SM与R-UIM共享此RK）。

命令	CLASS	INS	P1	P2	Lc	Le
BCMCS	A0	58	P1	P2	Lc	Le

P1参数：

P1	Class
'00'	获取 SK
'01'	更新 BAK
'02'	删除 BAK
'03'	获取 SRTP SK
'04'	生成认证签名
'05'	BCMCS 认证

10.3.2.2 获取 SK

10.3.2.2.1 命令描述

终端向R-UIM请求计算SK。

当R-UIM收到终端发送的“SK生成”命令时，将首先在EF（BAKPARA）中查找BCMCS_Flow_ID和BAK_ID记录，如果记录存在，则R-UIM使用对应的BAK通过f3算法计算SK。

否则，R-UIM在EF（UpBAKPARA）中查找BCMCS_Flow_ID和BAK_ID。如果对应记录存在，则R-UIM将其三元组参数（BCMCS_Flow_ID||BAK_ID|| BAK_Expire）复制到EF（BAKPARA）记录，且在卡内保存其对应的BAK。然后比较MBK_ID是否在BAK_Expire有效区间内，如果是，R-UIM使用该BAK通过f3算法计算SK，并向终端输出SK。如果MBK_ID不在BAK_Expire区间内，则USIM卡返回“6985”表示“使用条件不满足”。

如果上述两个文件中都没有BCMCS_Flow_ID和BAK_ID记录存在，则R-UIM返回“6A88”，表示“没有找到BAK密钥”错误。

SK计算方法见3GPP2 3GPP2 S.S0083-A_v1.0第4.5.4节。

输入：

— 服务类型 = '01'，表示“3GPP2 BCMCS”；

— BCMCS_Flow_ID；

— BAK_ID；

— SK_RAND；

— MBK_ID（节目流密钥标识）。

输出：

— SK。

10.3.2.2.2 命令格式

Code	Value
CLA	A0
INS	'58'
P1	'00'
P2	'01'
Lc	数据长度
Data	Service Type，BCMCS_Flow_ID，BAK_ID，SK_RAND，MBK_ID
Le	'12'

Data数据域：

字　节	描　述	长　度
1	Service Type = '01'（3GPP2 BCMCS）	1
2~*A*+1	BCMCS_Flow_ID TLV	*A*
A+2~*A*+*B*+1	BAK_ID TLV	*B*
A+*B*+2~*A*+*B*+*C*+1	SK_RAND TLV	*C*
A+*B*+*C*+2 ~*A*+*B*+*C*+5	MBK_ID TLV	4

TLV 对象的Tag编码定义在3GPP2 3GPP2 C.S0023-C_v1.0附件B。本标准新增MBK_ID，定义其 Tag为F0。

数据响应：

字　节	描　述	长　度
1~18	SK TLV	18

TLV 对象的Tag编码定义在3GPP2 3GPP2 C.S0023-C_v1.0附件B

10.3.2.3 更新BAK

10.3.2.3.1 命令描述

该命令要求R-UIM卡保存一个新的BAK。

当R-UIM卡收到终端发送的“更新BAK”命令时，首先从命令数据中提取出TK_RAND，利用在卡内保存的RK密钥根据f3算法计算出TK；然后用TK根据ESP_AES算法对加密的BAK进行解密得到明文BAK。最后R-UIM在卡内保存该BAK，同时在EF（UpBAKPARA）中保存与其对应的三元组（BCMCS_Flow_ID，BAK_ID和BAK_Expire）参数，同时在卡内保存对应的BAK。

TK计算方法见3GPP2 3GPP2 S.S0083-A_v1.0的第4.5.3。

BAK解密方法见3GPP2 3GPP2 S.S0083-A_v1.0的第4.5.2。

输入：

— 服务类型 = ‘01’，表示“3GPP2 BCMCS”；

— BCMCS_Flow_ID；

— BAK_ID；

— BAK_Expire；

— TK_RAND；

— 加密的 BAK（格式请参考 3GPP2 3GPP2 X.S0022-A 中的 8.3.3.2 节）。

输出：无。

10.3.2.3.2 命令格式

Code	Value
CLA	A0
INS	‘58’
P1	‘01’
P2	‘00’
Lc	数据长度
Data	ServiceType，BCMCS_Flow_ID，BAK_ID，BAK_Expire，TK_RAND，加密过的 BAK
Le	‘00’

Data数据域：

字节	描述	长度
1	Service Type = ‘01’（3GPP2 BCMCS）	1
2~*A*+1	BCMCS_Flow_ID TLV	*A*
A+2 ~*A*+*B*+1	BAK_ID TLV	*B*
A+*B*+2 ~*A*+*B*+*C*+1	BAK_Expire TLV	*C*
A+*B*+*C*+2 ~*A*+*B*+*C*+*D*+1	TK_RAND TLV	*D*
A+*B*+*C*+*D*+2~*A*+*B*+*C*+*D*+17	加密过的 BAK	16

TLV对象的Tag编码定义在3GPP2 3GPP2 C.S0023-C_v1.0附件B。

数据响应：无。

10.3.2.4 删除 BAK

10.3.2.4.1 命令描述

该命令要求R-UIM删除BAK以释放存储空间。此命令不能被用来终止用户定购关系。

当R-UIM卡收到终端发送的“删除BAK”命令时，则R-UIM首先在EF（BAKPARA）中查找与BCMCS_Flow_ID和BAK_ID相匹配的记录是否存在，如果对应记录存在，则R-UIM删除此记录，同时删除对应的BAK。如果对应记录不存在，则R-UIM继续在EF（UpBAKPARA）中查找与BCMCS_Flow_ID和BAK_ID相匹配的记录。如果对应记录存在，则R-UIM 删除此记录，同时删除与该BCMCS_Flow_ID和BAK_ID相对应的BAK。

输入：

— 服务类型 = ‘01’，表示“3GPP2 BCMCS”；

— BCMCS_Flow_ID；

— BAK_ID。

输出：无。

10.3.2.4.2 命令格式

Code	Value
CLA	A0
INS	‘58’
P1	‘02’
P2	‘00’
Lc	数据长度
Data	Service Type，BCMCS_Flow_ID，BAK_ID
Le	‘00’

Data数据域：

字 节	描 述	长 度
1	Service Type = ‘01’（3GPP2 BCMCS）	1
2~*A*+1	BCMCS_Flow_ID TLV	***A***
A+2~*A*+*B*+1	BAK_ID TLV	***B***

TLV 对象的Tag编码定义在3GPP2 3GPP2 C.S0023-C_v1.0附件B。

返回数据：无。

错误返回值：

状 态	描 述
‘9402’	无效的 BAK ID
‘9404’	无效的 BCMCS Flow ID

10.3.2.5 获取 SRTP SK

10.3.2.5.1 命令描述

该命令要求R-UIM计算与BCMCS_Flow_ID相关的SRTP SK。在这个过程中，R-UIM需要通过BCMCS_Flow_ID和BAK_ID查找BAK，然后由BAK通过SK_RAND和Packet_Index导出相应的SRTP SK。

首先在EF（BAKPARA）中查找BCMCS_Flow_ID和BAK_ID记录，如果记录存在，则比较MBK_ID是否在BAK_Expire的有效区间内，如果是，则使用对应的BAK及SK_RAND、Packet_Index（生成过程密钥的参量）计算SRTP SK。如果MBK_ID不在BAK_Expire区间内，则R-UIM卡返回“6985”，表示“使用条件不满足”。

否则，R-UIM在EF（UpBAKPARA）中查找BCMCS_Flow_ID和BAK_ID。如果对应记录存在，则R-UIM将其三元组参数（BCMCS_Flow_ID‖BAK_ID‖ BAK_Expire）复制到EF（BAKPARA）一条空记录中，且在卡内保存其对应的BAK。然后比较MBK_ID是否在BAK_Expire有效区间内，如果是，则R-UIM使用对应的BAK及SK_RAND、Packet_Index计算SK。如果MBK_ID不在BAK_Expire区间内，则USIM卡返回“6985”表示“使用条件不满足”。

如果上述两个文件中都没有BCMCS_Flow_ID和BAK_ID对应的记录存在，则R-UIM返回“6A88”，表示“没有找到BAK密钥”。

10.3.2.5.2 命令格式

CLA	A0
INS	58
P1	03
P2	01
LC	命令数据长度
DATA	Service Type，MBK_ID，BCMCS_FLOW_ID，BAK_ID，SK_RAND，Packet_Index
Le	12

DATA数据域：

字　节	描　述	长　度
1	Service Type = ‘01’（3GPP2 BCMCS）	1
2~*A*+1	BCMCS_FLOW_ID TLV	*A*
A+2~*A*+*B*+1	BAK_ID TLV	*B*
A+*B*+2~*A*+*B*+*C*+1	SK_RAND TLV	*C*
A+*B*+*C*+2~*A*+*B*+*C*+*D*+1	Packet Index TLV	*D*
A+*B*+*C*+*D*+2~*A*+*B*+*C*+*D*+5	MBK_ID TLV	4
注：TLV 结构的 Tag 值请参考 3GPP2 3GPP2 C.S0023-C_v1.0 的附录 B		

响应数据：

字　节	描　述	长　度
1~18	SRTP SK TLV	18
注：TLV 结构的 Tag 值请参考 3GPP2 3GPP2 C.S0023-C_v1.0 的附录 B		

10.3.2.6 生成认证签名

10.3.2.6.1 命令描述

该命令要求R-UIM生成一个认证签名。

为了认证终端是否有权访问某些广播数据流，业务系统需要向终端请求一个授权签名，为此终端要求R-UIM计算出与BCMCS_Flow_ID相应的认证签名。在这个过程中，R-UIM需要通过BCMCS_Flow_ID和BAK_ID查找BAK，然后通过EHMAC 算法对Timestamp计算得到认证签名。

10.3.2.6.2 命令格式

CLA	在 3GPP TS 31.101 中规定
INS	58
P1	04
P2	00
LC	命令数据长度
DATA	Service Type，BCMCS_Flow_ID，BAK_ID，Timestamp
Le	06

DATA数据域：

字节数	描 述	长 度
1	Service Type = '01'（3GPP2 BCMCS）	1
2~*A*+1	BCMCS_Flow_ID TLV	*A*
A+2~*A*+*B*+1	BAK_ID TLV	*B*
A+B+2~*A*+*B*+*C*+1	Timestamp TLV	*C*
注：TLV 结构的 Tag 值请参考 3GPP2 3GPP2 C.S0023-C_v1.0 附录 B		

响应数据：

字节数	描 述	长 度
1~6	Auth Signature TLV	6
注：TLV 结构的 Tag 值请参考 3GPP2 3GPP2 C.S0023-C_v1.0 的附录 B		

10.3.2.7 BCMCS 认证

10.3.2.7.1 命令描述

终端向R-UIM请求计算摘要响应（Digest Response）。R-UIM需要使用卡内保存的BCMCS RK来执行该计算。

10.3.2.7.2 命令格式

名 称	值
CLA	A0
INS	'58'
P1	'05'
P2	'00'
Lc	命令数据长度
Data（数据段）	RAND，Challenge
Le	'12'

DATA数据：

字节数	描 述	长 度
1	Service Type = '01'（3GPP2 BCMCS）	1
2~*A*+1	RAND TLV	*A*
A+2~*A*+*B*+1	Challenge TLV	*B*
注：TLV 结构的 Tag 值请参考 3GPP2 3GPP2 C.S0023-C_v1.0 的附录 B		

响应数据：

字节数	描　述	长　度
1~18	Digest Response TLV	18
注：TLV 结构的 Tag 值请参考 3GPP2 3GPP2 C.S0023-C_v1.0 的附录 B		

10.3.3　错误状态字与处理

终端应支持3GPP2 C.S0023-C V1.0和本规范中定义的错误状态字，主要有：

（1）如果MBK_ID不在BAK_Expire区间内，则R-UIM卡返回“6985”，表示“使用条件不满足”；

（2）执行获取SK、获取SRTP SK、生成认证签名命令时，R-UIM需要通过BCMCS_Flow_ID和BAK_ID查找BAK，如果在EF（BAKPARA）和EF（UpBAKPARA）两个文件中都没有BCMCS_Flow_ID和BAK_ID对应的记录存在，则R-UIM返回“6A88”，表示“没有找到BAK密钥”；

（3）执行删除BAK命令时，如果在EF（UpBAKPARA）中也没有找到与BCMCS_Flow_ID和BAK_ID相匹配的BAK记录，则R-UIM返回“9402”，表示无效的BAK ID；或者返回“9404”，表示无效的BCMCS Flow ID（注：这两错误状态字可能基本不会用到）。

（4）当有其他不可预期的“其他类型错误”时，使用错误状态字“6FF0”。

终端针对R-UIM卡返回的以上错误/异常状态码的处理流程：

（1）如果R-UIM卡返回“6985”，表示目前不在该节目的播报时间段内，终端应相应提示用户。

（2）如果返回的是“6A88”，可能是因为用户未定购或者已订购但未进行BAK更新，终端应该能够向网络询问用户是否已经订购该业务，如果是未定购，应提示用户“该业务未定购，是否要订购”，点击“确认”的话应进入订购流程，并由用户请求密钥；如果已定购，终端应向网络请求BAK更新。

11　电磁兼容性

GSM（GPRS）移动台应满足YD 1032-2000的要求。

CDMA移动台应满足GB 19484.1-2004的要求。

TD-SCDMA终端应满足YD/T 1592.1-2007的要求。

WCDMA终端应满足YD/T 1595.1-2007的要求。

cdma2000终端应满足YD/T 1597.1-2007的要求。

12　环境适应性

移动台应满足YD/T 1539-2006的要求。

13　电池及充电器

13.1　电池性能

各种锂离子电池性能应满足GB/T 18287-2000的要求；

各种金属氢化物镍电池性能应满足GB/T 18288-2000的要求；

各种金属镉镍电池性能应满足GB/T 18289-2000的要求。

各种锂电池安全要求应满足YD 1268-2003的要求。

13.2　充电器安全性

充电器的安全性应满足YD/T 965-1998和YD 1268-2003的要求。

参 考 文 献

1. OMA-RD-BCAST-V1_0-20080226-C；
2. OMA-AD-BCAST-V1_0-20080226-C。

http://www.ptsn.net.cn