

TWIG GPRS Protocol
for TWIG GSM/GPS products

Version 2.1
Licensed to: Twig Com Ltd.



Copyright © Twig Com Ltd.
All rights reserved
Version 2.1
Rev. January 26, 2011

LIMITED LICENSE AGREEMENT

Licensee:

Licensee contact person:

The licensor, Twig Com Ltd., Meriniitynkatu 11, FIN-24101 Salo, Finland ("Twig Com"), hereby grants the licensee a limited license to use this TWIG GPRS Protocol ("Document") solely for the Purpose of integrating TWIG devices by Twig Com to third party software. Any other use is expressly prohibited.

By accepting or using any part of this Document the Licensee agrees to the terms of this Limited License Agreement.

COPYRIGHTS AND OTHER IPR RETAINED

All copyrights and other intellectual property rights in this TWIG GPRS Protocol are and remain sole property of Twig Com.

This Document is for information only and no right to use it is hereby given unless it is licensed version and user is a licensee.

NON-DISCLOSURE

The licensee shall not disclose any part of this Document to its personnel or third parties without a need to know for implementation of Purpose. The licensee shall require from third parties with need to know a reasonable standard of non-disclosure and protection of Twig Com IPRs and no less stringent than it is applying itself. Any copies of Document not needed for Purpose shall be promptly destroyed.

LIMITATION OF LIABILITY

TWIG GPRS Protocol is distributed "as is" and the user will assume full responsibility for determining the suitability of the license for any particular purpose and for desired results. The Document may be inaccurate or incomplete.

In no event shall Twig Com be liable for any special, incidental or consequential damages, or commercial losses from any cause including but not limited to, loss of profit or revenues, whether or not Twig Com has received notice of a possibility or certainty of such damage or losses, caused by use of or operation with TWIG GPRS Protocol.

DAMAGES

Twig Com reserves the right to demand license fees and/or damages in case this Document is used unrightfully.

MORE INFORMATION

Please contact Twig Com Sales Office sales@twigworld.com, or Technical Support support@twigworld.com, or phone +358 40 5105058.

Twig Com reserves full rights to make any changes to Document without prior notice.

TABLE OF CONTENTS

1.	INTRODUCTION.....	5
1.1.	Scope	5
1.2.	TWIG MPTP Protocol.....	5
1.3.	Preparing TWIG mobile devices for GPRS	5
1.4.	AGPS.....	5
1.5.	For further information.....	5
1.6.	References	6
2.	OVERVIEW OF THE SYSTEM.....	7
3.	TWIG GPRS COMMUNICATION BASICS.....	8
3.1.	Network layer	8
3.2.	Transport layer	8
3.3.	Data encapsulation layer	8
3.4.	Data content layer	8
4.	CONNECTION MODES.....	9
5.	MESSAGE FORMAT	10
5.1.	Server To Device.....	10
5.2.	Device To Server.....	10
6.	ENCAPSULATION FIELD DEFINITIONS	11
6.1.	Protocol Header	11
6.2.	Code key	11
6.3.	GPRS User Device ID.....	11
6.4.	GPRS Fixed Device ID.....	11
6.5.	MPTP marker	12
6.6.	MPTP Command.....	12
6.7.	Termination code	12
6.8.	Checksum	12
6.9.	Complete message	13
6.10.	Messages from Server.....	13
7.	TRANSMIT-RECEIVE BEHAVIOUR	14
7.1.	Message Sequence	14
7.2.	Communication error.....	14
8.	COMMUNICATION EXAMPLES	15

8.1.	Simple example.....	15
8.2.	Advanced example.....	15
8.3.	Heartbeat.....	15
8.4.	Reconnect	15
9.	QUESTIONS AND ANSWERS	17

1. INTRODUCTION

1.1. Scope

The document describes the protocol used by TWIG GPRS devices to control GPRS connections and to encapsulate MPTP messages. Code library of TWIG GPRS Protocol implementation is available from Twig Com.

1.2. TWIG MPTP Protocol

TWIG MPTP (Mobile Phone Telematics Protocol) is a proprietary protocol of Twig Com Ltd. It is a key for building professional and consumer mobile telematics solutions in GSM networks. MPTP provides sophisticated telematics commands for service integrators and providers to build and provide various applications utilising location information.

MPTP enables, for example, the sending of location, tracking and alert messages between service centers and Twig Com MPTP enabled terminals. It uses SMS or GPRS as bearer, and is convenient to implement in service centers.

1.3. Preparing TWIG mobile devices for GPRS

- Specify option SW3008 GPRS Customer Gateway when ordering (also field upgradable)
- Program your mobile operator's GPRS parameters in the device: IP, port, APN etc
- Program GPRS on and select connection preferences

1.4. AGPS

GPS assistance data (AGPS) can be transmitted over TWIG GPRS Protocol to the following devices: TWIG Protector, TWIG Protector Ex, TWIG Protector Easy, TWIG DogLocator.

AGPS can in some cases speed up first GPS acquisition when several hours have elapsed from previous acquisition.

AGPS requires the Central Station to implement an AGPS gateway and to connect with TWIG AGPS server feed. Code library of TWIG AGPS Gateway is available from Twig Com.

1.5. For further information

<http://www.twigworld.com>

support@twigworld.com

1.6. References

This document references the following resources:

1. [TWIG MPTP Protocol specification version 3.17](#)
2. [TWIG Configurator PC applications](#) (one each for TWIG Protector product range, TWIG Locator product range and TWIG Discovery Pro)
3. [TWIG device configuration guides](#)
4. [TWIG GPRS Interface Module](#) (code library of TWIG GPRS Protocol and AGPS implementation)
5. [TWIG GPRS Interface Module API and Installation Guide](#)

2. OVERVIEW OF THE SYSTEM

TWIG devices communicate with Central Station using MPTP text strings (see TWIG MPTP Protocol specification). The Central Station is expected to have a MPTP parser module, which can transmit and receive message strings to and from TWIG mobile devices in MPTP format.

Simplest way is to send and receive MPTP strings as SMS messages. The phone number (MSISDN) of the Mobile Station (TWIG device + SIM card) is used for addressing, identification and authentication. The Central Station transmits and receives SMS messages either through a SMS modem or through a connection to Mobile Operator's SMS gateway.

When MPTP messages are transferred over GPRS bearer, TWIG devices add a layer of GPRS encapsulation information in the MPTP text string, resulting in GPRS text string.

For GPRS communication, the Central Station should implement the TWIG devices specific GPRS controls ("TWIG GPRS Protocol"):

- Abstraction of device identity. Mobile Station's phone number (MSISDN) or IMEI or another appropriate identity can be used as permanent device identity.
- Transmission acknowledgements
- GPRS connection control
- Queuing of mobile terminated (MT) messages: GPRS connection can be opened only by the Mobile Station. Mobile terminated (MT) messages thus have to be queued at the Central Station, until a GPRS connection is opened by the Mobile Station.

Central Station is also expected to implement generic GPRS connection functions:

- TCP connections management, including a connection identifier
- A fixed IP address and port for TCP access from the Mobile Operator's GPRS gateway
- Manage connection identifiers, to disambiguate between devices having connections open at the same time.

Example code for implementing the TWIG GPRS Protocol at Central Station is available from Twig Com ("TWIG GPRS Interface").

3. TWIG GPRS COMMUNICATION BASICS

GPRS communication can be divided into four layers. They and their respective protocols are:

Layer:	Protocol:
Data content layer	TWIG MPTP protocol
Data encapsulation layer	TWIG GPRS Protocol
Transport layer	TCP
Network layer	IP

3.1. Network layer

The network layer can also be called the addressing layer. The Internet Protocol (IP) is used in this layer.

The Central Station must have a fixed IP address and port number, and these are programmed in the mobile device using the Configurator application, or by sending a configuration MPTP message over SMS.

IP address is given in standard format Ipv4. Port number can be 0-65535.

IP address of the mobile device is dynamically given from the GSM/GPRS network.

3.2. Transport layer

Messages are send over GPRS using TCP.

3.3. Data encapsulation layer

The MPTP data is encapsulated in GPRS control fields.

3.4. Data content layer

The content of the data content layer shall be the same commands and information that is specified in the TWIG MPTP protocol. This protocol is identical for SMS and GPRS bearers.

4. CONNECTION MODES

GPRS connection strategy is controlled by the device GPRS parameters. These can be programmed either using the TWIG Configurator PC application, or over the air by sending MPTP configuration messages over SMS:

Connection mode (TWIG Protector Configurator parameter #20)

- Always: GPRS connection is always on
- Only reconnect: GPRS connection is always disconnected after transfer of pending messages. Connection is reopened when time [reconnect interval] (TWIG Protector Configurator #21) has elapsed since last connection.
- When in charger: connection always on when in charger, and reconnect when battery powered

Reconnect interval (TWIG Protector Configurator #21):

- Shorter time gives faster average delivery time for mobile terminated (MT) messages. Longer time gives better battery life and less data cost.

International roaming block (TWIG Protector Configurator #23):

- Allow GPRS connections only when mobile device is in its home network. International GPRS roaming is usually charged per kB and can be outrageously expensive, compared to domestic flat data rates.
- Care should be taken to control data cost when roaming.

GPRS Backup SMS Service Number (TWIG Protector Configurator #19)

- When GPRS Backup SMS is activated, then if GPRS connection for any reason cannot be made, MPTP is transmitted over SMS instead.
- Care should be taken to activate, since very high SMS costs can result.

5. MESSAGE FORMAT

5.1. Server To Device

Messages are ASCII with fields delimited by commas. They have the following format:

```
<ProtocolHeader>,0000,#<MPTP Command>#,<Termination Code>,<Checksum>
```

For example:

```
BENR,0000,#?LOC#,1000,nnn
```

5.2. Device To Server

Messages are ASCII with fields delimited by commas (please note when parsing that position MPTP messages have commas in them too). They have the following format:

```
<ProtocolHeader>,0000,<GPRS User Device Id>,<GPRS Fixed Device Id>,#<MPTP Command>#,<Termination Code>,<Checksum>
```

For example:

```
BENR,0000,+358401234567,12345678,#!TRG_01/01_7_1_norm_100%_gps_1_N60.17.26,4_E  
023.12.42,3_23.11.2007_17:51:03_000km/h_000deg_1096/0#,0011,nnn
```

This shows a tracking message from a device configured as GPRS User Device Id +3584012345678.

6. ENCAPSULATION FIELD DEFINITIONS

The GPRS message consists of the following fields:

- Header
- Code key
- User ID
- Fixed ID
- MPTP marker
- MPTP message
- MPTP marker
- Termination code
- Checksum

Each field is described in more detail below.

Fields are comma separated (.). Any field can be left empty, but the comma character must always be included.

6.1. Protocol Header

Letters "BENR" are used. The purpose is for the server to be able to identify and support different protocols.

6.2. Code key

A code key consisting of 4 digits "0000".

6.3. GPRS User Device ID

The default GPRS User Device ID is the international format telephone number related to the SIM card in the terminal. Also other systems resulting in unique ID can be used in the server.

The GPRS User Device ID must be programmed in the mobile terminal. E.g. in TWIG Protector Configurator, this is GPRS parameter #11.

6.4. GPRS Fixed Device ID

Every GSM device has a unique IMEI code. The last 8 digits from the IMEI code are used as GPRS Fixed Device ID.

6.5. MPTP marker

Since comma character is used as GPRS encapsulation field separator, and there is a chance that a MPTP message can contain comma character, the beginning and end of the MPTP message is marked with a “#”.

6.6. MPTP Command

This is a standard TWIG MPTP command surrounded by the “#” characters. Please note in parsing that if a Latitude and Longitude is present they will have commas as the decimal point of the Seconds part.

See the TWIG MPTP Protocol specification document for details of MPTP messages.

6.7. Termination code

All messages shall include a termination code. There are two main sets of termination codes, termination code inside a “standard” message, and termination code inside a response message.

Four digits are used as termination code:

Code	Explanation
Standard messages	
0000	End of this message. Communication line will be terminated. No response message is expected.
0001	End of this message. Communication line will be terminated after receiving correct response message.
0010	End of this message. Communication line will not be terminated. No response message is expected.
0011	End of this message. Communication line will not be terminated after receiving correct response message.
Response messages	
1000	Messages received without any problem.
1001	Incorrect message received.
1100	Messages received without any problem. Keep line open because I would like to transmit a new message soon.

6.8. Checksum

Standard 8 bit checksum, discard overflow, is used. All characters including separator character shall be included in the check sum calculation. Calculation shall be done on hex values, but included in the message with ASCII character.

Some device types may not transmit checksum, in which case this field is set to “nnn”. If checksum is used the algorithm is:

```
private int Checksum(string message)
{
    int iSum = 0;

    for (int i = 0; i < message.Length; i++)
    {
```

```
        byte ord = Convert.ToByte(message[i]);  
        iSum += ord;  
    }  
  
    int digit1 = iSum & 0xFF;  
    return digit1;  
}
```

Example:

Checksum on BENR =

BENR = 0x42 + 0x45 + 0x4E + 0x52 = 0x127

From 0x127 only last 8 bit is used = 0x27 = 39

39 is written in the message in 3 ASCII decimal digit(0x30 0x32 0x37) 039

6.9. Complete message

Here is an example given for a complete message

```
BENR,0000,+358401234567,#!LOC_01/01_norm_100%_gps_1_N 60.17.38,6  
E023.11.27,2_19.03.2010_21:43:17_021km/h_317deg_#,0000,nnn
```

6.10. Messages from Server

A message from a server is similar to a message from a terminal, but there is no ID included in the message.

Included fields are:

- Header
- Code key
- MPTP marker
- Termination code
- Checksum

7. TRANSMIT-RECEIVE BEHAVIOUR

All GPRS communication shall be initiated by the terminal. When there is an open TCP session both server and terminal can send messages.

When the server or the terminal has received a message, it shall send a response message.

7.1. Message Sequence

The Device will connect to the Server over TCP and usually send an empty or "Connect" message.

e.g. From Device: BENR,0000,+358401234567,12345678,##,0001,254

The server should respond with either an "Ack" which is an empty data message with a Termination Code of 1000.

e.g. From Server: BENR,0000,##,1000,158

OR

with an "MPTP Command Message" if there is one ready to send. The termination code should be 1000 if there is only one message to send, or 1100 if there is another message to follow.

e.g. From Server: BENR,0000,#?TRG_7_1_2#,1000,129

The device should respond with an "Ack"

e.g. From Device: BENR,0000,+358401234567,12345678,##,1100,047

Once this "Ack" is received, if there was another message to send it should be sent now.

Once the device connected, the device may send other messages such as tracking messages, the server will respond as above with an "Ack" or an "MPTP Command Message"

e.g. From Device:

BENR,0000,+358401234567,12345678,#!TRG_01/01_7_1_norm_060%_gps_1_N61.07.23,6_E022.49.36,2_24.03.2010_09:38:26_083km/h_228deg_81/0000#,0011,064

7.2. Communication error

There are a few potential problems that can occur during the GPRS session. The transmitting part (server or terminal) shall always be responsible for correct transmission.

This means if for instance the terminal transmits a message to the server, and doesn't get a response message from the server, the terminal is responsible for doing re-transmission (if wanted).

8. COMMUNICATION EXAMPLES

8.1. Simple example

From terminal:
BENR,0000,+358401234567,12345678,#!LOC_01/01_norm_100%_gps_1_N60.12.34,1_
E023.19.26,9_11.07.2010_12:39:07_012km/h_345deg_#,0001,nnn

From server:
BENR,0000,##,1100,nnn
or
BENR,0000,##,1100,159

8.2. Advanced example

From terminal:
BENR,0000,+358401234567,12345678,#!LOC_01/01_norm_100%_gps_1_N60.28.47,7_
E024.51.12,4_03.12.2010_23:58:51_047km/h_2083deg_#,0001,nnn

From server:
BENR,0000,##,1000,nnn
or
BENR,0000,##,1000,158

From terminal:
BENR,0000,+358401234567,12345678,##,0010,nnn

From server:
BENR,0000,#!CNF_01/01_0044_5_3_+3581234567890_1_+3581234567892_1#,0011,nnn

From terminal:
BENR,0000,+358401234567,12345678,##,1000,nnn

8.3. Heartbeat

Heartbeats are sent as an empty message. Its are sent after max 10mins from last communication.

From terminal:
BENR,0000,+358401234567,12345678,##,0011,nnn

From server:
BENR,0000,##,1000,nnn
or
BENR,0000,##,1000,158

8.4. Reconnect

Reconnects are sent as an empty message. It is sent when terminal reconnects GPRS.

From terminal:
BENR,0000,+358401234567,12345678,##,0011,169

From server:
BENR,0000,##,1000,158

9. QUESTIONS AND ANSWERS

Q: Cannot get GPRS connection. What is wrong?

A: Please check that the mobile operator's APN, DNS1, DNS2, username and password settings (TWIG Protector Configurator #12, #15, #16, #17 and #18) are correct. You can get the settings from your mobile operator. For many operators, only APN needs to be defined and other parameters can be left blank.

A: Also check that GPRS connection instead of SMS is selected (TWIG Protector configurator #22).

Q: I replaced the GPRS access point IP address and port by that of our server's (TWIG Protector Configurator settings #14 and #13). But no data is sent by the device. What is wrong?

Inverted G symbol appears on display, so GPRS connection is on. After powering off and on, the IP setting is changed back to default TWIG IP (192.83.5.99).

A: Please check that your devices were purchased with custom IP address option (e.g. TWIG Protector: sales code SW3008). You can also field upgrade a device with custom IP address option, by using the HW Tool PC application to program in the license key.

Q: Why does my TWIG device send location updates to server always with SMS? I have selected GPRS connection and it works.

A: When you send ?LOC or ?TRG commands to a TWIG device over SMS or GPRS, it responds in kind. So to activate e.g. GPRS tracking, please send ?TRG command with GPRS!

Q: Why does my TWIG device sometimes send location updates to server with SMS? I have selected GPRS connection and it works.

A: Have you enabled SMS backup for GPRS connections? If SMS backup (TWIG Protector Configurator #19) is enabled, then messages are sent using SMS if GPRS connection for some reason is not available.

Q: Can I use phone number (MSISDN) to identify and address the mobile devices in my tracking application?

Q: Can I use the IMEI number to identify and address the mobile devices in my tracking application?

A: Yes, it's ok to identify and address mobiles by IMEI, or MSISDN, or any other unique identifier.

TWIG GPRS air protocol has two identifiers for mobile station:

- GPRSDeviceFixedID: 8 last digits of the device IMEI. Read automatically from the device.
- GPRSDeviceUserID: Unique identifier programmed to the device by system administrator (TWIG Protector Configurator #11). Typically this is the MSISDN, but it could be also the IMEI, or another unique identifier, or it could be blank.

Q: How should my host application's outgoing GPRS messages queue work?

A: Twig GPRS protocol is now designed so that every mobile terminated (MT) message is acknowledged by the mobile before next one is sent by server. As an example the host application has a message '?LOC' to send. Device makes GPRS connection and the message is sent. Host application waits for the acknowledgement. When it gets it, it can send another message in the queue if there is one and so on.

Q: Can I send several messages to the mobile? Can the GPRS queue be several messages long?

A: Yes, it is ok to have more than 1 pending message. One message at a time is sent from the queue, and then system waits for response from the mobile, and then next message is sent and so on. The GPRS queue shall be implemented in the host application.

Q: How can I control GPRS connections?

A: GPRS connection strategy is controlled by the device GPRS parameters:

- Connection mode (TWIG Protector Configurator #20)
 - Always: GPRS connection is always on
 - Only reconnect: GPRS connection is always disconnected after transfer of pending messages. Connection is reopened when time [reconnect interval] (TWIG Protector Configurator #21) has elapsed since last connection.
 - When in charger: connection always on when in charger, and reconnect when battery powered
- Reconnect interval (TWIG Protector Configurator #21): Shorter time gives faster average delivery time for mobile terminated (MT) messages. Longer time gives better battery life and less data cost.
- International roaming block (TWIG Protector Configurator #23): Allow GPRS connections only when mobile device is in its home network. International GPRS roaming is usually charged per kB and can

be outrageously expensive, compared to domestic flat data rates. Care should be taken to control data cost when roaming.

Q: What happens if at the moment of alert there is no GPRS connection?

A: Whenever the mobile device has information to send to server, the device tries to open GPRS connection.

Q: What happens if no GPRS connection can be made?

A: If no GPRS connection with server can be established, the TWIG device will make a new attempt after reconnect interval time (TWIG Protector Configurator #21).

If GPRS SMS backup (TWIG Protector Configurator #19) is enabled, then the device will send SMS if GPRS connection is not available.

TWIG Protector and TWIG Discovery Pro always send emergency messages using SMS.

Q: Are messages that cannot be sent now sent later? Does the the Twig Protector have a memory that saves messages not sent?

A: TWIG devices generally do not store messages. If a message cannot be transmitted to server, it will be discarded.

TWIG Protector and TWIG Discovery Pro always send emergency messages using SMS. For emergency messages, several parallel SMS numbers can be specified.

Some TWIG devices can store location history in the device.