Version：V.0.0.9
Level：Confidential

GPS Tracker

Communication Protocol

（AZ735）

Content

i.Protocol Packet Format

Format	Length (Byte)	Description
Start Bit	2	0x780x78（packet length : 1bit）or 0x790x79（packet length 2 bits）
Packet Length	1(2)	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	Transmission packet type（see the following diagram for details）
Information Content	N	Content is defined by specific application and protocol number
Information Serial Number	2	Serial number of data sent later at each time will be automatically added ‘1’.
Error Check	2	Values of CRC-ITU from “Packet Length” to “Information Serial Number”. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value:0x0D 0x0A

1.1 **Protocol Number**

Login information	0x01
Heartbeat packet	0x23
Online command response by terminal	0x21
GPS location information	0x32
Location information (alarm)	0x33
Online command	0x80
Information Transmission Packet	0x98

ii. Protocol Packet

1. Login packet

Description：

- Login packet is the information packet connecting the terminal and platform, it can send terminal information to platform.
- If a GPRS connection is established successfully, the terminal will send a first login message packet to the server and, within five seconds, if the terminal receives a data packet responded by the server, the connection is considered to be a normal connection; if not, the terminal will send login packet again.
- If no packet returned by server within 5 seconds, then the response of login packet is timeout.
- Terminal reboot automatically after 3 timeouts.

a) Login Message Packet

Format		Length (Byte)	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x01
Info Content	IMEI	8	Example：IMEI number is 123456789123456，terminal ID is：0x01 0x23 0x45 0x67 0x89 0x120x34 0x56
	Model Identification Code	2	GB100 is 3605
	Time Zone Language	2	See the following chart for details of time zone language mark.
Information Serial Number		2	Serial number of data sent later at each time will be automatically added ‘1’.
Error Check		2	Values of CRC-ITU from “Packet Length” to “Information Serial Number with secret key”. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. JAR (only used this packet) is adopted to calculate.
Stop Bit		2	Fixed value:0x0D 0x0A

Example：78 78 11 01 08 68 12 01 48 37 35 71 36 05 32 02 00 39 DE F7 0D 0A

Time Zone Language

One and a half bits bit15—bit	15	Time zone value expands 100 times
	14	
	13	

4	12		
	11		
	10		
	9		
	8		
	7		
	6		
	5		
	4		
Lower half bit bit4-bit0	3	GMT	
	2	No definition	
	1	Language Select Bit	1
	0	Language Select Bit	0

Bit3 0-------Eastern time

1------- Western time

Example: Extended bit: 0x32 0x00 means GMT+8

Calculation method: 8*100=800 converts to HEX: 0X0320

Extended bit: 0x4D 0xD8 means GMT-12:45

Calculation method: 12.45*100=1245 converts to HEX: 0x04 0xDD

Here, to save 4 bytes, calculation result left shifted 4 bits and combined eastern time, western time and language bit.

b) **Login packet response（server response）**

Format	Length	Description
Start Bit	2	0x78 0x78
Packet Length	1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	0x01
Date Time（UTC）	6	Year（1byte）Month（1byte）Day（1byte）Hour（1byte）Min（1byte）Second（1byte）（converted to decimal）
Reserved Extension Bit Length	1	This bit is added for function extension. If the length of this bit is 0, then the bit is null.
Reserved Extension Bit	N	Function extension bit. If the length of reserved extension bit is 0, then the bit is null.
Information Serial Number	2	Serial number of data sent later each time will be automatically added '1'.
Error Check	2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)

Stop Bit	2	Fixed value: 0x0D 0x0A

Example：78 78 0C 01 11 03 14 08 38 39 00 00 39 95 70 0D0A

2. Heartbeat Packet

Description：

- Heartbeat packet is a data packet to maintain the connection between the terminal and the server.
- If a GPRS connection is established successfully, the terminal will send a heartbeat packet to the server and, within five seconds, if the terminal receives a data packet responded by the server, the connection is considered to be a normal connection; if not, the terminal will send heartbeat packet again.
- If no packet returned by server within 5 seconds, then the response of heartbeat packet is timeout.
- Terminal reboot automatically after 3 timeouts.

a) Heartbeat packet sent by terminal

		Length (Byte)	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x23
Info Content	Terminal Information Content	1	See the following diagram for details
	Voltage Level	2	Converting method: Divide by 100 after converting hex into decimal. Eg：0X01,0X9F, 019Fconverted decimal is 415; 415 divided by 100 is 4.15. 4.15 is the terminal voltage.
	GSM Signal Strength	1	0x00: no signal; 0x01: extremely weak signal; 0x02: very weak signal; 0x03: good signal; 0x04: strong signal.
	Language/Extended Port Status	2	latter bit 0x01 Chinese 0x02 English
Serial Number		2	Serial number of data sent later at each time will be automatically added ‘1’.
Error Check		2	Error check (From “Packet Length” to “Information Serial Number”) , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:0x0D 0x0A

Example：78 78 0B 23 C0 01 22 04 00 01 00 08 18 72 0D 0A

Terminal Information

One byte is consumed defining for various status information of the mobile phone.

Bit		Code Meaning
BYTE	Bit7	
	Bit6	1：GPS positioning
		0：GPS not positioning
	Bit3～Bit5	
	Bit2	1：Charging
		0：not charge
	Bit1	
	Bit0	1:Defense Activated (lock)
		0:Defense Deactivated(unlock)

b) Server Responds The Heartbeat Packet

	Length (Byte)	Description
Start Bit	2	0x78 0x78
Packet Length	1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	0x23
Serial Number	2	Serial number of data sent later at each time will be automatically added ‘1’.
Error Check	2	Error check (From “Packet Length” to “Information Serial Number”) , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D 0x0A

Example：78 78 05 23 01 00 67 0E 0D 0A

3. Location packet

Description：

- used to transmit terminal location and status

a) Location packet sent by terminal

		Length	Description
Start Bit		2	0x79 0x79
Packet Length		2	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x32(location)0x33 (alarm type)
Info Content	Date Time（UTC）	6	Year（1byte）Month（1byte）Day（1byte）Hour（1byte）Min（1byte）Second（1byte）（converted to a decimal）
	GPS Information Length	1	0 means no transmission. Default: 12
	Quantity of GPS information satellites	1	The first character is GPS information length， The second character is positioning satellite number （converted to a decimal）
	Latitude	4	Convert to a decimal and divide 1800000
	Longitude	4	Convert to a decimal and divide 1800000
	Speed	1	Convert to a decimal
	Course, Status	2	Convert to binary number of 16 bits and calculate by bits (see the following diagram)
	Main base station length	1	LBS main base station length. Default: 9. No LBS information transmitted if it is 0.
	MCC	2	Mobile Country Code
	MNC	1	Mobile Network Code(MNC)
	LAC	2	Mobile Network Code(MNC)
	CI	3	Cell Tower ID(Cell ID)
	RSSI	1	Signal level of community, range 0x00～0xFF, 0x00 Weakest signal 0xFF Strongest signal
	Sub-base station length	1	LBS sub- base station length. Default: 9. No LBS information transmitted if it is 0. 6 base station information transmitted when multiple base station locate.
	NLAC1	2	Same as LAC
	NCI1	3	Same as CI
	NRSSI1	1	Same as RSSI
	NLAC2	2	Same as LAC
	NCI2	3	Same as CI
	NRSSI2	1	Same as RSSI

	…		…
	WIFI Message Length	1	The WIFI information length should be 7 or the multiple of 7. Eg: 7 means sending one WIFI message while 14 means sending 2 WIFI messages. No transmission if it is 0.
	WIFI MAC1	6	MAC of received signal 1's WIFI（transmit by searched WIFI quantity. For example, transmit one if one WIFI searched; transmit several WIFI if several WIFI searched. No transmission if no WIFI)
	WIFI Strength 1	1	WIFI signal strength of 1
	WIFI MAC2	6	Same as above
	WIFI Strength 2	1	Same as above
	…		…
	Status	1	If protocol number is 0x32： 0x00 timing report 0x01 report in fixed distance 0x02 re-upload GPS data 0x0B LJDW report If protocol number is 0x33 0xA0 Lock report 0xA1 Unlock report 0xA2 Low internal battery alarm 0xA3 Low battery and shutdown alarm 0xA4 Abnormal alarm 0xA5 Abnormal unlocking alarm
	Reserved Extension Bit Length	1	This bit is added for function extension. If the length of this bit is 0, then the bit is null. (To increase the consistency of the server to identify the terminal and the Bluetooth unlocking, 3 extension bits are added. Note: This function only works on the alarm packet 33)
	Reserved Extension Bit	N	Function extension bit. If the length of reserved extension bit is 0, then the bit is null. (When the extension bit length is 3, this bit transmits the Bluetooth flag bit and GPS data, as shown in the table below)
Serial Number		2	Serial number of data sent later at each time will be automatically added '1'.
Error Check		2	Error check (From "Packet Length" to "Information Serial Number"), are values of CRC-ITU. CRC error occur when the received

		information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Serial Number	2	Fixed value: 0x0D 0x0A

Example：79 79 00 6F 33 11 03 14 09 06 08 00 09 01 CC 00 28 7D 00 1F 40 0E 24 28 7D 00 1F 71 07 28 7D 00 1E 3F 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 31 00 36 76 05 BB 5D 46 00 87 36 31 87 5B 48 CC 7B 35 36 61 A6 4C 00 E0 4B 8C BF 58 4F 78 A1 06 54 15 DE 4F 00 87 46 1B 9D 84 51 26 52 F3 AD B1 94 55 A1 00 00 08 38 B2 0D 0A

BYTE_1	Bit7	0
	Bit6	0
	Bit5	GPS real-time/differential positioning
	Bit4	GPS positioning or not
	Bit3	East Longitude, West Longitude
	Bit2	South Latitude, North Latitude
	Bit1	Course
	Bit0	
BYTE_2	Bit7	
	Bit6	
	Bit5	
	Bit4	
	Bit3	
	Bit2	
	Bit1	
	Bit0	

For example: the value is 0x15 0x4C, the corresponding binary is 00010101 01001100,

BYTE_1 Bit7 0
BYTE_1 Bit6 0
BYTE_1 Bit5 0 (real time GPS)
BYTE_1 Bit4 1 (GPS has been positioned)
BYTE_1 Bit3 0 (East Longitude)
BYTE_1 Bit2 1 (North Latitude)
BYTE_1 Bit1 0
BYTE_1 Bit0 1
BYTE_2 Bit7 0
BYTE_2 Bit6 1
BYTE_2 Bit5 0 → Course 332° (0101001100 in Binary, or 332 in decimal)
BYTE_2 Bit4 0
BYTE_2 Bit3 1
BYTE_2 Bit2 1
BYTE_2 Bit1 0
BYTE_2 Bit0 0

which means GPS tracking is on, real time GPS, location at north latitude, east longitude and the course is 332°.

Reserved Extension Bit

Reserved extension bit length	0x03
Bluetooth flag bit	0x11 0x00 （No alarm received or no Bluetooth flag bit if it is 0x00 0x00
Re-upload mark	0x00 real-time upload 0x01 re-upload

b) Server location packet response

Format	Length	Description
Start Bit	2	0x79 0x79
Packet Length	2	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	0x32 0x33 (the protocol number of location packet reply)
Serial Number	2	Serial number of data sent later at each time will be automatically added '1'. The server serial number needs to be consistent with the serial number of the terminal. The terminal needs to verify the serial number and ring to prompt.
Error Check	2	Error check (From "Packet Length" to "Information Serial Number") , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D 0x0A

Example：

4. Online command

Description：

- Use server online command to control terminal to execute task.
- Terminal response results to server.

a) Online command sent by server

		Length	Description
Start Bit		2	0x78 0x78
Length of data bit		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x80
Information Content	Length of Command	1	Server flag bit + command content length
	Server Flag Bit	4	Leave for server identification. Terminal receives the original data in Binary in response packet
	Command Content	M	Character string replied in ASCII coding. Command content is compatible with SMS command.
	Language	2	Latter 0x01 Chinese 0x02 English
Information Serial Number		2	Serial number of data sent later at each time will be automatically added ‘1’.
Error Check		2	Serial Number (including “Packet Length” and “Information Serial Number”) , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value:

Example：78 78 11 80 0B 00 00 00 00 55 4E 4C 4F 43 4B 23 00 01 53 54 0D 0A

b) Online command replied by terminal（0x21）

Terminal response（general command）

		Length	Description
Start Bit		2	0x79 0x79
Length of data bit		2	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x21
Info Content	Length of Command	4	Leave for server identification. Terminal receives the original data in Binary in response packet
	Server Flag Bit	1	0x01 ASCⅡ 0x02 UTF16-BE
	Command Content	M	Data to be sent（based on content coding）
Information Serial Number		2	Serial number of data sent later at each time will be automatically added ‘1’.

Error Check	2	Error check (From “Packet Length” to “Information Serial Number”) , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D 0x0A

Example：79 79 00 0D 21 00 00 00 00 01 4F 4B 21 00 07 A6 30 0D 0A

5. Information transmission packet

Information transmission packet sent by terminal

		Length	Description
Start Bit		2	0x79 0x79
Length of data bit		2	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x98
Information Content	Module number 1	1	Module number
	Module length 1	2	Module length
	Module content 1	M	Module content is decided by module number
	Module number 2	1	Module number
	Module length 2	2	Module length
	Module content 2	M	Module content is decided by module number
	…		…
Information Serial Number		2	Serial number of data sent later at each time will be automatically added ‘1’.
Error Check		2	Error check (From “Packet Length” to “Information Serial Number”) , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit		2	Fixed value: 0x0D 0x0A

Example：79 79 00 28 98 00 00 08 08 68 12 01 48 37 35 71 01 00 08 04 60 04 03 40 00 99 32 02 00 0A 89 86 02 B3 13 15 90 10 99 32 00 04 F5 81 0D 0A

Module Number

0x00	IMEI (hex)	0x10	
0x01	IMSI (hex)	0x11	
0x02	ICCID (hex)	0x12	
0x03	Chip ID (hex)	0x13	
0x04	Bluetooth MAC(hex)	0x14	
0x05		0x15	
0x06		0x16	
0x07		0x17	
0x08		0x18	
0x09		0x19	

0x0A		0x1A	
0x0B		0x1B	
0x0C		0x1C	
0x0D		0x1D	
0x0E		0x1E	
0x0F		0x1F	

a) Server reply to terminal

	Length	Description
Start Bit	2	0x79 0x79
Length of data bit	2	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number	1	0x98
Reserved Extension Bit Length	1	This bit is added for function extension. If the length of this bit is 0, then the bit is null.
Reserved Extension Bit	N	Function extension bit. If the length of reserved extension bit is 0, then the bit is null.
Information Serial Number	2	Serial number of data sent later at each time will be automatically added '1'.
Error Check	2	Error check (From "Packet Length" to "Information Serial Number") , are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet. (See Appendix 1)
Stop Bit	2	Fixed value: 0x0D 0x0A

Example: 79 79 00 06 98 00 00 00 C7 00 0D 0A

Appendix

1. code fragment of the CRC-ITU lookup table algorithm implemented based on C language

```
static const U16 crctab16[] =
{
    0X0000, 0X1189, 0X2312, 0X329B, 0X4624, 0X57AD, 0X6536, 0X74BF,
    0X8C48, 0X9DC1, 0XAF5A, 0XBED3, 0XCA6C, 0XDBE5, 0XE97E, 0XF8F7,
    0X1081, 0X0108, 0X3393, 0X221A, 0X56A5, 0X472C, 0X75B7, 0X643E,
    0X9CC9, 0X8D40, 0XBFDB, 0XAE52, 0XDAED, 0XCB64, 0XF9FF, 0XE876,
    0X2102, 0X308B, 0X0210, 0X1399, 0X6726, 0X76AF, 0X4434, 0X55BD,
    0XAD4A, 0XBCC3, 0X8E58, 0X9FD1, 0XEB6E, 0XFAE7, 0XC87C, 0XD9F5,
    0X3183, 0X200A, 0X1291, 0X0318, 0X77A7, 0X662E, 0X54B5, 0X453C,
    0XBDCB, 0XAC42, 0X9ED9, 0X8F50, 0XFBEF, 0XEA66, 0XD8FD, 0XC974,
    0X4204, 0X538D, 0X6116, 0X709F, 0X0420, 0X15A9, 0X2732, 0X36BB,
    0XCE4C, 0XDFC5, 0XED5E, 0XFCD7, 0X8868, 0X99E1, 0XAB7A, 0XBAF3,
    0X5285, 0X430C, 0X7197, 0X601E, 0X14A1, 0X0528, 0X37B3, 0X263A,
    0XDECD, 0XCF44, 0XFDDF, 0XEC56, 0X98E9, 0X8960, 0XBBFB, 0XAA72,
    0X6306, 0X728F, 0X4014, 0X519D, 0X2522, 0X34AB, 0X0630, 0X17B9,
    0XEF4E, 0XFEC7, 0XCC5C, 0XDDD5, 0XA96A, 0XB8E3, 0X8A78, 0X9BF1,
    0X7387, 0X620E, 0X5095, 0X411C, 0X35A3, 0X242A, 0X16B1, 0X0738,
    0XFFCF, 0XEE46, 0XDCDD, 0XCD54, 0XB9EB, 0XA862, 0X9AF9, 0X8B70,
    0X8408, 0X9581, 0XA71A, 0XB693, 0XC22C, 0XD3A5, 0XE13E, 0XF0B7,
    0X0840, 0X19C9, 0X2B52, 0X3ADB, 0X4E64, 0X5FED, 0X6D76, 0X7CFF,
    0X9489, 0X8500, 0XB79B, 0XA612, 0XD2AD, 0XC324, 0XF1BF, 0XE036,
    0X18C1, 0X0948, 0X3BD3, 0X2A5A, 0X5EE5, 0X4F6C, 0X7DF7, 0X6C7E,
    0XA50A, 0XB483, 0X8618, 0X9791, 0XE32E, 0XF2A7, 0XC03C, 0XD1B5,
    0X2942, 0X38CB, 0X0A50, 0X1BD9, 0X6F66, 0X7EEF, 0X4C74, 0X5DFD,
    0XB58B, 0XA402, 0X9699, 0X8710, 0XF3AF, 0XE226, 0XD0BD, 0XC134,
    0X39C3, 0X284A, 0X1AD1, 0X0B58, 0X7FE7, 0X6E6E, 0X5CF5, 0X4D7C,
    0XC60C, 0XD785, 0XE51E, 0XF497, 0X8028, 0X91A1, 0XA33A, 0XB2B3,
    0X4A44, 0X5BCD, 0X6956, 0X78DF, 0X0C60, 0X1DE9, 0X2F72, 0X3EFB,
    0XD68D, 0XC704, 0XF59F, 0XE416, 0X90A9, 0X8120, 0XB3BB, 0XA232,
    0X5AC5, 0X4B4C, 0X79D7, 0X685E, 0X1CE1, 0X0D68, 0X3FF3, 0X2E7A,
    0XE70E, 0XF687, 0XC41C, 0XD595, 0XA12A, 0XB0A3, 0X8238, 0X93B1,
    0X6B46, 0X7ACF, 0X4854, 0X59DD, 0X2D62, 0X3CEB, 0X0E70, 0X1FF9,
    0XF78F, 0XE606, 0XD49D, 0XC514, 0XB1AB, 0XA022, 0X92B9, 0X8330,
    0X7BC7, 0X6A4E, 0X58D5, 0X495C, 0X3DE3, 0X2C6A, 0X1EF1, 0X0F78,
};

// calculate the 16-bit CRC of data with predetermined length.
U16 GetCrc16(const U8* pData, int nLength)
{
    U16 fcs = 0xffff; // initialization
    while(nLength>0){
        fcs = (fcs >> 8) ^ crctab16[(fcs ^ *pData) & 0xff];
        nLength--;
        pData++;
    }
    return   ~fcs;              //    negated
}
```

2. Voltage-Battery Correspondence of Heartbeat Packet

Battery Percentage	Voltage
100%	4.16
95%	4.11
90%	4.08
85%	4.04
80%	4.01
75%	3.98
70%	3.95
65%	3.92
60%	3.88
55%	3.85
50%	3.82
45%	3.79
40%	3.76
35%	3.72
30%	3.69
25%	3.66
20%	3.63
15%	3.60
10%	3.56
5%	3.53
0%	3.50