ICS 33 060 99
M 37

YD

中华人民共和国通信行业标准

YD/T 1168-2007
代替 YD/T 1168-2001

CDMA 数字蜂窝移动通信网 用户识别模块（UIM）技术要求

Technical Specification CDMA Digital Cellular Mobile Communication Network User Identify Module(UIM)

2007-05-16 发布　　2007-05-16 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是CDMA数字蜂窝移动通信网用户识别模块（UIM）系列标准之一。该系列标准的名称及结构如下：

1．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》

2．YD/T 1682-2007《CDMA数字蜂窝移动通信网用户识别模块（UIM）测试方法》

3．YD/T 1683-2007《CDMA数字蜂窝移动通信网移动设备（ME）与用户识别模块（UIM）间接口测试方法》

本标准与YD/T 1682-2007《CDMA数字蜂窝移动通信网用户识别模块（UIM）测试方法》和YD/T 1683-2007《CDMA数字蜂窝移动通信网移动设备（ME）与用户识别模块（UIM）间接口测试方法》配套使用。

本标准代替YD/T 1168-2001《800MHz数字蜂窝移动通信网用户识别模块（UIM）技术要求》。相对于YD/T 1168-2001，本标准增加了与HRPD相关的内容以及与BCMCS相关的内容，以适应新的网络的要求。具体修订内容如下：

第4.4.4节更新为AKA（鉴权与密钥协商）过程和功能。

删除了4.9节及4.10节原保留的章节。

第5.5节增加了5.5.37、5.5.39-5.5.83节对应的基本文件的定义及描述，5.5.38节EF（ECC）标识符更新为6F47。

增加了5.6节分组数据安全相关参数的编码。

增加了5.7节在IETF协议中使用的共享保密数据的编码。

增加了5.8节对多模卡的要求。

第6.3.2节OTASP/OTAPA请求/响应消息增加了6.3.2.13至6.3.2.25节对应的13个请求/响应消息。

第6.5节增加了6.5.10到6.5.22节对应的13个OTASP/OTAPA命令描述。

增加了6.7节与数据包安全相关的功能描述。

增加了6.8节与分组数据安全相关的命令。

增加了6.9节BCMCS命令。

增加了6.10节应用鉴权命令的描述。

增加了6.11节与AKA相关的功能描述。

增加了6.12节AKA命令描述。

增加了第8章BCMCS过程。

本标准在技术内容上与3GPP2 C.S0023-C Ver1.0“扩频系统 可移动用户识别模块”保持一致。

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、中国联合通信有限公司

本标准主要起草人：刘东明、潘　娟、严　砥、邹　欣

本标准于2001年首次发布，本次为第一次修订。

CDMA数字蜂窝移动通信网用户识别模块（UIM）技术要求

1 范围

本标准规定了CDMA数字蜂窝移动通信网用户识别模块（UIM）的技术要求，内容包括UIM的物理、电气和逻辑特性、多模式UIM的文件结构，UIM的鉴权和安全，空中接口程序和BCMCS过程。本标准不包含UIM-ME应用工具箱的内容。

本标准适用于CDMA数字蜂窝移动通信网用UIM卡及机卡分离式CDMA（IS-95）、CDMA 1x和cdma2000数字移动台，以及具有CDMA 1x、cdma2000功能的机卡分离式双模或多模数字移动台。

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 RFC 2486	网络接入标识（NAI）
IETF RFC 3261	SIP：会话初始化协议
IETF RFC 3629	UTF-8，ISO10646的一种转换格式
ETSI TS 131.102	UMTS USIM应用特性
ETSI TS 102 221	智能卡：UICC—终端接口物理逻辑特性
3GPP2 C.S0015-B	扩频系统的短消息业务
3GPP2 C.S0005-D	cdma2000扩频系统层三信令标准
3GPP2 C.S0016-C	扩频系统移动台OTA业务预置（OTASP）
3GPP2 C.S0024-0	cdma2000高速分组数据空中接口规范
3GPP TS 51.011	终端：SIM-ME接口规范（Release 4）
3GPP2 S.S0053-0	通用密钥算法
TSG-X.S0016	MMS第二阶段，功能描述
TIA -95-B	宽带扩频蜂窝系统的移动台—基站兼容性标准

3 缩略语

下列缩略语适用于本标准。

A-KEY	Authentication key	鉴权密钥
AC	Authentication Center	鉴权中心
AKA	Authentication Key Agreement	鉴权与密钥协商
AN	Access Network	接入网
AT	Access Terminal	接入终端
AUTS	Automatic Update Transaction System	自动更新传输系统
BCMCS	BroadCast MultiCast Service	组播、多播业务
BAK	BCMCS Access Key	BCMCS接入秘钥
CAVE	Cellular Authentication Voice Ecryption	蜂窝鉴权与话音加密

CHAP	Challenge Handshake Authentication Protocol	询问握手鉴权协议
CHV	Card Holder Verification	持卡人校验信息
CRC	Cyclic Redundancy Code	循环冗余编码
DF	Dedicate File	专用文件
EAP	Extensible Authentication Protocol	可扩展鉴权协议
ECMEA	Enhanced Cellular Message Ecryption Algorithm	增强的分组加密算法
EF	Elementary File	基本文件
ESN	Electronic Serial Number	电子序列号
EUIMID	Expanded R-UIM Identifier	扩展的R-UIM标识符
HLR	Home Location Register	归属位置寄存器
ICC	Integrated Circuit Card	集成电路卡
ICCID	ICC Identification	ICC标识
IMAP	Internet Message Access Protocol	互联网信息访问协议
IMS	IP Multimedia Service	IP多媒体业务
IMSI	International Mobile Station Identity	国际移动台标识
LSB	Least Significant Bit	最低有效位
MAC	Message Authentication Code	消息鉴权码
MCC	Mobile Country Code	移动国家代码
MDN	Mobile Directory Number	移动目录号码
ME	Mobile Equipment	移动设备
MEID	Mobile Equipment Identifier	移动台识别码
MF	Master File	主文件
MIN	Mobile Identification Number	移动识别号码
MNC	Mobile Network Code	移动网络代码
M/O	Mandatory/Optional	必选/可选
MS	Mobile Station	移动台（包含ME和UIM卡）
MSB	Most Significant Bit	最高有效位
NAI	Network Access Identifier	网络访问标识
NAM	Number Assignment Module	号码分配模块
NID	Network Identification	网络识别码
OTAF	Over-the-Air Service Provisioning Function	空中下载业务准备功能
OTAPA	Over-the-Air Parameter Administration	空中下载参数管理
OTASP	Over-the-Air Service Provisioning	空中下载业务准备
P-CSCF	Proxy Call Session Control Function	代理呼叫会话控制功能
P-ESN	Pseudo-Electronic Serial Number	伪电子序列号
P-UIMID	Pseudo-UIMID	伪UIMID
PRL	Preferred Roaming List	首选漫游列表
R-UIM	Removable User Identify Module	可移动用户识别模块
RFU	Reserved for Future Use	保留用于将来的使用
SIM	Subscriber Identify Module	用户识别模块

SIP	Session Initialization Protocol	会话初始协议
SMCK	Secure Mode Ciphering Key	安全模式加密密钥
SPASM	Subcriber Parameter Administration Security Mechanism	用户参数管理安全机制
SPC	Service Programming Code	业务编程代码
SRTP	Secure Real-time Transport Protocol	安全实时传输协议
SSD	Shared Secret Data	共享保密数据
SID	System Identification	系统识别码
SIP	Session Initialization Protocol	会话初始协议
SSPR	System Selection for Preferred Roaming	首选漫游的系统选择
TMSI	Temporary Mobile Station Identity	临时移动台标识
UAK	User Authentication Key	用户鉴权密钥
UIM	User Identify Module	用户识别模块
URI	Universal Resource Identifier	惟一资源标识符
UTK	UIM Toolkit	UIM卡应用工具箱
VPM	Voice Privacy Mask	话音加密掩码

4 物理、电气和逻辑特性

4.1 物理接口

R-UIM 卡的物理特性应遵循 3GPP TS 51.011 相关章节的定义，见表 1。

表1 物理特性

章 节	标 题
4	物理特性
4.1	ID-1 UICC
4.2	嵌入式 UICC 卡
4.3	卡工作的温度范围
4.4	触点
4.4.2	触点激活与去活
4.4.3	非激活的触点
4.4.4	触点压力

4.2 电气接口

R-UIM 卡的电气特性遵循 3GPP TS 51.011 相关章节的定义。表 2 为 3GPP TS 51.011 中对应的章节。

表2 电信号和传输协议

章 节	标 题
5	电信号和传输协议
5.1	电气特性
5.2	初始通信建立过程
5.2.1	对于速率增强的错误处理
5.3	传输协议
5.4	时钟

支持 A 类以外的电压类别的终端和 R-UIM 应至少支持 2 个连续的电压类别，即 A 类和 B 类，或 B 类和 C 类。

4.3 逻辑接口

R-UIM 卡的逻辑接口应遵循 3GPP TS 51.011 相关章节的定义，见表 3。用于 CDMA 的专用文件的文件标识符（ID）是‘7F25’。

表3 逻辑模型

章 节	标 题
6	应用和文件结构
6.1	SIM 应用结构
6.4	文件类型
6.4.1	专用文件（DF）
6.4.2	基本文件（EF）
6.4.2.1	循环 EF
6.5	选择文件的方法

4.4 安全特性

与安全相关的过程和协议定义见第6章。

4.4.1 鉴权和密钥产生过程

见6.1和6.2节。

4.4.2 算法及处理

针对ANSI—41语音网络鉴权，R-UIM卡使用的是CAVE算法（见6.2节）；对于HRPD网络接入鉴权，R-UIM卡中的CDMA业务表EF_{CST}中的HRPD业务n5置为‘11’时（见5.4.18节注释）。R-UIM卡使用的是CHAP MD5算法，否则采用CAVE算法（见6.7节）。

4.4.3 文件访问条件

R-UIM 卡的文件访问条件应遵循 GSM11.11 中相关章节的定义，见表 4。

表4 文件访问条件

章 节	标 题
7．3	文件访问条件

4.4.4 AKA（鉴权与密钥协商）过程和功能

见6.11和6.12。

4.5 功能描述

R-UIM卡的功能应遵循3GPP TS 51.011中相关章节的定义，见表5。对于ANSI-41网络，在第6章使用了如下功能：Base Station Challenge、Update SSD、Confirm SSD、Run CAVE、Generate Key/VPM和Store ESN_MEID_ME。这些功能适用于CDMA模式，其他模式不在本标准中描述。只有在DF_{CDMA}或者DF_{CDMA}的子目录被选择为当前的目录并且成功执行了CHV1的验证后，这些功能才可以执行。

表5 功能描述

章 节	标 题
8	功能描述
8.1	SELECT
8.2	STATUS
8.3	READ BINARY
8.4	UPDATE BINARY

表5（续）

章　节	标　题
8.5	READ RECORD
8.6	UPDATE RECORD
8.7	SEEK
8.8	INCREASE
8.9	VERIFY CHV
8.10	CHANGE CHV
8.11	DISABLE CHV
8.12	ENABLE CHV
8.13	UNBLOCK CHV
8.14	INVALIDATE
8.15	REHABILITATE
8.17	SLEEP
8.18	TERMINAL PROFILE
8.19	ENVELOPE
8.20	FETCH
8.21	TERMINAL RESPONSE

4.6　命令描述

R-UIM 卡使用的命令应遵循 3GPP TS 51.011 相关章节的定义，见表 6。用于运行 CAVE 算法的命令描述见 6.4.4 节。

表6　命令描述

章　节	标　题
9	命令描述
9.1	映射原则
9.2	命令代码
9.2.1	SELECT
9.2.2	STATUS
9.2.3	READ BINARY
9.2.4	UPDATE BINARY
9.2.5	READ RECORD
9.2.6	UPDATE RECORD
9.2.7	SEEK
9.2.8	INCREASE
9.2.9	VERIFY CHV
9.2.10	CHANGE CHV
9.2.11	DISABLE CHV
9.2.12	ENABLE CHV
9.2.13	UNBLOCK CHV
9.2.14	INVALIDATE
9.2.15	REHABILITATE
9.2.17	SLEEP
9.2.18	GET RESPONSE

表 6（续）

章　节	标　题
9.2.19	TERMINAL PROFILE
9.2.20	ENVELOPE
9.2.21	FETCH
9.2.22	TERMINAL RESPONSE
9.3	定义和编码
9.4	卡返回的状态条件
9.4.1	命令正确执行的响应
9.4.2	命令推迟执行的响应
9.4.3	内存管理
9.4.4.	定位管理
9.4.5	安全管理
9.4.6	与应用无关的错误
9.4.7	命令对应的可能的状态响应

INCREASE 命令按照 ETSI TS 102 221 中的定义进行编码，但有以下几点不同：

- Class=“A0”；
- P1，P2=“00；”
- P3=“所选循环文件的记录长度”。

响应命令的参数见 ETSI TS 102 221。

在 DF_{CDMA} 情况下的响应参数/数据：

字　节	描　述	长　度
1～2	RFU	2
3～4	在所选目录下未分配的内存的大小	2
5～6	文件ID	2
7	文件类型	1
8～12	RFU	5
13	后跟数据的长度	1
14～34	CDMA特有的数据	21

CDMA 特有的数据：

字　节	描　述	长　度
14	文件特性	1
15	当前目录下直接子 DF 的数目	1
16	当前目录下直接子 EF 的数目	1
17	CHV、UNBLOCK CHV 和行政管理代码的数量	1
18	RFU	1
19	CHV1 的状态	1
20	UNBLOCK CHV1 的状态	1
21	CHV2 的状态	1
22	UNBLOCK CHV2 的状态	1
23	RFU	1
23～34	保留用于行政管理	0≤lgth≤11

字节 1 到字节 22 为必选项，R-UIM 必须返回这些字节。字节 23 和后续的字节为可选项，R-UIM 可以不返回这些字节。

对于以上字节，R-UIM 必须遵从 3GPP TS 51.011 中 9.2.1 节的定义。

R-UIM 供电电压的识别：

支持B类和C类操作条件的R-UIM应支持3GPP TS 51.011中9.2.1节定义的供电电压指示。下表列出了CDMA中与GSM等价的命令。

GSM 命令	CDMA等价命令
SELECT GSM	SELECT CDMA

4.7 EF 文件的内容

R-UIM中的EF文件应包含在表7中所列的3GPP TS 51.011中的相关章节的内容。

表7 EF 文件的内容

章　节	标　题
10.1	MF级EF的内容
10.1.1	EF_{ICCID}（ICC标识符）
10.2	GSM应用级的DF
10.5	电信级文件内容
10.5.1	EF_{ADN}（缩位拨叫号码）（注1）
10.5.2	EF_{FDN}（固定拨叫号码）（注1、注2）
10.5.8	EF_{LND}（最后拨叫的号码）（注1）
10.5.9	EF_{SDN}（业务拨叫号码）（注1）
10.5.10	EF_{EXT1}（扩展1）（注1）
10.5.11	EF_{EXT2}（扩展2）（注1）
10.5.12	EF_{EXT3}（扩展3）（注1）
10.6	电信级DF
10.6.1	电信图形级文件内容
10.6.1.1	EF_{IMG}（图像）
10.6.1.2	图像实例数据文件

注1：存储号码的格式和3GPP TS 51.011一样。

注2：参考3GPP TS 51.011附录B中FDN过程，下表为在FDN模式下涉及的GSM文件对应的CDMA文件。

GSM 文件	CDMA等效文件
DF_{GSM}	DF_{CDMA}
EF_{LOCI}	EF_{TMSI}
EF_{IMSI}	EF_{IMSI_M}，EF_{IMSI_T}

R-UIM 可选提供增强的电话簿，即在 ETSI TS 131.102 中定义的在 $DF_{TELECOM}$ 下的 $DF_{PHONEBOOK}$。$DF_{PHONEBOOK}$ 可包含表 8 中所列的 ETSI TS 131.102 中的相关章节，但有以下几点不同之处：

- PIN 对应 CHV1，PIN2 对应于 CHV2；
- SFI 不适用于 R-UIM。

如果存在 $DF_{PHONEBOOK}$ 文件，则应有 EF_{ADF} 和 EF_{PBR} 两个文件。

为了保证终端间的互操作，$DF_{PHONEBOOK}$ 下的第一个 AND 和 EXT1 文件被指向 $DF_{TELECOM}$ 下对应的文件，也就是 EF_{ADN}= ‘6F3A’，EF_{EXT1}= ‘6F4A’。这样可以保证 $DF_{PHONEBOOK}$ 下的文件和 $DF_{TELECOM}$ 下

的文件保持同步。

在 ETSI TS 131.102 中 4.4.2.14 节对电话簿的限制要求也适用于 R-UIM。

表8 支持增强电话簿的 R-UIM 中的 EF 内容

章 节	标 题
4.4.2.1	EFPBR（电话簿参考文件）
4.4.2.2	EFIAp（电话簿索引管理）
4.4.4.3	EFADN（缩位拨号）
4.4.4.4	EFEXT1（扩展1）
4.4.4.6	EFGRP（组文件）
4.4.4.7	EFAAS（附加号码字符串）
4.4.4.8	EFGAS（组信息字符串）
4.4.4.9	EFANR（附加号码）
4.4.4.10	EFSNE（别名项）
4.4.4.13	EFEMAIL（E-mail地址）

注：

- 文件EF_{PBC}（电话本控制）、EF_{UID}（惟一标识）和EF_{CCP1}（能力配置参数1）不适用于R-UIM。
- “AND文件的SFI”应解释为“ADF文件标识的最后一个字节”，也就是用一个字节来指向AND文件。

4.8 应用协议

R-UIM卡的应用协议应遵循表9中所列3GPP TS 51.011相关章节的定义。

表9 应用协议

章 节	标 题
11	应用协议
11.1	通用程序
11.2.5	管理信息请求
11.2.6（注1）	SIM卡业务列表请求
11.2.7（注2）	SIM卡版本请求
11.2.8	SIM卡检测和主动式轮询

注1：对于CDMA模式，ME应当读EF_{CDMA}业务列表。

注2：对于CDMA模式，ME应当读$EF_{R\text{-}UIM}$版本。

5 多模式 R-UIM 专用文件（DF）和基本文件（EF）结构

5.1 概述

多模R-UIM的文件结构见图1。DF‘7F10’下的文件为公共部分，用户在基于GSM和基于ANSI-41模式的操作中均可访问；DF‘7F20’下的文件为GSM模式下操作所需要的文件；DF‘7F25’下的文件为ANSI-41 CDMA模式下操作所需要的文件。

5.2 基于 ANSI-41 的应用 DF 和 EF

DF‘7F25’下的 EF 用于存储基于 CDMA 的号码分配模块（NAM）参数和 CDMA 操作所需要的操作参数。

5.4 节列出了这些 EF 的编码。本标准只支持单个 NAM 的操作。

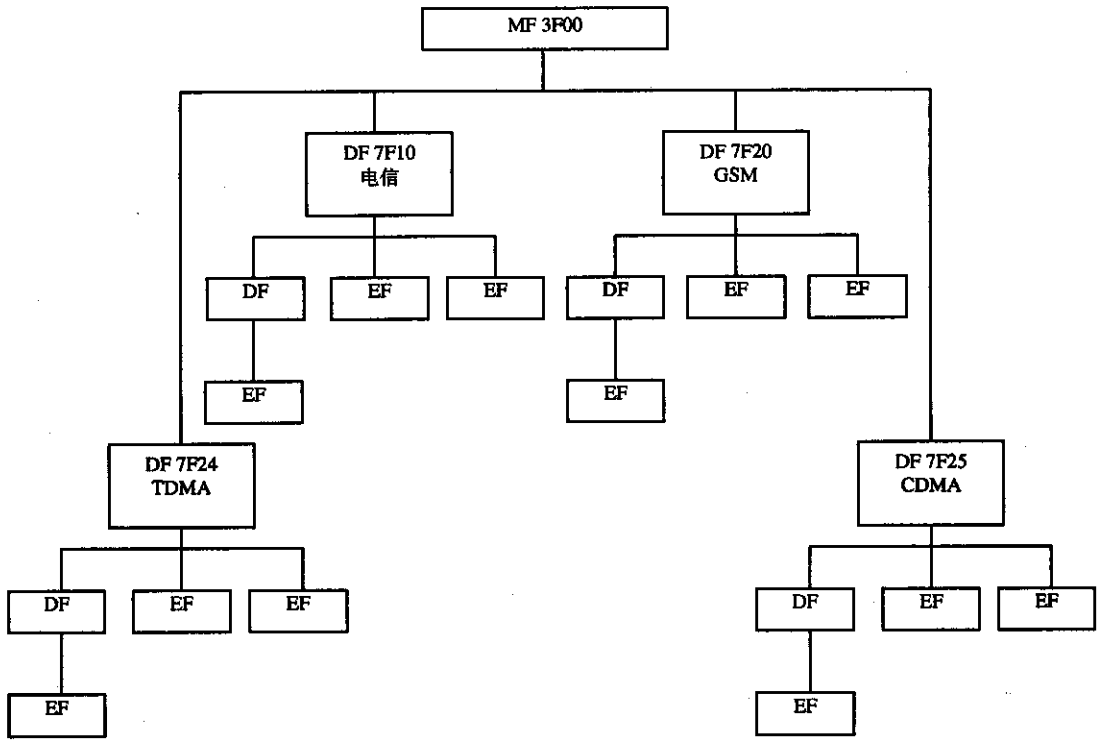


图 1　多模式 R-UIM 文件结构

5.3　文件标识符

每个文件由一个文件标识符（ID）标识。ID 由两个字节组成，编码为十六进制数。第一个字节标识文件类型，DF、EF 的编号沿用 3GPP TS 51.011 的规定：

- “3F”：主文件；
- “7F”：1 级专用文件；
- “5F”：2 级专用文件；
- “2F”：在主文件之下的基本文件；
- “6F”：在 1 级专用文件之下的基本文件；
- “4F”：在 2 级专用文件之下的基本文件。

文件 ID 应具备下述条件：

- 文件 ID 应该在相关文件建立时分配；
- 在同一父文件之下的两个子文件应具有不同的 ID；
- 子文件和任何父文件或直接或间接，不能有相同的文件 ID。

以上方式将使每个文件被惟一地识别。

5.4　保留的文件 ID

除了本标准定义的文件标识符外，下列标识符为GSM和CDMA保留使用。

专用文件：

- 管理使用：“7F4X”、“5F1X”、“5F2X”；
- 操作使用：“7F10”（$DF_{TELECOM}$）、“7F20”（DF_{GSM}）、“7F21”（$DF_{DCS1800}$）、“7F22”（DF_{IS-41}）、“7F23”（DF_{FP-CTS}）（见GSM11.19）、“7F24”（$DF_{TIA/EIA-136}$）、“7F25”（$DF_{TIA/EIA-95}$）和“7F2X”，其中：$6 \leqslant X \leqslant F$；

- “7F10”下保留：“5F50”（$DF_{GRAPHICS}$）；
- “7F20”下保留：“5F30”（$DF_{IRIDIUM}$）、“5F31”（$DF_{Globalstar}$）、“5F32”（DF_{ICO}）、“5F33”（DF_{ACeS}）、“5F3X”；其中：对于其他的MSS，4≤X≤F；
  “5F40”（$DF_{PCS-1900}$）、“5F4Y”，其中，1≤Y≤F；
  “5F5X”，其中0≤X≤F；
  “5F60”（DF_{CTS}）、“5F6Y”，其中1≤Y≤F；
  “5F70”（DFSoLSA）、“5F7Y”，其中1≤Y≤F；
  “5FYX”，其中8≤Y≤F；0≤X≤F。

基本文件：

- 管理使用：
  “6FXX”（在DF“7F4X”中）；
  “4FXX”（在DF“5F1X、5F2X”中）；
  “6F1X”（在DFs“7F10”、“7F20”、“7F21”、“7F25”中）；
  “4F1X”（在全部2级DF中）；
  “2F01”、“2FEX”（在MF“3F00”中）；
- 操作使用：
  “6F2X”、“6F3X”、“6F4X”（在“7F10”、“7F2X”中）；
  “4FYX”，其中在全部2级DF中，2≤Y≤F；
  “2F1X”（在MF“3F00”中）。

除非另外说明，上面提到的X值的范围应为0≤X≤F。

5.5 存储NAM参数和操作参数的EF编码

5.5.1 概述

如果没有特别说明，所有EF中的数为二进制数，所有没有使用的EF分配的字节设置为‘00’。标注为RFU的比特用于将来新增的参数，因此所有的RFU比特都应被设置为‘0’。ME应忽略RFU比特的状态。

本节所有EF使用的专用文件ID是‘7F25’（CDMA）。

TIA-95-B中的变量存储在几种存储器中，存入永久存储器中的变量用脚标p表示；存入半永久存储器的变量用脚标s.p表示。在使用R-UIM卡时，一些变量保留在R-UIM卡中，其他的变量则保留在ME中。

5.5.2 EF_{COUNT}（呼叫计数）

这个EF存储呼叫计数的值$COUNT_{S-P}$。

标识符：“6F21”	结构：循环	必选项
文件大小：2字节	更新频度：高	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INCREASE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字节	描述	M/O	长度（字节）
1～2	$COUNT_{S-P}$	M	2

$COUNT_{S-P}$包含在字节2的低6比特中，比特1为$COUNT_{S-P}$的LSB，比特6为$COUNT_{S-P}$的MSB，其他比特为RFU。

5.5.3 EF_{IMSI_M}

这个EF存储IMSI_M的5个部分。

标识符："6F22"	结构：透明	必选项
文件大小：10字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	CHV1	

字　节	描　述	M/O	长度（字节）
1	$IMSI\_M\ CLASS_P$	M	1
2～3	$IMSI_M_S_P$中的IMSI_M_S2	M	2
4～6	$IMSI_M_S_P$中的IMSI_M_S1	M	3
7	$IMSI\_M\_11\_12_P$	M	1
8	$IMSI\_M\_PROGRAMMED/IMSI\_M\_ADDR\_NUM_P$	M	1
9～10	MCC_M_P	M	2

$IMSI\_M\_CLASS_P$ - IMSI_M的等级分配

$IMSI\_M\_ADDR\_NUM_P$ - IMSI_M地址位数

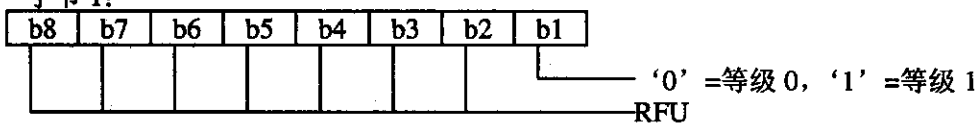
MCC_M_P - 移动国家代码

$IMSI\_M\_11\_12_P$ - IMSI_M的第11、12位数

$IMSI\_M\_S_P$ - IMSI_M的低10位数

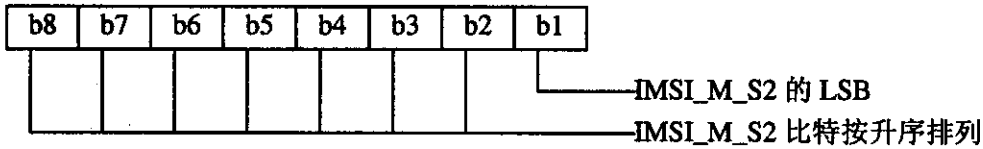
编码：

字节 1：

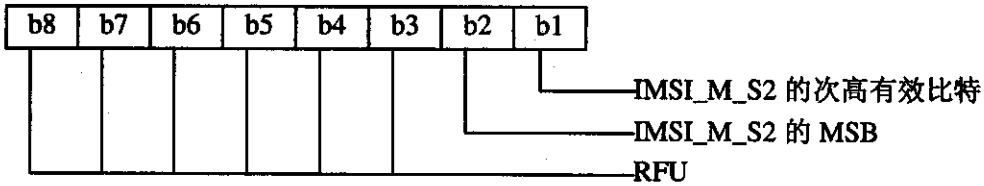


字节2、3、4、5、6的编码描述见TIA/EIA-95-B，6.3.1.1节。

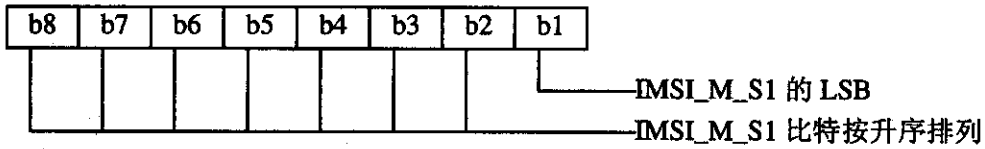
字节 2：



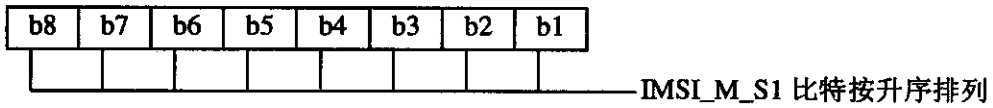
字节 3：



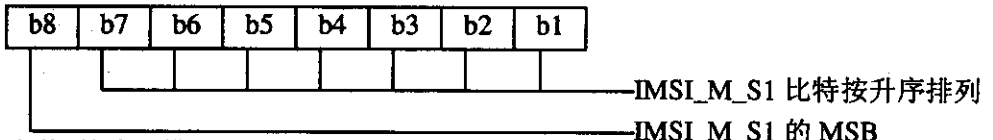
字节 4：



字节 5：

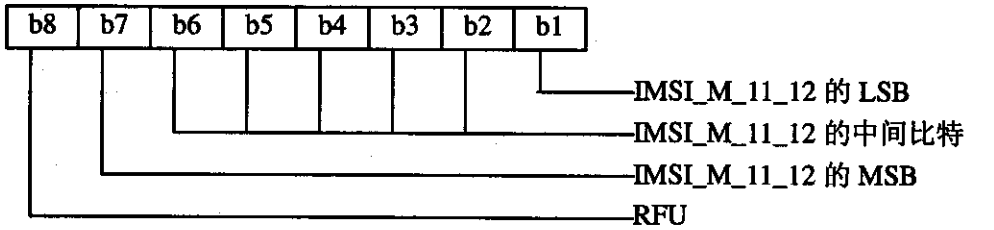


字节 6：



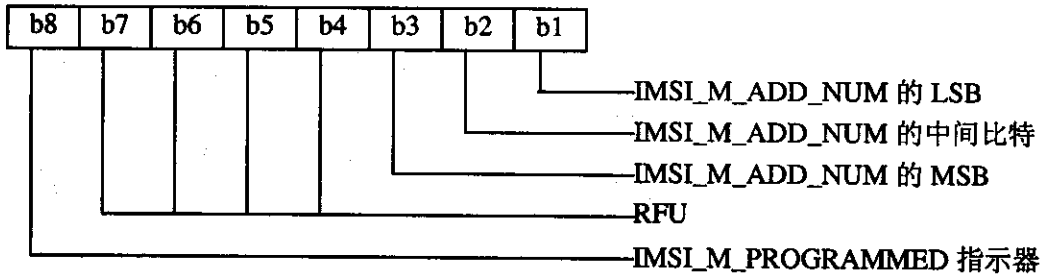
字节7的编码描述见TIA/EIA-95-B，6.3.1.2节。

字节 7：



字节8是IMSI_M_ADD_NUM的二进制表示，见TIA/EIA-95-B的6.3.1节。

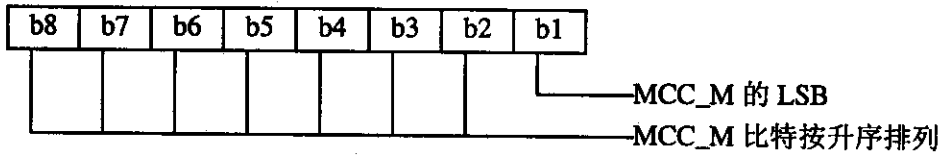
字节 8：



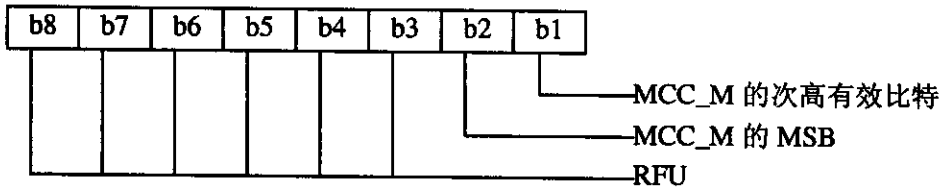
如果IMSI_M被设置，IMSI_M_PROGAMMED将设为‘1’，否则将设为‘0’。

字节9和10的编码见TIA/EIA-95-B的6.3.1.3节。

字节 9：



字节 10：



在符合TIA -95-B的系统中的R-UIM应用，参数“MIN”存储在EF_{IMSI_M}中。在上面这种情况下，字节2、3中存储10比特的“MIN2”，字节4、5、6中存储24比特的“MIN1”。

在鉴权过程中选择IMSI_M还是IMSI_T应根据TIA/EIA-95-B的6.3.12.1节中的规定，如果有IMSI_M则用IMSI_M的“MIN”部分，有IMSI_T则用IMSI_T的32比特的子集作为鉴权计算的输入。

5.5.4 EF_{IMSI_T}

此EF存储IMSI_T的5个部分。

标识符：“6F23”	结构：透明	必选项
文件大小：10字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	CHV1	

字　节	描　述	M/O	长度（字节）
1	IMSI_T $CLASS_P$	M	1
2～3	IMSI_T_S_P的IMSI_T_S2	M	2
4～6	IMSI_T_S_P的IMSI_T_S1	M	3
7	$IMSI\_T\_11\_12_P$	M	1
8	$IMSI\_T\_PROGRAMMED/IMSI\_T\_ADDR\_NUM_P$	M	1
9～10	MCC_T_P	M	2

所有字节描述、编码均与IMSI_M相同，只是将IMSI_M替换为IMSI_T。

IMSI_T不存储MIN号码。

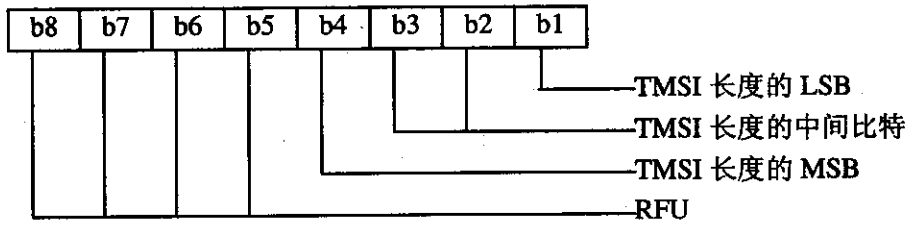
5.5.5 EF_{TMSI}

此EF存储TMSI。TMSI由移动台所在的网络分配，由4部分组成：TMSI长度（ASSIGNING_TMSI_ZONE_LENs.p）、TMSI区域（ASSIGNING_TMSI_ZONEs.p）、TMSI代码（TMSI_CODEs.p）、TMSI到期时间（TMSI_EXP_TIMEs.p）。

标识符：“6F24”	结构：透明	必选项
文件大小：16字节	更新频度：高	
访问条件		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	CHV1	

字　节	描　述	M/O	长度（字节）
1	ASSIGNING_TMSI_ZONE_LENs.p	M	1
2～9	ASSIGNING_TMSI_ZONEs.p	M	8
10～13	TMSI_CODEs.p	M	4
14～16	TMSI_EXP_TIMEs.p	M	3

字节 1：



字节2～9最多存储8个字节的TMSI区域（见TIA-95-B的6.3.15，6.3.15.1，和 6.3.15.2节）。字节按从低到高顺序连续存储，没有使用的字节设置为‘00’。

字节10～13存储TMSI代码。字节按从低到高顺序连续存储，没有使用的字节设置为‘00’。

字节14～16存储TMSI的到期时间。字节按从低到高顺序连续存储。

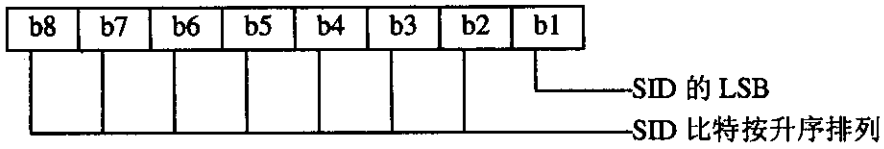
5.5.6 EF_{AH}（模拟网络归属 SID）

这个EF存储当移动台在模拟模式操作时的归属SID。

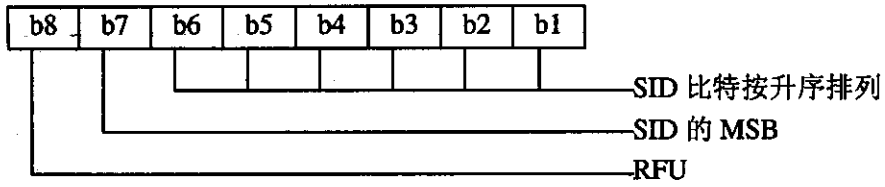
标识符：“6F25”	结构：透明	必选项
文件大小：2字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～2	模拟网络归属SID（HOME_SIDp）	M	2

字节 1：



字节 2：



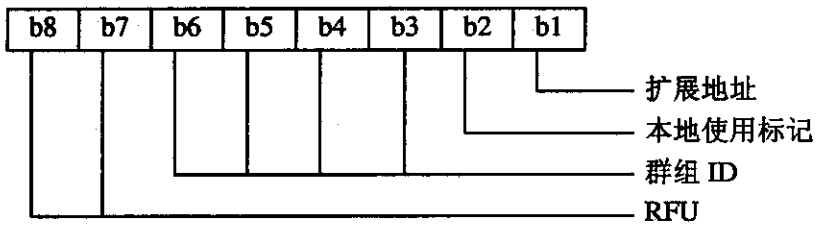
5.5.7 EF_{AOP}（模拟网络操作参数）

这个EF存储扩展地址位（Extended Address bit（Ex_P））、本地使用标记（LCM）和组群ID（GID）。

标识符：“6F26”	结构：透明	必选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字节	描　述	M/O	长度（字节）
1	模拟网络操作参数（Ex_P、LCM、GID）	M	1

字节 1：



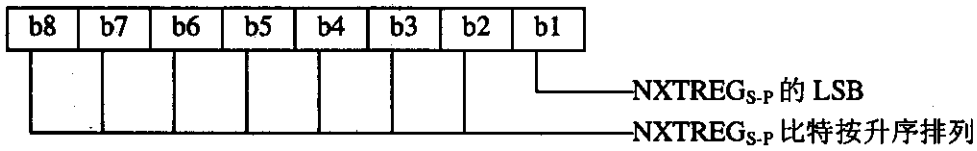
5.5.8 EF_{ALOC}（模拟模式位置和登记指示器）

这个EF存储与自治登记存储器（Autonomous Registration memory（$NXTREG_{S-P}$和SID_{S-P}））和位置区存储器（Location Area memory（$LOCAID_{S-P}$和$PUREG_{S-P}$））相关的参数。

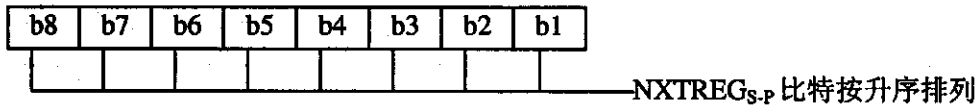
标识符："6F27"	结构：透明	必选项
文件大小：7字节	更新频度：高	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～3	NXTREGs.p	M	3
4～5	SIDs.p	M	2
6～7	LOCAIDs.p、PUREGs.p	M	2

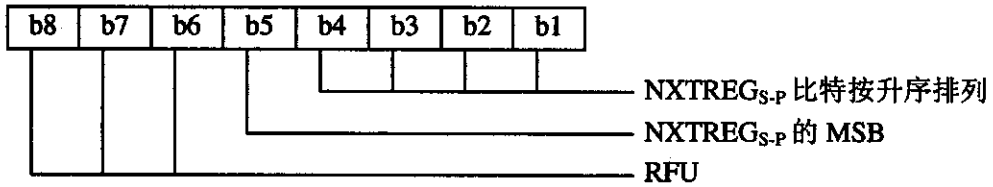
字节 1：



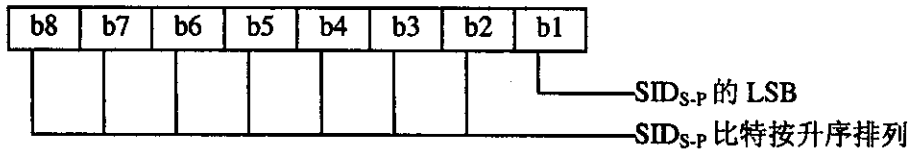
字节 2：



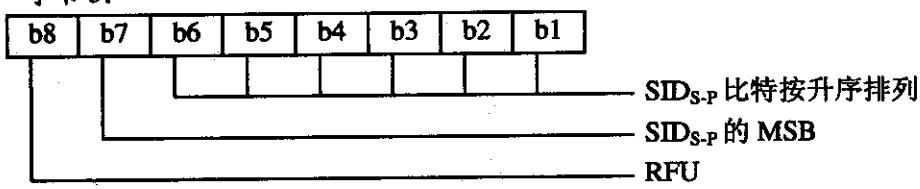
字节 3：



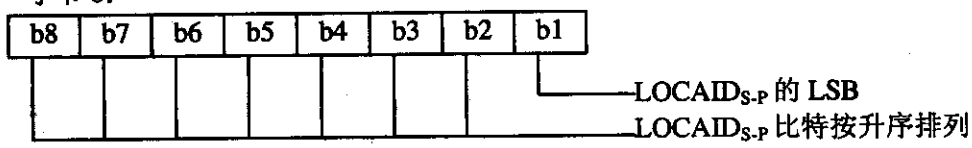
字节 4：



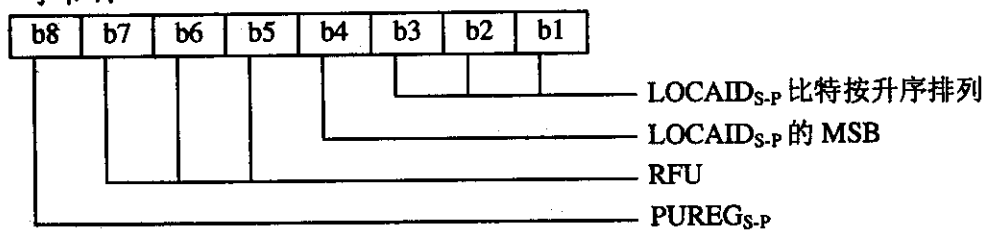
字节 5：



字节 6：



字节 7：



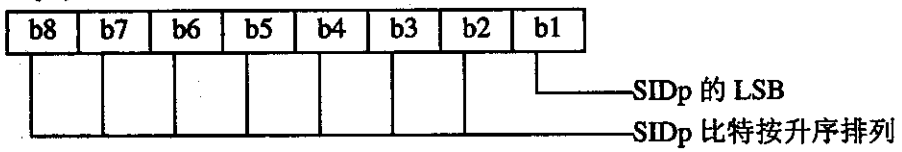
5.5.9 $EF_{CDMAHOME}$（CDMA 网络归属 SID、NID）

在移动台工作在CDMA模式时，这个EF存储归属SID和NID。

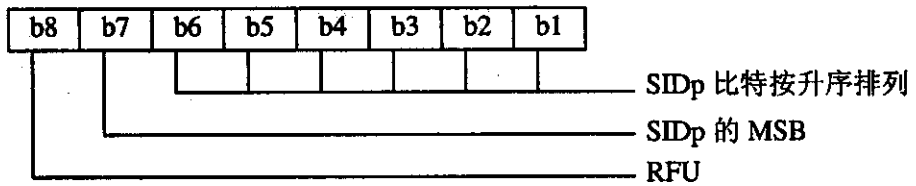
标识符："6F28"	结构：线性定长	必选项
记录大小：5字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1~2	CDMA 归属SID（SID_P）	M	2
3~4	CDMA 归属NID（NID_P）	M	2
5	频段类别	M	1

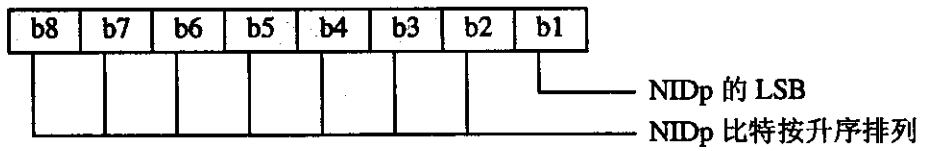
字节 1：



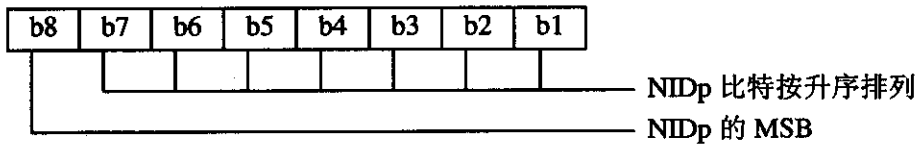
字节 2：



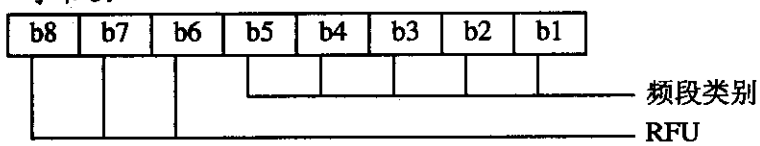
字节 3：



字节 4：



字节 5：



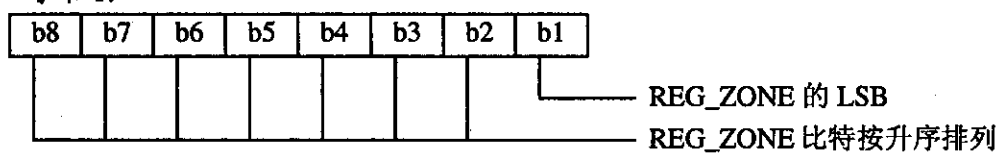
5.5.10 EF_{ZNREGI}（CDMA 基于区域的登记指示器）

这个EF存储基于区域的登记列表“ZONE_LIST”。这个列表包含一个REG_ZONE以及一个对应的SID、NID对。细节描述见TIA/EIA-95-B的6.3.4、6.6.5.1.5、6.6.5.5节。

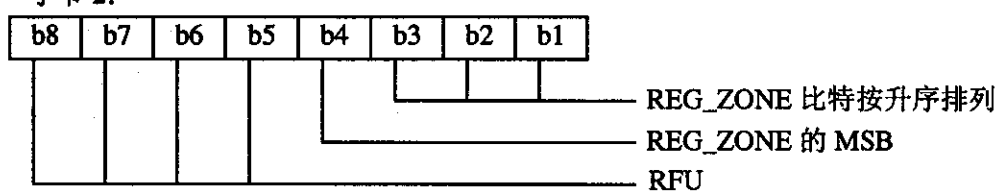
标识符：“6F29”	结构：线性定长	必选项
记录大小：8字节	更新频度：高	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～2	REG_ZONE	M	2
3～4	SID	M	2
5～6	NID	M	2
7～8	RFU	M	2

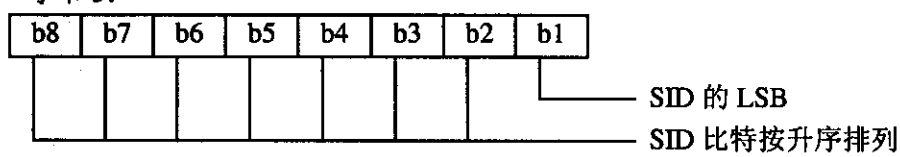
字节 1：



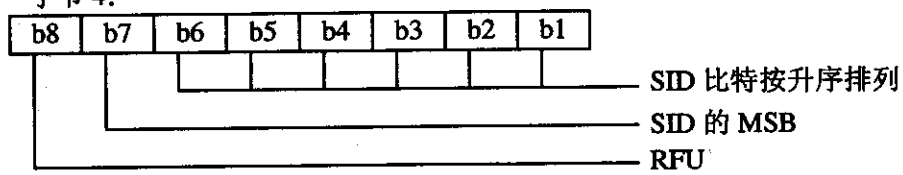
字节 2：



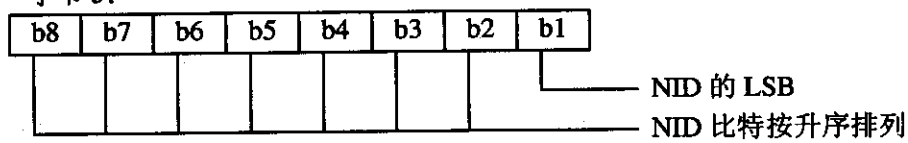
字节 3：



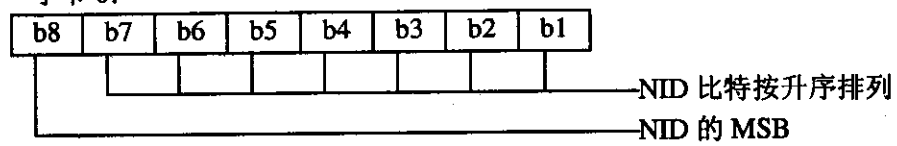
字节 4：



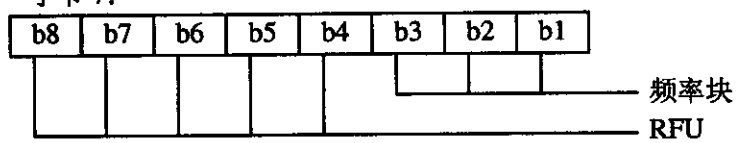
字节 5：



字节 6：



字节 7：



5.5.11 EF_{SNREGI}（CDMA 系统/网络登记指示器）

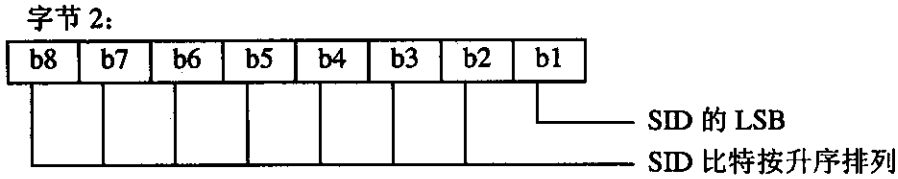
这个EF存储移动台上一次在其中登记过的无线网络的SID和NID。

标识符："6F2A"	结构：透明	必选项
文件大小：7字节	更新频度：高	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

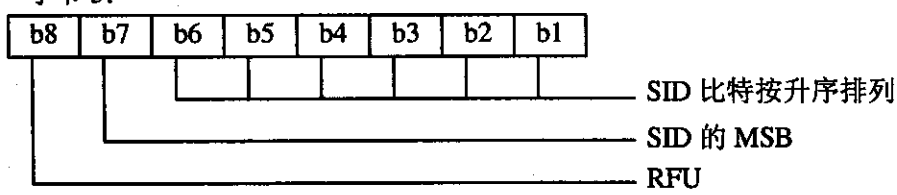
字　节	描　述	M/O	长（字节）
1	SID/NID列表的大小N（N=1）	M	1
2～3	SID	M	2
4～5	NID	M	2
6～7	RFU	M	2

字节1的b1=1，其他比特为RFU。

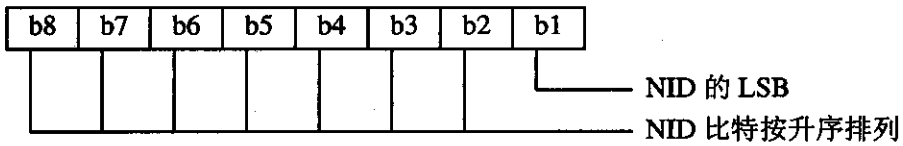
字节 2：



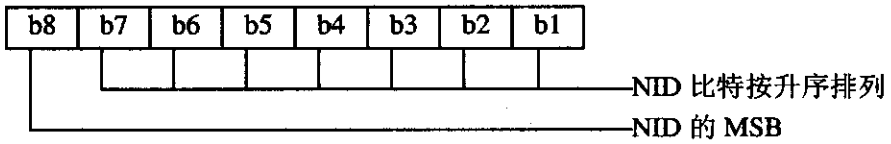
字节 3：



字节 4：



字节 5：



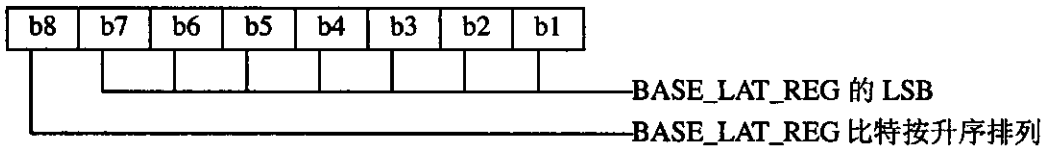
5.5.12 $EF_{DISTREGI}$（CDMA 基于距离的登记指示器）

这个EF存储基站纬度（BASE_LAT_REG）、基站经度（BASE_LONG_REG）和基站进入系统接入状态后发出第一个接入试探消息（登记消息、初始消息或寻呼响应消息）的登记距离（BASE_DIST_REG）。

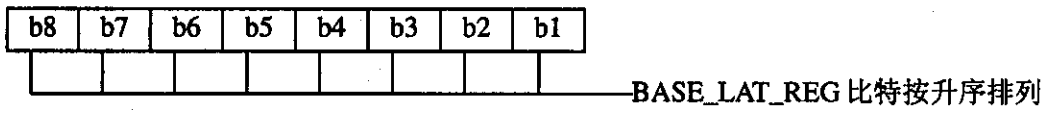
标识符："6F2B"	结构：透明	必选项
文件大小：8字节	更新频度：高	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1～3	BASE_LAT_REG	M	3
4～6	BASE_LONG_REG	M	3
7～8	REG_DIST_REG	M	2

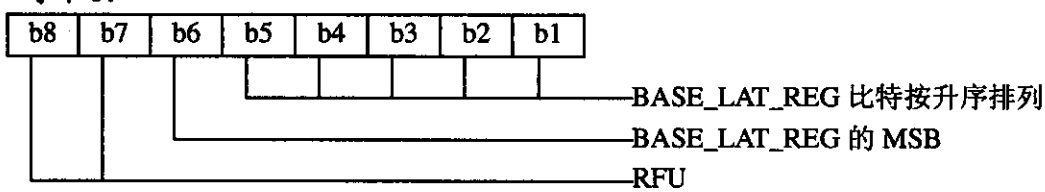
字节 1：



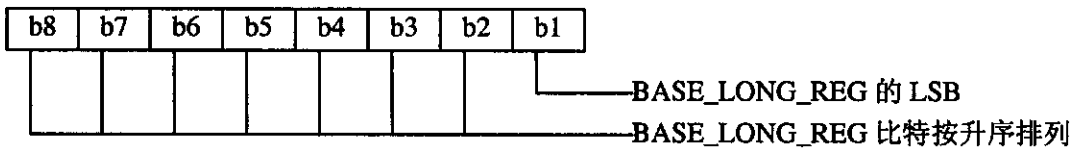
字节 2：



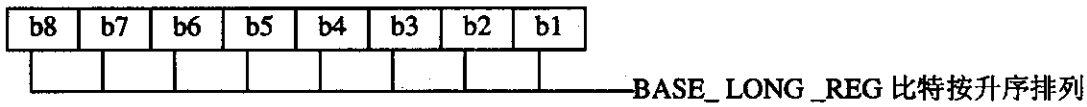
字节 3：



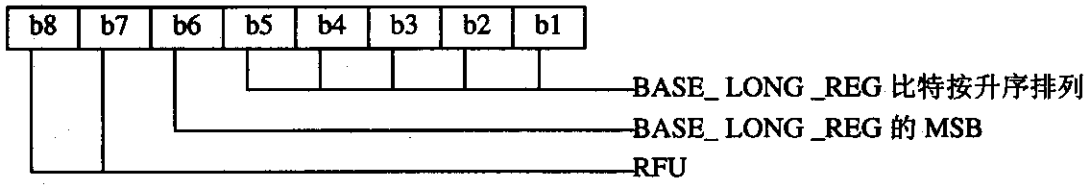
字节 4：



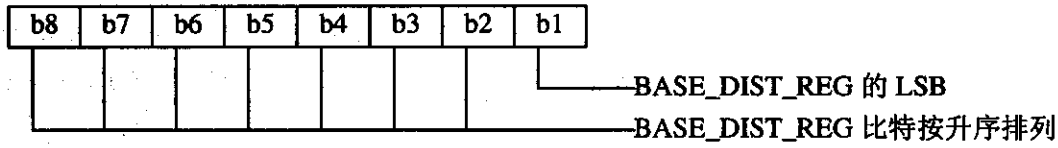
字节 5：



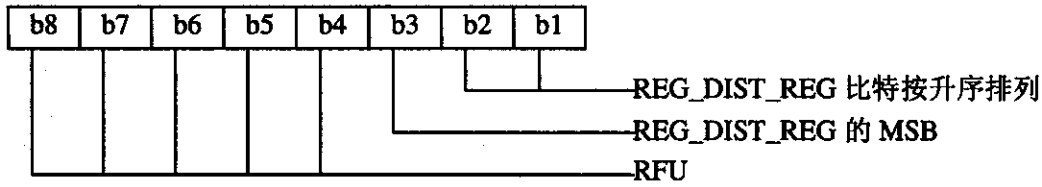
字节 6：



字节 7：



字节 8：



注：基于距离的登记的参数在TIA-95-B中的6.6.5.1.4节描述。

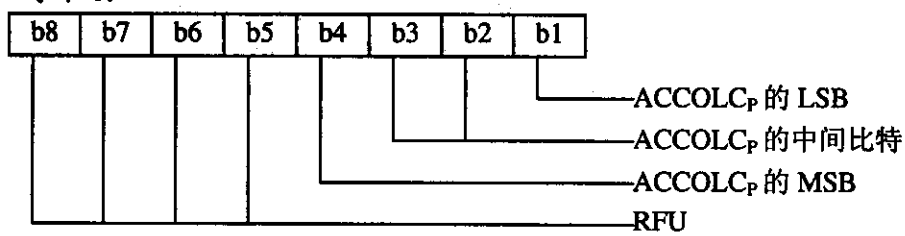
5.5.13 EF_{ACCOLC}（接入过载等级）

这个EF定义了移动台的接入过载等级。对于移动台来说，ACCOLC为IMSI_M的最后一位十进制数转换成的4比特二进制数。

标识符："6F2C"	结构：透明	必选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	接入过载等级（$ACCOLC_P$）	M	1

字节 1：



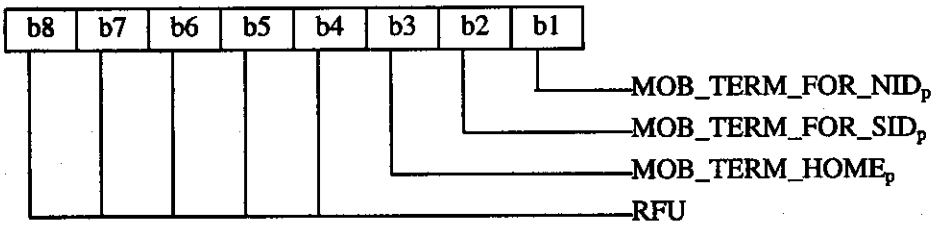
5.5.14 EF_{TERM}（被叫模式参数选择）

这个EF存储被叫参数$MOB_TERM_HOME_P$、$MOB\_TERM\_FOR\_SID_P$、$MOB\_TERM\_FOR\_NID_P$。

标识符："6F2D"	结构：透明	必选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	被叫终端的参数选择	M	1

字节 1：



$MOB\_TERM\_FOR\_NID_P$ = '0'：对于NID的漫游，不允许移动台被叫

'1'：对于NID的漫游，允许移动台被叫

$MOB\_TERM\_FOR\_SID_P$ = '0'：对于SID的漫游，不允许移动台被叫

'1'：对于SID的漫游，允许移动台被叫

$MOB\_TERM\_HOME_P$ = '0'：使用SID、NID时，不许移动台被叫

'1'：使用SID、NID时，允许移动台被叫

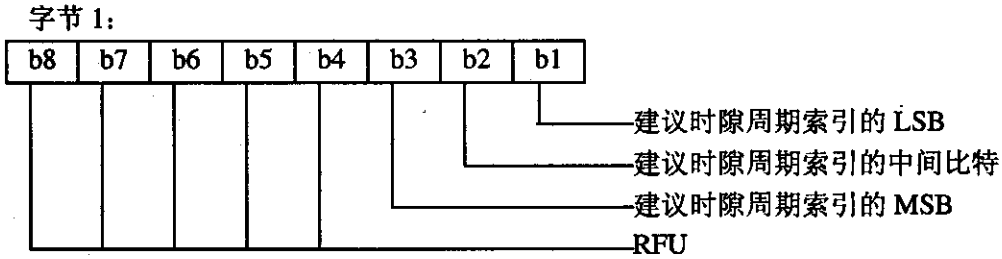
5.5.15 EF_{SSCI}（建议的时隙周期索引）

这个EF对CDMA操作的移动台给出了一个首选时隙周期索引值。

标识符："6F2E"	结构：透明	可选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	建议的首选时隙周期索引	M	1

字节 1：



5.5.16 EF_{ACP}（模拟信道选择）

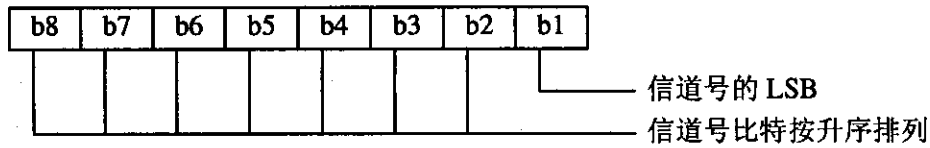
这个EF存储根据签约的条件由服务商确定的模拟模式下的信道参数选择。包括模拟初始寻呼信道（Analog Initial Paging Channel）、模拟系统A第一个专用控制信道（Analog First Dedicated Control Channel for System A）、模拟系统B第一个专用控制信道（Analog First Dedicated Control Channel for System B）和扫描的专用控制信道数（Number of Dedicated Control Channels ）。

标识符："6F2F"	结构：透明	必选项
文件大小：7字节	更新频度：低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

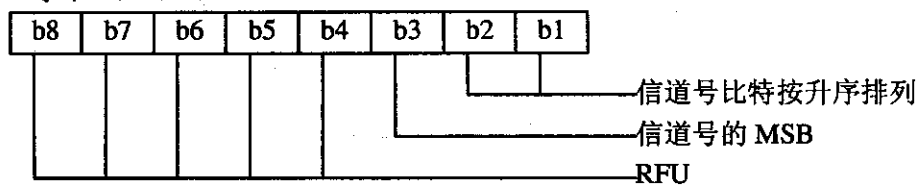
字　节	描　述	M/O	长度（字节）
1～2	模拟初始寻呼信道	M	2
3～4	模拟系统A第一个专用控制信道	M	2
5～6	模拟系统B第一个专用控制信道	M	2
7	扫描的专用控制信道数	M	1

每个信道由11比特的二进制数表示。

字节 1、3、5：



字节 2、4、6：



5.5.17 EF_{PRL}（首选漫游列表）

这个EF存储首选漫游列表（见3GPP2 C.S0016-C的3.5.3节）。首选漫游列表包含3GPP2 C.S0005-D中附录F的选择参数。

标识符："6F30"	结构：透明	必选项
文件大小：PR_LIST_SIZE_1+PR_LIST_SIZE_2+2（注）	更新频度：低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1～ PR_LIST_SIZE_1+PR_ LIST_SIZE_2+2	PR_LIST（注）	M	PR_LIST_SIZE（C.S0016-A） +PR_LIST_SIZE（C.S0016-C） +2

注：此处的PRL文件为两个不同版本的PRL文件的级连，在最后再附上对这两个PRL文件的2个字节长的CRC校验值。其中的PR_LIST_SIZE_x＝1～2为级连的不同版本的PRL文件内的相应PR_LIST_SIZE的值。

在级连的每个PRL文件内，所有保留比特均设置为‘0’（由于PR_LIST_SIZE的最小单位是8bit）。

5.5.18 EF_{RUIMID}

这个EF存储可惟一识别R-UIM的UIM_ID，其可存储最大长度为56bit的UIM_ID。UIM_ID可以代替ESN的功能。目前使用的ESN的长度为32bit，相应的UIM_ID也为32bit。如果将来ESN的长度增加了，UIM_ID的长度也将相应增加。UIM_ID与其所要插入的主设备的ESN没有关联关系。文件可以以下的结构来存储32bit的P-UIMID：8位MSB为0x80。24位LSB为EUIMID或LF_EUIMID或SF_EUIMID（取决于CDMA服务列表中的第8号业务）的SHA-1摘要的24位LSB。

标识符：“6F31”	结构：透明	必选项
文件大小：8字节	更新频度：低	
访问条件：		
READ	ALW	
UPDATE	Never	
INVALIDATE	Never	
REHABILITATE	Never	

字　节	描　述	M/O	长度（字节）
1	字节数	M	1
2	最低字节	M	1
3	:	M	1
4	:	M	1
5	:	M	1
6	:	O	1
7	:	O	1
8	最高字节	O	1

5.5.19 EF_{CST}（CDMA 业务列表）

这个EF指示分配了哪些业务以及分配的业务是否被激活。对于R-UIM卡中没有分配的业务或分配了却没有被激活的业务，ME不能选择这个业务。

标识符：“6F32”	结构：透明	必选项
文件大小：n字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	业务n1到n4	M	1
2	业务n5到n8	M	1
3	业务n9到n12	M	1
4	业务n13到n16	M	1
5	业务n17到n20	M	1
…	…		
n	业务（4n-3）到4n	O	1

- 业务：

业务 n1：CHV禁止功能

业务 n2：ADN

业务 n3：FDN

业务 n4：SMS

业务 n5[1]：HRPD

业务 n6：增强的电话簿

业务 n7：多媒体域（MMD）

业务 n8：基于SF_EUIMID的EUIMID

业务 n9：支持MEID

业务 n10：扩展1

业务 n11：扩展2

业务 n12：SMS 参数

业务 n13：LND

业务 n14：BC-SMS的业务种类编程

业务 n15：RFU

业务 n16：RFU

业务 n17：CDMA归属运营商名称

业务 n18：业务拨叫号码（SDN）

业务 n19：扩展3

业务 n20：3GPD-SIP

业务 n21：RFU

业务 n22：RFU

业务 n23：RFU

业务 n24：RFU

业务 n25：通过广播短消息下载数据

业务 n26：通过SMS-PP下载短消息

业务 n27：菜单选择

业务 n28：呼叫控制

业务 n29：主动式R-UIM

业务 n30：AKA

业务 n31：RFU

业务 n32：RFU

业务 n33：RFU

业务 n34：RFU

业务 n35：RFU

业务 n36：RFU

[1] CDMA 1x/HRPD 双模终端根据 n5 是否为‘11’（HRPD 分配并激活）来决定进行 HRPD 接入鉴权时使用 MD5 还是 CAVE 算法。当 n5 为‘11’时调用卡中的 MD5 算法，否则调用卡中的 CAVE 算法。

业务 n37：RFU

业务 n38：3GPD-MIP

业务 n39：BCMCS

业务 n40：MMS

业务 n41：扩展8

业务 n42：MMS用户连接参数

业务 n43：应用鉴权

业务 n44：组标识级别1

业务 n45：组标识级别2

业务 n46：解个性化控制密钥

业务 n47：合作网络列表

注：新增业务在这个EF文件中继续往下排。

● 编码：

每个字节编码为4项业务。每项业务由2比特编码：第一个比特为‘1’，表示分配了该业务，为‘0’表示未分配该业务，其中第一个比特是b1、b3、b5、b7；第二个比特为‘1’表示激活了该业务，为‘0’表示未激活该业务，其中第二比特为b2，b4，b6，b8；

“分配的业务”表示R-UIM有能力支持该业务；“激活的业务”表示该业务可用。

未定义的业务对应的比特为RFU，所有RFU字节设置为‘00’，所有RFU比特设置为‘0’。

如果R-UIM支持FDN特性，UIM卡中应有一个特别的机制在每个CDMA会话期间将EF_{IMSI_T}、EF_{IMSI_M}、EF_{TMSI}置于无效。在FDN使能时，该机制由UIM自动执行。此机制应至少在选择EF_{FDN}使能后下一个命令前执行。

如果第8号业务（基于SF_EUIMID的EUIMID）没有被激活（无论是否被分配），ME应用EF_{ICCID}中的ICCID填充EUIMID INFO RECORD来响应状态请求消息（Status Request Message）。否则，ME用EF_{SP_EUIMID}中的SF_EUIMID来填充EUIMID INFORECORD。

5.5.20 EF_{SPC}（业务编程代码）

这个EF存储业务编程代码（SPC），取值范围从0到999，999。默认值为0。

标识符：“6F33”	结构：透明	必选项
文件大小：3字节	更新频度：低	
访问条件：		
READ	ADM	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～3	业务编程代码	M	3

SPC是一个6位的数字d1d2d3d4d5d6，其中d1是最高位，d6是最低位。每一位以BCD格式编码。字节3的bit1到bit4包含d6的BCD编码，字节3的bit5到bit8包含d5的BCD编码，依次类推，字节1的bit1到bit4包含d2的BCD编码，字节1的bit5到bit8包含d1的BCD编码。

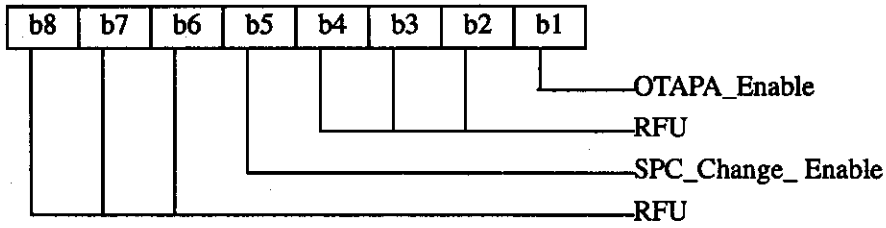
5.5.21 $EF_{OTAPASPC}$

这个EF包含用户输入的控制信息，该信息用于禁止或允许网络对SPC进行修改和禁止或允许通过OTAPA对NAM进行操作。在网络对R-UIM发起的基站查询成功响应后，网络才能经OTAPA对文件进行操作。

标识符："6F34"	结构：透明	可选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	OTAPA/SPC_Enable	M	1

字节 1：



OTAPA_Enable = 0表示用户同意由运营商对NAM执行OTAPA；OTAPA_Enable = 1则相反。

SPC_Change Enable = 0表示用户同意由运营商修改SPC的值；若为'1'则相反。

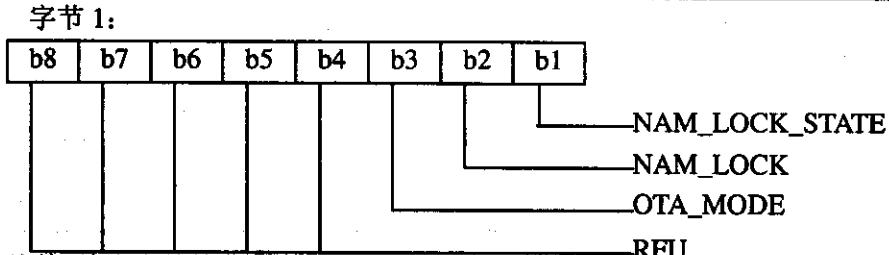
5.5.22 $EF_{NAMLOCK}$

这个EF存储NAM的锁死/去锁状态。

标识符："6F35"	结构：透明	必选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	SPASM保护指示器（NAM_LOCK）状态	M	1

字节 1：



比特1给出当前的NAM_LOCK_STATE，'1'表示NAM已由SPASM保护机制锁定，'0'表示NAM是去锁的。

比特2给出永久的NAM_LOCK设置，‘1’表示在网络初始化OTA时必须满足SPASM保护机制，‘0’表示不要求SPASM保护。

比特3给出当前OTA会话的OTA_MODE，‘0’表示由用户发起的，‘1’表示由网络发起的。

如果OTA编程会话由用户发起，SPASM不保护访问NAM参数和指示器。在这种情况下，ME将设置NAM_LOCK_STATE为‘0’，NAM_LOCK比特不变。

在网络初始化OTA任务的情况下，ME将设置NAM_LOCK_STATE=NAM_LOCK。

ME更新OTA_MODE以通知R-UIM OTA会话是如何发起的，ME应符合3GPP2 C.S0016-C中的要求。

5.5.23 EF_{OTA}（OTASP/OTAPA 特性）

这个EF存储R-UIM卡支持的OTASP/OTAPA特性列表和协议版本号。

标识符：“6F36”	结构：透明	必选项
文件大小：2*N*+1字节	更新频度：低	

访问条件：

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

字　节	描　述	M/O	长度（字节）
1	OTASP/OTAPA特性数量N	M	1
2	NAM数据下载（DATA_P_REV）ID	M	1
3	DATA_P_REV	M	1
4	密钥交换（A_KEY_P_REV）ID	M	1
5	A_KEY_P_REV	M	1
6	系统选择的首选漫游（SSPR_P_REV）ID	M	1
7	SSPR_P_REV	M	1
8	业务编程锁定（SPL_P_REV）ID	M	1
9	SPL_P_REV	M	1
10	OTAPA（OTAPA_P_REV）ID	M	1
11	OTAPA_P_REV	M	1
12	首选用户区域列表（PUZL_P_REV） ID	M	1
13	PUZL_P_REV	M	1
14	3G 数据包 （3GPD） ID	M	1
15	3GPD	M	1
16	安全模式 （SECURE_MODE_P_REV） ID	M	1
17	SECURE_MODE_P_REV	M	1
:	:	:	:
2*N*	特性*N*	M	1
2*N*+1	特性*N*的协议修订本	M	1

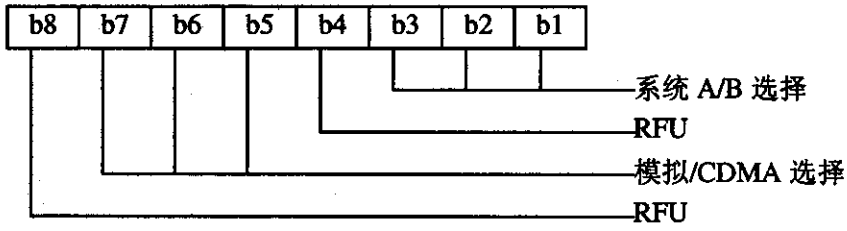
5.5.24 EF_{SP}（业务首选）

这个EF存储用户的首选业务。

标识符："6F37"	结构：透明	必选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	业务选择	M	1

字节 1：



b3b2b1 = 000 无首选
001 首选A
010 首选B
011 RFU
100 RFU
101 只选A
110 只选B
111 RFU

b7b6b5 = 000 无首选
001 首选模拟
010 首选CDMA
011 RFU
100 RFU
101 只选模拟
110 只选CDMA
111 RFU

5.5.25 EF_{ESNME}

这个EF存储最多56比特的ME的ESN。在ME判定R-UIM卡已经插入手机后将此参数传给R-UIM卡。

标识符："6F38"	结构：透明	必选项
文件大小：8字节	更新频度：低	
访问条件：		
READ	ALW	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	ESN_ME字节数	M	1
2	最低有效字节	M	1
3	:	M	1
4	:	M	1
5	:	M	1
6	:	O	1
7	:	O	1
8	最高有效字节	O	1

5.5.26 $EF_{Revision}$（R-UIM 版本）

这个EF允许ME与不同版本的R-UIM卡通信。

标识符："6F39"	结构：透明	必选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	ALW	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	R-UIM卡的版本	M	1

符合本规范的R-UIM版本应为'00000011'。

5.5.27 EF_{PL}（首选语言）

这个EF为ME提供一套语言（如中文、英语、德语等）。用户可以在这套语言中选取一种，使信息以该语言显示。

标识符："6F3A"	结构：透明	必选项
文件大小：2*n*字节	更新频度：低	
访问条件：		
READ	ALW	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～2	第一种语言代码（最高优先级）	M	2
3～4	第二种语言代码	O	2
:	:	:	:
2*n*-1～2*n*	第*n*种语言代码（最低优先级）	O	2

语言代码遵循3GPP2 C.R1001-C的要求，如代码'00000110'表示语言为中文，详见3GPP2 C.R1001-C的表9.2-1。

字节1：b1～b5=字符编码；b6～b8为RFU。

字节2：b1～b8=语言指示。

5.5.28 EF_{SMS}（短消息）

这个EF存储与短消息相关的信息。

标识符："6F3C"	结构：线性定长	可选项
记录大小：变长（注1）	更新频度：高	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1	状态	M	1
2	MSG_LEN	M	1
3～3+MSG_LEN	SMS传输层消息	M	MSG_LEN

注1：长度和字节分配根据消息的大小而变化。最大长度是255字节，包括短消息、"状态"、"MSG_LEN"。

● "状态"

"状态"字节可以用做SEEK命令的样本。对于MS向网络发送消息，当MS收到一个状态报告或成功发送一个与状态报告相关的SMS命令时应更新"状态"。

编码：

b3b2b1 =	XX0	表示可用空间
	XX1	表示已使用空间
	001	MS从网络收到消息；已读消息
	011	MS从网络收到消息；未读消息
	101	MS始发的消息；消息已发送给网络
	111	MS始发的消息；消息将要被发送
b6 =	0	短消息保护被关闭
	1	短消息保护被启用

其他比特为RFU。

● MSG_LEN

消息的长度不包括MSG_LEN。这个EF不允许成倍的出现包含"PARAMETER_ID"、"PARAMETER_LEN"和"Parameter Data"的片段。这三个字段重复的次数由MSG_LEN和每一个片段的参数"PARAMETER_LEN"决定。

● SMS传输层消息

见3GPP2 C.S0016-C中3.4.1节。SMS传输层消息由"SMS_MSG_TYPE"、"PARAMETER_ID"、"PARAMETER_LEN"和"Parameter Data"几部分组成。

5.5.29 EF_{SMSP}（短消息业务参数）

这个EF存储短消息业务字头参数，该参数可由ME用于辅助用户准备移动台发起的短消息。该EF可包含多条记录，每条记录可以含有一套SMS参数。第一个记录为默认参数集。为了区分不同的记录，在每个记录开头有一个4字节的电话业务标识符。当移动台发出短消息时，如果用户没有提供参数值，就使用R-UIM卡的记录中的参数值。

标识符："6F3D"	结构：线性定长	可选项
记录大小：可变	更新频度：高	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
注1，2	电信业务标识符	M	4
	参数指示器	M	2
	始发地址（注3）	M	可变（注1）
	目的地址（注4）	M	可变（注1）
	数据编码方案	M	1
	有效时段	M	1
	业务类别	O	4
	始发子地址（注3）	O	可变（注1）
	目的子地址（注4）	O	可变（注1）
	承载应答选择	O	3
	承载数据	O	可变（注1）

注：

1．见3GPP2 C.S0015-B；

2．开始和结束字节取决于注1；

3．对应于移动台被叫的消息（在移动端发起的消息中没有提供）；

4．对应于移动端发起的消息（在移动端被叫的消息中没有提供）。

编码：

对于所有可能的SMS参数，不管是否有该参数，均应分配存储空间。没有使用的字节应设置为"FF"。

支持的电信业务包括扩展协议增强业务、无线寻呼业务、无线消息业务、语音信箱通知和无线应用协议（WAP），详见3GPP2 C.S0015-B。

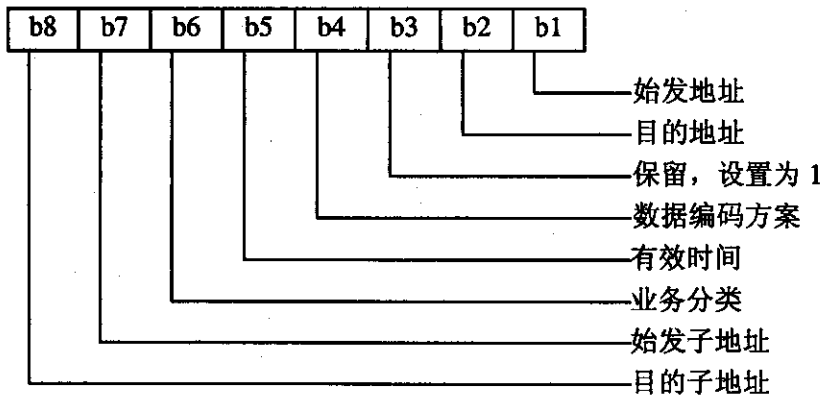
参数指示器

内容：

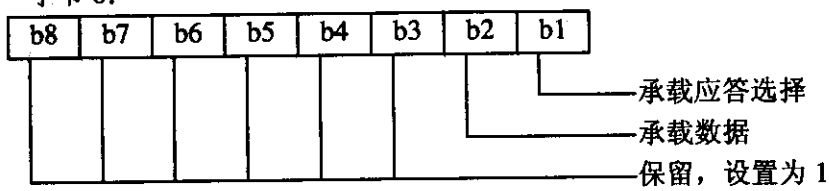
每个默认SMS参数由该字节中的不同比特标识为有或没有。

编码：

字节 5：



字节 6：



注：0表示有该参数；1表示没有该参数。

始发地址内容及编码见3GPP2 C.S0015-B。

目的地址内容及编码见3GPP2 C.S0015-B。

业务中心地址内容及编码见3GPP2 C.S0015-B。

数据编码方案内容及编码见3GPP2 C.R1001-C。

有效时段内容及编码见3GPP2 C.S0015-B。

业务分类内容及编码见3GPP2 C.S0015-B。

始发子地址内容及编码见3GPP2 C.S0015-B。

目的子地址内容及编码见3GPP2 C.S0015-B。

承载应答选择内容及编码见3GPP2 C.S0015-B。

承载数据内容及编码见3GPP2 C.S0015-B。

5.5.30 EF_{SMSS}（SMS 状态）

这个EF存储与SMS状态有关的信息，应与EF_{SMS}同时出现。

标识符："6F3E"	结构：透明	可选项
文件大小：5+*X*字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～2	MESSAGE_ID	M	2
3～4	WAP MESSAGE_ID	M	2
5	SMS "Memory Cap.Exceeded" 标志/SMS时间戳模式	M	1
6～5+*X*	保留	O	*X*

MESSAGE_ID

内容：是从一个电信业务Teleservice最后发出的SMS Submit Message中要求的除WAP业务之外的消息标识符。

编码：定义见3GPP2 C.S0015-B。

WAP MESSAGE_ID

内容：是WAP电信业务最后发出的SMS Submit Message中要求的WAP业务的消息标识符。

编码：定义见3GPP2 C.S0015-B。

SMS "Memory Cap.Exceeded" 标志/SMS时间戳模式

内容：包含一个标志指示是否有存储SMS消息的空间，还包含一个比特指示SMS时间戳是UTC还是non-UTC。

编码：b1=1表示没有设置标志位，有可用内存；b1=0表示设置了标志位。b3=0表示SMS时间戳模式为UTC；b3=1表示SMS时间戳模式为non-UTC。SMS时间戳模式由服务提供商配置。b4～b8保留，设置为1。

5.5.31 EF_{SSFC}（补充业务特性代码表）

这个EF存储ME使用的补充业务特性代码。在CDMA或模拟模式下经用户接口调用补充业务时，ME自动将特性代码插入拨出的数字串中。业务代码由运营商规定，这个EF就是使ME执行到特性代码的映射。

当在CDMA或模拟模式调用补充业务，移动台应读取补充业务特性代码表来确定所选补充业务的特性码，未确定的部分用“*”代替。

标识符：“6F3F”	结构：透明	可选项
文件大小：2*N*+1	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	*N*，特性代码个数	M	1
2～3	激活呼叫传递 （CD）	M	2
4～5	去激活呼叫传递（CD）	M	2
6～7	注册新的遇忙呼叫前转（CFB）至号码	M	2
8～9	注册遇忙呼叫前转（CFB）至语音信箱	M	2
10～11	注销遇忙呼叫前转（CFB）	M	2
12～13	激活遇忙呼叫前转（CFB）	M	2
14～15	去激活遇忙呼叫前转（CFB）	M	2
16～17	注册新的默认呼叫前转（CFD） 至号码	M	2
18～19	注册默认新呼叫前转（CFD） 至语音信箱	M	2
20～21	去激活默认呼叫前转（CFD）	M	2
22～23	激活默认呼叫前转（CFD）	M	2
24～25	去激活默认呼叫前转（CFD）	M	2
26～27	注册新的无应答呼叫前转（CFNA）至号码	M	2
28～29	注册无应答呼叫前转（CFNA） 至语音信箱	M	2
30～31	注销无应答呼叫前转 （CFNA）	M	2
32～33	激活无应答呼叫前转（CFNA）	M	2
34～35	去激活无应答呼叫前转（CFNA）	M	2
36～-37	注册新的无条件呼叫前转（CFU）至号码	M	2
38～39	注册无条件呼叫前转（CFU）至语音信箱	M	2
40～41	注销无条件呼叫前转（CFU）	M	2
42～43	激活无条件呼叫前转（CFU）	M	2
44～45	去激活无条件呼叫前转（CFU）	M	2
46～47	激活呼叫等待（CW）	M	2

字　节	描　述	M/O	长度（字节）
48～49	去激活呼叫等待（CW）	M	2
50～51	临时去激活呼叫等待（取消呼叫等待 - CCW）	M	2
52～53	临时激活呼叫号码识别限制 （CNIR） （单个呼叫阻塞）	M	2
54～55	临时去激活呼叫号码识别限制（CNIR） （单个呼叫允许接入）	M	2
56～57	调用会议电话 （CC）	M	2
58～59	调用退出最后一次会议电话（CC）的群组	M	2
60～61	激活请勿打扰（DND）	M	2
62～63	去激活请勿打扰（DND）	M	2
64～65	激活消息等待通知（MWN） Alert Pip Tone	M	2
66～67	去激活消息等待通知（MWN） Alert Pip Tone	M	2
68～69	激活消息等待通知（MWN） Pip Tone	M	2
70～71	去激活消息等待通知（MWN） Pip Tone	M	2
72～73	临时去激活消息等待通知（MWN） Pip Tone （取消 MWN - CMWN）	M	2
74～75	调用优先接入和信道分配 （PACA）	M	2
76～77	调用语音信箱重获（VMR）	M	2
78～79	激活呼叫名称显示（CNAP）	M	2
80～81	去激活呼叫名称显示（CNAP）	M	2
82～83	激活禁止呼叫名称显示（CNAR）	M	2
84～85	去激活禁止呼叫名称显示（CNAR）	M	2
86～87	激活自动回拨（AC）	M	2
88～89	去激活自动回拨（AC）	M	2
90～91	激活自动重拨（AR）	M	2
92～93	去激活自动重拨（AR）	M	2
94～95	注册新的网络已登记的，用户可选择的呼叫前转（USCF） 至目录号码	M	2
96～97	激活拒绝不期望的干扰电话 （RUAC）	M	2
98～99	去激活拒绝不期望的干扰电话（RUAC）	M	2
100～101	调用计费通知（AOC）	M	2
102～103	调用呼叫跟踪（COT）	M	2
:	:	:	:
2*N*～2*N*+1	FCN	M	2

其中*N*编码为十六进制数值，代表特性编码的号码。

四位数的特性代码采用BCD编码为两个字节的特性代码：

— 不支持的业务特性代码为‘FF’；

— 未使用的特性代码设置为‘F’；

— 最高位数编码为第一字节的高4比特；

— 下一位数编码为第一字节的低4比特；

— 接下来的一位编码为第二字节的高4比特；

— 最低位编码为第二字节的低4比特。

例如，带有预先登记号码的USCF的特性代码为‘*789’，字节2～3应为‘F789’。

5.5.32 EF_{SPN}（CDMA 归属运营商名称）

这个EF存储可由ME显示的归属运营商名称和一些提示信息。

标识符："6F41"	结构：透明	可选项
文件大小：35字节	更新频度：低	
访问条件： READ ALW UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1	显示条件	M	1
2	字符编码	M	1
3	语言指示	M	1
4～35	运营商名称	M	32

显示条件指示当MS在归属服务区登记时是否要显示运营商名称的指示，其编码为字节1。b1=0表示不要求显示所登记的系统；b1=1表示要求显示所登记的系统。b2～b8为RFU。

字节2：b1～b5为字符编码；b6～b8=RFU。

字节3：b1～b8为语言指示器，见3GPP2 C.R1001-C中表9.2-1。

字节4～35显示运营商的名称，编码见3GPP2 C.R1001-C中表9.1-1。不使用的字节设置为'FF'。

5.5.33 EF_{USGIND}（R-UIM ID 使用指示器）

这个EF文件指示UIM_ID还是ESN_ME，用作'ESN'参与CAVE鉴权和作为MS的标识，如6.6.1节所述。该文件同时也指示当分配了第8号业务时，56比特的SF_EUIMID还是MEID被用作"MEID"。

标识符："6F42"	结构：透明	必选项
文件大小：1字节	更新频度：低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1	UIM ID使用指示器	M	1

编码：

1bit用于UIM ID使用指示。

b1=0：ESN_ME用于CAVE鉴权并作为MS的标识。

b1=1：UIM_ID用于CAVE鉴权并作为MS的标识。

b1的缺省值为'0'。

b2～b8为RFU。

1bit用于SF_EUIMID使用指示。

b2=0：MEID用作MS的标识。

b2=1：SF_EUIMID用作MS标识。

如果没有分配第8号业务，则b2应被设置为'0'，且ME不解译该比特。

如果第8号业务被分配并被激活，ME分配了ESN，则ME不解译b2。

5.5.34 EF_{AD}（管理数据）

这个EF文件包括对应于UIM类型的UIM的操作模式信息，它指示是否有一些ME特征在操作中被激活。此外还包含在正常操作模式中是否要激活一些ME特性的指示。

标识符："6F43"	结构：透明	必选项
文件大小：3+X字节	更新频度：低	
访问条件： READ ALW UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1	MS操作模式	M	1
2～3	附加信息	M	2
4～3+X	RFU	O	X

字节1：

初始值：正常操作模式'00'

其他操作值见3GPP TS 51.011。

字节2（附加信息的第一字节）：如果字节1的b1为'1'，则指明设施。目前b1～b8为RFU。

字节3：b1～b8=RFU

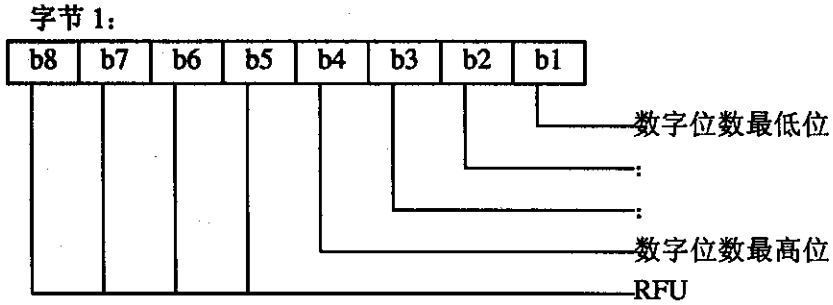
5.5.35 EF_{MDN}（移动目录号码）

这个EF文件存储MDN、号码类型、编号计划和屏幕指示器。

标识符："6F44"	结构：线性定长	可选项
记录大小：11字节	更新频度：低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字　节	描　述		M/O	长度（字节）
1	RFU	数字位数	M	1
2～9	MDN		M	8
10	NUMBER_TYPE和NUMBER_PLAN		M	1
11	PI和SI		M	1

字节 1：

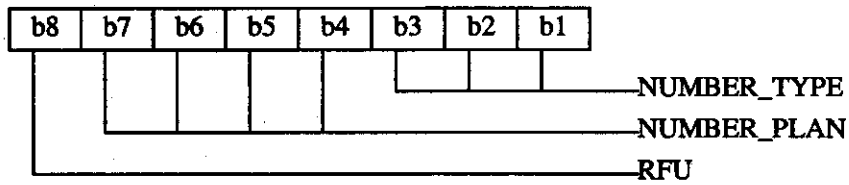


字节2～9存储多达16个数字的号码。如果MDN需要不到16个数字号码，则剩余的字节用‘FF’填充。

字节2：b1为第一个数字的最低位，b4为第一个数字的最高位；b5为第二个数字的最低位，b8为第二个数字的最高位。

字节3到字节9的格式同字节2。

字节 10：



字节11：b1b2=PI；b3b4=SI；b5-b8=RFU

5.5.36 EF_{MAXPRL}（PRL 文件大小的最大值）

此EF文件以八位字节的方式存储R-UIM可以支持的EF_{PRL}和EF_{EPRL}的最大尺寸，见3GPP2 C.S0016-C的3.5.5.1节。

标识符：“6F45”	结构：透明	必选项
文件大小：2或4字节	更新频度：不能更新	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～2	EF_{PRL} 的MAX_PR_LIST_SIZE	M	2
3～4	EF_{EPRL} 的MAX_PR_LIST_SIZE	O	2

PRL最大为1k字节。

5.5.37 EF_{SPCS}（SPC 状态）

这个EF存储了SPC的状态，用来识别EFscp是否被设置为缺省值并且是否在卡内进行了内部更新。如果SCP发生了改变，这些信息反映了在OTASP提交后SPC的当前状态。

标识符：“6F46”	结构：透明	必选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	NEVER	
INVALIDATE	NEVER	
REHABILITATE	NEVER	

字　节	描　述	M/O	长度（字节）
1	SCP状态	M	1

编码：

字节1中b1=0：SPC设置为缺省值；b1=1：SCP设置为非缺省值的其他值。

5.5.38 EF_{ECC}（紧急呼叫号码）

这个EF存储最多5个紧急呼叫号码。

标识符："6F47"	结构：透明	可选
文件大小：3*n*（*n*≤5）字节	更新频度：低	
访问条件：		
READ	ALW	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～3	第一个紧急呼叫代码	O	3
4～6	第二个紧急呼叫代码	O	3
...	...		
（3*n*-2）～3*n*	第*n*个紧急呼叫代码	O	3

字节1的低4比特存储第一个紧急呼叫号码的第一位数，字节1的高4比特存储第一个紧急呼叫号码的第二位数；字节2的低4比特存储第一个紧急呼叫号码的第三位数，字节2的高4比特及字节3为RFU，设置为'F'。

在R-UIM被激活后，ME首先选择专用文件DFCDMA，然后可选EF_{ECC}。如果可读取EF_{ECC}，则ME请求紧急呼叫号码。

5.5.39 $EF_{ME3GPDOPC}$（ME 3GPD 操作能力）

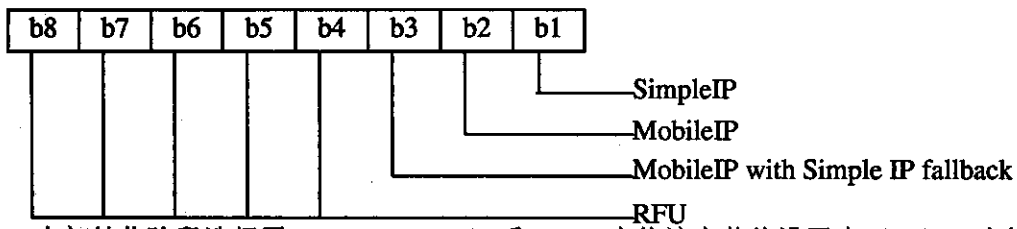
这个EF存储了ME支持的IP操作能力，见3GPP2 C.S0016-C。如果分配了第20号业务或第38号业务其中之一，则该EF应出现。

标识符："6F48"	结构：透明	可选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	ME_3GPD_OP_MODE	M	1

编码：

字节 1：



在初始化阶段选择了DF_{CDMA}（7F25）后，UIM应将该字节值设置为'00'。支持简单IP或移动IP的终端应将对应比特设置为'1'。

5.5.40 $EF_{3GPDOPM}$（3GPD 操作模式）

这个EF存储3GPD操作模式参数块，见3GPP2 C.S0016-C。如果分配了第20号业务或第38号业务其中之一，则该EF应出现。

标识符："6F49"	结构：透明	可选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	3GPD操作模式参数块	M	1

字节1的比特1和2指示了操作模式，比特3～8为RFU。

5.5.41 EF_{SIPCAP}（简单 IP 能力参数）

这个EF存储简单IP能力参数块，见3GPP2 C.S0016-C。如果分配了第20号业务，则该EF应出现。

标识符："6F4A"	结构：透明	可选项
文件大小：4字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～4	简单IP能力参数块	M	4

5.5.42 EF_{MIPCAP}（移动 IP 能力参数）

这个EF存储移动IP能力参数块，见3GPP2 C.S0016-C。如果分配了第38号业务，则该EF应出现。

标识符："6F4B"	结构：透明	可选
文件大小：5字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～5	移动IP能力参数块	M	5

5.5.43 EF_{SIPUPP}（简单 IP 用户概要参数）

这个EF存储简单IP用户概要参数块，见3GPP2 C.S0016-C。如果分配了第20号业务，则该EF应出现。

标识符："6F4C"	结构：透明	可选
文件大小：1+*X*字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	简单IP用户概要参数块长度	M	1
2～*X*+1	简单IP用户概要参数块	M	*X*

5.5.44 EF_{MIPUPP}（移动 IP 用户概要参数）

这个EF存储移动IP用户概要参数块，见3GPP2 C.S0016-C。如果分配了第38号业务，则该EF应出现。

标识符："6F4D"	结构：透明	可选
文件大小：1+*X*字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	移动IP用户概要参数块长度	M	1
2～*X*+1	移动IP用户概要参数块	M	*X*

5.5.45 EF_{SIPSP}（简单 IP 状态参数）

这个EF存储简单IP状态参数块，见3GPP2 C.S0016-C。如果分配了第20号业务，则该EF应出现。

标识符："6F4E"	结构：透明	可选项
文件大小：1	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	简单IP状态参数块	M	1

5.5.46 EF_{MIPSP}（移动 IP 状态参数）

这个EF存储移动IP状态参数块，见3GPP2 C.S0016-C。如果分配了第38号业务，则该EF应出现。

标识符："6F4F"	结构：透明	可选项
文件大小：*X*	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～*X*	移动IP状态参数块	M	*X*

5.5.47 $EF_{SIPPAPSS}$（简单 IP PAP SS 参数）

这个EF存储简单IP PAP SS参数块，见3GPP2 C.S0016-C。如果分配了第20号业务，则该EF应出现。

标识符："6F50"	结构：透明	可选项
文件大小：1+*X*字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	简单IP PAP SS参数块长度	M	1
2～*X*+1	简单IP PAP SS参数块	M	*X*

5.5.48 保留

5.5.49 保留

5.5.50 EF_{PUZL}（首选用户区列表）

这个EF存储首选用户区列表，见3GPP2 C.S0016-C中3.5.7节。

标识符："6F53"	结构：透明	可选项
文件大小：CUR_UZ_LIST_SIZE	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～CUR_UZ_LIST_SIZE	PUZL	M	CUR_UZ_LIST_SIZE

5.5.51 $EF_{MAXPUZL}$（PUZL 文件大小的最大值）

这个EF以字节方式存储UIM可以支持的首选用户区列表的最大尺寸以及EF_{PUZL}文件中用户区记录的最大数，见3GPP2 C.S0016-C。

标识符："6F54"	结构：透明	可选项
文件大小：5字节	更新频度：无	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～3	MAX_UZ_LIST_SIZE	M	3
4～5	MAX_UZ	M	2

5.5.52 EF_{MECRP}（ME 特定的配置请求参数）

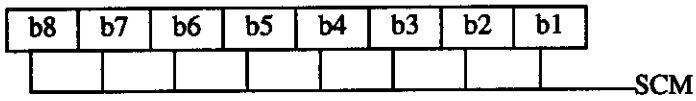
这个EF存储ME指定的配置请求参数，该参数用于形成在安全模式激活时配置请求命令的响应。ME应在初始化时更新该参数。

标识符："6F55"	结构：透明	必选项
文件大小：3字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	SCM	M	1
2	MOB_P_REV	M	1
3	本地控制	M	1

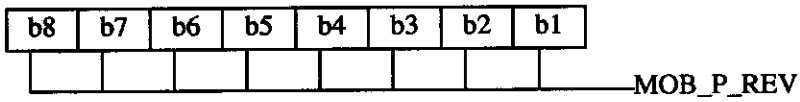
编码：

字节 1：

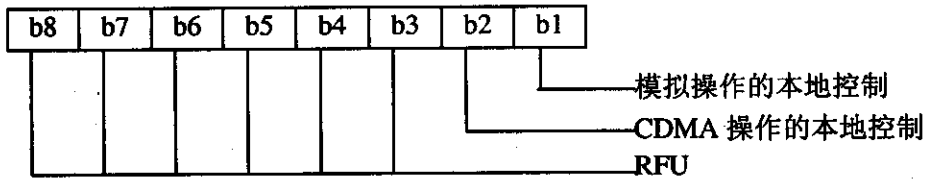


注：b6指示ME是否操作在时隙模式下。

字节 2：



字节 3：



5.5.53 $EF_{HRPDCAP}$（HRPD 接入鉴权能力参数）

这个EF存储HRPD接入鉴权能力参数块，见3GPP2 C.S0016-C中3.5.8.12节。如果分配了第5号业务，则该EF应出现。

标识符："6F56"	结构：透明	可选项
文件大小：2字节	更新频度：低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1～3	HRPD接入鉴权参数块	M	3

5.5.54 $EF_{HRPDUPP}$（HRPD 接入鉴权用户概要参数）

这个EF存储HRPD接入鉴权用户概要参数块，见3GPP2 C.S0016-C中3.5.8.13节。如果分配了第5号业务，则该EF应出现。

标识符："6F57"	结构：透明	可选项
文件大小：1+*X*字节	更新频度：低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1	HRPD接入鉴权用户概要参数块长度	M	1
2～*X*+1	HRPD接入鉴权用户概要参数块	M	*X*

5.5.55 EF_{CSSPR}（CUR_SSPR_P_REV）

这个EF存储EF_{PRL} 中当前首选漫游列表的协议版本。该信息用于ME解析EF_{PRL}。

标识符："6F58"	结构：透明	可选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	CUR_SSPR_P_REV	M	1

5.5.56 EF_{ATC}（接入终端类型）

这个EF存储用于进行持续测试的HRPD终端的类型（见3GPP2 C.S0024-0）。如果分配了第5号业务，则该EF应出现。

标识符："6F59"	结构：透明	可选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	接入终端类型	M	1

编码：

字节1的b1为AT类别的LSB，字节1的b2为AT类别的MSB。b8-b3为RFU。

5.5.57 EF_{EPRL}（扩展 PRL）

这个EF存储扩展的PRL列表，见3GPP2 C.S0016-C中第3.5.3节。

标识符："6F5A"	结构：透明	可选项
文件大小：PR_LIST_SIZE	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1~PR_LIST_SIZE	PR_LIST，见3GPP2 C.S0016-C中第3.5.5节	M	PR_LIST_SIZE

5.5.58 $EF_{BCSMScfg}$（广播短消息配置）

这个EF包含用于Broadcast SMS的广播配置。该信息由运营商决定，它规定了ME接收SMS广播所使用的过滤标准。如果存在$EF_{BCSMStable}$，则本文件出现。

标识符："6F5B"	结构：透明	可选项
文件大小：1字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	运营商广播配置	M	1

编码：

b2b1 = 00：不允许（Disallow）

01：仅允许列表中的业务（Allow Table Only）

10：全部允许（Allow All）

11：RFU

b8～b3：RFU

运营商的广播配置，包含服务提供商要求的过滤标准。

域　名	描　述
Disallow	该设置禁止了移动台‘SMS广播’的能力（也就是移动台将不处理SMS广播）
Allow Table Only	该设置允许移动台仅去接收在业务列表中列出的业务所对应的广播消息
Allow All	该设置允许移动台接收所有业务的广播消息

5.5.59 $EF_{BCSMSpref}$（广播短消息优先）

这个EF包含用于SMS广播的、由用户决定的广播配置。它规定了ME接收SMS广播所使用的过滤标准。如果存在$EF_{BCSMStable}$，则本文件出现。

标识符：“6F5C”	结构：透明		可选项
文件大小：1字节	更新频度：高		
访问条件：			
READ	CHV1		
UPDATE	CHV1		
INVALIDATE	ADM		
REHABILITATE	ADM		
字　节	描　述	M/O	长度（字节）
1	用户广播配置	M	1

编码：

b2b1 = 00：不允许（Disallow）

01：仅允许列表中的业务（Allow Table Only）

10：全部允许（Allow All）

11：RFU

b8～b3：RFU

用户的广播配置，包含由移动用户决定的过滤标准。

域　名	描　述
Disallow	该设置禁止了移动台‘SMS广播’的功能（也就是移动台将不处理SMS广播）
Allow Table Only	该设置允许移动台仅接收在业务列表中列出的业务所对应的广播消息，它受制于在$EF_{BCSMStable}$中基于用户优先级的任何额外的过滤标准。该设置仅当运营商配置不为“Disallow”时才有效。移动用户可以自己来选择“使能”或“禁止”对$EF_{BCSMStable}$中各记录的修改
Allow All	该设置允许移动台接收所有业务的广播消息。该设置仅当运营商配置为“Allow All”时才有效

5.5.60 $EF_{BCSMStable}$（广播短消息列表）

如果分配了第14号业务，则该EF应出现。这个EF包含由业务种类编程参数组成的信息，ME将这些信息用于SMS广播的过滤。详细信息见3GPP2 C.S0015-B中4.5.19节。

这个EF中的每一个记录都链接到EF_{BCSMSP}中有同样索引的记录。

标识符："6F5D"	结构：线性定长	可选项
文件大小：7+*X*字节	更新频度：高	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

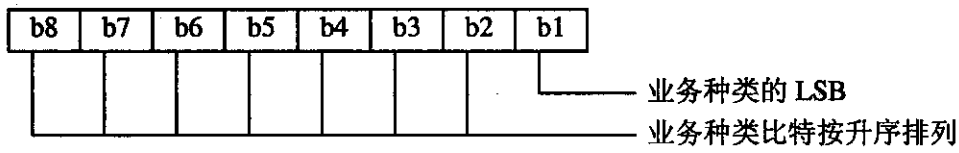
字　节	描　述	M/O	长度（字节）
1	状态	M	1
2～3	业务种类	M	2
4	语言	M	1
5	最大消息	M	1
6	告警选项	M	1
7	标签编码	M	1
8～7+*X*	标签	M	*X*

状态内容：记录的状态字节在SEEK命令中可以作为搜索的"式样"。

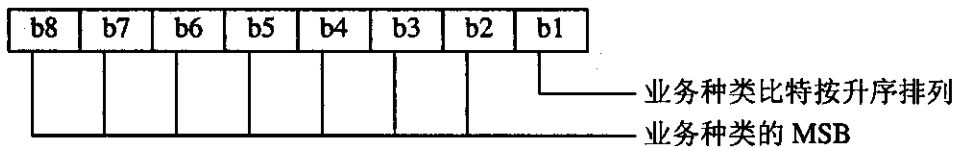
编码：

字节1的比特1如果等于'0'，则表示空间空闲；如果比特1等于'1'，则表示空间已被使用。字节1中的bit8～bit2为RFU。

字节 2：



字节 3：



字节4的8个比特编码为语言；字节5的8个比特编码为最大消息；字节6的比特4到1为告警选项，比特8～5为RFU；字节7的比特5～1为标签编码，比特8～6为RFU。

5.5.61 EF_{BCSMSP}（广播短消息参数）

如果分配了第14号业务，则该EF应出现。这个EF包含与业务种类相关的选择标记和优先权，ME使用这些参数用于BC-SMS的过滤。EF中的每一个记录都链接到$EF_{BCSMStable}$中有同样索引的记录。

标识符："6F5E"	结构：线性定长	可选项
文件大小：2字节	更新频度：高	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1	选择	M	1
2	优先权	M	1

编码：

字节1的比特1为'0'表示没有选择，为'1'表示已选择；比特8～2为RFU。

字节2的 b2b1 = 00：Normal

= 01：Interactive

= 10：Urgent

= 11：Emergency

字节2的比特8～3为RFU。

没有使用的字节用'FF'填充。当字节1的比特1设置为'1'时，ME将根据字节2中指示的优先权来过滤BC-SMS。

5.5.62 EF_{IMPI}（IMS私有用户身份）

如果分配了第7号业务，则该EF应出现。这个EF包含用户的私有用户身份。

标识符："6F5F"	结构：透明	可选项
文件大小：*X*字节	更新频度：低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1～*X*	NAI TLV数据对象	M	*X*

- NAI

内容：用户的私有用户身份。

编码：NAI TLV数据对象的内容及编码值见IETF RFC 2486。NAI应根据IETF RFC 3629中定义的UTF-8编码规则来编码为8位字符。NAI TLV数据对象的标签应为'80'。

5.5.63 EF_{DOMAIN}（归属网络的域名）

如果分配了第7号业务，则该EF应出现。这个EF包含归属运营商的网络域名SIP URI。

标识符："6F60"	结构：透明	可选项
文件大小：*X*字节	更新频度：低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1～*X*	URI TLV数据对象	M	*X*

URI

内容：归属网络域名 SIP URI。

编码：URI TLV数据对象值得内容和语法见IETF RFC 3261。URI应根据IETF RFC 3629中定义的UTF-8编码规则来编码为8位字符。URI TLV数据对象的标签值应为‘80’。

5.5.64 EF_{IMPU}（IMS 公共用户身份）

如果分配了第7号业务，则该EF应出现。这个EF包含用户的公共SIP身份（SIP URI）的值。这个EF由1个或多个记录组成，每一个记录中包含一套公共用户身份。

标识符：“6F61”	结构：线性定长	可选项
文件大小：*X*字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～*X*	URI TLV数据对象	M	*X*

- URI

内容：通过公共用户身份其他用户可以识别该用户，公共用户身份的格式为SIP URL、tel URL或两种都使用。

编码：URI TLV数据对象的内容及编码值见IETF RFC 3261。其标签应为‘80’。

5.5.65 EF_{PCSCF}（代理呼叫会话控制功能）

如果分配了第7号业务，则该EF应出现。

这个EF包含一个或多个代理呼叫会话控制功能地址。第一个记录具有最高优先级。最后一个记录具有最低的优先级。

标识符：“6F62”	结构：线性定长	可选项
文件大小：*X*字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～*X*	P-CSCF TLV数据对象	M	*X*

- P-CSCF

内容：代理呼叫会话控制功能的地址。地址格式为FQDN、IPv4或IPv6。

编码：P-CSCF TLV数据对象的标签应为‘81’。数据对象格式如下：

域	长度（字节）
标签	1
长度	2

地址类型	1
地址长度	1
P-CSCF地址	地址长度

地址类型：P-CSCF地址的类型。该域应根据下面的要求来设置P-CSCF地址类型。

值	名　字
00000000	FQDN
00000001	IPv4
00000010	IPv6
保留	保留

地址长度：P-CSCF的地址的长度。该域应以字节为单位设置P-CSCF的地址长度。

P-CSCF地址：代理呼叫会话控制功能的地址。该域应设置代理呼叫会话控制功能的地址。当P-SCSF类型设置为0x00时，P-CSCF应根据IETF RFC 3629中定义的UTF-8编码规则来编码为8位字符。

注：‘80’是指URI TLV数据对象；‘81’是指P-CSCF TLV数据对象。

5.5.66 $EF_{BAKPARA}$（当前使用的BAK参数）

如果分配了第39号业务，则该EF应出现。

这个EF包含3个已经被传送到R-UIM，并正在使用的BAK密钥的参数：BCMCS_Flow_ID、BAK_ID和BAK_Expire。

标识符：“6F63”	结构：线性定长	可选项
文件大小：*X*+*Y*+*Z*+3字节	更新频度：高	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	BCMCS_Flow_ID的长度	M	1
2～*X*+1	BCMCS_Flow_ID	M	*X*
X+2	BAK_ID的长度	M	1
X+3～*X*+*Y*+2	BAK_ID	M	*Y*
X+*Y*+3	BAK_Expire的长度	M	1
X+*Y*+4～*X*+*Y*+*Z*+3	BAK_Expire	M	*Z*

- BCMCS_Flow_ID的长度

内容：紧跟的后面的包含BCMCS流标识的数据项的字节数。

编码：二进制。

- BCMCS_Flow_ID

内容：BCMCS流标识。

编码：二进制。空字节应被设置为‘FF’，并且不作为数值的一部分。

- BAK_ID的长度

内容：紧跟的后面的包含BAK_ID标识的数据项的字节数。

- BAK_ID

内容：BAK_ID标识。

编码：二进制。空字节应被设置为‘FF’，并且不作为数值的一部分。

- BAK_Expire的长度

内容：紧跟的后面的包含BAK_Expire的数据项的字节数。

编码：二进制。

- BAK_Expire

内容：BAK_Expire。

编码：二进制。空字节应被设置为‘FF’，并且不作为数值的一部分。

5.5.67 $EF_{UpBAKPARA}$（更新的 BAK 参数）

如果分配了第39号业务，则该EF应出现。

这个EF包含3个已经被传送到R-UIM，但还没有被使用的BAK密钥的参数BCMCS_Flow_ID、BAK_ID和BAK_Expire。

标识符：“6F64”	结构：循环	可选项
文件大小：*X*+*Y*+*Z*+3字节	更新频度：高	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1	BCMCS_Flow_ID的长度	M	1
2～*X*+1	BCMCS_Flow_ID	M	*X*
X+2	BAK_ID的长度	M	1
X+3～*X*+*Y*+2	BAK_ID	M	*Y*
X+*Y*+3	BAK_Expire的长度	M	1
X+*Y*+4～*X*+*Y*+*Z*+3	BAK_Expire	M	*Z*

- BCMCS_Flow_ID的长度

内容：紧跟的后面的包含BCMCS流标识的数据项的字节数。

编码：二进制。

- BCMCS_Flow_ID

内容：BCMCS流标识。

编码：二进制。空字节应被设置为‘FF’，并且不作为数值的一部分。

- BAK_ID的长度

内容：紧跟的后面的包含BAK_ID标识的数据项的字节数。

编码：二进制。

- BAK_ID

内容：BAK_ID标识。

编码：二进制。空字节应被设置为‘FF’，并且不作为数值的一部分。

- BAK_Expire的长度

内容：紧跟的后面的包含BAK_Expire的数据项的字节数。

编码：二进制。

- BAK_Expire

内容：BAK_Expire。

编码：二进制。空字节应被设置为‘FF’，并且不作为数值的一部分。

5.5.68 EF_{MMSN}（MMS 通知）

如果分配了第40号业务，则该EF应出现。这个EF包含ME从网络接收到的组成MMS通知的信息（和相关参数）。

标识符：“6F65”	结构：线性定长	可选项
文件大小：4+*X*字节	更新频度：低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字　节	描　述	M/O	长度（字节）
1～2	MMS状态	M	2
3	MMS实现	M	1
4～*X*+3	MMS通知	M	*X*
X+4	扩展文件记录编号	O	1

- MMS状态

内容：状态字节包含通知的状态信息。

编码：b1指示了是否有有效数据或空间是否空闲。b2指示了MMS通知是否已经被读取。b3～b4指示了MM重获、MM拒绝或MM前转状态，字节1的b5～b8和字节2的所有比特为RFU。

字节 1：

b8	b7	b6	b5	b4	b3	b2	b1	
				X	X	X	0	空间空闲
				X	X	X	1	空间已使用
				X	X	0	1	通知未读
				X	X	1	1	通知已读
				0	0	X	1	MM 未被重获
				0	1	X	1	MM 被重获
				1	0	X	1	MM 被拒绝
				1	1	X	1	MM 被前转
								RFU

- MMS实现方式

内容：MMS实现指示了MMS的实现方式，例如WAP、M-IMAP和SIP。

编码：比特分配如下。

比特编号参数指示：

1 MMS使用WAP实现

2 MMS使用M-IMAP实现

3 MMS使用SIP实现

4～8 RFU

比特数值的含义：

0 不支持该实现方式

1 支持该实现方式

- MMS通知

内容：包含MMS通知。

编码：MMS通知按照字节3中指示的MMS实现方式编码。不使用的字节设置为‘FF’。

- 扩展文件记录编号

内容：这个字节标识了在EF_{EXTS}中包含了通知信息的扩展数据的记录的编号。该字节为可选项。如果不使用该字节则设置为‘FF’。

编码：二进制。

5.5.69 EF_{EXTS}（扩展 8）

如果分配了第41号业务，则该EF应出现。

这个EF包含MMS通知的扩展数据（多媒体消息业务）。

标识符：“6F66”	结构：线性定长	可选项
文件大小：X+2字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字 节	描 述	M/O	长度（字节）
1	记录类型	M	1
2～X+1	扩展数据	M	X
X+2	标识	M	1

内容和编码见3GPP TS31.102中EF_{EXT1}的内容和编码方式。

5.5.70 EF_{MMSICP}（MMS 业务提供者连接参数）

如果分配了第40号业务，则该EF应出现。

这个EF包含由发行商决定的多媒体消息连接参数值，ME可以将该参数用于MMS网络连接。这个文件可以包含一个或多个多媒体消息连接参数组。第一组参数作为缺省设置。每一组参数都可以包含一个或多个到核心网的接口和承载信息TLV对象（仅对于WAP），但只能包含一个MMS实现TLV对象（对于WAP，M-IMAP和SIP），即一个MMS 中继/服务商 TLV对象（对于WAP，M-IMAP和SIP）和一个网关TLV对象（仅对于WAP）。在MMS连接TLV对象中，到核心网的接口顺序和承载信息TLV对象定义了到核心网的接口和承载信息的优先级，其中第一个TLV对象具有最高优先级。

标识符："6F67"	结构：透明	可选项
文件大小：X_1+...+X_n字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～X_1	MMS连接参数TLV对象	M	X_1
X_1+1～X_1+X_2	MMS连接参数TLV对象	O	X_2
...	...		
X_1+...+X_{n-1}+1～X_1+...+X_n	MMS连接参数TLV对象	O	X_n

- MMS连接参数标签

描　述	标签值
MMS连接参数标签	'AB'
MMS中继/服务商标签	'80'
MMS实现参数标签	'81'
到核心网的接口和承载信息标签	'82'
网关标签	'83'
MMS鉴权机制标签	'84'
MMS鉴权ID标签	'85'

- MMS连接参数内容

表　述	值	M/O	长度（字节）
MMS连接参数标签	'AB'	M	1
长度	注1	M	注2
MMS实现方式标签	'80'	M	1
长度	1	M	1
MMS实现方式	--	M	1
MMS 中继/服务商 标签	'81'	M	1
长度	X	M	注2
MMS 中继/服务商 地址	--	M	X
到核心网的第1个接口和承载信息标签（最高优先级）	'82'	C2	1
长度	Y1	C2	注2
到核心网的第1个接口和承载信息	--	C2	Y1
到核心网的第2个接口和承载信息标签	'82'	C2	1
长度	Y2	C2	注2
到核心网的第2个接口和承载信息	--	C2	Y2
...			
到核心网的第n个接口和承载信息标签（最低优先级）	'82'	C2	1
长度	Y3	C2	注2
到核心网的第n个接口和承载信息	--	C2	Y3
网关标签	'83'	O	1
长度	Z	O	注2

表　述	值	M/O	长度（字节）
网关信息	--	O	Z
MMS鉴权机制标签	'84'	C1	1
长度	X	C1	注2
MMS鉴权机制	--	C1	X
MMS鉴权ID标签	'85'	C1	1
长度	X	C1	注2
MMS鉴权ID（Login_ID）	--	C1	X
注1：构造TLV对象的总大小 注2：长度编码遵照ISO/IEC 8825 C1：只有当标签80指示了M-IMAP或SIP时才出现 C2：只有当标签80指示了WAP时才出现			

- MMS实现方式标签'80'：内容和编码参考EF_{MMSN}中的信息。
- MMS中继/服务商标签'81'

内容：包含与MMS 中继/服务商相关的地址；另外，对于M-IMAP和SIP，鉴权机制和鉴权ID（Login ID）也包含在内。

编码：MMS中继/服务商地址编码为适合于MM1实现所使用的URI，例如SIP和M-IMAP。

- 到核心网的接口和承载信息标签'82'

内容：到核心网的接口和承载信息包含以下用于建立承载的信息：承载、地址、地址类型、速率、呼叫类别、鉴权类型、鉴权ID、鉴权口令。

编码：依据TSG-X.S0016-200中的要求来编码。如果MMS实现方式为WAP，则第一个到核心网的接口和承载信息为必选项。如果MMS实现方式为M-IMAP或SIP，则不需要到核心网的接口及承载信息。

- 网关标签'83'

内容：网关包含以下信息：地址、地址类型、端口、业务、鉴权类型、鉴权ID及鉴权口令。

编码：依据TSG-X.S0016-200中的要求来编码。

- MMS鉴权机制标签'84'

内容：MMS鉴权机制包含用于MMS的鉴权机制。对于M-IMAP和SIP该项为必选项。

编码：MMS鉴权机制按照6.10节的规定进行编码。

- MMS鉴权ID标签'85'

内容：MMS鉴权ID包含用于MMS的鉴权ID。对于M-IMAP和SIP该项为必选项。

编码：依据TSG-X.S0016-200中的要求来编码。

未使用的字节设置为'FF'。

5.5.71 EF_{MMSUP}（MMS 用户首选参数）

如果分配了第40号业务，则该EF应出现。

这个EF包含MMS用户首选参数，ME可以使用该参数作为移动多媒体消息准备时的用户辅助信息（例如：经常使用的缺省参数值）。

标识符："6F68"	结构：线性定长	可选项	
文件大小：*X*字节	更新频度：低		
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
字　节	描　述	M/O	长度（字节）
1～*X*	MMS用户首选参数TLV对象	M	*X*

- MMS用户优选标签

描　述	标签值
MMS实现方式标签	'80'
MMS用户首选概要名称标签	'81'
MMS用户首选信息标签	'82'

- MMS用户优选参数信息

描　述	值	M/O	长度（字节）
MMS实现方式标签	'80'	M	1
长度	1	M	注
MMS实现方式	--	M	1
MMS用户首选概要名称标签	'81'	M	1
长度	*X*	M	注
MMS用户概要名称	--	M	*X*
MMS用户首选信息标签	'82'	M	1
长度	*Y*	M	注
MMS用户首选信息	--	M	*Y*
注：长度按照ISO/IEC 8825进行编码。			

- MMS实现标签'80'，内容和编码参考EF_{MMSN}中的信息。
- MMS用户首选概要名称标签'81'

内容：MMS用户首选概要名称的Alpha标签。

编码：该Alpha标签可以使用以下两种方式。

■ SMS缺省7比特按照3GPP TS 23.038中定义的字母表进行编码，比特8设置为0；

■ ETSI TS 102 221中附录A所定义的UCS2编码选项。

- MMS用户首选信息标签'82'

内容：以下信息被编码：发送者显示、传送报告、读取-回复、优先权、终止时间和提前发送时间。

编码：取决于标签'80'中指示的MMS实现方式。

5.5.72 EF_{MMSUCP}（MMS 用户连接参数）

如果分配了第40号和42号业务，则该EF应出现。

这个EF包含由用户决定的MMS用户连接参数的值，ME可以使用该参数用于MMS网络连接。这个文件可以包含一个或多个MMS用户连接参数组。每一组参数都可以包含一个或多个到核心网的接口和承载信息TLV对象（仅对于WAP），但只能包含一个MMS执行TLV对象（对于WAP，M-IMAP和SIP），也即一个MMS 中继/服务商TLV对象（对于WAP，M-IMAP和SIP）和一个网关TLV对象（仅对于WAP）。在

MMS连接TLV对象中，到核心网的接口顺序和承载信息TLV对象定义了到核心网的接口和承载信息的优先级，其中第一个TLV对象具有最高优先级。

标识符："6F69"	结构：透明	可选项
文件大小：X_1+...+X_n字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1/CHV2	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～X_1	MMS连接参数TLV对象	M	X_1
X_1+1～X_1+X_2	MMS连接参数TLV对象	O	X_2
...	...		
X_1+...+X_{n-1}+1～X_1+...+X_n	MMS连接参数TLV对象	O	X_n

内容和编码见5.4.69节。

5.5.73 $EF_{AuthCapability}$（鉴权能力）

如果分配了第43号业务，则该EF应出现。这个EF存储R-UIM卡所支持的每一个应用的鉴权能力。

标识符："6F6A"	结构：线性定长	可选项
文件大小：5字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

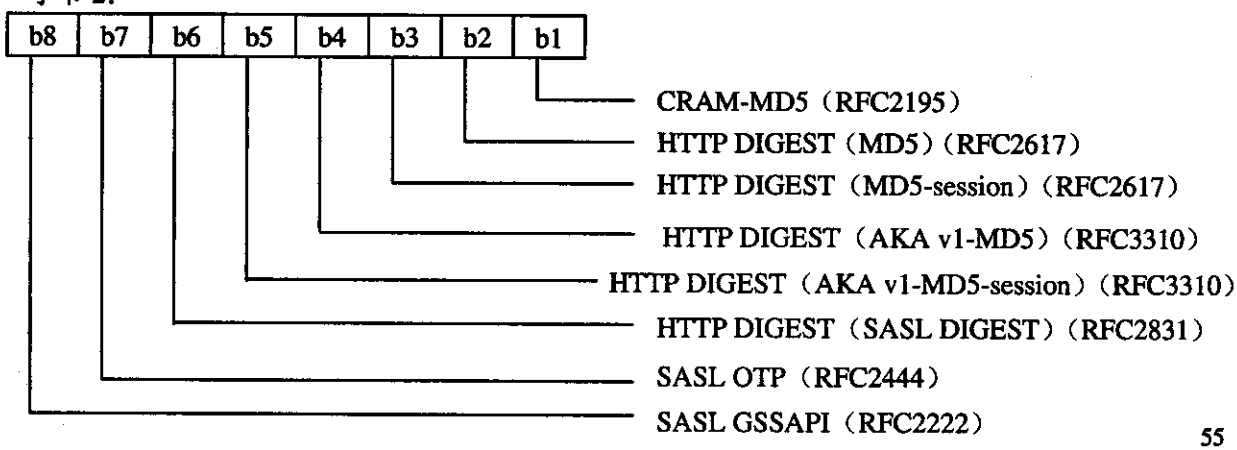
字　节	描　述	M/O	长度（字节）
1	应用ID	M	1
2～3	鉴权能力	M	2
4～5	保留	M	2

编码：

字节1：应用ID的编码如下：

二进制值	应用ID
'00000000'	MMS
'00000001'	MMD
'00000010' ～ '11111111'	保留

字节 2：



字节3到5为RFU。

R-UIM应设置每一个它所支持的鉴权机制对应的比特为‘1’。

5.5.74 EF_{3GCIK}（3G 加密密钥和完整性保护密钥）

如果分配了第30号业务，则该EF应出现。

这个EF包含加密密钥CK和完整性保护密钥IK。

标识符：“6F6B”	结构：透明	可选项
文件大小：32字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～16	加密密钥CK	M	16
17～32	完整性保护密钥IK	M	16

- 加密密钥CK

编码：CK的LSB为第16个字节的LSB，CK的MSB为第一个字节的MSB。

- 完整性保护密钥IK

编码：IK的LSB为第32个字节的LSB，IK的MSB为第17个字节的MSB。

5.5.75 EF_{DCK}（解个性化控制密钥）

如果分配了第46号业务，则该EF应出现。这个EF存储与OTA解个性化周期相关的解个性化控制密钥。

标识符：“6F6C”	结构：透明	可选项
文件大小：20字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	CHV1	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～4	网络类型1的解个性化控制密钥的8位数字	M	4
5～8	网络类型2的解个性化控制密钥的8位数字	M	4
9～12	服务提供商的解个性化控制密钥的8位数字	M	4
13～16	公司解个性化控制密钥的8位数字	M	4
17～20	HRPD网络的解个性化控制密钥的8位数字	M	4

空的密钥控制记录编码为‘FFFFFFFF’。

5.5.76 EF_{GID1}（组标识级别 1）

当分配了第44号业务时，该EF应存在。这个EF用于标识具有特殊应用的R-UIM群组。

标识符：“6F6D”	结构：透明	可选项
文件大小：1～*n*字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～*n*	R-UIM组标识符	O	*n*

5.5.77 EF_{GDI2}（组标识级别 2）

当分配了第45号业务时，该EF存在。这个EF用于标识具有特殊应用的R-UIM群组。

标识符："6F6E"	结构：透明	可选项
文件大小：1～*n*字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～*n*	R-UIM组标识符	O	*n*

注：EF_{GID1}和EF_{GID2}是相同的。网络运营商可以使用这两个EF来实现具有不同安全级别的应用。

5.5.78 $EF_{CDMACNL}$（CDMA 合作网络列表）

如果分配了第47号业务，则该EF应出现。这个EF包含具有个性化业务的多网络的合作网络列表。

标识符："6F6F"	结构：透明	可选项
文件大小：7n字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～7	合作网络列表单元1	M	7
7*n*-6～7*n*	合作网络列表单元n	O	7

- 合作网络列表

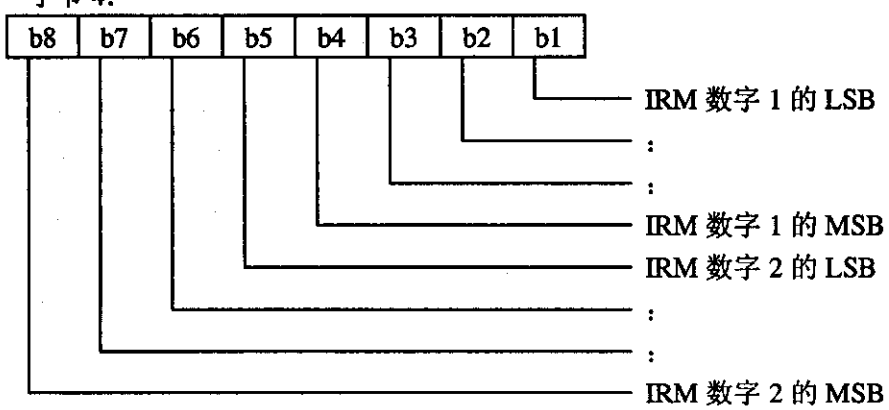
内容：业务提供商ID和合作网络法人ID。

编码：每7个字节构成一个单元。

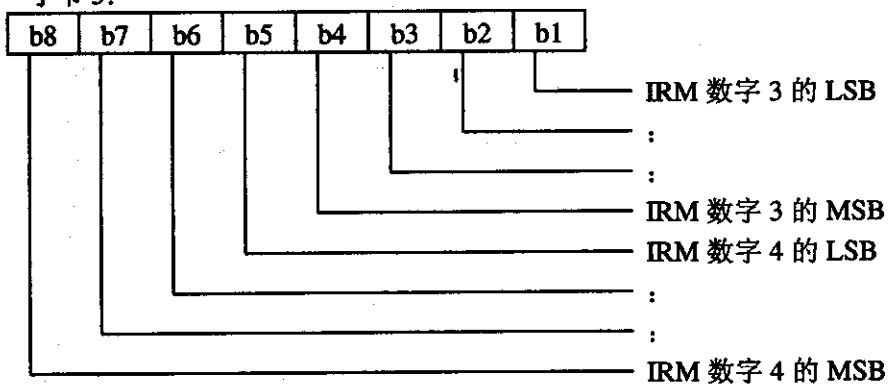
字节1到3：PLMN（MCC+MNC）

字节4到5：基于MIN的国际漫游（IRM）的4位有效数字。

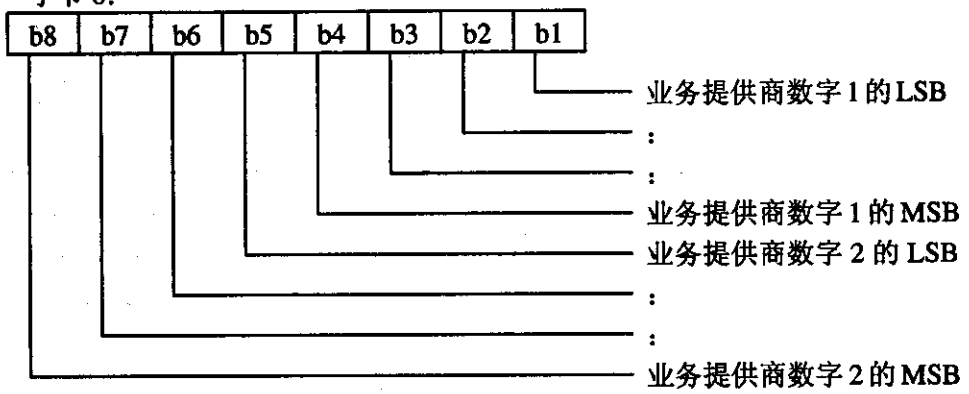
字节 4：



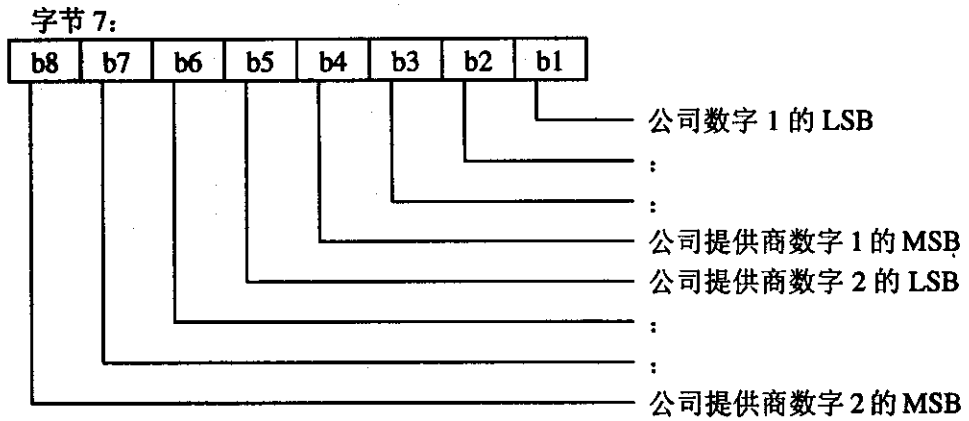
字节 5：



字节 6：



字节 7：



空的字节编码为‘FF’。

列表的结尾通过将第一个MCC域编码为‘FFF’来识别。

5.5.79 EF_{HOME_TAG}（归属系统标签）

这个EF包含归属系统标签，它在3GPP2 C.S0016-C的3.5.10.1节描述。

标识符：“6F70”	结构：透明	必选项
文件大小：X字节	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～X	归属系统标签	M	可变

5.5.80 EF_{GROUP_TAG}（组标签列表）

这个EF包含归组标签列表，它在3GPP2 C.S0016-C的3.5.11节描述。

标识符："6F71"	结构：透明	必选项
文件大小：'GROUP_TAG_LIST_SIZE'	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～GROUP_TAG_LIST_SIZE	归属系统标签	M	可变

5.5.81 $EF_{SPECIFIC\_TAG}$（特殊标签列表）

这个EF包含特殊标签列表，它在3GPP2 C.S0016-C的3.5.11节描述。

标识符："6F72"	结构：透明	必选项
文件大小：'SPEC_TAG_LIST_SIZE'	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～SPEC_TAG_LIST_SIZE	特殊标签列表	M	可变

5.5.82 EF_{CALL_PROMPT}（快速呼叫列表）

这个EF包含快速呼叫列表，它在3GPP2 C.S0016-C的3.5.11节描述。

标识符："6F73"	结构：透明	必选项
文件大小：'CALL_PRMPT_LIST_SIZE'	更新频度：低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

字　节	描　述	M/O	长度（字节）
1～CALL_PRMPT_LIST_SIZE	快速呼叫列表	M	可变

5.5.83 EF_{SF_EUIMID}（短 EUIMID）

5.5.84 如果分配了第 8 号业务，该文件应存在。这个 EF 存储了 56 比特的惟一识别 R-UIM 的电子标识码。

标识符："6F74"	结构：透明	必选项
文件大小：7字节	更新频度：低	
访问条件： READ ALW UPDATE Never INVALIDATE Never REHABILITATE Never		

字　节	描　述	M/O	长度（字节）
1	最低位字节	M	1
2	:	M	1
3	:	M	1
4	:	M	1
5	:	M	1
6	:	M	1
7	最高为字节	M	1

5.6 分组数据安全相关参数的编码

5.6.1 概述

本节规定了作为隐藏文件存储在UIM卡中的分组数据安全相关参数的编码。这些参数用于UIM卡对基于IP网络的鉴权操作。仅当安全模式打开时，这些参数也可以通过OTA命令（如：3GPD配置/下载请求命令）来读取或更新。如果R-UIM接收到3GPD配置请求命令或3GPD下载请求命令，命令包含简单IP CHAP SS的Block_ID，移动IP SS的Block_ID或HRPD接入鉴权CHAP SS参数块，并且安全模式没有被激活，那么R-UIM应返回SW1='69'和SW2='82'。

5.6.2 简单 IP CHAP SS 参数

如果分配了第20号业务，则应该具有简单IP CHAP SS参数，其编码如下：

字　节	描　述	长度（字节）
1	简单IP CHAP SS 参数块的长度	1
2～*X*+1	简单IP CHAP SS 参数块	*X*

参数块见3GPP2 C.S0016-C中第3.5.8.10节。

5.6.3 移动 IP SS 参数

如果分配了第38号业务，则应该具有移动IP CHAP SS参数，其编码如下：

字　节	描　述	长度（字节）
1	移动IP CHAP SS参数块长度	1
2～*X*+1	移动IP SS 参数块	*X*

参数块见3GPP2 C.S0016-C中第3.5.8.11节。

5.6.4 HRPD 接入鉴权 CHAP SS 参数

HRPD接入鉴权CHAP SS参数编码如下，当第5号业务被置为'11'时，应提供此参数。

字　节	描　述	长度（字节）
1	HRPD接入鉴权CHAP SS参数块长度	1
2～*X*+1	HRPD接入鉴权CHAP SS参数块	X

参数块见3GPP2 C.S0016-C中第3.5.8.14节。

5.7 在IETF协议中使用的共享保密数据的编码

本节定义了在R-UIM中安全存储的共享保密数据的编码，R-UIM使用该数据实现鉴权功能。

如果分配了第40号业务，则共享保密数据应存在，且其编码如下：

字　节	描　述	长度（字节）
1～2	共享保密数据的长度	2
3～*X*+2	共享保密数据	*X*

5.8 多模卡

多模卡（例如：CDMA和GSM）应同时满足本标准和3GPP TS51.011的要求。对于支持多模卡的多模终端，当一种模式初始化失败时，终端应尝试使用另一种模式进行初始化。

6 鉴权和安全

注：本章描述了ME与R-UIM卡之间的接口。包括参数存储和参数交换流程，与安全相关的功能和命令以及BCMCS命令等。对鉴权过程的测试使用3GPP2 S.S0053-0中第3章所描述的测试流程。

6.1 参数存储和参数交换流程

在R-UIM卡中存储了下列参数：

（1）鉴权算法和密钥生成算法。目前基于ANSI-41的安全操作采用CAVE算法。

（2）A-key，仅用于密钥生成运算。A-key可以由运营商直接写入R-UIM。ME无法读取A-key。在一些程序的执行期间，R-UIM卡中需要保存新旧两个A-key值。

（3）HRPD CHAP SS，用于MD5鉴权的密钥，可以由运营商直接写入R-UIM。ME无法读取HRPD SS。

（4）SSD，仅用于鉴权和密钥生成过程。ME无法读取SSD。在一些程序的执行期间，R-UIM卡中需要保存新旧两个SSD值。

（5）鉴权处理后密钥生成所使用的临时保密参数（如每个呼叫中产生的临时参数）。

（6）COUNT，可由ME读取。COUNT在网络命令下增加。

（7）IMSI，由IMSI_M 和IMSI_T组成。IMSI_M的低10位数字包含一个MIN。IMSI_T与MIN无关。ME可以读取签约标识。

（8）UIM_ID或伪UIMID（如果使用的是EUIM），保存在EF_{RUIMID}中，标识符为‘6F31’。

（9）SPC，标识符为‘6F33’，用于OTASP/OTAPA过程。

（10）OTAPA/SPC_Enable，标识符为‘6F34’。在OTASP/OTAPA 过程中，存储用户的输入。

（11）NAM_LOCK，标识符为‘6F35’。存储NAM的锁死/解锁状态。

（12）根密钥，只有Key Generation使用的算法可以访问根密钥。根密钥可以由业务提供商直接写入R-UIM，或者通过3GPP2 C.S0016-C所定义的程序写入R-UIM卡。ME不可以访问根密钥，因此本标准没有规定存储根密钥的方法。在执行某些程序的时候，需要存储新旧两个根密钥。

在ME中存储了下列参数：

（1）所有用于语音、用户数据和信令消息加密的算法；

（2）ECMEA和ECMEA_NF的密钥处理；

（3）ME的ESN；

（4）MEID；

（5）OTASP/OTAPA过程的控制机制。

在与安全相关的过程中下列参数从ME传递到R-UIM卡：

（1）RAND，统一随机查询。

（2）最后拨叫的号码，用于识别被叫方的号码的子集。R-UIM卡用这些参数组成“鉴权数据”域，见TIA/EIA-95-B中表6.3.12.1-1“Auth_Signature输入参数”。

（3）RANDU，由网络发出的一个单一随机查询。

（4）AUTHBS，在SSD更新过程中从网络发回的鉴权响应。

（5）RANDSeed，用于产生RANDBS的一个随机数。

（6）RANDSSD，初始化SSD更新时，随SSD更新命令由网络发出的参数。

（7）ME的ESN（ESN_ME），在R-UIM卡插入ME后从ME传递给R-UIM卡。在Run CAVE命令和Update SSD命令中ESN也被传递给R-UIM卡。如果UIM_ID使用指示='00'，那么使用在安全命令中接收到的ESN值用作鉴权算法的输入，而不管存储在EF_{ESN_ME}中的是什么值。

（8）ME Pseudo-ESN，在ESN不可获得的情况下，伴随Run CAVE命令和Update SSD命令出现的参数。

在OTASP/OTAPA过程中下列参数从ME传递到R-UIM卡：

（1）32bit的RANDSeed，伴随OTAPA请求的随机数。

（2）160bit的RANDSeed，MS密钥请求中的一个随机数参数。

（3）生成A-Key/Root Key的参数：P、P长度，G、G长度，A-Key协议版本，BS结果和BS结果长度。

（4）数据块ID、数据块长度、参数数据、偏移量和大小，这些参数涉及数据的存储，它们是配置、确认、下载请求消息的组成部分。

（5）开始/结束指示，OTAPA请求消息的一部分。

（6）P-ESN，伴随OTAPA请求命令产生的参数（如果ME分配了MEID，并且分配并激活了第9号业务）

在与安全相关的过程中下列参数从R-UIM卡传递到ME：

（1）AUTHR，是对“统一查询”的响应。

（2）与鉴权运算有关的密钥，密钥可以是64比特的密钥或不定长的‘VPM’。

（3）AUTHU，是对单一查询的响应。

（4）RANDBS，用于SSD更新过程的网络鉴权查询。

在OTASP/OTAPA过程中下列参数从R-UIM卡传递到ME：

（1）RAND_OTAPA，用于网络的确认。

（2）生成A-Key/Root Key的参数：MS结果和MS结果长度。

（3）结果代码，大多数命令使用结果代码指示成功/失败以及失败的原因。

（4）数据块ID、数据块长度、参数数据、偏移量和大小，用于识别存储数据的片断。

6.2 基于 ANSI-41 网络的与安全相关的功能描述

6.2.1 概述

ME应在同一DF环境下，按照一定的顺序，开始并结束与安全程序相关的所有命令的执行。

R-UIM卡主要执行3个操作：管理SSD、执行鉴权计算并产生密钥、管理呼叫历史记录参数。

6.2.2 管理 SSD

SSD用于所有鉴权响应计算和后续的密钥生成。SSD由存储在R-UIM中的“A-key”导出。当网络向手机发出含有RANDSSD参数的UPDATE SSD命令时，SSD开始更新过程。

用户的归属网络是惟一可以更新用户SSD的实体，见图2。当网络对某个用户发起一个SSD 更新时，用户的手机首先存储RANDSSD参数，然后产生一个随机数RANDSeed。手机向R-UIM卡传递RANDSeed参数，开始基站查询操作（Base Station Challenge Function）。随后，R-UIM卡产生RANDBS参数。RANDBS与RANDSeed的关系由R-UIM卡的发行者规定。例如，R-UIM卡可以设置RANDBS等于RANDSeed；RANDBS参数可以通过对RANDSeed参数进行伪随机处理导出或忽略RANDSeed而独立产生RANDBS。Base Station Challenge命令使R-UIM卡将RANDBS参数传递给手机再发给网络。

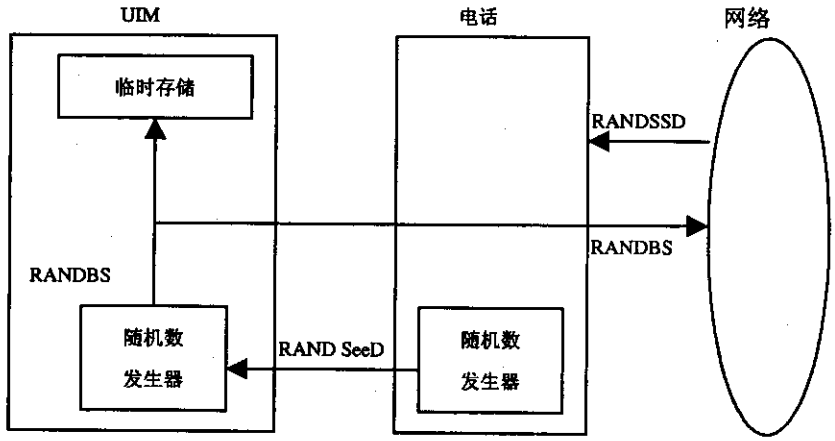


图 2　基站查询操作

接下来，手机通过向R-UIM卡发送命令执行Update SSD过程，该命令含有RANDSSD参数和控制数据域，见图3。然后R-UIM算出一个新的SSD值和一个预期的网络对RANDBS响应的AUTHBS值。计算中使用的ESN和IMSI值在R-UIM卡插入ME时已根据EF '6F42' 的指示确定。如果选择的是ESN而不是UIMID，那么鉴权算法所使用的参数应为从安全命令所接收到的值，而不管EF_{ESN_ME}中所存储的值。

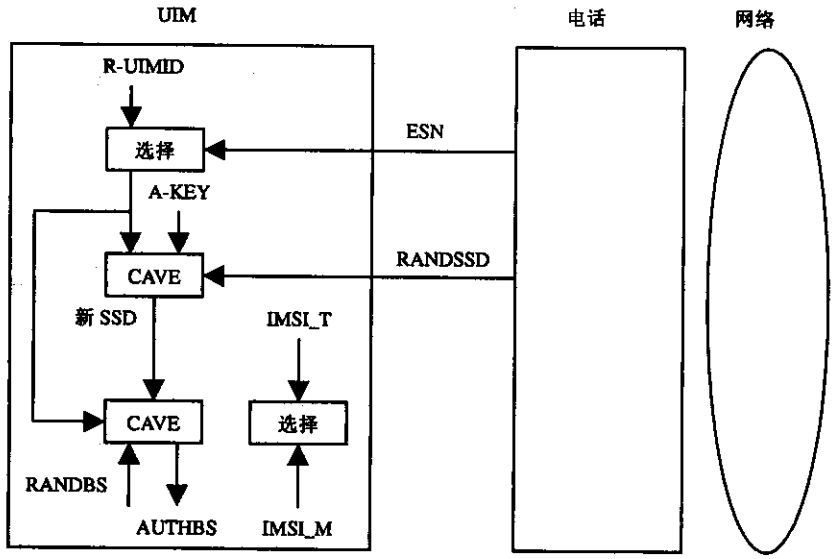


图 3　更新 SSD 操作、AuthBS 计算

在网络侧，RANDSSD参数用于为选定的R-UIM卡产生一个新的SSD值。网络从手机收到RANDBS参数后，与新的SSD一起算出AUTHBS，然后网络将AUTHBS发给手机，见图4。手机将收到的AUTHBS作为Confirm SSD命令的参数发给R-UIM卡。R-UIM卡比较收到的AUTHBS和它自己算出的AUTHBS值，如

果两个值相同，则SSD更新过程成功，SSD存入R-UIM卡的半永久内存并用于后面所有的鉴权计算。如果两个AUTHBS值不同，R-UIM就放弃新的SSD值仍保留当前的值，见图4。

如果SSD更新过程是OTASP/OTAPA过程的一部分，则在SSD更新过程执行中，手机应将“处理控制”的比特2设置为‘1’，这将使R-UIM卡在半永久内存中保留SSD的当前值而用新值重新进行鉴权计算。只有当R-UIM卡接收了网络发出的“Commit Request Message”后，才将SSD换为新值。

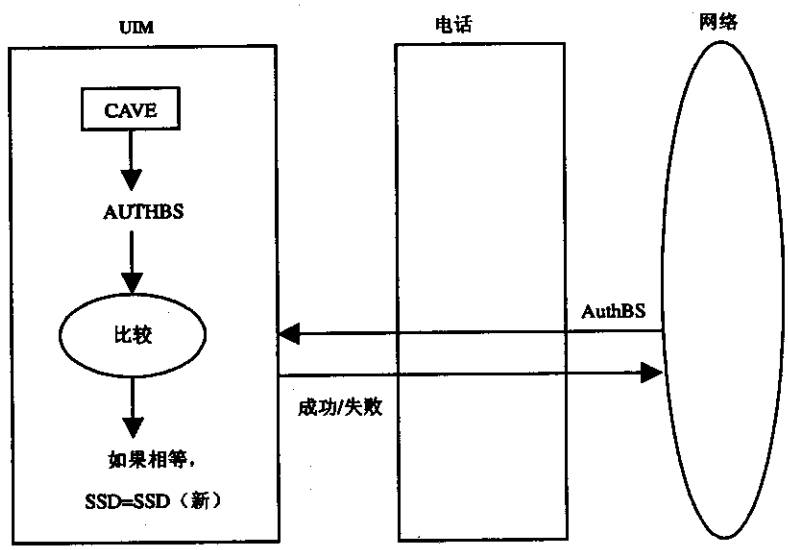


图 4 Confirm SSD 操作

6.2.3 执行鉴权计算和产生加密密钥

第二个与安全有关的R-UIM卡操作是执行鉴权计算和产生加密密钥，见图5，这个过程由RUN CAVE功能来实现。鉴权程序的输入参数为RAND （对于统一查询）或RANDU（对于单一查询）。其他由手机发出的参数可以是拨叫号码的一个子集。用于RUN CAVE操作的参数ESN和IMSI在R-UIM卡插入手机时确定。如果ESN（非UIMID）用于RUN CAVE功能，则将从安全命令中接收到的ESN值用于RUN CAVE算法，而不管EF_{ESN_ME}中存储了什么值。

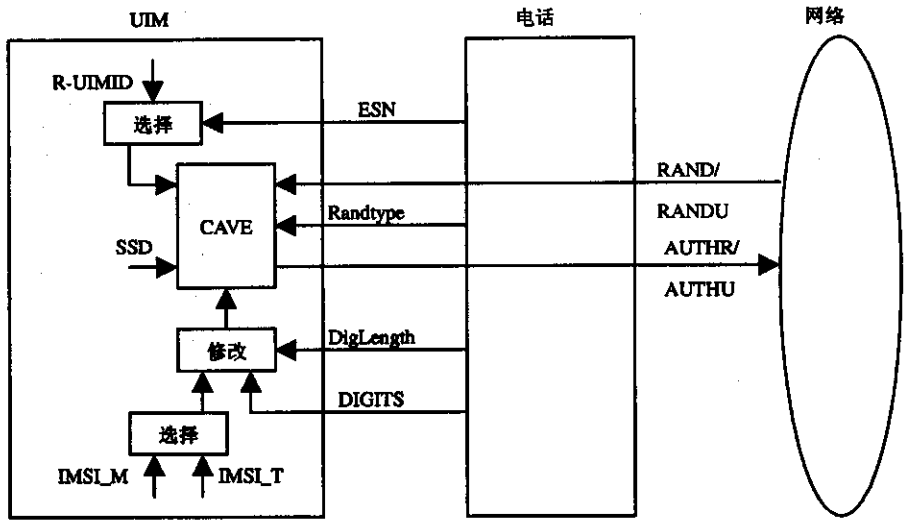


图 5 RUN CAVE 操作

R-UIM卡存储IMSI_M和IMSI_T，这两个参数的低10位数分别编码为34bit的两个子参数IMSI_M_S和IMSI_T_S。这两个参数的低7位再编码为24bit的IMSI_M_S1和IMSI_T_S1，第8-10位编码为10bit的

IMSI_M_S2和IMSI_T_S2。大多数应用的鉴权计算都使用IMSI_M_S1、IMSI_T_S1、IMSI_M_S2和IMSI_T_S2。这些计算中使用的IMSI在R-UIM卡插入手机时已确定。

Get RESPONSE命令使R-UIM卡将输出参数AUTHR或AUTHU传递给手机。临时参数则存储在R-UIM卡上用于计算加密密钥。

密钥的计算由Generate Key/VPM操作执行，见图6。Generate Key/VPM将处理在Run CAVE鉴权响应计算中产生并存储的临时参数，同时该操作将生成密钥。由Generate Key/VPM操作产生的密钥，有些直接用于手机加密，有些则在手机中进一步处理用于ECMEA和ECMEA_NF加密功能。

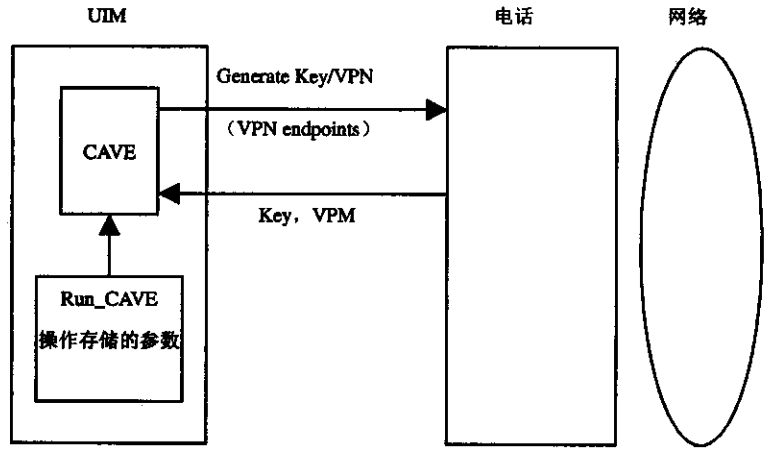


图 6　Generate Key/VPM 操作

6.2.4　管理呼叫历史记录参数

CALL COUNT用作复制检测器。在接入网络协议的时候，R-UIM卡向网络报告CALL COUNT的值，如果这个值与网络预期的值相同，网络就准予访问。在呼叫进行中可以由网络的命令增加CALL COUNT的值。

如果网络确认CALL COUNT的值不符，就查询R-UIM被复制的可能性，并采取补救措施。

通过标准的ME到R-UIM的命令可以增加和读取COUNT参数。

6.3　OTASP/OTAPA 功能描述（可选）

本节对支持OTASP/OTAPA的R_UIM卡的特性进行重点描述。首先介绍相关的EF，再介绍映射到R-UIM命令的“请求/响应”消息。某些情况下，OTASP/OTAPA功能需要ME来辅助完成。

6.3.1　OTASP/OTAPA 的基本文件

6.3.1.1　概述

OTASP/OTAPA有4个基本文件。

6.3.1.2　EF_{SPC}（业务编程代码）

该EF用于保护R-UIM不被未鉴权的程序修改其内容。

6.3.1.3　$EF_{OTAPASPC}$（OTAPA/SPC_Enable）

ME可以读和写这个EF。它允许用户激活对于R-UIM上的NAM的OTAPA保护。它也允许用户启用（或禁止）通过OTA来改变其SPC。

6.3.1.4　$EF_{NAMLOCK}$（NAM_LOCK）

3GPP2 C.S0016-C提供了在运营商的控制下，由用户提供适当的输入来“锁死”NAM内容的方法。这个EF存储NAM当前的状态（锁死/解锁）。

6.3.1.5 EF_{OTA}（OTASP/OTAPA 特性）

这个EF保存了OTASP/OTAPA 特性列表和相关的协议版本。ME读取该文件，并用参数组和这些信息来响应从网络发来的“协议能力请求消息”。

6.3.2 将 OTASP/OTAPA 请求/响应消息映射到 R-UIM 命令

6.3.2.1 概述

OTASP/OTAPA消息对在3GPP2 C.S0016-C中列出。在某些情况下，映射是一对一的。在其他情况下，ME会执行一些翻译工作以使用一些简单的R-UIM命令。还有一些情况，ME信赖基于安全的命令，并准备响应。

6.3.2.2 协议能力请求/响应消息

该消息请求同时存储在ME和R-UIM中的信息。ME读取“OTASP/OTAPA特性”文件以构成响应中的“特性”组成部分，然后添加ME中存储的信息来完成响应。

6.3.2.3 MS 密钥请求/响应消息

这个命令使R-UIM卡产生专用和公用密钥。这两个密钥用于Diffie/Hellman密钥交换以计算A-Key/Root Key。在从网络收到MS密钥请求消息后，手机产生一个160bit的随机数RANDSeed，并将RANDSeed与网络发出的模数P和发生器G一起发给R-UIM卡。R-UIM卡随后产生一个与RANDSeed相关的随机数x，R-UIM算出G^x模P，并将结果临时保存为MS_RESULT。R-UIM卡计算出“结果代码”并在MS密钥请求消息的响应中发给ME，ME再将其发给网络。

6.3.2.4 密钥生成请求/响应消息

这个请求/响应完成Diffie/Hellman密钥交换。网络向R-UIM 卡发送BS_RESULT，R-UIM卡返回MS_RESULT给网络。R-UIM卡计算（BS_RESULT）^{x}模P得出Diffie/Hellman结果，这个结果的一个子集临时保存为A-Key/Root Key。

6.3.2.5 SSD 更新

SSD更新是OTASP/OTAPA过程的一部分。在OTASP/OTAPA 过程期间，SSD更新过程使用临时的A-Key和SSD，直到R-UIM卡收到“Commit Request Message”后才将这些临时值存入半永久内存。这与TIA/EIA-95-B中有所不同，可以通过设置发给R-UIM卡的“UPDATE SSD”命令中的“处理控制”参数的bit2=1来标注这个不同之处。如果R-UIM接收到的内容超出了密钥生成过程的内容，则R-UIM将拒绝Update SSD命令，并返回SW1 SW2 = ‘9834’。

6.3.2.6 再鉴权请求/响应消息

在手机收到含有4字节RAND参数的再鉴权请求/响应消息后，按下列顺序产生响应消息：

（1）读EF_{COUNT}。

（2）准备AUTH_DATA （见3GPP2 C.S0016-C第3.3.2节）。

（3）截取RAND生成RANDC。

（4）用Run CAVE命令计算AUTHR，输入参数为：

a. RANDTYPE= ‘0000 0000’ （即32bit）

b. RAND=手机接收的RAND

c. 由AUTH_DATA指定的数位长度、数字

d. 处理控制：

bit0：0（未用）

bit1：0（未用）

bit2：1（存储A-Key、SSD前等待确认）

bit3：0（未用）

bit4：1（保存寄存器内容）

bit5：0（未用）

bit6：0（未用）

bit7：0（未用）

如果激活消息编码或话音加密，手机与R-UIM卡执行Generate Key/VPM操作。

6.3.2.7 确认请求/响应消息

手机接收到Validate Request消息，该消息是为了查询对数据块 “NUM_BLOCKS”（每个块长度为“BLOCK_LEN”）的确认。为了简化R-UIM卡命令编码，手机将数据放入不同的数据块，并用Validate 命令确认每个数据块的长度“BLOCK_LEN”，R-UIM卡用结果代码响应每个数据块，手机累加R-UIM卡的响应并发给网络。

6.3.2.8 配置请求/响应消息

手机接收的配置请求消息用于请求数据块“NUM_BLOCKS”配置细节。为了简化R-UIM命令编码，手机将该请求放入“NUM_BLOCK”单数据块请求中，并用Configuration Request命令向R-UIM卡查询每个数据块的配置细节。对于每个数据块，R-UIM卡用数据块ID、数据块长度、结果代码和参数数据响应。手机累积每个数据块的响应并发给网络。

6.3.2.9 下载请求/响应消息

手机接收的下载请求消息尝试将数据的“NUM_BLOCKS”下载到R-UIM卡，每个数据块包含数据块ID、数据块长度、具有“数据块长度”的参数数据。为简化R-UIM命令编码，手机将请求放入NUM_BLOCK单个数据块请求中，并尝试用Download Request 命令将数据块下载到R-UIM卡。在多个Download Request命令之前，手机可以查询适当的EF数据来确定在R-UIM卡的EF文件中是否有足够的存储空间完成下载操作。R-UIM 卡对每个Download Request 命令返回数据块ID和结果代码。手机累积数据块的响应并发给网络。

6.3.2.10 SSPR 配置请求/响应消息

网络请求存储在R-UIM卡中的SSPR数据。R-UIM卡用数据块ID、结果代码、数据块长度和参数数据响应。手机进行透明操作。

6.3.2.11 SSPR 下载请求/响应消息

网络使用此消息下载SSPR数据到R-UIM卡。数据包含数据块ID、数据块长度和具有“数据块长度”的参数数据。R-UIM卡用数据块ID、结果代码、数据段偏置和数据段大小响应。手机进行透明操作。

6.3.2.12 OTAPA 请求/响应消息

网络通过发送包含“起/止”参数的“OTAPA请求消息”初始化OTAPA。手机将此消息和RANDSeed发给R-UIM卡。R-UIM卡生成与RANDSeed相关的随机数RAND_OTAPA，R-UIM还为AUTH_OTAPA计算一个值（见3GPP2 C.S0016-C中第3.3.7节）。R-UIM卡将RAND_OTAPA、结果代码和NAM_LOCK指示发给手机，手机重新安排数据的格式并发给网络。

6.3.2.13 Commit 请求/响应消息

网络经手机将“Commit请求消息”发给R-UIM卡。手机将此消息转换为R-UIM卡的命令Commit。R-UIM卡用结果代码响应，手机用“Commit响应消息”将响应发给网络。

6.3.2.14 PUZL 配置请求/响应消息

网络请求存储在R-UIM特定区域中的PUZL数据。R-UIM用数据块ID、结果代码、数据块长度和参数数据来响应。该操作对于ME是透明的。参数的格式见3GPP2 C.S0016-C。

6.3.2.15 PUZL 下载请求/响应消息

网络尝试下载PUZL数据到R-UIM。数据包含数据块ID、数据块长度和具有“数据块长度”的参数数据。R-UIM用数据块ID、结果代码、标识符出现的标志、用户区域ID和用户区域系统ID来响应。对于该操作ME是透明的。

6.3.2.16 3GPD 配置请求/响应消息

ME接收到3GPD配置请求消息，该消息请求“NUM_BLOCKS”数据的详细配置信息，其中每一个数据块的长度都为“BLOCK_LEN”。为了简化R-UIM命令的编码，ME缓存请求到“NUM_BLOCKS”单个数据块请求中，然后通过向R-UIM发送3GPD配置请求命令为每一个数据块请求配置的详细信息。对于每一个数据块，R-UIM用数据块ID、数据块长度、结果代码和参数数据来响应。ME累积一组数据块的响应，把它们组合起来作为一个响应发送给网络。如果3GPD配置请求命令包含简单IP CHAP SS参数或移动IP SS参数的数据块ID，则R-UIM要检查安全模式是否被激活。如果安全模式没有被激活，那么R-UIM将返回响应SW1 SW2 = ‘69 82’。

6.3.2.17 3GPD 下载请求/响应消息

ME接收到3GPD下载请求消息，该消息尝试下载“NUM_BLOCKS”数据到R-UIM，每一个数据块都有数据块ID、数据块长度和具有‘数据块长度’的参数数据。为了简化R-UIM命令的编码，ME缓存请求到“NUM_BLOCK”单个数据块请求中，然后尝试通过3GPD下载请求命令下载每一个数据块到R-UIM。在发起多个下载请求前，ME首先查询相应的EF来判别R-UIM的EF是否具有足够的空间来成功的完成下载操作。每一次执行3GPD下载请求命令，R-UIM都返回数据块ID和结果代码。ME累积一组数据块的响应，把它们组合为一个响应发送给网络。如果3GPD下载请求命令包含简单IP CHAP SS参数或移动IP SS参数的数据块ID，则R-UIM要检查安全模式是否被激活。如果安全模式没有被激活，那么R-UIM将返回响应SW1 SW2 = ‘69 82’。

6.3.2.18 安全模式请求/响应消息

这个命令使R-UIM生成安全模式加密密钥（SMCK）。在安全模式被激活的情况下，R-UIM应使用SMCK作为在OTASP数据消息中R-UIM发送和接收到的所有参数块的PARAM-DATA的加密和解密密钥。

网络可以通过发送START_STOP域设置为‘1’的安全模式请求消息给ME来发起安全模式。在接收到START_STOP域设置为‘1’的安全模式请求消息时，ME翻译该消息为安全模式命令。R-UIM使用在该命令中接收到的RAND_SM和SSD来计算SMCK，然后R-UIM用结果代码来响应，ME通过“安全模式响应消息”转发该结果响应给网络。当安全模式激活时，在接收到以下消息的情况下，在发送任何其他命令前，ME应首先发送FRESH命令给R-UIM。

- SSPR配置请求消息
- PUZL配置请求消息
- 3GPD配置请求消息

- 下载请求消息
- SSPR下载请求消息
- PUZL下载请求消息
- 3GPD下载请求消息
- MMD配置请求消息
- MMD下载请求消息
- MMS配置请求消息
- MMS下载请求消息
- 系统标签配置请求消息
- 系统标签下载请求消息

对于配置请求消息，ME发送FRESH命令给R-UIM来请求选择15比特的FRESH值。选择可以是随机选择也可以通过设置一个单调增的计数器来选择。R-UIM用FRESH数值来响应该命令。

对于下载请求消息，ME发送FRESH命令给R-UIM将从网络接收到的FRESH值传送给R-UIM。

网络可以通过发送START_STOP域设置为“0”的安全模式请求消息给ME来终止安全模式。在接收到START_STOP域设置为“0”的安全模式请求消息时，ME翻译该消息为安全模式命令。R-UIM用结果代码来响应，然后ME通过“安全模式响应消息”转发该结果代码给网络。

6.3.2.19 业务密钥生成请求/响应消息

这个命令使R-UIM生成业务密钥，如：对于BCMCS、IMS、WLAN等的密钥。在生成业务密钥前，R-UIM应首先基于根密钥生成一个中间密钥。详细过程见3GPP2 C.S0016-C的3.3.10节。

6.3.2.20 MMD 配置请求/响应消息

网络请求存储在R-UIM特殊区域中的MMD数据。R-UIM用数据块ID、结果代码、数据块长度和参数数据来响应。ME进行透明传输。参数的格式见3GPP2 C.S0016-C。

6.3.2.21 MMD 下载请求/响应消息

网络请求下载MMD数据到R-UIM。数据包含数据块ID、数据块长度和参数数据，R-UIM用数据块ID和结果代码来响应。ME进行透明传输。

6.3.2.22 MMS 配置请求/响应消息

网络请求存储在R-UIM特殊区域中的MMS数据。R-UIM用数据块ID、结果代码、数据块长度和参数数据来响应。ME进行透明传输。参数格式见3GPP2 C.S0016-C。

6.3.2.23 MMS 下载请求/响应消息

网络下载MMS数据到R-UIM。数据包含数据块ID、数据块长度和参数数据。R-UIM用数据块ID和结果代码来响应。ME进行透明传输。

6.3.2.24 系统标签配置请求/响应消息

网络请求存储在R-UIM特殊区域中的系统标签数据。R-UIM用数据块ID、结果代码、数据块长度和参数数据来响应。ME进行透明传输。参数格式见3GPP2 C.S0016-C。

6.3.2.25 系统标签下载请求/响应消息

网络下载系统标签数据到R-UIM。数据包含数据块ID、数据块长度和参数数据。R-UIM用数据块ID、结果代码、数据分段偏移和数据分段大小来响应。ME进行透明传输。

6.4 基于 ANSI-41 网络的与安全相关的命令描述

6.4.1 概述

命令BASE STATION CHALLENGE、Update SSD、Confirm SSD按顺序执行。如果Update SSD或Confirm SSD命令顺序错误，R-UIM卡将返回SW1 SW2 = '9834'。

如果采用T=0协议，则命令APDU的映射按3GPP TS 51.011规范9.1节的规定处理。

在以下的命令处理过程中，RANDSSD、RANDSeed、RANDBS、AuthBS、RAND、RANDU、AUTHR及AUTHU等参数是按高字节在前进行编码。

ESN是按低字节在前进行编码，以与存储ESN_ME的EF文件'6F38'的编码相一致。

6.4.2 Update SSD

命　令	CLASS	INS	P1	P2	Lc	Le
UPDATE SSD	'A0'	'84'	'00'	'00'	'0F'	'00'

命令参数/数据：

字　节	描　述	长度（字节）
1～7	RANDSSD	7
8	Process_Control（注）	1
9～15	ESN	7

注：输入参数Process_Control编码如下：

bit0　保留。

bit1　保留。

bit2　规定了将最新计算出的SSD存入半永久内存的触发条件：

'000x 0000'表示经Confirm SSD 命令对AUTHBS成功确认；

'000x 0100'表示在OTASP/OTAPA期间接受Commit Request Message命令。

bit3　保留。

bit4　规定了是否需要保存存储器：

'0001 0x00'表示保存存储器ON；

'0000 0x00'表示保存存储器OFF。

如果保存存储器设置为ON，在产生鉴权响应后会使鉴权处理过程维持内部寄存器的状态。

bit4　只与Run CAVE命令有关，在该命令中在生成密钥后可以产生一个鉴权响应。

bit5～7　保留。

如果ME具有MEID，则Pseudo-ESN值将被用在ESN域中。如果EF_{USGIND}的比特1设置为0，那么R-UIM将使用接收到的ESN作为CAVE算法的输入。

6.4.3 BASE STATION CHALLENGE

命　令	CLASS	INS	P1	P2	Lc	Le
BASE STATION CHALLENGE	'A0'	'8A'	'00'	'00'	'04'	'04'

命令参数/数据：

字　节	描　述	长度（字节）
1～4	RANDSeed	4

响应参数/数据：

字　节	描　述	长度（字节）
1～4	RANDBS	4

6.4.4 Confirm SSD

命　令	CLASS	INS	P1	P2	Lc	Le
CONFIRM SSD	‘A0’	‘82’	‘00’	‘00’	‘03’	空

命令参数/数据：

字　节	描　述	长度（字节）
1～3	AuthBS	3

响应参数/数据：

该命令的执行无响应参数。命令执行成功，则SW1 SW2 = ‘90 00’；不成功，则SW1 SW2 = ‘98 04’。

如果ME分配了MEID，且EF_{USGIND}的比特1设置为0，那么在更新SSD命令中接收到的P-ESN被用作ESN输入到CAVE算法中进行AuthBS的计算。

6.4.5 Authenticate

6.4.5.1 概述

这个命令执行鉴权功能。

命　令	CLASS	INS	P1	P2	Lc	Le
Authenticate	‘A0’	‘88’	P1	‘00’	‘XX’	‘YY’

P1参数定义了鉴权命令的类型：

P1	含义
‘00’	Run Cave
‘01’	3G Access AKA
‘02’	EAP AKA

P1= ‘00’：2G鉴权-Run CAVE

命令参数/数据

字　节	描　述	长度（字节）
1	RANDTYPE（RAND/RANDU）	1
2～5	RAND/RANDU	4
6	DigLength（以bit为单位）	1
7～9	DIGIT	3
10	Process_Control	1
11～17	ESN	7

参数RANDTYPE的编码如下：

‘0000 0000’ RAND（统一随机查询）

‘0000 0001’ RANDU（单一随机查询）

RANDTYPE所有其他的值均为RFU。

如果RANDTYPE设置为RAND，那么RAND占用字节2～5。如果RANDTYPE设置为RANDU，那么RANDU占用字节3～5，字节2被忽略。

如果没有DIGITS输入给CAVE（例如：注册或单一查询），那么DigLenth=0并且字节7～9均为0。如果DIGITS包含在内，则字节9的b1～b4解码为DIGITS的最低位数字，下一位数字在字节9的b5～b8解码，

再下一位在字节8的b1～b4解码，依次类推直到字节7。如果输入的数字少于6个，则字节7～9用0填充。例如：如果数字为‘123’，则：

Byte6 = 0000 1100；

Byte7 = 0000 0000；

Byte8 = 0000 0001；

Byte9 = 0010 0011。

如果ME具有MEID，则在ESN域使用Pseudo-ESN值。R-UIM应使用接收到的ESN作为CAVE算法的输入。

响应参数/数据：

字　节	描　述	长度（字节）
1～3	AUTHR/AUTHU	3

输入参数Process_Control编码如下：

bit0　保留。

bit1　保留。

bit2　规定了将最新算出的SSD存入半永久内存的触发条件：

‘000x 0000’表示经Confirm SSD 命令对AUTHBS的成功确认；

‘000x 0100’表示在OTASP/OTAPA期间接受Commit Request Message命令。

bit3　保留，设置为‘0’。

bit4　规定了是否需要保存存储器：

‘0001 0x00’表示保存存储器ON；

‘0000 0x00’表示保存存储器OFF。

如果保存存储器设置为ON，在产生鉴权响应后会使鉴权处理过程维持内部寄存器的状态。

bit4　只与Run CAVE命令有关，在该命令中在生成密钥后产生一个鉴权响应。

bit5　保留，设置为‘0’。

程序控制（Process_Control）的bit6～7保留，设置为‘0’。

P1=‘01’：3G鉴权-AKA

在接收到该命令时，R-UIM可以使用根密钥生成IK、CK、RES、UAK（如果R-UIM支持这些参数），也可以发送AUTS（如果需要序列号再同步）。

命令参数/数据

字　节	描　述	长度（字节）
1～16	RANDA	16
17	AUTN长度（L1）	1
18～18+L1	AUTN	L1

其中AUTN=SQN ⊕ AK||AMF||MAC-A

响应参数/数据：

字　节	描　述	长度（字节）
1	同步失败标志	1

或者

2～17	加密密钥	16
18～33	完整性保护密钥	16
34	RES长度	1
35～35+RESLength-1	RES	RES 长度

或者

2～15	AUTS	14

如果R-UIM检测到无效的序列号，则R-UIM设置同步失败标志为‘00000001’，并且响应中包含AUTS；否则R-UIM设置同步失败标志为‘00000000’，并且响应中包含CK、IK、RES长度和RES。所有其他值都为RFU。

如果MACA比对失败，R-UIM返回状态字SW1 SW2=‘98 04’。

RES长度必须大于等于1。

P1=‘02’：WLAN鉴权-AKA

在接收到该命令时，R-UIM可以使用WLAN根密钥生成IK、CK、RES、UAK（如果R-UIM支持这些参数），也可以发送AUTS（如果需要序列号再同步）。

命令参数/数据：

字　节	描　述	长度（字节）
1～16	RANDA	16
17	AUTN的长度（L1）	1
18～18+L1	AUTN	L1

其中其中AUTN=SQN ⊕ AK||AMF||MAC-A

响应参数/数据：

字　节	描　述	长度（字节）
1	同步失败标志	1

或者

2～17	加密密钥	16
18～33	完整性保护密钥	16
34	RES长度	1
35～35+RESLength-1	RES	RES 长度

或者

2～15	AUTS	14

如果R-UIM检测到无效的序列号，则R-UIM设置同步失败标志为‘00000001’，并且响应中包含AUTS；否则R-UIM设置同步失败标志为‘00000000’，并且响应中包含CK、IK、RES长度和RES。所有其他值都为RFU。

如果MACA比对失败，R-UIM返回状态字SW1 SW2=‘98 04’。

RES长度必须大于等于1。

6.4.5.2 使用 Run CAVE 命令的注意事项

Run CAVE命令用于产生鉴权响应并允许后续命令调用来计算密钥。

如要生成加密密钥，Run CAVE命令将携带Process_Control参数，且该参数的比特4设置为‘1’。当鉴权响应经Get Response命令发出后，密钥生成命令可以被发出，该命令将基于Run CAVE命令执行时（Process_Control字节的比特4设置为‘1’）保存的参数执行密钥生成计算。

6.4.5.3 密钥生成命令的使用

在Run CAVE 命令(Process_Control字节的比特4设置为'1')执行后,可以随时调用Generate Key/VPM命令。在保存寄存器功能为OFF状态时可以执行一个或多个Run CAVE例程,但Generate Key/VPM的输入参数应该是在保存寄存器功能为ON状态时调用Run CAVE 命令后存储的参数值。在执行了GET RESPONSE命令后,Generate Key/VPM将向主机发送64比特的密钥。

6.4.6 Generate Key/VPM

Generate Key/VPM依赖于RUN CAVE命令的成功执行,且应激活"Save"功能。如果RUN CAVE命令没有成功执行,则在调用该命令时应返回状态字SW1 SW2 = '98 34'。

命 令	CLASS	INS	P1	P2	Lc	Le
GENERATE KEY/VPM	A0	8E	00	00	02	*

命令参数/数据:

字 节	描 述	长 度(字节)
1	输出VPM的第一个字节的偏移地址	1
2	输出VPM的最后一个字节的偏移地址	1

详细数值:

字 节		描 述	长 度(字节)
1	2		
XX	*YY*	重获的长度为(*YY*−*XX*+1)的VPM被输出	*YY*−*XX*+1
FF	FF	不输出VPM	0

注:如果有VPM输出,则XX和YY的值在00～40之间。

响应参数/数据:

字 节	描 述	长 度(字节)
1～8	密钥	8
9～*	VPM字节	*

*取决于由命令参数规定的输出VPM字节数。

6.5 OTASP/OTAPA 命令的描述(可选)

6.5.1 MS 密钥请求

命令	CLASS	INS	P1	P2	Lc	Le
生成公共密钥	A0	50	00	00	*	01

命令参数/数据

字 节	描 述	长度(字节)
1～20	RANDSeed	20
21	A-Key 协议版本	1
22	参数P的长度	1
23	参数G的长度	1
24～*X*	参数P	参数P的长度
X+1～*Y*	参数G	参数G的长度

*如果A-Key协议版本大于'00000010',参数P和参数G的长度设置为'00000000',并且参数P和参数G应被忽略。

命令参数的详细信息见3GPP2 C.S0016-C中4.5.1.3节"MS密钥请求消息"。

响应参数/数据:

字　节	描　述	长度（字节）
1	结果代码	1

6.5.2 密钥生成请求

命令	CLASS	INS	P1	P2	Lc	Le
密钥生成请求	A0	52	00	00	*	**

命令参数/数据：

字　节	描　述	长度（字节）
1	BS_RESULT长度	1
2～Lc	BS_RESULT	Lc-1

*注：Lc=BS结果长度（字节）+1

命令参数的详细信息见3GPP2 C.S0016-C中4.5.1.4节。

响应参数/数据：

字　节	描　述	长度（字节）
1	结果代码	1
2	MS_RESULT长度	1
3～Lc	MS_RESULT	Lc-2

**注：Le=MS结果长度（字节）+2

命令参数的详细信息见3GPP2 C.S0016-C中4.5.1.4节。

6.5.3 Commit

命令	CLASS	INS	P1	P2	Lc	Le
Commit	A0	CC	00	00	空	01

响应参数/数据：

字　节	描　述	长度（字节）
1	结果代码	1

Commit请求和响应的详细信息分别见3GPP2 C.S0016-C的第4.5.1.6节和第3.5.1.6节。

6.5.4 Validate

命令	CLASS	INS	P1	P2	Lc	Le
Validate	A0	CE	00	00	*	02

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	数据块长度	1
3～Lc	参数数据	Lc-2

这个命令请求对数据的单个块进行确认并构成“确认请求消息”的子集。

*注：Lc=参数数据的长度+2

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1

这个响应属于单个数据块，并构成“确认请求消息”的子集。

6.5.5 配置请求

命　令	CLASS	INS	P1	P2	Lc	Le
配置请求	A0	54	00	00	01	*

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1

这个命令请求单个数据块的详细配置信息并构成“配置请求消息”的子集。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	数据块长度	1
3	结果代码	1
4～Le	参数数据	Le-3

*注：Le=参数数据长度+3

这个响应提供了单个数据块的详细配置参数，并构成“配置请求消息”的子集。

6.5.6 下载请求

命　令	CLASS	INS	P1	P2	Lc	Le
下载请求	A0	56	00	00	*	02

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	数据块长度	1
3～Lc	参数数据	Lc-2

这个命令请求下载单个数据块，并构成“下载请求消息”的子集。

*注：Lc=参数数据长度+2

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1

这个响应属于单个数据块，并构成“下载请求消息”的子集。

6.5.7 SSPR 配置请求

命　令	CLASS	INS	P1	P2	Lc	Le
SSPR配置请求	A0	EA	00	00	04	*

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2～3	请求的偏移量	2
4	请求的最大尺寸	1

注：如果数据块ID=‘0000 0001’（首选漫游列表参数块），那么字节2～4作为该命令的输入。对于其他的数据块ID，字节2～4被忽略。

命令参数详见3GPP2 C.S0016-C的4.5.1.8节“SSPR配置请求消息”。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1
3	数据块长度	1
4～Le	参数数据	Le-3

*注：Le=参数数据长度+3

响应详见3GPP2 C.S0016-C的4.5.1.8节“SSPR配置请求消息”。

6.5.8 SSPR下载请求

命　令	CLASS	INS	P1	P2	Lc	Le
SSPR下载请求	A0	EC	00	00	*	05

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	数据块长度	1
3～Lc	参数数据	Lc-2

*注：Lc=参数数据长度+2

命令参数详见3GPP2 C.S0016-C的4.5.1.9节“SSPR下载请求消息”。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1
3～4	数据分段的偏移	2
5	数据分段的大小	1

*注：Le=参数数据长度+3

响应详见3GPP2 C.S0016-C的4.5.1.9节“SSPR下载请求消息”。

6.5.9 OTAPA请求

命　令	CLASS	INS	P1	P2	Lc	Le
OTAPA请求	A0	EE	XX	00	XX	06

以下任一条件成立，则P1设置为00：

- ME分配了ESN；
- ME分配了MEID，但是第9号业务没有被分配或被激活。

如果分配了第9号业务并且业务被激活，同时ME分配了MEID，则P1=01。

如果P1=00，命令参数/数据：

字　节	描　述	长度（字节）
1	开始/停止	1
2～5	RANDSeed	4

如果P1=01，命令参数/数据：

字　节	描　述	长度（字节）
1	开始/停止	1
2～5	RANDSeed	4
6～12	P-ESN	7

开始/停止参数的定义见3GPP2 C.S0016-C的4.5.1.11节，其编码如下：字节1的比特1～7均设置为0，比特8为 “开始/停止”比特。

响应参数/数据：

字　节	描　述	长度（字节）
1	结果代码	1
2	NAM_LOCK 指示器	1
3～6	RAND OTAPA	4

注：仅当结果代码为00，且NAM_LOCK_STATE为激活状态（=1）时，R-UIM才返回RAND_OTAPA（字节3～6）。

NAM_LOCK指示器参数在3GPP2 C.S0016-C的4.5.1.11节规定，编码如下：字节2的比特1为NAM_LOCK的指示器，字节2的比特2～8均设置为‘0’。

响应详见3GPP2 C.S0016-C的4.5.1.11节“OTAPA响应参数”。

6.5.10 PUZL配置请求

命　令	CLASS	INS	P1	P2	Lc	Le
PUZL配置请求	A0	F4	00	00	*	**

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID（0000 0000）	1

注：如果数据块ID=‘0000 0001’（PUZL首选参数块），那么字节2～4用作该命令的输入。

字　节	描　述	长度（字节）
1	数据块ID（0000 0001）	1
2～3	请求索引	2
4	请求最大入口	1

请求索引参数在3GPP2 C.S0016-C中规定，编码如下：字节2的比特4～1分别为请求索引的比特12～9，字节2的比特8～5设置为‘0’；字节3的比特8～1分别为请求索引的比特8～1。

注：如果数据块ID=‘0000 0010’（用户区域参数块），那么字节2～8用作该命令的输入。

字　节	描　述	长度（字节）
1	数据块ID（0000 0010）	1
2～3	UZ_ID	2
4～5	UZ_SID	2
6～7	请求偏移	2
8	请求最大值	1

参数UZ_SID参数如3GPP2 C.S0016-C所规定，其编码如下：字节4的比特7～1分别为UZ_SID的比特15～9，字节4的比特8设置为‘0’；字节5的比特8～1分别为UZ_SID的比特8～1。

请求偏移如3GPP2 C.S0016-C所规定，其编码如下：字节6的比特4～1分别为请求偏移的比特12～9，字节6的比特8～5设置为‘0’；字节7的比特8～1分别为请求偏移的比特8～1。

注：如果数据块ID=‘0000 0011’（首选用户区域列表参数块），那么字节2～6用作该命令的输入。

字　节	描　述	长度（字节）
1	数据块ID（0000 0011）	1
2～3	请求索引	2
4～5	请求偏移	2
6	请求最大值	1

命令参数的详细信息见3GPP2 C.S0016-C的4.5.1.12节“PUZL配置请求消息”。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1
3	数据块长度	1
4～Le	参数数据	Le-3

**注：Le=参数数据长度+3

响应详见3GPP2 C.S0016-C的4.5.1.12节“PUZL配置请求消息”。

6.5.11　PUZL 下载请求

命　令	CLASS	INS	P1	P2	Lc	Le
PUZL下载请求	A0	F6	00	00	*	05

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	数据块长度	1
3～Lc	参数数据	Lc-2

*注：Lc=参数数据长度+2

命令参数详见3GPP2 C.S0016-C中4.5.1.13节“PUZL下载请求消息”。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1
3	标识符出现标志	1
4～5	UZ_ID	2
6～7	UZ_SID	2

标识符出现标志参数在3GPP2 C.S0016-C中规定，其编码如下：字节3的比特1为标识符出现标志，字节3的比特8～2设置为‘0’。

如果标识符出现标志位设置为‘1’，则返回字节4～7。

响应详见3GPP2 C.S0016-C中3.5.1.13节“PUZL下载响应消息”。

UZ_SID参数在3GPP2 C.S0016-C中规定，其编码如下：字节6的比特7～1分别为UZ_SID的比特15～9，字节6的比特8设置为‘0’；字节7的比特8～1分别为UZ_SID的比特8～1。

6.5.12　3GPD 配置请求

命　令	CLASS	INS	P1	P2	Lc	Le
3GPD配置请求	A0	FC	00	00	01	*

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1

这个命令请求单个数据块的3GPD详细配置信息，并构成“3GPD配置请求消息”的子集，见3GPP2 C.S0016-C中4.5.1.15节。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	数据块长度	1
3	结果代码	1
4～Le	参数数据	Le-3

*注：Le=参数数据长度+3

响应提供单个数据块的3GPD详细配置信息，并构成“3GPD配置请求消息”的子集。

6.5.13 3GPD下载请求

命　令	CLASS	INS	P1	P2	Lc	Le
3GPD下载请求	A0	48	00	00	*	02

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	数据块长度	1
3～Lc	参数数据	Lc-2

这个命令请求单个数据块的3GPD下载，并构成“3GPD下载请求消息”的子集，见3GPP2 C.S0016-C中4.5.1.15节。

*注：Lc=参数数据长度+2

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1

响应属于单个数据块，并构成“3GPD下载请求消息”的子集。

6.5.14 安全模式

命　令	CLASS	INS	P1	P2	Lc	Le
安全模式	A0	4A	00：开始 01：停止	见以下描述	08 空	‘01’

P1=‘00’

命令参数/数据：

字　节	描　述	长度（字节）
1～8	RAND_SM	8

命令参数详见3GPP2 C.S0016-C中4.5.1.16节“安全模式请求消息”。

响应参数/数据：

字　节	描　述	长度（字节）
1	结果代码	1

响应参数详见3GPP2 C.S0016-C中4.5.1.16节“安全模式请求消息”。

P1=‘01’

命令参数/数据：不生成命令参数。

P2被用作“KEY_IN_USE”参数。

如果KEY_IN_USE=0000，那么P2=0x00

如果KEY_IN_USE=0001，那么P2=0x01

响应参数/数据：

字　节	描　述	长度（字节）
1	结果代码	1

响应参数详见3GPP2 C.S0016-C中4.5.1.16节“安全模式请求消息”。

6.5.15 FRESH

命　令	CLASS	INS	P1	P2	Lc	Le
FRESH	A0	4C	00：上传 01：下载	00	02 空	空 02

P1=‘00’

命令参数/数据：

字　节	描　述	长度（字节）
1～2	Crypto-Sync	2

响应参数/数据：

命令的执行不生成响应参数。命令成功执行，将返回SW1 SW2 = ‘90 00’。命令执行失败，则返回SW1 SW2 = ‘98 04’。

P1=‘01’

命令参数/数据：不生成命令参数。

响应参数/数据：

字　节	描　述	长度（字节）
1～2	Crypto-Sync	2

Crypto-Sync参数在3GPP2 C.S0016-C中规定，其编码如下：字节1的比特7～1分别为Crypto-Sync的比特15～9，字节1的比特8设置为‘0’；字节2的比特8～1分别为Crypto-Sync的比特8～1。

6.5.16 业务密钥生成请求

命　令	CLASS	INS	P1	P2	Lc	Le
业务密钥生成请求	A0	4E	00	00	02	01

命令参数/数据：

字　节	描　述	长度（字节）
1 ～2	KEY_ID	2

KEY_ID在3GPP2 C.S0016-C中表4.5.1.22-1中定义。字节1的比特1～5为RFU，b6为WLAN根密钥，b7为BCMCS根密钥，b8为IMS根密钥；字节2为RFU。

响应参数/数据：

字　节	描　述	长度（字节）
1	结果代码	1

响应参数详见3GPP2 C.S0016-C中3.5.1.22节。

6.5.17 MMD 配置请求

命　令	CLASS	INS	P1	P2	Lc	Le
MMD配置请求	A0	C4	00	00	01	*

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1

该命令请求单个数据块的详细配置信息来构成“MMS配置请求消息”的一部分。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1
3	数据块长度	1
4～Le	参数数据	Le-3

*注：Le=参数数据的长度+3。

响应内容详见3GPP2 C.S0016-C的3.5.1.18，“MMD配置响应消息”。

6.5.18 MMD下载请求

命　令	CLASS	INS	P1	P2	Lc	Le
MMD下载请求	A0	C6	00	00	*	02

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	数据块长度	1
3～Lc	参数数据	Lc-2

*注：Lc=参数数据长度+2。

命令参数详见3GPP2 C.S0016-C，“MMD下载请求消息”。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1

响应参数详见3GPP2 C.S0016-C的3.5.1.19节，“MMD下载响应消息”。

6.5.19 MMS配置请求

命　令	CLASS	INS	P1	P2	Lc	Le
MMD配置请求	A0	42	00	00	01	*

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1

该命令请求单个数据块的详细配置信息来构成“MMS配置请求消息”，见3GPP2 C.S0016-C中4.5.1.23节。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1
3	数据块长度	1
4～Le	数据块ID	Le-3

*注：Le=参数数据长度+3。

响应数据详见3GPP2 C.S0016-C中3.5.1.23，“MMS配置请求消息”。

6.5.20 MMS下载请求

命　令	CLASS	INS	P1	P2	Lc	Le
MMS下载请求	A0	46	00	00	*	02

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1
3～Le	数据块ID	Le-2

*注：Lc=参数数据长度+2。

命令参数详见3GPP2 C.S0016-C的4.5.1.24节，“MMS下载请求消息”。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1

响应参数详见3GPP2 C.S0016-C的4.5.1.24节，“MMS下载响应消息”。

6.5.21 系统标签配置请求

命　令	CLASS	INS	P1	P2	Lc	Le
系统标签配置请求	A0	C8	00	00	04	*

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2～3	请求的偏置	2
4	请求的最大字节数	1

注：如果数据块ID=‘0000 0001’[组标签列表]，‘0000 0010’[特定标签列表]，或者‘0000 0011’[快速呼叫列表]，那么字节2~4被作为该命令的输入。对于其他的数据块ID字节2～4被忽略。命令参数详见3GPP2 C.S0016-C的4.5.1.20节“系统标签配置请求消息”。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1
3	数据块长度	1
4～Le	参数数据	Le-3

*注：Le=参数数据长度+3。

响应参数详见3GPP2 C.S0016-C的4.5.1.20节，“系统标签配置响应消息”。

6.5.22 系统标签下载请求

命　令	CLASS	INS	P1	P2	Lc	Le
系统标签配置请求	A0	CA	00	00	*	05

命令参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	数据块	1
3～Lc	参数数据	Lc-2

*注：Lc=参数数据长度+2。

命令参数详见3GPP2 C.S0016-C的4.5.1.21节，“系统标签下载请求消息”。

响应参数/数据：

字　节	描　述	长度（字节）
1	数据块ID	1
2	结果代码	1
3～4	数据分段的偏置	2
5	数据分段的大小	1

*注：如果BLOCK_ID=‘0000 0001’[组标签列表]，‘0000 0010’[特定标签列表]，或者‘0000 0011’[快速呼叫列表]，那么要使用字节3～5，对于其他的BLOBK ID，则忽略字节3～5。

响应参数详见3GPP2 C.S0016-C的4.5.1.21节“系统标签下载响应消息”。

6.6 ESN 管理命令

如果使用T=0协议，APDU被映射到TPDU。

以下介绍存储ESN_MEID_ME。

命　令	CLASS	INS	P1	P2	Lc	Le
存储 ESN_MEID_ME	A0	DE	XX	00	08	01

如果以下任一条件成立，则P1设置为‘00’：

- ME分配了ESN；
- ME分配了MEID，但是没有分配第9号业务或激活第9号业务。

如果分配并激活了第9号业务，且ME分配了MEID，则P1=‘01’。

命令参数/数据：（P1=‘00’）

字　节	描　述	长度（字节）
1	ESN_ME的长度	1
2～8	ESN_ME	7

ESN采用低位字节在前的方式进行编码以匹配$EF_{ESN\text{-}ME}$的编码。

在ME和R-UIM初始化过程中，ME会调用“Store ESN_MEID_ME”命令来存储其ESN到EF‘6F38’。ESN_ME 长度以字节表示，字节1的bit0～3规定了其长度，其中b3为MSB，b0为LSB。

字节1的bit4～7为RFU。

响应参数/数据：

字　节	描　述	长度（字节）
1	更改标记及使用指示	1

字节1的比特0指示ESN_ME是否与EF‘6F38’中存储的ESN_ME/MEID相同。如果比特0设置为‘0’表示是相同的；如果设置为‘1’表示已经改变了。如果必要，手机可以按照7.1.1节的要求重新登记。

bit1～3是RFU设为‘000’。

bit4为‘使用指示器’标志位，在EF ‘6F42’中定义，它用以表示是采用EF‘6F38’中存储的低32比特ESN还是EF‘6F31’中存储的低32比特UIMID进行鉴权计算和相关操作。bit4 设置为‘1’表示使用

UIMID；设置为‘0’表示使用ESN_ME。

bit5～7是RFU，设置为‘000’。

如果不支持第9号业务的R-UIM被插入分配了MEID的ME，ME应发起“Store ESN_MEID_ME”（P1=00）的命令，命令中ESN域为P-ESN。

命令参数/数据：（P1=‘01’）

字　节	描　述	长度（字节）
1	MEID的长度	1
2～8	MEID	7

在ME和R-UIM初始化过程中，ME会调用“Store ESN_MEID_ME”命令来存储其MEID到EF‘6F38’。MEID 长度以字节表示，字节1的bit0-3规定了其长度，其中b3为MSB，b0为LSB。

字节1的bit4～7为RFU。

响应参数/数据：

字　节	描　述	长度（字节）
1	更改标记及使用指示	1

字节1的比特0指示MEID是否与EF‘6F38’中存储的ESN_ME/MEID相同。如果比特0设置为‘0’表示是相同的；如果设置为‘1’表示已经改变了。如果必要，手机可以按照7.1.1节的要求重新登记。

bit1～3是RFU设为‘000’。

bit4为‘使用指示器’标志位，在EF ‘6F42’中定义，它用以表示是采用EF‘6F38’中存储的低32比特ESN还是EF‘6F31’中存储的低32比特UIMID进行鉴权计算和相关操作。bit4 设置为‘1’表示使用UIMID；设置为‘0’表示使用ESN_ME。

bit5指示了在3GPP2 C.S0005-D中使用了MEID的地方是使用56比特的SF_EUIMID（存储在EF_{SF_EUIMID}中）还是使用56比特的终端MEID；如果比特5设置为‘1’，则使用SF_EUIMID，如果比特5设置为‘0’，则使用终端的MEID。如果分配了第8号业务，则终端不解译比特5的值。

Bit6～7是RFU，设置为‘00’。

6.7 与数据包安全相关的功能描述

6.7.1 概述

本节描述当R-UIM执行3G数据包业务的业务鉴权和接入鉴权功能时使用的ME和R-UIM间的接口。对于业务鉴权目前有两种接入方法：一种是简单IP一种是移动IP。简单IP是接入提供商的网络给MS分配IP地址并提供IP路由地址。当使用简单IP时，网络可以请求点到点的CHAP（Challenge Handshake Authentication Protocol）鉴权或点到点的PAP（Password Authentication Protocal）鉴权来认证用户。移动IP是指网络为用户提供IP路由到公共IP网络或提供安全的IP路由业务到私有网络。当使用移动IP时，网络通过移动IP的移动归属鉴权和移动IP的查询/响应鉴权来认证用户。

接入鉴权是一个过程，在这个过程中，AN-AAA（接入网络鉴权、授权和核算实体）对AT（接入终端）进行认证鉴权。

图7为数据业务和语音业务的鉴权模型。

6.7.2 管理SS（Shared Secrets）

UIM卡存储和管理执行数据业务鉴权计算的简单IP和移动IP所使用的共享保密数据。网络可以通过使用安全模式的OTASP/OTAPA消息来更新共享保密数据。

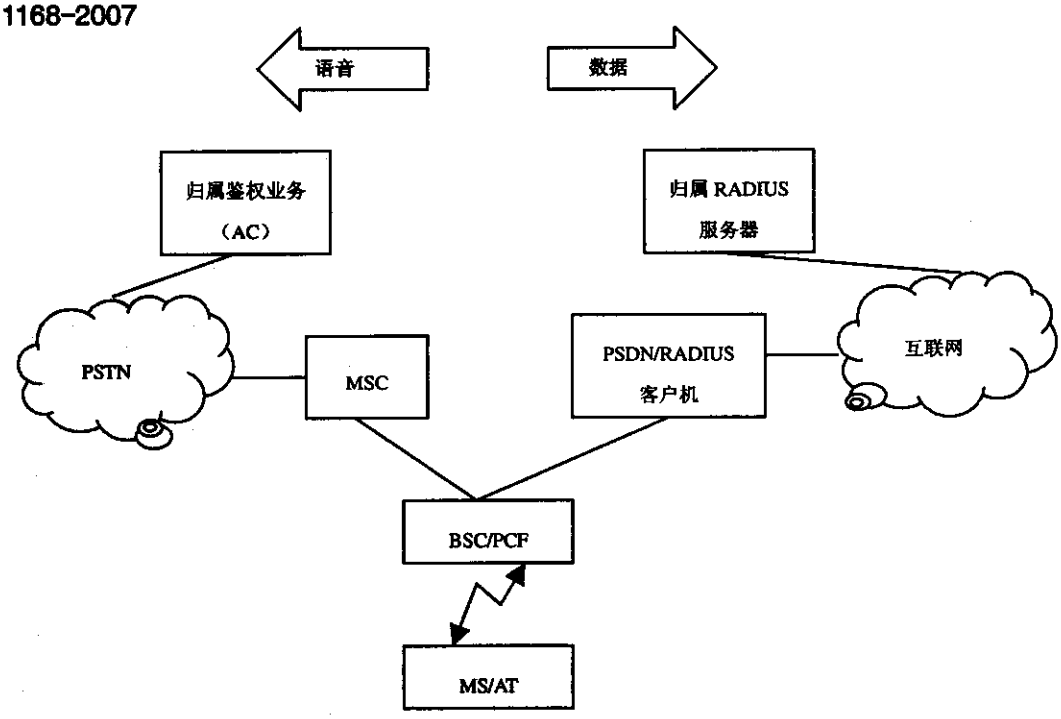


图 7　鉴权模型

6.7.3　执行简单 IP 鉴权

网络（PSDN）通过发送与移动台在接入请求中具有同样的CHAP-ID的CHAP-Challenge给移动台来开始简单IP的鉴权过程。ME使用Compute IP Authentication命令（CHAP选项）来转发该信息和接入请求中使用的NAI-Entry-Index给R-UIM。这个NAI-Entry-Index决定了SS将用于CHAP响应的计算。R-UIM计算CHAP响应并发送给ME，ME立刻转发给网络。如果ME发送的CHAP响应与网络计算出的CHAP响应相匹配，则网络将发回Access-Accept来认可业务。

6.7.4　执行移动 IP 鉴权

对于使用移动IP的移动台，在建立PPP或从移动台接收到代理请求（Agent Solicitation）消息后，PSDN立刻开始传送运营商可配置的几个代理公告。在移动台接收到代理公告（Agent Advertisement）消息和主机的查询后开始移动IP的鉴权。移动台通过发送移动IP注册请求（MIP-RRQ）消息给网络来开始鉴权过程。这个消息包含各种扩展，这些扩展允许鉴权数据从移动台传送到PDSN。然后PDSN使用接入请求（Access Request）消息发送鉴权数据给RADIUS服务器。一旦鉴权成功，RADIUS服务器会用接入接受（Access Accept）消息来接受业务或用接入拒绝（Access Reject）消息来拒绝业务。

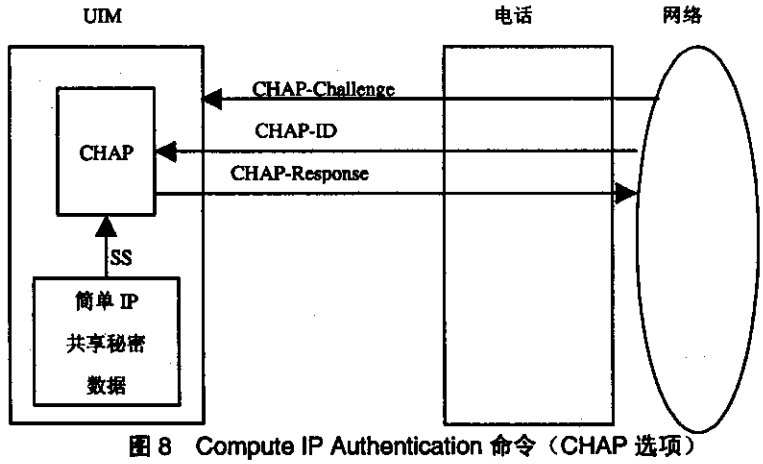


图 8　Compute IP Authentication 命令（CHAP 选项）

MIP-RRQ消息按照顺序包含以下扩展：

（1）MN-NAI扩展；

（2）MN-HA鉴权扩展；

（3）MN-FA查询扩展；

（4）MN-AAA扩展。

移动台使用静态归属代理（HA）地址。

为了计算MN-HA鉴权扩展，ME发送R-UIM的Compute IP Authentication命令（MN-HA鉴权选项）包含以下信息：

- NAI-Entry-Idenx指示了在请求中使用的NAI；
- MIP-RRQ（注册消息）保护的域。

保护的域有：

- UDP净荷；
- 全部首选扩展；
- 扩展的类型、长度和SPI。

R-UIM通过对与注册消息中被保护的域相关的NAI所指示的MN-HA共享保密数据进行HASH运算来返回MN-HA-Authenticator。

由于RADIUS协议不能够执行大于253的尺寸，所以在MN-AAA鉴权生成前，移动IP数据、类型、子类型（如果有）、长度和SPI被执行HASH运算。这可以通过使用Compute IP Authentication命令（MIP-RRQ HASH选项）来获得。在这个命令中，ME发送之前的MIP-RRQ数据给R-UIM，同时R-UIM计算该数据的HASH。该HASH不返回给ME。

紧接着，这个MIP-RRQ HASH从网络发起的CHALLENGE和识别移动台与归属RADIUS服务器共享的秘密数据的NAI-Entry-Index一起通过Compute IP Authentication命令（MN-AAA鉴权选项）发送给R-UIM。

R-UIM计算MN-AAA鉴权，并返回给ME，ME通过MIP-RRQ消息发送给网络。

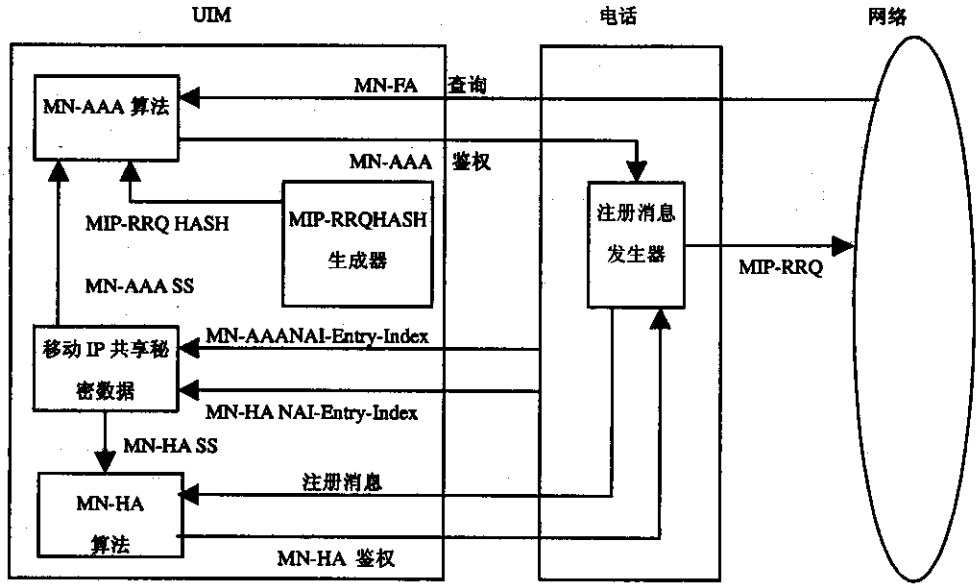


图 9 计算 MN-AAA 鉴权

6.7.5 HRPD 接入鉴权

在HRPD的接入鉴权过程中，接入终端（AT）被AN-AAA鉴权。

对于接入鉴权，AT和网络AN发起PPP和LCP协商。如果使用接入鉴权特性，在PPP建立期间，AN在初始链路控制协议（LCP）的配置请求中总是提出进行CHAP认证，并通过CHAP-Challenge消息将其产生的随机查询数送给接入终端。

当接入终端发现R-UIM卡中的CDMA业务表EF_{CST}中的HRPD 业务n5置为‘11’时，决定采用CHAP/MD5算法，接入终端通过Compute IP Authentication（HRPD接入鉴权）命令将上述信息前转给R-UIM卡。R-UIM卡计算CHAP响应，并将其通过AT发给网络。如果这个CHAP响应与网络侧计算出的CHAP响应一致，AN就向AT返回一个CHAP接入鉴权成功的指示。

当接入终端发现R-UIM卡中的CDMA业务表EF_{CST}中的HRPD业务n5未置为‘11’时，则使用RUN CAVE消息发起采用CAVE算法的鉴权操作，具体功能请见6.2节。

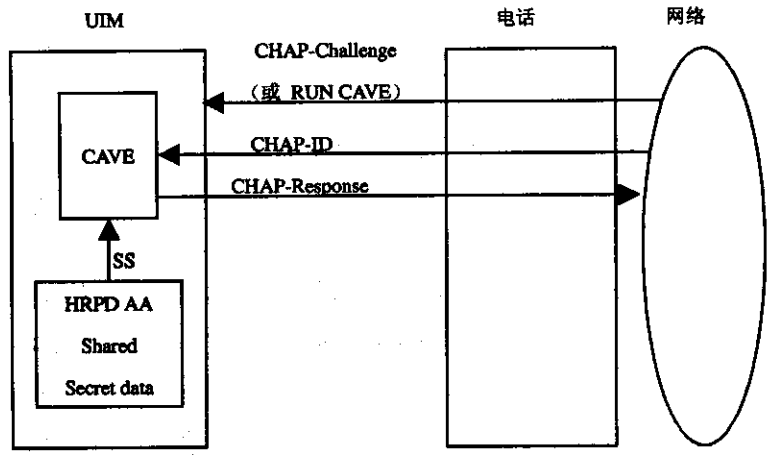


图 10 HRPD 接入鉴权命

6.8 与分组数据安全相关的命令

6.8.1 Compute IP Authentication

该命令计算用于简单IP、移动IP和HRPD接入鉴权的响应和鉴权。

命 令	CLASS	INS	P1	P2	Lc	Le
Compute IP Authentication	80	80	P1	P2	Lc	Le

P1定义了IP鉴权命令类型：

P1	类 型
00	CHAP
01	MN-HA Authenticator
02	MIP-RRQ Hash
03	MN-AAA Authenticator
04	HRPD Access Authenticator

移动台必须按顺序执行MN-HA Authenticator、MIP-RRQ Hash和MN-AAA Authenticator。如果没有按顺序执行，则R-UIM返回SW1 SW2 = ‘98 34’。然而在执行MIP-RRQ Hash前，移动台可以执行MN-HA Authenticator多次。

6.8.1.1 CHAP

该IP鉴权命令生成CHAP响应。

命　令	CLASS	INS	P1	P2	Lc	Le
Compute IP Authentication	80	80	00	00	*	10

命令参数/数据：

Octet（s）	描　述	长度（字节）
1	CHAP_ID	1
2	NAI-Entry-Index	1
3～*X*	CHAP-Challenge	Lc - 2

CHAP-ID：CHAP标识符。

NAI-Entry-Index：简单IP NAI-Entry-Index指示了要使用的在简单IP CHAP SS参数块中共享保密数据。

CHAP-Challenge：从网络侧接收到的用于计算CHAP-Response的查询。

*Lc = CHAP-Challenge长度+2

响应参数/数据：

字　节	描　述	长度（字节）
1～16	CHAP-Response	16

R-UIM 计算CHAP-Response：

CHAP-Response = Algo （CHAP-ID ‖ CHAP-SS ‖ CHAP-Challenge）

CHAP-SS：由NAI-Entry-Index所指示的简单IP CHAP共享保密数据。

Algo：采用MD5算法，运营商也可以选择其他的hashing算法。

6.8.1.2 MN-HA 鉴权

这个IP鉴权命令类型用来计算MN-HA鉴权。如果注册消息的最大长度超过了254字节，命令将分割注册消息成几个连续的具有最大长度为254字节的块。如果命令中各块的顺序被打乱，则卡返回SW1 SW2 = ‘98 34’。

命　令	CLASS	INS	P1	P2	Lc	Le
Compute IP Authentication	80	80	01	*	*	*

P2包含如下的连接信息：

P2	块
00	第一个数据块
01	下一个数据块
02	单个数据块
03	最后一个数据块

*Le：　对于P2= ‘00’ 或 ‘01’，0字节。

　　对于P2= ‘02’ 或 ‘03’，16字节。

命令数据基于P2的值：

P2= ‘00’ 或 ‘02’

命令参数/数据：

Octet（s）	描　述	长度（字节）
1	NAI-Entry-Index	1
2～*X*	Registration-Data	Lc - 1

P2= ‘01’ 或 ‘03’

命令参数/数据：

Octet（s）	描　述	长度（字节）
1～*X*	Registration-Data	Lc

NAI-Entry-Index：移动IP NAI-Entry-Index指示了要使用的在移动IP SS参数块中的MN-HA共享保密数据。

Registration-Data：注册消息中受保护的域。被保护的域包含UDP净荷、全部首选扩展以及扩展的类型、长度、SPI。Registration-Data的最大长度为254字节。

响应消息基于链接信息P2：

P2 = ‘00’ 或 ‘01’

响应：无

P2 = ‘02’ 或 ‘03’

响应参数/数据

Octet（s）	描　述	长度（字节）
1～16	MN-HA鉴权	16

R-UIM按照如下方法计算MN-HA：

MN-HA鉴权=Algo（MN-HA SS||Registration-Message||MN-HA SS）

MN-HA SS：由NAI-Entry-Index所指示的MN-HA共享保密数据。

Registration-Message：完整的注册消息包含在连续的命令消息中的注册数据块中。

Algo：采用MD5算法，运营商也可以选择其他的hashing算法。

6.8.1.3 MIP-RRQ Hash

这个IP鉴权命令类型计算出Preceding MIP-RRQ Hash。Preceding MIP-RRQ数据可以超过247字节，它应通过一个或多个连续的数据块发送给R-UIM卡，使用一个还是多个数据块取决于它的实际长度。如果命令块的顺序被打乱，则卡将返回SW1 SW2 = ‘98 34’。

命　令	CLASS	INS	P1	P2	Lc	Le
Compute IP Authentication	80	80	02	*	*	00

P2包含链接信息如下：

P2	块
00	第一个数据块
01	下一个数据块
02	单个数据块
03	最后一个数据块

命令数据基于P2的值：

P2= ‘00’ 或 ‘01’

命令参数/数据：

Octet（s）	描　述	长度（字节）
1～*X*	Preceding MIP-RRQ数据	Lc

P2= ‘02’ 或 ‘03’

命令参数/数据：

Octet（s）	描　述	长度（字节）
1～*X*	Preceding MIP-RRQ数据	Lc-8
X+1～*X*+8	MN-AAA 扩展头	8

MN-AAA扩展头：类型、长度和MN-AAA EXTENSION的SPI域。

Preceding MIP-RRQ数据：移动IP注册请求MN-AAA EXTENSION。MIP-RRQ数据的第一个和下一个数据块的最大长度为255字节，最后一个和单个数据块的最大长度为247字节。

响应参数/数据：无

R-UIM按照如下方法计算MIP-RRQ HASH：

MIP-RRQ Hash=Algo（PRECEDING-MIP-RRQ‖MN-AAA Extension Header）

PRECEDING-MIP-RRQ：完整的移动IP注册请求包含在连续的MIP-RRQ Hash选项中的Preceding MIP-RRQ数据。

Algo：采用MD5算法，运营商也可以选择其他的hashing算法。

6.8.1.4 MN-AAA 鉴权

这个IP命令类型计算MN-AAA鉴权。

命　令	CLASS	INS	P1	P2	Lc	Le
Compute IP Authentication	80	80	03	00	*	10

命令参数/数据：

Octet（s）	描　述	长度（字节）
1	NAI-Entry-Index	1
2～*X*	Challenge	Lc - 1

NAI-Entry-Index：移动IP NAI-Entry-Index指示了要使用的在移动IP SS参数块中的MN-AAA共享保密数据。

Challenge：Challenge在MN-AAA扩展中。如果ME接收到一个大于237字节的Challenge，他将发送从低到高的237位有效字节给R-UIM。如果Challenge少于238字节，这个R-UIM将使用包含两次Challenge的高位有效位字节进行计算，但是要确保Challenge确实是这样使用的。这里不使用额外的填充字节来增加Challenge的长度。

*Lc= Challenge长度+1字节

响应参数/数据：

Octet（s）	描　述	长度（字节）
1～16	MN-AAA鉴权	16

R-UIM将按照如下方法计算响应：

MN-AAA鉴权=Algo（Challenge的高位有效字节‖MN-AAA SS‖MIP-RRQ Hash‖ Challenge的从低到高237位有效字节）

MN-AAA SS：由NAI-Entry-Index指示的MN-AAA共享保密数据。

Algo：采用MD5算法，运营商也可以选择其他的hashing算法。

6.8.1.5 HRPD 接入鉴权

这个IP鉴权命令类型产生CHAP响应，用于HPPD接入鉴权。

命　令	CLASS	INS	P1	P2	Lc	Le
Compute IP Authentication	80	80	04	00	*	10

命令参数/数据：

Octet（s）	描　述	长度（字节）
1	CHAP_ID	1
2～X	CHAP-Challenge	Lc - 1

CHAP-ID：CHAP标识符。

CHAP-Challenge：从网络侧接收的用于计算CHAP-Response的查询。CHAP-Challenge的长度取决于生成字节所使用的方法，而与所使用的hash算法无关。

*Lc = CHAP-Challenge长度+1

响应参数/数据：

字　节	描　述	长度（字节）
1～16	CHAP-Response	16

R-UIM 按如下方法计算CHAP-Response：

CHAP-Response = Algo （CHAP-ID ‖ CHAP-SS ‖ CHAP-Challenge）

CHAP-SS：HRPD接入鉴权共享保密数据。

Algo：采用MD5算法，运营商也可以选择其他的hashing算法。

6.9 BCMCS 命令（可选）

6.9.1 概述

以下命令用于BCMCS密钥管理。不论BCMCS业务是否在CDMA业务列表中分配，R-UIM都要执行这些命令。这里假设BCMCS根密钥安全的存储在R-UIM中。

命　令	CLASS	INS	P1	P2	Lc	Le
BCMCS	A0	58	P1	P2	Lc	Le

P1参数定义了BCMCS命令的类型：

P1	命　令
00	RETRIEVE SK
01	UPDATE BAK
02	DELETE BAK
03	RETRIEVE SRTP SK
04	Generate Authentication Signature
05	BCMCS Authentication

6.9.2 RETRIEVE SK

6.9.2.1 命令描述

终端使用该命令来请求R-UIM计算与特定的BCMCS流标识（BCMCS_Flow_ID）相关的BCMCS短期密钥（SK）。对于该计算，R-UIM使用由广播接入密钥标识符（BAK_ID）标识的广播接入密钥（BAK）。

输入：

- 业务类别=‘01’对应于“3GPP2 BCMCS”
- BCMCS_Flow_ID
- BAK_ID
- SK_RAND

输出：

- SK

6.9.2.2 命令参数/数据：

代　码	值
CLA	A0
INS	58
P1	00
P2	00
Lc	后续数据字段的长度
数据	业务类别、业务标识符、会话密钥标识符、业务密钥种子
Le	12

命令数据：

字　节	描　述	长度（字节）
1	业务类别=‘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*
注：命令的TLV数据对象中的标签值在附录B规定。		

响应参数/数据：

字　节	描　述	长度（字节）
1～18	SK TLV	18
注：响应的TLV数据对象中的标签值在附录B规定		

6.9.3 Update BAK

6.9.3.1 命令描述

该功能请求R-UIM执行BCMCS BAK更新。

输入：

- 业务类别=‘01’对应于“3GPP2 BCMCS”
- BCMCS_Flow_ID
- BAK_ID
- BAK_Expire
- TK_RAND
- 加密BAK

输出：无

6.9.3.2 命令参数/数据：

代　码	值
CLA	A0
INS	58
P1	01
P2	00
Lc	后续数据字段的长度
数据	业务类别、业务标识符、会话密钥标识符、BAK_Expire、TK_RAND、加密BAK
Le	空、00，或期待的响应数据的最大长度

命令数据：

字　节	描　述	长度（字节）
1	业务类别：‘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BAK	16
注：命令的TLV数据对象中的标签值在附录B规定		

响应数据：无

6.9.4 Delete BAK

6.9.4.1 命令描述

该功能请求R-UIM执行BCMCS BAK删除过程来释放内存。该命令不用于结束与用户的签约。

输入：

- 业务类别=‘01’对应于“3GPP2 BCMCS”
- BCMCS_Flow_ID
- BAK_ID

输出：无

6.9.4.2 命令参数/数据：

代　码	值
CLA	A0
INS	58
P1	02
P2	00
Lc	后续数据字段的长度
数据	业务类别、业务标识符、会话密钥标识符
Le	00

命令数据：

字　节	描　述	长度（字节）
1	业务类别：‘01’（3GPP2 BCMCS）	1
2~*A*+1	BCMCS_Flow_ID TLV	*A*
A+2~*A*+*B*+1	BAK_ID TLV	*B*
注：命令的TLV数据对象中的标签值在附录B规定		

响应数据：无

命令响应的状态字：

‘9402’：无效BAK_ID；

‘9404’：BCMCS_Flow_ID。

6.9.5 RETRIEVE SRTP SK

6.9.5.1 命令描述

终端使用该命令请求R-UIM计算与特定的BCMCS流标识符（BCMCS_Flow_ID）相关的BCMCS SRTP短期密钥（SK）。对于该计算，R-UIM使用由广播接入密钥标识符（BAK_ID）确定的广播接入密钥（BAK）、SK_RAND和数据包索引。

输入：

- 业务类别=‘01’对应于“3GPP2 BCMCS”
- BAK_ID
- SK_RAND
- 数据包索引

输出：

- SRTP SK

6.9.5.2 命令参数/数据：

代　码	值
CLA	A0
INS	58
P1	03
P2	00
Lc	后续数据字段的长度
数据	会话密钥标识符、业务密钥种子、数据包索引
Le	12

命令数据：

字　节	描　述	长度（字节）
1	业务类别：‘01’（3GPP2 BCMCS）	1
2～*A*+1	BAK_ID TLV	*A*
A+2～*A*+*B*+1	SK_RAND TLV	*B*
A+*B*+2～*A*+*B*+*C*+1	数据包索引 TLV	*C*
注：命令的TLV数据对象中的标签值在附录B规定		

响应参数/数据：

字　节	描　述	长度（字节）
1～18	SRTP SK TLV	18
注：响应的TLV数据对象中的标签值在附录B规定		

6.9.6 生成鉴权签名

6.9.6.1 命令描述

终端使用该命令请求R-UIM计算与特定的BCMCS流标识符（BCMCS_Flow_ID）相关的鉴权签名。对于该计算，R-UIM使用由广播接入密钥标识符（BAK_ID）确定的广播接入密钥（BAK）和时间戳。

输入：

- 业务类别
- BCMCS_Flow_ID
- BAK_ID
- 时间戳

输出：

- 鉴权签名

6.9.6.2 命令参数/数据：

代　码	值
CLA	A0
INS	58
P1	04
P2	00
Lc	后续数据字段的长度
数据	业务类别、业务标识符、会话密钥标识符、时间戳
Le	06

命令数据：

字　节	描　述	长度（字节）
1	业务类别=‘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	时间戳TLV	*C*
注：命令的TLV数据对象中的标签值在附录B规定		

响应参数/数据：

字　节	描　述	长度（字节）
1～6	鉴权签名TLV	6
注：响应的TLV数据对象中的标签值在附录B规定		

6.9.7 BCMCS 鉴权

6.9.7.1 命令描述

终端使用该命令请求R-UIM计算BCMCS摘要响应。R-UIM使用BCMCS的Root Key进行计算。

输入：

- RAND
- Challenge

输出：

- 摘要响应

6.9.7.2 命令参数/数据：

代　码	值
CLA	A0
INS	58
P1	05
P2	00
Lc	后续数据字段的长度
数据	RAND、Challenge
Le	12

命令数据：

字　节	描　述	长度（字节）
1	业务类别=‘01’（3GPP2 BCMCS）	1
2～*A*+1	RAND TLV	*A*
A+2～*A*+*B*+1	Challenge TLV	*B*
注：命令的TLV数据对象中的标签值在附录B规定		

响应参数/数据：

字　节	描　述	长度（字节）
1～18	摘要响应TLV	18
注：响应的TLV数据对象中的标签值在附录B规定		

6.10 应用鉴权命令的描述

6.10.1 概述

ME根据R-UIM卡的能力和业务来选择鉴权机制，并给卡发送鉴权命令来生成响应和会话密钥。成功的鉴权计算返回SW1 SW2 = '90 00'；失败的鉴权计算返回SW1 SW2 = '98 04'。

6.10.2 应用鉴权命令

R-UIM生成响应和两组会话密钥。

命　令	CLASS	INS	P1	P2	Lc	Le
应用鉴权	A0	5A	00	00	*XX*	*XX*

命令参数/数据：

字　节	描　述	长度（字节）
1	鉴权机制和算法	1
2	应用ID	1
3～4	领域的长度（业务或主机名称）	2
5～*A*+4	领域（业务或主机名称）	*A*
A+5～*A*+6	当前服务器长度	2
A+7～*A*+*B*+6	当前服务器	*B*
A+*B*+7～*A*+*B*+8	当前客户机长度	2
A+*B*+9～*A*+*B*+*C*+8	当前客户机	*C*

鉴权机制和算法按照下表进行编码：

二进制数值	鉴权机制
0000 0000	CRAM-MD5
0000 0001	HTTP Digest（MD5）
0000 0010	HTTP Digest（MD5-sess）
0000 0011	HTTP Digest（AKAv1-MD5）
0000 0100	HTTP Digest（AKAv1-MD5-sess）
0000 0101	SASL DIGEST
0000 0110	SASL OTP
0000 0111	SASL GSSAPI
00001000 ～1111 1111	保留

响应参数/数据：

字　节	描　述	长度（字节）
1	响应长度	1
2～*X*+1	响应	*X*
X+2～*X*+3	会话密钥1长度	2
X+4～*X*+*Y*+3	会话密钥1	*Y*
X+*Y*+4～*X*+*Y*+5	会话密钥2长度	2
X+*Y*+6～*X*+*Y*+*Z*+5	会话密钥2	*Z*

如果需要会话密钥，则不同的鉴权机制算法决定了应返回多少个会话密钥。例如：SASL Digest返回两个会话密钥，HTTP Digest（MD5-session）返回一个会话密钥，HTTP Digest（MD5）不返回会话密钥。如果R-UIM不返回会话密钥，则R-UIM设置相应的会话密钥长度为0。

图11是MMS消息重获的呼叫流程。

6.11 与 AKA 相关的功能描述（可选）

6.11.1 概述

为了支持AKA，R-UIM应支持所有支持AKA所需要的算法。以下与AKA相关的参数存储在R-UIM中：

- 根密钥；
- 加密密钥和完整性保护密钥（CK、IK）；
- SQN_{MS}；
- UAK（如果支持）。

6.11.2 鉴权和密钥协商过程

本节对网络调用的鉴权机制以及加密密钥和完整性保护密钥的生成过程进行描述。鉴权机制使用户和网络通过提供R-UIM和鉴权中心共享的根密钥来获得双向鉴权。另外，R-UIM跟踪计数器SQN_{MS}来支持网络鉴权。SQN_{MS}指示了R-UIM已经接收的最大序列号。

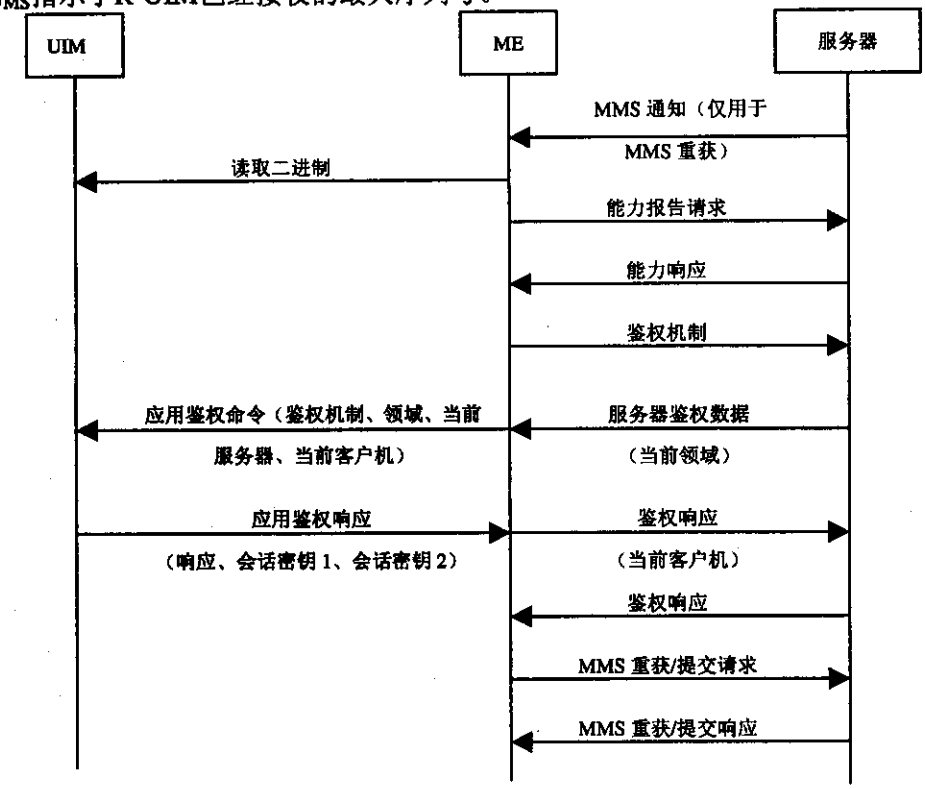


图11 MMS消息重获的呼叫流程

注：能力报告/响应/鉴权机制都为可选项；它们或者全部被使用，或者全部都不被使用。运营商决定是否使用它们。

R-UIM首先计算匿名密钥AK=f5（RANDA）并重获SQN=（SQN⊕AK）⊕AK。

然后R-UIM计算MACA=f1（SQN||RAND||AMF）。该值被用来与AUTN中的MAC-A进行比较。

R-UIM持续跟踪计数器SQN_{MS}来支持网络鉴权。SQN_{MS}指示了R-UIM所接收到的最大的序列号。如果R-UIM检测到无效的序列号，它应设置同步失败标签为‘00000001’并包含AUTS。

其中AUTS=ConSeq（SQN_{MS}）||MACS

ConSeq（SQN_{MS}）=SQN_{MS}⊕f5×（RAND）是R-UIM中计数器SQN_{MS}的隐含值，并且MACS=f1×（SQN_{MS}||RAND||AMF）。

6.11.3 加密功能

R-UIM所支持的加密功能的名称和参数在3GPP2 S.S0055中规定。

6.11.4 3G 鉴权命令描述

该功能在R-UIM到网络的鉴权以及网络到R-UIM的鉴权的过程中使用。另外，如果支持，则计算加密密钥、一致性保护密钥和UAK。

R-UIM使用根密钥执行命令，根密钥存储在R-UIM中。

6.11.5 生成 UMAC 命令描述

如果R-UIM支持UAK，则R-UIM使用UAK来转化MAC-I到UMAC。如果成功地生成UMAC，R-UIM通过设置成功标记为‘1’，并在响应中包含UMAC来响应ME；否则，R-UIM设置成功标记为‘0’并忽略UMAC。

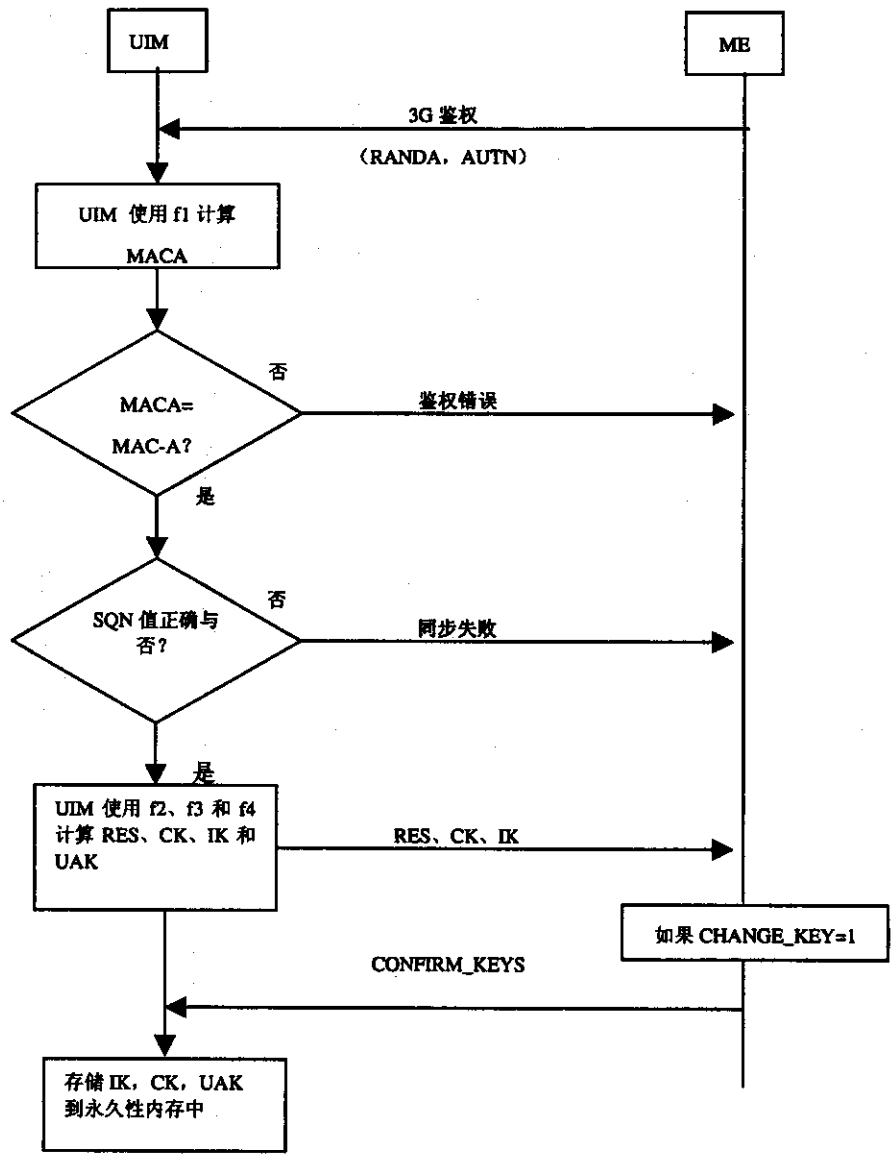


图12 AKA过程

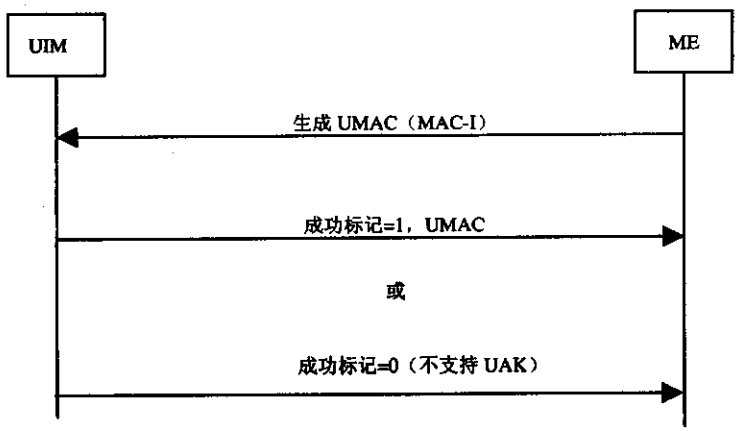


图 13 生成 UMAC

6.11.6 重存 3G 密钥

CK和IK在AKA过程中生成，并通过AKA更新。CK和IK存储在R-UIM中，并在ME中存有一个备份。当ME请求时，R-UIM发送CK和IK给ME。在关机或移出R-UIM后，ME从内存中删除CK和IK。当开机时，ME检查R-UIM的版本和业务列表，如果支持AKA并且AKA处于激活状态，则ME从R-UIM中读取EF_{3GCIK}，并存储他们。

6.11.7 CONFIRM_KEYS 命令描述

该功能在3G鉴权中使用。当接收到3G鉴权命令时，由R-UIM计算出的（IK、CK）和UAK被存储在永久性内存中。

6.12 AKA 命令描述（可选）

6.12.1 UMAC Generation

命　令	CLASS	INS	P1	P2	Lc	Le
UMAC Generation	A0	5E	00	00	04	XX

命令参数/数据：

字　节	描　述	长度（字节）
1～4	MAC-I	4

响应参数/数据：

字　节	描　述	长度（字节）
1	SUCCESS TAG	1
2～5	UMAC	0或4

如果R-UIM成功地生成UMAC，则R-UIM设置成功标记为‘0000 0001’，并且响应中包含UMAC；如果R-UIM不支持UAK，R-UIM设置成功标记为‘0000 0000’，并且忽略UMAC。所有其他值为RFU。

6.12.2 CONFIRM_KEYS

命　令	CLASS	INS	P1	P2	Lc	Le
CONFIRM_KEYS	A0	5C	00	00	空	空

命令参数/数据：无

响应参数/数据：无

7 附加空中接口过程

7.1 登记过程

7.1.1 插拔 R-UIM 卡

当将R-UIM从开机状态的ME拔出时，ME应删除临时内存中与R-UIM卡相关的参数。

当R-UIM插入开机状态的ME中时，ME应执行以下操作：

- 执行ME/R-UIM初始化过程。
- 更新R-UIM中的NAM参数。对于R-UIM中可获得的并处于激活状态的业务，应使用R-UIM中可获得的参数。
- 执行TIA-95-B中6.6.5.5.1.1节和3GPP2 C.S005-D中2.6.5.5.1.1节的过程。
- 在开机提示下，输入由系统决定的子状态。

7.1.2 TMSI 已分配时 ESN 改变的登记过程

当ME检测到插入了一个新的R-UIM，就用Store ESN_MEID_ME命令将其ESN或MEID发给R-UIM。如果该命令的“响应参数/数据”字节1的bit0设置为1，$REG\_ENABLED_S$=“YES”，并且在R-UIM中已分配一个TMSI（EF_{TMSI}的$TMSI_CODE_{S\text{-}P}$域设置为1），ME应执行如下过程：

- ME将USE_TMSI_S的值存入一个临时变量；
- ME将USE_TMSI_S设置为0；
- ME不管$POWER_UP_REG_S$、$REGISTERED_S$、$REG_ENABLED_S$的状态而开始一个开机登记过程；
- ME从临时变量中保存USE_TMSI_S的值。

如果由于访问尝试失败而导致登记失败或由于用户发起一个初始化或检测到一个寻呼映射而导致取消登记，ME应通过设置EF_{TMSI}的$TMSI_CODE_{S\text{-}P}$域为‘1’删除R-UIM中的TMSI。

7.2 在 R-UIM 未插入 ME 时的 NAM 参数

在R-UIM未插入ME时，ME使用下列默认NAM参数集（见3GPP2 C.S0016-C）：

- $IMSI_M_CLASS_P$设置为“0”；
- MCC_M_P、$IMSI\_M\_11\_12_P$、$IMSI_M_S_P$按照IMSI_M的编码值进行设置，IMSI_M的低4位设置为ESN_P，直接将二进制转换为十进制，模10000，其他设置为“0”；
- $IMSI_M_ADDR_NUM_P$设置为“000”；
- $IMSI_T_CLASS_P$设置为“0”；
- MCC_T_P、$IMSI\_T\_11\_12_P$、$IMSI_T_S_P$按照IMSI_T的编码值进行设置，IMSI_T的低4位设置为ESN_P，直接将二进制转换为十进制，模10000，其他设置为“0”；
- $IMSI_T_ADDR_NUM_P$设置为“000”；
- $ACCOLC_P$根据TIA/EIA-95-B的6.3.5节的描述设置；
- $HOME_SID_P$设置为“0”；
- 其他选定的NAM参数设置为厂商定义的默认值。

在未插入R-UIM时，ME应可以执行相关规范允许的任何操作，包括接入网络。

7.3 R-UIM 中无 IMSI 时 ME 中与 IMSI 相关的参数

EF IMSI_M的IMSI_M_PROGRAMMED设置为“0”时，ME使用下列与IMSI_M相关的值：

- $IMSI_M_CLASS_P$设置为“0”；

- MCC_M_P、IMSI_11_12$_P$、IMSI_M_S_P按照IMSI_M的编码值进行设置，IMSI_M的低4位设置为ESN_P. 直接将二进制转换为十进制，模10000，其他设置为“0”；
- IMSI_M_ADDR_NUM_P设置为“000”；
- $ACCOLC_P$根据TIA/EIA-95-B的6.3.5节的描述设置。

当EF IMSI_T的IMSI_T_PROGRAMMED设置为“0”时，ME使用下列与IMSI_M相关的值：

- IMSI_T_$CLASS_P$设置为“0”；
- MCC_T_P、IMSI_T_11_12$_P$、IMSI_T_S_P按照IMSI_T的编码值进行设置，IMSI_M的低4位设置为ESN_P. 直接将二进制转换为十进制，模10000，其他设置为“0”；
- IMSI_T_ADDR_NUM_P设置为“000”。

7.4 首选接入信道移动台 ID 类型

操作要求：

如果UIMID使用指示= ‘0’ 或SF_EUIMID使用指示= ‘0’（分配了第8号业务，该业务被激活，EF_{USGIND}的比特1或2设置为‘0’），相应的PREF_MSID值应被设置在消息头中。

8 BCMCS 过程（可选）

8.1 R-UIM 和 ME 功能

8.1.1 R-UIM

- 从BCMCS根密钥生成TK，并使用TK解密BAK；
- 从BAK和SK_RAND计算SK并传送SK给ME；
- 存储注册的密钥、BAK、BCMCS_Flow_ID、BAK_ID和BAK_EXPIRE；
- 当必要时，从BCMCS根密钥生成Auth-Key并计算响应；
- 当必要时，使用AES生成SRTP会话的加密密钥；
- 使用EHMAC从BAK和时间戳生成授权签名。

8.1.2 ME

- 使用SK解密BCMCS的内容；
- 决定是否通过BAK_ID和SK_RAND的检查发起Retrieve SK命令；
- 向网络发起BAK请求并发起BAK更新命令；
- 存储BCMCS_FLOW_ID、BAK_ID、BAK_EXPIRE、SK和SK_RAND；
- 确定BAK的状态：是否到期，如果需要，发送删除BAK命令；

8.2 密钥管理

如果分配了第39号业务，当前BAK秘密列表和更新的BAK秘密列表被安全的存储在R-UIM中（ME不可以访问）。当ME发送Update BAK命令，R-UIM将在$EF_{UpBAKPARA}$中建立一个新的记录，并将解密的BAK放置到$EF_{UpBAKPARA}$中更新的BAK秘密列表的记录中。

当ME发送Delete BAK命令，R-UIM将在$EF_{BAKPARA}$中搜寻给定的BCMCS_Flow_ID和BAK_ID。如果找到了这样的记录，R-UIM将删除在BAK秘密列表中对应于该BCMCS_Flow_ID和BAK_ID的BAK的记录（用‘FF’填充相应的字节）。如果在$EF_{BAKPARA}$中没有找到相应的记录，则R-UIM将在$EF_{UpBAKPARA}$中搜寻BCMCS_Flow_ID和BAK_ID。如果在$EF_{UpBAKPARA}$中找到了这样的记录，R-UIM将删除在$EF_{UpBAKPARA}$中的相应的记录，并删除在更新的BAK秘密列表中对应于BCMCS_Flow_ID和BAK_ID的BAK。

当ME发送Retrieve SK命令，如果在$EF_{BAKPARA}$中找到了与BCMCS_Flow_ID和BAK_ID相匹配的记录，R-UIM将使用BAK秘密列表中对应的BAK来生成SK。如果在$EF_{UpBAKPARA}$中找到了与BCMCS_Flow_ID和BAK_ID匹配的记录，则R-UIM拷贝BCMCS_Flow_ID、BAK_ID、BAK_Expire 这三个参数到$EF_{BAKPARA}$，并从更新的BAK秘密列表中拷贝相应的BAK到BAK秘密列表中，然后使用这个BAK生成SK。如果在$EF_{BAKPARA}$和$EF_{UpBAKPARA}$中都找不到与BCMCS_Flow_ID和BAK_ID相匹配的记录，则R-UIM返回错误状态字‘6A88’——没有找到引用的数据。

附 录 A
资料性附录
建议的文件内容

表A.1汇总了本标准中定义的R-UIM中文件的基本要求。

（1）除非另有声明，附录中所有的大小以字节定义。

（2）表中所定义的缺省值仅当其可以获得时适用，并且这些值仅作参考值。某些情况下，无缺省值时，运营商必须定义确切的参数值。当必须有参数值时，应列出有效值或其范围。

（3）缺省值或参数值仅用于一般的快速参考，而不进行细节的定义。要定义更加详细的内容，请参考相应的文件。

（4）这里不包含GSM特有的文件。

（5）如果没有分配值给EF，那么这些文件的的参数值是不清楚的，本附录这种情况的EF值推荐了参数值。

表A.1 R-UIM文件汇总

文件名	文件 ID	文件类型	访问条件 - Read	访问条件- Update	访问能条件 – Invalidate- Rehabilitate	大小 Byte	强制（M）或 可选（O）	缺省值（D）和/或参数值（P） Byte
鉴权 –NAM 参数和操作参数								
A-Key	—	—	Never	Never	—	8	M	由运营商定义
Root Key	—	—	Never	Never	—	16	M	由运营商定义
BCMCS Root Key	—	—	Never	Never	—	16	O	由运营商定义
IMS Root Key	—	—	Never	Never	—	16	O	由运营商定义
WLAN Root Key	—	—	Never	Never	—	16	O	由运营商定义
SSD	—	—	Never	Never	—	16	M	—
EF_{COUNT}	3F00/7F25/6F21	CY	CHV1	CHV1	ADM-ADM	2	M	D = '00 00'
BAK	—	—	Never	Never	—	16	O	由运营商定义
UpdatedBAK	—	—	Never	Never	—	16	O	由运营商定义
SharedSecret	—	—	Never	Never	—	可变	O	由运营商定义
UAK	—	—	Never	Never	—	16	O	由运营商定义
SQN_{MS}	—	—	Never	Never	—	6	O	—
UpdatedBAK	—	—	Never	Never	—	16	O	由运营商定义
SharedSecret	—	—	Never	Never	—	可变	O	由运营商定义
UAK	—	—	Never	Never	—	16	O	由运营商定义
SQN_{MS}	—	—	Never	Never	—	6	O	—
NAM Parameters and Operational Parameters								
EF_{IMSI_M}	3F00/7F25/6F22	TR	CHV1	ADM	ADM-CHV1	10	M	P = 由运营商定义 or D='00...00'
EF_{IMSI_T}	3F00/7F25/6F23	TR	CHV1	ADM	ADM-CHV 1	10	M	P = 由运营商定义 or D='00...00'

表 A.1（续）

文件名	文件 ID	文件类型	访问条件- - Read	访问条件- Update	访问能条件- - Invalidate- Rehabilitate	大小 Byte	强制（M）或可选（O）	缺省值（D）和/或参数值（P） Byte
EF_{TMSI}	3F00/7F25/6F24	TR	CHV1	CHV1	ADM-CHV 1	16	M	D = '00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00'
EF_{AH}	3F00/7F25/6F25	TR	CHV1	CHV1	ADM-ADM	2	M	P = 由运营商定义 or D = '00 00'
EF_{AOP}	3F00/7F25/6F26	TR	CHV1	CHV1	ADM-ADM	1	M	—
EF_{ALOC}	3F00/7F25/6F27	TR	CHV1	CHV1	ADM-ADM	7	M	—
$EF_{CDMAHOME}$	3F00/7F25/6F28	LF	CHV1	CHV1	ADM-ADM	5	M	P = 由运营商定义 or D = '00 00 00 00 00'
EF_{ZNREGI}	3F00/7F25/6F29	LF	CHV1	CHV1	ADM-ADM	8	M	D = '00 00 00 00 00 00 00 00'
EF_{SNREGI}	3F00/7F25/6F2A	TR	CHV1	CHV1	ADM-ADM	7	M	-
$EF_{DISTREGI}$	3F00/7F25/6F2B	TR	CHV1	CHV1	ADM-ADM	8	M	D = '00 00 00 00 00 00 00 00'
EF_{ACCOLC}	3F00/7F25/6F2C	TR	CHV1	ADM	ADM-ADM	1	M	P = '00' to '0F' 由 IMSI_M / IMSI_T 得到
EF_{TERM}	3F00/7F25/6F2D	TR	CHV1	CHV1	ADM-ADM	1	M	由运营商定义 P = '00' to '07'
EF_{SSCI}	3F00/7F25/6F2E	TR	CHV1	CHV1	ADM-ADM	1	O	由运营商定义 P = '00' to '07'
EF_{ACP}	3F00/7F25/6F2F	TR	CHV1	CHV1	ADM-ADM	7	M	由运营商定义
EF_{PRL}	3F00/7F25/6F30	TR	CHV1	ADM	ADM-ADM	可变	M	由运营商定义
EF_{RUIMID}	3F00/7F25/6F31	TR	ALW	NEVER	NEVER-NE VER	8	M	由制造商定义
EF_{CST}	3F00/7F25/6F32	TR	CHV1	ADM	ADM-ADM	可变	M	由运营商定义
EF_{SPC}	3F00/7F25/6F33	TR	ADM	ADM	ADM-ADM	3	M	D = '00 00 00' or P = '00 00 00' to '99 99 99'
$EF_{OTAPASPC}$	3F00/7F25/6F34	TR	CHV1	CHV1	ADM-ADM	1	M	由运营商定义 or D = '00'
$EF_{NAMLOCK}$	3F00/7F25/6F35	TR	CHV1	CHV1	ADM-ADM	1	M	由运营商定义
EF_{OTA}	3F00/7F25/6F36	TR	CHV1	ADM	ADM-ADM	可变	M	P=在3GPP2 C.S0016-C 中定义
EF_{SP}	3F00/7F25/6F37	TR	CHV1	CHV1	ADM-ADM	1	M	由运营商定义 .
EF_{ESNME}	3F00/7F25/6F38	TR	ALW	ADM	ADM-ADM	8	M	D ='00...00'
$EF_{Revision}$	3F00/7F25/6F39	TR	ALW	ADM	ADM-ADM	1	M	D = '03'
EF_{PL}	3F00/7F25/6F3A	TR	ALW	CHV1	ADM-ADM	可变	M	D = 'FF... FF'
EF_{SMS}	3F00/7F25/6F3C	LF	CHV1	CHV1	ADM-ADM	可变	O	D = '00 FF...FF'
EF_{SMSP}	3F00/7F25/6F3D	LF	CHV1	CHV1	ADM-ADM	可变	O	D = 'FF...FF'
EF_{SMSS}	3F00/7F25/6F3E	TR	CHV1	CHV1	ADM-ADM	可变	O	D = 'FF...FF '
EF_{SSFC}	3F00/7F25/6F3F	TR	CHV1	CHV1	ADM-ADM	可变	O	由运营商定义
EF_{SPN}	3F00/7F25/6F41	TR	ALW	ADM	ADM-ADM	35	O	由运营商定义
EF_{USGIND}	3F00/7F25/6F42	TR	CHV1	ADM	ADM-ADM	1	M	D = '00' 如果使用 ESN D ='01' if 如果使用 UIM ID

表 A.1（续）

文件名	文件 ID	文件类型	访问条件- Read	访问条件- Update	访问能条件- Invalidate- Rehabilitate	大小 Byte	强制（M）或可选（O）	缺省值（D）和/或参数值（P） Byte
EF_{AD}	3F00/7F25/6F43	TR	ALW	ADM	ADM-ADM	可变	M	D = '00...00'
EF_{MDN}	3F00/7F25/6F44	LF	CHV1	CHV1	ADM-ADM	11	O	由运营商定义
EF_{MAXPRL}	3F00/7F25/6F45	TR	CHV1	ADM	ADM-ADM	2 或 4	M	由运营商定义
EF_{SPCS}	3F00/7F25/6F46	TR	CHV1	NEVER	NEVER-NEVER	1	M	P = 如果 EF 6F33 被设置为缺省值那么 D = '00' 否则 D = '01'
EF_{ECC}	3F00/7F25/6F47	TR	ALW	ADM	ADM-ADM	可变	O	D = 'FF'
$EF_{ME3GPDOPC}$	3F00/7F25/6F48	TR	CHV1	CHV1	ADM-ADM	1	O	D = '00'
$EF_{3GPDOPM}$	3F00/7F25/6F49	TR	CHV1	CHV1	ADM-ADM	1	O	由运营商定义
EF_{SIPCAP}	3F00/7F25/6F4A	TR	CHV1	ADM	ADM-ADM	4	O	由运营商定义
EF_{MIPCAP}	3F00/7F25/6F4B	TR	CHV1	ADM	ADM-ADM	5	O	由运营商定义
EF_{SIPUPP}	3F00/7F25/6F4C	TR	CHV1	ADM	ADM-ADM	可变	O	由运营商定义
EF_{MIPUPP}	3F00/7F25/6F4D	TR	CHV1	ADM	ADM-ADM	可变	O	由运营商定义
EF_{SIPSP}	3F00/7F25/6F4E	TR	CHV1	CHV1	ADM-ADM	1	O	由运营商定义
EF_{MIPSP}	3F00/7F25/6F4F	TR	CHV1	CHV1	ADM-ADM	可变	O	由运营商定义
$EF_{SIPPAPSS}$	3F00/7F25/6F50	TR	CHV1	CHV1	ADM-ADM	可变	O	由运营商定义
SimpleIP CHAP SS	—	—	Never	Never	—	可变	O	由运营商定义
MobileIP SS	—	—	Never	Never	—	可变	O	由运营商定义
Shared Secret	—	—	Never	Never	—	可变	O	由运营商定义
EF_{PUZL}	3F00/7F25/6F53	TR	CHV1	ADM	ADM-ADM	可变	O	由运营商定义
$EF_{MAXPUZL}$	3F00/7F25/6F54	TR	CHV1	ADM	ADM-ADM	5	O	由运营商定义
EF_{MECRP}	3F00/7F25/6F55	TR	CHV1	CHV1	ADM-ADM	3	M	D = '00 00 00'
$EF_{HRPDCAP}$	3F00/7F25/6F56	TR	CHV1	ADM	ADM-ADM	2	O	由运营商定义
$EF_{HRPDUPP}$	3F00/7F25/6F57	TR	CHV1	ADM	ADM-ADM	可变	O	由运营商定义
HRPD AA CHAP SS	—	—	Never	Never	—	可变	O	由运营商定义
EF_{CSSPR}	3F00/7F25/6F58	TR	CHV1	ADM	ADM-ADM	1	O	D = 'FF'
EF_{ATC}	3F00/7F25/6F59	TR	CHV1	ADM	ADM-ADM	1	O	由运营商定义
EF_{EPRL}	3F00/7F25/6F5A	TR	CHV1	ADM	ADM-ADM	可变	O	由运营商定义

附 录 B
资料性附录
与 BCMCS 相关的 TAG 值

Tag	数据单元的名称	使 用
80	BCMCS Flow ID TLV对象	BCMCS命令
81	BAK_ID TLV 对象	BCMCS 命令
82	RAND、SK RAND或TK RAND TLV对象	BCMCS 命令
83	BAK Expire TLV对象	BCMCS 命令
84	数据包索引TLV对象	BCMCS 命令
85	SK TLV对象或SRTP SK TLV对象	BCMCS 命令
86	时间戳TLV对象	BCMCS 命令
87	Auth 签名TLV对象	BCMCS 命令
88	Challenge TLV对象	BCMCS 命令
89	分类响应TLV对象	BCMCS 命令

参 考 文 献

1. 3GPP2 C.S0001-D,Introduction to cdma2000 Spread Spectrum Systems,March 2004
2. 3GPP2 C.S0002-D,Physical Layer Standard for cdma2000 Spread Spectrum Systems,March 2004
3. 3GPP2 C.S0004-D,Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems,March 2004
4. ITU-T Recommendation E.212,"Identification Plan for Land Mobile Stations",1988
5. 3GPP2 X.S0004-E V2.0,Cellular Radio-Telecommunications Intersystem Operations,July,2005
6. TIA/EIA/IS-91-A,Base Station – Mobile Station Compatibility Specification for 800 MHz Cellular, Auxiliary,and Residential Services，November 1999
7. 3GPP2 X.S0011-C cdma2000 Wireless IP Network Standard，August，2003
8. IETF RFC 2002,IP Mobility Support，October 1996
9. IETF RFC 2794,Mobile IP Network Access Identifier Extension for IPv4,March 2000
10. IETF RFC 2865,Remote Authentication Dial In User Service(RADIUS),June 2000
11. IETF RFC 3012,Mobile IPv4 Challenge/Response Extensions，November 2000
12. 3GPP2 A.S0008-0,Interoperability Specification(IOS)for High Rate Packet Data(HRPD)Network Access Interfaces，Addendum 1,May 2003
13. ETSI TS 131.103 Digital cellular telecommunications system(Phase 2+);Universal Mobile Telecommunications System （UMTS）;Characteristics of the IP Multimedia Services Identity Module (ISIM)application(Release 6)
14. 3GPP2 X.S0013 All-IP Core Network Multimedia Domain(MMD) Overview,December,2003
15. 3GPP2 S.S0083-A，Broadcast-Multicast Service Security Framework,Jan 2005
16. ETSI TS 123.038 Alphabets and language-specific information
17. TSG-X.S0016-310 MMS MM1 Stage-3 Using OMA/WAP,May 2003
18. TSG-X.S0016-311 MMS MM1 Stage-3 Using M-IMAP for message submission and retrieval
19. TSG-X.S0016-312 MMS MM1 Stage-3 Using SIP,June 2004
20. 3GPP2 S.S0055-A V3.0 Enhanced Cryptographic Algorithms September 2005
21. 3GPP2 C.S0024-A,cdma2000 High Pate Packet Data Air Interface Specification,March 2004
22. 3GPP2 C.S0068-0 ME Personalization,2006-6
23. 3GPP2 S.S0086-B IMS Security Framework,December 2005