SMS PDU

	AUTHOR	APPROVALS		QUALITY
		LEVEL 1	LEVEL 2	
NAME	Tang wei	Liu Alan	Yu miao	
FUNCTION	Engineer	Team Leader	Section manager	
DATE	12/11/14			
SIGNATURE	Tang wei			

DOCUMENT HISTORY

Version	Date	Author	Type of Modification
0.1	12/11/14	Tang wei	Create the draft.

Table of Contents

1 SMS PDU 基本组成元素

缩写词

MS: Mobile Station 移动站台，负责系统交换管理，控制来自或发往其他电话或数据系统的通信

SME: Short Message Entity 短消息实体，负责接收和发送短消息。可以位于固话系统、移动基站或其他服务中心内

下列元素是用于 SMS-SUBMIT 和 SMS-DELIVER 中的部分

元素	名称	长度	描述
SCA	Service Center Adress	1~12	服务中心的电话号码
PDU-Type	Protocol Data Unit Type	1	协议数据单元类型
MR	Message Refercence	1	所有成功的 SMS-SUBMIT 参考数目（0…255）
OA	Originator Adress	2~12	发送方 SME 的地址
DA	Destination Adress	2~12	接收方 SME 的地址
PID	Protocol Identifier	1	参数显示 SMSC 以何种方式处理 SM（比如 FAX、Voicemail 等）
DCS	Data Coding Scheme	1	参数表示用户数据（UD）采用什么编码方案
SCTS	Service Center Time Stamp	7	参数表示 SMSC 接收到消息时的时间戳
VP	Validity Period	0,1,7	参数表示消息在 SMSC 中不再有效的时长
UDL	User Data Length	1	用户数据段长度
UD	User Data	0~140	SM 数据

1.1 发送方 PDU 格式 SMS-SUBMIT-PDU(Mobile Originated)

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

1.2 接收方 PDU 格式 SMS-DELIVED-PDU(Mobile Terminated)

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

1.3 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

Len：短消息中心地址长度。指（91）+（68 31 08 20 05 05 F0）的 8 个字节。如果 Len 被设置为 00&h，并不提供后面的部分，那么终端设备将读取 SIM 中设置的 SCA 填充到 SMS-PUD 中。

Type：短消息中心地址的类型，是国际的号码还是国内的号码（81&h 表示国内的，91 表示国际的）。91&h 是 TON、NPI 遵守 International/E.164 标准，指在号码前需要加‘+’号；此外还有其他数值，单 91&h 最常用。

Bit No.	7	6	5	4	3	2	1	0
	1	数据类型			号码鉴别			

第 7 位永远置为 1

数据类型（Type of Number）：

000：未知

001：国际（以+开始的地址）

010：国内

111：留作扩展

号码鉴别（Numbering plan identification）：

0000：未知

0001：ISDN/电话号码（E.164/E.163）

1111：留作扩展

示例：

服务中心号码	PDU 格式编码

+8613800250500	08 91 86 31 08 20 05 05 F0
13800512500	07 81 31 08 50 21 05 F0
123456	04 81 21 43 65

1.4 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	

RP：应答路径（Reply Path），0-未设置；1-设置

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

SRR：请求状态报告（Status Report Request）

0- 不需要报告

1- 需要报告

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）

VPF：有效期格式（Validity Period Format）

0- VP 段没有提供（长度为 0）

1- 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）

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

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

MTI：信息类型指示（Message Type Indicator）

0- SMS-DELIVER (SMSC - MS)

0- 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

1.5 MR 信息参考（Message Reference）

设为 00 即可

1.6 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

0D	91	683158714209F8

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

1.7 PID 协议标识（Protocol Identifier）

对于标准情况下的 MS-to-SC 短消息传送，只需设置 PID 为 00

1.8 DCS 数据编码方案（Data Coding Scheme）

见下面协议

1.9 VP 信息有效期（Validity Period）

第一种情况（相对的）：VPF 设置为 10， VP=AA(四天)

VP 为一个字节，给定有效期的长度

从 SMS-SUBMIT 被 SMSC 接收开始计算

有效期表示格式如下所示：

VP	相应的有效期
00 - 8F	（VF+1）*5 分钟，从 5 分钟间隔到 12 小时
90 - A7	12 小时+（VF -143）*30 分钟
A8 - C4	（VP-166）*1 天
C5 - FF	（VP-192）*1 周

第二种情况（绝对的）：VPF 设置为 11

年	月	日	时	分	秒	时区
30	80	02	90	54	33	20

表示 03-08-20 09:45:33

VP 段以整形或半个 8 位组（semi-octet）形式提供

VP 为 7 个字节，给定有效期终止的绝对时间

这种情况下的时间形式与 SCTS（Service Center TimeStamp）形式一致

1.10 SCTS 服务中心时间戳（Service Center Time Stamp）

占用 7 个字节，格式如 VP 的第二种情况所示

1.11 UDL 用户数据长度（User Data Length）

UDL 表示后面用户数据段的数据长度。

数据根式有 3 种：7bit，8bit，16bit。

用户数据（UD）的编码方式请见下面章节。

2 实例

Hero2 手机在跨运营商收发短信时，当短信中包含某些特殊的 7 bit default 字符(拉丁文)时，会出现乱码。

2.1 SMS send pdu

2.1.1 Log 信息

radio_log ：

11-18 16:18:41.196 767 776 D use-Rlog/RLOG-AT: AT> AT+EMGS=16,"0011000b818126117302f10000ff028402"

2.1.2 发送数据流分析

00 11 00 0b 81 8126117302f1 00 00 ff 02 8402

SCA	PDUType	MR	DA	PID	DCS	VP	UDL	UD
1~12	1	1	2~12	1	1	0,1,7	1	0~140
00	11	00	0b818126117302f1	00	00	ff	02	8402

11：有效期格式为 relative formate, pdu 类型为 SMS SUBMIT(即指明了该条数据是发送出去的短信)

Bit No.	7	6	5	4	3	2	1	0
	RP	UDHI	SRR	VPF		RD	MTI	
	0	0	0	10		0	01	

VPF=10，VP 段以整形形式提供（相对的）
MTI=01，SMS- SUBMIT (MS - SMSC)

0b：目的号码长度是 11 位
81：目的号码的类型及格式

8126117302f1：目的号码的内容，即 18621137201　f 是填充位
00：TP-protocol-identifier （TP-PID）无需关注
00：TP-DCS（Data-Coding-Scheme） 0000 0000 携带的主要信息是无 message class, use 7bit default
ff：有效期的值
根据指定格式选择合适的公式计算，有效期为 255-192=63weeks

02：短信内容长度为 2
8402：短信内容，参考 7 比特表解析出来是 èé
短信内容详细解析步骤如下：
84： 1000 0100　　最后 7 位即 000 0100，对照 7bitdefault 表即 è
02： 0000 0010
把上面的最高位 1 移到下面的最低位位置，且取最后七位，即 00 0010 1 对照
7bitdefault 表即 é 剩下的最高位 00 是填充位。

2.1.3 重要的信息

00, TP-DCS 0000 0000 携带的主要信息是无 message class, use 7bit default。

相关协议(23038)，如下面的图所示：（23038）

第一个 0，对应的下面 7...4 高位，是 00xx， Bit 5, if set to 0, indicates the text is uncompressed。Bit 4, if set to 0, indicates that bits 1 to 0 are reserved and have no message class meaning。

第二个 0，对应的下面的 Use of bits 3..0，也就是低 4 位。Bit 3 Bit2 Character set: 0 0， GSM 7 bit default alphabet。 Bit 1 Bit 0 根据 Bit 4 为 0，得知这 2 位是预留位。

Coding Group Bits 7..4	Use of bits 3..0
00xx	General Data Coding indication Bits 5..0 indicate the following: 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] 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:: 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]) Bits 3 and 2 indicate the character set being used, as follows : Bit 3 Bit2 Character set: 0 0 GSM 7 bit default alphabet 0 1 8 bit data 1 0 UCS2 (16bit) [10] 1 1 Reserved NOTE: The special case of bits 7..0 being 0000 0000 indicates the GSM 7 bit default alphabet with no message class

84： 1000 0100 最后 7 位即 000 0100，对照 7bitdefault 表即 è

02： 0000 0010

把上面的最高位 1 移到下面的最低位位置，且取最后七位，即 00 0010 1 对照 7bit default 表即 é 剩下的最高位 00 是填充位。

相关协议(23038), 如下所示：

SMS Packing

Packing of 7-bit characteristics

If a character number α is noted in the following way:

b7	b6	b5	b4	b3	b2	b1
αa	αb	αc	αd	αe	αf	αg

The packing of the 7-bitscharacters in octets is done by completing the octets with zeros on the left.

For examples, packing: α

- one character in one octet:
  - bits number:

7	6	5	4	3	2	1	0
0	1a	1b	1c	1d	1e	1f	1g

- two characters in two octets:
  - bits number:

7	6	5	4	3	2	1	0
2g	1a	1b	1c	1d	1e	1f	1g
0	0	2a	2b	2c	2d	2e	2f

- three characters in three octets:
  - bits number:

7	6	5	4	3	2	1	0
2g	1a	1b	1c	1d	1e	1f	1g
3f	3g	2a	2b	2c	2d	2e	2f
0	0	0	3a	3b	3c	3d	3e

- seven characters in seven octets:
  - bits number:

7	6	5	4	3	2	1	0
2g	1a	1b	1c	1d	1e	1f	1g
3f	3g	2a	2b	2c	2d	2e	2f
4e	4f	4g	3a	3b	3c	3d	3e
5d	5e	5f	5g	4a	4b	4c	4d
6c	6d	6e	6f	6g	5a	5b	5c
7b	7c	7d	7e	7f	7g	6a	6b
0	0	0	0	0	0	0	7a

- eight characters in seven octets:
  - bits number:

7	6	5	4	3	2	1	0
2g	1a	1b	1c	1d	1e	1f	1g
3f	3g	2a	2b	2c	2d	2e	2f
4e	4f	4g	3a	3b	3c	3d	3e
5d	5e	5f	5g	4a	4b	4c	4d
6c	6d	6e	6f	6g	5a	5b	5c
7b	7c	7d	7e	7f	7g	6a	6b
8a	8b	8c	8d	8e	8f	8g	7a

The bit number zero is always transmitted first.
Therefore, in 140 octets, it is possible to pack (140x8)/7=160 characters.

2.2 SMS receive pdu

2.2.1 Log 信息

radio_log:

11-18 16:18:47.214 725 734 D use-Rlog/RLOG-AT: AT<
0891683110304105F0240D91685120817050F10000411181618144230220 10

2.2.2 接收数据流分析

08 91 683110304105F0 24 0D 91 685120817050F1 00 00 41118161814423 02 2010

SCA	PDUType	OA	PID	DCS	SCTS	UDL	UD
1~12	1	2~12	1	1	7	1	0~140
0891683110304105F0	24	0D91685120817050F1	00	00	41118161814423	02	2010

08：SMSC 信息的长度
91：SMSC 的地址类型（91 意味着国际格式的电话号码）
683110304105F0：服务中心的号码，即 8613010314500 f 是填充位

24：

Bit No.	7	6	5	4	3	2	1	0
	RP	UDHI	SRI			MMS	MTI	
	0	0	1	0	0	1	00	

SRI=1，状态报告指示（Status Report Indication），此值仅被短消息中心（SMSC）设置，状态报告将返回给短消息实体（SME）
MMS=1，在 SMSC 中没有更多的信息等待 MS
MTI=00，SMS-DELIVER (SMSC - MS)

0D：源号码长度
91：源号码的类型及格式
685120817050F1：源号码的内容，即 8615021807051 f 是填充位
00：TP-protocol-identifier 无需关注
00：TP-DCS 0000 0000 携带的主要信息是无 message class,use 7bit default
41118161814423：接收时间是 14 年/11 月/18 日 16:18:44
23 指时区 23*1/4=8 北京时间

02：接收的短信内容长度为 2
2010：短信内容 参考 7 比特表解析出来是 SPSP --SP 指空格
短信内容详细解析步骤如下：

20： 0010 0000 最后 7 位即 010 0000，对照 7 bit default 表即 SP
10： 0001 0000
把上面的最高位 0 移到下面的最低位位置，且取最后七位，即 01 0000 0 对照 7bit default 表即 SP 剩下的最高位 00 是填充位。

2.2.3

可见发送 èé 的数据流没错，接收到空格的数据流也没错。错误就出在传送途中，对数据流进行了篡改。是不同运营商之间网络兼容性问题导致的。

END OF DOCUMENT