短信解码设计文档

**更改历史**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 状态 | 日期 | 责任人 | 更改原因 |
| 1.0 | 草稿 | 2020-03-19 | Leo.Liu(刘永琪) | 创建 |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[短信解码设计文档 1](#_Toc35536285)

[1 介绍 3](#_Toc35536286)

[1.1 文档目的 3](#_Toc35536287)

[1.2 术语和缩写 3](#_Toc35536288)

[1.3 参考文档 3](#_Toc35536289)

[2 内容简介 4](#_Toc35536290)

[3 LTE短信 4](#_Toc35536291)

[3.1 LTE短信的消息格式 4](#_Toc35536292)

[3.1.1 Uplink NAS Transport 4](#_Toc35536293)

[3.1.2 CP-User data分为三种类型 7](#_Toc35536294)

[3.1.3 RP-DATA 9](#_Toc35536295)

# 介绍

## 文档目的

这里短信相关的协议流程，编码格式，用于指导解码工具的开发。

## 术语和缩写

CDMA：Code Division Multiple Access，码分多址

## 参考文档

《TS 24.301 》

《TS 24.011 Point-to-Point (PP) Short Message Service (SMS)》短信的格式

《XS.0057》

《TS 23.040》

# 内容简介

本文档介绍手机通讯业务中的短信业务，主要包括短信在各个制式下的交互流程，短信编码方案，以及解码的设计方案。

目前手机通讯中，主要使用到的短信业务分为如下五类：

1. IMS短信
2. LTE NAS短信
3. GSM短信
4. WCDMA短信
5. CDMA短信

其中，短信的编码方式主要有两种：GSM的编码方式，和CDMA的编码方式。本文将根据使用的频率对各种短信业务分别予以分析。

# LTE短信

LTE短信业务通过LTE的NAS信令发送。承载的消息为：

1. Uplink NAS Transport，UE发送短信
2. Downlink NAS Transport，UE接收短信

参考文档：《TS 24.301》

## LTE短信的消息格式

### Uplink NAS Transport

UE发送此消息给网络，用于携带SMS消息。消息格式如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Element | Type/Reference | Presence | Format | Length | Position |
| Protocol discriminator | Protocol discriminator  9.2 | M | V | 1/2 | 低4bit |
| Security header type | Security header type  9.3.1 | M | V | 1/2 | 高4bit |
| Uplink NAS transport message identity | Message type  9.8 | M | V | 1 |  |
| NAS message container | NAS message container  9.9.3.22 | M | LV | 3-252 |  |

表中的各个域的取值如下：

#### Protocol discriminator

Protocol discriminator的取值为首字节的低4bit，各个bit组合的含义如下表。

|  |  |
| --- | --- |
| **bits 4 3 2 1** | **Description** |
| 0 0 0 0 | group call control |
| 0 0 0 1 | broadcast call control |
| 0 0 1 0 | EPS session management messages |
| 0 0 1 1 | call control; call related SS messages |
| 0 1 0 0 | GPRS Transparent Transport Protocol (GTTP) |
| 0 1 0 1 | mobility management messages |
| 0 1 1 0 | radio resources management messages |
| 0 1 1 1 | EPS mobility management messages |
| 1 0 0 0 | GPRS mobility management messages |
| 1 0 0 1 | SMS messages |
| 1 0 1 0 | GPRS session management messages |
| 1 0 1 1 | non call related SS messages |
| 1 1 0 0 | Location services specified in 3GPP TS 44.071 [8a] |
| 1 1 1 0 | extension of the PD to one octet length |
| 1 1 1 1 | used by tests procedures described in 3GPP TS 44.014 [5a], 3GPP TS 34.109 [17a], 3GPP TS 36.509 [26] and 3GPP TS 38.509 [29]. |

#### Security header type

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security header type (octet 1) | | | | |
|  | | | | |
| 8 | 7 | 6 | 5 |  |
| 0 | 0 | 0 | 0 | Plain NAS message, not security protected |
|  |  |  |  |  |
|  |  |  |  | Security protected NAS message: |
| 0 | 0 | 0 | 1 | Integrity protected |
| 0 | 0 | 1 | 0 | Integrity protected and ciphered |
| 0 | 0 | 1 | 1 | Integrity protected with new EPS security context (NOTE 1) |
| 0 | 1 | 0 | 0 | Integrity protected and ciphered with new EPS security context (NOTE 2) |
| 0 | 1 | 0 | 1 | Integrity protected and partially ciphered NAS message (NOTE 4) |
|  |  |  |  |  |
|  |  |  |  | Non-standard L3 message: |
| 1 | 1 | 0 | 0 | Security header for the SERVICE REQUEST message |
|  |  |  |  |  |
| 1 | 1 | 0 | 1 | These values are not used in this version of the protocol. |
| to | | | | If received they shall be interpreted as '1100'. (NOTE 3) |
| 1 | 1 | 1 | 1 |  |
|  |  |  |  |  |
| All other values are reserved. | | | | |
|  | | | | |
| NOTE 1: This codepoint may be used only for a SECURITY MODE COMMAND message.  NOTE 2: This codepoint may be used only for a SECURITY MODE COMPLETE message.  NOTE 3: When bits 7 and 8 are set to '11', bits 5 and 6 can be used for future extensions of the SERVICE REQUEST message.  NOTE 4: This codepoint may be used only for a CONTROL PLANE SERVICE REQUEST message. | | | | |

#### Message Type

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Bits** | | | | | | | | **Description** | **DEC** | **HEX** |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |  |
| 0 | 1 | - | - | - | - | - | - | EPS mobility management messages |  |  |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | Attach request | 65 | 41 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | Attach accept | 66 | 42 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | Attach complete | 67 | 43 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | Attach reject | 68 | 44 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | Detach request | 69 | 45 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | Detach accept | 70 | 46 |
|  |  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | Tracking area update request | 72 | 48 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | Tracking area update accept | 73 | 49 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | Tracking area update complete | 74 | 4A |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | Tracking area update reject | 75 | 4B |
|  |  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | Extended service request | 76 | 4C |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | Control plane service request | 77 | 4D |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | Service reject | 78 | 4E |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | Service accept | 79 | 4F |
|  |  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | GUTI reallocation command | 80 | 50 |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | GUTI reallocation complete | 81 | 51 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | Authentication request | 82 | 52 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | Authentication response | 83 | 53 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | Authentication reject | 84 | 54 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | Authentication failure | 92 | 5C |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | Identity request | 85 | 55 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | Identity response | 86 | 56 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | Security mode command | 93 | 5D |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | Security mode complete | 94 | 5E |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | Security mode reject | 95 | 5F |
|  |  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | EMM status | 96 | 60 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | EMM information | 97 | 61 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | Downlink NAS transport | 98 | 62 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | Uplink NAS transport | 99 | 63 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | CS Service notification | 100 | 64 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | Downlink generic NAS transport | 104 | 68 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | Uplink generic NAS transport | 105 | 69 |

#### NAS message container

此信元用于封装UE与网络之间的SMS消息，信元的长度从最小的4个字节到最大的253个字节。

各个字节的分布如下图。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NAS message container IEI | | | | | | | | octet 1 |
| Length of NAS message container contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
| NAS message container contents | | | | | | | |  |
|  | | | | | | | | octet n |

NAS message container contents (octet 3 to octet n)

This IE can contain an SMS message (i.e. CP-DATA, CP-ACK or CP-ERROR) as defined in subclause **7.2 in 3GPP TS 24.011** [13A].

### CP-User data

CP-User data分为三种类型：CP-DATA，CP-ACK，CP-ERROR。

#### CP‑DATA

The CP‑DATA message is sent between an MSC and an MS, in both directions. The message contains the user data to be relayed between the CM‑users, and associated parameters. See table 7.1/ 3GPP TS 24.011.

Table 7.1/3GPP TS 24.011: CP‑DATA message content

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information element | Reference | Presence | Format | Length |
| Protocol discriminator | 3GPP TS 24.007 | M | V | 1/2 octet |
| Transaction identifier | 3GPP TS 24.007 | M | V | 1/2 octet |
| Message type | Subclause 8.1.3 | M | V | 1 octet |
| CP‑User data | Subclause 8.1.4.1 | M | LV | ≤ 249 octets |

#### CP‑ACK

The CP‑ACK message is sent between an MSC and an MS, in both directions, and is used to acknowledge the reception of a CP‑DATA message. See table 7.2/3GPP TS 24.011.

Table 7.2/3GPP TS 24.011: CP‑ACK message content

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information element | Reference | Presence | Format | Length |
| Protocol discriminator | 3GPP TS 24.007 | M | V | 1/2 octet |
| Transaction identifier | 3GPP TS 24.007 | M | V | 1/2 octet |
| Message type | Subclause 8.1.3 | M | V | 1 octet |

#### CP‑ERROR

The CP‑ERROR message is sent between an MSC and an MS, in both directions, and used to convey error information. See table 7.3/3GPP TS 24.011.

Table 7.3/3GPP TS 24.011: CP‑ERROR message content

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information element | Reference | Presence | Format | Length |
| Protocol discriminator | 3GPP TS 24.007 | M | V | 1/2 octet |
| Transaction identifier | 3GPP TS 24.007 | M | V | 1/2 octet |
| Message type | Subclause 8.1.3 | M | V | 1 octet |
| CP‑Cause | Subclause 8.1.4.2 | M | V | 1 octet |

三种类型中的字段解析如下：

#### Protocol Descriminator

首字节的低4bit

|  |
| --- |
| bits 4 3 2 1 |
| 0 0 0 0 | group call control | |
| 0 0 0 1 | broadcast call control | |
| 0 0 1 0 | EPS session management messages | |
| 0 0 1 1 | call control; call related SS messages | |
| 0 1 0 0 | GPRS Transparent Transport Protocol (GTTP) | |
| 0 1 0 1 | mobility management messages | |
| 0 1 1 0 | radio resources management messages | |
| 0 1 1 1 | EPS mobility management messages | |
| 1 0 0 0 | GPRS mobility management messages | |
| 1 0 0 1 | SMS messages | |
| 1 0 1 0 | GPRS session management messages | |
| 1 0 1 1 | non call related SS messages | |
| 1 1 0 0 | Location services specified in 3GPP TS 44.071 [8a] |
| 1 1 1 0 | extension of the PD to one octet length | |
| 1 1 1 1 | used by tests procedures described in 3GPP TS 44.014 [5a], 3GPP TS 34.109 [17a], 3GPP TS 36.509 [26] and 3GPP TS 38.509 [29]. | |

#### Transaction identifier

首字节的第5到8bit，用于在一个会话中区分多达16个不同的双向消息流（相同PD中）。

#### Message type

Message type和protocol discriminator一起标识信息的功能。

|  |
| --- |
| 8 7 6 5 4 3 2 1 |
| 0 0 0 0 0 0 0 1 CP‑DATA |
| 0 0 0 0 0 1 0 0 CP‑ACK |
| 0 0 0 1 0 0 0 0 CP‑ERROR |

一字节，目前只定义了三种消息类型。

#### CP‑Cause element

如果是CP-ERROR类型的消息，则还有Cause域，该域的编码和描述如下。

|  |  |  |
| --- | --- | --- |
| Cause value | Cause nr. | Cause |
|  |  |  |
| 7 6 5 4 3 2 1 | # |  |
| 0 0 1 0 0 0 1 | 17 | Network failure |
| 0 0 1 0 1 1 0 | 22 | Congestion |
| 1 0 1 0 0 0 1 | 81 | Invalid Transaction Identifier value |
| 1 0 1 1 1 1 1 | 95 | Semantically incorrect message |
| 1 1 0 0 0 0 0 | 96 | Invalid mandatory information |
| 1 1 0 0 0 0 1 | 97 | Message type non‑existent or not implemented |
| 1 1 0 0 0 1 0 | 98 | Message not compatible with the short message protocol state |
| 1 1 0 0 0 1 1 | 99 | Information element non‑existent or not implemented |
| 1 1 0 1 1 1 1 | 111 | Protocol error, unspecified |
|  |  |  |
| All other cause values shall be treated as cause number 111. | | |

#### CP‑User data element

CP-User Data用于传送RPDU。RPDU的最大长度为248字节。

|  |  |  |
| --- | --- | --- |
| 8 7 6 5 4 3 2 1 | |  |
| 0 | 0 0 0 0 0 0 1  CP‑User Data IEI | 1 octet |
| Length indicator | | 1 octet |
| RPDU  Maximum length 248 octets | | ? octet |

### RP-DATA

RP-DATA区分上行和下行。

#### RP‑DATA (Network to Mobile Station)

This message is sent in MSC ‑> MS direction. The message is used to relay the TPDUs. The information elements are in line with 3GPP TS 23.040. See table 7.4/3GPP TS 24.011.

**Table 7.4/3GPP TS 24.011: RP‑DATA message content**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information element | Reference | Presence | Format | Length |
| RP‑Message Type | Subclause 8.2.2 | M | V | 3 bits |
| RP‑Message Reference | Subclause 8.2.3 | M | V | 1 octet |
| RP‑Originator Address | Subclause 8.2.5.1 | M | LV | 1‑12 octets |
| RP‑Destination Address | Subclause 8.2.5.2 | M | LV | 1 octet |
| RP‑User Data | Subclause 8.2.5.3 | M | LV | ≤ 233 octets |

#### RP‑DATA (Mobile Station to Network)

This message is sent in MS ‑> MSC direction. The message is used to relay the TPDUs. The information elements are in line with 3GPP TS 23.040. See table 7.5/3GPP TS 24.011.

**Table 7.5/3GPP TS 24.011: RP‑DATA message content**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information element | Reference | Presence | Format | Length |
| RP‑Message Type | Subclause 8.2.2 | M | V | 3 bits |
| RP‑Message Reference | Subclause 8.2.3 | M | V | 1 octet |
| RP‑Originator Address | Subclause 8.2.5.1 | M | LV | 1 octet |
| RP‑Destination Address | Subclause 8.2.5.2 | M | LV | 1‑12 octets |
| RP‑User Data | Subclause 8.2.5.3 | M | LV | ≤ 233 octets |

各个信元的介绍如下。

#### RP-Message Type

用于指示RP-DATA，RP-ACK，RP-ERROR发送的方向。

|  |  |  |
| --- | --- | --- |
| Bit value | Direction | RP‑Message |
| 3 2 1 |  |  |
| 0 0 0 | ms ‑> n | RP‑DATA |
| 0 0 0 | n ‑> ms | Reserved |
| 0 0 1 | ms ‑> n | Reserved |
| 0 0 1 | n ‑> ms | RP‑DATA |
| 0 1 0 | ms ‑> n | RP‑ACK |
| 0 1 0 | n ‑> ms | Reserved |
| 0 1 1 | ms ‑> n | Reserved |
| 0 1 1 | n ‑> ms | RP‑ACK |
| 1 0 0 | ms ‑> n | RP‑ERROR |
| 1 0 0 | n ‑> ms | Reserved |
| 1 0 1 | ms ‑> n | Reserved |
| 1 0 1 | n ‑> ms | RP‑ERROR |
| 1 1 0 | ms ‑> n | RP‑SMMA |
| 1 1 0 | n ‑> ms | Reserved |
| 1 1 1 | ms ‑> n | Reserved |
| 1 1 1 | n ‑> ms | Reserved |

#### Message reference

此信元长度1字节，范围0到255，用于联系RP-ACK或者RP-ERROR到对应的RP-DATA或者RP\_SMMA消息。

#### Originator address element

在MT时，此地址为发起服务中心的地址。如果号码额数字为奇数，则最后一个字节的bit5-8为1111，号码按照BCD码编码。

|  |  |  |  |
| --- | --- | --- | --- |
| 8 7 6 5 4 3 2 1 | | | |
|  | RP‑Originator Address IEI | | octet 1 |
| Length of RP‑Originator Address contents | | | octet 2 |
| 1 ext | type of number | Numbering plan identification | octet 3 |
| Number digit 2 | | Number digit 1 | octet 4 |
| Number digit 4 | | Number digit 3 | octet 5 |
|  | |  | : |
|  | |  | : |
|  | |  |

#### RP‑User data element

RP-User data域中包含TPDU，也是必带的。RP-User data也可能出现的RP-Error消息中。该域的长度可变，最大为233个字节，在RP-Error和RP-ACK中，长度可达234个字节。

RP-User data信元的编码如下

|  |  |  |
| --- | --- | --- |
| 8 7 6 5 4 3 2 1 | | |
| 0 | 1 0 0 0 0 0 1  RP‑User Data IEI | 1 octet |
| Length indicator | | 1 octet |
| TPDU  Maximum length 232 octets | |  |

Figure 8.7/3GPP TS 24.011: RP‑User data element layout

### TPDU

TPDU通过TP-MTI分类为七种类型，各种类型的短信格式不相同。

#### TP‑Message‑Type‑Indicator (TP‑MTI)

The TP-Message-Type-Indicator is **a 2-bit field, located within bits no 0 and 1** of the first octet of all PDUs which can be given the following values:

bit1 bit0 Message type

0 0 SMS‑DELIVER (in the direction SC to MS)   
 0 0 SMS‑DELIVER REPORT (in the direction MS to SC)   
 1 0 SMS‑STATUS‑REPORT (in the direction SC to MS)   
 1 0 SMS‑COMMAND (in the direction MS to SC)   
 0 1 SMS‑SUBMIT (in the direction MS to SC)   
 0 1 SMS‑SUBMIT‑REPORT (in the direction SC to MS)   
 1 1 Reserved

If an MS receives a TPDU with a "Reserved" value in the TP‑MTI it shall process the message as if it were an "SMS‑DELIVER" but store the message exactly as received.

#### SMS‑SUBMIT type

| Abbr. | Reference | P1) | P2) | Description |
| --- | --- | --- | --- | --- |
| TP‑MTI | TP‑Message‑Type‑Indicator | M | 2b | Parameter describing the message type. |
| TP‑RD | TP‑Reject‑Duplicates | M | b | Parameter indicating whether or not the SC shall accept an SMS‑SUBMIT for an SM still held in the SC which has the same TP‑MR and the same TP‑DA as a previously submitted SM from the same OA |
| TP‑VPF | TP‑Validity‑Period‑Format | M | 2b | Parameter indicating whether or not the TP‑VP field is present. |
| TP‑RP | TP‑Reply‑Path | M | b | Parameter indicating the request for Reply Path. |
| TP‑UDHI | TP‑User‑Data‑Header‑Indicator | O | b | Parameter indicating that the TP‑UD field contains a Header. |
| TP‑SRR | TP‑Status‑Report‑Request | O | b | Parameter indicating if the MS is requesting a status report. |
| TP‑MR | TP‑Message‑Reference | M | I | Parameter identifying the SMS‑SUBMIT. |
| TP‑DA | TP‑Destination‑Address | M | 2‑12o | Address of the destination SME. |
| TP‑PID | TP‑Protocol‑Identifier | M | o | Parameter identifying the above layer protocol, if any. |
| TP‑DCS | TP‑Data‑Coding‑Scheme | M | o | Parameter identifying the coding scheme within the TP‑User‑Data. |
| TP‑VP | TP‑Validity‑Period | O | o/7o | Parameter identifying the time from where the message is no longer valid. |
| TP‑UDL | TP‑User‑Data‑Length | M | I | Parameter indicating the length of the TP‑User‑Data field to follow. |
| TP‑UD | TP‑User‑Data | O | 3) |  |

#### 9.2.2.1 SMS‑DELIVER type

Basic elements of the SMS‑DELIVER type:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Abbr. | Reference | P1) | R2) | Description |
| TP‑MTI | TP‑Message‑Type‑Indicator | M | 2b | Parameter describing the message type. |
| TP‑MMS | TP‑More‑Messages‑to‑Send | M | b | Parameter indicating whether or not there are more messages to send |
| TP-LP | TP-Loop-Prevention | O | b | Parameter indicating that SMS applications should inhibit forwarding or automatic message generation that could cause infinite looping. |
| TP‑RP | TP‑Reply‑Path | M | b | Parameter indicating that Reply Path exists. |
| TP‑UDHI | TP‑User‑Data‑Header‑Indicator | O | b | Parameter indicating that the TP‑UD field contains a Header |
| TP‑SRI | TP‑Status‑Report‑Indication | O | b | Parameter indicating if the SME has requested a status report. |
| TP‑OA | TP‑Originating‑Address | M | 2‑12o | Address of the originating SME. |
| TP‑PID | TP‑Protocol‑Identifier | M | o | Parameter identifying the above layer protocol, if any. |
| TP‑DCS | TP‑Data‑Coding‑Scheme | M | o | Parameter identifying the coding scheme within the TP‑User‑Data. |
| TP‑SCTS | TP‑Service‑Centre‑Time‑Stamp | M | 7o | Parameter identifying time when the SC received the message. |
| TP‑UDL | TP‑User‑Data‑Length | M | I | Parameter indicating the length of the TP‑User‑Data field to follow. |
| TP‑UD | TP‑User‑Data | O | 3) |  |