BD

中国第二代卫星导航系统重大专项标准

BD 430077.1—2022

北斗三号区域短报文通信用户终端接口规范 第 1 部分：用户管理模块

Interface specifications of BDS-3 regional short message communication user terminal— Part 1：User management module

2022-12-30 发布　　2023-01-30 实施

中国卫星导航系统管理办公室 批准

目　　次

前　言

本文件是BD 430077《北斗三号区域短报文通信用户终端接口规范》的第1部分。BD 430077已经发布了以下部分：

——第 1 部分：用户管理模块；

——第 2 部分：通用数据接口。

本文件由中国卫星导航系统管理办公室提出。

本文件由全国北斗卫星导航标准化技术委员会（SAC/TC 544）归口。

本文件起草单位：中兵北斗应用研究院有限公司、中国卫星导航工程中心、中国信息通信研究院技术与标准研究所、中国移动上海产业研究院、中电华大电子设计有限责任公司、武汉天喻信息产业股份有限公司、中国电子科技集团第五十四研究所、广州海格通信集团、中国兵器工业计算机应用技术研究所、博鼎实华（北京）技术有限公司。

本文件主要起草人：胡　江、潘　颖、胡光明、周　益、王　超、徐湖伟、吴智雄、郑海霞、李　罡、汪陶胜、李晓峰、李　安、赵　勇、李胜昌、曾　帅、乔　阳、王晓玲、钟世广、黄荷仙、赵　悟、赵敬超。

北斗三号区域短报文通信用户终端接口规范

第 1 部分：用户管理模块

1 范围

本文件规定了北斗三号区域短报文通信用户终端用户管理模块的功能与组成、物理接口、电气特性、传输协议、应用文件、应用命令集和命令说明等。

本文件适用于北斗三号区域短报文通信用户终端和用户管理模块的设计、研制、测试和应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 16649.1-2006 识别卡 带触点的集成电路卡 第1部分：物理特性

GB/T 16649.2-2006 识别卡 带触点的集成电路卡 第2部分：触点的尺寸和位置

GB/T 16649.3-2006 识别卡 带触点的集成电路卡 第3部分：电信号和传输协议

GB/T 16649.4-2010 识别卡 集成电路卡 第4部分：用于交换的结构、安全和命令

GB/T 20276-2016 信息安全技术 具有中央处理器的IC卡嵌入式软件安全技术要求

GB/T 22186-2016 信息安全技术 具有中央处理器的IC卡芯片安全技术要求

GB/T 39267 北斗卫星导航术语

JR/T 0025.1-2010 中国金融集成电路（IC）卡规范 第1部分：电子钱包/电子存折应用卡片规范

ISO/IEC 7816-1-2003 识别卡-带触点的集成电路卡 第1部分：物理特性（Identification cards — Integrated circuit cards — Part 1: Physical characteristics）

ETSI TS 102.221 V16.4.0 智能卡；UICC-终端接口；物理和逻辑特性（第16版）（Smart Cards; UICC-Terminal interface; Physical and logical characteristics（Release 16））

3 术语和定义、缩略语

3.1 术语和定义

GB/T 16649.1、GB/T 16649.2、GB/T 16649.3、GB/T 16649.4和GB/T 39267界定的以及下列术语和定义适用于本文件。

3.1.1

区域短报文通信 regional short message communication；RSMC

一种通过北斗GEO卫星在一定覆盖区域范围内，为用户提供短报文通信、应急搜救和位置报告的通信服务。

3.1.2

用户管理模块　user management module

一种为北斗三号区域短报文通信用户终端提供用户身份认证和短报文信息加解密功能的模块，通过加载不同的软件和数据支持普通型用户终端和管理型用户终端，也可称为北斗专用USIM卡或北斗USIM卡。

3.1.3

普通型用户终端　user terminal

一种可接收广播信息、通播报文、组播报文和点播报文，可发送点播报文和组播报文的终端设备，也可称为用户终端或用户机。

3.1.4

管理型用户终端　management terminal

一种具备用户终端所有功能，并能发送通播报文和兼收下级用户机所有点播报文的终端设备，也可称为管理型终端或管理机。

3.1.5

点播 ID　unicast ID

北斗三号区域短报文系统为用户终端分配的点播地址，即用户ID。用户终端之间可通过点播地址进行点对点通信。

3.1.6

组播 ID　multicast ID

北斗三号区域短报文系统为每一个组分配的唯一地址，处于一个组的用户均可发送组播报文，并可接收到所有其他组内用户发送的组播报文。

3.1.7

通播 ID　communicast ID

北斗三号区域短报文系统为管理型终端分配的通播地址，管理型终端可通过该通播地址发送通播报文，其所有下级用户机均拥有该通播地址，并通过该通播地址接收通播报文。

3.1.8

广播　broadcast

由北斗三号系统向所有区域短报文服务用户按空间接口约定发送短报文广播信息的过程。

3.1.9

认证码　authentication code

由北斗三号区域短报文通信专用USIM卡通过专用命令计算得到的，用于系统入站鉴别报文发送方身

份是否合法的22比特校验码。

3.2 缩略语

下列缩略语适用于本文件。

AAD：应用附加数据（Application Additional Data）

AID：应用标识符（Application Identifier）

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

C-APDU：命令应用协议数据单元（Command Application Protocol Data Unit）

CLA：命令报文的类别字节（Class Byte of the Command Message）

IMEI：国际移动设备识别码（International Mobile Equipment Identity）

IMSI：国际移动用户识别码（International Mobile Subscriber Identity）

INS：命令报文的命令字节（Instruction Byte of Command Message）

R-APDU：响应应用协议数据单元（Response Application Protocol Data Unit）

SW1：状态字1（Status Word One）

SW2：状态字2（Status Word Two）

USIM：通用用户识别模块（Universal Subscriber Identity Module）

4 用户管理模块功能与组成

4.1 模块组成

用户管理模块由硬件芯片、芯片操作系统、应用软件组成，其组成结构示意图见图1。

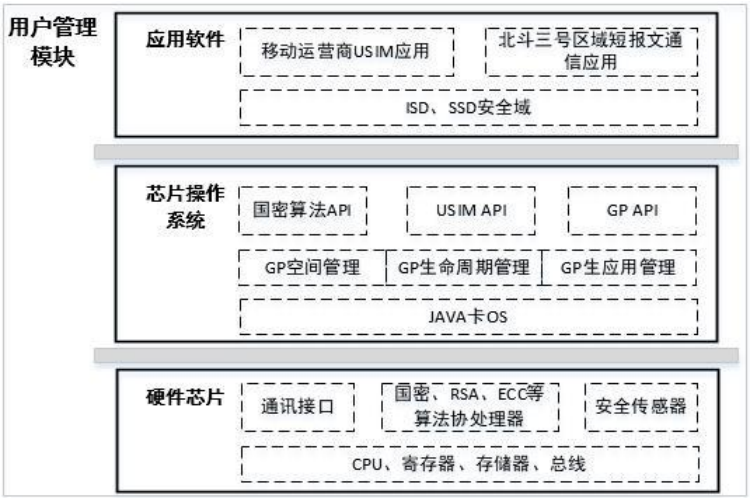

图 1 用户管理模块组成示意图

用户管理模块运行的应用软件应支持北斗三号区域短报文通信应用和移动运营商USIM应用。其中北斗三号区域短报文通信应用应支持该短报文通信服务平台要求的身份认证功能、数据加解密功能、应用信息管理功能。移动运营商USIM应用功能见运营商发布的产品功能要求。

4.2 模块功能

4.2.1 数据存储

用户管理模块应存储与北斗用户有关的用户信息和密钥数据以及民用短报文通信服务平台所需的应用信息和其他密钥数据。若用户选择开通运营商服务，用户管理模块还应存储接入运营商网络所需的文件信息和密钥数据。

4.2.2 移动运营商应用功能

若用户选择开通移动运营商服务，用户管理模块应具备接入移动运营商通信平台的能力，支持通信鉴权功能、菜单功能、文件结构和用户信息管理功能。用户可使用运营商指定的途径注册开通其提供的移动通信服务。

4.2.3 北斗三号区域短报文通信应用功能

北斗三号区域短报文通信用户管理模块应提供满足北斗三号区域短报文通信服务要求的身份认证、数据加解密、应用信息管理和终端绑定认证等功能。

5 物理接口、电气特性及传输协议

5.1 物理特性

用户管理模块除了应符合GB/T 16649.1-2006中规定的物理特性要求外，模块高度还应符合ISO/IEC 7816-1-2003中4.2.3规定的要求：

a） 模块表面的最高点不应高于卡表面平面 0.10mm。

b） 模块表面的最低点不应低于卡表面平面 0.10mm。

5.2 触点的数量和位置

用户管理模块上触点的分配按照GB/T 16649.2-2006第5章规定的8个触点，每个触点的编号按照表1中规定的要求分配。北斗三号区域短报文通信用户管理模块以USIM卡为载体，包含ID-1 USIM、Plug-in USIM、Mini-USIM、4FF形态，模块外观、尺寸和触点位置应符合ETSI TS 102.221[16]第4章规定的要求，详见附录A。

表 1 触点的分配

触点号	分配	触电号	分配
C1	电源电压（VCC）	C5	地（GND）
C2	复位信号（RST）	C6	可变电源电压（VPP） （例如编程电压）
C3	时钟信号（CLK）	C7	输入/输出（I/O）
C4	预留	C8	预留

5.3 触点的尺寸

用户管理模块触点的尺寸应符合GB/T 16649.2-2006第3章规定的要求，每个触点尺寸不应小于2mm×1.7mm，触点尺寸都应符合ETSI TS 102.221[16]第4章规定的要求，详见附录A。

5.4 电气特性

用户管理模块的触点电气特性应符合 ETSI TS 102.221[16]第 5 章规定的要求，其中模块 C1 触点供电电压支持 A，B，C 三类，见表 2 定义。本文件使用的用户管理模块触点 C1 电压应至少支持 B 和 C 两个连续的电压级别。

表 2 操作电压

符号	条件	最小值	最大值	单位
Vcc	类型 A	4.50	5.50	V
Vcc	类型 B	2.70	3.30	V
Vcc	类型 C	1.62	1.98	V

5.5 安全性

用户管理模块的硬件芯片需支持国密算法，芯片选型应选择 GB/T 20276-2016 中 5.3.3 规定的至少通过 EAL4+评测的芯片，其安全评测要求应符合 GB/T 22186-2016 规定的 EAL4+安全要求。

5.6 传输协议

5.6.1 激活和复位

用户管理模块与终端之间的传输过程首先是由终端对用户模块进行上电激活、复位开始，其过程应符合 GB/T 16649.3-2006 第 5 章规定的要求。

5.6.2 复位应答

用户管理模块被激活、复位后，向终端返回复位应答。复位应答由一系列字节组成，其格式应符合 GB/T 16649.3-2006 第 6 章规定的要求。

5.6.3 协议和参数选择

终端根据复位应答参数按照 GB/T 16649.3-2006 第 6 章规定的要求，选择终端和用户管理模块共同支持的传输协议以及传输参数。用户管理模块应支持协议 T=0（异步半双工字符传输协议）或协议 T=1（异步半双工块传输协议），其传输过程应符合 GB/T 16649.3-2006 第 8 和第 9 章规定的要求。

6 应用文件

6.1 概述

用户管理模块可以包含一个或多个应用，其应用文件结构应符合 GB/T 16649.4-2010 中 5.3 规定的要求。基本文件又分为二进制文件和定长记录文件：

a） 二进制文件的内容可以被看作一个数据单元序列，该序列可以通过读、写二进制命令访问；

b） 定长记录文件内容可被看作可独立标识的记录序列，该序列可以通过读、写记录命令访问。

6.2 用户信息文件

用户信息文件见表 3，用于存储北斗三号区域短报文通信北斗用户管理模块的用户 ID。用户 ID 是北斗三号短报文用户的唯一身份标识。

表 3 用户信息文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
用户信息文件	01h	二进制文件	6 字节	读 = 自由 写 = 维护密钥明文更新	HEX 编码，详见表 4

用户信息文件内容见表 4。

表 4 用户信息文件内容

数据项	长度（字节）	说明
用户 ID	6	北斗用户的唯一身份标识

6.3 组播信息文件

组播信息文件见表5，用于存储北斗三号短报文用户的组播信息。文件包括已加入的组播ID和已退出的组播ID，以及与组播ID关联的组播子密钥ID。有关密钥信息，参见6.9用户密钥文件。

表 5 组播信息文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
组播信息文件	02h	定长记录文件	8 * 128 字节（最多支持 128 个组播 ID）	读 = 使用 GET GROUP INFO 命令 写 = 维护密钥明文更新 写 = 使用 UPDATA GROUP ID 命令	HEX 编码，详见表 6

组播信息文件内容见表 6。

表 6 组播信息文件内容

数据项	长度（字节）	说明
组播 ID 1	6	组播 ID 1
组播 ID 1 对应 KeyID	1	组播 ID 1 对应的组播子密钥 ID
组播 ID 1 状态	1	00：表示组播 ID 1 正在使用中 01：表示组播 ID 1 已经回收，不可使用
组播 ID 2	6	组播 ID 2
组播 ID 2 对应 KeyID	1	组播 ID 2 对应的组播子密钥 ID
组播 ID 2 状态	1	00：表示组播 ID 2 正在使用中 01：表示组播 ID 2 已经回收，不可使用
……	……	……

注：组播信息文件内容缺省值为全 0。

6.4 通播信息文件

通播信息文件见表7，用于存储北斗三号短报文用户的通播信息。文件包括所属集团的通播ID、所属管理型终端（如有）的通播ID、已加入的其他通播ID，以及与通播ID关联的通播密钥ID。有关密钥信息，参见6.9用户密钥文件。

表 7　通播信息文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
通播信息文件	03h	定长记录文件	7 * 16 字节（最多支持 16 个通播 ID）	读 = 自由 写 = 维护密钥明文更新	HEX 编码，详见表 8

通播信息文件内容见表 8。

表 8　通播信息文件内容

数据项	长度（字节）	说明
通播 ID 1	6	集团通播 ID
通播 ID 1 对应 KeyID	1	通播 ID 1 对应的通播密钥 ID
通播 ID 2	6	管理型终端通播 ID
通播 ID 2 对应 KeyID	1	通播 ID 2 对应的通播密钥 ID
……	……	……

注：通播信息文件内容缺省值为全 0，该文件至少包含一组集团通播 ID。

6.5　系统参数文件

系统参数文件见表 9，用于存储北斗三号区域短报文通信用户终端工作时所需的物理参数。

表 9　系统参数文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
系统参数文件	04h	二进制文件	30 字节	读 = 自由 写 = 自由	HEX 编码，详见表 10

系统参数文件内容见表 10。

表 10　系统参数文件内容

数据项	长度（字节）	说明
搜救中心地址	6	低 24 比特有效，高 24 比特预留。
入站扩频码参数	21	终端生成入站信号需要入站扩频码，入站扩频码通过扩频码参数控制，共包括 m1、m2、m3 序列的生成多项式和初相，其中生成多项式由 4 个大小不超过 24 的十进制数组成（可用 1 个 32 比特的数据表示），初相为一个 24 比特的二进制参数。按上述表示方法，三类序列共需 168 比特。
入站频点选择参数	1	最低比特有效，即最右边 1 比特；其余比特保留。 用于告知终端入站频点是 Lf1 还是 Lf2。用 1 个比特表示，0 表示 Lf1，1 表示 Lf2。
入站频度控制参数	1	低四比特有效，即最右边 4 比特；其余比特保留。 用于控制入站业务的标称发送频度，参数内容用 4 个比特表示，具体含义参见图 2。
通信长度限制	1	低四比特有效，即最右边 4 比特；其余比特保留。 用于控制用户发送的入站通信电文长度，不超过北斗三号区域短报文通信用户管理模块中给定的长度等级限制，参数内容用 4 比特表示，具体含义参见图 3。

注：系统参数文件内容缺省值为全 0。

频度编码	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
频度	1s	2s	3s	5s	6s	8s	10s	20s	30s	40s	50s	1m	2m	5m	15m

注：第一行频度编码为4比特二进制编码，第二行为十进制时间计数。

图2　入站频度控制参数

通信长度等级	0001	0010	0011	0100	0101
有效电文长度	692	1835	3883	7979	14000

注：第一行通信长度等级为4比特二进制编码，第二行为十进制数（单位是比特）。

图3　通信长度限制参数

6.6　终端信息文件

终端信息文件见表 11，用于存储北斗三号区域短报文通信用户终端的唯一标识号码。

表 11　终端信息文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
终端信息文件	05h	二进制文件	8 字节	读 = 禁止 写 = 维护密钥密文更新	BCD 编码，详见表 12

终端信息文件内容见表 12。

表 12　终端信息文件内容

数据项	长度（字节）	说明
IMEI	8	国际移动设备识别码标识终端唯一标识号，长度为 8 字节，BCD 格式编码。由 IMEI 号前 15 个数字组成，每个数字占用半字节，最低半字节填 f。

注：终端信息文件内容缺省值为全 0，代表模块未与终端进行绑定。

6.7　自由信息文件

自由信息文件见表 13，提供给北斗三号区域短报文通信用户终端自由使用。

表 13　自由信息文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
自由信息文件	06h	二进制文件	最大 2048 字节	读 = 自由 写 = 自由	HEX 编码，详见表 14

自由信息文件内容见表 14。

表 14　自由信息文件内容

数据项	长度（字节）	说明
自由读写区	2048	用户管理模块提供 2048 字节自由读写区，供终端存储必要的业务数据。

注：自由信息文件内容缺省值为全 0。

6.8　模块信息文件

模块信息文件见表15，用于存储北斗三号区域短报文通信用户管理模块的唯一标识号码。

表 15　模块信息文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
模块信息文件	--	内部文件	9 字节	读 = 使用 GET IMSI 命令 写 = 禁止	BCD 编码，详见表 16

模块信息文件内容见表 16。

表 16　模块信息文件内容

数据项	长度（字节）	说明
用户管理模块唯一标识号码	9	用户管理模块唯一标识号码，是点播密钥和认证密钥的分散因子之一，长度是 9 字节，BCD 格式。

6.9　用户密钥文件

用户密钥文件见表17，用于存储北斗三号区域短报文通信用户管理模块中与北斗三号短报文身份认证、数据加解密有关的所有业务密钥。

表 17　用户密钥文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
用户密钥文件	--	内部文件	应用自定义	读 = 禁止 写 = 禁止	HEX 编码，详见表 18

用户密钥文件内容见表 18。

表 18　用户密钥文件内容

数据项	长度（字节）	说明
主控密钥	应用自定义	拥有密钥更新权限，并保护密钥更新过程。
维护密钥		拥有文件更新权限，并保护文件更新过程。
认证密钥		用于计算上行报文里的认证码。
点播密钥		用于 DECRYPT DATA 命令解密点播报文、ENCRYPT DATA 命令加密上行报文。
通播密钥		用于 DECRYPT DATA 命令解密通播报文。
组播子密钥		用于 DECRYPT DATA 命令解密组播报文。
组播母密钥		用于生成组播子密钥。
组播母密钥（备用）		备用的组播母密钥。
管理型终端管理密钥		管理机专有管理密钥，用于生成下级用户机的通播密钥和点播密钥。

6.10　组播管理文件

组播管理文件见表19，用于存储北斗三号区域短报文通信用户管理模块的组播母密钥索引号及对应的密钥ID。

表 19　组播管理文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
组播管理文件	--	内部文件	7 * 6 字节（最多支持存储 6 条组播母密钥）	读 = 禁止 写 = 禁止	HEX 编码，详见表 20

组播管理文件内容见表 20。

表 20　组播管理文件内容

数据项	长度（字节）	说明
组播母密钥 1 索引	6	组播母密钥 1 的索引号（默认）。
组播母密钥 1 的 KeyId	1	组播母密钥 1 的 KeyId。
组播母密钥 2 索引	6	组播母密钥 2 的索引号（备用）。
组播母密钥 2 的 KeyId	1	组播母密钥 2 的 KeyId。
……	……	……
组播母密钥 6 索引	6	组播母密钥 6 的索引号（备用）。
组播母密钥 6 的 KeyId	1	组播母密钥 6 的 KeyId。

6.11　初始向量文件

初始向量文件见表21,用于存储北斗三号区域短报文通信用户管理模块的解密算法初始向量索引号及对应的初始向量编码。

表 21　初始向量文件

文件头					文件内容
文件名称	文件标识 SFI	文件类型	文件大小	文件访问	
初始向量文件	--	内部文件	22 * 5 字节（最多支持存储 5 条初始向量）	读 = 禁止 写 = 禁止	HEX 编码,详见表 22

初始向量文件内容见表 22。

表 22　初始向量文件内容

数据项	长度（字节）	说明
初始向量 IV_1 的索引号	6	默认初始向量（编号 1）的索引号。
初始向量 IV_1	16	默认初始向量（编号 1）。
初始向量 IV_2 的索引号	6	备用初始向量（编号 2）的索引号。
初始向量 IV_2	16	备用初始向量（编号 2）。
……	……	……
初始向量 IV_5 的索引号	6	备用初始向量（编号 5）的索引号。
初始向量 IV_5	16	备用初始向量（编号 5）。

7　应用命令集

7.1　命令和响应格式

北斗三号区域短报文通信用户终端通过表 24 定义的命令集访问用户管理模块。命令和响应格式应符合 GB/T 16649.4-2010 中 5.1 规定的命令-响应对格式要求，一个命令-响应对，即一个命令报文（C-APDU）跟随着一个相反方向上的响应报文（R-APDU），通过接口的命令响应对不可以有交叉，也就是说响应报文（R-APDU）应在发起下一个命令-响应对之前接收到，命令-响应对格式见表 23。

终端向用户管理模块发送的命令报文（C-APDU）格式由表 23 定义的命令头、Lc 字段、命令数据字段、Le 字段组成。

用户管理模块收到指令后，向终端反馈的响应报文（R-APDU）格式由表 23 定义的响应数据字段、响应尾标组成。

表 23　命令-响应对

字段	描述	字节数	说明
命令头	类别字节 CLA	1	C-APDU 命令报文
	指令字节 INS	1	
	参数字节 P1 - P2	2	
Lc 字段	命令数据字段不存在则 Lc 字段不存在;命令数据字段存在则 Lc 字段存在，且 Lc 字段值为命令数据字段字节数	1 或 0	
命令数据字段	命令数据字段又称命令报文数据域，如果命令报文数据不存在，则该字段不存在；如果命令报文数据存在，则该字段存在，且内容为命令报文数据	命令报文数据长度	
Le 字段	响应数据字段不存在则 Le 字段不存在;响应数据字段存在则 Le 字段存在，且 Le 字段值为期望的响应数据字段字节数	1 或 0	
响应数据字段	响应数据字段又称响应报文数据域，如果命令的响应不存在响应报文数据，则该字段不存在；如果命令的响应存在响应报文数据，则该字段存在，且内容为命令的响应报文数据	响应报文数据长度	R-APDU 响应报文
响应尾标	响应尾标又称响应状态码，由状态字节 SW1、SW2 组成，SW1、SW2 各占 1 字节	2	

7.2　命令列表

北斗三号区域短报文通信用户终端使用表24中所列APDU命令与北斗三号区域短报文通信用户管理模块通信，包括读取或更新文件内容、获取身份认证校验码、执行数据加密、执行数据解密、更新用户管理模块状态等命令。

表 24　APDU 命令列表

命令	CLA	INS	类型
产生认证码（GENERATE AUTH CODE）	80	C2	专用命令
加密数据（ENCRYPT DATA）	80	C4	
解密数据（DECRYPT DATA）	80	C6	
对比终端唯一标识号（COMPARE IMEI）	80	C8	
获取组信息（GET GROUP INFO）	80	D0	
更新组 ID 值（UPDATA GROUP ID）	80	D2	
开关认证码（CONTROL AUTH CODE GENERATION）	84	F0	
获取用户管理模块唯一标识号码（GET IMSI）	80	F2	
切换母密钥/初始向量(IV)（SWITCH KEY IV）	84	F4	
选择文件（SELECT）	00	A4	通用命令
取随机数（GET CHALLENGE）	00	84	
外部认证（EXTERNAL AUTHENTICATE）	00	82	
读二进制文件（READ BINARY）	00/04	B0	
写二进制文件（UPDATE BINARY）	00/04	D6	
读记录文件（READ RECORD）	00/04	B2	
修改记录文件（UPDATE RECORD）	00/04	DC	
取响应（GET RESPONSE）	00	C0	

注：用户终端提供上行报文身份认证、加密和下行报文解密功能的使用流程如下：

a）上行报文发送用于短报文入站，用户终端首先使用产生认证码（Generate Auth Code）指令对指定数据计算认证码，然后使用加密数据（Encrypt Data）指令对短报文内容加密，流程示例见附录图 B.1；

b）下行报文解析流程用于终端接收出站短报文。终端需使用解密数据（Decrypt Data）指令对短报文内容进行解密，流程示例见附录图 B.2。

7.3 逻辑通道

逻辑通道处理应符合GB/T 16649.4-2006中5.1.1规定的要求。APDU命令报文里CLA的最低2比特表示逻辑通道号。设置为00b表示0通道，设置为01b表示1通道。移动运营商USIM应用命令固定占用0通道。本文件所列北斗三号区域短报文通信应用用户管理模块命令均应在1通道下执行。

示例：

GENERATE AUTH CODE命令的CLA为0x80，那么使用1通道时，需要把CLA的bit0置1，即0x81。

终端给USIM卡上电后，先执行SELECT命令选择北斗应用并激活1通道，然后执行COMPARE IMEI命令检查USIM卡是否绑定了指定终端。这两条命令上电之后只需要执行一遍，若未断电或者未执行复位，不必再执行。

选中北斗应用并激活了1通道后，后续命令全部走1通道，以下列举的APDU命令代码中的数字均为十六进制数：

a) SELECT命令：01 A4 04 00 ……；

b) COMPARE IMEI命令：81 C8 00 00 08 ……；

c) GENERATE AUTH CODE命令：81 C2 00 00 ……；

d) ENCRYPT DATA命令：81 C4 00 00 ……。

8 专用命令说明

8.1 产生认证码（GENERATE AUTH CODE）命令

8.1.1 定义与范围

该命令用于计算认证码。用户管理模块应记录认证码的产生状态，作为执行ENCRYPT DATA命令的前置条件。GENERATE AUTH CODE命令的执行状态将一直保留，直至终端对用户管理模块进行复位或者下电。由于终端时间需参与认证码计算，因此终端应在每一组信息发送前生成新的认证码。认证码按系统空间接口约定长度为22比特。

8.1.2 命令报文

命令报文见表25。

表25 产生认证码（GENERATE AUTH CODE）命令报文

代码	值
CLA	80
INS	C2
P1	00
P2	00
Lc	18
DATA	用于计算认证码的输入数据
Le	不存在

8.1.3 命令报文数据域

用于计算认证码的输入数据由入站信息AAD、终端IMEI和终端时间构成，详见表26。

表 26　产生认证码（GENERATE AUTH CODE）命令报文数据

序号	名称	长度（byte）	描述
1	入站信息 AAD	9	包含用户 ID 和一些通讯参数用于附加认证。按系统空间接口约定，由用户 ID、数长指示、入站序号、响应卫星号、响应波束号和响应时间组成，共 72 比特。
2	终端 IMEI	8	终端 IMEI 定义见 6.6。
3	终端时间	7	时间格式为 YYYYMMDDHHMMSS，采用 BCD 编码。如：2020 年 9 月 5 日 16 点 6 分 26 秒，表示为：0x20200905160626。 终端应取当前精确时间（北京时区 UTC+8），然后使用附录 C 的时间模糊算法计算得到模糊时间，作为终端时间传输给 USIM 卡。

8.1.4　命令处理流程

GENERATE AUTH CODE命令的基本处理流程如下：

a)　检查USIM卡产生认证码功能是否开启。若被关闭，返回0x6A81。

b)　检查USIM卡是否绑定了指定终端。若绑定过终端（终端信息文件不是全0x00），则有如下情况：

1)　USIM卡在上电后，若COMPARE IMEI命令执行失败或未执行，执行GENERATE AUTH CODE命令将返回0x6985；

2)　若COMPARE IMEI命令执行成功，则检查GENERATE AUTH CODE命令输入的IMEI是否与COMPARE IMEI命令输入的一致，若不一致将返回0x6A80。

8.1.5　响应报文数据域

响应报文数据为3字节认证码，其中高22比特为有效位。

8.1.6　响应状态码

响应状态码见表27。

表 27　产生认证码（GENERATE AUTH CODE）响应状态码

SW1	SW2	含义
90	00	成功
6A	86	P1 和 P2 错误
67	00	Lc 错误
6A	80	数据域格式错误
6A	82	未找到文件
69	85	使用条件不满足
94	03	未找到用户 ID 或未找到用户 ID 对应的密钥
6A	81	功能不支持

8.2　加密数据（ENCRYPT DATA）命令

8.2.1　定义与范围

该命令用于数据加密。当终端需要发送一组加密信息时，首先使用GENERATE AUTH CODE命令产生认证码，然后使用该命令对指定的信息内容加密。

8.2.2　命令报文

命令报文见表28。

表 28　加密数据（ENCRYPT DATA）命令报文

代码	数值
CLA	80
INS	C4
P1	bit7：1 表示结束帧模式；0 表示中间帧模式 bit7 为 0 时，bit6~0 为帧序号，在 0x01~0x7F 范围内从 0x01 开始依次递增且可循环计数
P2	00
Lc	待加密数据长度
DATA	待加密数据
Le	不存在

8.2.3　命令报文数据域

命令报文数据域的信息为待加密数据，其最大长度为255字节，当信息长度大于255字节时应进行分帧传输，待加密数据的分帧规则见表29。

表 29　加密数据（ENCRYPT DATA）命令报文数据

序号	名称	长度（byte）	描述
1	待加密数据	Lc 或 240	当待加密数据小于等于 255 字节时，使用“结束帧模式”发送全部待加密数据。 当待加密数据大于 255 字节时，使用“中间帧模式”以每帧 240 字节分段发送待加密数据，直到剩余待加密数据小于等于 255 字节时，使用“结束帧模式”发送剩余待加密数据。

示例1：

报文明文长度为288字节，分两帧：

a)　中间帧为：240字节；

b)　结束帧为：48字节。

示例2：

报文明文长度为735字节，分三帧：

a)　中间帧1为：240字节；

b)　中间帧2为：240；

c)　结束帧为：255。

示例3：

报文明文长度为1750字节，分八帧：

a)　前7帧为中间帧，中间帧1至中间帧7均为：240字节；

b)　结束帧为：70字节。

8.2.4　命令处理流程

ENCRYPT DATA命令执行前，应至少成功执行过一次GENERATE AUTH CODE命令。

GENERATE AUTH CODE命令的执行状态将一直保留，直至终端对USIM卡进行复位或者下电。由于终端时间需参与认证码计算，因此终端应在每一组信息发送前生成新的认证码。

USIM卡上电之后如果从未执行过GENERATE AUTH CODE命令，直接执行ENCRYPT DATA命令将返回错误码0x6985。

8.2.5　响应报文数据域

响应报文数据是报文密文，长度与本帧命令报文输入的报文明文一致。

8.2.6 响应状态码

响应状态码见表30。

表 30 加密数据（ENCRYPT DATA）命令响应状态码

SW1	SW2	含义
90	00	成功
6A	86	P1 和 P2 错误
67	00	Lc 错误
6A	80	数据域格式错误
6A	82	未找到文件
69	85	使用条件不满足
94	03	未找到用户 ID 或未找到用户 ID 对应的密钥

8.3 解密数据（DECRYPT DATA）命令

8.3.1 定义与范围

该命令用于解密报文密文。

8.3.2 命令报文

命令报文见表31。

表 31 解密数据（DECRYPT DATA）命令报文

代码	数值
CLA	80
INS	C6
P1	bit7：1 表示结束帧模式；0 表示中间帧模式 bit7 为 0 时，bit6~0 为帧序号，在 0x01~0x7F 范围内从 0x01 开始依次递增且可循环计数
P2	报文类型 01：点播 02：通播 03：组播 04：兼收点播
Lc	待解密数据长度
DATA	待解密数据
Le	不存在

8.3.3 命令报文数据域

命令报文数据域的信息为待解密数据，其最大长度为255字节，当信息长度大于255字节时应进行分帧传输，待解密数据的分帧规则分为两类，其首帧格式不同。

其中当报文类型为点播、通播或组播时，首帧格式由地址和报文密文组成，首帧格式见表32。

表 32 解密数据（DECRYPT DATA）命令报文数据（非兼收报文）

序号	名称	长度（byte）	描述
1	地址（ID）	6	根据报文类型查找对应业务 ID。 点播：用户 ID（点播 ID） 通播：通播 ID 组播：组播 ID
2	报文密文	LC-6 或 240	当报文密文小于等于 249 字节时，使用“结束帧模式”发送全部报文密文。 当报文密文大于 249 字节时，首帧使用“中间帧模式”发送 240 字节报文密文，剩余报文密文发送见表 34。

报文类型为兼收点播时，首帧格式由下属用户管理模块的IMSI值、下属用户ID和报文密文组成，首帧格式见表33。

表 33　解密数据（DECRYPT DATA）命令报文数据（兼收报文）

序号	名称	长度（byte）	描述
1	IMSI	9	USIM 卡的 IMSI 值
2	地址（ID）	6	根据报文类型查找对应业务 ID。 兼收点播：下属用户 ID（点播 ID）
3	报文密文	LC-15 或 240	当报文密文小于等于 240 字节时，使用“结束帧模式”发送报文密文。 当报文密文大于 240 字节时，首帧使用“中间帧模式”发送 240 字节报文密文，剩余报文密发送见表 34。

首帧传输后，如传输信息大于255字节，分帧发送剩余报文密文格式见表34。

表 34　解密数据（DECRYPT DATA）命令报文数据（非首帧报文）

序号	名称	长度（byte）	描述
1	报文密文	LC 或 240	当报文密文小于等于 255 字节时，使用“结束帧模式”发送全部报文密文。 当报文密文大于 255 字节时，使用“中间帧模式”以每帧 240 字节分段发送报文密文，直到剩余报文密文小于等于 255 字节时，使用“结束帧模式”发送剩余报文密文。

8.3.4　命令处理流程

若USIM卡绑定了终端（终端信息文件不是全0x00），并且COMPARE IMEI命令未执行或执行失败，DECRYPT DATA命令不允许执行。

8.3.5　响应报文数据域

响应报文数据是报文明文，长度与本帧命令报文输入的报文密文一致。

8.3.6　响应状态码

响应状态码见表 35。

表 35　解密数据（DECRYPT DATA）响应状态码

SW1	SW2	含义
90	00	成功
6A	86	P1 和 P2 错误
67	00	Lc 错误
6A	80	数据域格式错误
6A	82	未找到文件
69	85	使用条件不满足
94	03	未找到业务 ID 或未找到业务 ID 对应的密钥

8.4　对比终端唯一标识号（COMPARE IMEI）命令

8.4.1　定义与范围

该命令用于检查终端的身份合法性。

若USIM卡绑定了终端（终端信息文件不是全0x00），那么该命令将检查输入的IMEI是否与卡内预存的一致。若不一致，该命令将返回错误码，并禁止使用ENCRYPT DATA和DECRYPT DATA命令。

若USIM卡未绑定终端（终端信息文件是全0x00），该命令不作任何处理。

8.4.2 命令报文

命令报文见表 36。

表 36 对比终端模块唯一标识号（COMPARE IMEI）命令报文

代码	数值
CLA	80
INS	C8
P1	00
P2	00
Lc	08
DATA	终端 IMEI 码
Le	不存在

8.4.3 命令报文数据域

命令报文数据是长度为8字节的终端IMEI码。

8.4.4 命令处理流程

查找IMEI文件，比较文件中的IMEI长度和值是否与输入的IMEI的长度和值一致。

a） 返回0x6A82，表示该USIM卡未创建终端信息文件，即不绑定IMEI。

b） 返回0x6A88，表示该USIM卡未设置过IMEI，即尚未绑定IMEI。

c） 返回0x63CX，表示该USIM卡绑定了IMEI，但与终端传入的IMEI不一致。此时终端应终止流程并提示错误。其中，“X”表示剩余次数。

d） 返回0x6983，表示该USIM卡绑定了IMEI，但终端执行COMPARE IMEI命令返回0x6988的次数超过尝试上限。此时终端应终止流程并提示错误。

e） 返回0x9000，表示该USIM卡绑定了IMEI，且与终端传入的IMEI一致，校验通过。

8.4.5 响应报文数据域

响应报文数据域不存在。

8.4.6 响应状态码

响应状态码见表 37。

表 37 对比终端模块唯一标识号（COMPARE IMEI）响应状态码

SW1	SW2	含义
90	00	成功
6A	86	P1 和 P2 错误
67	00	Lc 错误
6A	80	数据域格式错误
6A	82	未找到终端信息文件
6A	88	终端信息文件内容为空（USIM 卡里没有写入 IMEI）
63	CX	IMEI 不一致，“X”表示剩余次数
69	83	尝试次数已达上限

8.5 获取组信息（GET GROUP INFO）命令

8.5.1 定义与范围

该命令用于获取USIM卡当前的组播编组信息概况。

8.5.2 命令报文

命令报文见表 38。

表 38 获取组信息（GET GROUP INFO）命令报文

代码	数值
CLA	80
INS	D0
P1	00
P2	00：统计组播记录总数 01：统计空闲组播记录总数 02：枚举所有组播记录 03：获取剩余的组播记录
Lc	不存在
DATA	不存在
Le	00

8.5.3 命令报文数据域

命令报文数据域不存在。

8.5.4 响应报文数据域

当P2为0x00时，响应报文数据见表39。

表 39 组播记录总数

序号	名称	长度（byte）	描述
1	组播记录总数	1	已写入的组播记录总数,即已经加入或加入过的组的数量

当P2为0x01时，响应报文数据见表40。

表 40 空闲组播记录数

序号	名称	长度（byte）	描述
1	空闲组播记录数	1	可以写入的组播记录数，即还可以加入多少个组

当P2为0x02、0x03时，响应报文数据见表41。

表 41 当前已加入组的信息汇总表（含组状态）

序号	名称	长度（byte）	描述
1	枚举剩余的组播 ID 的总长度	2	如果该长度为 0000，则后面没有数据需要获取，如果该长度大于 0000 则需要使用获取剩余的组播记录命令获取
2	组播 ID 1	6	
3	组播 ID 1 状态	1	00 表示使用中，01 表示已回收
4	组播 ID 2	6	
5	组播 ID 2 状态	1	00 表示使用中，01 表示已回收
……	……	--	--

8.5.5 响应状态码

响应状态码见表 42。

表 42　获取组信息（GET GROUP INFO）响应状态码

SW1	SW2	含义
90	00	成功
6A	86	P1 和 P2 错误
67	00	Lc 错误
6A	82	未找到组播信息文件
69	85	使用条件不满足

8.6　更新组 ID 值（UPDATA GROUP ID）命令

8.6.1　定义与范围

该命令用于更新组ID。

8.6.2　命令报文

命令报文见表 43。

表 43　更新组 ID 值（UPDATA GROUP ID）命令报文

代码	数值
CLA	80
INS	D2
P1	00
P2	00：新增 01：回收
Lc	见命令报文数据域
DATA	见命令报文数据域
Le	不存在

8.6.3　命令报文数据域

当 P2 为 00 时，命令报文数据见表 44。

表 44　新增组 ID

序号	名称	长度（byte）	描述
1	组播 ID	6	--
2	进组口令	8	--

当P2为01时，命令报文数据见表45。

表 45　回收组 ID

序号	名称	长度（byte）	描述
1	组播 ID	6	--

8.6.4　命令处理流程

当P2为00时，表示新增组ID。新增组ID流程细节如下：

a）　若组ID已存在，则根据组播信息文件（详见表6，下同）中的KeyID在用户密钥文件中查找并更新对应的密钥，并将组播信息文件中对应的组播ID状态置为0x00（表示“组播ID正在使用中”）。

b）　若组ID不存在，则为其分配空闲的KeyID，然后将组ID和KeyID存储到组播信息文件里的空闲记录，并将状态改为正在使用中（0x00）。最后将分散得到的组播子密钥保存到密钥文件中KeyID对应的记录里。

当P2为01时，表示回收组ID，此时USIM卡需将组播ID对应的状态字节改为已回收（0x01）。

8.6.5 响应报文数据域

响应报文数据域不存在。

8.6.6 响应状态码

响应状态码见表 46。

表 46 更新组 ID 值（UPDATA GROUP ID）响应状态码

SW1	SW2	含义
90	00	成功
6A	86	P1 和 P2 错误
67	00	Lc 错误
6A	82	未找到组播信息文件
69	85	使用条件不满足
94	03	索引不支持

8.7 开关认证码（CONTROL AUTH CODE GENERATION）命令

8.7.1 定义与范围

该命令用于限制 GENERATE AUTH CODE 命令使用。

8.7.2 命令报文

命令报文见表 47。

表 47 开关认证码（CONTROL AUTH CODE GENERATION）命令报文

代码	数值
CLA	84
INS	F0
P1	00
P2	00：打开认证码服务 01：关闭认证码服务
Lc	24
DATA	随机数的密文 | MAC
Le	不存在

8.7.3 命令报文数据域

命令报文数据由北斗三号民用短报文应用服务平台的用户管理分系统生成,用户终端收到后应透传给USIM卡。

8.7.4 响应报文数据域

响应报文数据域不存在。

8.7.5 响应状态码

响应状态码见表 48。

表 48 开关认证码（CONTROL AUTH CODE GENERATION）响应状态码

SW1	SW2	含义
90	00	成功
6A	86	P1 和 P2 错误
67	00	Lc 错误

8.8 获取用户管理模块唯一标识号码（GET IMSI）命令

8.8.1 定义与范围

该命令用于获取用户管理模块唯一标识号码。

8.8.2 命令报文

命令报文见表 49。

表 49 获取用户管理模块唯一标识号码（GET IMSI）命令报文

代码	数值
CLA	80
INS	F2
P1	00
P2	00
Lc	不存在
DATA	不存在
Le	09

8.8.3 命令报文数据域

命令报文数据域不存在。

8.8.4 响应报文数据域

响应报文数据见表 50。

表 50 获取用户管理模块唯一标识号码（GET IMSI）响应报文数据

序号	名称	长度（byte）	描述
1	用户管理模块唯一标识号码	9	用户管理模块唯一标识号码，在注册时写入，用于唯一表示北斗三号区域短报文通信用户管理模块

8.8.5 响应状态码

响应状态码见表 51。

表 51 获取用户模块唯一标识号码（GET IMSI）响应状态码

SW1	SW2	含义
90	00	成功
6A	86	P1 和 P2 错误
67	00	Lc 错误

8.9 切换母密钥/初始向量(IV)（SWITCH KEY IV）命令

8.9.1 定义与范围

该命令用于切换指定组播母密钥或初始向量（IV）。

8.9.2 命令报文

命令报文见表 52。

表 52　切换母密钥/初始向量(IV)（SWITCH KEY IV）命令报文

代码	数值
CLA	84
INS	F4
P1	00
P2	00 - 切换组播母密钥 01 - 切换初始向量（IV）
Lc	14
DATA	组播母密钥索引或初始向量索引的密文
Le	不存在

8.9.3　命令报文数据域

组播母密钥索引或初始向量索引的密文，以及命令数据的MAC。该命令由北斗三号民用短报文应用服务平台的用户管理分系统生成，用户终端收到后应透传给USIM卡。

8.9.4　响应报文数据域

响应报文数据域不存在。

8.9.5　响应状态码

响应状态码见表 53。

表 53　切换母密钥/初始向量(IV)（SWITCH KEY IV）响应状态码

SW1	SW2	含义
90	00	成功
6A	86	P1 和 P2 错误
67	00	Lc 错误
6A	82	未找到组播管理文件或初始向量文件（即未写入备用的组播母密钥或初始向量）
69	88	MAC 校验错误
69	82	密文格式错误
69	85	使用条件不满足
94	03	索引不支持/不匹配

9　通用命令说明

通用命令说明应符合 JR/T 0025.1-2010 中第 6 章规定的要求。

附 录 A
（规范性）
产品形态

ID-1 USIM是标准IC卡形态，类似于银行卡、一卡通等标准卡。外形尺寸为：宽85.6mm，高53.98mm，厚0.76mm。图A.1展示了ID-1 USIM的具体规格。

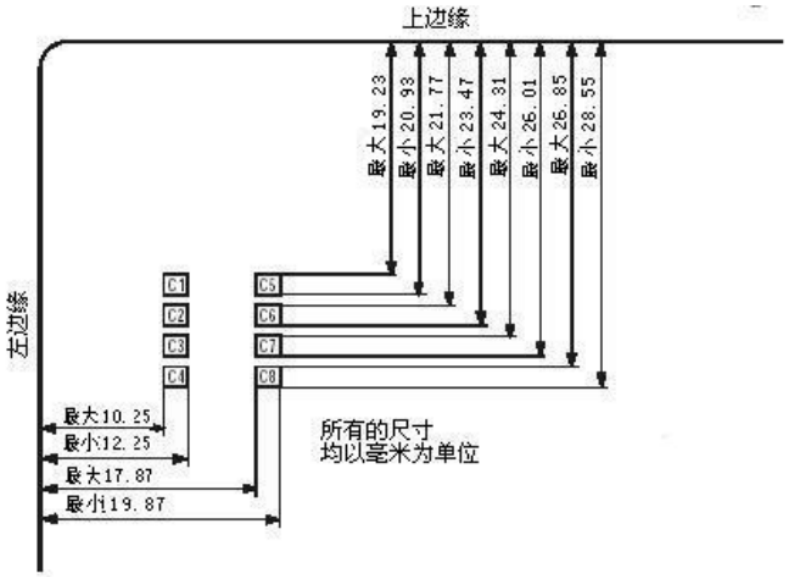

图 A.1　ID-1 USIM 规格示意图

Plug-in USIM是标准USIM卡形态。外形尺寸为：宽25 mm，高15 mm，厚度与ID-1 USIM一致。图A.2展示了Plug-in USIM的具体规格。

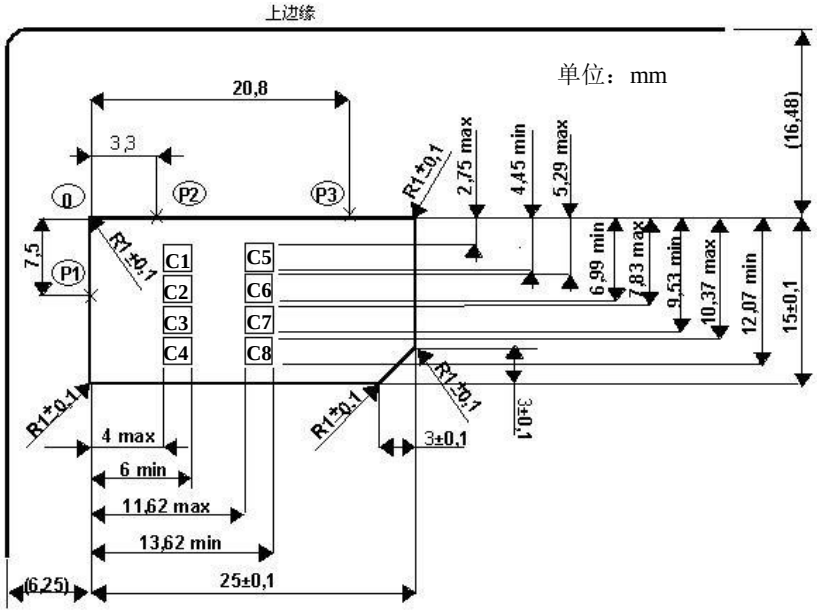

图 A.2　Plug-in USIM 规格示意图

Mini-USIM是Plug-in USIM的缩小版，即市面上常见的Mini USIM卡。外形尺寸为：宽15 mm，高12 mm，厚度与ID-1 USIM一致。图A.3展示了Mini-in USIM的具体规格。

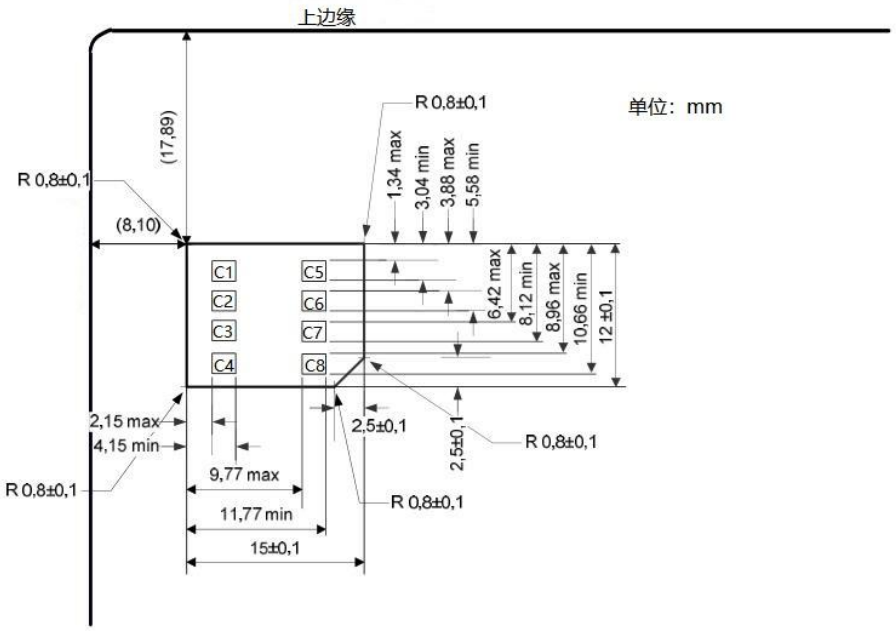

图 A.3　Mini-in USIM 规格示意图

4FF是目前最小规格的插拔式USIM卡，即市面上常见的Nano USIM卡。外形尺寸为：宽12.3mm ±0.1mm，高8.8mm ±0.1mm，厚度约为0.67mm + 0.03mm/-0.07mm 。图A.4展示了4FF的具体规格。

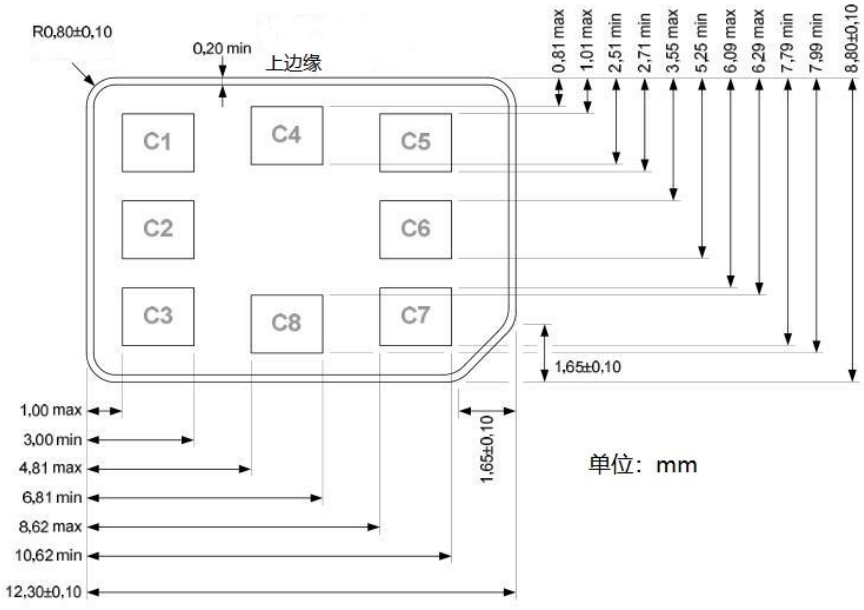

图 A.4　4FF 规格示意图

附 录 B
（资料性）
终端和用户管理模块交互示例

终端与用户管理模块之间的上行报文发送示例如图B.1所示。

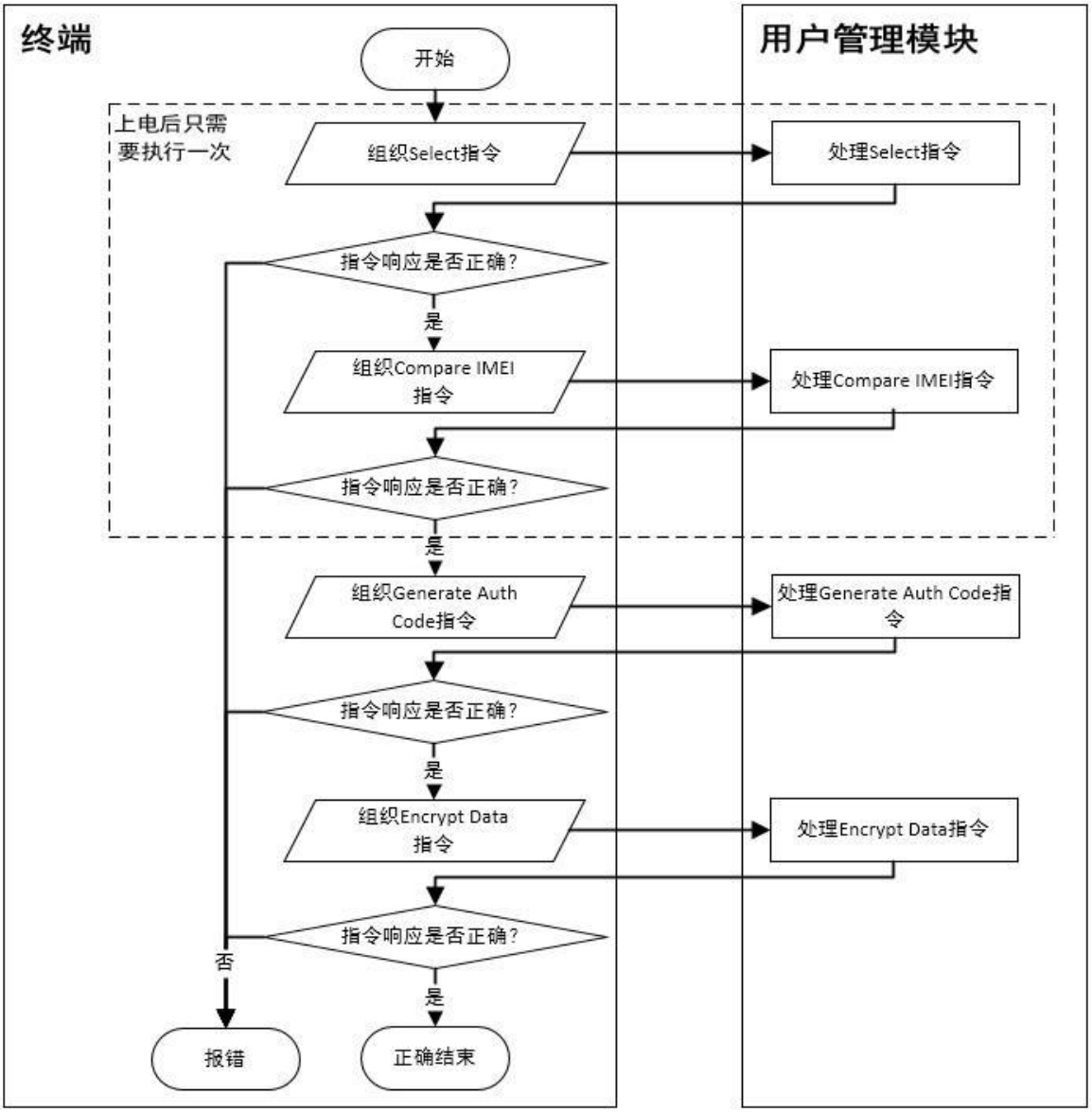

图 B.1　上行报文发送示例图

通信终端与用户管理模块之间的下行报文接收示例如图B.2所示。

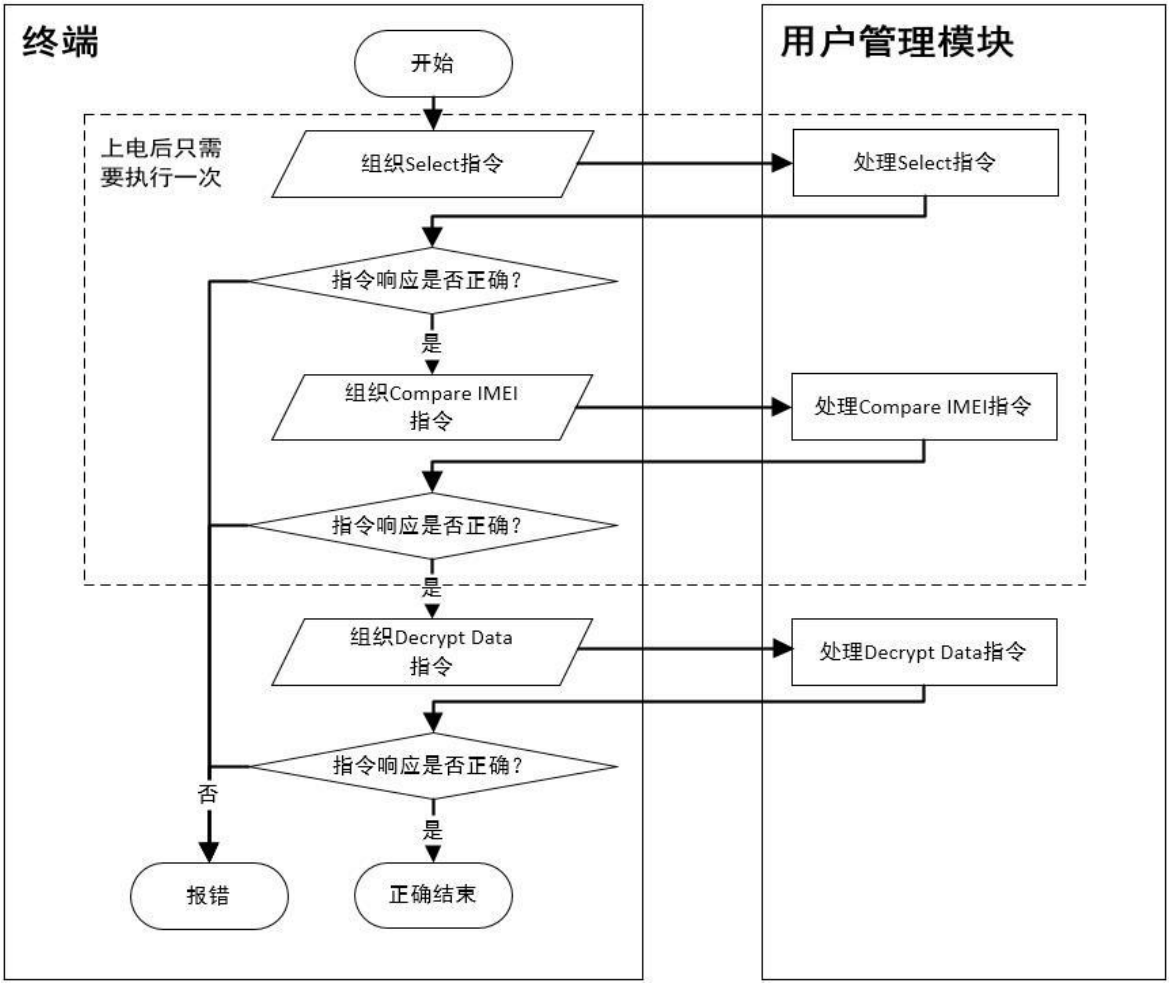

图 B.2　下行报文接收示例图

附 录 C
（规范性）
北斗三号区域短报文通信用户终端时间模糊算法

终端的时间模糊算法计算过程如下所示：

a) 终端取当前系统时间或设备时间，时区为UTC+8。

b) 以整5分钟为最小时间单位，将当前时间向上取整，举例如下：

1） 以5分钟为最小时间单位：秒数值恒为0，分钟数值为0、5、10、15、20、25、30、35、40、45、50、55分钟中的一个。

2） 将当前时间向上取整：以当前精确时间为基点，向上找最近的5分钟整点，如下：

——例1：当前时间是2020.10.16 16:14:35，模糊处理后得到2020.10.16 16:15:00。

——例2：当前时间是2020.10.16 17:15:49，模糊处理后得到2020.10.16 17:20:00。

3） 如果当前时间已经是5分钟整点，则不需要进行时间模糊计算。

c) 将模糊计算完毕的时间的格式转换为YYYYMMDDHHMMSS，编码设置为7字节BCD码，举例如下：

模糊时间是2020.10.16 16:15:00，完成格式转换和BCD编码后得到{ 0x20, 0x20, 0x10, 0x16, 0x16, 0x15, 0x00 }。