

目录

SMS（短信技术讲解）

- 1、SMS简介
- 2、SMS基本业务流程
- 3、SMS 代码类图
- 4、SMS 发送/接收流程
- 5、短信协议（3GPP协议 23.040）
- 6、编码方式（3GPP协议 23.038）
- 7、长短信（Concatenated Short Message）
- 8、参考协议文档
- 9、AT 命令
- 10、LOG分析

1、SMS 简介

短信: Short Message Service, 简称SMS, 是用户通过手机或其他电信终端直接发送或接收的文字或数字信息, 内容以文本、数字或二进制非文本数据为主, 目前, 这种短消息的长度被限定在 140 byte之内 用户每次能接收和发送短信的字符数, 是 160 个英文 (7BIT) 或数字字符, 或者 70 个中文 (16BIT) 字符。

短消息采用存储转发方式, 其承载通道为控制信令信道, 信息容量有限, 一条短消息 , 最多包含 140Byte。短消息分为小区广播短消息业务和点对点短消息业务。其中点对点的短 消息业务又可以分为下面两种基本业务。

SMS包含2个基本的业务:

1、SMS MO (Short Message Mobile Originated)

MS向SC发送短信的业务;

是由移动终端(MT)发起的短消息, 描述 GSM 系统 中 MT 通过短消息中心 (SMC, Short Message Center) 向一个短消息实体 (SME, Short Message Entity) 发送短消息的能力。SME 可以是 MT, 也可以是固网用户, 联网 PC 等。

2、SMS MT (Short Message Mobile Terminated)

SMSC(short message service center)向MS(mobile station)发送短信的业务;

到达移动终端的短消息, 描述 GSM 系统从 SMC 向 被呼移动终端转发短消息的能力。

基本流程见下图:

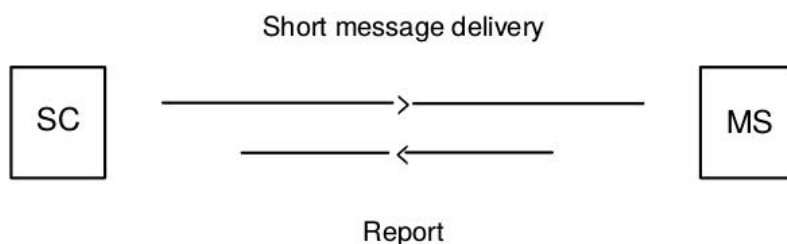


Figure 1: The Short Message Service mobile terminated

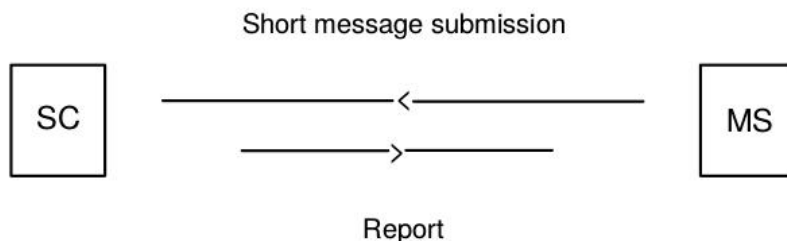
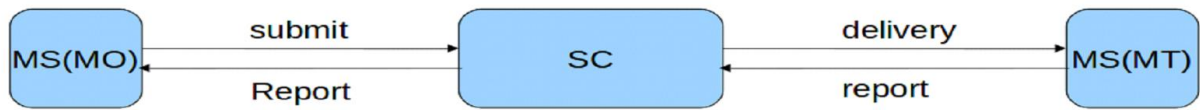


Figure 2: The Short Message Service mobile originated

2、SMS基本业务流程

基础架构



Submit: SMS-SUBMIT

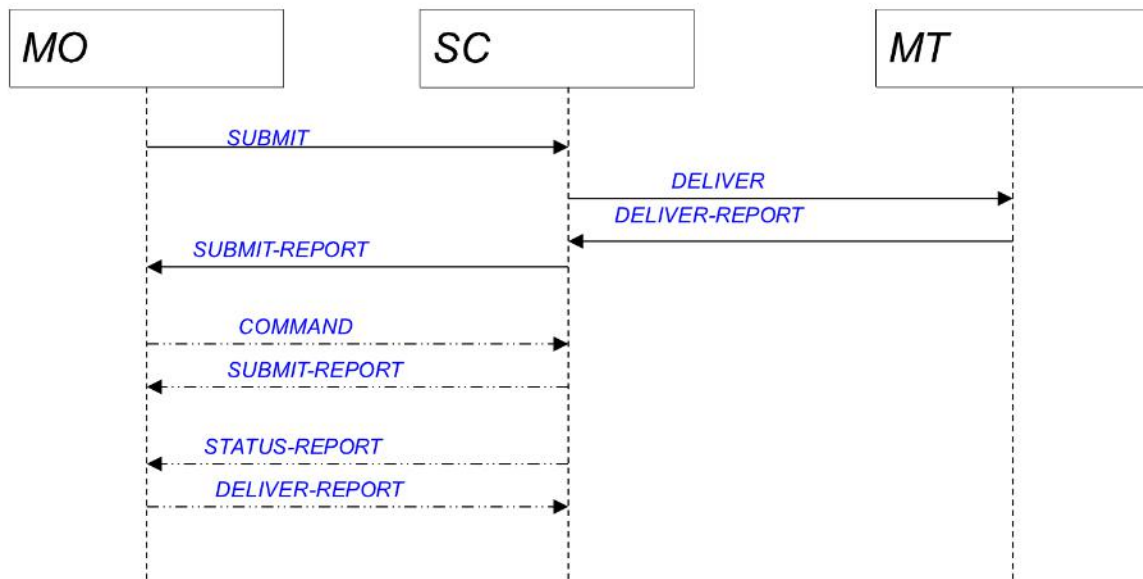
Delivery: SMS-DELIVER

Report: 成功或者失败以及失败的原因

SC: 一个或多个 Service Center，通过路由找到目的地

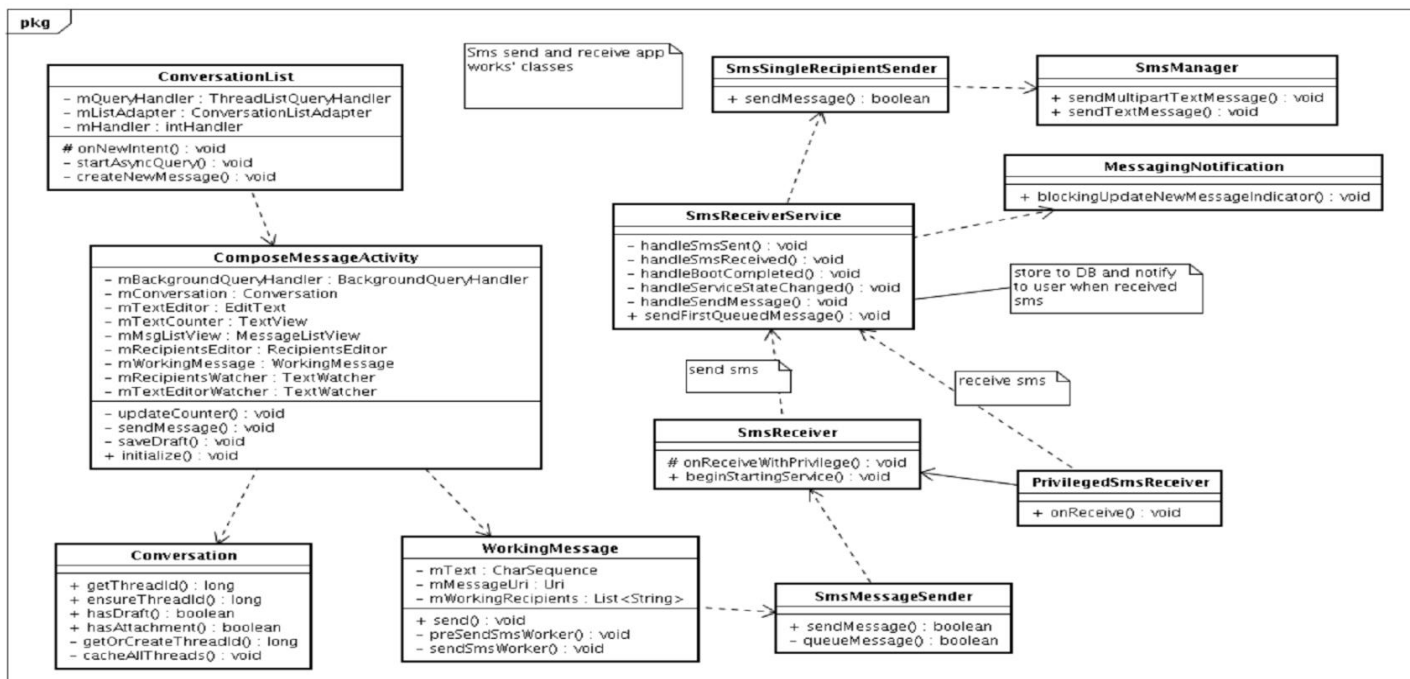
TPDU Type:

1. SMS-DELIVER,
2. SMS-DELIVER-REPORT for RP-ERROR
3. SMS-DELIVER-REPORT for RP-AK
4. SMS-SUBMIT
5. SMS-SUBMIT-REPORT for RP-ERROR
6. SMS-SUBMIT-REPORT for RP-AK
7. SMS-STATUS-REPORT
8. SMS-COMMAND

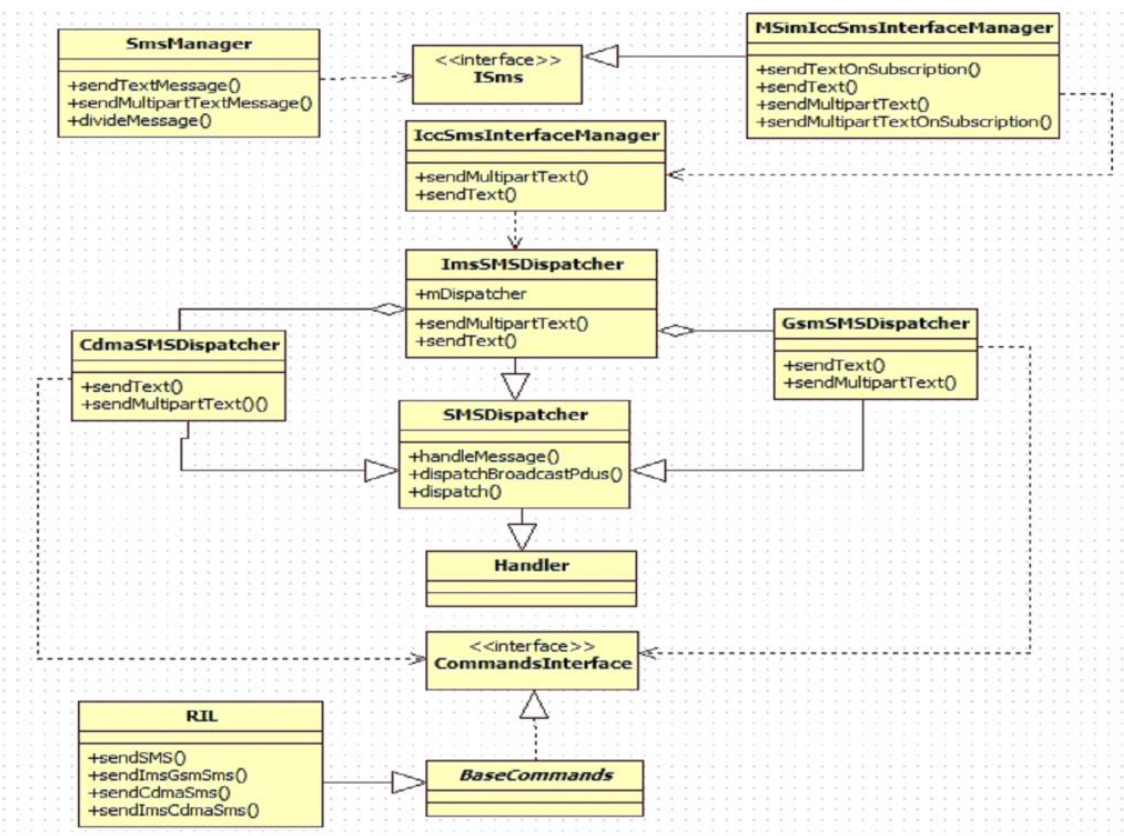


3、SMS 代码类图

3.1 、APP主要类图：



3.2 、Framework主要类图

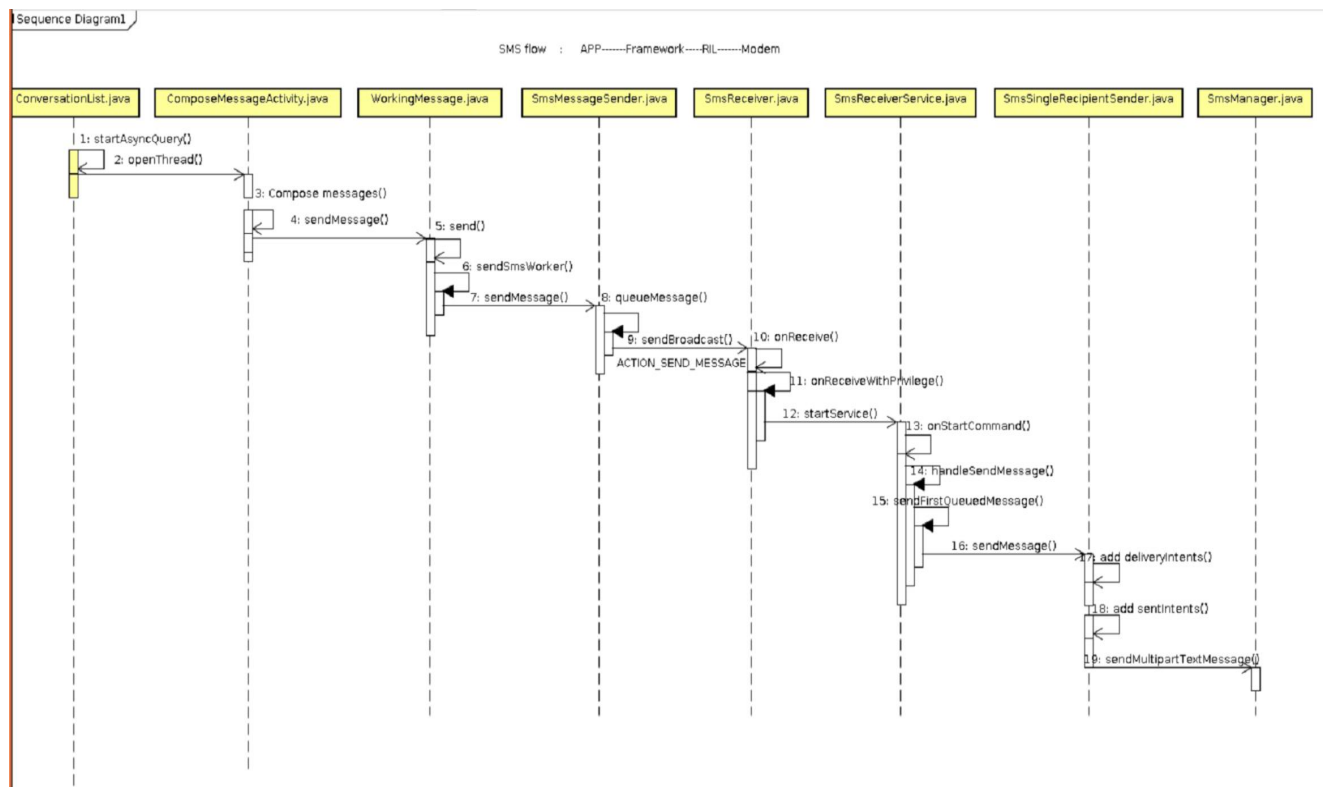


4、SMS 发送/接收流程

4.1 、SMS MO 流程

短信发送的流程比较冗长，发送请求从AP层经过多个步骤传递到Framework，在Framework完成**拆分，保存，创建pdu对象**等操作，最终调用RIL对象中发送sms的方法，通过AT传递到Modem，然后传送给网络；同时，短信发送的添加的发送状态和发送报告的回调，当短信发送成功或失败时上报给APP作响应处理。以Smsmanager为分割点，我们将sms发送流程分为2部分，APP 和 Framework and RIL，具体流程我们以流程图的方式展示，请结合代码跟踪分析。

APP:



SmsManager->RIL:

sendTextMessage 和 sendMultipartTextMessage 的过程其实差不多,无非是sendMultipartTextMessage 对长短信 进行了一下处 理,为每一个 part 设置了SmsHeader。

ImsSMSDispatcher 中包含了两种不同的 SmsDispatcher,IccSmsInterfaceManager 调用 SmsDispatcher 中各个方法时,会根据手机类型的不同,调用不 同 SmsDispatcher 的 相应方法。大致过程为:

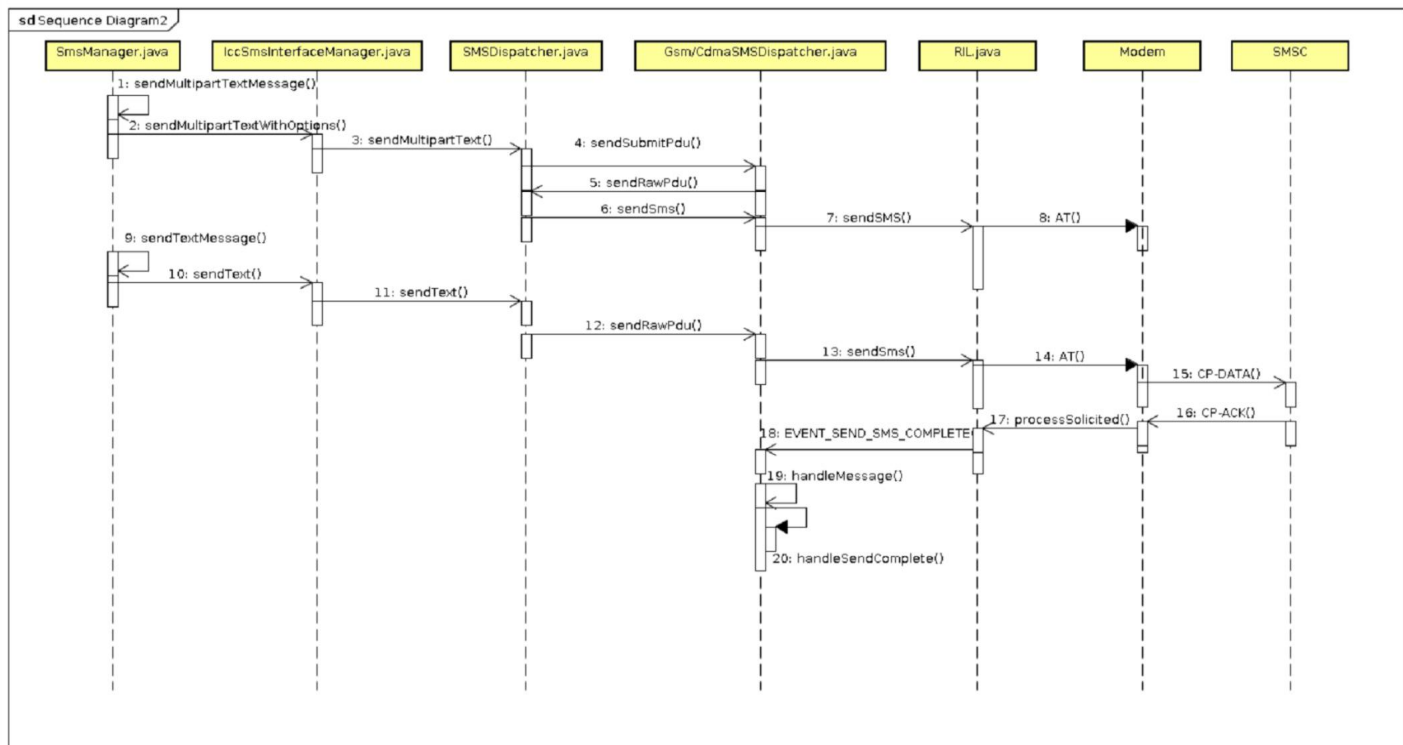
- 1、计算编码方式;
- 2、对每一个分段构造 SmsHeader、SubmitPdu、 SmsTracker,并设置 RadioTechnologyFamily;
- 3、利用 SmsTracker 构造当消息正常发送后调用的 Message 对 象;
- 4、调用与网络类型有关的 RIL 中的相应方法发送。

RIL 请求命令根据网络类型不同分为下面几类:

GSM: sendSMS - **RIL_REQUEST_SEND_SMS**、

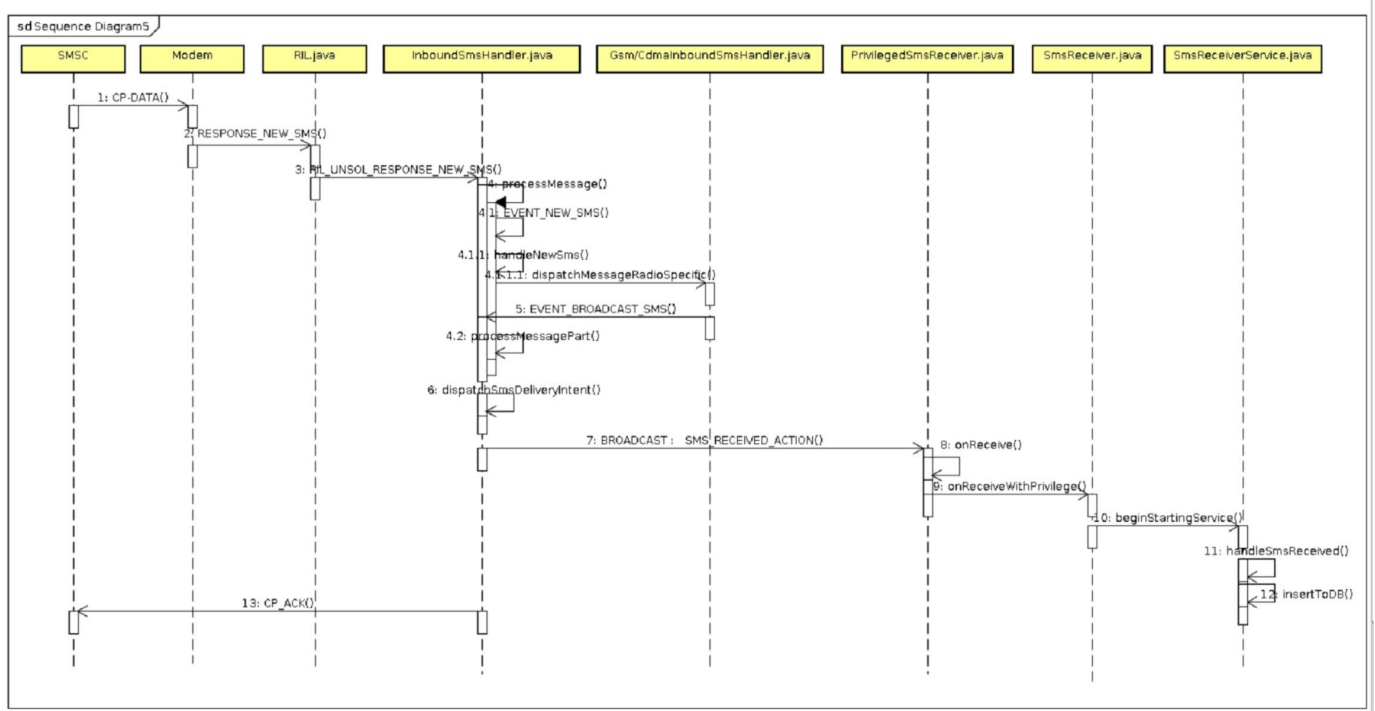
CDMA: sendCdmaSms **RIL_REQUEST_CDMA_SEND_SMS**、

IMS : sendImsGsmSms&sendImsCdmaSms- **RIL_REQUEST_IMS_SEND_SMS**



4.2 、SMS MT 流程

短信接收相对于发送短信流程比较简单，SMSC发送一条短信到手机，最早是在modem先收到信息，然后上报给RIL，RIL层将新短信转换成EVENT_NEW_SMS信息发送给Framework，在framework进行处理，解析PDU，保存等操作，然后上报给AP，AP拿到新短信，保存数据及更新UI；具体请查看下面的流程图，请结合代码跟踪分析。



5、短信协议（3GPP协议 23.040）

SMS PDU TYPE及其基本组成元素

短信PDU类型主要分为以下几种：

SMS-DELIVER ,

conveying a short message from the SC to the MS;

SMS-DELIVER-REPORT,

a) a failure cause (if necessary);

b) information as part of a positive or negative acknowledgement to an SMS-DELIVER or SMS-STATUS-REPORT;

SMS-SUBMIT,

conveying a short message from the MS to the SC;

SMS-SUBMIT-REPORT,

conveying;

a) a failure cause (if necessary);

b) information as part of a positive or negative acknowledgement to an SMS-SUBMIT or SMS-COMMAND;

SMS-STATUS-REPORT,

conveying a status report from the SC to the MS;

SMS-COMMAND, conveying a command from the MS to the SC.

5.1、SMS-SUBMIT 发送方PDU格式及其参数 (Mobile Originated)

SMS-MO 参数:

9.2.2.2 SMS-SUBMIT type

Basic elements of the 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)	

- 1) Provision; Mandatory (M) or Optional (O).
- 2) Representation; Integer (I), bit (b), 2 bits (2b), Octet (o), 7 octets (7o), 2-12 octets (2-12o).
- 3) Dependent on the TP-DCS

SMS MO PDU 结构:

SCA	PDUType	MR	DA	PID	DCS	VP	UDL	UD
1-12	1	1	2-12	1	1	0, 1, 7	1	0-140

单位: Octet

示例：

向发送一条 SMS，消息容为：“Test”

0031000D209F80000A704D4F29C0E

向发送一条 SMS，消息容为：“测试”

0031000B9F80008A7046D4B8BD5

SCA	PDUType	MR	DA	PID	DCS	VP	UDL	UD
1-12	1	1	2-12	1	1	0,1,7	1	0-140
00	31	00	0D209F8	00	00	A7	04	D4F29C0E
00	31	00	0B9F8	00	18	A7	04	6D4B8BD5

5.2、SMS-SUBMIT-REPORT PDU格式及其参数

(i) SMS-SUBMIT-REPORT for RP-ERROR

Basic elements of the SMS-SUBMIT-REPORT type:

Abbr.	Reference	p1)	p2)	Description
TP-MTI	TP-Message-Type-Indicator	M	2b	Parameter describing the message type
TP-UDHI	TP-User-Data-Header-Indication	O	b	Parameter indicating that the TP-UD field contains a Header
TP-FCS	TP-Failure-Cause	M	l	Parameter indicating the reason for SMS-SUBMIT failure
TP-PI	TP-Parameter-Indicator	M	o	Parameter indicating the presence of any of the optional parameters which follow
TP-SCTS	TP-Service-Centre-Time-Stamp	M	7o 5)	Parameter identifying the time when the SC received the SMS-SUBMIT See clause 9.2.3.11
TP-PID	TP-Protocol-Identifier	O	o	See clause 9.2.3.9
TP-DCS	TP-Data-Coding-Scheme	O	o	see clause 9.2.3.10
TP-UDL	TP-User-Data-Length	O	o	see clause 9.2.3.16
TP-UD	TP-User-Data	O	3) 4)	see clause 9.2.3.24

1) Provision: Mandatory (M) or Optional (O).

2) Representation: Integer (I), bit (b), 2bits (2b), octet (o).

Layout of SMS-SUBMIT-REPORT:

[illegible]

(ii) SMS-SUBMIT-REPORT for RP-ACK

[illegible]

5. 3、SMS-DELIVER PDU格式及其参数

MT 参数：

9.2.2.1 SMS-DELIVER type

Basic elements of the SMS-DELIVER type:

Abbr.	Reference	p1)	p2)	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	l	Parameter indicating the length of the TP-User-Data field to follow.
TP-UD	TP-User-Data	O	3)	

- 1) Provision; Mandatory (M) or Optional (O).
- 2) Representation; Integer (I), bit (b), 2 bits (2b), Octet (o), 7 octets (7o), 2-12 octets (2-12o).

MT PDU 结构:

SCA	PDUType	OA	PID	DCS	SCTS	UDL	UD
1-12	1	2-12	1	1	7	1	0-140

5. 4、SMS-DELIVER-REPORT PDU格式及其参数

SMS-DELIVER-REPORT 结构同 SMS-SUBMIT-REPORT, 这里不再重复，具体参考 3GPP协议 23. 040

5.5、PDU参数格式解析

1、SCA短消息服务中心地址格式

1 Octet	0~1 Octet	0~10 Octets
Len	Type	Addr
SCA 长度	SCA 类型	SCA 地址
08	91	683108200505F0

2、PDU Type

1 个字节

发送方：SMS-SUBMIT

Bit No.	7	6	5	4	3	2	1	0
	RP	UDHI	SRR	VPF		RD	MTI	

接收方：SMS-DELIVER

Bit No.	7	6	5	4	3	2	1	0
	RP	UDHI	SRI			MMS	MTI	

TP-RP:应答路径(Reply Path), 0-未设置;1-设置

TP-UDHI:用户数据头标识(User Data Header Indicator)

0- 用户数据(UD) 部分不包含头信息

1- 用户数据(UD) 开始部分包含用户头信息, 长短信时会设置为1, 头信息占 UD 的 6 个字节, 具体的字段解释请见下章节。

TP-SRR:请求状态报告(Status Report Request)

0- 不需要报告

1- 需要报告

TP-SRI:状态报告指示(Status Report Indication),
此值仅被短消息中心
(SMSC) 设置

0- 状态报告将不会返回给短消息实体(SME)

1- 状态报告将返回给短消息实体(SME)

TP-VPF:有效期格式(Validity Period Format)

00-VP 段没有提供(长度为 0)

01-保留

10-VP 段以整形形式提供(相对的)

11-VP 段以 8 位组的一半(semi-octet)形式提供(绝对的)

TP-RD:拒绝复本(Reject Duplicate)

0- 通知短消息服务中心(SMSC)接受一个 SMS-SUBMIT,即使该消息是先前已提交过的,并还存在于 SMSC 中未发送出去。MS 重复的条件是:消息参考(MR)、接收方地址(DA)及发送方地址(OA)相同

1- 通知 SMSC 拒绝一个重复的 SMS

TP-MMS:有更多的信息需要发送时,此值被 SMSC 设置

0- 在 SMSC 中有更多的信息等待 MS

1- 在 SMSC 中没有更多的信息等待 MS

TP-MTI:信息类型指示(Message Type Indicator)

00-SMS-DELIVER (SMSC - MS)

00-SMS- DELIVER REPORT (MS - SMSC)

01-SMS- SUBMIT (MS - SMSC)

01-SMS- SUBMIT REPORT (SMSC - MS)

10- SMS- STATUS REPORT (SMSC - MS)

10- SMS-COMMAND (MS - SMSC)

11-保留

3、TP-MR 信息参考(Message Reference)

表示MS给SC提交的TPDU的Reference Number，用于SC区分MS提交的TPDU；
每提交一个SMS-SUBMIT或SMS-COMMAND，MS给TP-MR递增 1；

4、TP-DA/OA

接收方地址与发送方地址

OA 与 DA 格式是一样的, 2-12 个字节, 如下所示

1 Octet	0 - 1 Octet	0 - 10 Octets
Len	Type	Addr
长度	类型	地址

比如：0D 91 683158714209F8

Len:地址长度。指 8613851724908 的长度。这与 SCA 中的定义不一样。

5、TP-PID 协议标识(Protocol Identifier)

表示使用的更高层协议的类型

对于标准情况下的 MS-to-SC 短消息传送, 只需设置 PID 为 00

6、TP-DCS 数据编码方案(Data Coding Scheme)

短信编码方式参考相关协议(23038),

Coding Group Bits 7..4	Use of bits 3..0																														
00xx	<p>General Data Coding indication Bits 5..0 indicate the following:</p> <p>Bit 5, if set to 0, indicates the text is uncompressed Bit 5, if set to 1, indicates the text is compressed using the compression algorithm defined in 3GPP TS 23.042 [13]</p> <p>Bit 4, if set to 0, indicates that bits 1 to 0 are reserved and have no message class meaning Bit 4, if set to 1, indicates that bits 1 to 0 have a message class meaning::</p> <table><tr><th>Bit 1</th><th>Bit 0</th><th>Message Class</th></tr><tr><td>0</td><td>0</td><td>Class 0</td></tr><tr><td>0</td><td>1</td><td>Class 1 Default meaning: ME-specific.</td></tr><tr><td>1</td><td>0</td><td>Class 2 (U)SIM specific message</td></tr><tr><td>1</td><td>1</td><td>Class 3 Default meaning: TE specific (see 3GPP TS 27.005 [8])</td></tr></table> <p>Bits 3 and 2 indicate the character set being used, as follows :</p> <table><tr><th>Bit 3</th><th>Bit 2</th><th>Character set:</th></tr><tr><td>0</td><td>0</td><td>GSM 7 bit default alphabet</td></tr><tr><td>0</td><td>1</td><td>8 bit data</td></tr><tr><td>1</td><td>0</td><td>UCS2 (16bit) [10]</td></tr><tr><td>1</td><td>1</td><td>Reserved</td></tr></table> <p>NOTE: The special case of bits 7..0 being 0000 0000 indicates the GSM 7 bit default alphabet with no message class</p>	Bit 1	Bit 0	Message Class	0	0	Class 0	0	1	Class 1 Default meaning: ME-specific.	1	0	Class 2 (U)SIM specific message	1	1	Class 3 Default meaning: TE specific (see 3GPP TS 27.005 [8])	Bit 3	Bit 2	Character set:	0	0	GSM 7 bit default alphabet	0	1	8 bit data	1	0	UCS2 (16bit) [10]	1	1	Reserved
Bit 1	Bit 0	Message Class																													
0	0	Class 0																													
0	1	Class 1 Default meaning: ME-specific.																													
1	0	Class 2 (U)SIM specific message																													
1	1	Class 3 Default meaning: TE specific (see 3GPP TS 27.005 [8])																													
Bit 3	Bit 2	Character set:																													
0	0	GSM 7 bit default alphabet																													
0	1	8 bit data																													
1	0	UCS2 (16bit) [10]																													
1	1	Reserved																													

Bits 7-6 00XX General Data Coding Indication

Bit 5 表示文本内容是否被压缩;

0 没有压缩;

1 采用规定的压缩算法压缩;

Bit 4 表示Bit1, 0 是否有短信的Class类别;

0 Bit1, 0 保留;

1 Bit1, 0 为短信Class类别;

Bits 3, 2 表示字符编码

00 GSM 7Bit default alphabet

01 8 Bit data

10 UCS2 (16Bit)

11 Reserved

Bits 1, 0 表示短信Class类型

00 Class 0

01 Class 1 Default meaning: ME-specific

10 Class 2 (U)SIM specific message

11 Class 3 Default meaning: TE specific

Class0 短信: 直接跳出, 默认不保存

Class1, class3 短信: 存在手机上

Class2 短信, 手机和SIM卡同时存储

7、TP-VP 信息有效期(Validity Period)

根据TP-VPF 的设置其相应的格式（占用字节：0, 1, 7o）

8、TP-SCTS 服务中心时间戳(Service Center Time Stamp)

占用 7 个字节

9、TP-UDL 用户数据长度(User Data Length)

10、TP-UD 用户数据

短信内容

TP-UD 结构：

UD 包括 UDH 用户数据头+SM 短信内容，即：UD = UDH + SM.

根据PDU TYPE中的TP-UDHI 参数我们可以判断UD 是否包含 UDH，

如果TP-UDHI 为 0 ：表示不包含UDH，只有内容

如果TP-UDHI 为 1 ：表示包含UDH

比如长短信一定包含UDH

UDH长度固定为 6 或 7 byte，长度为 6 的常用，

根据编码方式不同UD的结构可以分为 2 中：

7BIT编码：

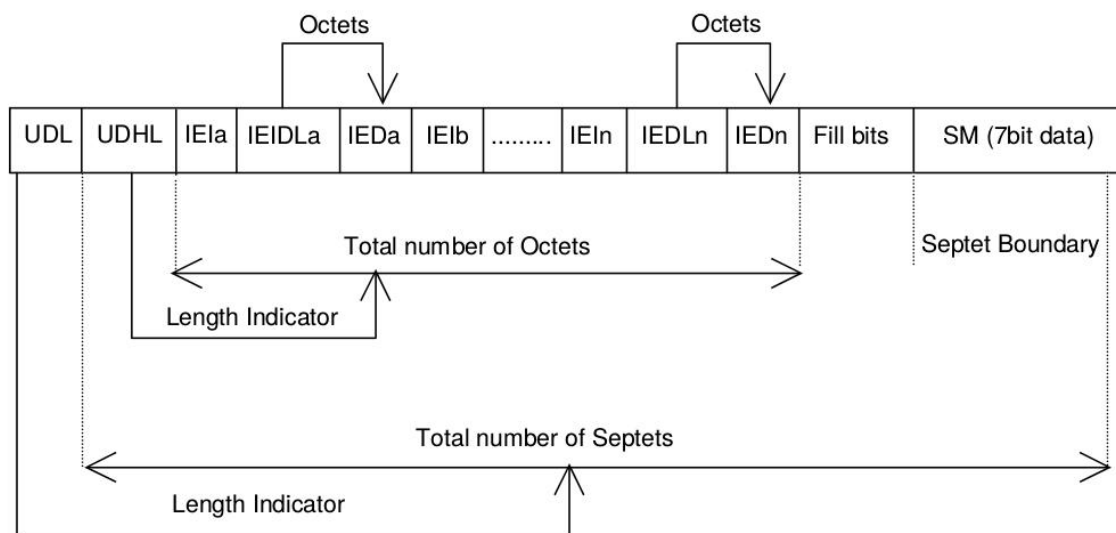


Figure 9.2.3.24 (a)

8BIT/16BIT:

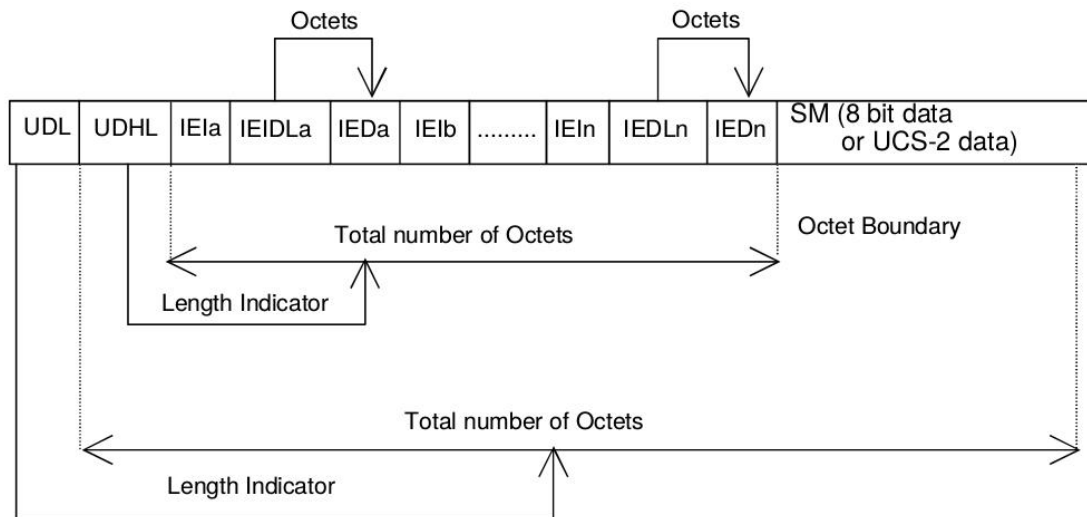


Figure 9.2.3.24 (b)

区别在于 7BIT编码可能存在填充字节 Fill Bits

什么是填充字节？ 如何计算是否有Fill Bits？

可以这样算，一条短信最长是 140 个byte，
 如果 UDH 占用 6 个 byte，那SM 部分还剩 134 个byte，也就是 $134 \times 8 = 1072$ 个bit位，
 如果用 7bit编码，那就是 $1072 / 7 = 153$ 余上个 1bit ，也就是 153 GSM characters and 1 bit.
 那多出来的这个 1 bit 就是 fill bit，填充到SM的第一个 byte 的最后一个bit位，

同理，我们解析的时候，就要把这多出来的一个bit[0] 给去掉，后面的就按照 7bit 编码正常编解码

SMS PDU 解析示例 参考：

<https://blog.csdn.net/hlx156/article/details/53996445>

6、编码方式（3GPP协议 23.038）

6.1、7BIT编码

一页短信可以容量是 140 个byte（8bit）

7bit编码是一个字符用 7 个bit位来编， $140 \times 8 \text{bit} / 7 \text{bit} = 160$

所以一页短信如果是 7bit的编码方式，可以存放 160 个字符

可以根据其默认字符表进行编码，每个字符用 7 个bit来编码：

6.2.1 GSM 7 bit Default Alphabet

Bits per character: 7

CBS/USSD pad character: CR

Character table:

					b7								
					b6								
					b5								
b4	b3	b2	b1			0	1	2	3	4	5	6	7
0	0	0	0	0	@	Δ	SP	0	i	P	¿	p	
0	0	0	1	1	f	_	!	1	A	Q	a	q	
0	0	1	0	2	\$	Φ	"	2	B	R	b	r	
0	0	1	1	3	¥	Γ	#	3	C	S	c	s	
0	1	0	0	4	è	Λ	¤	4	D	T	d	t	
0	1	0	1	5	é	Ω	%	5	E	U	e	u	
0	1	1	0	6	ù	Π	&	6	F	V	f	v	
0	1	1	1	7	ì	Ψ	'	7	G	W	g	w	
1	0	0	0	8	ò	Σ	(8	H	X	h	x	
1	0	0	1	9	ç	Θ)	9	I	Y	i	y	
1	0	1	0	10	LF	Ξ	*	:	J	Z	j	z	
1	0	1	1	11	Ø	1)	+	;	K	Ã	k	ã	
1	1	0	0	12	ø	Æ	,	<	L	Ö	l	ö	
1	1	0	1	13	CR	æ	-	=	M	Ñ	m	ñ	
1	1	1	0	14	Å	ß	.	>	N	Ü	n	ü	
1	1	1	1	15	å	É	/	?	O	Š	o	à	

扩展 7bit字符表, 编码特殊字符 , 每个字符用 2 个 7bit来编码:

一页短信可以存放 160 个 7bit字符, 如果遇到扩展 7bit字符表里的内容, 计数+2, 即一页可以存放 80 个扩展 7bit的字符。

在编码的过程中, 如果发现字符不在default table里, 而是在extension table里, 那就先加入一个 0x1B, 之后继续添加字符在extension table里的位置就可以了。同理, 在解码的时候, 如果发现 0x1B, 那就说明后面的字符在extension table里面。

					b7	0	0	0	0	1	1	1	1
					b6	0	0	1	1	0	0	1	1
					b5	0	1	0	1	0	1	0	1
b4	b3	b2	b1		0	1	2	3	4	5	6	7	
0	0	0	0	0									
0	0	0	1	1									
0	0	1	0	2									
0	0	1	1	3									
0	1	0	0	4		^							
0	1	0	1	5									
0	1	1	0	6									
0	1	1	1	7									
1	0	0	0	8			{						
1	0	0	1	9			}						
1	0	1	0	10	3)								
1	0	1	1	11		1)							
1	1	0	0	12				[
1	1	0	1	13				~					
1	1	1	0	14]					
1	1	1	1	15			\						

长短信 7BIT编码,

刚才提到的, 长短信包含UDH,

140-6 = 134byte
(134*8) / 7 = 153 + 1bit

所以说长短信的 7Bit编码一条消息里面最多可以发送 153 个字符.

6.2、8BIT/16BIT (UCS2)编码

一页短信可以容量是 140 个byte (8bit)

UCS2 编码是一个字符用 16 个bit位来编, $140 * 8 \text{bit} / 16 \text{bit} = 70$

所以一页短信如果是UCS2 的编码方式, 可以存放 70 个字符

如果是长短信, 最多可以存放 67 个unicode 字符:

$140 - 6 = 134 \text{byte}$

$(134 * 8) / 16 = 67$

参考文章:

https://blog.csdn.net/diangangqin/article/details/102525963?utm_medium=distribute.pc_relevant.none-task-blog-searchFromBaidu-2.not_use_machine_learn_pai&depth_1-utm_source=distribute.pc_relevant.none-task-blog-searchFromBaidu-2.not_use_machine_learn_pai

7、长短信（Concatenated Short Message）

普通短信UD区长度为 140 字节，超过 140 字节就得拆分成多条短信，拆分后的短信经过短信网关、短信中心的存储转发后到达终端的顺序可能和原发送顺序不同，这就使得接收方对于信息内容的理解出现困扰，1996 年颁布GSM03.40V4.13.0 中定义了长短信（Concatenated Short Message），所谓的长短信就是由一组相互独立的不超过普通短信长度的子短信组成，在网络传输中被视为多条普通短信，而在终端上被合并显示。

长短信的PDU结构和普通短信的PDU 结构的区别之处在于长短信的UD(UserData)中含有UDH 数据头

PDU-Type	普通短信	长短信
UDHI标识位	0	1
MMS标识位	1	最后一条为1其余为0

4.3UDL用户数据长度

	普通短信	长短信
UDL	短信内容长度	UDH用户数据头长度 + SM拆分后短信内容长度

4.4UD用户数据

	普通短信	长短信
UD	全部为短信内容	UDH用户数据头 + SM拆分后短信内容

UDH = UDHL + IE

UDHL	IEI	IEDL	IED		
			Reference No.	Maximum No.	Current No.
05	00	03	C6	02	01

1) UDHL用户数据头长度 (User Data Header Length)

一个字节，表示用户数据头的字节数，不包含本字节，UDHL+1=整个用户数据头长度

2) IE用户数据头信息单元 (Information Element)

a) IEI信息单元标识 (Information Element Identifier)

00: Concatenated short messages

01: Special SMS Message Indication

02: Reserved

03: Value not used to avoid misinterpretation as <LF> character

04: Application port addressing scheme, 8bit address

05: Application port addressing scheme, 16 bit address

06: SMSC Control Parameters

07: UDH Source Indicator

08: Concatenated short message [16-bit reference number]

09: Wireless Control Message Protocol

0A-6F: Reserved for future use

70-7F: SIM Toolkit Security Headers

80- 9F: SME to SME specific use

A0 - BF: Reserved for future use

C0 - DF: SC specific use

E0 - FF: Reserved for future use

00 和 08 都表示长短信，区别在于 00 是用一个字节表示“参考编号”，而 08 用两个字节表示“参考编号”（见 IED 组成说明）。

IEI Code:

The Information Element Identifier octet shall be coded as follows:

VALUE (hex)	MEANING	Classification	Repeatability
00	Concatenated short messages, 8-bit reference number	SMS Control	No
01	Special SMS Message Indication	SMS Control	Yes
02	Reserved	N/A	N/A
03	Value not used to avoid misinterpretation as <LF> character	N/A	N/A
04	Application port addressing scheme, 8 bit address	SMS Control	No
05	Application port addressing scheme, 16 bit address	SMS Control	No
06	SMSC Control Parameters	SMS Control	No
07	UDH Source Indicator	SMS Control	Yes
08	Concatenated short message, 16-bit reference number	SMS Control	No
09	Wireless Control Message Protocol	SMS Control	Note 3
0A	Text Formatting	EMS Control	Yes
0B	Predefined Sound	EMS Content	Yes
0C	User Defined Sound (iMelody max 128 bytes)	EMS Content	Yes
0D	Predefined Animation	EMS Content	Yes
0E	Large Animation (16*16 times 4 = 32*4 =128 bytes)	EMS Content	Yes
0F	Small Animation (8*8 times 4 = 8*4 =32 bytes)	EMS Content	Yes
10	Large Picture (32*32 = 128 bytes)	EMS Content	Yes
11	Small Picture (16*16 = 32 bytes)	EMS Content	Yes
12	Variable Picture	EMS Content	Yes
13	User prompt indicator	EMS Control	Yes
14	Extended Object	EMS Content	Yes
15	Reused Extended Object	EMS Control	Yes
16	Compression Control	EMS Control	No
17	Object Distribution Indicator	EMS Control	Yes
18	Standard WVG object	EMS Content	Yes
19	Character Size WVG object	EMS Content	Yes
1A	Extended Object Data Request Command	EMS Control	No
1B-1F	Reserved for future EMS features (see subclause 3.10)	N/A	N/A
20	RFC 5322 E-Mail Header	SMS Control	No
21	Hyperlink format element	SMS Control	Yes
22	Reply Address Element	SMS Control	No
23	Enhanced Voice Mail Information	SMS Control	No
24	National Language Single Shift	SMS Control	No
25	National Language Locking Shift	SMS Control	No
26 – 6F	Reserved for future use	N/A	N/A
70 – 7F	(U)SIM Toolkit Security Headers	SMS Control	Note 1
80 – 9F	SME to SME specific use	SMS Control	Note 2
A0 – BF	Reserved for future use	N/A	N/A
C0 – DF	SC specific use	SMS Control	Note 2
E0 – FF	Reserved for future use	N/A	N/A

b) IEDL信息单元数据长度 (Length of Information Element)

一个字节，表示信息单元长度，也就是IED的字节数，不包含本字节IED信息单元数据 (Information Element Data)

c) 长短信的IED由 3 字节组成

即IEI为 00 或 08 时的IED如下

第一字节：参考编号 (Reference Number)，参考编号相同的为同一长短信

第二字节：总条数 (Maximum number)，长短信拆分后的总条数

第三字节：当前短信序号 (Current number)，当前短信是长短信中的第几条

通过这三个参数就可以对长短信进行处理，存储，查询 和 拼接。

长短信介绍参考文献: <https://www.cnblogs.com/deanding/p/7729385.html>

8、参考协议文档

1) 3GPP TS 23.038

Alphabets and language-specific information

2) 3gpp TS 23.040 (GSM 03.40)

Technical realization of the Short Message Service (SMS)

3) 3gpp TS 24.011

Point-to-Point (PP) Short Message Service (SMS)

学习文献: <https://online.mediatek.com/QuickStart/QS00122>

9、AT 命令

短信操作步骤及相关命令：

- (1) 设置短信格式——AT+CMGF
- (2) 设置短信存储载体——AT+CPMS
- (3) 设置短信接收提示方式——AT+CNMI
- (4) 发送短信——AT+CMGS
- (5) 显示短信——AT+CMGL

具体介绍请参考学习：<https://www.cnblogs.com/top5/archive/2012/04/17/2453932.html>

10、LOG分析

参考5G_SMS_MMS_LOG流程分析.doc