ICS 35.030
CCS L 80

中华人民共和国国家标准化指导性技术文件

GB/Z XXXXX—XXXX

网络安全技术 卫星通话与短消息安全指南

Cybersecurity technology—Security guidelines satellite call and short message service

征求意见稿

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布

国家市场监督管理总局
国家标准化管理委员会 发布

目　　次

前言 ····· III
1　范围 ····· 1
2　规范性引用文件 ····· 1
3　术语和定义 ····· 2
4　缩略语 ····· 4
5　总体架构 ····· 5
5.1　应用架构 ····· 5
5.2　应用模式 ····· 5
5.3　安全架构 ····· 6
6　应用安全 ····· 7
6.1　卫星通话安全 ····· 7
6.2　卫星短消息安全 ····· 9
7　网络安全 ····· 11
7.1　用户域网络安全 ····· 11
7.2　空间数据传输安全 ····· 14
7.3　服务域网络安全 ····· 14
7.4　感知预警与攻击防御 ····· 15
8　数据安全与个人信息保护 ····· 15
8.1　基本要求 ····· 15
8.2　通信数据分类与分级 ····· 16
8.3　安全措施 ····· 16
8.4　个人信息保护安全策略与用户权利保障 ····· 17
8.5　第三方接入与管理 ····· 17
8.6　个人信息泄露应急响应 ····· 17
9　密码安全 ····· 18
9.1　密码算法 ····· 18
9.2　密钥管理 ····· 18
10　安全管理 ····· 20
附录 A（资料性）业务流程实例 ····· 22
附录 B（资料性）通用的数字卫星通信假设参考数字通道 ····· 27
参考文献 ····· 28

前　言

本文件为规范类指导性技术文件。

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中移量子科技有限公司、国家计算机网络应急技术处理协调中心、中国移动通信集团有限公司、中国电子技术标准化研究院、四川大学、北京邮电大学、紫光同芯微电子有限公司、清华大学、中国工业互联网研究院（工业和信息化部密码应用研究中心）、中国信息通信研究院、北京天地和兴科技股份有限公司、北京浩瀚深度信息技术股份有限公司、中移系统集成有限公司、北京神州绿盟科技有限公司、国网新疆电力有限公司电力科学研究院、中国软件评测中心（工业和信息化部软件与集成电路促进中心）。

本文件主要起草人：魏瑛、于庆军、粟栗、雷正朝、陈悦、袁璐、李小文、邱勤、王秉政、李炜、王祥通、谷勇浩、张艺隆、宁晓魁、刘献伦、朱伟光、谢佳轩、刘君、庞韶敏、李瀛、郑庆国、崔婷婷、叶帅辰、李峰、韩斐、蔡伟霞、袁豪杰、李泽村。

网络安全技术 卫星通话与短消息安全指南

1 范围

本文件提出了卫星通话与短消息的基本安全框架及安全技术指南，包括安全架构、应用安全、网络安全、数据安全与个人信息保护、密码算法和密钥管理，以及安全管理需考虑的因素。

本文件适用于卫星通话与短消息安全产品的设计、应用与实施。

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 9361 计算机场地安全要求

GB/T 15843.2—2024 网络安全技术 实体鉴别 第 2 部分：采用鉴别式加密的机制

GB/T 15843.3—2023 信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制

GB/T 15843.4—2024 网络安全技术 实体鉴别 第4部分：采用密码校验函数的机制

GB/T 15852.1—2020 信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制

GB/T 15852.2—2024 网络安全技术 消息鉴别码 第2部分：采用专门设计的杂凑函数的机制

GB/T 15852.3—2019 信息技术 安全技术 消息鉴别码 第 3 部分：采用泛杂凑函数的机制

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918.2 SM2 椭圆曲线公钥密码算法 第 2 部分 数字签名算法

GB/T 33133（所有部分）祖冲之序列算法

GB/T 36624 信息技术 安全技术 可鉴别的加密机制

GB/T 37027—2025 网络安全技术 网络攻击和网络攻击事件判定准则

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38636 信息安全技术 传输层密码协议(TLCP)

GB/T 39335 信息安全技术 个人信息安全影响评估指南

GB/T 39575—2020 具有融合功能的移动终端安全能力技术要求

GB/T 39720—2020 信息安全技术 移动智能终端安全技术要求及测试评价方法

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GB/T 42037—2022 空间数据与信息传输系统 参考体系架构

GB/T 42453—2023 信息安全技术 网络安全态势感知通用技术要求

GB/T 43697—2024 数据安全技术 数据分类分级规则

YD/T 2035 移动终端垃圾短消息过滤技术要求

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

卫星通话 satellite call

通信设备之间基于卫星通信链路进行双向语音通话，能提供一种或多种方式进行拨号、接听、通话、挂断操作等。

3.2

卫星短消息/短信 satellite short message

通过卫星通信链路在用户通信设备之间，或业务提供者与用户通信设备之间发送和接收的有限长度文本或其他格式的数据，以下简称：短消息。

3.3

卫星通话/短消息用户 satellite call / short message user

可以通过卫星通话/短消息终端使用卫星通话业务/短消息业务的用户，以下简称用户。

[来源：YD/T 2035—2009，3.4，有修改]

3.4

卫星通话/短消息用户设备 satellite call / short message user terminal

能够开展卫星通话和（或）卫星短消息等通信业务的用户设备，以下简称用户设备。

3.5

具有融合功能的移动终端 mobile terminal with syncretic function

可对人或物进行信息采集和处理，具备蜂窝网络和互联网络接入功能，支持语音或数据通信，具有融合功能的终端设备。

[来源：GB/T 39575—2020，3.1.1]

3.6

短消息业务平台 short message service platform

在基于卫星/星座网络及地面移动通信网络，为用户设备实现短消息收发功能进行中继、路由、存储和前转短消息的实体。

[来源：YD/T 2035—2009，3.2，有修改]

3.7

主叫 caller

通话过程中，主动发起呼叫一方。短消息过程中的发送方。

[来源：GM/T 0098—2020，3.3，有修改]

3.8

被叫 callee

通话过程中，接收呼叫的一方，或短消息过程中的接收方。

[来源：GM/T 0098—2020，3.2，有修改]

3.9

用户密钥 user key

存储在用户密码模块的用于密码运算的非对称密钥，包含签名密钥对和加密密钥对。

[来源：GM/T 0098—2020，3.23]

3.10

会话密钥 session key

处于层次化密钥结构中的最低层，仅在一次会话中使用的密钥，依据用途可分为会话加密密钥和会话鉴别密钥。

[来源：GM/T 0098—2020，3.14]

3.11

一话一密 per-session key

每新建立的卫星通话、短消息的端到端会话密钥都重新产生。

3.12

端到端加密 end-to-end encipherment/encryption

数据在源端进行加密，在目的端解密。

[来源：GM/Z 4001—2013，2.18]

3.13

密钥加密密钥 key encryption key（KEK）

用于对密钥进行加密或解密的密钥。

注：通过密钥存储介质充注或在线更新，加载到用户设备中预存使用的密钥，可用于用户设备与密钥管理模块之间，获取会话密钥时的加密。

[来源：GM/Z 4001，2.78，有修改]

3.14

密钥协商/密钥交换 key agreement/key exchange

两个或多个实体通过相互传送一些消息来共同建立一个共享的秘密密钥的协议,且各个实体无法预先确定这个秘密密钥的值。

[来源：GM/Z 4001，2.83]

3.15

访问控制 access control

一种确保数据处理系统的资源只能由经授权实体以授权方式进行访问的手段。

[来源：GB/T 25069，3.147]

3.16

通信数据个人信息保护 protection ofpersonal informationin communication data

确保在卫星通信过程中涉及的用户身份数据、位置数据、通信内容数据等不被非法收集、使用、泄露、篡改或损毁的措施集合。

3.17

接入 access

设备之间建立链路并实现数据可达的过程。

3.18

安全策略 security policy

用于治理某一组织及其系统内管理、保护并分发影响安全及有关元素的资产（包括敏感信息）的一组规则、指导和实践。

[来源：GB/T 25069，3.3]

3.19

SRM 保证 **safety,reliability and maintainability assurance**

为使人们确信产品达到规定的安全性、可靠性和维修性要求，在产品研制、生产和使用的全过程，所进行的一系列有计划、有组织的SRM管理、设计与分析、验证与评价的技术与管理活动，以保证产品以最佳费效比完成所要求的任务。

[来源：GB/T 35439—2017，3.2]

3.20

脱敏 desensitization

通过模糊化等方法处理原始数据，以实现屏蔽敏感数据且屏蔽后的数据不可逆向恢复的数据保护方式。

[来源：GB/T 39575—2020，3.1.3]

4 缩略语

下列缩略语适用于本文件。

APT：高级持续性威胁（Advanced Persistent Threat）

CCM：分组密码链接-消息认证码（Counter with CBC-MAC）

DDoS：分布式拒绝服务（Distributed Denial of Service）

DoS：拒绝服务（Denial of Service）

GCM：Galois 计数器模式（Galois Counter Mode）

HRDP：假设参考数字通道（Hypothetical Reference Digital Path）

ID：标识符（Identifier）

IF：中频（Intermediate Frequency）

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）

IP：网络之间互连的协议（Internet Protocol）

IPS：入侵防御系统（Intrusion Prevention System）

ISL：卫星间链路（Inter-Satellite Link）

JTAG：联合测试工作组（Joint Test Action Group）

MAC：消息鉴别码（Message Authentication Code）
NNI：网络节点接口（network node interface）
QoS：服务质量（Quality of Service）
RF：射频（Radio Frequency）
SIM：用户身份模块（Subscriber Identity Module）
SP：业务提供者（Service Provider）
SRM 安全性、可靠性和可维修性（Safety，Reliability and Maintainability）
TCP：传输控制协议（Transmission Control Protocol ）
TMSI：临时移动用户标识（Temporary Mobile Subscriber Identity）
UART：通用异步收发器（Universal Asynchronous Receiver/Transmitter）
WAF： Web应用防火墙（Web Application Firewall）

5 总体架构

5.1 应用架构

支持卫星通话与短消息收发的用户设备在完成相关软硬件准备、卫星用户账号注册开通后，即可开展卫星通话或短消息收发。

开展卫星通话与短消息的通信实体应用架构主要包括且不限于用户设备（含主叫、被叫）、管理单元、通信平台和密钥管理模块，见图1。



图 1 通信实体应用架构示意图

图1中，各组成的基本功能宜包括且不限于：

a) 用户设备具有卫星用户账号，能完成卫星通话和短消息功能的入网鉴权、通信数据的安全传输、语音和短消息端到端数据的保护；
b) 通信平台主要负责卫星通话与短消息的通信接入，为注册及授权的用户提供通话语音或短消息等数据的端到端的通信传输，包括且不限于卫星及地球站；卫星用户账号的注册及授权一般由卫星的运营单位提供支持；
c) 管理单元提供业务的管理支撑，可包括短消息业务平台、群组中心设备、业务提供者（SP)服务平台等，以下简称管理单元；
d) 密钥管理模块完成用户设备密码模块/芯片的初装、认证鉴权、密钥分发与管理。

注：用户设备的密码模块实体形态可包括且不限于插卡式、安全芯片等；管理单元可包括密码服务器等形态，以下统称密码模块。

5.2 应用模式

用户设备的主叫与被叫之间，或管理单元与用户设备之间开展卫星通话与短消息业务时，根据用户设备或管理单元接入卫星的路径不同，可包括两类：

——直连卫星接入，简称直连接入；

——通过地面站接入，简称非直连接入。

通信的路径根据直连接入或非直连接入的不同，在用户设备之间、管理单元和用户设备之间的端到端卫星通话与短消息（点对点）的通信路径，可包括且不限于：

——用户设备 1——卫星——地面站及运控单元——卫星——用户设备 2；

——用户设备 1——地面站及运控单元——卫星——用户设备 2；

——用户设备 1——地面站及运控单元——卫星——地面站及运控单元——用户设备 2；

——用户设备 1——卫星——地面站及运控单元——卫星——地面站及运控单元——用户设备 2。

注1：非直连接入通用的数字卫星通信假设参考数字通道（HRDP）见附录B。

向中华人民共和国境内提供终端设备直连卫星服务，应当将关口站、地球站等地面设施建设在境内，或者使用境内的地面设施，接入在境内合法运营的地面通信网络。

境内用户数据应当在境内地面设施处理，未经批准不得经由卫星转发至境外关口站、地球站等设施。

用户设备之间、管理单元与用户设备之间通信时，宜完成用户安全接入的鉴权、接入网络的授权使用和接入流量管控等基本控制。安全架构见5.3。

注2：附录A.1给出了用户设备直连接入卫星进行通话业务的一个流程实例。附录A.2给出了直连接入卫星进行短消息通信的一个流程实例。

注3：非点对点卫星通话/短消息（如业务提供者与用户之间的卫星通话/短消息）；定制类非点对点卫星通话/短消息（如通过运营商网络形成定制关系并由运营商代收费的非点对点卫星通话/短消息）；北斗卫星消息业务（即支持北斗短报文的终端通过北斗卫星导航系统区域短报文信号与相关短消息业务平台进行消息互通的通信业务）等可据实际需求参考本指南的建议。

5.3 安全架构

卫星通话与短消息安全架构见图2。



图 2 安全架构

图2中，卫星通话与短消息安全架构主要包括安全功能及安全管理。安全功能包括且不限于应用安全、通信实体安全、空间数据传输安全、网络边界安全、密码密钥安全、数据安全与个人信息保护等。安全管理包括且不限于应用安全管理、网络安全管理、密码安全管理、数据安全管理及其他。

6 应用安全

6.1 卫星通话安全

6.1.1 卫星通话应用结构

进行卫星通话的用户设备主叫和被叫之间端到端通信应用结构见图3。

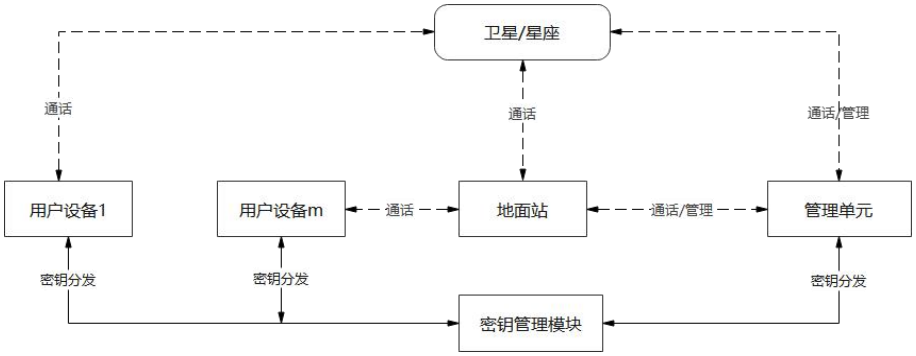


图 3 卫星通话应用结构示意图

如图3所示，主叫发起会话，经由卫星或地面站等通信系统（简称：通信平台）与被叫建立通信会话。密钥管理模块为通信双方分发密钥。主叫和被叫应用密钥分发或密钥协商形成的会话密钥对卫星通话的语音、短消息数据或管理信息进行安全保护。用户设备1、用户设备m、以及管理单元之间，以主叫与被叫的方式通过直接接入卫星，或通过地面站接入卫星，实现通信交互。

6.1.2 卫星通话安全

卫星通话的应用安全侧重实时性、低延迟与通信安全与效率平衡，具体可包括对信令安全、语音数据媒体流的加密、号码鉴权与显示、抗干扰或欺骗等安全措施。

a） 信令安全措施

——注册、鉴权、呼叫建立信令宜进行真实性、完整性保护（防篡改、防伪造）和加密（防窃听）；

——宜防范信令风暴攻击。

b） 语音数据的媒体流加密

——语音载荷（Voice Payload）在空口传输前宜采取相应的加密措施，包括链路（或空口）加密和端到端的加密（见 6.1.3）；

——算法安全措施见 9.1；

——会话密钥宜一话一密，每次呼叫动态生成，密钥分发见 9.2.2，密钥协商见 9.2.3，宜支持根据密钥更新策略（如每通话持续时间阈值更新策略等）进行通话过程中的密钥更新。

c） 号码鉴权与显示

——网络侧宜对主叫的标识进行鉴权，防止身份伪造或欺骗；

——应用设备宜根据应用需求，选择提示用户当前通话是否处于“加密”状态。

d） 干扰与抗欺骗

——终端宜具备信号异常检测能力，当检测到强干扰或伪基站特征时，宜采取安全策略配置的措施，如自动阻断、切换链路，并通知提示主叫或被叫用户。

6.1.3 端到端加密

宜采用会话密钥对卫星通信数据进行加密，可选进行消息鉴别码MAC计算实现通信数据的完整性保护。加密通信的安全业务过程包括且不限于如下过程：

a） 主叫对通信数据进行加密，即对已被编码过的整个语音包/数据包进行对称算法加密运算。可选对已被编码过的整个语音包的密文进行消息鉴别码 MAC 计算；

b） 通信数据的接收方在收到数据后，要做解密运算；并按需对密文数据进行 MAC 值校验；

c） 当加密通信结束后，应用设备宜释放会话密钥资源。

加密的数据报文示意图见图4。

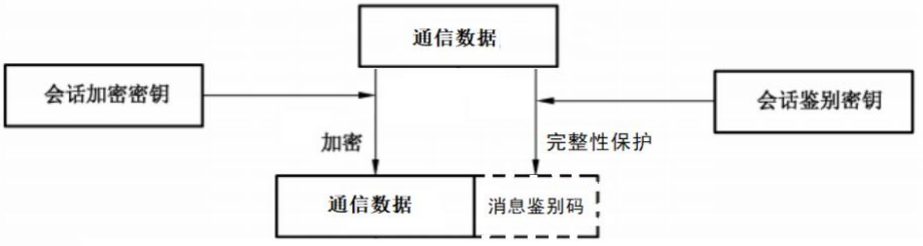


图4 加密的数据报文示意图

使用会话加密密钥对卫星通话与短消息的通信数据进行加密，使用会话鉴别密钥计算消息鉴别码MAC，使用的密码算法见 9.1.1 和 9.1.5。

6.1.4 群组加密

群组通信可包括群组卫星通话或群组卫星短消息等，当主叫与多个被叫进行点对多点群组通信时，基本过程包括且不限于：

a) 用户设备预先配置好所有参与点对多点群组通信的参与方；
b) 由主叫在发起通信前，选取所有参与点对多点群组通信的参与方；
c) 当进行点对多点的组播或广播业务时，主叫与所有被叫获取会话密钥的过程原则上宜一致，包括密钥分发方式或密钥协商方式；
d) 主叫通过通信平台，将本次会话密钥的获取的参数信息分发给每一个被叫；

——通过密钥管理模块进行密钥分发时，参数信息包括主叫 ID、本次会话 ID 及其他必要参数，被叫将依此向密钥管理模块安全获取会话密钥（见 9.2.2）；

——采用密钥协商模式时，参数信息宜包括会话密钥分发协议数据，被叫对该协议数据进行处理，通过应用设备初装的用户密钥和（或）密钥加密密钥（KEK）对密钥协商数据进行验证及解密处理，验证通过后获取到本次通信的会话密钥（见 9.2.3）；

主叫和多个被叫将利用本次会话密钥进行双向加密通信。

注1：当群组通信并考虑主叫与所有被叫之间的会话密钥两两各不相同时，主叫与所有被叫之间两两进行会话密钥的获取，可采取密钥分发或密钥协商的不同方式。

注2：当群组通信并考虑本次会话中，群组任何人的话音及短消息都可以让群组其他人听见，则可采用主叫与所有被叫进行密钥协商，同步会话密钥

6.2 卫星短消息安全

6.2.1 卫星短消息应用结构

进行卫星短消息收发的用户设备之间点对点短消息业务应用结构见图5。

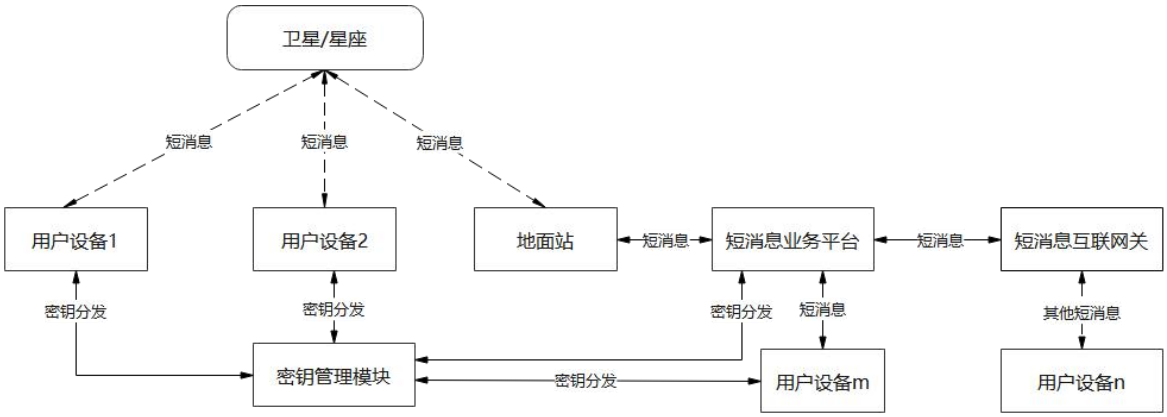


图 5 卫星短消息应用结构示意图

如图5所示，卫星短消息收发的点对点短消息业务应用结构由卫星/星座、地面站、用户设备，短消息业务平台、短消息互联网关等部分相互协作，与密钥管理模块、业务控制/计费系统（未体现在图5中）等共同完成。不同的系统可能有不同的实现。

支持用户设备与卫星/星座直接通信（如图5中用户设备1、用户设备2）、或通过地面站，与短消息业务平台及卫星/星座通信完成短消息业务处理及收发（如图5中用户设备m、用户设备n）。

短消息业务平台通过信令链路与地面站相连，支持用户设备通过卫星/星座发送和接收的短消息，包括：从地面站接收用户设备发送的短消息；查询路由信息，并向接收方用户设备所在交换系统转发短消息等。短消息业务平台通过数据链路与短消息互联网关相连，实现网间短消息的转发和缓存功能。当主叫用户发起短消息时，经相应的业务控制授权后，短消息业务平台向被叫用户下发短消息或将短消息前转至短消息互联网关。其中：

——短消息业务平台可以是卫星/星座与运营商星地互通平台中有关短消息业务的功能模块；

——短消息互联网关可以支持同一电信企业不同网络间短消息业务的接口网关；也可支持不同电信企业短消息网络的接口网关。

6.2.2 卫星短消息安全

短消息的应用安全宜包括对关键指令、短消息数据的安全实施，涉及指令安全、数据完整性保护及抗重放，具备安全措施包括且不限于：

a) 短消息数据在应用设备到通信平台（通过地面站/核心网）之间宜根据应用对应的安全保护等级采取相应端到端加密，在空口及链路上采取通信系统的加密策略；保护对象的安全保护等级确定方法见 GB/T 22240；

b) 短消息的完整性保护可通过增加消息认证码，防止短消息内容的篡改或伪造攻击；

c) 短消息的协议报文头中宜包含时间戳、流水号或序列号，接收端宜校验并丢弃重复或过期的消息；

d) 涉及短消息端到端链路上的网元具有存储与转发处理时（如卫星或短信网关等支持存储转发），宜对存储的短信采取加密措施，且加密密钥由授权的管理者进行管理及维护；

e) 用户设备宜具备卫星短消息发送的用户提示与确认机制，对于非预设置应用软件发起的发送请求，宜在获得用户明确确认后，再执行发送操作；

f) 用户设备宜具备卫星短消息接收的用户提示与确认机制，对于非预设置应用软件发起的接收请求，宜在获得用户明确确认后，再执行接收操作；

g) 用户设备宜具备卫星短消息读、写和删除操作的用户提示与确认操作，对于非预设置应用软件发起的操作请求，建议在获得用户明确确认后，再执行相关操作；

h) 当用户设备在短消息业务平台地址设置发生变更时，宜向用户设备提供明确的提示信息，告知其当前设置已发生变化，并由用户确认变更操作，以防止因误操作或第三方应用诱导修改导致的短信功能异常；

i) 与地面网络互通时，宜根据互通机制差异部署信令网关、短消息网关等，仅允许与短消息有关消息载荷、短消息状态、计费话单等数据通过，并实现上述数据传输时的逻辑隔离，同时宜具备信令过滤和异常信令分析告警能力；

j) 与行业用户间的业务数据及管理信令交互时，宜采用认证、鉴权、加密及消息鉴别、抗重放等数据传输安全措施；

k) 通信平台宜支持短消息黑名单功能，能根据安全通告，依据群发频次、内容关键词等维度生成黑名单，并由短消息业务平台或网关等网元执行具体的拦截操作。垃圾短信的界定和过滤宜符合 YD/T 2035；

l) 通信平台宜支持针对具有批量发送需求的特殊用户或专业应用用户的白名单能力，并建立白名单的申请、审批、复核和退出机制；

m) 通信平台宜通过短消息业务平台或网关类网元设定差异化的发送阈值，包括但不限于：单号码单位时间发送条数、单 IP 或单账号日累计发送量、通道整体每秒发送峰值等。对于达到或超过阈值的发送行为，宜由相关网元自动触发相应的管控动作，如拦截、限速，并告警。

6.2.3 端到端短消息加密

卫星短消息业务过程中的端到端加密机制宜符合6.1.3。

6.2.4 群组短消息加密

卫星短消息业务过程中的群组短消息加密机制宜符合6.1.4。

7 网络安全

7.1 用户域网络安全

7.1.1 通用安全

用户设备采用移动智能终端结构时，相应的硬件安全、系统安全、应用软件安全、通信连接安全、用户数据安全等安全技术要求宜符合 GB/T 39720—2020。

具有融合功能的移动终端安全能力，包括硬件安全能力、操作系统安全能力、应用软件安全能力、通信连接安全能力、个人信息安全保护能力的相关技术要求宜符合 GB/T 39575—2020 。

7.1.2 身份标识

用户设备、管理单元及其用户身份标识模块（如 SIM）宜具备唯一的用于标识其身份，且不可篡改的设备标识码（如 IMEI，或其他扩展）和身份标识码（如 IMSI，或其他扩展）。

7.1.3 用户认证与业务鉴权

7.1.3.1 安全业务过程

安全业务过程主要包括用户接入鉴权、会话密钥分发和加密通信：

a) 加密通信前，需对用户设备的主叫、被叫和（或）管理单元进行用户身份认证；
b) 密钥分发宜保证所分发密钥的机密性和完整性，并保证密钥的存储及使用安全；
c) 根据业务应用安全需求，宜对卫星通话或短消息采取加密措施保证通信传输数据的机密性、完整性和可用性；
d) 通信过程宜具备业务层防 DoS / DDoS，及异常攻击检测的能力。

7.1.3.2 身份认证

用户设备和管理单元宜具有身份认证的功能，认证方法宜符合9.1.3。

任何一种方式都宜保证身份认证的完整性和有效性。用户身份认证宜至少包括卫星用户账号的认证、基于密码的实体鉴别，以及其他访问控制措施（如用户设备的唯一识别等），可按用户系统访问控制策略进行访问控制。

用户设备和管理单元上的应用软件启动后，提示进行用户登录与身份鉴别，包括卫星用户账号认证、密码模块向密钥管理模块的密码认证，宜全部认证通过后用户设备完成身份鉴别，并提示身份认证的结果。

7.1.3.3 用户接入控制

用户接入控制包括且不限于：

a) 卫星通话与短消息系统接入前向运营部门（业务主管部门）办理入网及接入申请，经审核批准后方可接入；
b) 宜建立终端接入审核机制，对接入终端的合法性、完整性和真实性（包括且不限于核对接入时间、流水号、地理位置合理性等）进行检查与评估；

c） 宜对接入终端实施身份认证、接入控制与安全策略校验，防止未授权或违规终端接入系统；
d） 对远程接入行为，宜采取加密传输措施，防止鉴别信息在传输过程中被窃听、篡改或重放；
e） 宜记录接入行为日志，日志内容宜包括接入时间、接入主体、来源地址、认证结果等信息。

7.1.3.4 用户身份与权限管理

用户身份与授权管理安全措施包括且不限于：
a） 用户账户的创建、变更与注销宜履行审批流程，经运营部门（业务主管部门）批准后方可实施；
b） 用户账号具有唯一性，且不可篡改；
c） 用户身份的标识及其扩展宜体现用户的类型，如普通用户、管理类用户等；
d） 宜按照最小权限原则分配访问权限，并根据用户权限、管理职责等实施分级授权管理，用户权限宜配置有效期；
e） 对管理类用户宜实施严格控制，宜采用双因素或多因素身份认证机制；
f） 宜及时停用或删除冗余账户、过期账户及离岗人员账户，不宜存在共享账户；
g） 远程运维操作时，宜对访问账户的权限范围、使用时长和访问资源进行限制，仅满足单次操作所需的最小权限；
h） 宜定期开展账户与权限审计，发现异常权限宜及时整改；
i） 宜根据通信平台策略及用户授权，对直连接入的设备实施带宽、连接数、信令频率配额、权限管控。

7.1.3.5 交互过程安全措施

不同通信平台及密钥管理模块在用户接入鉴权时可以有不同的交互过程及步骤。本文件提供一种用户接入鉴权的业务流程实例，见附录A.3。需要考虑的安全措施宜包括且不限于：
a） 对密码模块与密钥管理模块进行基于密码的实体鉴别，鉴别方法见 9.1.3；
b） 当用户设备与通信平台之间具有传输层加密链路时，传输层密码协议宜符合 GB/T 38636。

7.1.4 加密通信

卫星通话与短消息的加密通信见第6章。卫星通话与短消息加密通信配置的密码算法和密钥种类见第9章。

7.1.5 密钥管理

7.1.5.1 密钥初装与状态查询

通过密钥管理模块宜支持对用户设备密码模块的用户密钥、密钥加密密钥等的密钥初装、密钥分发或更新、状态查询。

用户设备和管理单元的密码模块的密钥状态包括且不限于：
a） 密钥状态是否正常，或存在何种常见错误；
b） 是否在有效期；
c） 是否存在锁定、销毁状态；
d） 其他状态。

7.1.5.2 密钥协商

用户设备之间、用户设备与管理单元之间的会话密钥同步宜支持密钥协商，见9.2.3。

7.1.5.3 密钥分发

用户设备之间、用户设备与管理单元之间的会话密钥同步可支持密钥分发，见9.2.2。

7.1.5.4 密钥更新

用户设备及管理单元中，会话密钥的更新频率与更新量，宜满足用户系统对卫星通话与短消息的加密能力和安全性需求。加密通信的会话密钥推荐采取一话一密的更新频率。

7.1.5.5 密钥销毁

用户设备及管理单元密码模块中的密钥支持销毁功能。密钥管理模块中的密钥销毁按照系统密钥管理方案执行。

7.1.5.6 随机数生成

密码模块或安全芯片宜具有随机数生成功能，宜采用基于物理原理的随机数生成方案。在使用随机数前，宜能够根据安全级别与使用场景因素，对生成的随机数进行检测，随机性检测宜符合 GB/T 32915。

7.1.6 紧急呼叫安全

紧急呼叫时，宜优先保障信令可达，并宜对建议上报的位置信息进行加密保护，防止位置信息泄露。

7.1.7 软件及数据保护

7.1.7.1 软件安全

用户设备及管理单元上运行的卫星通话与短消息相关的软件模块（以下简称：软件）宜具备用户身份鉴别、会话密钥同步、加密通信、通信录管理等功能，并具有卫星通话与短消息通信过程中的状态显示或语音提示。

软件宜支持且不限于：

a) 健壮性，软件宜保持通话或短消息业务过程中的功能正确、运行稳定，并具备相宜的恢复能力，以在出现异常状态时具备一定的恢复能力。如在一般异常时，可提供稳定的状态提示，并根据配置人工或自动重新恢复应用软件的功能；
b) 可恢复性，软件与相应的卫星通信链路或网络连接时，宜具备一定的弹性（可恢复性），以应对在一般的网络攻击（如 DoS / DDoS，异常流量、病毒木马入侵、APT 攻击等）情况下的功能的稳定、自动恢复及状态保持；
c) 可维护性，软件宜根据配置信息支持自动升级或手动升级。

7.1.7.2 数据保护

用户设备及管理单元上的卫星通话与短消息数据的保护宜包括且不限于：

a) 宜确保通话记录、通话数据、短消息数据只有授权用户可访问；
b) 宜支持授权用户对通话记录、通话数据、短消息数据的备份、删除；
c) 必要时，宜对存储在用户设备上的卫星通话及短消息留存数据进行加密存储；
d) 支持对敏感数据的脱敏显示，如在屏幕中显示时用“*”的方式显示；
e) 用户设备在加密通话时，用户设备操作系统宜具备自动关闭系统通话录音功能，防止本地录音及第三方软件录音。

7.1.8 密码模块配置

用户设备及管理单元配置的密码模块、安全芯片等的安全宜符合 GB/T 37092。配置的密码模块或安全芯片等的安全保护等级宜不低于用户设备的安全保护等级。

7.1.9 用户设备安全策略

卫星通话及短消息应用所承载的用户设备及管理单元操作系统等运行环境宜确保软硬件环境安全，宜具有宿主机的安全检查功能。不符合安全策略的宿主机将无法使用设备。安全策略包括且不限于下措施：

a) 宜安装并启用反病毒软件；
b) 宜安装最新的操作系统安全补丁；
c) 宜为系统设置了登录口令、指纹等登录控制措施；

d) 可安装并启用个人防火墙；
e) 禁止未授权的调试接口（JTAG / UART）开放；
f) 对卫星通话及短消息应用所必须的软硬件提供系统可用性支持，包括且不限功能支持、状态维护及一般故障的恢复。

7.2 空间数据传输安全

空间数据传输安全宜符合GB/T 42037—2022中9.2的相关要求。

7.3 服务域网络安全

7.3.1 接入鉴权与通信安全

接入鉴权与通信安全具备安全措施包括且不限于：
a) 平台之间的接口通信宜进行双向身份认证；
b) 接口请求宜采用接入鉴权的认证机制进行身份校验与完整性保护；
c) 鉴权算法宜采用国家密码管理准用的的密码算法；
d) 平台间传输的数据宜采用加密保护措施，防止数据在传输过程中被窃听、篡改或伪造。

7.3.2 网络边界防护

网络边界防护具备安全措施包括且不限于：
a) 通信平台宜部署边界防护设备，包括但不限于防火墙、入侵检测或入侵防御系统；
b) 宜通过技术措施防范针对网络平台相关设施的侵入，操控，保证网络域边界清晰、控制平面可控；
c) 宜根据业务功能与安全保护等级，必要时划分为不同的安全域；域间边界宜部署访问控制机制，禁止非授权跨域访问；虚拟化环境下的租户网络宜实施强隔离；
d) 准入流量隔离：未经身份鉴别的终端所产生的流量宜限制在受限的隔离区域，仅允许其访问认证服务器及补丁升级服务；准入流量宜实施速率限制与深度检测，防止未授权设备发起扫描或攻击；
e) 防范针对卫星链路、地面传输链路及关键网元的拒绝服务攻击（DoS / DDoS）、资源耗尽攻击及路由劫持。可通过于冗余设计、流量清洗及业务弹性恢复的功能提供提升可用性；
f) 宜采用安全网关、堡垒机等进行远程运维通道的加密与控制。

7.3.3 跨域隔离与流量监控

重要网络区域和其它网络区域之间有可靠的技术隔离措施与流量监控，包括且不限于：
a) 宜进行安全域划分，如依据业务和管理的规划将通信平台网络划分出管理域、业务域、运控维护域等；
b) 部署多层防火墙、入侵防御系统（IPS）、Web 应用防火墙（WAF）等，实现分区隔离和异常行为拦截；
c) 对用户接入的控制：对不同用户群体、不同安全保护等级的业务流量宜在接入层实施逻辑隔离；宜采用网络分片，以专用承载通道实现不同级别用户流量的隔离；隔离策略宜与用户认证结果及签约信息动态关联；
d) 宜通过通信协议及安全协议的综合设计防范与阻断协议欺骗、中间人攻击、重放攻击、DoS/DDoS 等恶意流量。

7.3.4 网络节点主机安全

宜对承载卫星通话及短消息业务的服务器、虚拟机、容器等主机设备防范漏洞利用、恶意代码植入、权限错误及日志篡改。网络主机具备安全措施包括且不限于：

a) 提供主机安全的系统加固、补丁管理及运行时的完整性监控等控制措施；
b) 宜部署恶意代码防护机制，并及时更新规则库与特征库；
c) 宜建立访问控制策略，并定期对访问控制规则进行复核与优化；
d) 当出现非法访问、异常流量或系统安全性受到破坏时，系统宜能够自动告警，并保留相关安全事件记录。

7.3.5 业务 QoS 保障维护

为使卫星通话与短消息业务 QoS 指标满足用户安全要求（即用户对运营商或服务提供商提供相关业务的具体安全要求），宜进行有计划、有组织的SRM保证以满足 QoS 保障中安全性要求，且满足：

a) 网络设备的业务处理能力、网络各个部分带宽满足业务高峰期需求；
b) 提供安全通信网络和关键网络设备、关键安全设备及密码设备的硬件冗余；
c) 宜支持链路备份，使得业务链路中断，能启用备份链路或重新路由到可用链路。

7.3.6 设施与环境安全

通信平台的设施与环境安全宜符合GB/T 9361。

注：使用在工控系统、室外、野外等特殊场景的设施与环境安全符合相应的场景及用户要求。

7.4 感知预警与攻击防御

7.4.1 态势与数据模型感知与预警

网络安全态势感知通用技术要求宜符合 GB/T 42453。可通过人工智能等技术，进一步完善安全态势与数据模型的分析、监测与预警的能力，相关能力宜包括且不限于异常检测覆盖率、告警时效、数据模型的可信性评估等。

7.4.2 攻击面管理与主动防御

各种类型网络攻击的判定条件可参考 GB/T 37027—2025 中6.2。网络攻击和网络攻击事件的判定方法可参考 GB/T 37027—2025 附录C。

攻击面管理与主动防御措施可包括且不限于：

a) 通过被动发现、主动探测和网管采集等方式对管理单元资产及状态进行动态识别；
b) 主动减少非必要暴露的卫星通话与短消息资产、服务、数据等信息，阻断潜在的攻击路径；
c) 依托人工智能等技术进行持续的入侵行为分析及自主安全验证；
d) 通过人工智能的算法，对攻击类型、判定条件进行学习进化，实现主动防御的能力演进及
e) 应急处置；
f) 将攻击面管理、主动防御技术与现有安全能力体系的集成与数据互通，形成协同防御合力；
g) 依托大数据、人工智能和可视化技术，实现量化风险管理，支撑可持续运营。

8 数据安全与个人信息保护

8.1 基本要求

卫星通话与短消息的通信数据个人信息保护安全措施与管理因素包括且不限于：

a) 保护范围宜包括且不限于用户身份、位置、通信内容及用户元数据等个人信息；

b） 在处理相关数据时，服务提供者宜履行数据安全和个人信息保护义务，遵循合法、正当、必要、诚信原则；
c） 宜建立全生命周期的数据保护策略，涉及数据出境的，宜遵守国家相关规定。

8.2 通信数据分类与分级

8.2.1 需考虑的因素

服务提供者宜落实数据分类分级保护相关要求，需考虑的因素包括且不限于：
a） 在推出新的卫星通信服务或宜用新技术前，宜开展个人信息安全影响评估，参照 GB/T 39335 执行；
b） 对卫星通话与短消息系统中的数据进行分级分类，宜符合 GB/T 43697，并采取保护措施保证全生命周期的数据安全；
c） 卫星通话与短消息服务的境内用户数据应当在境内地面设施处理，不得经由卫星转发至境外关口站、地球站等设施。

8.2.2 数据类别

根据通信数据的性质和敏感程度，通信数据可划分为以下类别：
a） 身份数据：包括姓名、证件号码、IMSI、电话号码等；
b） 通信内容数据：包括通话录音、短消息正文等；
c） 位置数据：包括实时地理位置、历史轨迹等；
d） 服务使用元数据：包括通信时间、通信时长、通信对端号码等。

8.3 安全措施

8.3.1 数据最小化原则

服务提供者采集数据宜仅限于实现服务目的的最小范围。不宜强制采集与业务无关的个人信息。

8.3.2 身份信息保护

身份信息保护的措施包括且不限于：
a） 终端在接入卫星网络时，宜优先采用临时识别码（如 TMSI）替代永久识别码（如 IMSI）在空中接口传输；
b） 宜采取加密等技术措施防止攻击者在空口通过窃听获取用户永久身份标识。

8.3.3 通信内容保护

通信内容的保护的措施包括且不限于：
a） 卫星通话语音数据在空口传输过程中宜采用符合国家密码管理准用的密码算法进行加密；
b） 卫星短消息数据在存储和传输过程中宜采用端到端加密、链路加密等措施，确保内容不被非法窃取；
c） 推荐对即时消息类宜采用端到端加密技术。

8.3.4 位置信息保护

位置信息保护的措施包括且不限于：
a） 宜对用户地理位置信息的传输和存储采取加密保护；
b） 除法律法规另有规定或用户另行授权外，不宜将用户实时位置信息披露给第三方；

c） 可根据业务需求，提供模糊化位置服务选项，允许用户仅授权大致位置而非精确位置。

8.3.5 传输与存储安全

传输与存储过程的个人信息保护措施包括且不限于：

a） 卫星馈电链路和用户链路宜采取加密措施，防止数据在传输过程中被截获或篡改；

b） 境内用户数据宜在境内地面设施进行处理和存储，未经批准不得由境外关口站或设施处理；

c） 宜具备重要数据备份和恢复能力，防止数据意外丢失；

d） 备份数据宜进行完整性校验，并定期验证恢复能力；

e） 短消息内容在用户设备本地存储、在通信平台存储、及在通信传输链路的存储转发（若有）时，宜根据数据的安全级别采取相宜的加密措施。

8.3.6 数据安全审计

数据安全审计管理具备安全措施宜包括且不限于：

a） 平台宜建立数据备份机制，定期开展本地备份与异地备份；

b） 宜对重要数据的访问、修改、删除等操作进行日志记录；

c） 宜定期开展日志审计与数据安全审计，形成审计报告，并对发现的问题及时整改。

8.4 个人信息保护安全策略与用户权利保障

8.4.1 个人信息保护安全策略

服务提供者宜制定并向服务提供者公开个人信息安全策略，至少宜包括：

a） 收集、使用个人信息的目的、方式和范围；

b） 数据存储的地点和期限；

c） 用户对其个人信息的查询、更正、删除等权利及行使方式；

d） 数据泄露事件的应急处置流程及通知机制。

8.4.2 用户权利保障

服务提供者宜提供用户权利保障机制，至少包括：

a） 服务提供者宜保障用户的知情权与选择权，为用户提供便捷的渠道撤回同意、注销账号、删除个人信息；

b） 服务提供者宜建立健全投诉举报机制，及时响应用户关于个人信息泄露或违规处理的投诉。

8.5 第三方接入与管理

服务提供者宜制定并公开第三方接入与管理政策，至少包括：

a） 卫星通信平台对接入的第三方应用服务提供者宜进行安全评估；

b） 宜与第三方签订数据保护协议，明确其数据处理的权限和责任，第三方处理用户数据的行为参考本文件提出的建议；

c） 宜对第三方应用访问敏感个人信息（如通信录、位置）的行为进行实时监控和动态授权管理。

8.6 个人信息泄露应急响应

服务提供者宜制定个人信息泄露应急响应机制，至少包括：

a） 宜建立个人信息安全事件应急响应机制，明确事件分类、分级、处置流程和责任部门；

b） 发生或可能发生用户数据泄露、损毁、丢失时，宜立即启动应急响应，采取补救措施，并按照规定及时告知受影响的用户并向有关主管部门报告。

9 密码安全

9.1 密码算法

9.1.1 语音及短消息加密

卫星通话语音、短消息数据的加密宜采用符合国家密码算法使用要求的对称密码算法。当采用SM4算法时符合GB/T 32907；采用祖冲之序列密码算法（ZUC）时符合GB/T 33133。采用可鉴别的加密机制时符合GB/T 36624。

宜通过提升密钥长度等方法提升抗量子计算攻击能力。

9.1.2 密钥分发

密钥管理模块向用户设备进行密钥分发、用户设备之间进行密钥协商/密钥交换时，相应报文数据宜进行加密及完整性保护。宜采用符合 GB/T 36624 要求的可鉴别加密模式 GCM 或 CCM。

9.1.3 实体鉴别

用户设备的实体鉴别方法宜符合以下一种或者多种：

a） 采用符合 GB/T 15843.2—2024 的鉴别式加密的实体鉴别；

b） 采用符合 GB/T 15843.3—2023 的数字签名技术的实体鉴别；

c） 采用符合 GB/T 15843.4—2024 的密码校验函数的实体鉴别。

9.1.4 数字签名

用户设备密码模块与密钥管理模块之间可选用非对称密码算法进行数字签名、签名验签：

a） 采用 SM2 密码算法宜符合 GB/T 32918.2；

b） 可采用符合国家密码算法使用要求的后量子密码算法进行签名运算。

注：在国家相关标准发布前作为前瞻性指引。

9.1.5 消息鉴别

用户设备密码模块、密钥管理模块可采用杂凑算法计算消息摘要，如采用GB/T 32905规定SM3杂凑算法。

用户设备密码模块、密钥管理模块进行消息鉴别码计算时，建议采用已经发布的消息鉴别码计算方案，包括且不限于：

a） 符合 GB/T 15852.1—2020 的分组密码的机制构造消息鉴别码；

b） 符合 GB/T 15852.2—2024 的专门设计的杂凑函数的机制构造消息鉴别码；

c） 符合 GB/T 15852.3—2019 的泛杂凑函数的机制构造消息鉴别码。

9.2 密钥管理

9.2.1 密钥分类

用户设备的密码种类主要包括鉴权密钥、密钥加密密钥和会话密钥等，对这些密钥进行密钥生命周期管理是必要的。

用户设备密钥的分发一般包括密钥分发或密钥协商：

a) 密钥分发：指密钥管理模块根据密钥获取请求分别为主叫和被叫分发会话密钥，以实现会话密钥在通信双方的同步；

b) 密钥协商：指主叫或被叫中的一方与密钥管理模块获取会话密钥或通过本地噪声源产生会话密钥，再通过主叫和被叫之间的密钥协商协议将会话密钥同步给另一方。

9.2.1.1 鉴权密钥

鉴权密钥用于用户设备的实体鉴别。实体鉴别可用于用户设备与通信平台之间、用户设备与密钥管理模块之间，以及用户设备与用户设备之间的鉴权。

鉴权密钥可以是非对称密钥对，包含签名鉴权密钥对和加密密钥对；鉴权密钥也可是对称密钥，由需要鉴权的通信双方共享。

9.2.1.2 密钥加密密钥

密钥加密密钥（KEK）宜在对密码模块初装时完成预置，预置的KEK数量宜满足用户设备密钥维护周期内的使用，可支持在线更新。该密钥用于：

a) 用户设备密码模块从密钥管理模块进行会话密钥获取的加密及完整性保护；

b) 用户设备主叫、被叫之间进行密钥协商/密钥交换时，对会话密钥等数据进行加密及完整性保护。

9.2.1.3 会话密钥

会话密钥分为会话加密密钥和会话鉴别密钥，其中：

a) 会话加密密钥用于加密主、被叫之间通信的通话信息和数据，保障通话信息和数据的机密性。用户设备一方使用会话加密密钥加密语音或数据，用户设备另一方使用会话加密密钥解密语音或数据；

b) 会话鉴别密钥用于保证双方通话信息和数据的完整性。用户设备一方使用会话鉴别密钥对通话信息或数据进行完整性保护，用户设备另一方使用会话鉴别密钥进行通话信息或数据的完整性校验。

用户设备的会话密钥用完即刻销毁，不再复用。会话密钥密文在密钥管理模块可继续保存。

9.2.2 密钥分发

9.2.2.1 交互过程

密钥分发的业务过程通常在主叫向被叫发起加密通信过程前发起。加密通信前，主叫和被叫都已完成用户接入鉴权。主叫和被叫分别向密钥管理模块申请端到端会话密钥。一次加密通话的会话密钥申请可以从主叫或被叫任意一方发起，申请方获得会话密钥的特征信息（如用户ID、会话密钥ID等）后，通过通信平台同步给另一方。另一方据此特征信息向密钥管理模块获取本次会话密钥。

密钥分发的数据报文在密钥管理模块后台存储，用于会话密钥的恢复取证。

密钥分发业务流程可以有不同的顺序及步骤。附录A.4以主叫首先发起会话密钥申请为例，提供一种密钥分发的业务交互流程。

9.2.2.2 密钥分发请求

用户设备的密钥分发请求将被发送到密钥管理模块并得到服务。该请求数据将被发送到密钥管理模块。密钥分发请求数据的传输过程可采用不同的方法，包括且不限于：

a) 主叫和被叫的密钥分发请求数据分别通过 TCP/IP 通信协议与密钥管理模块进行交互；

b) 主叫和被叫的密钥分发请求报文可分别通过通信平台转发，通信报文格式由通信平台定义。

9.2.2.3 密钥分发响应

密钥管理模块对用户设备密钥分发请求的处理响应。密钥分发响应数据的传输过程可采用不同的方法，包括且不限于：

a） 密钥管理模块的密钥分发响应数据可直接通过 TCP/IP 协议与用户设备进行交互；
b） 密钥管理模块的密钥分发响应报文可通过通信平台转发，通信报文格式由通信平台定义。

9.2.3 密钥协商

9.2.3.1 交互过程

用户设备之间通过密钥协商/密钥交换完成双方会话密钥的同步。会话密钥分发过程采用请求—响应模式。用户设备任意一方申请会话密钥获得成功后，宜通过密钥协商协议向另一方进行密钥同步。

当加密通信结束后，用户设备宜释放会话密钥资源。

密钥管理模块的密钥分发数据报文在后台存储，用于会话密钥的恢复取证。

密钥协商业务流程可以有不同的顺序及步骤。附录A.5以主叫发起密钥协商请求，被叫从密钥管理模块获取会话密钥并同步给主叫的业务流程为例，提供一种密钥协商的业务交互流程实例。

9.2.3.2 密钥协商请求

用户设备之间的密钥协商请求数据将从用户设备的发送方分发到用户设备的接收方。密钥协商请求数据的传输过程可采用不同的协议方法。

9.2.3.3 会话密钥申请

用户设备之间每次进行卫星通话或收发短消息时，会话密钥宜重新申请。会话密钥支持更新，更新过程与重新申请一致。会话密钥申请的方法可包括且不限于：

a） 任意请求方向密钥管理模块申请会话密钥；
b） 条件具备时，主叫或被叫可从本地物理噪声源获得会话密钥；
c） 上述情况都不满足时，主叫或被叫可从密码模块初装的基础密钥库按配置的选取策略获取会话密钥，且满足一话一密的要求。

9.2.3.4 密钥协商响应

用户设备接收方对密钥协商请求数据进行验证处理，按照双方协商的具体方法进行处理，并生成密钥协商响应报文。

9.2.4 密钥生存周期管理

密钥的随机性检测宜符合GB/T 32915，密钥生存周期管理参见GB/T 39786—2021中附录B。

10 安全管理

安全管理宜包括对卫星通话与短消息所涉及的应用安全、网络安全、密码密钥及数据安全等多层面，开展必要的安全管理；技术管理措施还包括且不限于：

a） 卫星短消息宜能够通过不良消息管理功能或相关系统实现对不良消息的识别和处理等；
b） 卫星通话宜具备不良呼叫号码检测分析能力；
c） 卫星通话宜具备向卫星通话终端用户提供疑似不良呼叫号码的风险提示服务能力；
d） 通信平台宜自动对卫星通话与短消息相关操作进行日志记录，如安全接入、退出；密钥管理；用户注册信息登记或变更等，保存管理周期内的日志信息，并通过授权及数据完整性保护等措施防止日志信息的删除、篡改、伪造等。确保系统操作的可追溯及日志的真实性、完整性及可用性；
e） 宜定期或根据安全事件控制策略对密码应用安全日志进行审计核查，排查违规操作、安全漏洞，优化密码安全策略；
f） 通信平台及用户设备宜具备监测卫星通话与短消息业务过程中的异常或错误情况，并及时触发告警、主动故障规避等技术措施；

g） 通信平台及用户设备的安全接入、卫星通话及短消息应用时的安全隐患或风险当达到规定的安全判定阈值（门限）时启动应急措施，根据安全策略的配置，如报警、限流、列入黑名单、阻断等；

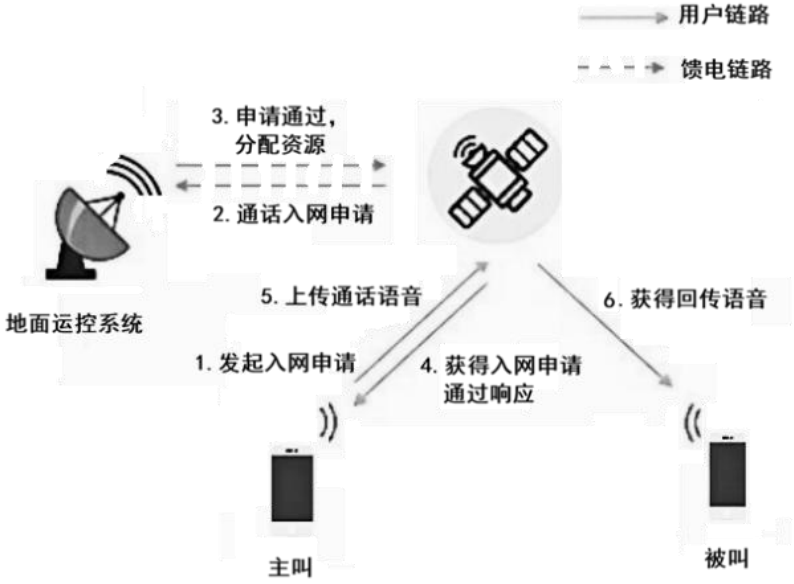
h） 通信平台应建立应急恢复、备用技术措施等保障系统安全功能及服务的连续性及可靠性；

i） 宜定期开展机房环境安全检查与风险评估。

附 录 A
（资料性）
业务流程实例

A.1 卫星通话业务流程实例

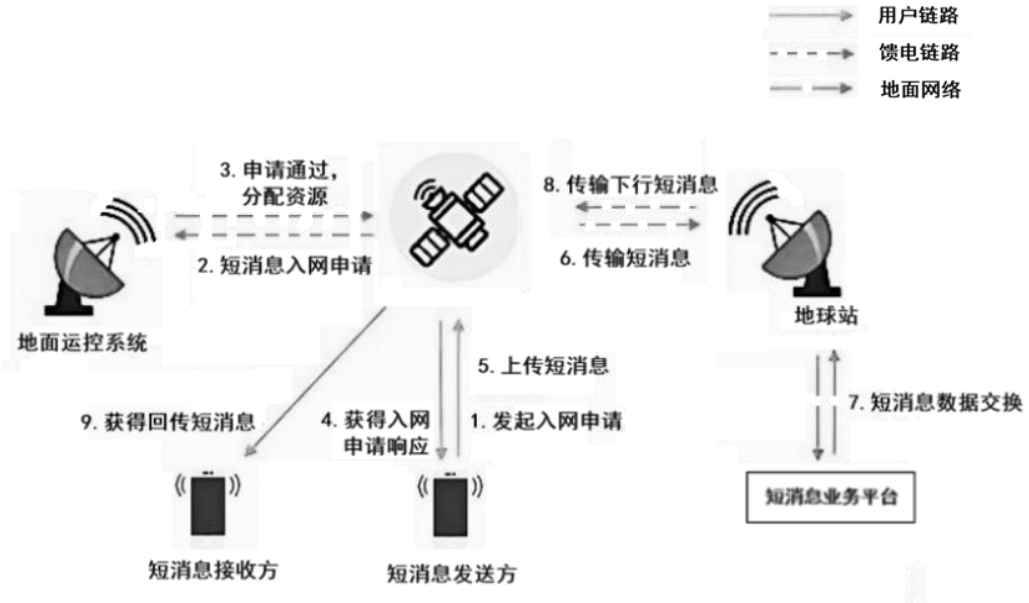
图A.1 给出了主叫直连接入卫星，经地面运控系统授权接入，与被叫进行通话的一种业务流程实例。



图A.1 直连接入卫星通话业务流程实例

A.2 卫星短消息业务流程实例

图A.2 给出了用户设备短消息发送方直连接入卫星，经地面运控系统授权接入、短消息业务平台完成业务数据处理及数据交换，并经地球站转发给信息接收方的一种短消息通信业务流程实例。



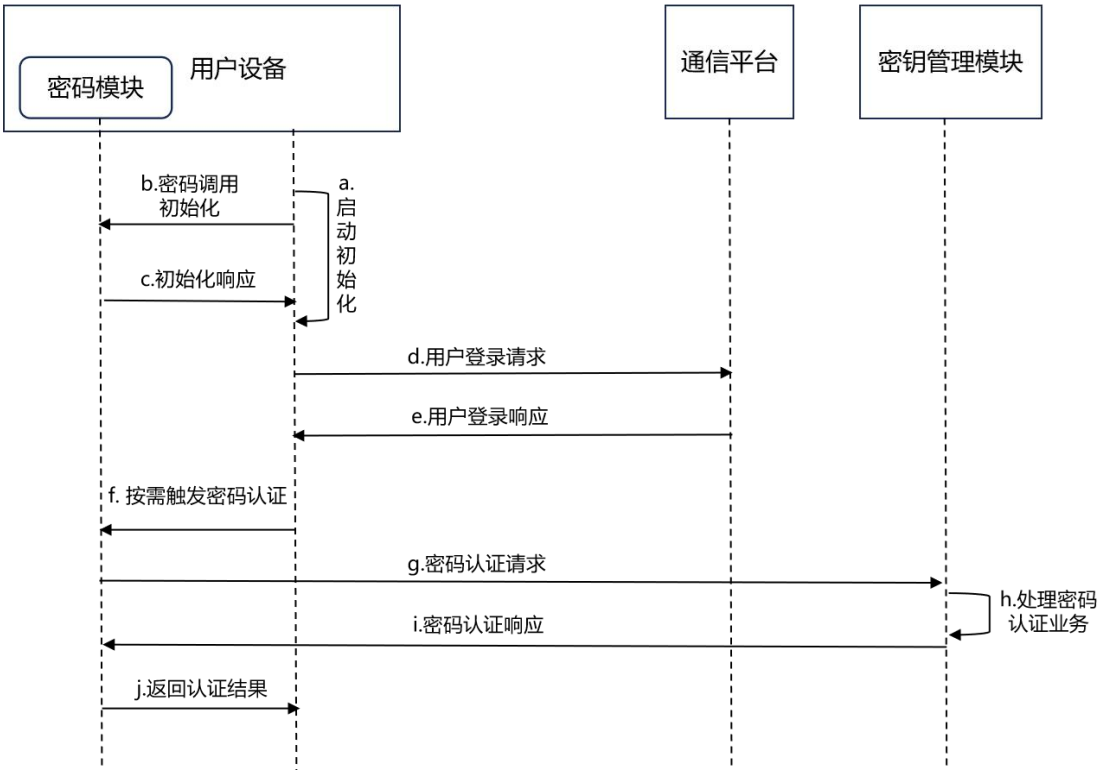
图A.2 直连接入卫星短消息业务流程实例

A.3 接入鉴权业务流程实例

不同通信平台及密钥管理模块在用户接入鉴权时可以有不同的顺序及步骤。一种用户接入鉴权的业务流程实例见图A.3。

在进行用户接入鉴权前，用户设备宜已完成在通信平台及密钥管理模块的用户注册、用户密码资源在密码模块的初装。

对卫星用户的登录认证，用户设备通过登录消息附带请求及响应的方法向通信平台完成用户登录。当用户设备向密钥管理模块获取本次会话密钥前，宜完成在密钥管理模块的身份认证。



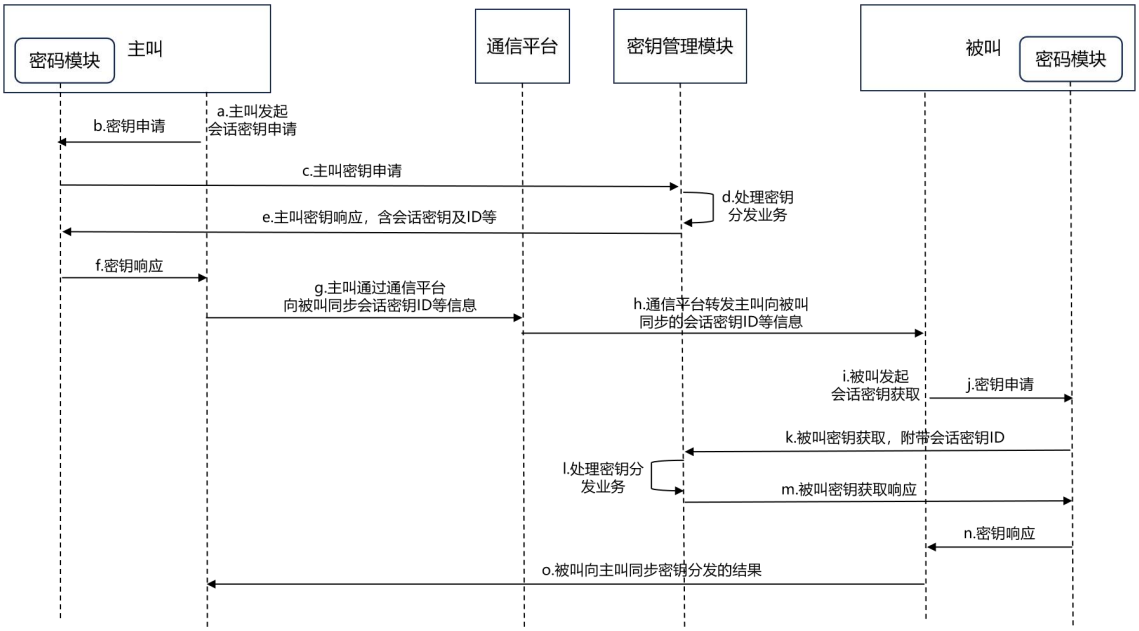
图A.3 接入鉴权业务流程实例

用户接入鉴权的交互过程包括且不限于如下过程：

a) 用户设备启动初始化，进行自检；
b) 对密码模块进行密码调用初始化。若密码模块初始化成功，则继续下面的过程，否则提示错误，中止后续过程；
c) 密码模块初始化，完成自检，并返回初始化响应；
d) 用户设备向通信平台发送用户登录请求，请求数据中宜包括用户的账号、认证信息、协调性配置信息等参数（如加密算法、协议配置等）；
e) 通信平台收到用户登录请求后，校验账号、认证信息，并获取协调性配置信息用于后续操作；用户接入鉴权通过后，通信平台向用户设备返回用户登录成功响应；否则，通信平台向用户设备返回用户登录失败响应，并释放该用户登录状态及配置信息等；
f) 当密码模块要向密钥管理模块获取会话密钥前，用户设备向密码模块触发密码认证；
g) 密码模块向密钥管理模块发起密码认证请求；
h) 密钥管理模块处理密码认证业务；
i) 密钥管理模块向密码模块返回密码认证响应；
j) 密码模块向用户设备返回认证结果数据。

A.4 密钥分发业务流程实例

密钥分发业务流程可以有不同的顺序及步骤。以主叫首先发起会话密钥申请为例，提供一种密钥分发的业务交互流程见图A.4。



图A.4 密钥分发业务流程实例

以主叫发起会话密钥申请为例，密钥分发交互过程如下：

a) 主叫发起会话密钥申请；
b) 向密码模块发起密钥申请；
c) 密码模块向密钥管理模块进行主叫端到端会话密钥的申请；
d) 密钥管理模块处理密钥分发业务；
e) 密钥管理模块向主叫密码模块返回密钥响应，若密钥响应成功，响应信息中包括会话密钥密文及 ID（如用户 ID、密钥 ID 等）等信息；
f) 密码模块将密钥响应处理结果、密钥 ID、会话密钥融合模式等信息返回给主叫。若密钥响应处理成功，则继续后续步骤。否则报错退出；
g) 主叫通过通信平台将 ID 信息、会话密钥融合模式等信息同步给被叫；
h) 通信平台转发主叫向被叫同步的会话密钥 ID、会话密钥融合模式等信息；
i) 被叫启动会话密钥获取；
j) 被叫通过密码模块发起本次加密通信的会话密钥获取，申请中携带会话密钥 ID 等信息；
k) 被叫密码模块根据会话密钥 ID 等密钥信息，向密钥管理模块进行本次端到端会话密钥密文的获取；
l) 密钥管理模块处理密钥分发业务；
m) 密钥管理模块向被叫密码模块返回会话密钥获取响应，响应信息中包括会话密钥密文等信息；
n) 被叫密码模块将密钥获取的响应处理结果、会话密钥融合模式等信息返回给被叫；
o) 被叫向主叫同步密钥分发的处理结果、会话密钥融合模式等信息。若密钥分发成功，主叫、被叫后续将采用本次获得的会话密钥进行加密通信。否则，主叫和被叫分别提示错误信息。

步骤g)和步骤o)中描述的主叫和被叫交互信息中包括会话密钥融合模式的信息，该信息用于主叫和被叫根据该信息的值，确定对会话密钥获取结果的应用策略，会话密钥融合模式可包括：强制密钥分发、密钥协商、其他；应用策略可包括且不限于：

——通信双方均为强制密钥分发模式时，若会话密钥获取失败，则会话协商失败；

——通信双方均为密钥协商模式时，若密钥协商失败，则会话协商失败；

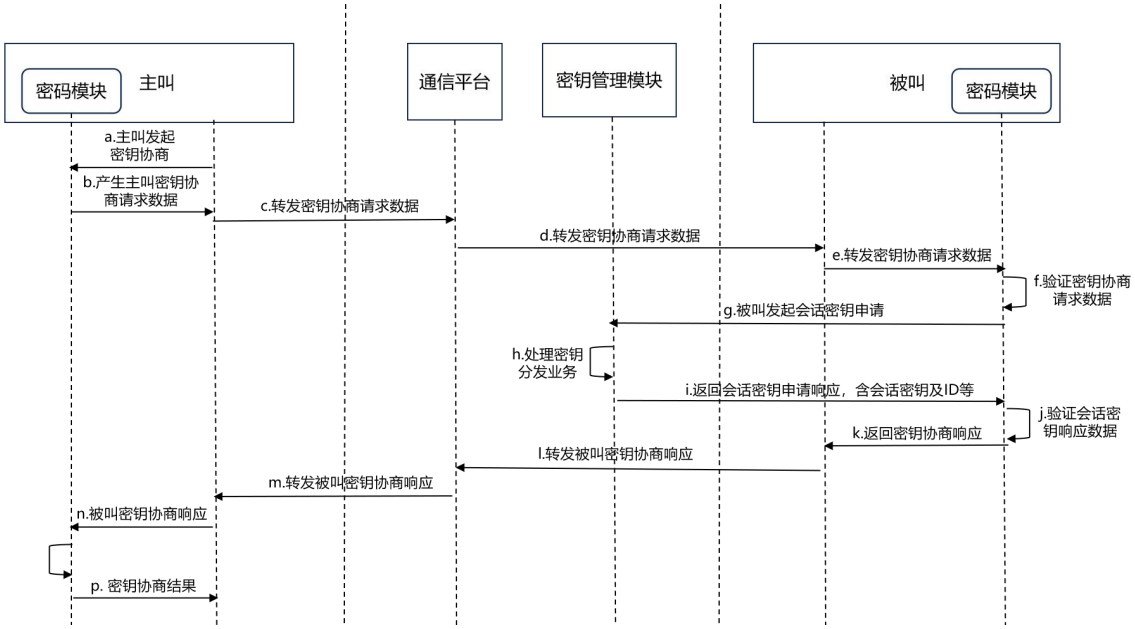
——一方为强制密钥分发模式，另一方为密钥协商或其他模式时，按照强制密钥分发模式执行；

——一方为密钥协商模式，另一方为其他时，按照密钥协商模式执行；

——通信双方均为其他模式时，则由主叫可选择其他密钥分发方式，如从预存密钥库中获取本次会话密钥。

A.5 密钥协商业务流程实例

密钥协商业务流程可以有不同的顺序及步骤，本实例以主叫发起密钥协商请求，被叫从密钥管理模块获取会话密钥并同步给主叫的业务流程为例，见图A.5。



图A.5 密钥协商业务流程实例

图A.5中，主要交互过程包括：

a) 主叫通过密码模块发起密钥协商请求；

b) 密码模块产生密钥协商请求数据给主叫；

c) 主叫通过通信平台转发密钥协商请求数据给被叫；

d) 通信平台转发密钥协商请求数据给被叫；

e) 被叫将密钥协商请求数据发给本地密码模块；

f) 被叫密码模块验证密钥协商请求数据，并得到本次会话密钥获取策略：由被叫通过密钥管理模块获取本次会话密钥；

g) 被叫密码模块向密钥管理模块发起会话密钥申请；

h) 密钥管理模块处理密钥分发业务；

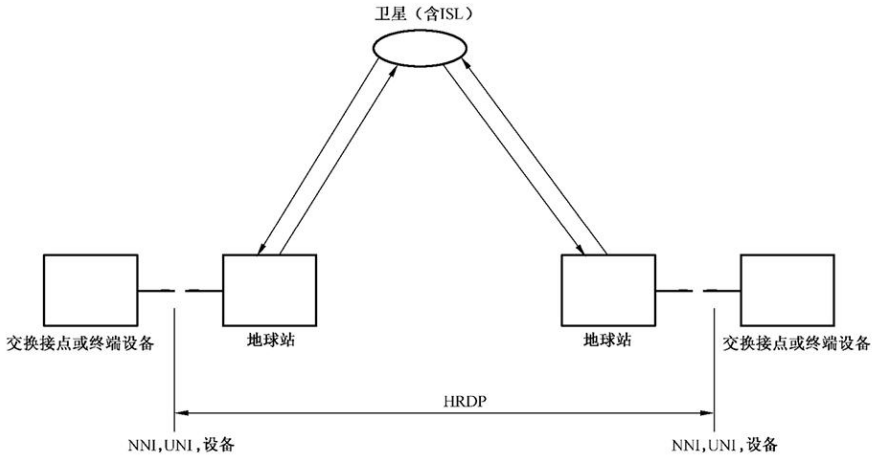
i) 密钥管理模块向被叫密码模块返回会话密钥申请响应，响应信息中包括会话密钥密文及 ID 等信息；

j) 被叫密码模块验证会话密钥响应数据，验证通过后获得本次通话的会话密钥；

k) 被叫密码模块将密钥协商响应数据返回给被叫；
l) 被叫通过通信平台向主叫转发密钥协商响应数据；
m) 通信平台转发密钥协商响应数据给主叫；
n) 主叫向主叫密码模块转发密钥协商响应数据，密钥协商响应数据中含会话密钥密文及 ID 等信息；
o) 主叫密码模块验证密钥协商响应数据，并获得会话密钥及 ID 等信息；
p) 主叫密码模块将密钥协商处理的结果返回给主叫。主叫根据处理结果了解并显示相应过程的状态信息。若密钥协商过程处理成功，主叫、被叫后续将采用协商同步的会话密钥进行本次加密通信。

附 录 B
（资料性）
通用的数字卫星通信假设参考数字通道

非直连接入通用的数字卫星通信假设参考数字通道（HRDP）如图 B.1 所示。



NNI:网络节点接口；
UNI:用户网络接口；
ISL:卫星间链路。

图B.1 假设参考数字通道示意图

HRDP 由具有 1 个或多个 ISL 的 1 个或多个地—星—地链路组成。HRDP 不仅适用于点—点业务，而且适用于多点和非对称业务。对于位置分集地球站，HRDP 还应包括把分集地球站连到分集交换点的必要的陆上链路和任何相关设备。在用户终端或地球站内（HRDP相关的）包括 RF / IF，解调 / 调制，误码校正，存储，处理和复用 / 分解设备等。

注1：地球站和与它相连的陆上数字交换机之间的链路应当属于陆上网络的一部分，它不应包括在 HRDP 内。

注2：终端设备或交换点可以以任何约定的速率与 HRDP 接口。

注3：本 HRDP 不适用于广播卫星业务端—端链路。

参 考 文 献

[1] GB/T 22080 信息技术 安全技术 信息安全管理体系 要求
[2] GB/T 35273 信息安全技术 个人信息安全规范
[3] GB/T 35439 空间站应用有效载荷安全性、可靠性与维修性保证通用要求
[4] GB/T 44086.1 北斗三号区域短报文通信用户终端信息接口 第 1 部分：用户管理模块接口