第一部分：物理及电器标准

1 总则

本标准规定了 900/1800MHZ TDMA 数字蜂窝移动通信网移动台人机接口（MMI）和用户识别模块（SIM）与移动设备（ME）之间接口技术要求。

本标准适用于 900/1800MHZ TDMA 数字蜂窝移动通信网移动台

2 参考文献

下列标准所包含的条文，通过在标准中引用而构成为本标准的条文。本标准推出时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

1．ISO639
2．ISO7810 识别卡的物理特性
3．ISO7811 识别卡 记录技术 第 1 部分：凸印
4．ISO7816-1 识别卡 带触点的集成电路卡 第 1 部分：物理特性
5．ISO7816-2 识别卡 带触点的集成电路卡 第 2 部分：尺寸和触点的位置
6．ISO7816-3 识别卡 带触点的集成电路卡 第 3 部分：电信号和传输协议
7．GSM02.07 数字蜂窝通信系统((Phase 2+)：移动基站（MS）特性
8．GSM02.09 数字蜂窝通信系统((Phase 2+)：安全特性
9．GSM02.11 数字蜂窝通信系统((Phase 2+)：服务接入特性
10.GSM02.17 数字蜂窝通信系统((Phase 2+)：用户识别模块（SIM）功能特性
11.GSM02.24 数字蜂窝通信系统((Phase 2+)：资费建议信息
12.GSM02.86 数字蜂窝通信系统((Phase 2+)：资费辅助服务-Stage1
13.GSM03.03 数字蜂窝通信系统((Phase 2+)：编码，地址和识别
14.GSM03.20 数字蜂窝通信系统((Phase 2+)：与安全有关的网络功能
15.GSM03.38 数字蜂窝通信系统((Phase 2+)：字母表和语言细节信息
16.GSM03.41 数字蜂窝通信系统((Phase 2+)：小区广播短信服务的实现
17.YD/T910.1-1997 900/1800MHz TDMA 数字蜂窝移动通信网移动台（第 2 阶段）人机接口
18.YD/T1025-1999 900/1800MHz TDMA 数字蜂窝移动通信网移动台人机接口和 SIM-ME 接口技术要求（第 2+阶段）

3 符号和缩略语

3．1 符号

Vcc 供电电压。

Vpp 编程电压。

‘ 0 ’到‘ 9 ’和‘ A ’到‘ F ’十六进制数字。

3．2 缩略语

A3 算法3，鉴权算法；用来鉴别用户 Algorithm 3, authentication algorithm; used for authenticating the subscriber

A5 算法5，加密算法，用于数据加密/解密 Algorithm 5, cipher algorithm; used for enciphering/deciphering data

A8 算法8，密钥产生算法，用于产生Kc Algorithm 8, cipher key generator; used to generate K_c

A38 执行A3和A8功能的一个单一算法 A single algorithm performing the functions of

A3 and A8

ACM 累积呼叫计数 Accumulated Call Meter

ADN 缩位拨号 Abbreviated Dialling Number

ADM 在创建EF的管理者控制下的对此EF的存取条件 Administrator

ALW 总是（EF的存取条件之一） Always

AoC 计费通知 Advice of Charge

APDU 应用协议数据单元 Application Protocol Data Unit

ATR 复位响应 Answer To Reset

BCCH 广播控制信道 Broadcast Control CHannel

BCD 十进制数的二进制编码 Binary Coded Decimal

BTS 基站 Base Transmitter Station

CB 小区广播 Cell Broadcast

CBMI 小区广播消息识别 Cell Boardcast Message Identifier

CCITT 国际电报电话咨询委员会（现在也叫 ITU 电信标准化部）The International Telegraph and Telephone Consultative Committee

CCP 能力配置参数 Capability/Configuration Parameter

CHV 卡持有人校验信息；用来校验用户身份的存取条件 Card Holder Vertification

CLA 命令类 Class

CRn 致性需求‘n’ Conformance Requirement’n’

DCS 数字蜂窝系统 Digital Cellular System

DF 专用文件（数据域的正式称谓） Dedicated File

DTMF 双音多频 Dual Tone multiple Frequence

EF 基本文件 Elementary File

ETS 欧洲电信标准 European Telecommunications Standards

ETSI 欧洲电信标准委员会 European Telecommunications Standards Institute

ETU 基本时间单元 Elementary Time Unit

FDN 固定拔号 Fixed Dailling Number

FT 固定终端 Fixed Terminal

GSM 全球移动通信系统 Global System for Mobile communications

HPLMN 归属 PLMN Home PLMN

IC 集成电路 Integrated Circuit

ICC 集成电路卡 Integrated Circuit Card

ICS 实现一致性声明 ImplementationConformance Statement

ID 用户识别 Identifier

IEC 国际电子技术委员会 International Electrotechnical Commission

IMSI 国际移动用户识别 International Mobile Subscribler Identity

ISO 国际标准化组织 international Organization for Standardization

IUT 经测试实现 Implementation Under Test

Kc 密钥；在加密算法 A5 中使用 Cryptographic Key

Ki 用户鉴权密钥；在鉴权算法 A3 和密钥生成算法 A8 中使用的密钥 Subscribler Authentication Key

LAI 位置区信息；识别一个或一组小区的信息 Location Area Information

LGTH 数据单元的长度 Length

LND 最后拔号存储 Last Number Dailled
LSB 最低有效位 Least Significant Bit
MCC 国家移动代码 Mobile Country Code
ME 移动设备 Mobile Equipment
MF 主文件 Master File
MMI 人一机接口 Man Machine Interface
MNC 移动网号 Mobile Network Code
MS 移动台 Mobile Station
MSISDN 移动站国际 ISDN 号 Mobile Station international ISDN number
MSB 最高有效位 Most Significant Bit
NET 网络 Network
NEV 永远不 Never
NPI 编号方案识别 Numbering Plan Identifier
PIN/PIN2 个人识别号码/个人识别号码 2（相应地 CHV1 和 CHV2 失效） Personal Identification Number
PLMN 公共陆地移动网络 Pulic Land Mobile Network
PTS 协议类型选择（对 ATR 的响应） Protocol Type Select
PUK/PUK2 PIN 解锁号码/PIN2 解锁号码（相应地取代了 UNBLOCK CHV1 和 UNBLOCK CHV2） PIN Unblocking Key
RADN 网站发布的一个随机数呼叫 Random
RFU 保留未用 Reserve For Future Use
SIM 用户识别模块 Subscrible Indentity Module
SMS 短消息业务 Short Message Service
SRES SIM 计算的签名响应 Signed Response
SSC 补充业务控制串 Supplementary Service Control string
SW1/SW2 状态字 1/状态字 2 Status Word
TMSI 临时移动用户识别 Temporary Mobile Subscrible Indentity
TON 号码类型 Type Of Number
TP 传输层协议 Transfer layer Protocol
TPDU 传输协议数据单元 Transfer Protocol Data Unit
TS 技术规范 Technical Specification
UNBLOCK CHV1/2 解锁 CHV1/CHV2 的值
VPLMN 拜访 PLMN Visited PLMN

Vih 输入电压上限 High level input voltage
Vil 输入电压下限 Low level input voltage
Vcc 供电电源 Power supply voltage at VCC
Vpp 编程电压 Programming voltage at VPP
Voh 输出电压上限 High level output voltage
Vol 输出电压下限 Low level output voltage
tr 信号上升时间 Rise time between 10% and 90% of signal amplitude
tf 信号下降时间 Fall time between 90% and 10% of signal amplitude
Iih 输入电流上限 High level input current
Iil 输入电流下限 Low level input current

Icc	工作供电电流	Supply current at VCC
Ipp	编程电流	Programming current at VPP
Ioh	输出电流上限	High level output current
Iol	输出电流下限	Low level output current
Cin	输入电容	Input capacitance
Cout	输出电容	Output capacitance

4 物理特性（ID-1 卡和 Plug-in 卡）

4．1 主要性能指标

符合国际标准的 SIM 卡主要由 ISO7811-1，2，3，4，5；ISO7812；ISO7813；ISO7816-1 等定义。其主要特性指标如下：

- **抗紫外线——**所有保护指标超过环境紫外线指标的标准，由 SIM 卡的制造商制定。
- **X 射线——**卡面每边在受到 0.1GY，相当于 70-140KV 中等能量的 X 射线照射时（一年累计），卡的功能不会丧失。
- **触点与卡基表面的误差——**所有触点与临近卡基表面的高度差应小于 0.01mm。
- **机械强度**——在每个触点（以及整个电极表面）上，以等效于在 1mm 直径的钢球上施加 1.5N 力的情况下,不应损坏卡片。
- **电阻（触点）——**在两个短路的触点间，施加 50uA-300mA 的直流电，其触点之间的接触电阻应小于 0.5Ω。在施加 4MHz，10mA 的交流电时，其触点之间的阻抗的压降小于 10mV。
- **抗磁场干扰——**卡片在稳定的 79500A/m（1000Qe）磁场下，不应使集成电路丧失功能。
- **抗静电能力——**在卡的任何触点与地之间通过 1000PF 的电容，1500Ω电阻，在 1500V 静电放电时，卡的性能不应受到影响。
- **抗弯曲特性：**
  纵向：最大变形：2cm；周期：30 次每分钟
  横向：最大变形：1cm；周期：30 次每分钟
  ——卡在 1000 次弯曲之后应该正常工作。
- **SIM 卡的工作温度——**SIM 卡在 -25°C 和 +70°C 之间应该正常工作,偶尔达到最高温度+85°C（每次不能超过 4 个小时，在卡的有效寿命期内不能超过 100 次）

4．2 格式和布局

4．2．1 最小接触面积

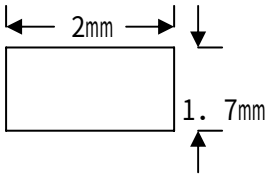


图1

4．2．2 ID-1 卡的几何尺寸

85．6（长）mm*53.98(宽)mm*0.76(厚)mm

4．2．3 嵌入式 SIM 卡

PLUG—IN SIM 卡可以通过切除一个 ID-1 SIM 卡的多余塑料部份获得。下图中括号里的值表明了 PLUG-IN 和 ID-1 SIM 之间位置上的关系：

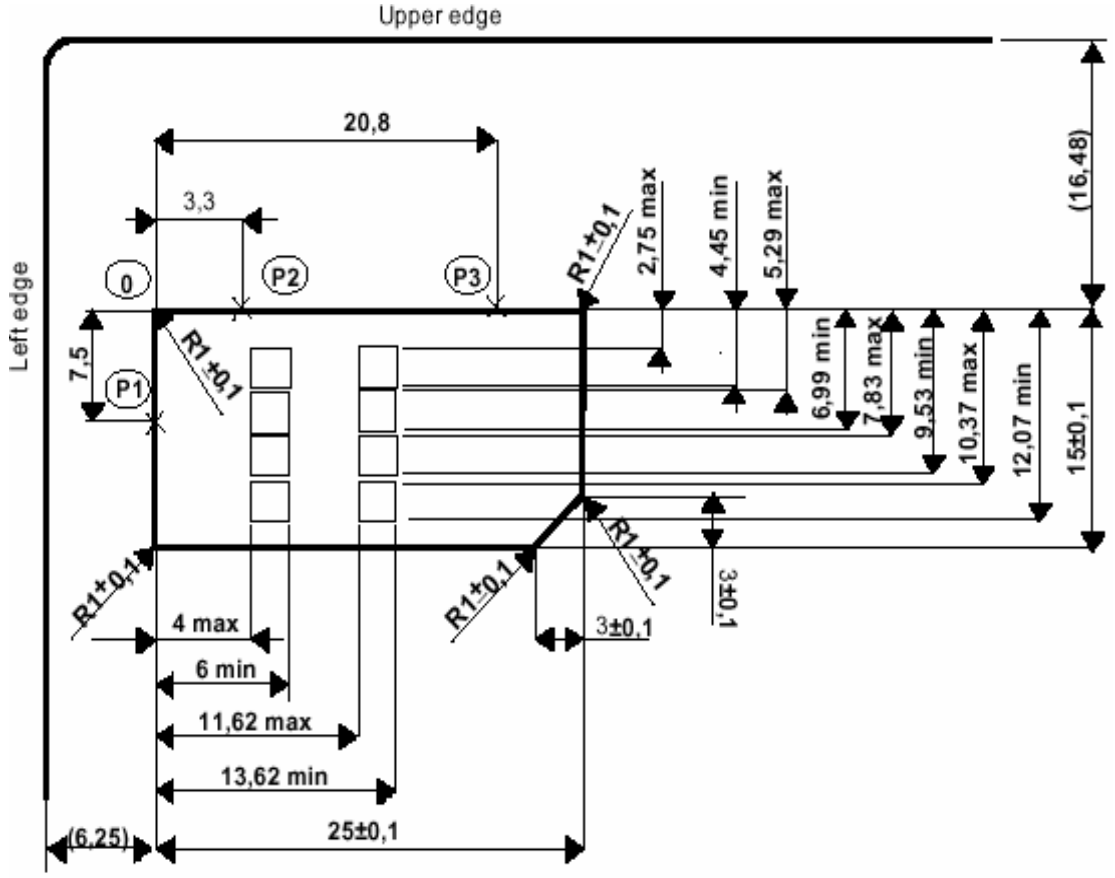


图 2 PLUG-IN SIM 卡尺寸

最大的弯曲度和弯曲次数

1．

2．卡运作时的温度范围

3．触点位置，接触面积，分布

参考 ISO7816—1（物理特性），ISO7816—2（触点尺寸和位置），ISO7810（各种识别卡的物理特性），ISO7813（金融交易卡的阻燃性和外形尺寸）

GSM11.11_4，GSM02.07 ，ISO7811，GSM02.17

5 电器特性

1．供电电压 Vcc（触点 C1）

2．复位 RST （触点 C2）（冷复位，热复位）

3．时钟 CLK（触点 C3）

4．I/O（触点 C7）

5．电源打开时工作状态

5 电气特性

5．1 电信号描述

I/O（C7）：卡的输入或输出连续数据端

VPP（C6）：编程电压输入（可选）端

GND（C5）：地（参考电压）端

CLK（C3）：时钟信号输入端
RST（C2）：复位信号输入端
VCC（C1）：供电电源输入端

5．2 电压和电流

5．2．1 供电电压 Vcc(触点 C1)

5．2．1．1 电压限制

SIM 应该能在下面所述的供电电压条件下运作，以保障在 GSM 的环境下正常的运作。
当触点 C1（VCC）的供电电压在表 1的范围内时，SIM 应该能进行运作。

表1 供电电压 Vcc

卡类型	最小电压 Vmin（单位：V）	最大电压 Vmax（单位：V）
5V	4.5	5.5
3V	2.7	3.3
1.8V	1.62	1.98

5．2．1．2 电流限制

在正常的操作条件下 SIM 卡的电流消耗不得超过规定限度，以保证在 GSM 环境中正常运作见表 2、表 3。

表2 Vcc 上的电流消耗

卡类型	正常条件下的 Imax(平均值，见注) (单位：mA)	正常条件下的最大 CLK 频率 f_{max} (单位：Mhz)	试验时 Vcc 上的电压 Vcc_{max} (单位：V)
5V	10	5	5.5
3V	6	4	3.3
1.8V	4	4	1.98
注：Imax 是包含电流尖峰在内的 Vcc 电流的平均值。			

表3 Vcc 上的电流尖峰

卡类型	Imax (单位：mA)	最大电荷 (单位：nAs)	最大持续时间 (单位：ns)
5V	200	40	400
3V	60	12	400
1.8V	60	12	400
注：Imax 是包含电流尖峰在内的 Vcc 电流的平均值。			

5．2．1．3 空闲电流的限制

在空闲条件下 SIM 卡的电流消耗不得超过规定限度见表 4，以保证在 GSM 环境中正常运作。

表4 空闲模式下的电流消耗

卡类型	最大电流 Imax（单位：uA） 空闲状态下，时钟频率 1Mhz	试验期间 Vcc 上的最大电压 Vcc_{max}（单位：V）
5V	200	5.5
3V	200	3.3
1.8V	200	1.98

5．2．1．4 在全频率下的电流限制

在空闲条件下 SIM 卡的电流消耗不得超过规定限度见表 5，以保证在 GSM 环境中正常运作。

表5 空闲模式全频率下的电流消耗

卡类型	空闲状态下的 Imax(平均值)(单位：uA)	空闲模式下的最大 CLK 频率 f_{max}(单位：Mhz)	试验时 Vcc 上的最大电压 Vcc_{max}(单位：V)
5V	1000	5	5.5
3V	1000	4	3.3
1.8V	1000	4	1.98

5．2．1．5 时钟停模式的电流限制

在时钟停条件下 SIM 卡的电流消耗不得超过规定限度见表 6,以保证在 GSM 环境中正常运作。

表6 时钟停模式下的电流消耗

卡类型	时钟停模式下最大电流 Imax（平均值）（单位：uA）	试验期间 Vcc 上的最大电压 Vcc_{max}（单位：V）
5V	200	5.5
3V	100	3.3
1.8V	100	1.98

5．2．2 复位 RST （触点 C2）

SIM 操作时，复位信号 RST 应满足以下限制，以保证在 GSM 环境中正常运作。

SIM 操作（静态操作）对 RST 有以下限制见表 7。

表7 复位信号 RST

卡类型	V_{OL}min (单位：V)	V_{OL}max (单位：V)	I_{OL}max (单位：uA)	V_{OH}min (单位：V)	V_{OH}max (单位：V)	I_{OH}max (单位：uA)
5V	-0.3	0.6	-200	0.7*Vcc	Vcc+0.3V	+20
3V	-0.3	0.2*Vcc	-200	0.8*Vcc	Vcc+0.3V	+20
1.8V	-0.3	0.2*Vcc	-200	0.8*Vcc	Vcc+0.3V	+20

t_R 和 t_F 不得超过 400μs，并且 Cout 和 Cin 等于 30pF。

5．2．3 时钟 CLK（触点 C3）

5．2．3．1 频率和占空比

SIM 操作时，时钟信号 CLK 应满足以下限制，以保证在 GSM 环境中正常运作。

- SIM 不应支持内置时钟。
- 在稳定的运行期间，SIM 应该支持时钟源 40%~60%之间的占空比。
- SIM 操作对 CLK 有以下限制见表 8。

表8 时钟信号 CLK

卡类型	V_{OL}min (单位：V)	V_{OL}max (单位：V)	V_{OH}min (单位：V)	V_{OH}max (单位：V)	T_R&$T_F$max	fmax (单位：Mhz)
5V	-0.3	0.5	0.7*Vcc	Vcc+0.3V	9%, 最大 0.5us	5
3V	-0.3	0.2*Vcc	0.8*Vcc	Vcc+0.3V	50ns	4
1.8V	-0.3	0.2*Vcc	0.8*Vcc	Vcc+0.3V	50ns	4
注：必须在 V_{OL} 和 V_{OH} 的 10%和 90%之间测量 t_R 和 t_F，并且 Cout 和 Cin 等于 30pF。						

5．2．3．2 电压和电流

SIM 操作时，时钟信号 CLK 应满足以下限制，以保证在 GSM 环境中正常运作。

- SIM 操作时对 CLK 有如下限制见表 9。

表9 时钟信号 CLK 电压和电流

卡类型	V_{OL}min (单位 :V)	V_{OL}max (单位 :V)	I_{OL}max(单位：uA)	V_{OH}min (单位 :V)	V_{OH}max (单位 :V)	I_{OH}max(单位：uA)	T_R&$T_F$max	fmax (单位：Mhz)
5V	-0.3	0.5	-200	0.7*Vcc	Vcc+0.3V	+20	9%,最大 0.5us	5
3V	-0.3	0.2*Vcc	-20	0.8*Vcc	Vcc+0.3V	+20	50ns	4
1.8V	-0.3	0.2*Vcc	-20	0.8*Vcc	Vcc+0.3V	+20	50ns	4

5．2．4 I/O（触点 C7）

5．2．4．1 电压和电流

SIM 操作时，I/O 信号应满足以下限制，以保证在 GSM 环境中正常运作。

- SIM 操作时对 I/O 有如下限制见表 10、表 11。

表10 I/O 信号要求 1

卡类型	V_{OL}min (单位 :V)	V_{OL}max (单位 :V)	I_{OL}max(单位：uA)	V_{OH}min (单位 :V)	V_{OH}max (单位 :V)	I_{OH}max(单位：uA)	T_R&$T_F$max	fmax (单位：Mhz)
5V	-0.3	0.5	-1000	3.8	Vcc+0.3V	+20	1us	5
3V	-0.3	0.4	-1000	0.7*Vcc	Vcc+0.3V	+20	1us	4
1.8V	-0.3	0.3	-1000	0.7*Vcc	Vcc+0.3V	+20	1us	4

表11 I/O 信号要求 2

卡类型	V_{IL}min (单位 :V)	V_{IL}max (单位 :V)	I_{IL}max(单位：uA)	V_{IH}min (单位 :V)	V_{IH}max (单位 :V)	I_{IH}max(单位：uA)	T_R&$T_F$max	fmax (单位：Mhz)
5V	-0.3	0.8	+1000	0.7*Vcc	Vcc+0.3V	±20	1us	5
3V	-0.3	0.2*Vcc	+1000	0.7*Vcc	Vcc+0.3V	±20	1us	4
1.8V	-0.3	0.2*Vcc	+1000	0.7*Vcc	Vcc+0.3V	±20	1us	4

5．2．5 状态

电源打开时会有两种状态：操作状态和空闲状态。当 SIM 正确执行一条命令时，是操作状态；在任何其他时间是空闲状态。

- SIM 应该能确切地支持下面其中一项。

——允许时钟停止 ,没有优先电平
——允许时钟停止，高电平的优先
——允许时钟停止，低电平的优先
——不允许时钟停止。
——不允许时钟停止，除非在高电平上
——不允许时钟停止，除非在低电平上

- 当 SIM 在空闲状态下时，所有相关的数据应该保留下来。
- 在成功地解码了一个从 PHASE I 的 ME 接收到的 SLEEP 命令以后，一个 PHASE II、或更新的 SIM 应该总是发送状态信息“命令正常结束”(SW1=90,SW2=00)。

6 传输协议

在 SIM 卡和 ME 的数据交互的过程中，SIM 卡的传输协议应符合 ISO-7816 的规定，现行的 ISO-7816 标准规定了 T=0 和 T=1 两种传输协议。

6．1 SIM 卡的复位

SIM 卡的复位是由 ME 触发的，在 SIM 卡的复位之前 ME 对 SIM 卡的触点接通有以动作：

-RST 处于低电平；
-VCC 开始供电；
-I/O ME的I/O应该处于接收状态
-VPP 被置为空闲状态
-CLK 应当提供适当的、稳定的时钟
图 1 为 ME 对 SIM 的复位时序图：

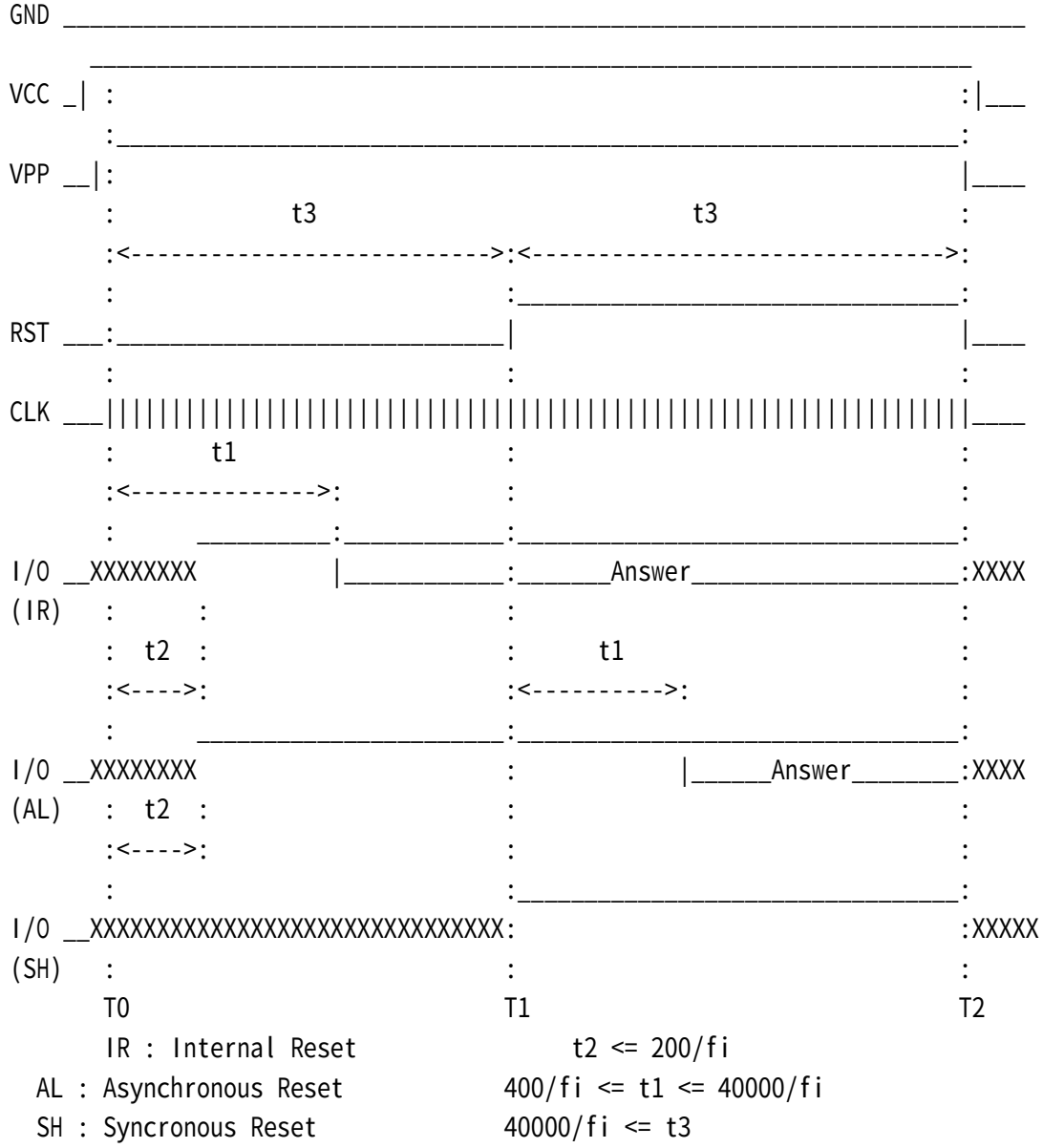


图 1：SIM 卡的复位

当 SIM 卡的触点接通序列结束后（RST 处于低电平，VCC 稳定供电， ME 的 I/O 应该处于接收状态，VPP 被置为空闲状态，CLK 应当提供适当的、稳定的时钟），SIM 卡准备复位。如图 1 所示：

- 时钟信号在 T0 时刻加到 CLK 触点，I/O 总线在时钟信号加到 CLK 触点 200 个时钟周期（T0 时刻之后的 t2 时间段）之内应该处于高阻状态；
- 内部复位的 SIM 卡，在几个时钟周期之后开始复位，复位应答应该在 400-40000

个时钟周期内开始（T0 时刻之后的 t1 时间段之内）；

- 低电平复位的 SIM 卡的复位信号至少在 40000 个时钟周期内 RST 触点维持低电平（T0 之后的 t3 时间段内），如果在 40000 个时钟周期内没有复位应答，则 RST 触点被置为高电平；
- I/O 端的复位应答必须在 RST 上升沿开始的 400-40000 个时钟周期内开始(T1 时刻之后的 t1 时间段之内)
- 如果复位应答在在 400-40000 个时钟周期内没有开始 (T1 时刻之后的 t3 时间段之内)，则 RST 触点的电平将被置为低电平（在 T2 时刻），触点也将被 ME 释放。

6．2 复位应答

SIM 卡的数据以异步半双工方式经 I/O 线在 ME 和 IC 卡之间双向传送。由 ME 向 SIM 卡提供时钟信号，并以次来控制数据时序。信息交换的数字和字符应该符合 ISO7816 标准规定的 T=0 和 T=1 两种传输协议。

6．2．1 数位宽度

I/O 线上所用的数位宽度被确定为基本的时间单位（etu—elementary time uint)。

- 对于内部时钟卡，初始的 etu=1/9600s
- 对于外部时钟卡 etu 和时钟频率间存在着线性关系：初始 etu=372/fi s fi 为初始的时钟频率，fi 的取值范围为 1-5MHz。

6．2．2 字符帧

在传输字符帧之前，I/O 被置为高电平。

一个字符帧含有 10 个连续的 bits

- 一个 bit 的起始字位，A 电平（0-t1)；
- 8 个 bits 的数据位，ba-bh；
- 一个 bit 的奇偶校验位，bi。

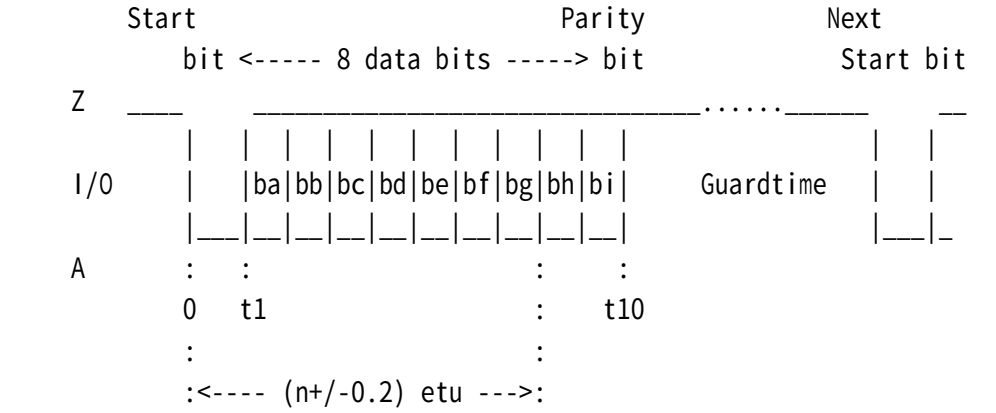


图 2 字符帧

起始位存在的核实必须在 0.7 个 etu 之内进行，相继的各位必须在（n+0.5±0.2）etu 区间内被接收。

在一个字符帧内，从它的起始位前沿起到第 n 位的后沿间的时间是（n±0.2）etu。

相连两个字符帧的起始位前沿之间的区间包括了字符宽度（10±0.2）etu，在保护时间内，SIM 卡和 ME 二者都处于接收方式（I/O 线处于状态 Z)。

6．2．3 复位应答的结构和内容

6．2．3．1 复位应答的一般构成

1．构成

复位应答最多由 32 个字节组成（包括历史字节，但不包括 TS)，如下图所示

Reset

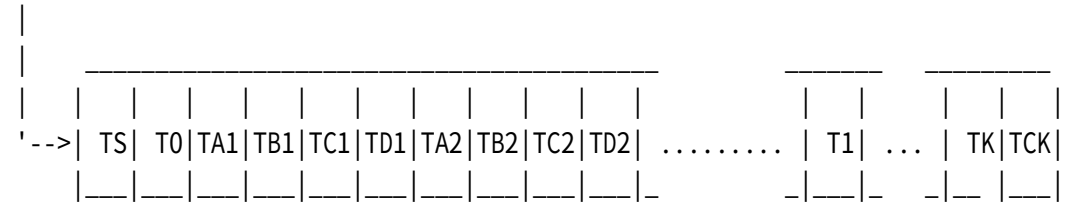


图 3 复位应答的一般构成

TS ：初始字符
T0 ：格式字符
TAi ：接口字符 [全局代码 FI,DI]
TBi ：接口字符 [全局代码 II,PI1]
TCi ：接口字符 [全局代码 N]
TDi ：接口字符 [全局代码 Yi+1, T]
T1, ... , TK ：历史字符 (最多15个字符)
TCK ：校验字符

2．时序

在复位应答期间，相连两个字符的起始位的前沿之间的最小区间为 12 初始 etu，而相连两个字符的起始位的前沿之间的最大区间为 9600 初始 etu。

SIM 卡把复位应答期间要回送的字符在 19200 初始 etu 之内传送。这段时间的度量是在第一个字符（TS）的起始位前沿和最后一个字符的起始位的前沿之后的 12 个初始 etu 之间。

6．2．3．2 复位应答回送的字符

1．初始字符 TS

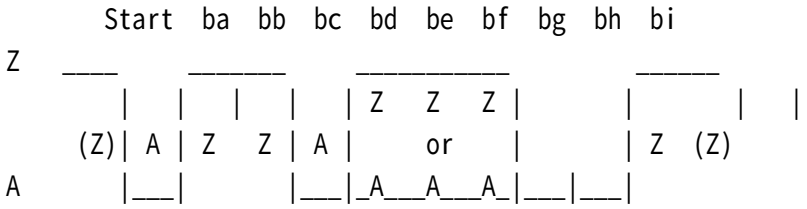


图 4 初始字符 TS

TS 执行两项功能：

- 向终端提供一个已知的位组合模型，以便于同步；
- 提示所用逻辑约定，以便对后继的字符进行解释。

基本响应：SIM 卡必须以下列二值之一来回送 TS

- 反向约定 (Z)ZZAAAAAZ，其值为“ 3F ”；
- 正向约定(Z)ZZAZZZAAZ，其值为“ 3B ”

终端反应：终端必须拒绝回送的 TS 不等于 3B 或 3F 之值的 SIM 卡

2．格式字符 T0

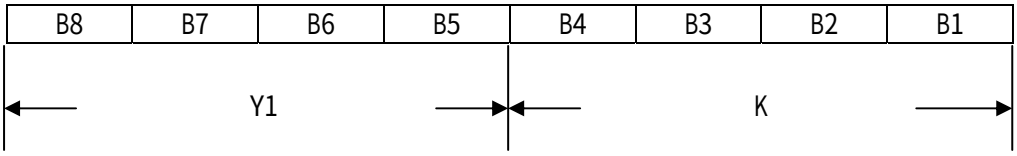


图 5 T0 的构成

T0 由两部分组成，高四位 (B5-B8) 称之为 Y1，用来指示后继字符 TA1 至 TD1 是否存在，

B5-B8 位被置为“ 1 ”状态的，相应地表明 TA1-TD1 的存在。低四位（B1-B4）称之为 K，表明历史字节存在的数量（0-15)。

3． TAi、TBi、TCi、TDi（i=1，2，3…）接口字符，指明了协议参数

TDi 指明了协议类型和是否存在后继接口字符，参看图 6。TDi 包括 Yi+1 和 T 两部分，Yi+1 为高四位组，分别表示后续接口字符 TAi+1、TBi+1、TCi+1、TDi+1 是否存在，T 为低四位组，表示后续发送的协议类型。

T=0：异步半双工字符传输协议

T=1：异步半双工字组传输协议

T=2-15：保留

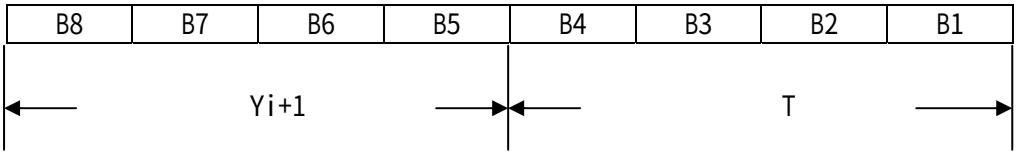


图 6 TDi 指明的信息

TA1：接口控制参数，给出时钟频率变换因数 F 和比特率调整因数 D 的数值

TB1：接口控制参数，给出最大编程电流因子和编程电压因子，它们定义了 Vpp 的工作状态。

TC1：接口控制参数，给出了额外保护时间 N 的值

以上参数的缺省值为：F=372，D=1，I=50，P=5，N=0

4． 历史字符 TK

由 T0 的低四位组 K 来指明历史字符的个数，为 T1、T2…，TK，K≤15。

历史字符给出一般的信息，如：卡的制造者，卡中所用芯片型号，芯片的掩膜 ROM，卡的寿命说明等等。

5．校验字符 TCK

TCK 具有之值使复位应答中所传送数据的完整性得以校验。TCK 之值应使自 T0 至 TCK 的所有字节的异或值为 0。

6．3 协议类型选择（PTS-Protocol type selection）

在 GSM 系统中，SIM 卡如果要实现增强速率，则 SIM 至少要支持两种协议：F=372、D=1 和 F=512、D=1。

SIM 卡在复位应答中的回送的接口控制字符 TA1 不等于‘ 11 ’或‘ 01 ’则 ME 将执行 PTS 过程：

1．ME 只支持缺省速率（F=372，D=1）如图 7 所示

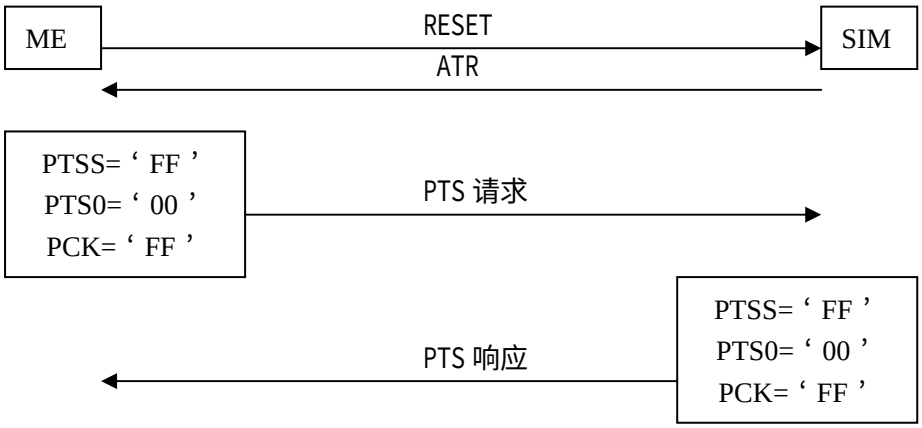


图 7 PTS 过程 ME 只支持缺省速率（F=372，D=1）

2．ME 只支持一种增强速率（F=512，D=8）如图 8 所示

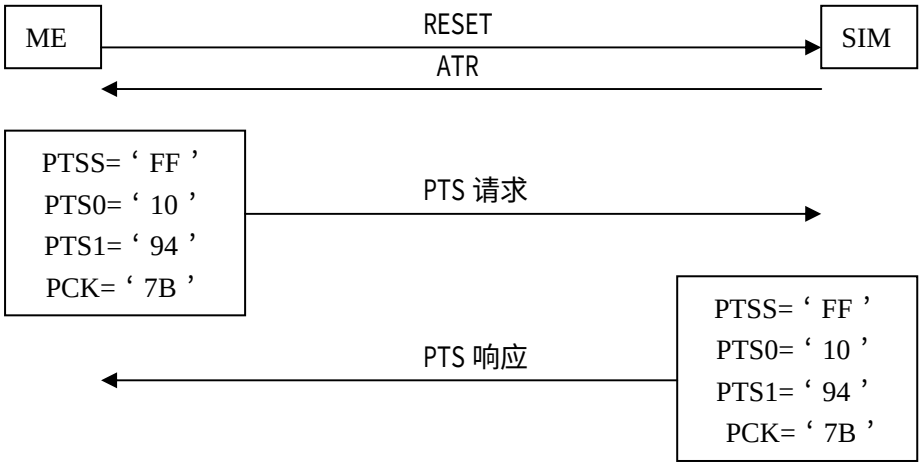


图 8 PTS 过程 ME 支持增强速率（F=512，D=8）

6．4 ME 向 SIM 卡发送的命令头标（T=0 字符协议）

命令总是由 ME 传向 SIM 卡，命令头标由 5 个连续的字节组成：

CLA	INS	P1	P2	P3

CLA：命令类别，取值为“ A0 ”，当 CLA=FF 时，为 PTS 过程的头标；

INS：指令代码；

P1，P2：指令附加参数；

P3：由 INS 的编码而定，或是表示命令中送给 IC 卡的数据长度，或是等待从 SIM 卡响应的最大数据长度。

6．5 过程字节（T=0 字符协议）

SIM 收到命令头标后，应该回送给 ME 一个过程字节。过程字节指示 ME 下一步必须采取的措施，如下表所示：

	过程字节	措施
1	INS	由 ME 传送命令字节,或准备接收 SIM 卡的响应数据
2	“60”	由 ME 提供附加等待时间
3	“9X”(状态字节 SW1)	ME 等待更进一步的状态字节 SW2

7 命令描述

7.1 应用协议数据单元(APDU)的信息结构

一个 APDU 可以是命令的 APDU，也可以是响应的 APDU

命令 APDU 格式：

CLA	INS	P1	P2	P3	DATA

参考 6.4 节

响应 APDU 格式：

DATA	SW1	SW2

SW1 和 SW2 指示命令执行的结果正确与否

以下五种 APDU 交换类型用于普通的 SIM 卡指令传输：

⑴无输入/无输出

CLA	INS	P1	P2	P3
				lgth（=00）

SW1	SW2
90	00

⑵无输入/有固定长度输出

CLA	INS	P1	P2	P3
				lgth

DATA with length lgth	SW1	SW2
	90	00

⑶无输入/有不定长度输出

CLA	INS	P1	P2	P3
				Lgth（=00）

SW1	SW2
9F	lgth1

CLA	INS	P1	P2	P3
GET RESPONSE				lgth2

DATA with length lgth2≤lgth1	SW1	SW2
	90	00

⑷有输入/无输出

CLA	INS	P1	P2	P3	DATA with length lgth
				lgth	

SW1	SW2
90	00

⑸有输入/有固定或不定长度输出

CLA	INS	P1	P2	P3	DATA with length lgth
				lgth	

SW1	SW2
9F	lgth1

CLA	INS	P1	P2	P3
GET RESPONSE				lgth2

DATA with length lgth2≤lgth1	SW1	SW2
	90	00

以上五种 APDU 交换类型也可以应用于 SIM 卡的主动式命令

⑴无输入/正确响应无输出，插入 SIM 卡的主动式命令

CLA	INS	P1	P2	P3
				lgth（=00）

SW1	SW2
91	lght

正常的 GSM 操作情况下，可能的命令响应对

CLA	INS	P1	P2	P3
FETCH				lgth1

DATA with length lgth1	SW1	SW2
	90	00

⑵无输入/正确响应有固定长度输出，插入 SIM 卡的主动式命令

CLA	INS	P1	P2	P3
				lgth

DATA with length lgth	SW1	SW2
	91	lgth1

正常的 GSM 操作情况下，可能的命令响应对

CLA	INS	P1	P2	P3
FETCH				lgth1

DATA with length lgth1	SW1	SW2
	90	00

⑶无输入/正确响应，有不定长度输出，插入 SIM 卡的主动式命令

CLA	INS	P1	P2	P3
				lgth（=00）

SW1	SW2
9F	lgth1

CLA	INS	P1	P2	P3
GET RESPONSE				lgth2

DATA with length lgth2≤lgth1	SW1	SW2
	91	lgth3

正常的 GSM 操作情况下，可能的命令响应对

CLA	INS	P1	P2	P3
FETCH				lgth3

DATA with length lgth3	SW1	SW2
	90	00

⑷有输入/正确响应，无输出，插入 SIM 卡的主动式命令

CLA	INS	P1	P2	P3	DATA with length lgth
				lgth	

SW1	SW2
91	lgth1

正常的 GSM 操作情况下，可能的命令响应对

CLA	INS	P1	P2	P3
FETCH				lgth1

DATA with length lgth1	SW1	SW2
	90	00

⑸有输入/有固定或不定长度输出

CLA	INS	P1	P2	P3	DATA with length lgth
				lgth	

SW1	SW2
9F	lgth1

CLA	INS	P1	P2	P3
GET RESPONSE				lgth2

DATA with length lgth2≤lgth1	SW1	SW2
	91	lgth3

正常的 GSM 操作情况下，可能的命令响应对

CLA	INS	P1	P2	P3
FETCH				lgth3

DATA with length lgth3	SW1	SW2
	90	00

7．2 命令编码

下表列出了 GSM 命令的编码：

命令	INS	P1	P2	P3	S/R
Select	‘A4’	‘00’	‘00’	‘02’	S/R
Status	‘F2’	‘00’	‘00’	长度	R
Read Binary	‘B0’	高偏移量	低偏移量	长度	R
Update Binary	‘D6’	高偏移量	低偏移量	长度	S
Read Record	‘B2’	记录号	方式	长度	R
Update Record	‘DC’	记录号	方式	长度	S
Seek	‘A2’	‘00’	类型/方式	长度	S/R
Increase	‘32’	‘00’	‘00’	‘03’	S/R
Verify CHV	‘20’	‘00’	CHV 号码	‘08’	S
Change CHV	‘24’	‘00’	CHV 号码	‘10’	S
Disable CHV	‘26’	‘00’	‘01’	‘08’	S
Enable CHV	‘28’	‘00’	‘01’	‘08’	S
Unblock CHV	‘2C’		‘00’/‘02’	‘10’	S
Invalidate	‘04’	‘00’	‘00’	‘00’	-
Rehabilitate	‘44’	‘00’	‘00’	‘00’	-
Run GSM Algorithm	‘88’	‘00’	‘00’	‘10’	S/R
Sleep	‘FA’	‘00’	‘00’	‘00’	-
Get Response	‘C0’	‘00’	‘00’	长度	R
Terminal Profile	‘10’	‘00’	‘00’	长度	S
Envelope	‘C2’	‘00’	‘00’	长度	S/R
Fetch	‘12’	‘00’	‘00’	长度	R
TerminalResponse	‘14’	‘00’	‘00’	长度	S

7．2．1 SELECT

——功能描述：此功能根据输入参数 FILE ID 在文件体系中按照合法路径选取相匹配的根目录、应用目录或数据文件，SELECT 指令是一种不受约束的指令。功能执行成功后，对于线性固定文件，无需设定记录指针；对于循环文件，记录指针指向最新执行过 UPDATE 或 INCREASE 功能的记录。

——使用条件与安全：

当选中根目录或根目录下的某个数据文件后，则可选择：

. 根目录下的任何应用目录

. 根目录下的任何数据文件

当选中现行应用目录或现行应用目录下的某个数据文件后，则可选择：

. 根目录下的另一应用目录

. 根目录

. 现行应用目录下的任何数据文件

注意：一旦某个目录或数据文件被选中，则可对其进行无限次数的操作，而无需进行重复多次选择，直到另一个目录或数据文件被选中为止。

——输入：文件标识符

——输出：

- 如果选择的是 MF 或者 DF：文件标识符，应用空间，CHV 激活/屏蔽，CHV 状态和其他的 GSM 特殊数据。
- 如果选择的是 EF：文件标识符，文件大小，进入条件，文件有效/无效指示，EF 文件的结构和记录长度

——命令描述：

命令	CLA	INS	P1	P2	P3
SELECT	A0	A4	00	00	02

命令参数/数据

字节	描述	长度
1-2	文件标识符	2

7．2．2 STATUS

——功能描述：此功能返回与当前文件目录（根目录或应用目录）的信息，此功能对 EF 文件不适用。

——使用条件与安全：这条命令可在任何时候使用，以获得与 GSM 应用有关的信息。

——输入：无

——输出：文件标识符，应用空间，CHV 激活/屏蔽，CHV 状态和其他的 GSM 特殊数据。

——命令描述：

命令	CLA	INS	P1	P2	P3
STATUS	A0	F2	00	00	lgth

响应的参数/数据同 SELECT 命令的响应数据相同

7．2．3 READ BINARY

——功能描述：此功能允许 SIM 卡从透明文件中读取字节串。

——使用条件与安全：如果不满足 EF 文件 READ 指令的访问准予条件，SIM 卡拒绝该功能。

——输入：相关字节串的地址和长度

——输出：字节串

——命令描述：

命令	CLA	INS	P1	P2	P3
READ BINARY	A0	B0	offset high	offset low	lgth

响应的参数/数据

字节	描述	长度
1-2	文件标识符	2

7．2．4 UPDATE BINARY

——功能描述：此功能更新透明文件的字节串。

——使用条件与安全：如果不满足 EF 文件 UPDATE 指令的访问准予条件，SIM 卡拒绝该该功能。

——输入：相关字节串的地址和长度；要写入的数据

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
UPDATE BINARY	A0	D6	offset high	offset low	lgth

命令参数/数据

字节	描述	长度
1-2	数据	lgth

7．2．5 READ RECORD

——功能描述：此功能读取线性固定文件或循环文件的记录。

——使用条件与安全：如果不满足 EF 文件 READ 指令的访问准予条件，SIM 卡拒绝该功能。若操作失败，记录指针不改变。

读记录定义了 4 种模式：

- **CURRENT** 模式：读当前的记录，记录指针不变
- **ABSOLUTE** 模式：读给定记录号的记录，记录指针不变
- **NEXT** 模式：功能执行前记录指针加一，然后读取指针指向的记录。
  若 EF 文件记录指针事先没有设定，此功能将读取该文件的首记录，同时将指针指向首记录。
  若记录指针指向线性固定文件的最后一条记录，NEXT 模式不再读取任何记录，同时不修改记录指针。
  若记录指针指向循环文件的最后一条记录，NEXT 模式将指针指向 EF 文件的首记录，同时读取此首记录。
- **PREVIOUS** 模式：功能执行前记录指针减一，然后读取指针指向的记录。
  若 EF 文件记录指针事先没有设定，此功能将读取该文件的最后一条记录，同时将指针指向最后一条记录。
  若记录指针指向线性固定文件的首记录，PREVIOUS 模式不再读取任何记录，时不修改记录指针。
  若记录指针指向循环文件的首记录，PREVIOUS 模式将指针指向 EF 文件的最后一条记录，同时读取最后一条记录。

——输入：模式、记录号（**ABSOLUTE** 模式）、记录长度

——输出：记录

——命令描述：

命令	CLA	INS	P1	P2	P3
READ RECORD	A0	B2	REC NO.	MODE	lgth

P2：读记录模式

—02：next record；

—03：previous record；

—04：absolute 模式/current 模式，在 current 模式下 P1=‘00’（记录号）

在 next，previous 模式下 P1 被置成‘00’。为兼容 phase1 的移动设备和 phase2 SIM 卡，SIM 卡将不解释移动设备发送来的 P1 值。

响应的参数/数据

字节	描述	长度
1-lgth	记录数据	lgth

7．2．6 UPDATE RECORD

——功能描述：向线性定长记录的 EF 文件或循环记录 EF 文件写入一条完整的记录。

——使用条件与安全：如果不满足 EF 文件 UPDATE 指令的访问准予条件，SIM 卡拒绝该功能。若操作失败，记录指针不改变。

写记录定义了 4 种模式：（循环文件仅适用 PREVIOUS 模式）

- **CURRENT 模式**：更新当前记录，记录指针不受影响。
- **ABSOLUTE 模式**：更新给定记录号的记录，记录指针不受影响。
- **NEXT 模式**：功能执行前记录指针加一，然后更新指针指向的记录。
  若 EF 文件记录指针事先没有设定，此功能将更新该文件的首记录，同时将指针指向首记录。
  若记录指针指向线性固定文件的最后一条记录，NEXT 模式不再更新任何记录，同时不修改记录指针。
- **PREVIOUS 模式**：对于线性固定文件，功能执行前记录指针减一，然后更新指针指向的记录。
  若线性固定文件记录指针事先没有设定，此功能将更新该文件的最后一条记录，同时将指针指向最后一条记录。若记录指针指向线性固定文件的首记录，PREVIOUS 模式不再更新任何记录，同时不修改记录指针。
  对于循环文件，更新最旧的记录，指针指向该记录，同时该记录的记录号设定为’1’。

——输入：模式、记录号（**ABSOLUTE** 模式）、记录长度、记录数据

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
UPDATE RECORD	A0	DC	REC NO.	MODE	lgth

P2：读记录模式

—02：next record；

—03：previous record；

—04：absolute 模式/current 模式，在 current 模式下 P1=‘ 00 ’（记录号）

在 next，previous 模式下 P1 被置成‘ 00 ’。为兼容 phase1 的移动设备和 phase2 SIM 卡，SIM 卡将不解释移动设备发送来的 P1 值。

命令参数/数据

字节	描述	长度
1-lgth	记录数据	lgth

7．2．7 SEEK

——功能描述：在线性固定文件中，此功能按照给定的关键字，查找起始部分与关键字相匹配的记录。

——使用条件与安全：

如果不满足EF文件READ指令的访问准予条件，SIM卡拒绝该功能。关键字长度在1～16字节范围内，且其长度不可超过每条记录长度。若查找成功，指针定位在此匹配的记录上；若查找不成功，SIM卡不改变指针的当前位置。

SEEK 命令定义了两种类型：

- **TYPE 1**：记录指针指向相匹配的记录，不返回数据。
- **TYPE 2**：记录指针指向相匹配的记录，返回该记录号。

SEEK 命令定义了四种查找模式：

- 从文件的开始部分开始向后查找
- 从文件的结尾部分开始向前查找
- 从定位的记录开始向下查找
- 从定位的记录开始向上查找

——输入：类型、模式、匹配的数据和匹配数据的长度

——输出：类型 1：无输出；类型 2：记录号

——命令描述：

命令	CLA	INS	P1	P2	P3
SEEK	A0	A2	00	Type/Mode	lgth

P2：查找的类型和模式

—X0：从文件的开始部分开始向后查找

—X1：从文件的结尾部分开始向前查找

—X2：从定位的记录开始向下查找

—X3：从定位的记录开始向上查找

‘ X ’ =0：类型 1；‘ X ’ =1：类型 2。

命令参数/数据

字节	描述	长度
1-lgth	匹配数据	lgth

响应的参数/数据（类型 2）

字节	描述	长度
1	记录号	1

7．2．8 INCREASE

——功能描述：此功能将 ME 给的数值与当前循环文件中经最新 INCREASE/UPDATE 操作的记录相加，结果存入最旧的记录，记录指针指向此记录，同时将此记录号置 1。

——使用条件与安全：

如果不满足 EF 文件 INCREASE 指令的访问准予条件，SIM 卡拒绝该功能。若相加结果超过每条记录的最大值（全’FF’），INCREASE 功能不执行。

——输入：被加的数值

——输出：被增加数值的记录和增加的数值。

——命令描述：

命令	CLA	INS	P1	P2	P3
INCREASE	A0	32	00	00	03

命令参数/数据

字节	描述	长度
1-3	增加的数值	3

响应的参数/数据（类型 2）

字节	描述	长度
1-X	被增加数值的记录	X
X+1-X+3	增加的数值	3

7．2．9 VERIFY CHV

——功能描述：此功能通过将 ME 传来的 CHV 与 SIM 卡中存储的 CHV 比较，对 CHV 进行校验。

——使用条件与安全：

功能执行的前提是：-CHV not disable；-CHV not blocked。在执行其他功能时，若被操作的文件访问准予条件是 CHV1 或 CHV2，执行该功能前需要先校验 CHV，除非 CHV 状态是 “ disable ”。

若 CHV 校验正确，此 CHV 校验重试次数复位为其初始值 3。

若 CHV 校验失败，此 CHV 校验重试次数减一。当校验失败出现 3 次，此 CHV 被锁住，访问准予条件不满足，除非对此 CHV 成功执行 UNBLOCK CHV 功能。

——输入：指示 CHV1/CHV2 参数，CHV 的值

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
VERIFY CHV	A0	20	00	CHV NO.	08

P2 指示 CHV 编号：

- ‘ 01 ’=CHV1；
- ‘ 02 ’=CHV2。

命令参数/数据

字节	描述	长度
1-8	CHV 的数值	8

7．2．10 CHANGE CHV

——功能描述：此功能给 CHV 赋新值。

——使用条件与安全：功能执行的前提是：-CHV not disable；-CHV not blocked。命令参数给出 CHV 的新值和旧值。

若旧值校验正确，此 CHV 校验重试次数复位为其初始值 3，同时 CHV 新值有效。

若旧值校验失败，此 CHV 校验重试次数减一，同时 CHV 保持旧值不变。当校验失败出现 3 次，此 CHV 被锁住，访问准予条件不满足，除非对此 CHV 成功执行 UNBLOCK CHV 功能。

——输入：指示 CHV1/CHV2 参数，旧的 CHV 值，新的 CHV 的值

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
CHANGE CHV	A0	24	00	CHV NO.	10

P2 指示 CHV 编号：

- ‘ 01 ’=CHV1；
- ‘ 02 ’=CHV2。

命令参数/数据

字节	描述	长度
1-8	旧 CHV 的数值	8
9-16	新 CHV 的数值	8

7．2．11 DISABLE CHV

——功能描述：此功能仅适用于 CHV1。功能执行成功后，使访问准予条件为 CHV1 的文件，其准予条件成为“ ALWAYS ”。

——使用条件与安全：功能执行的前提是：-CHV not disable；-CHV not blocked。

若 CHV1 校验正确，此 CHV1 校验重试次数复位为其初始值 3，同时 CHV1 状态成为“ disable ”。

若 CHV1 校验失败，此 CHV 校验重试次数减一，同时 CHV1 保持状态“ enable ”不变。当校验失败出现 3 次，此 CHV 被锁住，访问准予条件不满足，除非对此 CHV1 成功执行 UNBLOCK CHV 功能。

——输入：CHV1

——输出：无

——命令描述

命令	CLA	INS	P1	P2	P3
DISABLE CHV	A0	26	00	01	08

P2 指示 CHV1 编号。

命令参数/数据

字节	描述	长度
1-8	CHV1 的数值	8

7．2．12 ENABLE CHV

——功能描述：此功能仅适用于 CHV1，是 DISABLE CHV 功能的反向操作。

——使用条件与安全：功能执行的前提是：-CHV not enable；-CHV not blocked。

若 CHV1 校验正确，此 CHV1 校验重试次数复位为其初始值 3，同时 CHV1 状态成为“ enable ”。

若 CHV1 校验失败，此 CHV 校验重试次数减一，同时 CHV1 保持状态“ disable ”不变。当校验失败出现 3 次，此 CHV 被锁住，访问准予条件不满足，除非对此 CHV1 成功执行 UNBLOCK CHV 功能。

若 CHV1 的状态同时为“ blocked ”和“ disabled ”，访问准予条件为“ ALWAYS ”。

若 CHV1 的状态同时为“ blocked ”和“ enabled ”，访问准予条件不满足，除非对此 CHV1 成功执行 UNBLOCK CHV 功能。

——输入：CHV1 的数值

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
ENABLE CHV	A0	28	00	01	08

P2 指示 CHV1 编号。

命令参数/数据

字节	描述	长度
1-8	CHV1 的数值	8

7．2．13 UNBLOCK CHV

——功能描述：此功能对由于 3 次校验失败而被锁住的 CHV 进行解锁。

——使用条件与安全：

无论相关 CHV 的状态是否为 " blocked "，此功能都可执行。

若 UNBLOCK CHV 校验正确，命令参数中的 CHV 赋值给 SIM 卡中的 CHV。此 UNBLOCK CHV 校验重试次数复位为其初始值 10，相关的 CHV 校验重试次数复位为其初始值 3。功能执行成功后，CHV 状态为 " enabled "，相关的访问准予条件满足。

若 UNBLOCK CHV 校验失败，此 UNBLOCK CHV 校验重试次数减一。当校验失败出现 10 次，UNBLOCK CHV 被锁住。此时，错误的 UNBLOCK CHV 不影响 SIM 卡原来的 CHV 状态。

——输入：指示 CHV1/CHV2 参数，UNBLOCK CHV 值，新的 CHV 的值

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
UNBLOCK CHV	A0	2C	00	CHV NO.	10

P2 指示 CHV 编号：

- ' 00 ' =CHV1；
- ' 02 ' =CHV2。

命令参数/数据

字节	描述	长度
1-8	UNBLOCK CHV 的数值	8
9-16	新的 CHV 的数值	8

7．2．14 INVALIDATE

——功能描述：此功能使当前 EF 无效。指令执行成功后，此 EF 文件状态中的有关标志位要相应进行改变。

——使用条件与安全：功能执行的前提是被操作的 EF 文件需满足 INVALIDATE 指令的访问准予条件。

一个 " invalidated " 的文件，只能进行 SELECT 和 REHABILITATE 操作，其他指令不允许执行，除非此 EF 文件的状态指出可以执行 READ 和 UPDATE 指令。

——输入：无

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
INVALIDATE	A0	04	00	00	00

7．2．15 REHABILITATE

——功能描述：此功能使当前无效的 EF 恢复有效状态。指令执行成功后，此 EF 文件

状态中的有关标志位要相应进行改变。

——使用条件与安全：功能执行的前提是被操作的 EF 文件需满足 REHABILITATE 指令的访问准予条件。

——输入：无

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
REHABILITATE	A0	44	00	00	00

7．2．16 RUN GSM ALGORITHM

——功能描述：此功能用来起动 SIM 卡中的 GSM 算法 A3 和 A8。在该指令后需用 GET RESPONSE 命令，以输出 SRES/Kc 数据，这些输出数据与移动终端发出的 RAND 数据值相对应。如果其后执行的是其他命令，则数据 SRES/Kc 将会丢失。

——使用条件与安全：在执行该指令之前，必须先选择 GSM 目录作为当前目录。

——输入：随机数

——输出：SRES，KC

——命令描述：

命令	CLA	INS	P1	P2	P3
RUN GSM ALGORITHM	A0	88	00	00	10

命令参数/数据

字节	描述	长度
1-16	随机数	16

响应参数/数据

字节	描述	长度
1-4	SRES	4
5-12	KC	8

7．2．17 SLEEP

——功能描述：该命令只被 Phase1 的移动设备支持，对于 Phase2 或者以后的移动设备不会使用该命令。

——输入：无

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
SLEEP	A0	FA	00	00	00

7．2．18 GET RESPONSE

——功能描述：此功能用于返回 RUN GSM ALOGRITHM、SEEK、INCREASE 和 ENVELOP 等指令的响应数据。

——使用条件与安全：GET RESPONSE 要求直接跟在前一功能后面，在两条功能之间不能插入其他功能。由于在 SIM 卡激活时，根目录 MF 是隐含选中的目录，所以允许 GET RESPONSE 指令作为激活后的第 1 条指令。

——命令描述：

命令	CLA	INS	P1	P2	P3
GET RESPONSE	A0	C0	00	00	lgth

——响应参数/数据

字节	描述	长度
1-lgth	数据	lgth

7．2．19 TERMINAL PROFILE

——功能描述：由移动设备用来向 SIM 卡传送移动设备所支持的 SIM 卡应用工具箱的功能列表。详细解释见 STK 部分。

——输入：终端功能列表

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
TERMINAL PROFILE	A0	10	00	00	lgth

——命令参数/数据

字节	描述	长度
1-lgth	终端功能列表	lgth

7．2．20 ENVEOPE

——功能描述：向 SIM 卡的应用工具箱传递数据，详细解释见 STK 部分。

——输入：数据串

——输出：在 GSM11.14 中定义的数据格式的数据

——命令描述：

命令	CLA	INS	P1	P2	P3
ENVELOPE	A0	C2	00	00	lgth

——命令参数/数据：

长度为 lgth 的数据，数据格式符合 11.14 中定义的数据格式

——响应参数/数据：

GSM11.14 中定义的数据格式的数据。

7．2．21 FETCH

——功能描述：SIM 卡使用该命令向移动设备传递主动式命令，详细解释见 STK 部分。

——输入：无

——输出：在 GSM11.14 中定义的数据格式的数据

——命令描述：

命令	CLA	INS	P1	P2	P3
FETCH	A0	12	00	00	lgth

——响应参数/数据：

长度为 lgth 的数据，数据格式在 11.14 中定义

7．2．22 TERMINAL RESPONSE

——功能描述：移动设备使用此命令通知SIM卡主动式命令的执行结果，详细解释见

STK部分。

——输入：长度为lgth的数据，数据格式在11.14中定义

——输出：无

——命令描述：

命令	CLA	INS	P1	P2	P3
TERMINAL RESPONSE	A0	14	00	00	lgth

——命令参数/数据：

长度为 lgth 的数据，数据格式在 11.14 中定义

7．3 命令响应状态字

SIM卡用命令的响应状态字SW1、SW2通知移动设备命令执行的结果。

7．3．1正确执行命令的响应

SW1	SW2	描述
‘ 90 ’	‘ 00 ’	指令正常结束
‘ 91 ’	‘ XX ’	指令正常结束，并通知移动设备有主动命令作为附加信息，‘ XX ’为响应数据的长度
‘ 9E ’	‘ XX ’	SIM卡数据下载出错，响应数据的长度为‘ XX ’
‘ 9F ’	‘ XX ’	长度为‘ XX ’的响应数据

7．3．2 命令延时的响应

SW1	SW2	描述
‘ 93 ’	‘ 00 ’	SIM卡应用工具箱忙，当前命令不能执行，稍候可以尝试正常的指令

7．3．3 存储器管理

SW1	SW2	描述
‘ 92 ’	‘ 0X ’	命令正确执行，但是经过‘ X ’次重写之后才成功
‘ 92 ’	‘ 40 ’	存储器问题

7．3．4 索引管理

SW1	SW2	描述
‘ 94 ’	‘ 00 ’	没有EF文件被选中
‘ 94 ’	‘ 02 ’	地址超出范围
‘ 94 ’	‘ 04 ’	文件标识符没有找到 匹配字符没有找到
‘ 94 ’	‘ 08 ’	文件和命令矛盾

7．3．5 安全管理

SW1	SW2	描述
‘ 98 ’	‘ 02 ’	CHV没有初始化
‘ 98 ’	‘ 04 ’	进入条件不满足 CHV校验不成功，最少还有一次机会 UNBLOCK CHV 校验不成功，最少还有一次机会重试 验证出错（Phase1）
‘ 98 ’	‘ 08 ’	CHV的状态矛盾
‘ 98 ’	‘ 10 ’	与无效状态矛盾
‘ 98 ’	‘ 40 ’	CHV验证不成功，没有机会重试 UNBLOCK CHV 校验不成功，没有机会重试 CHV锁住 UNBLOCK CHV锁住
‘ 98 ’	‘ 50 ’	INCREASE 命令不能被执行，达到最大值

7．3．6 与应用无关的错误

SW1	SW2	描述
‘ 67 ’	‘ XX ’	P3参数错，‘ XX ’代表应有的数值
‘ 6B ’	‘ XX ’	P1或P2参数错
‘ 6D ’	‘ XX ’	命令中有未知的结构编码
‘ 6E ’	‘ XX ’	命令中有错误的命令类型
‘ 6F ’	‘ XX ’	不能给出原因的技术错误

7．3．7 命令与可能产生的状态字

下表列出了每条命令可能产生的状态字（SW1、SW2）

	OK				Busy	Mem Sta		Refer. Status				Security Status						Application Independent Errors				
命令	90 00	91 XX	9E XX	9F XX	93 00	92 0X	92 40	94 00	94 02	94 04	94 08	98 02	98 04	98 08	98 10	98 40	98 50	67 XX	6B XX	6D XX	6E XX	6F XX
Select				*			*			*								*	*		*	*
Status	*	*					*											*	*		*	*
Update Binary	*	*				*	*	*			*		*		*			*	*		*	*
Update Record	*	*				*	*	*	*		*		*		*			*	*		*	*
Read Binary	*	*					*	*			*		*		*			*	*		*	*
Read Record	*	*					*	*	*		*		*		*			*	*		*	*
Seek	*			*			*	*		*	*		*		*			*	*		*	*
Increase				*		*	*	*			*		*		*		*	*	*		*	*
Verify CHV	*	*				*	*					*	*	*		*		*	*		*	*
Change CHV	*	*				*	*					*	*	*		*		*	*		*	*
Disable CHV	*	*				*	*					*	*	*		*		*	*		*	*
Enable CHV	*	*				*	*					*	*	*		*		*	*		*	*
Unblock CHV	*	*				*	*					*	*	*		*		*	*		*	*
Invalidate	*	*				*	*	*					*		*			*	*		*	*
Rehabilitate	*	*				*	*	*					*		*			*	*		*	*
Run GSM Algorithm				*			*				*		*					*	*		*	*
Sleep	*																	*	*		*	*
Get Response	*	*					*											*	*		*	*
Terminal Profile	*	*				*	*											*	*		*	*
Envelope	*	*	*	*	*	*	*											*	*		*	*
Fetch	*						*											*	*		*	*
TerminalResponse	*	*				*	*											*	*		*	*

8 SIM 卡的逻辑模式

本章主要讨论 SIM 卡文件系统的逻辑结构。

8．1 概述

图 8.1 给出了 SIM 卡文件的逻辑结构，文件分层组织的结构形式,文件被定义为 1 或 3 种类型,文件可能是管理文件或者是应用文件。操作系统处理和访问不同文件中的数据。

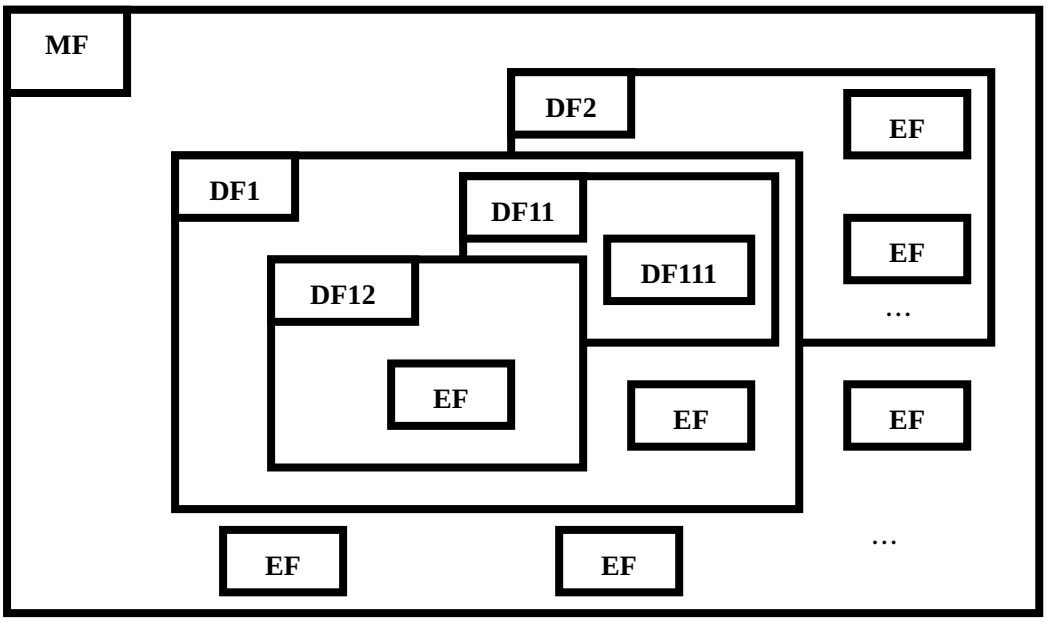


图 8.1 存储器组织结构

8．2 文件标识符

文件标识符通常用于寻址或者识别每种专有文件，文件标识符由两个 16 进制字节组成，第一个字节代表文件的类型，在 GSM 系统中：

——‘3F’：主文件；
——‘7F’：第一层专有文件；
——‘5F’：第二层专有文件；
——‘2F’：主文件下的专有文件；
——‘6F’：在第一层专有文件下的基本文件；
——‘4F’：在第二层专有文件下的基本文件。

文件标识符应该符合下列条件：

——文件标识符应该在相关文件建立时分配；
——同一个父目录下的两子文件不应该有相同的文件标识符；
——子文件和任何父文件，或直接或间接，不能有相同的文件标识符。

这样标识的文件每一个文件都被唯一标识。

8．3 专有文件

一个专有文件（DF）是一个具有许多文件的功能性分组，它由自身和所有在其上层结构中含有该专有文件的文件组成（即由 DF 和其完整子树组成）。DF 只由文件头组成，没有

文件体部分。

本规范定义了 2 种第一层的专有文件：

——DFGSM：包含 GSM 和 DCS1800 两种应用的专有文件；

——DFTELECOM：包含了电信服务的应用。

这两个专有文件都是主文件的直接子文件,并可共存于一个具有多功能应用的 SIM 卡中。

8．4 基本文件

一个基本文件（EF）由文件头和文件体组成，下列三种结构的基本文件被 GSM 系统应用

8．4．1 透明基本文件

透明结构的基本文件由一系列的字节组成。当需要对文件进行读写操作时，需要给出一个偏移量作为询址的参考，这个偏移量包括字节的起始位置和被读写字节的长度。透明文件的第一个字节的相对地址为‘0000’。透明文件的文件体总长度要在文件头中定义。

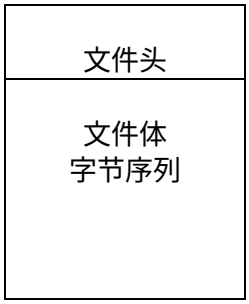


图 8.4.1 透明的 EF 文件

8．4．2 线性定长的基本文件

线性定长的基本文件由具有相同（固定）长度的记录组成。第一个记录的记录号为记录 1 号，如图所示。

一个线性定长的基本文件的总长度等于每个记录的长度与总记录数的乘积。

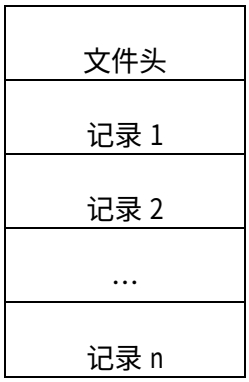


图 8.4.2 线性定长的基本文件

访问线性定长的 EF 文件的记录有下列 4 种方法:

——根据记录号访问

——当没有设置记录的指针时,则使用 NEXT 或者 PREVIOUS 的访问模式对第一个或者最后一个记录进行操作。

——当记录指针已经设置好了，则对于这个记录，上一个记录（除非记录指针设置在第一个记录上）和下一个记录（除非记录指针设置在最后一个记录上）均可进行操作。

——采用匹配字符查找一个记录：

——从文件的头部正向查找；

——从记录指针指向记录的下一个记录开始正向查找（除非记录指针设置在最后的记录上）；

——从文件的尾部开始反向查找；

——从记录指针指向记录的上一个记录开始反向查找（除非记录指针设置在第一个记录上）。

若选择记录的操作失败，则记录指针将保持原设置指针位置不变

注：

1. 线性定长的文件中，总记录数不能超过 255 个，记录长度不能大于 255 个字节
2. 这种结构的文件在 GSM 系统中被视为“ 已格式化 ”文件

8．4．3 循环结构的基本文件

循环文件按照时间顺序存储记录，当所有记录空间都存储了记录，则新记录的存储将覆盖最老的记录信息。

循环记录的基本文件由具有相同长度的记录组成，如图 8.4.3 组成。将最后一个记录链接到第一个记录，当记录指针指向最后一个记录 n 时，则下一个记录的号码就成为记录 1，反之当记录指针指向记录 1 时，则上一个记录为记录 n。最新更新的记录包含有最新数据的记录为记录 1，最老记录在记录 n 上。

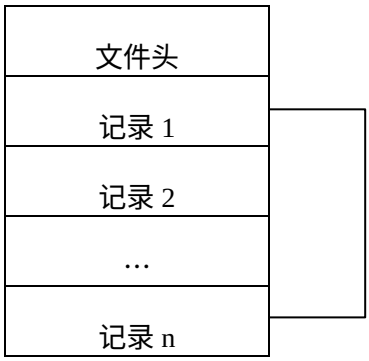


图 8.4.3 循环文件的结构

对于循环文件的更新操作仅有 PREVIOUS 模式被支持，当选择了循环文件之后，记录指针应该定位在最新更新或增加的记录处，若选择循环文件的操作失败，则记录指针将维持原位置不变。

注：循环文件中，总记录数不能超过 255 个，记录长度不能大于 255 个字节

8．5 选择文件的方法

在复位应答（ATR）之后主要文件（MF）被隐含选中，成为当前目录。然后，可采用符合下列原则的 SELECT 命令来选择每种文件：

——选择 DF 或 MF 作为当前的目录；

——选择一个 EF 文件作为当前的 EF 文件，当前的路径是被选中的 EF 文件的父目录（DF 或 MF）。

任何应用命令只有在但前路径下是合法的才是可操作的。

在选择了当前文件之后，下列文件是可以选择的：

——属于当前目录的直接子文件；

——属于当前目录文件（DF）的直接目录文件（DF）；
——当前目录的父目录
——当前的 DF 文件
——MF 文件

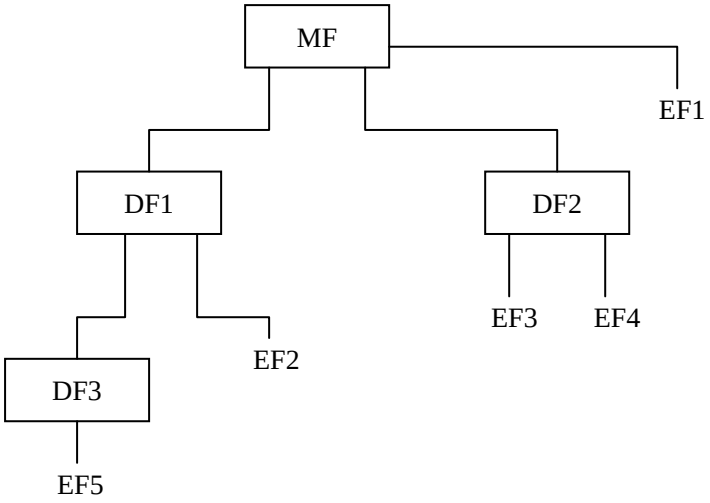


图 8.5 逻辑结构

下表给出了图 8.5 关于 GSM 逻辑结构的有效选择方式。并允许选择最近选择的文件，但是表中没有给出

最后选择的文件	有效的选择
MF	DF1、DF2、EF1
DF1	MF、DF2、DF3、EF2
DF2	MF、DF1、EF3、EF4
DF3	MF、DF1、EF5
EF1	MF、DF1、DF2
EF2	MF、DF1、DF2、DF3
EF3	MF、DF1、DF2、EF4
EF5	MF、DF1、DF3

表 8.5 文件选择方式

8．6 保留的文件标识符

在现有的标准中，下列的文件标识符被 GSM 系统保留了下来。

专用文件：

——管理应用：‘7F4X’、‘5F1X’、‘5F2X’；

——操作应用：‘7F10’（$DF_{TELECOM}$）、‘7F20’（DF_{GSM}）‘7F21’（$DF_{DCS1800}$）和‘7F2X’，其中：2≤X≤F。

基本文件：

——管理应用：‘6FXX’（在 DFS‘7F4X’中的），‘6F1X’（ 在 DFS‘7F10’,‘7F20’,‘7F21’中的），‘2F01’、‘2FEX’（在 MF‘3F00’中的）。

——操作应用：‘6F2X’,‘6F3X’,‘6F4X’（在‘7F10’,‘7F2X’中的），‘2F1X’（在 MF‘3F00’中的），其中 0≤X≤F。

9 安全特性

内容：

- 用户鉴权
- 在空中接口上的数据保密性
- 文件访问条件

9．1 鉴权方法及密钥生成过程

网络向 MS 发送一个随机数（RAND）。ME 采用 RUN GSM ALGORITHM 命令把 RAND 传送给 SIM 卡。SIM 卡采用下述算法和程序导出 SRES 和 KC 回送给 ME。然后 ME 将 SRES 向网络发送。网络侧用自己计算出的 SRES 进行比较，比较这些 SRES 值即为鉴权。ME 用 KC 值为网络的通信信息进行加密，直到下一次再进行鉴权。

在这个过程中，采用一个用户鉴权密钥 Ki。Ki 长度为 128bit，存储在 SIM 卡之中。

9．2 算法与过程

SIM 卡支持的算法的名称和参数，其中：

- 算法 A3 用于 MS 登记到网络时的鉴权。
- 算法 A8 用于产生密钥。

这些算法在 SIM 卡中可以单独存在或合并（变成 A38），在这两种情况下，SIM/ME 接口上的输出信号是 12 字节。向 A3 和 A8 或 A38 输入的信号为 Ki（128bit），以及 RAND（128bit）。其输出信号则是 SRES（32bit）/Kc（64bit）。

9．3 文件的访问条件

每个文件对于每个命令都有特定的访问条件。最近选择的文件的相关访问条件应该在请求的动作开始之前得到。

每个文件：

- READ 与 SEEK 命令的访问条件是相同的。
- SELECT 与 STATUS 命令的访问条件是无条件的（ALW）。
- MF 和 DFS 的访问条件待定。

下表给出定出访问条件的级别。

表 9.3 访问条件级别编码

级别	访问条件
0	ALW
1	CHV1
2	CHV2
3	保留
4-14	ADM
15	NEV

在上表中:

ALW：无条件执行；

CHV1：（卡持有者认证 1）：能够满足下列 3 种条件之一者，可执行动作：

- 在当前对话期间，一个正确的 CHV1 值已经提供给 SIM 卡；
- CHV1 使能/不使能指示器已处于“ 不使能 ”状态；
- 当前对话期间已经成功的执行了 UNBLOCK CHV1。

CHV2：（卡持有者认证 2）能满足下列两条件之一者，能够执行动作：

- 在当前对话期间，一个正确的 CHV2 值已经提供给 SIM 卡；
- 当前对话期间已经成功的执行了 UNBLOCK CHV2。

ADM：这些级别的安排和这些级别要完成的的要求都是管理权限的范围。
NEVER：在 SIM/ME 接口上，不能执行动作。SIM 卡可执行内部动作。
条件级别是不分层的。例如，当正确的 CHV2 出现，则免去执行 CHV1 请求的动作。只要相应的密码保持解锁状态即可，一个已达标的条件级别直到 GSM 对话结束为止都保持有效即可。达标的 CHV 条件的级别是适合于 DF_{GSM} 和 $DF_{TELECOM}$ 文件的。

通过对 STATUS 命令的响应，ME 决定 CHV2 是否可用，若 CHV2 没有初始化，则关于 CHV2 的命令（例如 VERIFY CHV2）将不能使用。

10 SIM 卡的文件结构

如前所述 SIM 卡中的文件结构分为目录文件（MF，DF）和基本文件（EF），其中基本文件分为‘文件头’和‘文件体’两部分，目录文件则只有文件头部分。

10．1SIM 卡中文件头的编码

表 10.1_1 中规定了目录文件（ME，DF）的文件头的编码，表 10.1_2 中规定了基本文件（EF）的文件头的编码：

表 10.1_1 目录文件文件头编码

字节	描述	长度
1-2	保留	2
3-4	在所选择的目录下面，所选择的目录的存储总量是不分配给 DF 或 EF 的。	2
5-6	文件标识符	2
7	文件类型（见 10.2 节）	1
8-12	保留	5
13	后面数据的长度	1
14	文件特性（见说明 1）	1
15	当前目录下的 DF 数量	1
16	当前目录下的 EF 数量	1
17	CHV，UNBLOCK CHV 的数量和管理编码	1
18	保留	1
19	CHV1 状态（见说明 2）	1
20	UNBLOCK CHV1 状态（见说明 2）	1
21	CHV2 状态（见说明 2）	1
22	UNBLOCK CHV2 状态（见说明 2）	1
23	保留	1
24-34	保留为内部管理数据（可选）	0≤长度≤11

注：

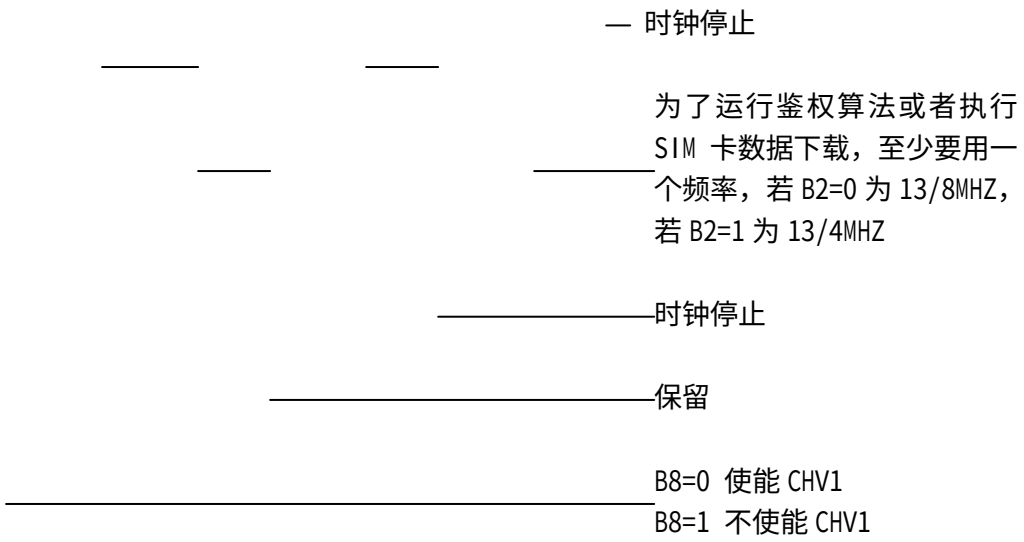
1．字节 35 以后为保留字节

2．MF，DF_{GSM}，$DF_{TELECOM}$ 的状态信息能提供一些相同的应用程序特定的数据，如 CHV 状态。在多种应用卡上 MF 将不包括任何应用程序的数据，这些数据可由终端从特定的应用目录中得到。

同样，检验 CHV 命令不应该在 MF 上实现，而在相关的应用目录中实现（例如 DF_{GSM}）

说明 1：文件特性

B8	B7	B6	B5	B4	B3	B2	B1



关于时钟停止的条件编码如下：

B1	B3	B4	
1	0	0	允许时钟停止，但没有优先级
1	1	0	允许时钟停止，有高优先级
1	0	1	允许时钟停止，有低优先级
0	0	0	不允许时钟停止
0	1	0	不允许时钟停止，除非在高优先级上
0	0	1	不允许时钟停止，除非在低优先级上

若 B1（列 1）编码为 1，则在高低优先级上均可停止时钟。在这种情况下 B3（列 2）和 B4（列 3）给出关于可以停止时钟的优先级（高或低）的信息。

若 B1（列 1）编码为 0，只有在列 2（B3=1，即在高优先级上停止时钟）或在列 3（B4=1，即在低优先级上停止时钟）上的必选条件得到满足时钟才能停止。若 3 个 bit 都是 0，则时钟不停止。

说明 2：密码的状态字节

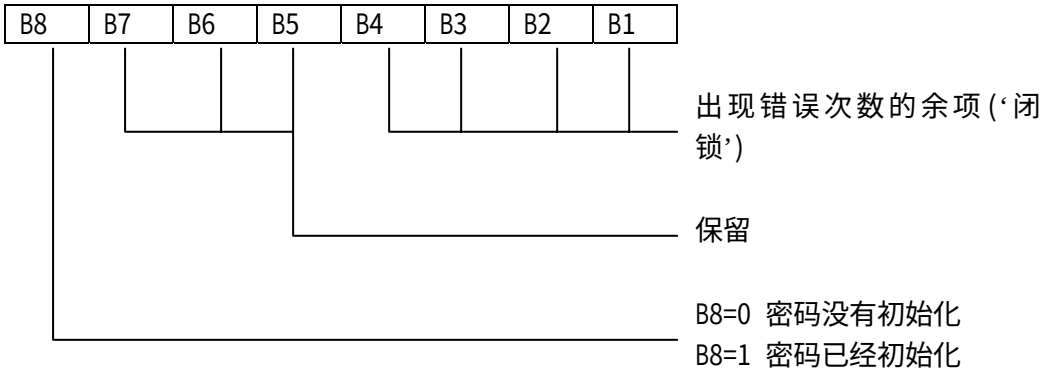


表 10.1_2 基本文件文件头编码

字节	描述	长度

1-2	保留	2
3-4	文件大小(透明 EF：文件主体长度；线性固定或循环的 EF：记录数×记录长度)	2
5-6	文件标识符	2
7	文件类型(见 10.2 节)	1
8	见说明 3	1
9-11	访问条件(见 10.2 节)	3
12	文件状态(见 10.2 节)	1
13	后面跟随数据的长度	1
14	EF 的结构	1
15	记录长度	1

注：字节 16 及以后的均为 RFU。

说明 3：字节 8

对于透明的和线性固定的 EF，该字节为保留字节。对于循环 EF，除 B7 外所有的 bit 都是保留的，B7=1 表示对于当前所选择的循环文件可以执行 INCREASE 命令。

10．2 定义和编码

在命令的响应参数/数据中用到的定义和编码：

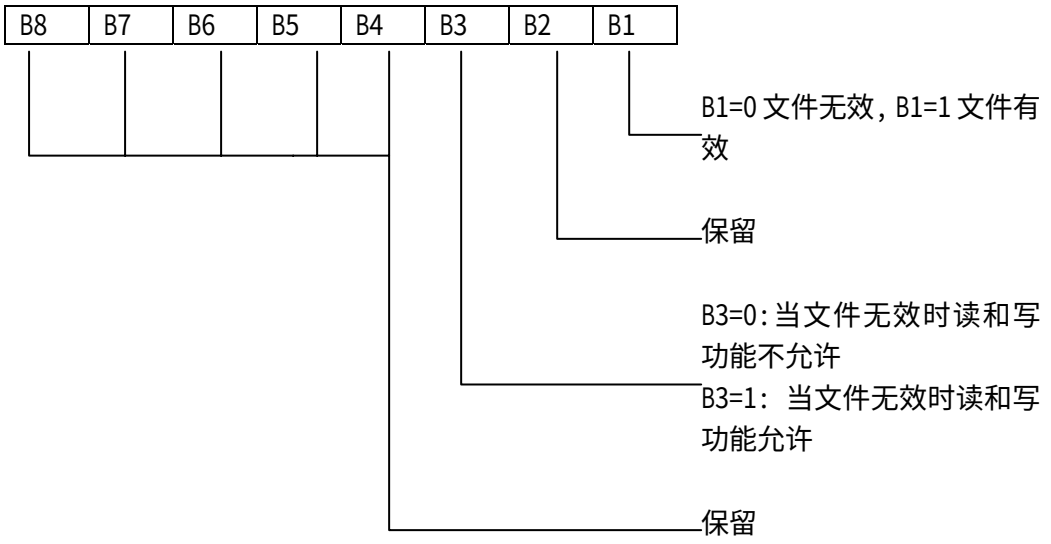
- 编码

每个字节均用 B8 到 B1 表示，B8 是最高有效位（MSB），B1 是最低有效位（LSB）。

- 为将来应用设置的保留字节

在 GSM 专用卡中所有的保留字节均设置为‘00’，而且保留位设置位 0。

- 文件状态



- 文件结构

‘00’：透明文件

‘01’：线性定长文件

‘03’：循环文件

- 文件类型：

‘00’：保留

‘01’：MF

‘02’：DF

‘04’：EF

- CHV 的编码和解锁 CHV

CHV 以 8 个字节编码，只采用（十进制）数字 0-9，最少位数为 4，若用户提供的位数低于 8 位，则 ME 向 SIM 卡发送 CHV 之前用‘FF’补足 8 位。

UNBLOCK CHV 的编码与 CHV 的编码是相同的。另外，其位数总为 8 位。

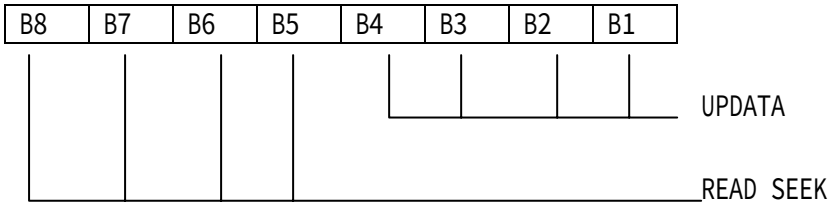
- 访问条件的编码方式

命令的访问条件在文件头的字节 9、10 和 11 上定义的。每一种访问条件以 4bit 进行编码，如表 10.2 所示

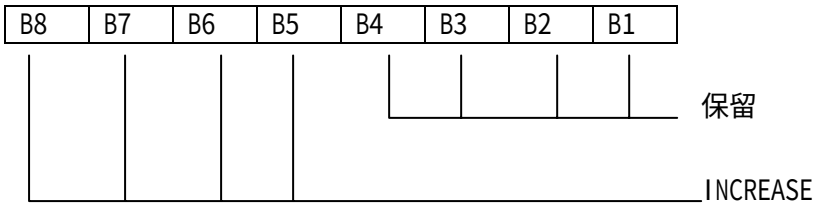
表 10.2 访问条件

ALW	‘0’
CHV1	‘1’
CHV2	‘2’
保留	‘3’
ADM	‘4’
…	…
ADM	‘E’
NEV	‘F’

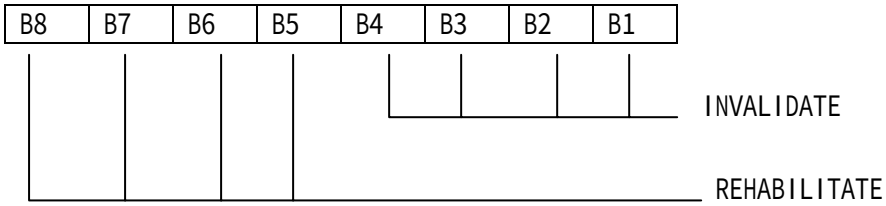
字节 9：



字节 10：



字节 11：



10．3 基本文件的内容

为定义访问条件、数据项和编码方式的 GSM 对话过程定义了基本文件（EF）。

数据项是 EF 的一部分，它代表一个完整的逻辑实体，例如，在一个 EFADN 记录中的 α 标识符。

无指配值得或在 GSM 对话期间被 ME 清除的 EF 或数据项应将其字节设为‘FF’。在管理阶段之后，所有的数据项应该有一个确定值或所有字节设为‘FF’。若数据项在 GSM 对话期间被删除，则采用‘FF’，而且不分配数据项。例如对于在 EFLOCI 中删除的 LAI，最后一个字节取值‘FE’。

EF 可分为必选（M）和可选（O）。可选的 EF 文件大小可为 0。所有文件大小大于 0 的已经实现的 EF 将包括全部的必选数据项。可选的数据项可用‘F’填满或当处于文件末尾时，可以不要可选的数据项存在。

当采用 CCITT 推荐的编码规则时，所有字节的 bit8 均设为 0。

图 10.3 列出了所有的 EF。

10．3．1 在 MF 层上的基本文件内容

在 MF 层上有两个 EF。

10．3．1．1 EF_{ICCID}（ICC 识别）

为 SIM 卡提供一个唯一的识别号。

文件标识符 ‘2FE2'	透明文件	必选	
文件容量 10 个字节		更新频率 低	
访问条件： READ ALW UPDATE NEVER INVALIDATE ADM REHABILITATE ADM			
字节	描述	M/O	长度
1~10	识别号码	M	10

- 识别号码

内容：

按照 CCITT 的推荐，SIM 卡的识别号长度为 20 位

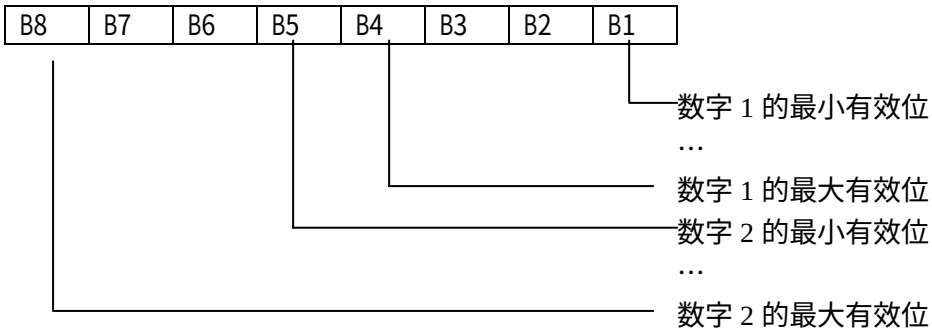
目的：

卡的识别号码

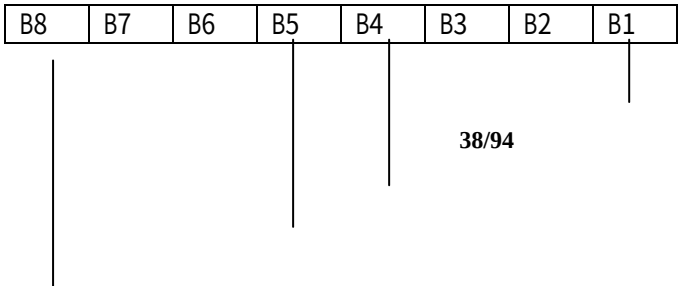
编码：

采用 BCD 编码，左对齐，并用‘F’填补空位。在填满一个字节之后，高半字节和低半字节交换，如下所示：

字节 1：



字节 2：



——数字 3 的最小有效位
…
——————————— 数字 3 的最大有效位
——————————————数字 4 的最小有效位
…
————————————————————————— 数字 4 的最大有效位

其它字节的编码同上。

10．3．1．2 EF_{ELP}（扩展语言选择）

该 EF 包括 n 种语言的编码

文件标识符 ‘2F05'	透明文件	可选
文件容量 2n 个字节	更新频率 低	
访问条件： READ ALW UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~2	第一种语言编码（高优先级）	O	2 字节
1~2	第二种语言编码	O	2 字节
2n-1~2n	第 n 种语言编码（低优先级）	O	2 字节

编码：

每种语言的编码采用一对 α 数字字符，每一个 α 数字字符采用默认的 7bit 编码，没有用到的语言编码被置为‘FF FF’。

10．3．2 GSM 应用层下的目录文件

为了兼容其他基于 GSM 交换平台的应用系统和特殊的 GSM 服务，目录文件应该作为 DF_{GSM} 的子目录。下面定义了这些子目录：

$DF_{IRIDIUM}$ '5F30'
$DF_{GLOBALSTAR}$ '5F31'
DF_{ICO} '5F32'
DF_{ACeS} '5F33'
DF_{MExE} '5F3C'
$DF_{EIA/TIA-553}$ '5F40'
DF_{CTS} '5F60'
DF_{SoLSA} '5F70'

本文主要讨论 GSM 目录下的 EF 文件，对上述的目录文件不再论述

10．3．3 GSM 应用层下的基本文件

在 DF_{GSM} 下的基本文件包含了与网络有关的信息

10．3．3．1 EF_{LP}（语言选择）

该 EF 包括 1 种或多种语言的编码。

文件标识符 ‘6F05'	透明文件	必选

文件容量 1~n 个字节		更新频率 低	
访问条件： READ ALW UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
字节	描述	M/O	长度
1	第一种语言编码（高优先级）	M	1 字节
2	第二种语言编码	M	1 字节
n	第 n 种语言编码（低优先级）	O	1 字节

编码：

每种语言的编码采用默认的 7bit 编码。

ME 用 GET-RESPONSE 命令可以得知该 EF 的文件大小。

10．3．3．2 EF_{IMSI} （国际移动用户识别符）

该 EF 包含了国际移动用户识别符（IMSI）

文件标识符 ‘6F07'	透明文件	必选	
文件容量 9 个字节		更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE CHV1			
字节	描述	M/O	长度
1	IMSI 的长度	M	1 字节
2~9	IMSI	M	8 字节

- IMSI 的长度

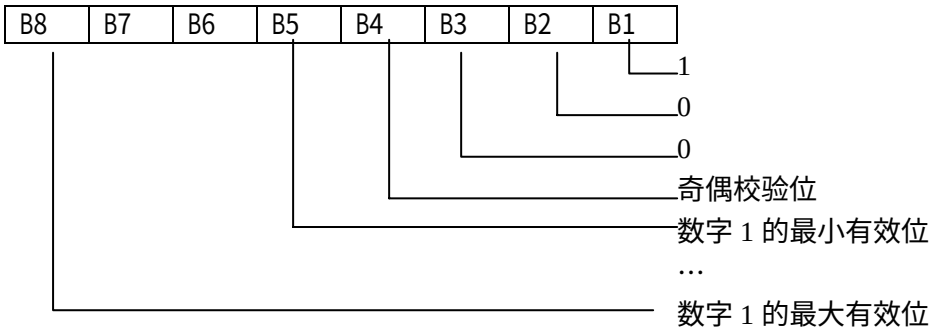
内容：长度的值定义了有意义的字节的数量，不包括长度字节本身。

- IMSI

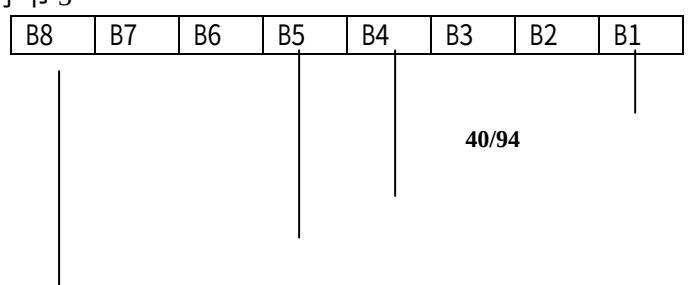
内容：国际移动用户识别符

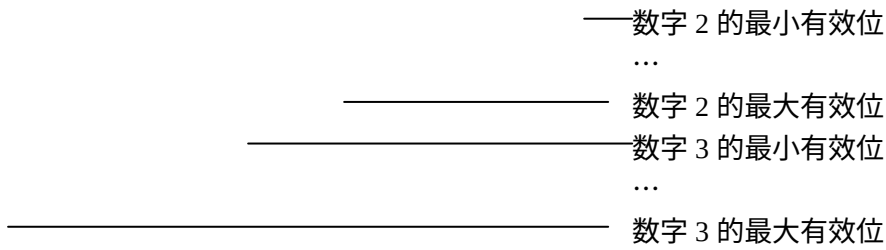
编码：信息单元的长度是可变值，若网络运营者选择了一个少于 15 位数字的 IMSI，则不用的半字节将被填充为‘F’。

字节 2：



字节 3





其它字节编码同字节 3

10．3．3．3 EF_{Kc} (计算密钥 Kc)

该 EF 包含了计算密钥 Kc 和计算密钥序列号 n。

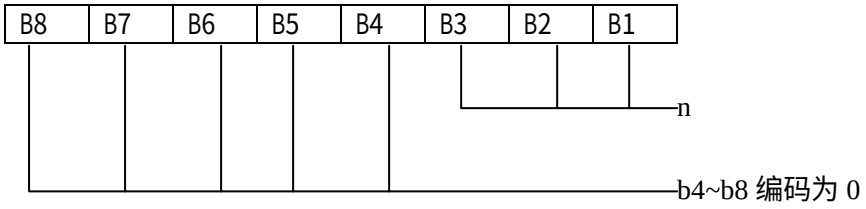
文件标识符 ‘6F20'	透明文件	必选
文件容量 9 个字节	更新频率 高	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~8	密钥 Kc	M	8 字节
9	密钥 Kc 序列号码 n	M	1 字节

- 计算密钥 Kc

编码：Kc 的最低有效位是第八字节的最低有效位，而最高有效位是第一字节的最高有效位。

- 密钥 Kc 序列号码 n



注：n=‘111’被注释为“密钥不可用”。因此，在管理阶段提供的初始值为‘07’，而不是‘FF’。

10．3．3．4 $EF_{PLMNsel}$ （公用陆地移动网选择器）

该 EF 包含了 n 种公用陆地移动网（PLMN）的编码，n 的最小值为 8。

文件标识符 ‘6F30'	透明文件	可选
文件容量 3n 个字节（n≥8）	更新频率 低	
访问条件：		

READ	CHV1		
UPDATE	CHV1		
INVALIDATE	ADM		
REHABILITATE	ADM		
字节	描述	M/O	长度
1~3	第一个 PLMN	M	3 字节
22~24	第八个 PLMN	M	3 字节
25~27	第九个 PLMN	O	3 字节
(3n-2) ~3n	第 n 个 PLMN	O	3 字节

- PLMN

内容：移动国家编码（MCC）后面跟着移动网号（MNC）

编码：

若要求存储的信息少于最大可能的数目 n 时，则超出的字节设置为‘ FF ’。

10．3．3．5 EF_{HPLMN} (母网搜索周期)

该 EF 包含了两次搜索母网的时间间隔。

文件标识符 ‘ 6F31'	透明文件	必选
文件容量 1 个字节	更新频率 低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	
字节	描述	M/O 长度
1	时间间隔	M 1 字节

- 时间间隔：

内容：两次搜索母网的时间间隔。

编码：

‘ 00 ’：不搜索母网

‘ 01 ’：n 分钟

‘ 02 ’：2n 分钟

…

‘ YZ ’：(16Y+Z) n 分钟，(最大值)

所有其它的值都被 ME 默认为缺省值。

n 的取值为 6，即搜索母网的时间间隔取值从 6 分钟到 8 小时，缺省值为 30 分钟。

10．3．3．6 EF_{ACMmax} (累积呼叫表的最大值)

该 EF 包含了累积呼叫表的最大值。

文件标识符 ‘ 6F37'	透明文件	可选
文件容量 3 个字节	更新频率 低	
访问条件：		

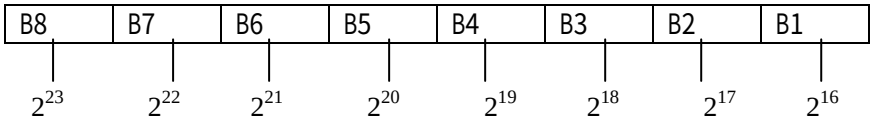
READ CHV1 UPDATE CHV1/CHV2 INVALIDATE ADM REHABILITATE ADM			
字节	描述	M/O	长度
1~3	最大值	M	3 字节

- 最大值

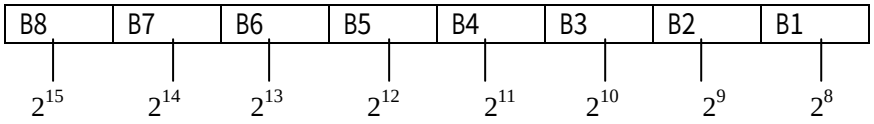
内容：累积呼叫表（ACM）的最大值

编码：

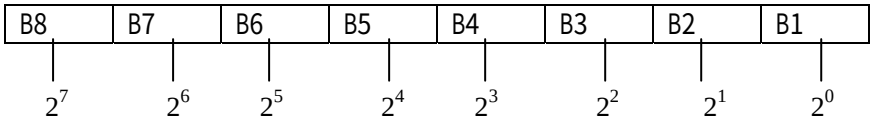
第一字节：



第二字节：



第三字节：



例如：‘ 00 ’‘ 00 ’‘ 30 ’描述为 $2^5 + 2^4$

全部的 ACM 数据存在 SIM 卡中，在 SIM/ME 接口上是以二进制进行传输。

若以‘ 000000 ’编码，则 ACM_{MAX} 无效。

10．3．3．7 EF_{SST} (SIM 卡服务列表)

该 EF 文件指示出 SIM 卡提供的服务种类，在 SIM 卡没有配置或没有激活的业务 ME 不能选择。

文件标识符 ‘ 6F38'	透明文件	必选
文件容量 X 个字节 X≥2	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1	业务 NO.1~ NO.4	M	1 字节
2	业务 NO.5~ NO.8	M	1 字节
3	业务 NO.9~ NO.12	O	1 字节
4	业务 NO.13~ NO.16	O	1 字节
5	业务 NO.17~ NO.20	O	1 字节
6	业务 NO.21~ NO.24	O	1 字节
7	业务 NO.25~ NO.28	O	1 字节
8	业务 NO.29~ NO.32	O	1 字节
…	…	…	1 字节
X	业务 NO.（4X-3）~ NO.4X	O	1 字节

- 业务：

内容：

业务 NO.1： CHV1 码屏蔽

业务 NO.2： 缩位拨号（ADN）
业务 NO.3： 固定拨号
业务 NO.4： 短信息存储
业务 NO.5： 付费通知
业务 NO.6： 能力配置
业务 NO.7： 网络选择
业务 NO.8： 保留
业务 NO.9： 国际综合业务网号码
业务 NO.10： 扩展 1
业务 NO.11： 扩展 2
业务 NO.12： 短信息参数
业务 NO.13： 最后拨号
业务 NO.14： 小区广播识别
业务 NO.15： 分组识别 1
业务 NO.16： 分组识别 2
业务 NO.17： 服务提供商名称
业务 NO.18： 服务电话
业务 NO.19： 扩展 3
业务 NO.20： 保留
业务 NO.21： VGCS 分组识别列表
业务 NO.22： VBS 分组识别列表
业务 NO.23： enhanced Multi-Level Precedence and Pre-emption Service
业务 NO.24： ？eMLPP 自动回答
业务 NO.25： 通过小区广播短消息下载数据
业务 NO.26： 通过点到点短消息下载数据
业务 NO.27： 菜单选择
业务 NO.28： 呼叫控制
业务 NO.29： 主动 SIM 卡
业务 NO.30： 小区广播标识符归类
业务 NO.31： 禁止拨号（BDN）
业务 NO.32： 扩展 4
业务 NO.33： 解网络个人化控制密钥
业务 NO.34： 互操作网络表
业务 NO.35： 短信息状态报告
业务 NO.36： 基站网络示警
业务 NO.37： Mobile Originated Short Message control by SIM
业务 NO.38： 分组交换（GPRS）
业务 NO.39： 图像(IMG)
业务 NO.40： 本地业务的支持（SoLSA）
业务 NO.41： 呼叫控制中的非结构化补充业务数据（USSD）
业务 NO.42： RUN AT COMMAND 命令
业务 NO.43： PLMN Selector List with Access Technology
业务 NO.44： OPLMN Selector List with Access Technology
业务 NO.45： HPLMN Access Technology

业务 NO.46： CPBCCH 信息
业务 NO.47： 调查浏览 Investigation Scan
业务 NO.48： 扩展性能配置参数
业务 NO.49： 移动基站应用执行环境（MexE）

对于第二阶段的 SIM 卡，其 EF 中至少要包括相当于第一阶段的业务字节（2 个字节），还可以增加更多的字节。但是，若该 EF 中包括了可选的字节，则该 EF 必须包含该字节之前的所有其它字节。这样，将来其它业务可利用以后的字节进行编码。

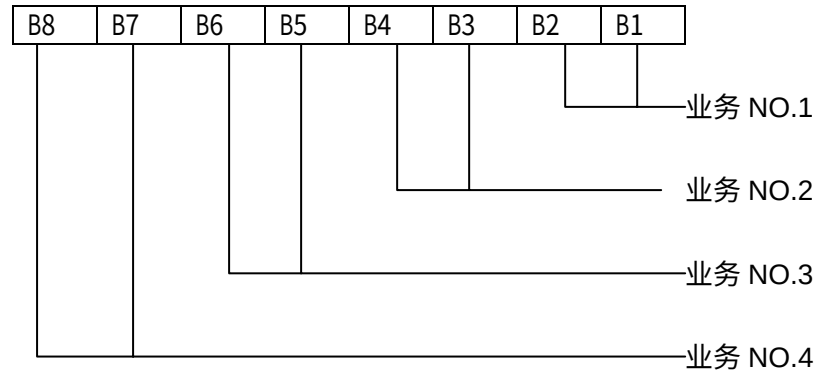
注：

1. 业务 NO.8 在第一阶段中已被分配做被叫用户子地址，因此，为了防止不兼容性，NO.8 的业务不再重新分配。
2. BDN 的业务依赖于呼叫控制特性，只有已经配置并激活业务 NO.28（呼叫控制），BDN 业务才能配置和激活。

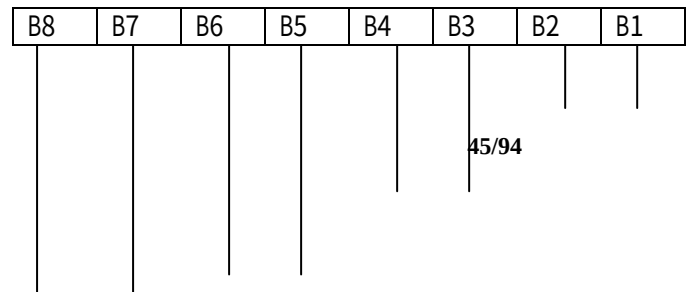
编码：
采用 2 个 bit 对每种业务进行编码：
第一个 bit=1：业务已经配置
第一个 bit=0：业务没有配置
第一个 bit 是 b1，b3，b5 和 b7
第二个 bit=1：业务已经激活
第二个 bit=0：业务没有激活
第二个 bit 是 b2，b4，b6 和 b8
已经配置的业务意味着 SIM 卡有支持该业务的能力。已经激活的业务意味着 SIM 卡用户可以获得该项服务。
编码情况如下：

第二比特	第一比特	描述
1	0	未配置业务（第二比特无意义）
0	0	未配置业务（第二比特无意义）
0	1	业务已配置，但未激活
1	1	业务已配置并已激活

第一个字节：



第二个字节：



————业务 NO.5

———————— 业务 NO.6

————————————业务 NO.7

————————————————————业务 NO.8

以后字节编码同上。

下面的例子是第一个字节中 NO.1 号业务“ CHV1 不使能 ”的编码，虽被配置但未激活：

B8	B7	B6	B5	B4	B3	B2	B1
X	X	X	X	X	X	0	1

若 SIM 卡支持 FDN 特性（已配置和激活 FDN），则 SIM 卡应用一种特定的机制在每次 GSM 对话中使 EF_{IMSI} 和 EF_{LOCI} 失效一次。若 FDN 已使能，则 SIM 卡自动激活该机制。这种失效方式至少在选择任何一个 EF 之后，下一次命令来到之前发生。当失效或未激活 ADN 时，则使能 FDN。

若 SIM 卡提供 BDN 功能（已配置和已激活 BDN），则在 SIM 卡中存在一个特殊的机制。即在每个 GSM 对话中，使 EF_{IMSI} 和 EF_{LOCI} 失效一次并禁止 REHABILTATE 命令对已失效的 EF_{IMSI} 和 EF_{LOCI} 的恢复，直至执行了 PROFILE DOWNLOAD 程序表示 ME 支持“ SIM 卡控制呼叫 ”业务。若 BDN 功能使能，则由 SIM 卡自动提供上述机制。而且，失效 EF_{IMSI} 和 EF_{LOCI} 文件应在选择了任何一个文件之后，在下一个命令到来之前发生。当 EFBDN 未失效时，可使用 BDN 功能。

10．3．3．8 EF_{ACM} (呼叫累积表)

该文件包含了当前的呼叫和以前的呼叫的单位总和

注：这种信息为用户提供计费通知，可作为计算呼叫费用的基础。

文件标识符 ‘ 6F39'	循环文件	可选
记录长度 3 个字节	更新频率 高	

访问条件：

READ	CHV1
UPDATE	CHV1/CHV2
INCREASE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

字节	描述	M/O	长度
1~3	单位的累加计算	M	3 字节

- 单位的累加计算

内容：ACM 的值

编码：详见 EF_{ACMmax} 的编码。

10．3．3．9 EF_{GID1} (1 级组识别符文件)

该 EF 包含特定的 SIM-ME 组合的标识符。可以识别一组特定的 SIM 卡。

文件标识符 ‘ 6F3E'	透明文件	可选
文件容量 1~n 个字节	更新频率 低	

访问条件：			
READ	CHV1		
UPDATE	ADM		
INVALIDATE	ADM		
REHABILITATE	ADM		
字节	描述	M/O	长度
1~n	SIM 卡的组识别符	O	n 字节

10．3．3．10 EF_{GID2} (2 级组识别符文件)

该 EF 包含特定的 SIM-ME 组合的标识符。可以识别一组特定的 SIM 卡。

文件标识符 ‘ 6F3F'	透明文件	可选
文件容量 1~n 个字节	更新频率 低	
访问条件：		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	
字节	描述	M/O 长度
1~n	SIM 卡的组识别符	O n 字节

注：EF_{GID1} 和 EF_{GID2} 的结构相同，允许网络运营者根据应用来确定安全的不同级别。

10．3．3．11 EF_{SPN} (网络运营商的名称)

该 EF 包含了网络运营商的名称和 ME 显示的相应要求。

文件标识符 ‘ 6F46'	透明文件	可选
文件容量 17 个字节	更新频率 低	
访问条件：		
READ	ALW	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	
字节	描述	M/O 长度
1	显示条件	M 1 字节
2~17	网络运营商名称	M 16 字节

- 显示条件

内容：根据登记的 PLMN，网络运营商的显示条件。

编码：

b1=0：不要求显示已登记的 PLMN

b1=1：要求显示已登记的 PLMN

- 网络运营商名称

内容：要显示的网络运营商字符串

编码：字符串采用 b8=0 的 7bit 编码方式，左对齐，不用的字节设置为 ‘ FF ’。同时支持 UCS-2 编码方式。

10．3．3．12 EF_{PUCT} (呼叫单位价格和货币表)

该 EF 包含了每个呼叫单位的价格和货币表（PUCT）。PUCT 是与计费通知有关的信息，ME 用这个信息结合 EFACM，以用户选择的货币来计算呼叫费用。

文件标识符 ‘ 6F41'	透明文件	可选

文件容量 5 个字节		更新频率 低	
访问条件： READ ALW UPDATE CHV1/CHV2 INVALIDATE ADM REHABILITATE ADM			
字节	描述	M/O	长度
1~3	货币编码	M	3 字节
4~5	单价	M	2 字节

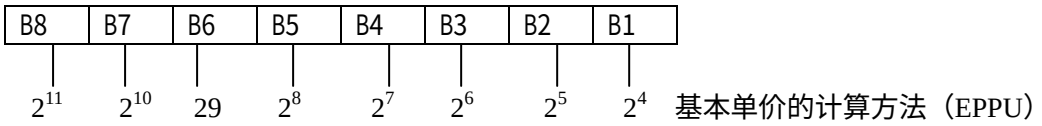
货币编码：

- 内容：货币码的α识别符
- 编码：字节 1、2、3 分别为α识别符的第一、第二、第三个字符。α识别符的缺省值采用 7bit 的编码方式，bit8 置为 0。

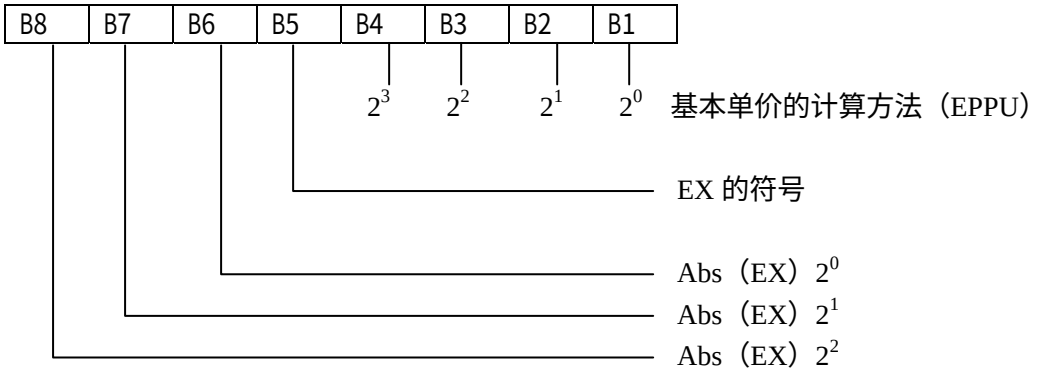
每呼叫单位价格：

- 内容：以 1~3 字节编码的货币来表示单价。
- 编码：字节 4 和字节 5 的 b1~b4 表示当前已编码的 1~3 字节中的货币基本单价（EPPU）。而字节 5 的 b5~b8 表示乘法因子的十进制对数（EX）的绝对值和 EX 符号的编码：0 代表正号；1 代表负号。

字节 4：



字节 5：



这个单价由 ME 提供的下列公式计算：

$$单价=EPPU*10^{EX}$$

10．3．3．13 EF_{CBMI} (小区广播信息标识符选择)

该 EF 包括消息识别符参数，本参数规定了用户喜欢 MS 采纳的小区广播消息内容的类型

在 SIM 卡中已经存储了小区广播信息标识符参数的任何号码，没有优先级可应用。

文件标识符 ‘6F45'	透明文件	可选
文件容量 2n 个字节		更新频率 低
访问条件：		

READ	ALW		
UPDATE	CHV1		
INVALIDATE	ADM		
REHABILITATE	ADM		
字节	描述	M/O	长度
1~2	小区广播信息标识符 1	O	2 字节
3~4	小区广播信息标识符 2	O	2 字节
…			
（2n-1）~2n	小区广播信息标识符 n	O	2 字节

- 小区广播信息标识符
  编码：已列出的数值表示将被 MS 接受的消息类型。没有被采用的输入号码设置为‘FFFF’

10．3．3．14 EF_{BCCH} (广播控制信道)

该 EF 包含了涉及到 BCCH 的相关信息。由于 BCCH 的存储，在选择小区时，MS 可以缩小对 BCCH 载波的搜索范围。BCCH 仅存储系统信息 2 消息，而不存储 2bis 扩展消息。

文件标识符 ‘6F74'	透明文件	必选	
文件容量 16 个字节		更新频率 高	
访问条件：			
READ	CHV1		
UPDATE	CHV1		
INVALIDATE	ADM		
REHABILITATE	ADM		
字节	描述	M/O	长度
1~16	BCCH 信息	M	16 字节

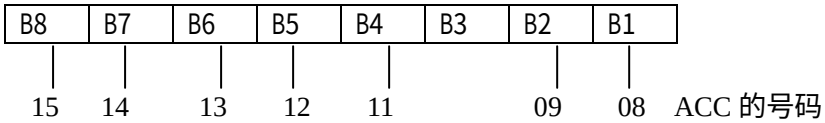
10．3．3．15 EF_{ACC} (访问控制级别)

该 EF 包含了已经分配了的访问控制级别，访问控制级别是控制 RACH 运行的一个参数。15 个等级中的 10 个随机分配给一般的用户，5 个分配给高优先级的用户。

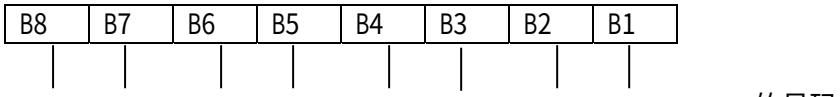
文件标识符 ‘6F78'	透明文件	必选	
文件容量 2 个字节		更新频率 高	
访问条件：			
READ	CHV1		
UPDATE	ADM		
INVALIDATE	ADM		
REHABILITATE	ADM		
字节	描述	M/O	长度
1~2	访问控制级别	M	2 字节

- 访问控制级别
  编码：每个 ACC 占用一个 bit 编码。bit=1：ACC 已分配；bit=0：ACC 未分配。第一个字节的 bit3=0。

第一字节：



第二字节：



10．3．3．16 EF_{FPLMN} (禁用的 PLMN)

该 EF 包括 4 个禁用的 PLMN 编码。是 SIM 卡初始化的一部分，由 ME 读出，指明 MS 不能自动接入 PLMN。若网络由于“ PLMN 不允许 ”，拒绝位置更新，则这个 PLMN 被写入到该 EF 文件中，ME 将按照下面所列的方法管理的 PLMN：

当 EF 中已有 4 个禁用的 PLMN 时，此时 ME 又从网络收到一个“ PLMN 不允许 ”，ME 将用更新命令修改基本文件。这个新的 PLMN 将被存储在第四个位置上，使现有的表格移位使原先在第一个位置上的内容丢失。

当 EF 中存有少于 4 个 FPLMN 时，则存储一个另外的 FPLMN 不会引起任何已存的 FPLMN 丢失。

通常依靠程序来存储和删除 EF 文件中的 FPLMN，当 EF 文件中存储的 PLMN 少于 4 个时，则‘ FFFFFF ’出现在任何位置都是可能的，ME 应该分析 EF 文件中所有位置上的 FPLMN，而不会将‘ FFFFFF ’作为有效的终止数据。

文件标识符 ‘ 6F7B'	透明文件	必选	
文件容量 12 个字节		更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
字节	描述	M/O	长度
1~3	PLMN1	M	3 字节
4~6	PLMN2	M	3 字节
7~9	PLMN3	M	3 字节
10~12	PLMN4	M	3 字节

- PLMN
  内容：移动国家码（MCC）后跟随移动网号（MNC）。

10．3．3．17 EF_{LOCI} (位置信息)

该EF文件包含下列位置信息：

- 临时移动用户识别符（MNC）
- 位置区信息（LAI）；
- TMSI时长；
- 位置更新状态。

文件标识符 ‘ 6F7E'	透明文件	必选
文件容量 11 个字节	更新频率 高	
访问条件： READ CHV1 UPDATE CHV1		

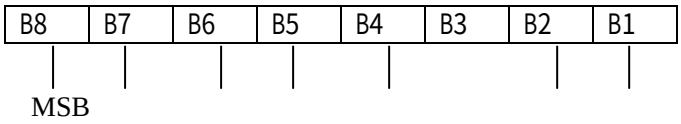
INVALIDATE REHABILITATE	ADM CHV1		
字节	描述	M/O	长度
1~4	TMSI	M	4 字节
5~9	LAI	M	5 字节
10	TMSI 时长	M	3 字节
11	位置更新状态	M	3 字节

- TMSI

  内容：TMSI

  编码：

  TMSI 的第一字节：

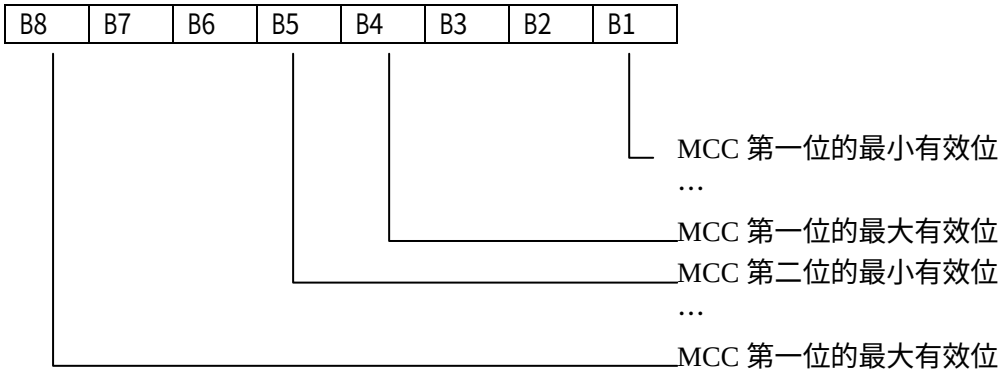


- LAI

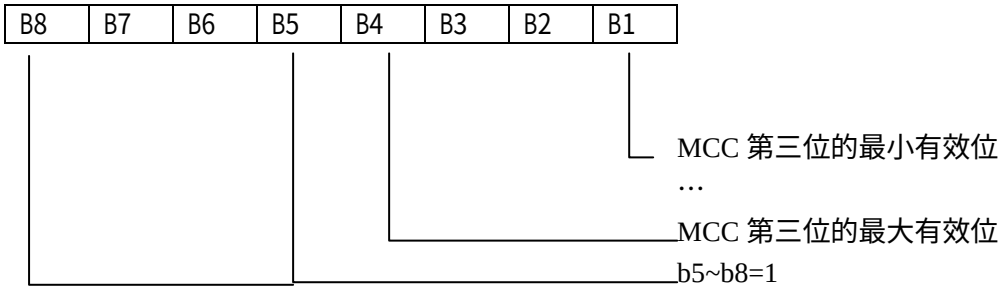
  内容：LAI

  编码：

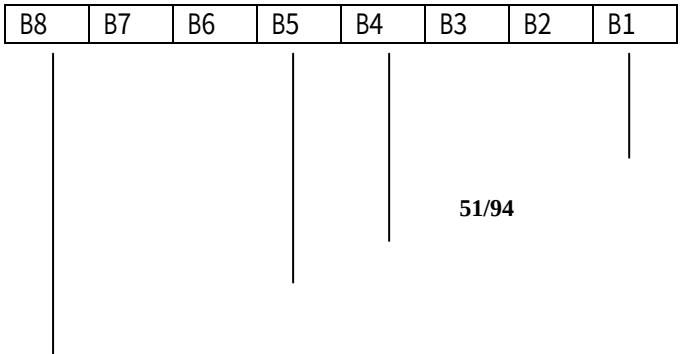
  LAI 的第一字节（MCC）：



  LAI 的第二字节（MCC）：



  LAI 的第三字节（MNC）：



MNC 第一位的最小有效位
…
MNC 第一位的最大有效位
MNC 第二位的最小有效位
…
MNC 第一位的最大有效位

LAI 的第四、五字节同上

- TMSI 时长

内容：周期性位置更新定时器（T3212）的当前值。次字节只用于PHASE1的ME，PHASE2的ME已经不用。

- 位置更新状态

内容：位置更新状态

编码：

字节11：

bit b3 b2 b1

0 0 0 ：已更新
0 0 1 ：未更新
0 1 0 ：禁用PLMN
0 1 1 ：不允许的位置区
1 1 1 ：保留

bit4~bit8 ：保留

10．3．3．18 EF_{AD} (管理数据)

该EF包括有关SIM卡操作模式的信息。例如：常规模式（PLMN用户用于GSM网络操作），型号认证模式（允许ME在无线设备的认证期间的特殊应用）；小区测试模式（在小区商用之前，进行小区测试），制造商特定模式（允许ME制造商在维护阶段进行特定的性能自动测试）。

在常规操作期间，如果ME的某些特性没有被激活，也必须给出指示。

文件标识符 ‘6FAD'	透明文件	必选
文件容量 3+X 个字节	更新频率 低	
访问条件： READ ALW UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1	MS 操作模式	M	1 字节
2~3	附加信息	M	2 字节
4	IMSI 中的 MNC 长度	O	1 字节
5~（4+X）	保留	O	X 字节

- MS 的操作方式

内容：MS 的操作方式。

编码：初始值

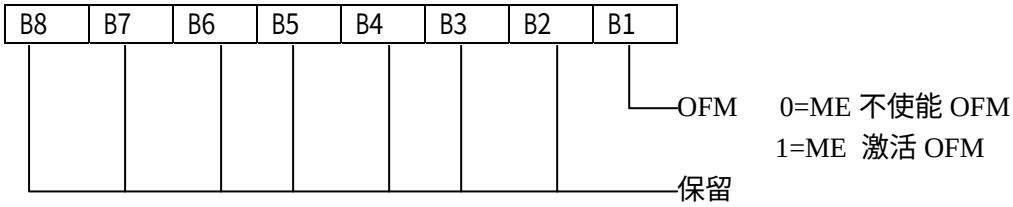
- 正常操作：‘ 00 ’

- 型号认证操作：‘ 80 ’
- 标准操作+特殊设备：‘ 01 ’
- 型号认证操作+特殊设备‘ 81 ’
- 维护（脱机）‘ 02 ’
- 小区测试操作‘ 04 ’

- 附加信息

  编码：

  - 特殊的设备号码（如果第一个字节中的 b1=1）
  - 字节 2（附加信息中的第一个字节）：保留
  - 字节 3（附加信息中的第二个字节）



注：OFM 为附加信息的一种信息。

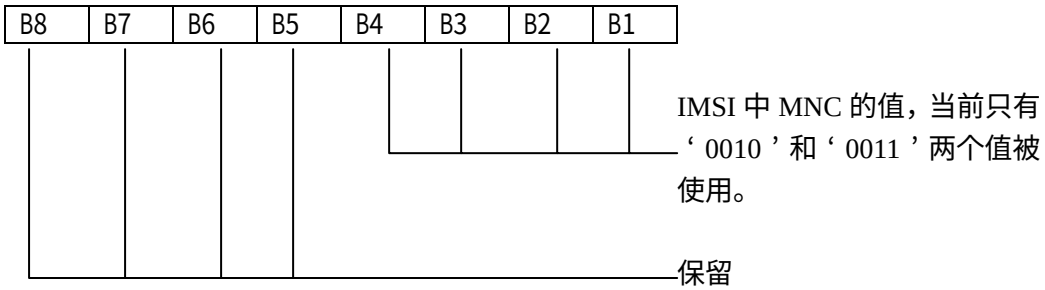
  - ME 制造特定的信息（若在第一个字节中的 b2=1）

- IMSI 中 MNC 的长度

  内容：数字长度指示器，用来从 IMSI 中提取 MNC

  编码：

  字节 4：



10．3．3．19 EF_{Phase} (Phase identification)

该 EF 包含了关于 SIM 卡阶段信息

文件标识符 ‘ 6FAE'	透明文件	必选
文件容量 1 个字节		更新频率 低
访问条件： READ ALW UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1	SIM 卡的阶段	M	1 字节

- SIM 卡的阶段

  编码：

  阶段 1：‘ 00 ’

  阶段 2：‘ 02 ’

  阶段 2+：‘ 03 ’（要求 PROFILE DOWNLOAD：概要信息下载）

  阶段的编码值：‘ 00 ’ - ‘ 0F ’都是被 SIM 卡支持的编码，‘ 04 ’ - ‘ 0F ’为保留编码。

  EF_{Phase} 的编码取值为‘ 00 ’，表示 SIM 卡支持阶段 1 的功能，同时 ME 也可以支持阶段 2 的一些特性。但是业务表中的 NO.3 号业务（FDN）和 NO.5 号业务（AoC）只有在 EF_{Phase} 的编码取值为阶段 2 的编码‘ 02 ’或高于阶段 2 的编码的 SIM 卡才能被置位和激活。

  若 EF_{Phase} 的编码取值为‘ 03 ’或更高阶段，由支持 SIM 卡应用工具箱的 ME 执行 PROFILE DOWNLOAD 程序。（详见 SIM 卡应用工具箱部分）

10．3．3．20 EF_{VGCS} (语音群呼业务)

该 EF 包含一系列用户已经签约的 VGCS 群识别符，该文件由 ME 在群呼叫建立和呼叫接受时使用。

文件标识符 ‘ 6FB1'	透明文件	可选
文件容量 4n 个字节 n≤50	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~4	群识别符 1	M	4 字节
5~8	群识别符 2	O	4 字节
(4n-3) ~4n	群识别符 n	O	4 字节

- 群识别符

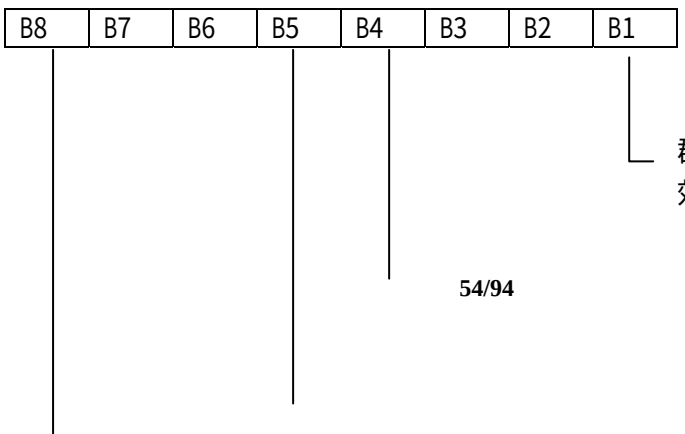
  内容：群识别符

  编码：

  VGCS 的群识别符是一串可变长度的数字，最大长度为 8 位数字。每个 VGCS 的群识别符采用四字节编码，每个字节的四个 bit 采用 BCD 编码，代表一个群识别符。如果群识别符的长度不足 8 位数字，则没有用到的半字节组被置为‘ F ’。

  群识别符 1 是群识别符中最重要的。

  第一字节：



…

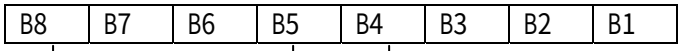
群识别组 1 的数字 1 的最大有效位

群识别组 1 的数字 2 的最小有效位

…

群识别组 1 的数字 2 的最大有效位

第二字节：



群识别组 1 的数字 3 的最小有效位

…

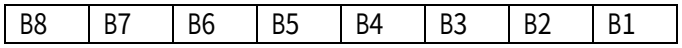
群识别组 1 的数字 3 的最大有效位

群识别组 1 的数字 4 的最小有效位

…

群识别组 1 的数字 4 的最大有效位

第三字节：



群识别组 1 的数字 5 的最小有效位

…

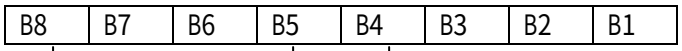
群识别组 1 的数字 5 的最大有效位

群识别组 1 的数字 6 的最小有效位

…

群识别组 1 的数字 6 的最大有效位

第四字节：



群识别组 1 的数字 7 的最小有

效位
…
群识别组 1 的数字 7 的最大有效位

群识别组 1 的数字 8 的最小有效位
…
群识别组 1 的数字 8 的最大有效位

…

第 4n 字节：

B8	B7	B6	B5	B4	B3	B2	B1

群识别组 n 的数字 7 的最小有效位
…
群识别组 n 的数字 7 的最大有效位

群识别组 n 的数字 8 的最小有效位
…
群识别组 n 的数字 8 的最大有效位

如果存储少于 n 个群识别组，则剩余的字节被置为‘ FF ’。

10．3．3．21 EF_{VGCSS} (语音群呼状态)

该 EF 包含了 VGCS 群识别符的激活状态，与 EF_{VGCS} 有直接关系。如果配置了 EF_{VGCS} 则 EF_{VGCSS} 也必须配置。

文件标识符 ‘ 6FB2'	透明文件	可选
文件容量 7 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~7	激活/去活标识符	M	7 字节

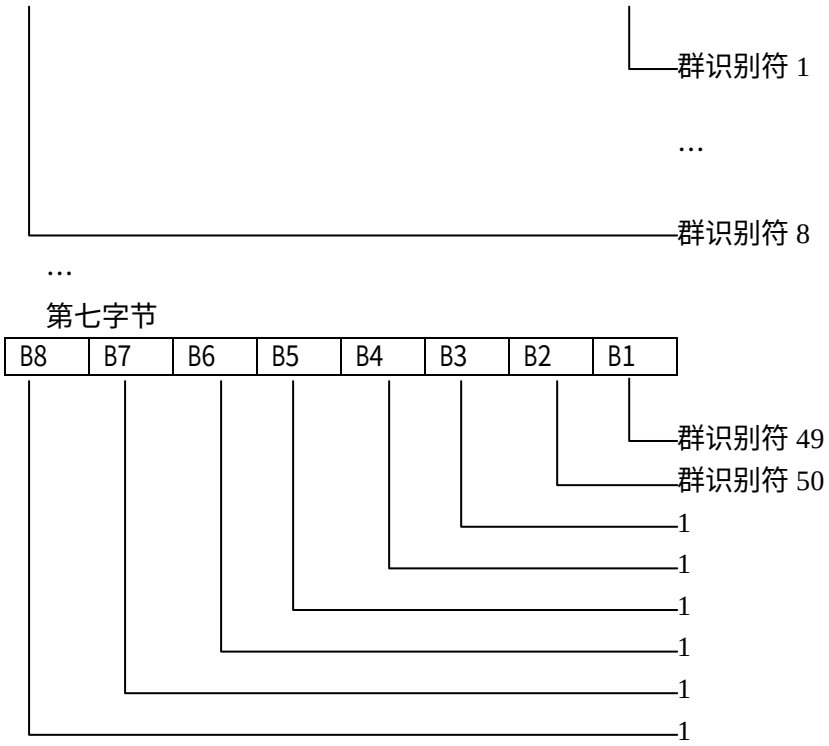
- 激活/去活标识符

  内容：群识别符的激活/去活标识符

  编码：bit=0：群识别符去活；bit=1：群识别符激活

  第一字节

B8	B7	B6	B5	B4	B3	B2	B1



10．3．3．22 EF_{VBS} (语音广播业务)

该 EF 包括一系列用户已经签约的 VBS 群的识别符，在广播呼叫建立和广播呼叫接收时由 ME 使用的 EF。

文件标识符 ‘6FB3'	透明文件	可选
文件容量 4n 个字节 n≤50	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~4	群识别符 1	M	4 字节
5~8	群识别符 2	O	4 字节
(4n-3) ~4n	群识别符 n	O	4 字节

- 群识别符
  内容：VBS 群识别符
  编码：参看 EF_{VGCS}。

10．3．3．23 EF_{VBSS} (语音广播业务业务状态)

该 EF 包含了 VBS 群识别符的激活状态，与 EF_{VBS} 有直接关系。如果配置了 EF_{VBS} 则 EF_{VBSS} 也必须配置。

文件标识符 ‘6FB4'	透明文件	可选
文件容量 7 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM		

REHABILITATE	ADM		
字节	描述	M/O	长度
1~7	激活/去活标识符	M	7 字节

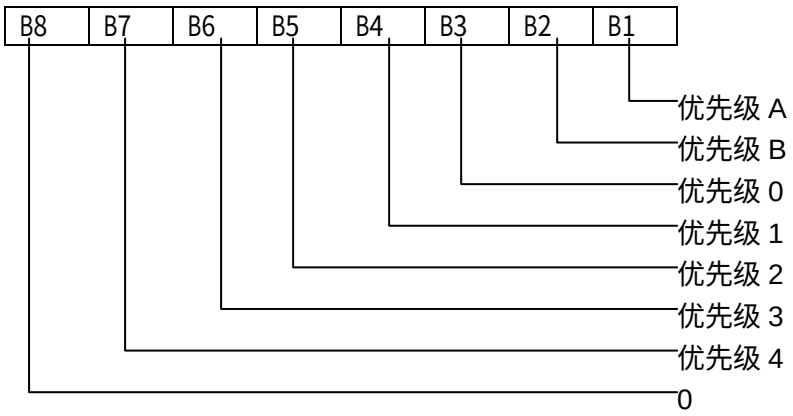
- 激活/去活标识符
  内容：群标识符激活/去活标识
  编码：参见 EF_{VGCSS} 内容编码

10．3．3．24 EF_{eMLPP} （增强型多优先级及抢占优先级）

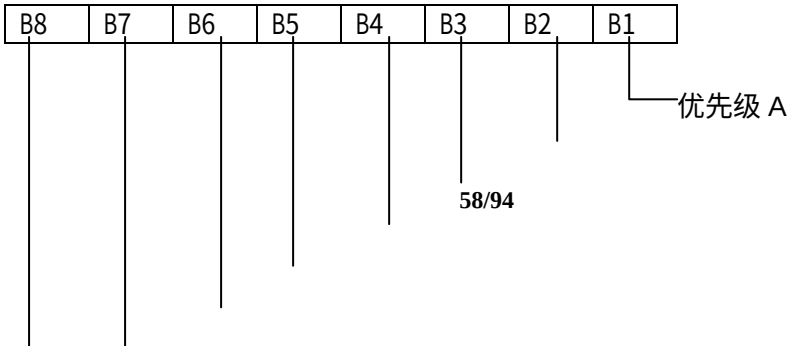
该 EF 包括用户采用的增强型多优先级及抢占业务的优先级和快速呼叫建立条件的信息。

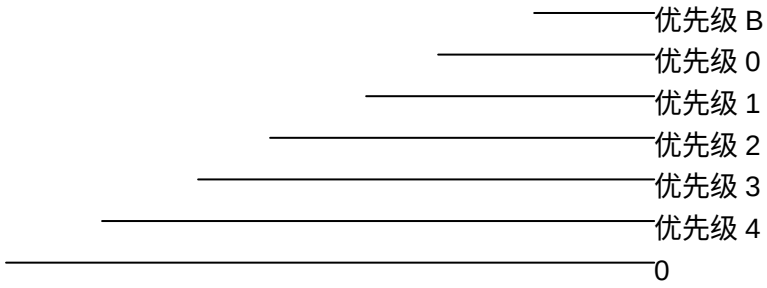
文件标识符 ‘6FB5'	透明文件	可选
文件容量 2 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		
字节	描述	M/O	长度
1	优先级	M	1 字节
2	快速呼叫建立条件	M	1 字节

- 优先级
  内容：要签约的 eMLPP 优先权。
  编码：每个 eMLPP 编码为一个 bit。签约的优先级的对应 bit 设为 1，未签约的 bit 设为 0，bit8 保留为 0。
  第一字节：



- 快速呼叫建立条件
  内容：对每个 eMLPP 优先级，具有执行快速呼叫程序的能力。
  编码：每个 eMLPP 优先权以一个 bit 进行编码。执行快速呼叫建立时对应 bit 设为 1，不执行快速呼叫建立时对应 bit 设为 0，bit8 为 0。
  第二字节：对以下优先级快速呼叫建立条件。





10．3．3．25 EF_{AAeM} (eMLPP 业务的自动应答文件)

该 EF 包括移动台对入局呼叫自动应答的优先级（对增强型多优先级及抢占业务）。

文件标识符 ‘6FB6'	透明文件	可选
文件容量 1 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

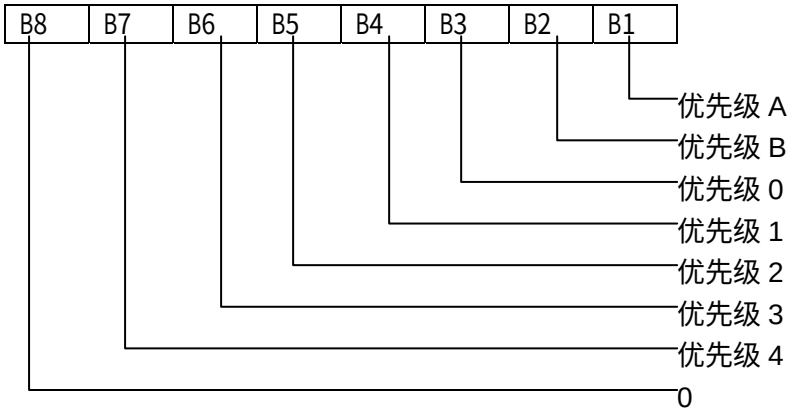
字节	描述	M/O	长度
1	自动应答优先级	M	1 字节

- 自动应答优先级

内容：对每个 eMLPP 优先级，MS 具有对入局呼叫的自动应答能力（结合相应的 eMLPP 优先级）。

编码：每个 eMLPP 以 1 个 bit 进行编码。允许自动应答的移动台优先级的对应 bit 设为 1，不允许自动应答的移动台优先级的对应 bit 设为 0，bit8 保留为 0。

第一字节：



10．3．3．26 EF_{CBMID} (数据下载的小区广播消息识别符)

该 EF 包含了定义小区广播消息的内容类型的消息识别参数。该消息将向 SIM 卡传送。SIM 卡中可存储任何数目的 CB 消息识别符，没有优先级。

文件标识符 ‘6F48'	透明文件	可选
文件容量 2n 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM		

REHABILITATE	ADM		
字节	描述	M/O	长度
1~2	CB 消息识别符 1	O	2 字节
3~4	CB 消息识别符 2	O	2 字节
（2n-1）~2n	CB 消息识别符 n	O	2 字节

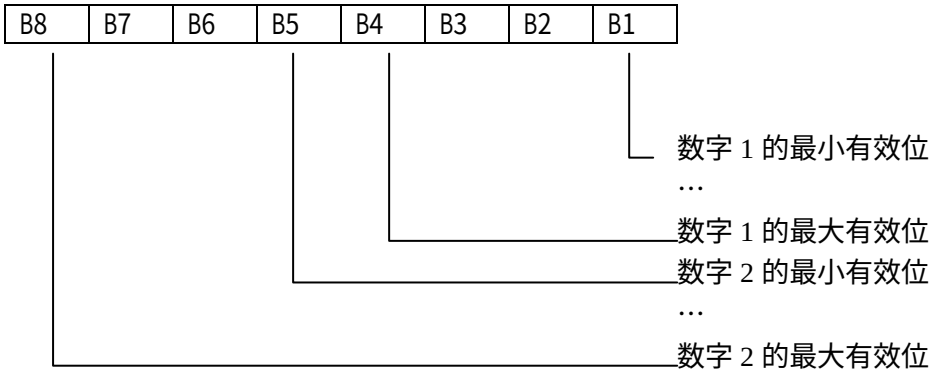
- 小区广播识别符
  移动台将收到的上述消息传输给 SIM 卡。无用的设为‘ FF ’‘ FF ’

10．3．3．27 EF_{ECC} (紧急呼叫码)

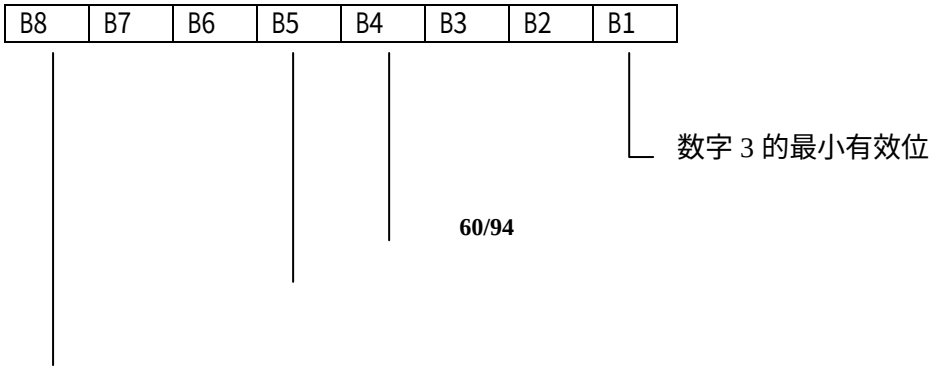
该 EF 包含 5 个紧急呼叫编码。

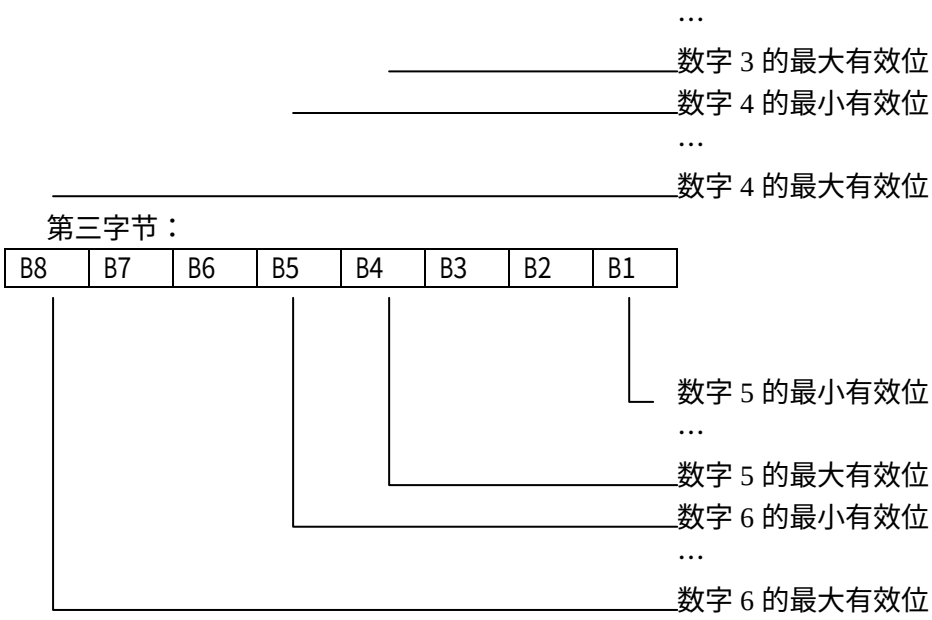
文件标识符 ‘ 6FB7'	透明文件	可选
文件容量 3n 个字节 n≤5	更新频率 低	
访问条件： READ ALW UPDATE ADM INVALIDATE ADM REHABILITATE ADM		
字节	描述	M/O	长度
1~3	紧急呼叫编码 1	O	3 字节
4~6	紧急呼叫编码 2	O	3 字节
（3n-2）~3n	紧急呼叫编码 n	O	3 字节

- 紧急呼叫编码
  内容：紧急呼叫编码
  编码：紧急呼叫码的长度可变，最大为 6 位数。每一个紧急呼叫码的编码为 3 个字节，每个数字编码为 4 个 bit，若选择的编码小于 6 位，则未使用的 bit 设为‘ F ’。
  第一字节：



第二字节：





10．3．3．28 EF_{CBMIR} (小区广播消息识别符范围的选择)

该 EF 包含用户希望 MS 采纳的小区广播消息识别符的范围。

SIM 卡中可存储任何数量的小区广播消息识别符参数，没有优先级。

文件标识符 ‘6F50'	透明文件	可选
文件容量 4n 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~4	CB 消息识别范围 1	O	4 字节
5~8	CB 消息识别范围 2	O	4 字节
(4n-3) ~4n	CB 消息识别范围 n	O	4 字节

- CB 消息识别范围

  内容：CB 消息识别范围

  编码：每个范围识别符的 1 和 2 字节等于一个较小的小区广播范围而字节 3 和 4 等于一个较大的小区广播范围。上表所列数值均由 MS 采纳。未使用的设为“ FF FF FF FF ”。

10．3．3．29 EF_{DCK} （解网络个人化控制密钥文件）

该 EF 用于存储与个人化有关的解网络个人化控制密钥。

文件标识符 ‘6F2C'	透明文件	可选
文件容量 16 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM		

REHABILITATE ADM			
字节	描述	M/O	长度
1~4	解网络个人化控制密钥的八位数字	M	4 字节
5~8	解网络子个人化控制密钥的八位数字	M	4 字节
9~12	解运营者个人化控制密钥的八位数字	M	
13~16	解团体个人化控制密钥的八位数字	M	4 字节

空闲控制密钥记录应编码位‘ FFFFFFFF ’

10．3．3．30 EF_{CNL} (互操作网络表)

该 EF 包含用于多网络个人化业务的互操作网络表。

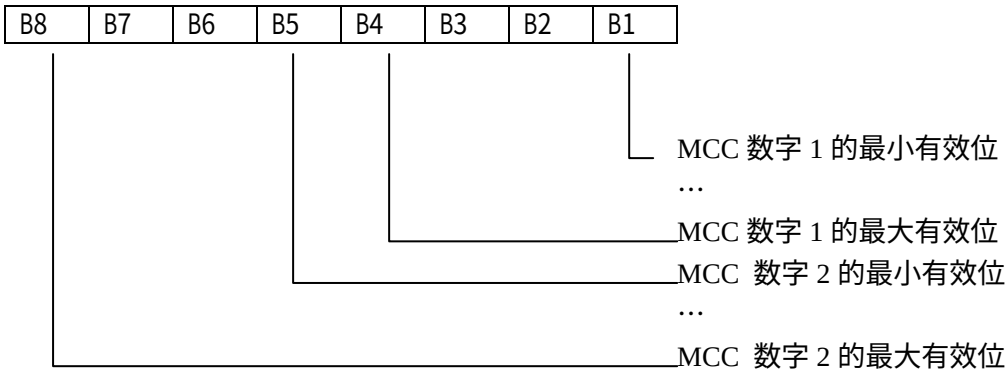
文件标识符 ‘ 6F32'	透明文件	可选
文件容量 6n 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		
字节	描述	M/O	长度
1~6	互操作网络表单元 1	O	6 字节
…			
（6n-5）~6n	互操作网络表单元 n	O	6 字节

- 互操作网络表

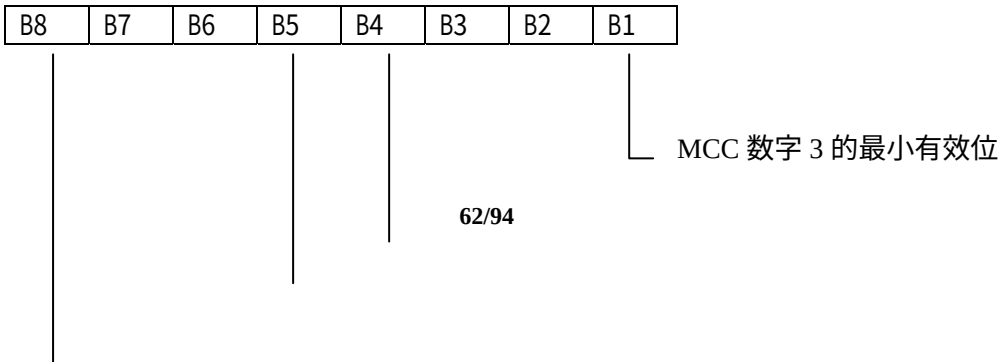
  内容：包括 MCC，MNC，网络子集，业务运营者 ID 和互操作网络的集体识别符。

  编码：每个单元 6 个字节

  第一字节：



  第二字节：



…

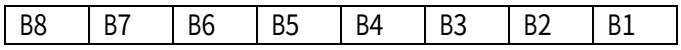
MCC 数字 3 的最大有效位

MCC 数字 3 的最小有效位

…

MCC 数字 3 的最大有效位

第三字节：



MNC 数字 1 的最小有效位

…

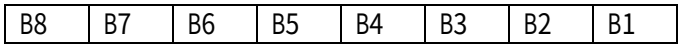
MNC 数字 1 的最大有效位

MNC 数字 2 的最小有效位

…

MNC 数字 2 的最大有效位

第四字节：



网络子集数字 1 最小有效位

…

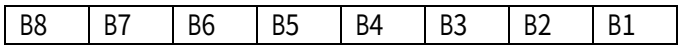
网络子集数字 1 最小有效位

网络子集数字 2 最小有效位

…

网络子集数字 2 最小有效位

第五字节：



运营者数字 1 的最小有效位

…

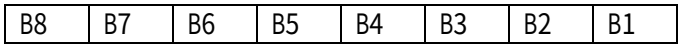
运营者数字 1 的最小有效位

运营者数字 2 的最小有效位

…

运营者数字 2 的最小有效位

第六字节：



团体代号 1 的最小有效位

…

团体代号 1 的最小有效位

团体代号 2 的最小有效位

…

团体代号 2 的最小有效位

空字段编码应采用‘ FF ’。用编码‘ FFF ’的 MCC 字段定界表的结尾。

10．3．3．31 EF_{NIA} (网络报警指示)

该 EF 包含了网络报警指示的种类和与之相关的文本。

文件标识符 ‘ 6F51'	线性定长文件	可选
记录长度 X+1 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1	报警种类	M	1 字节
X	信息文本	M	X 字节

10．3．3．32 EF_{KcGPRS} (GPRS 计算密钥 KcGPRS)

该 EF 包含了 GPRS 加密密钥 KcGPRS，和密钥序号 n。

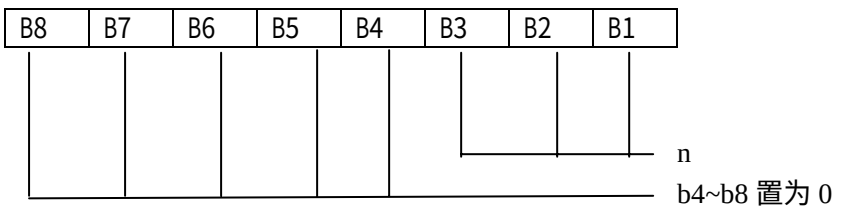
文件标识符 ‘ 6F52'	透明文件	可选
文件容量 9 个字节	更新频率 高	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~8	加密密钥 KcGPRS	M	8 字节
9	密钥序号 n	M	1 字节

- 加密密钥 KcGPRS

  编码：KcGPRS 的最低有效位为第 8 个字节的最低位，最高有效位为第 1 个字节的最高位
- 密钥序号 n

  编码：



注：如果 n=111，则表示“密钥不可用”。因此值‘07’而不是‘FF’作为管理阶段代码。

10．3．3．33 $EF_{LOCIGPRS}$ (GPRS 位置信息)

该 EF 包含了下列位置信息：

- 打包的临时移动用户身份号(P-TMSI)；
- 打包的临时移动用户身份号签名值(P-TMSI signature value)；
- 路由区域信息(RAI)；
- 路由区域更新状态。

文件标识符 ‘6F53'	透明文件	可选
文件容量 14 个字节	更新频率 高	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~4	P-TMSI	M	4 字节
5~7	P-TMSI 签名值	M	3 字节
8~13	RAI	M	6 字节
14	路由区更新状态	M	1 字节

- P-TMSI

  内容：临时移动用户识别数据包

  编码：

  第一字节：P-TMSI 的第一字节

B8	B7	B6	B5	B4	B3	B2	B1

  最高有效位

- P-TMSI 签名值

  内容：临时移动用户识别数据包签名值

  编码：

  第五字节：P-TMSI 签名值的第一字节

B8	B7	B6	B5	B4	B3	B2	B1

  最高有效位

- RAI

  内容：路由区域信息

  编码：

  第八字节：RAI 第一字节

B8	B7	B6	B5	B4	B3	B2	B1

最高有效位

- 路由区更新状态
  内容：路由区域更新的状态
  编码：
    字节14:
      Bits: b3 b2 b1
        0 0 0：更新
        0 0 1：不更新
        0 1 0：不允许接入PLMN
        0 1 1：不允许接入路由区域
        1 1 1：保留
    b4~b8：保留。

10．3．3．34 EF_{SUME} (建立菜单单元)

该 EF 包含了含有简单的 TLV 编码格式的菜单标题信息，用于 SIM 卡主动式应用命令—SET UP MENU。

文件标识符 ‘6F54'	透明文件	可选
文件容量 X+Y 个字节	更新频率 低	
访问条件： READ ADM UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~X	标题α标识符	M	X 字节
X+1~X+Y	标题图标标识符	O	Y 字节

- 标题α标识符
  内容：采用简单的 TLV 格式编码的菜单标题文本。
  编码：详见本标准的 STK 部分
- 标题图标标识符
  内容：采用简单的 TLV 格式编码的标题图标。
  编码：详见本标准的 STK 部分

10．3．4 电信目录下的文件

在专用文件$DF_{TELECOM}$中的EF包含与业务有关的文件

10．3．4．1 EF_{ADN} (缩位拨号)

包含缩位拨号号码（ADN）和补充业务控制串（SSC），另外，还包括相关的网络/承载能力的识别符，以及扩展记录的识别符，还包括相关的α识别符。

文件标识符 ‘6F3A'	线性定长文件	可选
记录长度 X+14 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE CHV2 REHABILITATE CHV2		

字节	描述	M/O	长度
1~X	α标识符	O	X 字节
X+1	BCD 号码/SSC 内容的长度	M	1 字节
X+2	TON 和 NPI	M	1 字节
X+3~X+12	拨号号码/SSC 串	M	10 字节
X+13	能力/配置识别符	M	1 字节
X+14	扩展 1 记录识别符	M	1 字节

- α标识符

  内容：与拨号有关的α标识符

  编码：α识别符将采用 7bit 字符编码，bit8=0，左对齐。不用的字节都设置为‘FF’。

注 1：0＜X＜241，用 GET RESPONS 命令 ME 能决定 X 的数值。

- BCD 号码/SSC 内容的长度

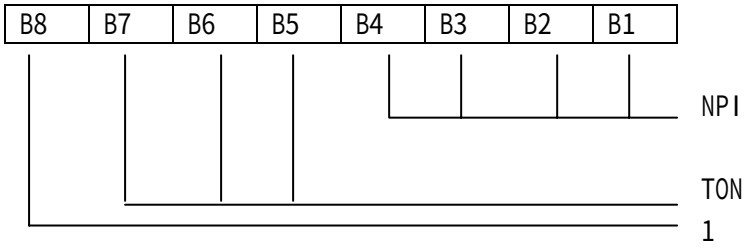
  内容：这个字节给出实际的 BCD 号码/SSC 串信息两项数据项的字节数量。这意味着最大值只能是 11 个字节，即使当实际的 AND/SSC 串信息的长度超过 11。当 AND/SSC 要求大于 20 位时，则用不等于‘FF’的扩展 1 识别符表示。其余项以溢出数据记录的余项长度被存储在 EF_{EXT1} 之中，其中，溢出数据是以适当的溢出记录自身的编码的数据出现。

- TON 和 NPI

  内容：号码类型（TON）和编码方案（NPI）。

  编码：若 AND/SSC 串不包括拨打号码，例如：利用一种控制串去活一种业务，则 TON/NPI 应由 ME 设置为‘FF’。（见注 2）

注 2：若拨打号码空缺，则在空中接口上没有 TON/NPI 字节的发射，因此，ME 将不用对‘FF’加以解释，也不用在空中接口上进行发射。



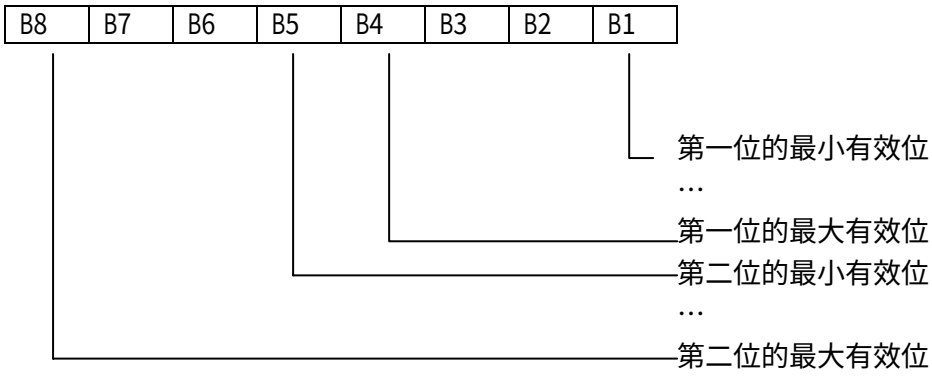
- AND/SSC 串：

  内容：最多 20 位的电话号码和/或 SSC 串信息。

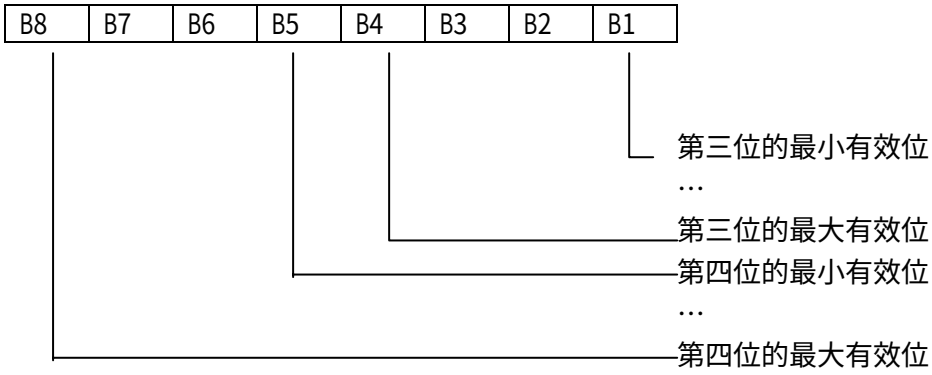
  编码：扩展 BCD 编码方式见表 10.3.4.1 所示。若电话号码或 SSC 多于 20 位时，则第一个 20 位存储在这个数据项中，而将溢出数据存储在 EF（EXT1）的相关记录中。

这个记录由扩展 1 记录识别符来识别。若 AND/SSC 要求少于 20 位，则在数据项末端的空字节设为‘ F ’。

字节 X+3：



字节 X+4：



其余字节同字节 X+4

- 能力/配置识别符

内容：能力/配置识别字节。用来识别在 EF_{CCP} 中的记录号码，该记录含有呼叫所要求的相关能力/配置参数。该字节为可选项。若未被使用设置为‘ FF ’。

编码：二进制编码。

- 扩展 1 记录识别符

内容：扩展 1 记录识别符字节。用来识别在 EF_{EXT1} 中的记录的号码，该记录包括相关的被叫用户子地址或溢出数据。该字节为可选项，若未被使用设置为‘ FF ’。

若 AND/SSC 同时需要溢出数据和被叫用户子地址时，则该字节识别溢出记录，是一个 EF_{EXT1} 内的连锁机制。EF 识别被叫用户子地址的记录。

编码：二进制编码。

注 3：由于 EF_{ADN} 是 $DF_{TELECOM}$ 的一部分。它可以用于 GSM，也可在多应用卡中另有所用。若非 GSM 应用不识别 TON 和 NPI，则与国家拨号计划相关的信息必须保持在 AND/SSC 串的数据中，并将 TON 和 NPI 的字段设置为 UNKNOWN。这种格式对 GSM 操作和忽略 TON 和 NPI 字段的非 GSM 应用均是可接受的。

例如：SIM 卡存储采用 CCITT 编码方案的国际号码：

	TON	NPI	数据段
GSM 应用	001	0001	abc…
与 GSM 应用相兼容的其它应用	000	0000	XXX…abc…。

其中“ abc… ”表示用户号码位（包括国家码），“ XXX… ”表示转意位或国家前缀替代 TON 和 NPI。

注 4：当 ME 为了识别一个在 α 识别符中的字符串，用 SEEK 命令在 EF_{ADN} 上操作时，若 MMI 允许用户提供一个较大的字符数量，ME 必须保证用作为 SEEK 参数的字符的数量少于或等于 X 值。

表 10.3.4.1

BCD 值	字符/意义
‘ 0 ’	“ 0 ”
…	
‘ 9 ’	“ 9 ”
‘ A ’	“ * ”
‘ B ’	“ # ”
‘ C ’	DTMF 控制数字分离器
‘ D ’	“ 通配符 ”值，将引起 MMI 对一个单数位用户的激励。
‘ E ’	扩展位（‘ 移位键 ’） 它有一个把‘ 10 ’加到后跟位上的作用。以后后跟位的 BCD 位均在‘ 10 ’~‘ 1E ’范围内得到解释。关于这个范围内的位的用途，待定。
‘ F ’	结束标识 例如：在一个位为奇数的情况下。

BCD 值‘ C ’‘ D ’和‘ E ’不通过空中接口发射。

注 5：关于作为 DTMF 位的‘ D ’‘ E ’和‘ F ’值的解释方式，待定。

注 6：用一个 3 秒终止方式描述一个两次子序列‘ C ’BCD 的值。

10．3．4．2 EF_{FDN} (固定拨号)

该 EF 包括固定拨号（FDN）和/或补充业务控制字串（SSC），还包括相关网络/承载能力的识别符和扩展记录的识别符，以及有关的 α 识别符。

文件标识符 ‘ 6F3B'	线性定长文件	可选
记录长度 X+14 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV2 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~X	α 标识符	O	X 字节
X+1	BCD 号码/SSC 内容的长度	M	1 字节
X+2	TON 和 NPI	M	1 字节
X+3~X+12	拨号号码/SSC 串	M	10 字节
X+13	能力/配置识别符	M	1 字节
X+14	扩展 2 记录识别符	M	1 字节

注：在 α 标识符中表示字节数的 X 值与 EF_{ADN} 中表示长度的 X 不同。

所有数据项的内容和编码按 10．3．4．1 的数据项,只有扩展记录存储在 EF_{EXT2} 之中。

10．3．4．3 EF_{SMS} (段消息)

该 EF 包含短消息信息及相关参数。其中有 MS 从网络侧接收的，有 MS 发出的消息。

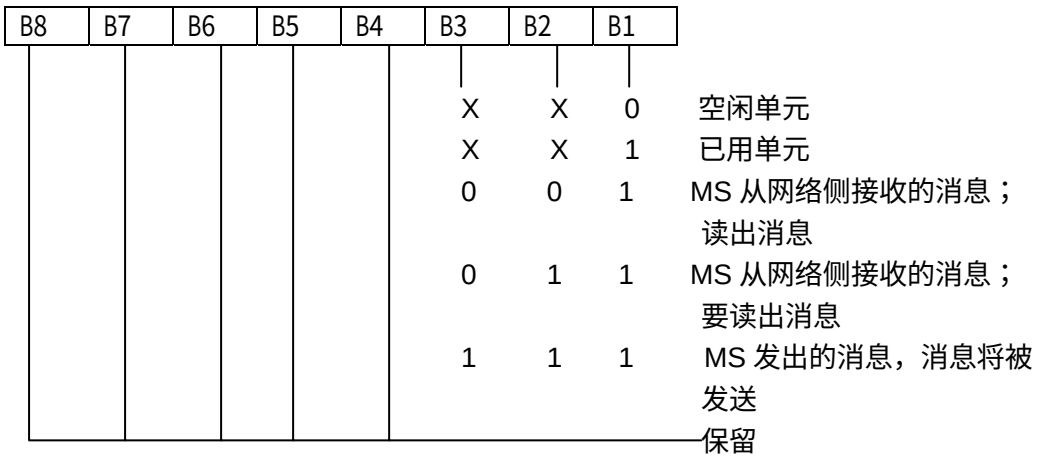
文件标识符 ‘6F3C'	线性定长文件	可选
记录长度 176 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV2 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1	状态	M	1 字节
2~176	余项	M	175 字节

- 状态

内容：在 SEEK 命令中，作为图样记录的状态字节。MS 产生短信息并发送到网络，当 MS 收到状态报告后，或者成功发送短信命令，状态将被写入。

编码：



- 余项：

内容：这个数据项以 TS-业务-中心-地址开始。紧跟在 TS-业务-中心-地址后的字节含有一个短消息 TPDU，具有相同的编码和参数顺序。

编码：任何存储在 SIM 卡中的由 MS 发起的消息的 TP-消息参考，将有下列数值：

TP-消息-参考的数值

要发送的消息： ‘FF’

向网络侧发送的消息： 在向网络侧发送的消息中采用 TP- 消息-参考的数值。

跟在 TPDU 记录中的任何字节填充‘FF’。

对于一个最大允许长度的 TS-业务-中心-地址，例如包括超过 18 个地址位的数字，有可能与一个最大长度的 TPDU 结合，这样它们总长度为 176 字节。在这种情况下，除了 TPDU 的最后一个字节不存储之外，ME 应不经修改地把 TS-业务-中心-地址和 TPDU 存储到 SIM 卡中的 2-176 字节中。

10．3．4．4 EF_{CCP} (能力配置参数)

该 EF 包括所需要的网络和承载能力的参数，以及当采用缩位拨号号码，固定拨号号码，MSISDN 或末位拨号方式建立呼叫时相关的 ME 配置。

文件标识符 ‘6F3D'	线性定长文件	可选

记录长度 14 个字节		更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
字节	描述	M/O	长度
1~10	承载能力信息单元	M	10 字节
11~14	保留的字节（见下述内容）	M	4 字节

- 承载能力信息单元：

  信息单元标识符（IEI）。例如：记录的第一个字节是承载能力信息的长度。

字节 11-14 被置成‘ FF ’并且不被 ME 解释。

10．3．4．5 EF_{MSISDN} （移动基站国际综合业务网号（MSISDN））

该 EF 包含了与用户有关的 MSISDN，其中包括网络/承载能力和扩展记录的识别符，以及α标记

文件标识符 ‘ 6F40'	线性定长文件	可选	
记录长度 X+14 个字节		更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
字节	描述	M/O	长度
1~X	α标识符	O	X 字节
X+1	BCD 号码/SSC 内容的长度	M	1 字节
X+2	TON 和 NPI	M	1 字节
X+3~X+12	拨号号码/SSC 串	M	10 字节
X+13	能力/配置识别符	M	1 字节
X+14	扩展 2 记录识别符	M	1 字节

注：

1. 若 SIM 卡在初始化过程中存储了多个 MSISDN 号码，则存储在第一个记录中的 MSISDN 应该优先显示。
2. 在α标识符中表示字节数的 X 值与 EF_{ADN} 中表示长度的 X 不同。

关于全部数据项的内容与编码分别见 EF_{ADN} 的数据项

10．3．4．6 EF_{SMSP} (短消息参数文件)

该 EF 包括短消息业务首部参数的数据（SMSP），ME 利用这些数据协助移动用户发送短消息。

还包括一个或多个记录，而都能够保持一个 SMS 参数的设置。在 EF 中的第一个记录（或只有一个）应用，如果没有可选择的其它记录，则其作为参数的缺省值。

为识别记录，每个记录中都含有一个α识别符，在 Y 字节上进行编码。

存储在记录中的 SMS 参数可以独立地存在或空缺。当 MS 要发送一个短消息时，如果用户没有提供参数则采用 SIM 卡中记录的参数。

文件标识符 ‘ 6F42'	线性定长文件	可选
记录长度 28+Y 个字节	更新频率 低	

访问条件：			
READ	CHV1		
UPDATE	CHV1		
INVALIDATE	ADM		
REHABILITATE	ADM		
字节	描述	M/O	长度
1~Y	α标识符	O	Y 字节
Y+1	参数显示器	M	1 字节
Y+2~Y+13	TP-目的地址	M	12 字节
X+14~Y+25	TS-业务中心地址	M	12 字节
Y+26	TP-协议标识符	M	1 字节
Y+27	TP-数据编码方案	M	1 字节
Y+28	TP-有效周期	M	1 字节

对于所有可能的 SMS 参量，不管它们是否存在，都要分配存储单元。任何不用的字节均要设置为‘ FF ’。

- α标识符：

  内容：与 SMS 有关的α标识符。

  编码：参考 10．3．4．1

注：Y 值可以为 0，即不用α标识符。ME 利用 GET RESPONSE 命令可确定 Y 的数值。

- 参数显示器

  内容：采用参数显示器字节中的单个 bit 标示出存储在记录的余项内的 SMS-参数缺省值为空缺或存在的情况。

  编码：bit 的配置：

bit	参数内容
1	TP-目的地地址
2	TS-业务中心地址
3	TP-协议地址
4	TP-数据编码方案
5	TP-有效周期
6	暂定为 1
7	暂定为 1
8	暂定为 1

bit 值	意义
0	存在参数
1	空缺参数

- TP-目的地址：

  内容与编码：规定 SM-TL 地址字段。

- TP-业务中心地址：

  内容与编码：规定 RP-目的地地址中心地址。

10．3．4．7 EF_{SMSS} (短信息状态)

该 EF 包含了与短信息业务有关的状态信息，并与 EF_{SMSP} 相关。两个文件在 SIM 卡中

同时存在或空缺。

文件标识符 ‘6F43'	透明文件	可选
记录长度 2+X 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1	最后采用的 TP-MR	M	1 字节
2	SMS “超过存储器的能力”通知标识	M	1 字节
3~2+X	RFU	O	X 字节

- 最后采用的 TP-MR

  内容：移动台最后发送的短消息 TP-消息-参考参数的数值。

- SMS “超过存储器的能力”通知标识

  内容：这个标识是用来控制流量的。因此，一旦 MS 的存储能力可用，网络就会得到通知。

  编码：

  b1=1 未设标识，存储量可用；

  b1=0 已设标识；

  b2~b8 保留并设为 1。

10．3．4．8 EF_{LND} (最后拨叫号码（LND）)

该 EF 包含最后拨叫号码（LND）和/或各自的补充业务控制串（SSC），其中包括相关网络/承载能力的识别符和扩展记录的识别符，也包括相关的α标识符。

文件标识符 ‘6F44'	循环文件	可选
记录长度 X+14 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INCREASE NEVER INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~X	α标识符	O	X 字节
X+1	BCD 号码/SSC 内容的长度	M	1 字节
X+2	TON 和 NPI	M	1 字节
X+3~X+12	拨号号码/SSC 串	M	10 字节
X+13	能力/配置识别符	M	1 字节
X+14	扩展 1 记录识别符	M	1 字节

内容与编码：见 EF_{ADN}

在 EF_{LND} 中的 X 值可与 EF_{ADN} 和 EF_{FDN} 中的 X 值不同。

若在 EF_{LND} 中的 X 值长于要存储号码α识别符的长度，则 ME 将用‘FF’填满α识别符。反之，则 ME 截去超过的字节。

10．3．4．9 EF_{SDN} (业务拨号号码)

该 EF 包括特定的业务号码（SDN）和/或补充业务控制字符串（SSC)。另外还包括与网络/承载有关的识别符和扩展记录识别符及相关的α标识。

文件标识符 ‘6F49'	线性定长文件	可选
记录长度 X+14 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1~X	α标识符	O	X 字节
X+1	BCD 号码/SSC 内容的长度	M	1 字节
X+2	TON 和 NPI	M	1 字节
X+3~X+12	拨号号码/SSC 串	M	10 字节
X+13	能力/配置识别符	M	1 字节
X+14	扩展 3 记录识别符	M	1 字节

内容与编码：见 EF_{ADN}

注：X 值（α标识符）可能与 EF_{ADN} 中的 X 值不同

10．3．4．10 EF_{EXT1} (扩展文件 1)

该 EF 包括 AND/SSC，MSISDN 或 LND 的扩展数据。扩展数据是由下列原因造成的：

- AND/SSC（MSISDN，LND）在超出（AND/SSC）基本文件的 20 位的情况下，将余项以记录的方式存在这个 EF 中。余项在 AND/SSC（MSISDN，LND）基本文件内部用一个特殊的识别字节进行识别。在这种情况下的 EXT1 记录被规定为溢出数据；
- 相关被叫用户子地址。在这种情况下的 EXT1 记录被规定为子地址。

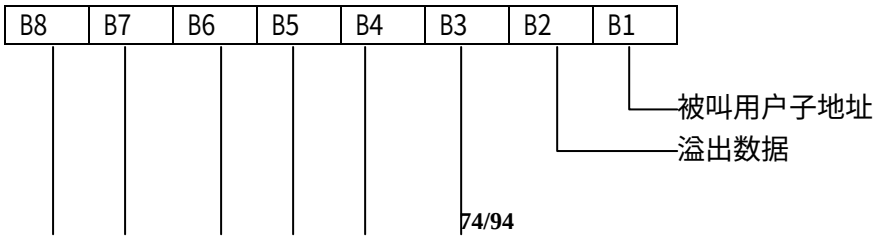
文件标识符 ‘6F4A'	线性定长文件	可选
记录长度 13 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1	记录类型	M	1 字节
2~ 12	扩展数据	M	11 字节
13	识别符	M	1 字节

- 记录类型

  内容：记录的类型。

  编码：



——————————————————————保留

b3~b8 保留并设为 0；

一个 bit 被置为 1 来识别记录的类型；

只有一种类型被设置；

‘ 00 ’表示“ 未知 ”类型。

下面编码的例子表示扩展数据的类型是“ 溢出数据 ”：

B8	B7	B6	B5	B4	B3	B2	B1
0	0	0	0	0	0	1	0

- 扩展数据：

  内容：溢出数据或被叫用户子地址，依赖于记录的类型。

  编码：

  情况 1：EXT1 记录是溢出数据：

  扩展数据的第一个字节给出 AND/SSC（MSISDN，LND）余项的字节个数，余项字节的编码为 BCD，符合 AND/SSC（MSISDN，LND）的编码。在末端的无用字节必须设为‘ F ’。若溢出字节数字位数超出溢出记录的能力，则有可能用字节 13 中的识别符去链接 EXT1 基本文件内的另一个记录。

  情况 2：EXT1 记录是被叫用户子地址：

  除了信息单元识别符外，其它的信息都存储在 SIM 卡中，这个地址数据的最大长度为 2 位。在需要两个扩展记录的情况下，这些记录是用识别符字段连接起来的。含有被叫用户子地址的第一部分的扩展记录指向含有子地址第二部分的记录。

- 识别符

  内容：下一个扩展记录的识别符能存储长于 11 字节的信息。

  编码：下一个记录的号码，‘ FF ’表示链接的结束。

10．3．4．11 EF_{EXT2} (扩展文件 2)

该 EF 包括 FDN/SSC 的扩展数据。

文件标识符 ‘ 6F4B'	线性定长文件	可选
记录长度 13 个字节	更新频率 低	
访问条件： READ CHV1 UPDATE CHV2 INVALIDATE ADM REHABILITATE ADM		

字节	描述	M/O	长度
1	记录类型	M	1 字节
2~ 12	扩展数据	M	11 字节
13	识别符	M	1 字节

内容与编码参见 EF_{EXT1}。

10．3．4．12 EF_{EXT3} (扩展文件 3)

该 EF 包括 SDN 的扩展数据。

文件标识符 ‘ 6F4C'	线性定长文件	可选
记录长度 13 个字节	更新频率 低	

访问条件：			
READ	CHV1		
UPDATE	ADM		
INVALIDATE	ADM		
REHABILITATE	ADM		
字节	描述	M/O	长度
1	记录类型	M	1 字节
2~ 12	扩展数据	M	11 字节
13	识别符	M	1 字节

内容与编码参见 EF_{EXT1}。

10．3．4．13 EF_{BDN} (禁止号码)

该 EF 包括禁用的拨号（BDN）和补充业务控制字符串（SSC），还包括有关网络/承载容量的识别符，扩展记录的识别符，也包括有关的α识别符。

文件标识符 ‘6F4D'	线性定长文件	可选
记录长度 X+15 个字节	更新频率 低	
访问条件：		
READ	CHV1	
UPDATE	CHV2	
INVALIDATE	CHV2	
REHABILITATE	CHV2	

字节	描述	M/O	长度
1~X	α标识符	O	X 字节
X+1	BCD 号码/SSC 内容的长度	M	1 字节
X+2	TON 和 NPI	M	1 字节
X+3~X+12	拨号号码/SSC 串	M	10 字节
X+13	能力/配置识别符	M	1 字节
X+14	扩展 4 记录识别符	M	1 字节
X+15	比较方法的信息	M	1 字节

关于内容与编码方式，扩展数据除例外的存储在 EF_{EXT4} 扩展记录中的比较方法信息之外，均按照 EF_{ADN}。

注：X 值与 EF_{ADN} 的 X 可以不同。

- 比较方法的信息

  内容：这一个字节描述与 BDN 有关的比较方法，不做规定，可由运营者在 SIM 卡上规定执行 BDN 特性的方法。

  编码：二进制，允许值：0-255。

10．3．4．14 EF_{EXT4} (扩展文件 4)

该 EF 包含 BDN/SSC 的扩展数据。

文件标识符 ‘6F4E'	线性定长文件	可选
记录长度 13 个字节	更新频率 低	
访问条件：		
READ	CHV1	
UPDATE	CHV2	

INVALIDATE	ADM		
REHABILITATE	ADM		
字节	描述	M/O	长度
1	记录类型	M	1 字节
2~ 12	扩展数据	M	11 字节
13	识别符	M	1 字节

内容与编码参见 EF_{EXT1} 。

10．4 GSM 的文件

如图 10．4 所示。

采用 7F20 选择 DF_{GSM}，若选择失败，则 GSM 的 MES 可以用 DCS1800 ME 的标识符 7F21 选择 DF_{GSM}。

注 1：若选择 7F20 选择 DF_{GSM} 失败，而采用识别符 7F21 选择 DF_{GSM}，这样，才能保证与仅采用目录标识符 7F21 选择第一阶段的 $DF_{DCS1800}$ 的第一阶段 1800SIM 卡向后兼容性。

注 2：为保证与第一阶段 1800 ME 的后兼容性，规定两种方法去选择 DF_{GSM}：

1）在操作系统中建立 7F21 指向 7F20；

2）在文件系统中建立 7F21 目录，该目录下具有 7F20 的文件。

11 应用协议

当涉及到 GSM 管理操作时，SIM 卡与相应的终端接口。这部分内容不在本规范内。

当涉及到 GSM 网络操作时，SIM 卡接口与 ME 交换消息，该消息可能是命令或是响应。

- 一个 GSM 命令/响应对由一个命令与相关的响应组成；
- 一个 GSM 程序由一个或多个 GSM 命令/响应对组成。 这些命令/响应对用来执行面向应用的全部任务或部分任务。一个程序应看作一个整体。即完成一个程序就是执行一个相应的任务。当按照厂商的手册操作时，ME 应保证不能因任何未规定的命令/响应对的序列的中断导致程序自身的失败。
- 在 GSM 应用中，SIM 卡的 GSM 对话只是一段时间间隔，在完成 SIM 卡初始化程序时开始，结束有两种情况，或是在 GSM 对话终止程序开始时结束，或是在 SIM 卡与 ME 之间的连接第一次中断时结束。

在 GSM 网络操作阶段期间，ME 主控，SIM 卡服从。

在 SIM/ME 接口上的某些程序需要 MMI 互操作，所以在下表中把它们标识为“ MMI ”。在 MS 和网络之间的某些程序需要互操作，所以在下面程序表中把它们标识为“ NET ”。

有些程序是由 ME 自动发起的，所以在下面程序表中把它们标识为“ ME ”。

在 GSM 网络中的 SIM/ME 接口上的程序如下：

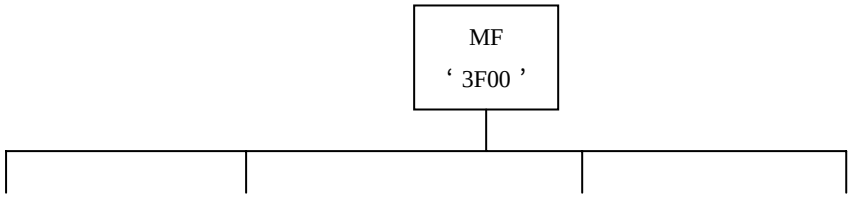
a） 通用程序

——读出 EF ME

——更新 EF ME

——增加 EF ME

b） SIM 卡管理程序



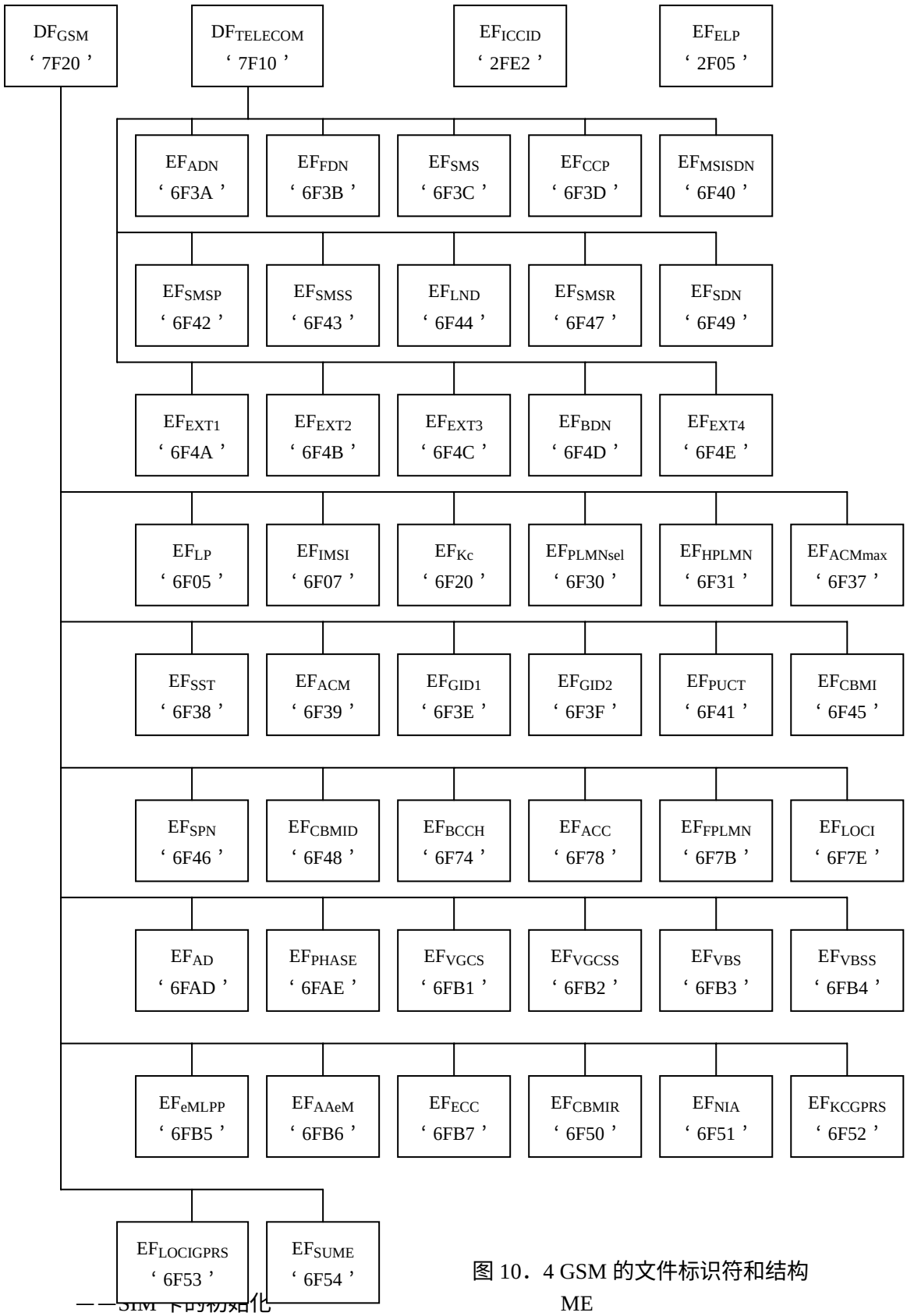


图 10．4 GSM 的文件标识符和结构

——SIM 下的初始化 ME
——GSM 对话终止 ME
——紧急呼叫编码请求 ME
——优先语言请求 ME

——管理信息请求 ME
——SIM 卡业务表请求 ME
——SIM 卡阶段请求 ME

c） CHV 相关程序
——CHV 证实方式 MMI
——CHV 值替代方式 MMI
——CHV 不使能 MMI
——CHV 使能 MMI
——CHV 解锁 MMI

d） 有关 GSM 安全的程序
——GSM 算法的计算方式 NET
——IMSI 请求 NET
——接入控制请求 NET
——HPLMN 搜索周期请求 NET
——位置信息请求 NET
——密钥 NET
——BCCH 信息 NET
——禁用的 PLMN 信息 NET

e） 签约相关程序
——拨号（AND，FDN，MSISDN，LND，SDN，BDN） MMI/ME
——短消息（SMS） MMI
——计费通知（AoC） MMI
——容量配置参数（CCP） MMI
——PLMN 选择器 MMI
——小区广播消息识别符（CBMI） MMI
——1 级组识别符（GID1） MMI/ME
——2 级组识别符（GID2） MMIME
——业务运营者名称（SPN） ME
——语音群呼业务（VGCS） MMI/ME
——语音广播业务（VBS） MMI/ME
——增强型多优先级及预占（eMLPP） MMI/ME
——解网络个人化控制密钥 ME

f）与 SIM 卡应用工具箱有关的程序
——通过 SMS-CB 下载数据（CBMID） NET
——通过 SMS-PP 下载数据 NET
——菜单选择 MMI
——呼叫控制 MMI/ME/NET
——预激活 SIM 卡 MMI/ME/NET

为了执行 c），d）和 e）的程序，需要 b）所列出的基本程序。其中 c）和 d）所列出的程序为必选项，若 e）所列的程序与 SIM 卡提供的业务相关，为可选项。

若程序与 SIM 卡业务表规定的业务有关，只有相应的 bit 指明这种业务“ 已配置和以激活 ”时（按照 EF_{SST}）才能执行该程序。其它情况不执行程序。

11．1 通用程序

11．1．1 读 EF

ME 选择 EF 并发送一个 READ 命令，包括要读出数据的位置。若已满足了 READ 的访问条件，SIM 卡向 ME 发送被读的 EF 数据。若条件不满足，则 EF 中的数据不变，且返回一个错误码信息。

11．1．2 更新 EF

ME 选择 EF 并发送一个 UPDATE 命令，包括要更新数据的位置和将要存储的新数据。若已满足了 UPDATE 的访问条件，则 SIM 用命令中的数据替代在 EF 中的原有数据从而更新选中的 EF。若条件不满足 UUPDATE 的访问条件，则 EF 中的数据不变，新的数据将不存储，且返回一个错误码信息。

11．1．3 增加 EF

ME 选择 EF 并发送一个 INCREASE 命令，包括必须添加到最后跟新/增加的记录的内容上的值。若已满足了 INCREASE 的访问条件，SIM 卡用命令中的数据增加 EF 的原有数据值，而后将结果存储起来。若不能满足 INCREASE 访问条件，则原有的 EF 的数据不变，且返回一个错误码信息。

注 :在以上程序中运作的 EF 数据的识别方式已规定在命令之中。对于 11.1.1 和 11.1.2 中的程序数据可先用 SEEK 命令识别。例如，对于一个 α 图样进行搜索。

11．2 SIM 卡管理程序

即使第一阶段 SIM 卡不符合全部第二阶段的必选项要求，第二阶段的 ME 也支持所有符合第一阶段必选项要求的 SIM 卡。此外，第二阶段 MEs 应考虑与第一阶段 SIMs 的潜在的不兼容性，这种不兼容性是由于使用不适当的命令或响应数据的错误解释而造成的。

11．2．1SIM 卡的初始化

在 SIM 卡激活之后，ME 选择专用文件 DF_{GSM} 并发出首选语言请求。若这个 EF 不可用或 ME 不支持在 EF 中的语言，则 ME 选择一个缺省语言，然后运行 CHV1 验证程序。

若成功地执行了 CHV1 的验证程序，则 ME 运行 SIM 卡阶段请求程序。若 ME 确定 SIM 卡是第一阶段的 SIM 卡，则将忽略下面与 FDN 相关的程序并继续运行管理信息请求程序。此时，ME 可以忽略在第一阶段中没有定义的程序，如 HPLMN 搜索周期请求程序。

对于第二阶段 SIM 卡，只有满足下列条件之一，GSM 操作才能开始。

- 若 EF_{IMSI} 和 EF_{LOCI} 有效，则 GSM 操作立即启动。
- 若使 EF_{IMSI} 和 EF_{LOCI} 无效，则 ME 恢复这两个文件（EFs）

如果 ME 没有 FDN 能力将不能恢复 EF_{IMSI} 和 EF_{LOCI}，因此，就不能访问这些 EFs。GSM 操作将被禁止。这种机制是通过对这种业务的 SIM 卡的应用去控制 NO.3 业务的。这种业务总是至少在下一个命令选择两个 EF 中的一个 EF 之前，失效两个 EF，见附录 D。

若 FDN 能力程序指示为：

a）在 SIM 卡中已配置和激活了 FDN，并且将 FDN 设置为 “ 使能 ”，即 ADN 无效或未激活，而 ME 还是支持 FDN 功能；或 b）FDN 在 SIM 卡中已配置并激活，而且 FDN 设置为 “ 不使能 ”，即 ADN 有效；或 c）FDN 未配置和未激活。则 GSM 操作应该启动。而在所有其它情况下 GSM 操作将不启动。之后，ME 运行下列程序：

管理信息请求

SIM 卡业务表请求

IMSI 请求

访问控制条件请求

HPLMN 搜索周期请求

PLMN 选择器请求
位置信息请求
密钥请求
BCCH 信息请求
禁用 PLMN 请求
这样 SIM 卡成功地完成了初始化工作。MS 准备进行 GSM 对话。

11．2．2 GSM 对话终止
注：这个程序不能与去活程序相混淆。
GSM 对话由 ME 终止。
ME 要运行所有必要的程序将以下用户相关的信息传递给 SIM 卡：
位置信息更新
密钥更新
BCCH 信息更新
计费通知增加
禁用 PLMN
一旦 SIM 卡表示已完成这些程序，同时去活 ME/SIM 链路。
最后，ME 从存储器中删除所有与用户相关的信息单元。
注：ME 在 GSM 对话期间已经更新了与用户相关的信息，直到 GSM 对话终止，其值没有变化，可略去各自更新程序。

11．2．3 语言优先权
请求：ME 用 EF_{LP} 执行读出程序
更新：ME 用 EF_{LP} 执行更新程序

11．2．4 管理信息请求
ME 用 EF_{AD} 执行读出程序

11．2．5 SIM 卡业务表请求
ME 用 EF_{SST} 执行读出程序。

11．2．6 SIM 卡阶段请求
ME 用 EF_{PHASE} 执行读出程序

11．2．7 SIM 卡存在的检查
SIM 卡存在的检查，作为一种附加机制。为了保证 SIM 卡在一个对话期间不被移出，ME 在每次呼叫期间频繁地发出 STATUS 命令。其间隔不超过 30s。若响应数据不是当前 DF 的响应数据，则呼叫应立刻终止。除了用机器或设备检查 SIM 卡的移出之外，否则必须采用此程序。

11．3 CHV 有关的程序
下面程序的成功完成授予了 GSM 对话相应的 CHV 的访问权。这个访问权对 GSM 应用中所有受该 CHV 保护的文件都是有效的。
当连续 3 次校验 CHV 出现错误后，CHV 状态处于“ 闭锁 ”状态，先前由这个 CHV 授

予的访问权立刻失去。

若下述任何一个程序没有成功地被完成或失败则不授予访问权。

11．3．1 CHV 验证

ME 检查 CHV 状态，若为“ 闭锁 ”状态，则终止程序。

若 CHV 状态处于“ 解锁 ”状态，则 ME 读出 CHV 使能/不使能指示器。若设置为“ 不使能 ”，则完成程序。

若 CHV 状态处于“ 解锁 ”状态而且使能/不使能指示器设置为“ 使能 ”，则 ME 利用 VERIFY CHV 功能。若 ME 提供的 CHV 与存储在 SIM 卡中的 CHV 相同，则完成程序。若 ME 提供的 CHV 与存储在 SIM 卡中的 CHV 不相同，则终止程序。

11．3．2 CHV 值更新

ME 检查 CHV 状态，若 CHV 状态为闭锁或不使能，则终止程序。

若 CHV 状态处于“ 闭锁 ”状态而且使能/不使能指示器设置为“ 使能 ”，则 ME 利用 CHANGE CHV 功能。若 ME 提供原来的 CHV 与 SIM 卡中存储的 CHV 相同时，则 ME 提供新的 CHV 替代存储在 SIM 卡之中的 CHV，完成程序。

若 ME 提供的原来的 CHV 与 SIM 卡中存储的 CHV 不相同，则终止程序。

11．3．3 CHV 不使能

要求：业务 NO.1“ 已配置及已激活 ”。

ME 检查 CHV1 状态，若 CHV1 状态处于“ 闭锁 ”状态，则终止程序。

若 CHV1 为“ 解锁 ”状态，则 ME 读出 CHV1 使能/不使能指示器。若为“ 不使能 ”状态时，则终止程序。

若 CHV1 为“ 解锁 ”状态，而且，使能/不使能指示器设置为“ 使能 ”，则 ME 采用 DISABLE CHV 功能。若 ME 提供 CHV1 与 SIM 卡中存储的 CHV1 相同时，则 CHV1 状态置于“ 不使能 ”，完成程序。若不相同，则终止程序。

11．3．4 CHV 使能

ME 检查 CHV1 状态，若 CHV1 状态处于“ 闭锁 ”状态，则终止程序。

若 CHV1 为“ 解锁 ”状态，则 ME 读出 CHV1 使能/不使能指示器。若为“ 使能 ”状态时，则终止程序。

若 CHV1 为“ 解锁 ”状态，而且，使能/不使能指示器设置为“ 不使能 ”，则 ME 采用 ENABLE CHV 功能。若 ME 提供 CHV1 与 SIM 卡中存储的 CHV1 相同时，则 CHV1 状态置于“ 使能 ”，完成程序。若不相同，则终止程序。

11．3．5 CHV 解锁

CHV 解锁程序的执行不取决于相应的 CHV 状态，即在闭锁或不闭锁状态均可。

ME 检查 UNBLOCK CHV 状态，若 UNBLOCK CHV 为“ 闭锁 ”状态，则终止程序。

若 UNBLOCK CHV 状态处于“ 解锁 ”状态，则 ME 采用 UNBLOCK CHV 功能；若 ME 提供的 UNBLOCK CHV 与 SIM 卡中存储的 UNBLOCK CHV 相同，则有关的 CHV 状态变成“ 解锁 ”状态，完成程序；若不相同，终止程序。

11．4 与 GSM 安全有关的程序

11．4．1 与 GSM 算法有关的程序

ME 选择 DF_{GSM} 并运行 RUN GSM ALGORITHM 功能。当用后面跟随的 GET RESPONSE 命令请求时，将响应 SRES-Kc 发给 ME。

11．4．2 IMSI 请求

ME 利用 EF_{IMSI} 执行读出程序

11．4．3 访问控制请求

ME 利用 EF_{ACC} 执行读出程序

11．4．4 HPLMN 搜索周期请求

ME 利用 EF_{HPLMN} 执行读出程序

11．4．5 位置信息

请求：ME 利用 EF_{LOCI} 执行读出程序

更新：ME 利用 EF_{LOCI} 执行更新程序

11．4．6 密钥

请求：ME 利用 EF_{KC} 执行读出程序

更新：ME 利用 EF_{KC} 执行更新程序

11．4．7BCCH 信息

请求：ME 利用 EF_{BCCH} 执行读出程序

更新：ME 利用 EF_{BCCH} 执行更新程序

11．4．8 禁用 PLMN

请求：ME 利用 EF_{FPLMN} 执行读出程序

更新：ME 利用 EF_{FPLMN} 执行更新程序

11．5 签约相关程序

11．5．1 拨打号码

下面过程不仅适合于 EFADN 和它的有关扩展文件 EFCCP 及 EFEXT1，也适合于 EFFDN，EFMSISDN，EFLND 以及与它们相关的扩展文件程序。若这些文件没有配置及激活，则当前程序失败且 EFs 应维持不变。

例如：一个适合 ADN 的程序

要求：业务 NO.2 “ 已配置和已激活 ”

（FDN 为 NO.3，MSISDN 为 NO.9，LND 为 NO.13）

更新：ME 把下面要存储的信息进行分解和集合（下面使用的字节识别符按 EF_{ADN}，EF_{CCP}，EF_{EXT1} 所采用的标识符）

a） ME 识别 α 识别符，能力/配置识别符和扩展/记录识别符。

b） 分析拨号号码/SSC 串并将其分配给 EF 的字节；

若出现 “ + ” 符，则 TON 设置为 “ 国际 ”；

若维持在 20 或低于 20 位将形成拨号号码/SSC 串；

若超过 20 位，应执行下列程序。

请求：

业务 NO.10，“ 配置并激活 ”（ 业务 NO.10 也适合 MSISDN 和 LND；业务 NO.11 为 FDN）。

ME 在 EFEXT1 找到一个空的记录。若扩展 1 记录没有标出 “ 空的 ”，则 ME 运行清除程序；若扩展 1 记录仍处于不可用，则终止程序。

首先，在拨号号码/SSC 串中存储 20 位，BDC 号码/SSC 内容的长度值设置最大值为 11 字节。这个扩展 1 记录识别符是用与在 EFEXT1 中相关的记录号码编码，其余位存储在已

选择的扩展 1 记录中，记录的类型设置为 “ 益出数据 ”。扩展 1 记录的第一个字节设置为剩下的溢出数据字节的数量，包括位信息的字节的数量是 EFADN 的 BCD 号码/SSC 内容的长度和所有包括溢出数据的有关的已连接的扩展 1 记录的字节 2 的长度之和

c） 若被叫用户子地址与 AND/SSC 有关，则将执行下列程序：

请求 :业务 NO.10，“ 配置并激活 ”（ 业务 NO.10 也适合 MSISDN 和 LND ;业务 NO.11 为 FDN）。

若被叫用户子地址的长度低于或等于 11 字节，ME 在 EFEXT1 中寻找空记录；若扩展 1 的记录没有标为 “ 空的 ” 标记，ME 运行删除程序；若扩展 1 记录仍然不可利用，则终止程序。

ME 在扩展 1 记录中存储被叫用户子地址,并设置扩展 1 记录类型为‘ 被叫用户子地址 ”。

若被叫用户子地址长度大于 11 字节，ME 在 EFEXT1 中寻找两个空记录；若没有找到，ME 运行删除程序；若两个扩展记录仍然不可用，则 ME 终止程序。

ME 将被叫用户子地址存储在两个扩展 1 记录中，当包括子地址数据的第一部分和包括子地址数据的第二部分时，则利用与 EF_{EXT1} 有关的记录号码编码扩展 1 记录。两个扩展 1 记录类型均设置为 “ 被叫用户子地址 ”。

一旦考虑了 a)、b)、c）ME 用 EFADN 执行更新程序，若 SIM 卡没有剩余空间去存储接收到的 AND/SSC 或程序已经终止，则 ME 通知用户。

注 :出于存储器效率的原因，允许 ME 分析全部的扩展 1 记录以确认要存储的溢出数据或子地址数据是否已经存储与 EF_{EXT1} 之中。在这种情况下，ME 可以利用现有的链路或多于一个 ADN（LND，MSISDN）中的现有的链路的最后的部分。只允许 ME 在空的记录中存储扩展数据。若现有的记录用于多方访问，则 ME 不改变在这些数据中任何数据以防止现有的链路中断。

删除：ME 发送要删除的信息识别方式。EF_{ADN} 中的已识别记录内容标记为 “ 空的 ”。

请求：ME 发送要读出的信息的识别方式。ME 应分析 EFADN 的数据以确定附加数据是与 EF_{EXT1} 相关还是与 EF_{CCP} 相关。如果必要，则 ME 在这些 EFs 上执行读出程序以集合完整的 ADN/SSC。

清除：ME 应该访问每个参考 EF_{EXT1}（EF_{EXT2}）来存储 EF 并且应该识别这些文件中采用扩展数据（溢出数据或被叫用户子地址）的那些记录。应注意现有链路必须跟踪到末端。所有归因于扩展 1 记录的均由 ME 注明，而所有的不注明的扩展 1（扩展 2）记录由 ME 通过设置整个记录为 ‘ FF ’ 来标记为 “ 空的 ”。

注：有可能将扩展 1 记录标记为 “ 占用 ”（不等于 ‘ FF ’），即使实际上它们不再与一个 AND/SSC 记录有关，但是依赖于 ME 的实现方式，特别是由第一阶段 MEs 删除 AND/SSC 记录的可能性，因为第一阶段的 ME 对 EF_{EXT1} 不认识。

下面 3 种程序只应用于 NO.3（FDN）：

FDN 能力请求。ME 必须对业务 NO.3 的状态进行检查，即是否 FDN 为 “ 使能 ” 或 “ 不使能 ” 状态。在 FDN 使能情况，ME 必须转换到限制式中断方式。为了确认 FDN 的状态，ME 要在 EFSST 中检查 ADN 是否已激活。若 ADN 没有激活，则业务 NO.3 使能；若已激活，则 ME 检查 EFSST 的响应数据；若 EFADN 失效，则业务 NO.3 使能；在其它情况下，业务 NO.3 是不使能的。

FDN 不使能。FDN 使能程序要求成功地执行 CHV2 验证程序和激活 ADN。若没有，则 FDN 不使能程序将不能成功地饿完成。为了不使能 FDN，则 ME 恢复 EFADN。EFADN 的无效/恢复标识是和业务 NO.3 的状态指示器同时由 REHABILITATE 命令隐含设置的。若 ADN 未激活,FDN 的不使能是不可能的,因此业务 NO.3 总是被使能的(见 FDN 能力请求)。

注：若采用一个管理终端 FDN 不使能（恢复 EFADN）时，则这个管理终端的 FDN 不

使能程序也需要恢复 EFIMSI 和 EFLOCI，以保证 SIM 卡在第一阶段的 ME 或第二阶段不支持 FDN 的 ME 中的正常运作。

FDN 使能。FDN 使能程序要求 CHV2 验证程序已经成功执行。若没有，则 FDN 使能程序将不能成功地完成。为了使能 FDN，ME 使 EFADN 失效。EFADN 的无效/恢复标识是和业务 NO.3 的状态指示器同时由 INVALIDATE 命令隐含清除的。若 ADN 未激活，NO.3 总是被使能的。

11．5．2 短消息

要求：业务 NO.4 “ 配置及激活 ”

请求：SIM 卡寻找已识别的短消息。若找到，ME 用 EFSMS 执行读出程序。若在 SIM 卡存储器中没有找到这个消息，则 SIM 卡向 ME 发出指示。

更新：ME 寻找关于下一个可利用的空间以存储短消息，若有可利用的空间，则 ME 利用 EFSMS 执行更新程序。

若在 SIM 卡中没有可利用的空间以存储接收的短消息，则为了不丢失消息，必须设置一个特定的 MMI。

删除：ME 在 SIM 卡中选择要删除的短消息空间。根据 MMI 的要求，在存储区标做“ 空的 ”之前可以读出消息，在用 EFSMS 执行更新程序之后，分配给这个短消息的 SIM 存储空间可用于新来的消息。SIM 卡的存储器中仍然含有原来的消息直到这个空间已存储了新的消息为止。

11．5．3 计费通知（AoC）

要求：业务 NO.5 “ 配置及激活 ”

累加呼叫表（ACM）

请求：ME 用 EFACM 执行读出程序。SIM 卡返回 ACM 最后的更新数值。

初始化：ME 用新的初始值以 EFACM 执行更新程序。

增加：ME 发送被增加的值，用 EFACM 执行增加程序。

累加呼叫表最大值（ACM）

请求：ME 用 EF_{ACMmax} 执行读出程序。

初始化：ME 用新的初始最大值以 EF_{ACMmax} 执行更新程序。

单价和货币表（PUCT）

请求：ME 用 EF_{PUCT} 执行读出程序

更新：ME 用 EF_{PUCT} 执行更新程序

11．5．4 能力配置参数

要求：业务 NO.6 “ 配置及激活 ”

请求：ME 用 EF_{CCP} 执行读出程序

更新：ME 用 EF_{CCP} 执行更新程序

删除：ME 向 SIM 卡发送将要删除的请求信息识别。在 EFCCP 中的已识别记录的内容标记为 “ 空的 ”。

11．5．5 PLMN 选择器

要求：业务 NO.7 “ 配置及激活 ”
请求：ME 用 $EF_{PLMNsel}$ 执行读出程序
更新：ME 用 $EF_{PLMNsel}$ 执行更新程序

11．5．6 广播消息识别符
要求：业务 NO.14 “ 配置及激活 ”
请求：ME 用 EF_{CBMI} 执行读出程序
更新：ME 用 EF_{CBMI} 执行更新程序

附录A

SIM卡中的α标识符区使用的编码——UCS2编码

如果 16bit 的 UCS2 字符被用在α标识符区，则编码格式一定采用三种格式之一。如果 ME 支持 SIM 卡中的采用 UCS2 编码的α标识，则 ME 就应该支持所有的三种编码方案：字符数量为 128 个字符或少于 128 个字符；字符数量多于 128 个字节，ME 至少支持第一种编码方案。如果含有α字符的记录只含有 GSM 默认的α字符，则不会使用三种编码方案中的

任何一种。在一个记录中，只有一种编码方案被使用，GSM 的默认α字符或者下列描述的三种方案之一：

1） 如果第一个八位位组α字符串是‘ 80 ’，则剩下的八位位组串是 16bit 的 UCS2 字符，低位的八位位组要比高位的八位位组更有意义。不用的八位位组置为‘ FF ’，

例 1

Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7	Octet 8	Octet 9
'80'	$Ch1_{MSO}$	$Ch1_{LSO}$	$Ch2_{MSO}$	$Ch2_{LSO}$	$Ch3_{MSO}$	$Ch3_{LSO}$	FF	FF

2) 如果第一个八位位组α字符串是‘ 81 ’, 则第二个八位位组指示字符串中的字符数量，第三个八位位组组成16bit的基址指针用于后续字节，编码为‘ 0xxx xxxx x000 0000 ’， 第四个和后续的八位位组，如果bit8为0则剩余的7个bit表示GSM默认的α字符，如果bit8为1则剩余的7个bit表示偏移地址（用于加上16bit的基址：结果为UCS2代码指针）

例 2

Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7	Octet 8	Octet 9
'81'	‘ 05 ’	‘ 13 ’	‘ 53 ’	‘ 95 ’	‘ A6 ’	‘ XX ’	‘ FF ’	‘ FF ’

上例中：

- Octet 2表示字符串中有5个字符。
- Octet 3 基址指针，孟加拉字符开始位置为 0980（0000 1001 1000 0000）
- Octet 4 GSM默认的α字符，‘ 53 ’ 表示 “ S ”。
- Octet 5 指示UCS2字符集基址指针的偏移地址‘ 15 ’，α字符的地址为‘ 0995 ’，孟加拉文字为KA
- Octet 8 的值为‘ FF ’，但是由于字符串的长度是5，所以这是一个有意义的数值，指示α字符的地址为‘ 09FF ’。

2） 如果第一个八位位组α字符串是‘ 82 ’，则第二个八位位组指示字符串中的后续字符数量，第三个和第四个八位位组16bit的基址指针用于后续字节，后续字节编码同第二种情况。

例3

Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7	Octet 8	Octet 9
'82'	‘ 05 ’	‘ 05 ’	‘ 30 ’	‘ 2D ’	‘ 82 ’	‘ D3 ’	‘ 2D ’	‘ 31 ’

上例中：

- Octet 2表示字符串中有5个字符。
- Octet 3 Octet 4基址指针，亚美尼亚字符开始位置为 0530
- Octet 5 GSM默认的α字符，‘ 2D ’ 表示 “ * ”。
- Octet 6 指示UCS2字符集基址指针的偏移地址‘ 02 ’，α字符的地址为‘ 0532 ’， 表示亚美尼亚的首都 BEN
- Octet 7 的值为‘ D3 ’， 指示UCS2字符集基址指针的偏移地址‘ 53 ’，α字符的地址为‘ 0583 ’， 表示亚美尼亚字符小的 PIWR。

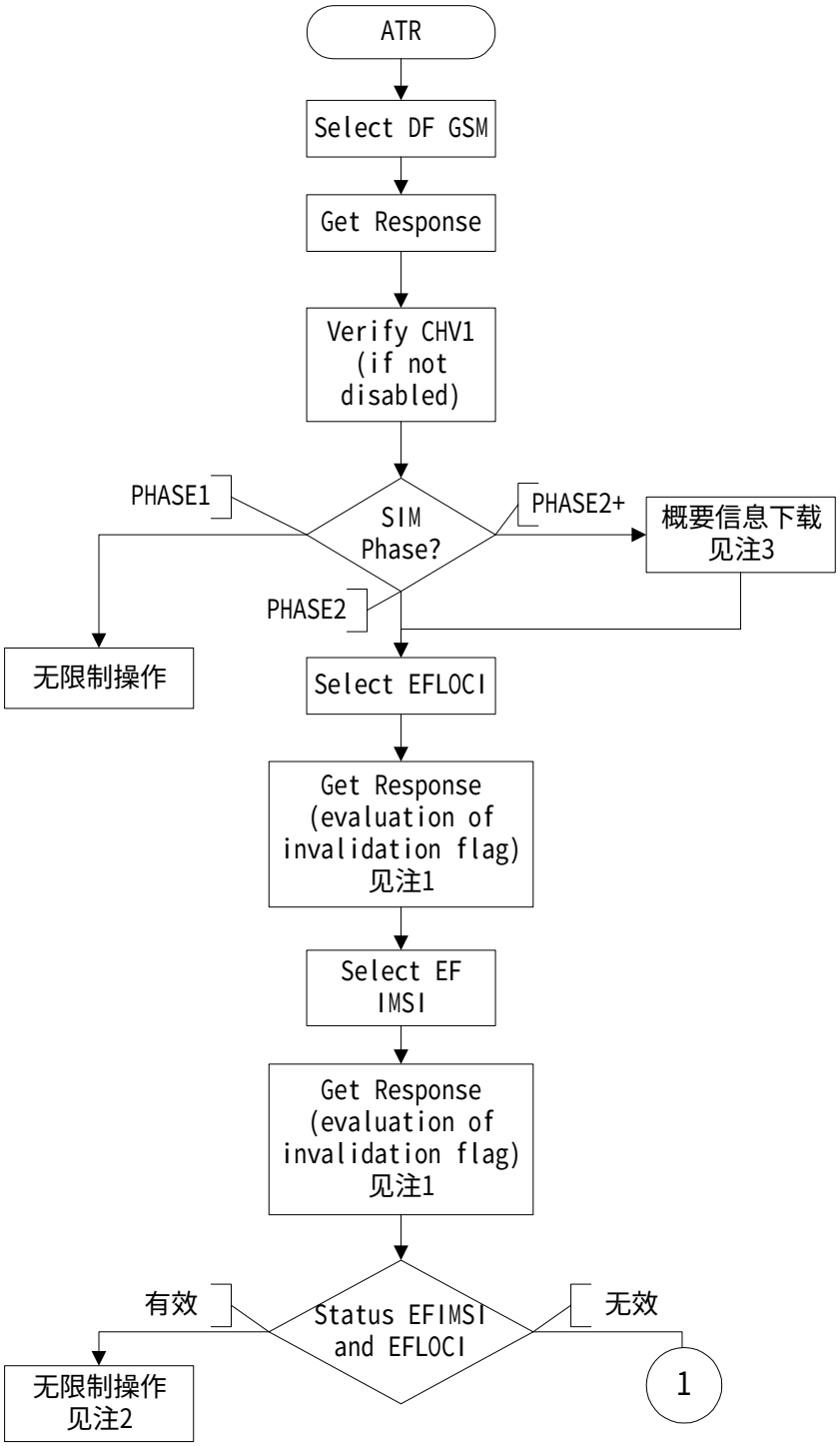
附录B

EFs预个人化建议值

文件标识符	描述	值
‘ 2FE2 ’	ICC标识符	网络运营商决定
‘ 2F05 ’	扩展语言选择	‘ FF…FF ’
‘ 6F05 ’	语言选择	‘ FF ’

‘ 6F07 ’	IMSI	网络运营商决定
‘ 6F20 ’	密钥Kc	‘ FF…FF 07 ’
‘ 6F30 ’	PLMN选择器	‘ FF…FF ’
‘ 6F31 ’	HPLMN搜索周期	‘ FF ’
‘ 6F37 ’	ACM最大值	‘ 000000 ’
‘ 6F38 ’	SIM卡业务表	网络运营商决定
‘ 6F39 ’	累加呼叫表	‘ 000000 ’
‘ 6F3E ’	分组识别符1	网络运营商决定
‘ 6F3F ’	分组识别符2	网络运营商决定
‘ 6F41 ’	PUCT	‘ FF FF FF 00 00 ’
‘ 6F45 ’	CBMI	‘ FF…FF ’
‘ 6F46 ’	网络提供商名称	‘ FF…FF ’
‘ 6F48 ’	CBMID	‘ FF…FF ’
‘ 6F74 ’	BCCH信息	‘ FF…FF ’
‘ 6F78 ’	接入等级	网络运营商决定
‘ 6F7B ’	禁用的PLMNs	‘ FF…FF ’
‘ 6F7E ’	位置信息	‘ FFFFFFFF xxxxxx 0000 FF 01 ’
‘ 6FAD ’	管理数据	网络运营商决定
‘ 6FAE ’	阶段识别符	网络运营商决定
‘ 6F51 ’	网络报警指示	‘ FF…FF ’
‘ 6F52 ’	GPRS密钥KcGPRS	‘ FF…FF 07 ’
‘ 6F53 ’	GPRS位置信息	‘ FFFFFFFF FFFFFF xxxxxx 0000 FF 01 ’
‘ 6F54 ’	SetUpMenu 元素	网络运营商决定
‘ 6F3A ’	缩位拨号	‘ FF…FF ’
‘ 6F3B ’	固定拨号	‘ FF…FF ’
‘ 6F3C ’	短消息	‘ 00 FF…FF ’
‘ 6F3D ’	能力配置参数	‘ FF…FF ’
‘ 6F40 ’	MSISDN存储	‘ FF…FF ’
‘ 6F42 ’	短消息参数	‘ FF…FF ’
‘ 6F43 ’	短消息状态	‘ FF…FF ’
‘ 6F44 ’	末位拨号	‘ FF…FF ’
‘ 6F4A ’	扩展1	‘ FF…FF ’
‘ 6F4B ’	扩展2	‘ FF…FF ’
‘ 6F4C ’	扩展3	‘ FF…FF ’
‘ 6F4D ’	禁止拨号	‘ FF…FF ’
‘ 6F4E ’	扩展4	‘ FF…FF ’

附录C
FDN/BDN程序

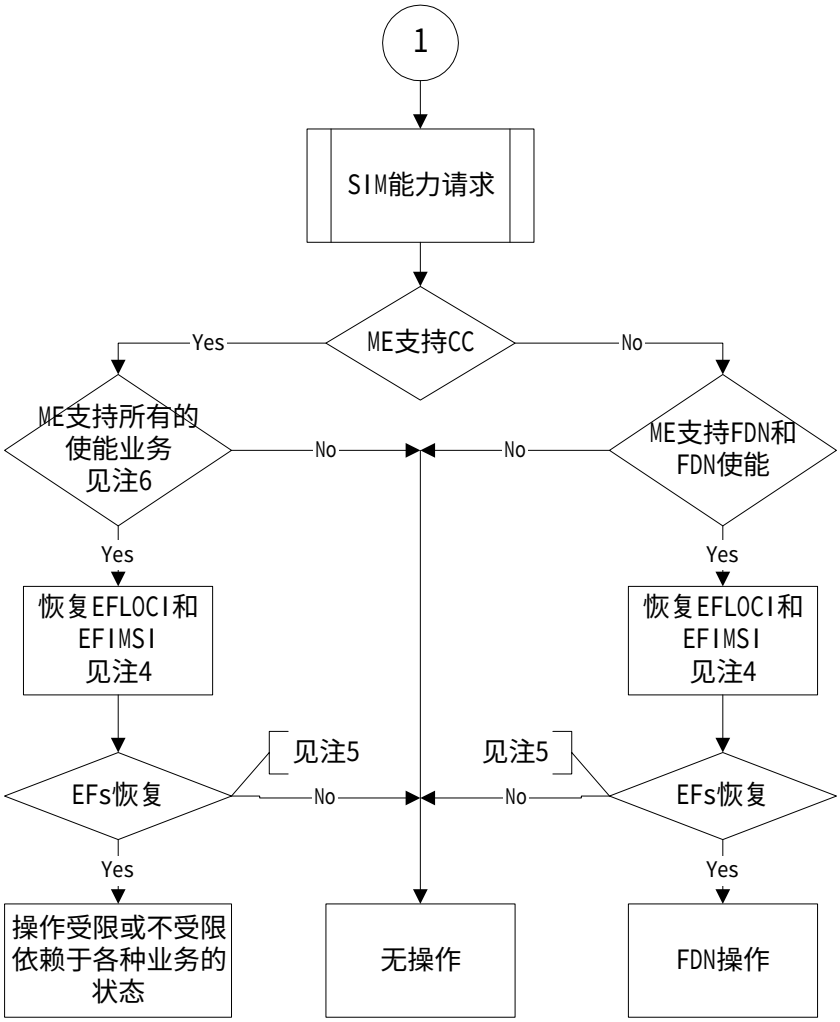


图C1 FDN/BDN初始化程序实例

注1：在已激活FDN和/或BDN的情况下，SIM卡在这级之前就已经失效了当前的EF

注2：对于FDN和BDN，不能只失效两个EF中的一个文件

注3：对于具有已使能的FDN的SIM卡，本程序用于检查ME是否有SIM卡设备提供的呼叫控制。



图C2 FDN/BDN 初始化程序实例

注4：在BDN已使能的情况下，若ME向SIM卡指示了CC能力（用PROFILE DOWNLOAD），则SIM卡允许恢复EF_{IMSI}和EF_{LOCI}文件。

注5：采用SIM卡失效的内部机制为今后“受限”业务提供可能性。

注6：若ME对全部已使能业务不给予支持（例如：FDN、BDN），则停止操作。在BDN使能的情况下，ME只需支持“呼叫控制特性”便满足运作要求。今后可能增加新的“授限”业务，对ME是未知的。在这种情况下，ME将执行恢复的子序列程序，但不能恢复EF_{IMSI}和EF_{LOCI}。

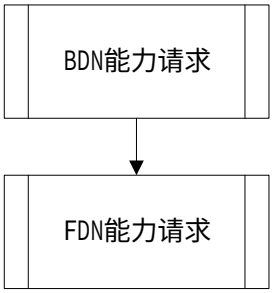
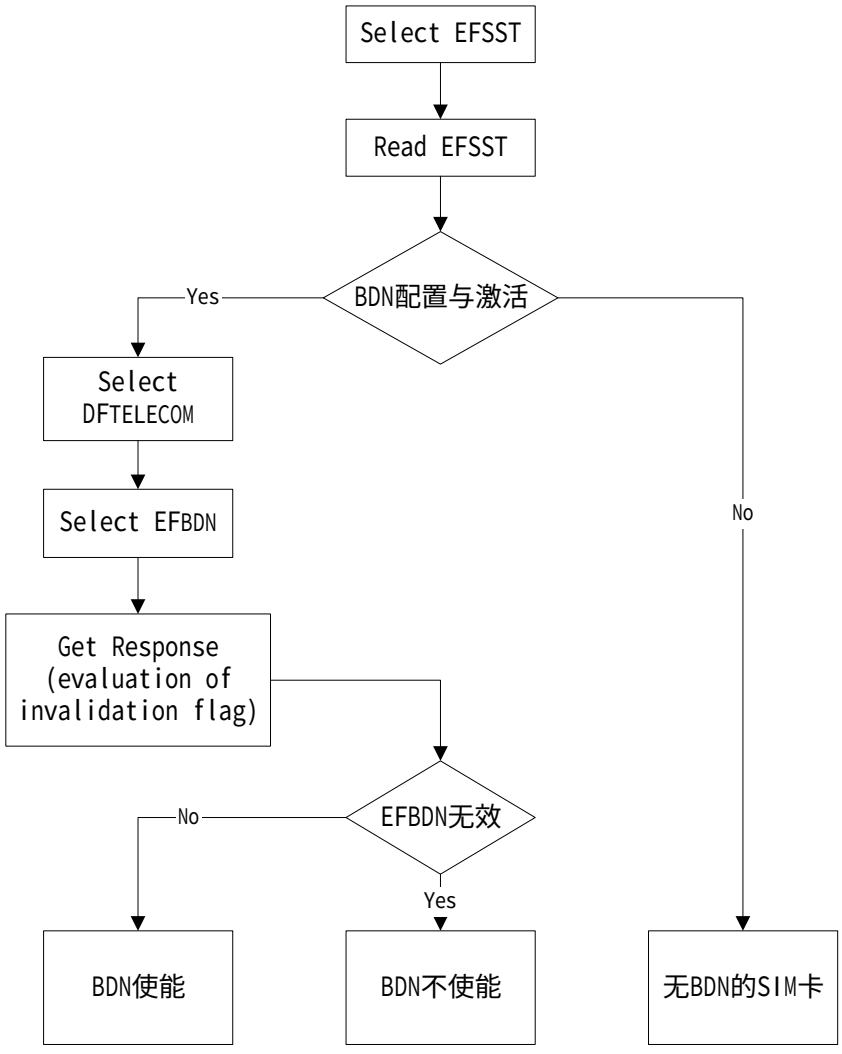
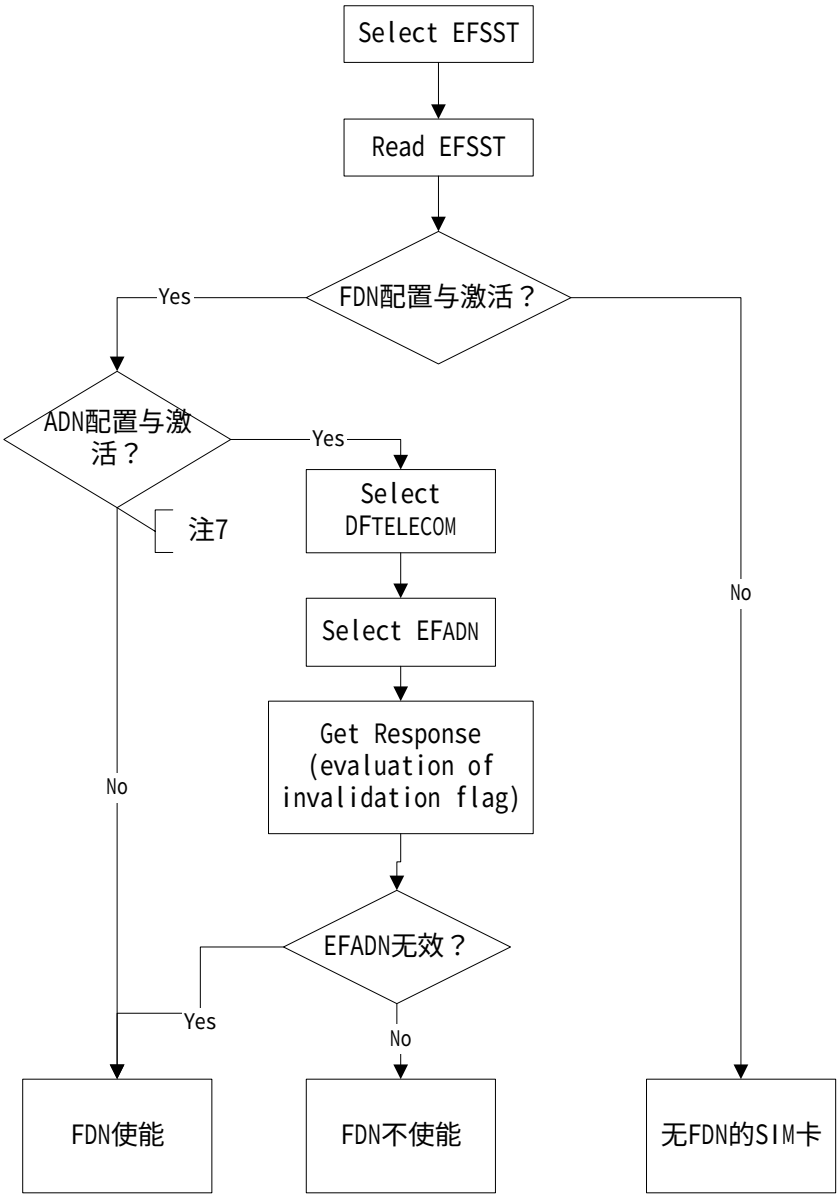


图 C3 SIM卡能力请求

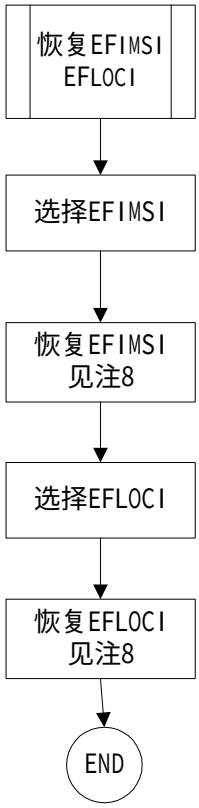


图C4 BDN能力请求



注7：在这种情况下没有不使能FDN的可能性。

图C5 FDN能力请求



注8：若SIM卡中的BDN已使能，PROFILE DOWNLOAD程序并未指示ME支持“呼叫控制”，则SIM卡不能恢复该EF。

图6 执行恢复GSM文件的程序