

开发者指南

SMS with the SMS PDU-mode

翻译整理: 犬犬(心帆)

E-Mail: shuixin13@163.com

最后修定日期: 2004-10-18

SMS with the SMS PDU-mode	1
编者序.....	3
版本变动历史.....	4
1、绪论.....	5
2、缩写词.....	6
3、设置指令.....	7
3.1 服务中心号码 (+CSCA).....	7
3.2 选择消息服务 (+CSMS).....	7
3.3 选择消息格式 (+CMGF).....	8
4、SMS 文本模式.....	9
5、SMS PDU 模式.....	9
5.1 发送方 SMS-Submit (Mobile Originated).....	9
5.1.1 向 SIM 卡存储区写入一条 SMS (+CMGW).....	10
5.1.2 发送 SIM 卡存储区中的一条 SMS (+CMSS).....	10
5.1.3 直接从终端设置发送 SMS (+CMGS).....	11
5.2 接收方 SMS-DELIVER (Mobile Terminated).....	12
5.2.1 列取消息 (+CMGL).....	12
5.2.2 读取消息 (+CMGR).....	12
5.2.3 删除消息 (+CMGD).....	13
6、SMS PDU 基本组成元素.....	13
6.1 发送方 PDU 格式 SMS-SUBMIT-PDU (Mobile Originated).....	14
6.2 接受方 PDU 格式 SMS-DELIVER-PDU (Mobile Terminated).....	14
6.3 SCA 短消息服务中心地址格式.....	15
6.4 PDU Type (第一个八位位组).....	16
6.5 MR 信息参考 (Message Reference).....	17
6.6 DA/OA 接收方地址与发送方地址.....	17
6.7 PID 协议标识 (Protocol-Identifier).....	18
6.8 DCS 数据编码方案 (DataCoding-Scheme).....	18
6.9 VP 信息有效期 (Validity Period).....	19
6.10 SCTS 服务中心时间戳 (Service Center TimeStamp).....	20
6.11 UDL 用户数据长度 (User-Data-Length (Amount of Characters)).....	20
7、常用 AT 指令.....	20
8、PDU 操作实例.....	21
8.1 准备工作.....	21
8.2 连接手机.....	22
8.3 发送 PDU SMS.....	22
9、SMS 编码方案与编程实现.....	25
附.....	27
Message service error.....	27
error codes:.....	27
默认的字符表.....	29

编者序

前些天 QQ 上 Delphi 群里的有人做手机 SMS 相关的项目，我就把本本中的所有资料都传给了他，可他还是有好些不明白的地方，可能是我的文档不是太清晰，以致误人子弟了吧！狂汗中！_-|||

这个文章是出于 2003-08，那时我正在山东做项目，也是有关手机 SMS 通信方面的，因为手上只有英文资料，而组中的成员需要中文资料，因而有了它了。

再次打开这个文档，手触键盘时不禁感慨万千！

2003-07-08，我由南京去山东，正值学生放暑假，这一天竟只买到了一张站票去河南的商丘！1566 次沪开郑，16 车，22：30 时，这一天，这一时，上天将我推到了一个女孩身边。当第一眼遇着她那眼睛时，我凝滞了，就如很久未见的好友，突然间的相逢，感觉是那么得亲切而没有隔阂，那时我从心底的最深处笑了。:)）

这一夜我站到了清晨，终是斗胆地与她要了 E-Mail，好怕怕，因为如果不这样子的话，我知我一定会后悔的。其它已不敢再多问什么，至少我已知道了她是从苏州上车，应该是在苏州上学的了。:-)

到了山东后，给她去了好些 Mail，可一封都没有回复，一切都消失了。上天既然将我推到她面前，为什么又如此快地收回呢？好后悔当时为什么不再问她的姓名，她的电话，或是她的学校.....

8-20 号，项目文档整理完毕。

23 号，终于回到了南京，辞去工作，休息一天后，我于 25 号到了苏州，一个陌生的城市，一丝丝的兴奋，一丝丝的沉忧.....

.....

十月六号这一天，上天竟是如此地厚爱我，竟让我找到了她.....

.....

一年了，我们相识了很多，如今的我，心情已平静，她在努力着她的学业，我奋斗着我的工作，我们间会有真正地交集吗？我不知道.....

随缘吧

随缘而来

随缘而去

多年后，至少我们会说：我不后悔，因为我们曾经努力过，也曾开心着.....

犬犬

2004-10-19 0:56:40

于苏州

版本变动历史

2003-08-20 第一版

2004-10-18 修订第二版

修正 [6.6 DA/OA 接收方地址与发送方地址](#) 协议格式翻译错误

增加 AT 指令介绍

增加 [8、PDU 操作实例](#)

1、绪论

SMS 提供了在 GSM 移动站台(MS)与一个短消息实体(SME)之间通过服务中心(SC)传送短消息的方法。SC 提供了在 MS 与 SME 之间消息传送的相互联系和转播的功能。

SMS 采用存储转发模式，短消息被发送出去之后，不是直接地发送给接收方，而是先存储在 SMS（短消息服务中心），然后再由 SMC 将其转发给接收方。如果接收方当时关机或不在服务区内，SMC 会自动保存该短消息，排队并尝试再次发送给接收方。

点到点短消息服务包含两个基本服务：

- ? SM MT (点到点短消息移动接收)
- ? SM MO (点到点短消息移动发送)

通过 SM MT 或 SM MO 方法传送的文本消息包含 140 个八位位组(最大 160 个拉丁字母字符、70 个双字节字符)。

本文仅仅给出了简单地一些 AT 指令及 SMS PDU 模式的描述。更多的详细资料，请参看下列标准：

GSM 03.04

GSM 03.38

GSM 03.41

GSM 07.05

GSM 07.07

2、缩写词

缩写	全称	说明
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
SMSC	Short Message Service Center	短消息服务中心 负责在移动基站和 SME 之间中继、存储或转发短消息
PDU	Protocol Data Units	协议数据单元
PDU Type	Protocol Data Unit Type	协议数据单元类型
MR	Message Reference	消息参考
OA	Originator Adress	发送方地址
DA	Destination Adress	接收方地址
PID	Protocol Identifier	协议标识
DCS	Data Coding Scheme	数据编码方案
SCTS	Service Center Time Stamp	服务中心的时间戳
VP	Validity Period	消息有效期
UDL	User Data Length	用户数据长度
UD	User Data	用户数据
RP	Reply Path	应答路径
UDHI	User Data Header Indicator	用户数据头标识
SRI	Status Report Indication	状态报告指示
SRR	Status Report Request	请示状态报告
VPF	Validity Period Format	有效期格式
MMS	More Messages to Send	有更多的信息需要发送
RD	Reject Duplicate	拒绝复本
MTI	Message Type Indicator	消息类型指示
ME	Mobile Equipment	移动设备
TE	Terminal Equipment	终端设备
SIM	Subscriber Identity Modul	
SC	Service-Center	服务中心
SCA	Service Center Address	服务中心地址
SM MT	Short Message Mobile Terminated Point-to-Point	点到点短消息移动接收
SM MO	Short Message Mobile Originaed Point-to-Point	点到点短消息移动发送

3、设置指令

3.1 服务中心号码 (+CSCA)

服务中心(SC)负责转播和存储转发 SME 和 MS 之间的短消息。如果 MS 支持 SMS-MO (短消息服务移动发送), 为了使用 SMS, 必须在 MS 中设置 SMSC (短消息服务中心, SCA)。

使用指令“AT+CSCA?”可以查看存储在 SIM 卡中的当前服务中心地址。

使用 AT 指令“AT+CSCA=<SCA>[,<TOSCA>]”加入短消息服务号码。

句法：

输入	执行	注释
AT+CSCA?	<CR>	查询当前服务中心地址(SCA)设置 (从 SIM 卡中读取)
响应		
+CSCA: “<SCA>” OK		

AT+CSCA="<SCA>"	<CR>	定义服务中心地址(SCA) (存储到 SIM 卡)
-----------------	------	---------------------------

参数：

<SCA>	服务中心地址 (字符型)
<TOSCA>	服务中心地址的类型设置 (编码方式)

示例：

AT+CSCA="+8613800250500"	<CR>	以国际号格式定义服务中心地址(SCA)
AT+CSCA="+13800250500"	<CR>	以国内号格式定义服务中心地址(SCA)

注意：

⇒ 为了避免漫游时出现问题, 推荐国际号码格式存储所有地址 (以“+”和国家代码开头)。

⇒ 向你本地的网络提供商询问正确的短消息服务中心号码

⇒ SC 地址是 SMS 的一部分! 当任何一个 SMS 被存储到 SIM 卡上时, SC 地址也同时该 SMS 中。

3.2 选择消息服务 (+CSMS)

这个指令用于选择消息服务。

句法：

输入	执行	注释
AT+CSMS?	<CR>	返回当前的服务类型及 ME 支持的信息

AT+CSMS=?	<CR>	返回所有支持的服务类型
-----------	------	-------------

AT+CSMS=<SERVICE>	<CR>	选择消息服务
响应		
+ CSMS: <SERVICE>,<MT>,<MO>,<BM>		
OK		

参数：

<SERVICE>	消息服务
<MT>	接收短消息
<MO>	发送短消息
<BM>	接收小区广播消息

示例：

读取指令

输入	执行	注释
AT+CSMS?	<CR>	返回当前的服务类型及 ME 支持的信息
响应		
+ CSMS: 0,1,1,1		指令返回当前的消息服务和移动设备支持的服务选项
OK		

设置指令

输入	执行	注释
AT+CSMS=1	<CR>	设置支持的消息类型
响应		
+ CSMS: 0,1,1,1		返回移动设备支持的服务选项
OK		

参数：

参数	值	描述
<SERVICE>	0	SMS AT 指令的句法兼容 GSM Phase 2
	1	SMS AT 指令的句法兼容 GSM Phase 2+
	2...127	保留
	128	厂商自定义
<MT>,<MO>,<BM>	0	不支持
	1	支持

3.3 选择消息格式 (+CMGF)

这个指令用于选择短消息格式。它的参数指示发送、列取、读取和写入的消息所使用的格式。

句法：

输入	执行	注释
AT+CMGF?	<CR>	返回当前的 SMS 格式

AT+CMGF=?	<CR>	返回所有支持的 SMS 格式
-----------	------	----------------

AT+CMGF=<MODE>	<CR>	选择 SMS 格式
响应		
OK		

支持的值：

<MODE>	含义
0	PDU 模式 (默认的)
1	Text 模式

示例：

读取指令

输入	执行	注释
AT+CMGF?	<CR>	返回当前的 SMS 格式
响应		
+ CMGF: 0 OK		返回当前的 SMS 格式

设置指令

输入	执行	注释
AT+CMGF=1	<CR>	设置 SMS 类型为 Text

4、SMS 文本模式

略

5、SMS PDU 模式

一个完整的 SMS 消息所包含的所有报头信息被以二进制字符串格式传送。这个二进制串由十六进制格式的 IA5 字符组合而成。

使用 AT 指令“AT+CMGF=0”切换到协议数据模式，之后所有的 SMS 输入与显示将以 PDU 格式执行。

5.1 发送方 SMS-Submit (Mobile Originated)

SMS-SUBMIT 的意思就是 GSM-Mobile 传送一条 SMS 到服务中心。

5.1.1 向 SIM 卡存储区写入一条 SMS (+CMGW)

执行指令"AT+CMGW"用于存储一条消息在 SIM 卡的存储区中。命令返回消息被存储的索引号。

句法：

输入	执行	注释
AT+CMGW=<LENGTH>[,<STAT>]	<CR>	
> <PDU> *)	<CTRL-Z>/<ESC> **)	
响应		
+CMGW: <INDEX> OK	如果命令正确执行，返回消息存储位置的索引号	

参数：

<LENGTH>	给定的 TP 层数据单元的八位位组代码数目(不包含服务中心地址的八位位组数目)
<STAT>	除存储未发送的状态之外的状态值 在 PDU 模式下该值为整型（默认值为 0） 在文本模式下该值为字符型（默认值为"REC UNREAD"）
<PDU>	PDU 数据
<INDEX>	存储位置

支持的值：

<STAT>	含义
0 "REC UNREAD"	已接收未读的消息（例如新消息）
1 "REC READ"	已接收已读的消息
2 "STO UNSENT"	已存储未发送的消息
3 "STO SENT"	已存储已发送的消息
4 "ALL"	所有的消息（仅适用于 +CMGL 命令）

注：

*) 符号">"是移动终端设置返回而产生的

**> <CTRL>+<Z> 执行命令；<ESC>不保存/发送、直接退出执行

5.1.2 发送 SIM 卡存储区中的一条 SMS(+CMSS)

AT 指令"AT+CMSS=<INDEX>[,<DA>[,<TODA>]]"将 SIM 卡消息存储区中<INDEX>索引位置的消息发送到网络中（SMS-SUBMIT）。如果指定新的接收地址<DA>，它将代替原消息中存储的接收地址。

如果消息传送成功，消息参考值<MR>将返回到终端设备（TE）。通常（当+CSMS<SERVICE>值为 1，并且网络支持时），同时返回服务中心时间戳<SCTS>。

句法：

输入	执行	注释
----	----	----

AT+CMSS=<INDEX>	<CR>	
响应		
+CMSS: <MR>[,<SCTS>]		
OK		

参数：

<INDEX>	SIM 卡内存位置索引
<MR>	消息参考
<SCTS>	服务中心时间戳

示例：

输入	执行	注释
AT+CMSS=1	<CR>	SIM 卡中存储位置 1 的消息将被发送到服务中心
响应		
+CMSS: 255		SMS 被发送到服务中心，消息参考为 255
OK		

5.1.3 直接从终端设置发送 SMS (+CMGS)

这个指令用于从一个终端向网络中发送消息 (SMS-SUBMIT)，而不会在 SIM 卡中保存所发送的 SMS 消息。

如果消息传送成功，消息参考值<MR>将返回到终端设备 (TE)。通常 (当+CSMS<SERVICE>值为 1，并且网络支持时)，同时返回服务中心时间戳<SCTS>。

句法：

输入	执行	注释
AT+CMGS=<LENGTH>	<CR>	转换 SMS 输入模式，SMS 将会被以“未发送”状态保存。命令后所跟的 PDU 字符串的长度必须在这个命令中指定。
> <PDU> (*)	<CTRL-Z>/<ESC> (**)	直接从终端中发送一条 SMS，而不将其保存到 SIM 卡。
响应		
+CMGS: <MR>[,<SCTS>]		如果发送成功将返回消息参考
OK		

参数：

<LENGTH>	给定的 TP 层数据单元的八位位组代码数目 (不包含服务中心地址的八位位组数目)
<PDU>	PDU 数据
<MR>	消息参考
<SCTS>	服务中心时间戳

注：

- *) 符号">"是移动终端设备返回而产生的
- **) <CTRL>+<Z> 执行命令；<ESC>不保存/发送、直接退出执行

5.2 接收方 SMS-DELIVER (Mobile Terminated)

SMS-DELIVER 意味着终端设置从服务中心接收到一条 SMS 消息。

5.2.1 列取消息 (+CMGL)

句法：

输入	执行	注释
AT+CMGL=<INDEX>	<CR>	列取内存中指定类型的 SMS
响应		
+CMGL: <index><stat>[,<alpha>],<length> <pdu> [+CMGL: <index><stat>[,<alpha>],<length> <pdu> [...]]		
AT+CMGL=?	<CR>	查看设备支持的<stat>类型

参数：

参数	描述										
<STAT>	<p>在 PDU 模式下该值为整型（默认值为 0）</p> <p>在文本模式下该值为字符型（默认值为"REC UNREAD"）</p> <p>指示内存中消息的状态</p> <p>定义的值：</p> <table border="1"> <tbody> <tr> <td>0 "REC UNREAD"</td> <td>已接收未读的消息（例如新消息）</td> </tr> <tr> <td>1 "REC READ"</td> <td>已接收已读的消息</td> </tr> <tr> <td>2 "STO UNSENT"</td> <td>已存储未发送的消息</td> </tr> <tr> <td>3 "STO SENT"</td> <td>已存储已发送的消息</td> </tr> <tr> <td>4 "ALL"</td> <td>所有类型的消息</td> </tr> </tbody> </table>	0 "REC UNREAD"	已接收未读的消息（例如新消息）	1 "REC READ"	已接收已读的消息	2 "STO UNSENT"	已存储未发送的消息	3 "STO SENT"	已存储已发送的消息	4 "ALL"	所有类型的消息
0 "REC UNREAD"	已接收未读的消息（例如新消息）										
1 "REC READ"	已接收已读的消息										
2 "STO UNSENT"	已存储未发送的消息										
3 "STO SENT"	已存储已发送的消息										
4 "ALL"	所有类型的消息										

5.2.2 读取消息 (+CMGR)

句法：

输入	执行	注释
AT+CMGR=<INDEX>	<CR>	读取内存中指定索引位置的 SMS

响应	
+CMGR: <STAT>[,<ALPHA>],<LENGTH> <PDU>	
OK	

参数：

参数	描述								
<STAT>	在 PDU 模式下该值为整型（默认值为 0） 在文本模式下该值为字符型（默认值为“REC UNREAD”） 指示内存中消息的状态 定义的值 <table border="1" data-bbox="391 660 1104 831"> <tr> <td>0 “REC UNREAD”</td> <td>已接收未读的消息（例如新消息）</td> </tr> <tr> <td>1 “REC READ”</td> <td>已接收已读的消息</td> </tr> <tr> <td>2 “STO UNSENT”</td> <td>已存储未发送的消息</td> </tr> <tr> <td>3 “STO SENT”</td> <td>已存储已发送的消息</td> </tr> </table>	0 “REC UNREAD”	已接收未读的消息（例如新消息）	1 “REC READ”	已接收已读的消息	2 “STO UNSENT”	已存储未发送的消息	3 “STO SENT”	已存储已发送的消息
0 “REC UNREAD”	已接收未读的消息（例如新消息）								
1 “REC READ”	已接收已读的消息								
2 “STO UNSENT”	已存储未发送的消息								
3 “STO SENT”	已存储已发送的消息								
<ALPHA>	以字符型的数字文字表示的，在 SIM 电话簿中找到的相应<OA>条目								
<LENGTH>	给定的 TP 层数据单元的八位位组代码数目(不包含服务中心地址的八位位组)								
<PDU>	PDU 数据								

注意：

⇒ 切不可直接提交一个 DELIVER-SMS！因为它的 PDU 数据中头信息是与用于提交的 PDU 不一样的！

⇒ 在内存(SIM)中至少有最后一个空闲空间，以保证能接收到新的 SMS！

5.2.3 删除消息 (+CMGD)

句法：

输入	执行	注释
AT+CMGD=<INDEX>	<CR>	删除在 SIM 卡中索引<INDEX>位置的 SMS
响应		
OK		

6、SMS PDU 基本组成元素

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 Reference	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,、 Voice 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

6.1 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

示例：

向13851724908发送一条SMS，消息内容为：“Test”

0031000D91683158714209F80000A704D4F29C0E

向13851724908发送一条SMS，消息内容为：“测试”

0031000B813158714209F80008A7046D4B8BD5

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	0D91683158714209F8	00	00	A7	04	D4F29C0E
00	31	00	0B813158714209F8	00	18	A7	04	6D4B8BD5

6.2 接受方 PDU 格式 SMS-DELIVER-PDU (Mobile Terminated)

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

示例：

从13851724908接收到一条SMS，消息内容为：“Test”

0891683108200505F0240D91683158714209F800004001528035350004D4F29C0E

从13851724908接收到一条SMS，消息内容为：“测试”

0891683108200505F0240D91683158714209F8000840015280452400046D4B8BD5

SCA	PDUType	OA	PID	DCS	SCTS	UDL	UD
1-12	1	2-12	1	1	7	1	0-140
0891683108200505F0	24	0D91683158714209F8	00	00	40015280353500	04	D4F29C0E
0891683108200505F0	24	0D91683158714209F8	00	08	40015280452400	04	6D4B8BD5

6.3 SCA 短消息服务中心地址格式

服务中心地址包含三个部分：

SCA 组成：1-12 个八位位组

例：0891683108200505F0

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) 的八位位组数目。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，通过 “AT+CSCA=xxxxx” 指令可以设置 SIM 卡中存储的 SCA 值。

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，91&h 表示国际的)。91&h 是 TON/NPI 遵守 International/E.164 标准，指在号码前需加‘+’号；此外还有其它数值，但 91&h 最常用。

例：91 &h = 1001 0001 &b

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

数值类型 (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；

Addr：依照 ISDN 编号方式的短消息中心地址。

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

注：

指令 AT+CMGW 和 AT+CMGS 的参数 <length> 是从 PDUType 部分开始计算 PDU 的长度，不包括 SCA 的长度。所以：

输入： AT+CMGS=19<cr>
输出： AT+CMGS=19<cr><cr><lf>>
输入： 0891863108200505F031000D91683158714209F80000A704D4F29C0E<ctrl+z>
输出： 0891863108200505F031000D91683158714209F80000A704D4F29C0E<ctrl+z><cr><lf>+CMGS:

```
111<cr><lf><cr><lf>OK<cr><lf>
```

SCA = 0891863108200505F0

输入：

```
AT+CMGS=19<cr>
```

输出：

```
AT+CMGS=19<cr><cr><lf>>
```

输入：

```
0031000D916813158714209F80008A7046D4B8BD5<ctrl+z>
```

输出：

```
0031000D91683158714209F80008A7046D4B8BD5<ctrl+z><cr><lf>+CMGS:
```

```
112<cr><lf><cr><lf>OK<cr><lf>
```

SCA = 00

<cr> = 0D&h

<lf> = 0A&h

<ctrl+z> = 1A&h

6.4 PDU Type (第一个八位位组)

PDUType 是 SMS-SUBMIT、SMS-DELIVER 的第一个八位位组。它分别由下面几个部分组成：

PDUType 组成：1 个八位位组

发送方：SMS-SUBMIT

例：31&h = 0011 0001&b

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

接收方：SMS-DELIVER

例：04&h = 0000 0100&b

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

RP： 应答路径 (Reply Paht) ，

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), 此值仅被短消息服务中心 (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),
 00 – VP 段没有提供 (长度为 0),
 01 – 保留 ,
 10 – VP 段以整型形式提供 (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, 并且还存在于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 (More Messages to Send) , 此值仅被 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)
00 – SMS-DELIVER (SMSC → MS)
00 – SMS-DELIVER REPORT (MS → SMSC)
 当手机接收到 SMS-DELIVER 时自动产生
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
- 注 : (粗体代表手机支持的类型 , 并不是所有的 PDU 类型均被服务中心支持)

注意 :

PDType是PDU的第一个八位位组 , 而并不是服务中心号码后的第一个字节 !

6.5 MR 信息参考 (Message Reference)

设为 00 即可

6.6 DA/OA 接收方地址与发送方地址

OA 与 DA 格式是一样的 , 如下所示 :

DA 组成 : 2-12 个八位位组

例：0D91683158714209F8

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！

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，91&h 表示国际的)

Addr：依照 ISDN 编号方式的短消息中心地址。

示例：

电话号码	PDU格式编码
+8613851724908	0D 91 86 31 58 71 42 09 F8
13851724908	0B 81 31 58 71 42 09 F8
106051268812345 *)	0F A1 01 06 15 62 88 21 43 F5
123456	06 81 21 43 65

*) 小灵通号码

6.7 PID 协议标识 (Protocol-Identifier)

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

6.8 DCS 数据编码方案 (DataCoding-Scheme)

Bit No.	7	6	5	4	3	2	1	0	描述
示例：	0	0	0	0	0	0	0	0	= 00&h 7 bit 数据编码 默认字符集
	1	1	1	1	0	1	1	0	= F6&h 8 bit 数据编码 Class 1
	0	0	0	0	1	0	0	0	= 08&h USC2(16bit)双字节字符集

Bit No.7与 Bit No.6：

一般设置为 00；

Bit No.5：

0 – 文本未压缩，1 – 文本用GSM标准压缩算法压缩；

Bit No.4：

0 – 表示 Bit No.1、Bit No.0 为保留位，不含信息类型信息，

1 – 表示 Bit No.1、Bit No.0 含有信息类型信息；

Bit No.3与 Bit No.2：

00 – 默认的字母表，每个字符占用 7 比特位，此时最大可以传送 160 字符

01 – 8bit，此时最大只能传送 140 个字符

10 – USC2 (16bit)，传送双字节字符集

11 – 预留；

Bit No.1与 Bit No.0：

- 00 – Class 0, 短消息直接显示在屏幕上
 01 – Class 1,
 10 – Class 2 (SIM卡特定信息),
 11 – Class 3。

示例：

DSC	字符集	信息 Class
00	default (7-bit)	No Class
F0	default (7-bit)	Class 0 (immediate display)
F1	default (7-bit)	Class 1 (Mobile Equipment- specific)
F2	default (7-bit)	Class 2 (SIM specific message)
F3	default (7-bit)	Class 3 (Class3 Terminate Equipment- specific)
F4	8-bit	Class 0 (immediate display)
F5	8-bit	Class 1 (Mobile Equipment- specific)
F6	8-bit	Class 2 (SIM specific message)
F7	8-bit	Class 3 (Class3 Terminate Equipment- specific)
08	16-bit	No Class
18	16-bit	Class 0 (immediate display)

6.9 VP 信息有效期 (Validity Period)

第一种情况 (相对的) : $VPF = 10$ $VP = AA H$ (四天)

第二种情况 (绝对的) : $VPF = 11$

年	月	日	时	分	秒	时区
30	80	02	90	54	33	20

表示 03-08-20 09:45:33

VP 段以整型或半个8位组 (semi-octet) 形式提供。

第一种情况, VP为一个8位组, 给定有效期的长度,

从 SMS-SUBMIT 被 SMSC 接受开始计算。

第二种情况, VP为七个8位组, 给定有效期终止的绝对时间。

在第一种情况下, 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 个小时
90 – A7	12 小时 + (VF – 143)*30 分钟
A8 – C4	(VP – 166) * 1 天
C5 – FF	(VP – 192) * 1 周

第二种情况下的时间形式与 SCTS (Service Center TimeStamp) 形式一致。

6.10 SCTS 服务中心时间戳 (Service Center TimeStamp)

占用七个8位组，格式如 VP 的第二种情况所示

6.11 UDL 用户数据长度 (User-Data-Length (Amount of Characters))

UDL 以整型形式提供，表示后面用户数据段的数据长度。

数据格式有 3 种：7bit，8bit，16bit。

其中 7bit 采用 GSM 字符集，8bit 采用 ASCII 字符集，16bit 采用 Unicode 字符集。

1 octet	0 .. 140 octets
UDL	UD
05	E8 32 9B FD 06

如：7bit 数据 "Test"

UDL = 04, UD = D4 F2 9C 0E

又如：16bit 数据 "Test"

UDL = 08, UD = 00 54 00 65 00 73 00 74

用户数据 (UD) 的编码方式请参考[第 9 章 SMS 编码方案与编程实现](#)

7、常用 AT 指令

AT 指令	功 能
AT+CMGC	Send an SMS command (发出一条短消息命令)
AT+CMGD	Delete SMS message (删除 SIM 卡内存的短消息)
AT+CMGF	Select SMS message formate (选择短消息信息格式：0-PDU;1-文本)
AT+CMGL	List SMS message from preferred store (列出SIM卡中的短消息PDU/text 0/ " REC UNREAD " -未读 1/ " REC READ " -已读 2/ " STO UNSENT " -待发 3/ " STO SENT " -已发 4/ " ALL " -全部的)
AT+CMGR	Read SMS message (读短消息)
AT+CMGS	Send SMS message (发送短消息)
AT+CMGW	Write SMS message to memory (向 SIM 内存中写入待发的短消息)
AT+CMSS	Send SMS message from storage (从 SIM 内存中发送短消息)

AT+CNMI	New SMS message indications (显示新收到的短消息)
AT+CPMS	Preferred SMS message storage (选择短消息内存)
AT+CSCA	SMS service center address (短消息中心地址)
AT+CSCB	Select cell broadcast messages (选择蜂窝广播消息)
AT+CSMP	Set SMS text mode parameters (设置短消息文本模式参数)
AT+CSMS	Select Message Service (选择短消息服务)

8、PDU 操作实例

8.1 准备工作

一台支持 AT 操作的手机或手机模块，建议使用 SIEMENS 的，我使用的是西门子 2118。

一根串口数据线。

串口调试软件：

串口调试助手 V2.2

RoaringWindStudio 啸峰工作室

<http://www.gjwtech.com/>

用于通过串口发送和接收数据。

Portmon

Mark Russinovich

<http://www.sysinternals.com>

用于监听系统中正在使用中的串口或并口当前传送的数据。

西门子手机工作室

通过上面的监听程序分析它的动作，你可以学到很多。

8.2 连接手机

将数据线插在主机的 COM1 上,然后运行串口调试助手 V2.2,设置串口为 COM1,波特率为 19200,校验位为 NONE,数据位为 8,停止位为 1。然后输入 AT 再加一个回车,之后点发送按钮,如果手机应答 AT<cr><cr><cl>OK<cr><cl>,则说明电脑已与手机正常连接!如下图所示:



8.3 发送 PDU SMS

如前面所述,向号码为 +8613851724908 手机发送一条内容为“Test”的 SMS, PDU 串是 0031000D91683158714209F80000A704D4F29C0E, 它的长度是 20 个八位位组, 而最左方的 00 位组是 PDU 串中的短消息服务中心字段, AT+CMGS=<length>指令的<length>不将其计算在内, 所以首先应该发送 AT+CMGS=19<cr>:



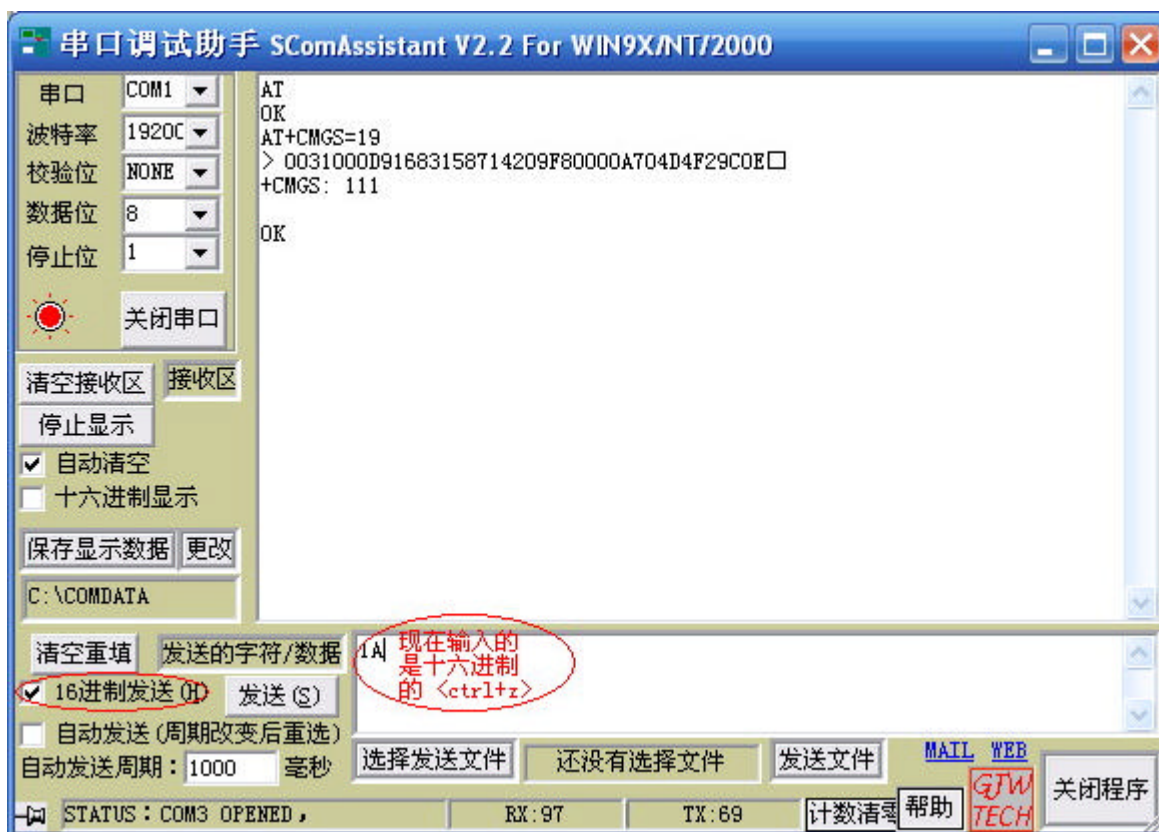
如上图所示，手机返回了

```
AT+CMGS=19
>
```

这是要尽快输入PDU串：0031000D91683158714209F80000A704D4F29C0E



正确输入了 PDU 串后，还需要输入一个控制字符<ctrl+z> 1A &h 通过手机立即将它发送出去，或输入<esc> 1B &h 通过终端设备放弃。



手机返回

```
+CMGS: 111
OK
```

说明短消息发送成功！返回的消息参考是 111，表示这是发送成功的第 111 条消息（服务中心不保证该值绝对准确）。

9、SMS 编码方案与编程实现

a. 英文编码

参见表，设短信息内容为“Hello World!”。缺省的GSM 字符集为7位编码，可以简单地理解为ASCII码（ASCII值小于80Hex，因此，Bit8被忽略），依次将下一7位编码的后几位逐次移至前面，形成新的8位编码，参见表2箭头指示。GSM并非支持所有的ASCII字符显示。

编号	字符	ASCII码	8位二进制	7位二进制	移位变换后	最后编码
1	H	48	0100 1000	100 1000	<u>1</u> 100 1000	C8
2	e	65	0110 0101	110 010 <u>1</u>	<u>00</u> 11 0010	32
3	l	6C	0110 1100	110 11 <u>00</u>	<u>100</u> 1 1011	9B
4	l	6C	0110 1100	110 1 <u>100</u>	<u>1111</u> 1101	FD
5	o	6F	0110 1111	110 <u>1111</u>	<u>0000</u> 0110	06
6	[sp]	20	0010 0000	01 <u>0</u> 0000	<u>0101</u> 1101	5D
7	w	57	0101 0111	<u>101</u> 0111	<u>1101</u> 1111	DF
8	o	6F	0110 1111	<u>110</u> 1111	<u>0111</u> 0010	72
9	r	72	0111 0010	<u>111</u> 0010	<u>00</u> 11 0110	36
10	l	6C	0110 1100	110 110 <u>0</u>	<u>0011</u> 1001	39
11	d	64	0110 0100	110 01 <u>00</u>	<u>0000</u> 0100	04
12	!	21	0010 0001	010 <u>0001</u>		

下面是实现英文编码的部分Delphi 5代码：

```
function Encode1(var s: String): String;
var
  i, j, len: Integer;
  cur: Integer;
  t: String;
begin
  Result := "";
  len := Length(s);
  //j 用于移位计数
  i := 1;
  j := 0;
  while i <= len do
  begin
    if i < len then
      //数据变换
      cur := (Ord(s[i]) shr j) or ((Ord(s[i+1]) shl (7 - j)) and $ff)
    else
      cur := (Ord(s[i]) shr j) and $7f;
    FmtStr(t, '%2.2X', [cur]);
```

```

Result := Result + t;
inc(i);
//移位计数达到7位的特别处理
j := (j + 1) mod 7;
if j = 0 then
    inc(i);
end;
end;
end;

```

b. 中文编码

通过Delphi的WideString类型转换，可以巧妙地实现GB2312到Unicode的编码转换（注意代码页和操作系统相关联）。下面是实现中文编码的部分

编号	字符	GB2312编码	GB2312 编码 BIN	Unicode 编码 BIN 代码页CP936
1	中	D6	1101 0110	0100 1110
		D0	1101 0000	0010 1101
2	文	CE	1100 1110	0110 0101
		C4	1100 0100	1000 0111

Delphi 5代码：

```

function Encode2(var s: WideString): String;
var
    i, len: Integer;
    cur: Integer;
    t: String;
begin
    Result := '';
    len := Length(s);
    i := 1;
    while i <= len do
    begin
        cur := Ord(s[i]);
        //BCD转换
        FmtStr(t, '%4.4X', [cur]);
        Result := Result + t;
        inc(i);
    end;
end;
end;

```

附

Message service error

These are the error codes for +CMS ERROR.

0-127	GSM 04.11 Annex E-2 values
128-255	GSM 03.40 section 9.2.3.22 values
300	Phone failure
301	SMS service of phone reserved
302	Operation not allowed
303	Operation not supported
304	Invalid PDU mode parameter
305	Invalid text mode parameter
310	SIM not inserted
311	SIM PIN necessary
312	PH-SIM PIN necessary
313	SIM failure
314	SIM busy
315	SIM wrong
320	Memory failure
321	Invalid memory index
322	Memory full
330	SMSC (message service center) address unknown
331	No network service
332	Network timeout
500	Unknown error
512	Manufacturer specific

error codes:

0	phone failure
1	no connection to phone
2	Phone-adaptor link reserved
3	operation not allowed
4	operation not supported
5	PH-SIM PIN necessary
10	SIM not inserted
11	SIM PIN required
12	SIM PUK required
13	SIM failure

14	SIM busy
15	SIM wrong
16	incorrect password
20	memory full
21	invalid index
22	not found
23	memory failure
24	text string too long (+CPBW)
25	invalid characters in text string
26	dial string too long
27	invalid characters in dial string
30	no network service
31	network timeout
100	unknown
265	PUK for theft protection necessary
266	PUK2 for SIM necessary
267	PIN2 for SIM necessary

默认的字符表

				b7	0	0	0	0	1	1	1	1
				b6	0	0	1	1	0	0	1	1
				b5	0	1	0	2	0	1	0	1
b4	b3	b2	b1		0	1	2	3	4	5	6	7
0	0	0	0	0	@	Δ	SP	0	-	P	¨	p
0	0	0	1	1			!	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		Λ		4	D	T	d	t
0	1	0	1	5		Ω	%	5	E	U	e	u
0	1	1	0	6		Π	&	6	F	V	f	v
0	1	1	1	7		Ψ	'	7	G	W	g	w
1	0	0	0	8		Σ	(8	H	X	h	x
1	0	0	1	9		Θ)	9	I	Y	i	y
1	0	1	0	10	LF	Ξ	*	:	J	Z	j	z
1	0	1	1	11			+	;	K	Ä	k	ä
1	1	0	0	12			,	<	L	Ö	l	ö
1	1	0	1	13	CR		-	=	M		m	
1	1	1	0	14		β	.	>	N	Ü	n	ü
1	1	1	1	15			/	?	O		o	