Abstract

This document describes the protocol used by the positioning functions of the wireless platform and their interaction with the CellLocate Service. The protocol supports both GNSS assistance provision and position estimation from GSM, UTRAN and CDMA cell observations.

INTERNAL USE ONLY

www.u-blox.com

Document Information	
Title	STYLEREF
Document type	
Document number	UBX-13000213
Document status	Preliminary UBX_DOCSTATUS="Preliminary" "This document contains preliminary data, revised and supplementary data may be published later." ""

Contents

1 Introduction

☞ An index finger points out key information pertaining to integration and performance.

⚠ **A warning symbol indicates actions that could negatively impact performance or damage the device.**

1.1 Background

The wireless modem supports 4 different types of GNSS aiding:

- Stand-alone
- AssistNow Online
- AssistNow Offline
- AssistNow Autonomous

The operation of these modes is described below [1].

Stand-alone aiding is where the wireless modem stores recent GNSS aiding information while the GNSS device is powered down. The information is obtained from the device prior to power-down and restored to the GNSS on power-up.

The AssistNow Offline service provides long-term almanac information over the network, and is intended for applications with extended offline status.

The AssistNow Online aiding requests the CellLocate Service to provide current GNSS satellite information to the device over the network. The information is valid for a period of a few hours. The CellLocate Service uses cellular data (GSM/UTRAN/CDMA) to provide a position estimate and to select the relevant subset of ephemeris information suitable for the device. The CellLocate Service is a useful service providing approximate position information for scenarios where the GNSS function is unable to operate, or even where there is no GNSS connected to the wireless module at all (although note that when no GNSS is connected the device will not contribute position information to the service, so no improvement in positioning performance over time will result).

The AssistNow Autonomous feature provides functionality similar to Assisted-GNSS (A-GNSS) without the need for a host and a connection. Based on a broadcast ephemeris downloaded from the satellite (or obtained by A-GNSS) the receiver can autonomously (i.e. without any host interaction or online connection) generate an accurate satellite orbit representation («AssistNow Autonomous data») that is usable for navigation much longer than the underlying broadcast ephemeris was intended for. It, therefore, renders the need to download or assist new ephemeris data for the first fix unnecessary for subsequent start-ups of the receiver.

This document describes the communications protocol for the CellLocate Service.

1.2 Aiding protocol for GNSS

Where the wireless module has an attached u-blox GNSS device, the protocol is used to obtain aiding information which the wireless module will forward to the GNSS device. If the GNSS device is subsequently able to obtain a position fix, this information is transmitted back to the CellLocate Service to associate the position with the previously transmitted cell information. In this way, the protocol supports the development of the cell location database to improve future positioning requests.

The aiding information provided attempts to account for the network latency. The initial aiding request message includes the expected round-trip latency. The aiding message is time stamped allowing for that latency and includes a timing accuracy set to half the latency setting. If the wireless module observes that the actual latency for the response to the request falls outside of the expected range, it may opt to repeat the request with a modified latency figure.

1.3 Location Estimation

Whether or not the wireless module has no attached u-blox GNSS device, or the device already has up-to-date aiding information, the protocol can be used to obtain a location estimate based on the observed cell information. The returned message is processed by the wireless module to present a location estimate to the user.

This mode of operation is a simplification of the GNSS-present case: it requires only the UBX message (UBX-MGA-INI), and communications latency does not need to be compensated. A position confirmation message is required only if there is a GNSS device present and produces a position fix after the request.

2 HTTP Protocol Definition

The preferred protocol for accessing CellLocate Service is HTTP. Upon reception of an HTTP request, the CellLocate Service will respond with the appropriate data, or an error string in text format. After delivery of all data, the server will terminate the connection.

2.1 Query String format

HTTP requests from the client to the server typically contain a standard HTTP query string in the request URL. The query string consists of a set of key=value parameters in the following form:

key=value;key=value;key=value;

The following rules apply:

- The order of parameters is not important.
- Keys and values are case sensitive
- Keys and values must be separated by an equals character ('=')
- Key/value pairs must be separated by semicolons (';')
- If a value contains a list, each item in the list must be separated by a comma (',')
- All numeric values must conform to the following regular expression: =^-?[0-9]+(\.[0-9]+)?$=

2.2 Authorization Tokens

Authorization tokens are used as a means of authorizing access to the u-blox services and for gathering anonymised statistics.

For internal use, u-blox employees each have an authorization token assigned to them (see here).

All external customers should use the following form to obtain a token: http://www.u-blox.com/services-form.html

2.3 Interfaces

CellLocate Service provides the following interfaces:

Pages	Description
\CellGetOnlineData.ashx	Get Online assistance (and/or CellLocate position estimate)
\CellSubmitPos.ashx	Submit position (and/or cell observations)
\CellGetOfflineData.ashx	Get Offline assistance

Note: The above will need to be prefixed with e.g. http://cell-live1.services.u-blox.com for the full URL.

2.3.1 CellGetOnlineData.ashx

The CellGetOnlineData.ashx interface is used to get a position estimate and/or assistance data from the CellLocate Service. The request must be made via an HTTP POST, with the GSMCLO binary message provided as the content of the POST.

2.3.1.1 Parameters

The following parameters are supported:

Key name	Unit /Range	Mandatory /Optional	Default	Valid values	Comment
token	String	Mandatory	n/a		The authorization token supplied by u-blox when a customer registers to use the service
celltype	String	Mandatory	n/a	gsm, cdma	The cellular device type
datatype	String	Optional	n/a	eph, alm, aux, pos	A comma separated list of the data types required by the client. Time data is always returned for each request (even if this parameter is not supplied).
format	String	Optional	mga	mga, aid	Specifies the format of the data returned mga = UBX-MGA-* (u-M8 onwards) aid = UBX-AID-* (u7 or earlier)
gnss	String	Optional	gps	gps, qzss, glo	A comma separated list of the GNSS for which data should be returned.
tacc	Numeric [seconds]	Optional	10	min: 0, max: 3600	The timing accuracy (see time parameters note below).
latency	Numeric [seconds]	Optional	0	min: 0, max: 3600	Typical latency between the time the server receives the request, and the time when the assistance data arrives at the GNSS receiver. The server can use this value to correct the time being transmitted to the client.

A position-only request can be made by setting the datatype=pos. While making a position-only request, the parameter gnss is invalid.

2.3.1.1.1 Position

If the datatype 'pos' is requested, the server will return the position and accuracy in the response data. When this data is supplied to the u-blox GNSS receiver, depending on the position accuracy estimated by the CellLocate Service, the receiver can then choose to select a better start-up strategy. For example, if the position accuracy result is 100km or better, the u-blox receiver might choose to go for a more optimistic start-up strategy. This will result in quicker start-up time. The receiver will decide which strategy to choose, depending on the accuracy of the estimated position.

The server determines the currently visible satellites at the user position, and only sends the ephemeris data of those satellites which should be in view at the location of the user. This reduces bandwidth requirements. In this case the accuracy of the estimated position is taken into account, meaning that the server will return all SVs visible in the given uncertainty region.

2.3.1.1.2 Time parameters (tacc and latency)

Time data is always returned with each request. The time data refers to the time at which the response leaves the server, corrected by an optional ‘latency’ value. This time data provided by the service is accurate to approximately 10ms but by default the time accuracy is indicated to be +/-10 seconds in order to account for network latency and any time between the client receiving the data and it being provided to the receiver.

If both the network latency and the client latency can safely be assumed to be very low (or are known), the client can choose to set the accuracy of the time message (tacc) to a much smaller value (e.g. 0.5s). This will result in a faster TTFF. The latency can also be adjusted as appropriate. However, these fields should be used with caution: if the time accuracy is not correct when the time data reaches the receiver, the receiver may experience prolonged or even failed start-ups.

Response

The response message from the Service based on the format requested is detailed below:

2.3.1

Format	Position available	Response
mga	Yes	If the CellLocate Service successfully calculates a position, then it will always respond with UBX-MGA-INI-TIME_UTC and UBX-MGA-INI-POS_LLH followed by aiding data if requested.
mga	No	If a position cannot be calculated by the service, then the response will not contain the UBX-MGA-INI-POS_LLH message. The service will respond with just the UBX-MGA-INI-TIME_UTC message followed by aiding data if requested.
aid	Yes	The CellLocate Service will always respond with UBX-AID-INI followed by aiding data if requested. If a position is successfully calculated, the 'pos' bitfield in the flags will be set to indicate that the position is valid.
aid	No	If a position cannot be calculated by the service, then the response will still contain the UBX-AID-INI message followed by aiding data if requested, but the 'pos' bitfield in the flags will be unset to indicate that the position is invalid.

Example

2.3.1.3

To request GPS and GLO data in UBX-MGA format:

```
/CellGetOnlineData.ashx?celltype=gsm;token=XXXXXXXXXXXXXXXXXXXXXX;datatype=pos,eph,alm,aux;filteronpos;format=mga;gnss=gps,glo;
```

To request GPS data in UBX-AID format:

```
/CellGetOnlineData.ashx?celltype=gsm;token=XXXXXXXXXXXXXXXXXXXXXX;datatype=pos,eph,alm,aux;filteronpos;format=aid;
```

To request position only in UBX-MGA format:

```
/CellGetOnlineData.ashx?celltype=gsm;token=XXXXXXXXXXXXXXXXXXXXXX;datatype=pos;format=mga;
```

To request position only in UBX-AID format:

```
/CellGetOnlineData.ashx?celltype=gsm;token=XXXXXXXXXXXXXXXXXXXXXX;datatype=pos;format=aid;
```

2.3.2.1

2.3.2 CellSubmitPos.ashx

The CellSubmitPos.ashx interface is used to submit a position to the CellLocate database. The request must be made via an HTTP POST, with the GSMCLL binary message provided as the content of the POST.

Parameters

The following parameters are supported:

Key name	Unit /Range	Mandatory /Optional	Default	Valid values	Comment
token	String	Mandatory	n/a		The authorization token supplied by u-blox when a customer registers to use the service
celltype	String	Mandatory	n/a	gsm, cdma	The cellular device type
datatype	String	Optional	n/a	eph, alm, aux, pos	A comma separated list of the data types required by the client. Time data is always returned for each request (even if this parameter is not supplied)

Response

There is no response message from this interface.

2.3.2.2 Example

```
/CellSubmitPos.ashx?token=XXXXXXXXXXXXXXXXXXXXXX;celltype=gsm
```

2.3.3 CellGetOfflineData.ashx

The CellGetOfflineData.ashx interface is used to provide offline assistance data.

2.3.3.1 Parameters

The following parameters are supported:

Key name	Unit /Range	Applies to	Mandatory /Optional	Default	Valid values	Comment
token	String		Mandatory	n/a		The authorization token supplied by u-blox when a customer registers to use the service
format	String	all requests	Optional	mga	mga, aid	Specifies the format of the data returned mga = UBX-MGA-* (u-M8 onwards) aid = UBX-AID-* (u7 or earlier)
gnss	String	mga only	Mandatory	n/a	gps, glo	A comma separated list of the GNSS for which data should be returned.
period	Numeric [weeks]	mga only	Optional	4	One of: 1,2,3,4 or 5	The number of weeks into the future the data should be valid for
2.3.3.2 resolution	Numeric [days]	mga only	Optional	1	One of: 1, 2 or 3	The resolution of the data: 1=every day, 2=every other day, 3=every third day
days	Numeric [days]	aid only	Optional	14	One of: 1,2,3,5,7,10 or 14	The number of days into the future the data should be valid for

Response

If MGA Data is requested the response data will be ordered on timestamp and then by GNSS. Hence, the response data will be ordered as follows.

```
04/09/2013 [GPS SV1, GPS SV2, GPS SV3....GPS SV32]
04/09/2013 [GLO SV1, GLO SV2, GLO SV3....GLO SV24]
```

```
05/09/2013 [GPS SV1, GPS SV2, GPS SV3....GPS SV32]
05/09/2013 [GLO SV1, GLO SV2, GLO SV3....GLO SV24]
.
.
.
09/10/2013 [GPS SV1, GPS SV2, GPS SV3....GPS SV32]
09/10/2013 [GLO SV1, GLO SV2, GLO SV3....GLO SV24]
```

Example

To request for latest data for GPS and GLONASS:

```
/GetOfflineData.ashx?token=XXXXXXXXXXXXXXXXXXXXXX;gnss=gps,glo;
```

2.4 Service Hostnames

The hostnames used to access the CellLocate Service are:

- cell-live1.services.u-blox.com
- cell-live2.services.u-blox.com

2.5 Dual endpoints

The most significant source of service downtime is due to problems affecting the physical platform and infrastructure on which a service is running. In order to address this, each service has two (or more) independent instances running, on separate platforms, provided by different hosting providers. Clients of the CellLocate Service should be configured with two different service addresses and if they cannot retrieve data from one of the endpoints, they should timeout quickly and then immediately try the other one.

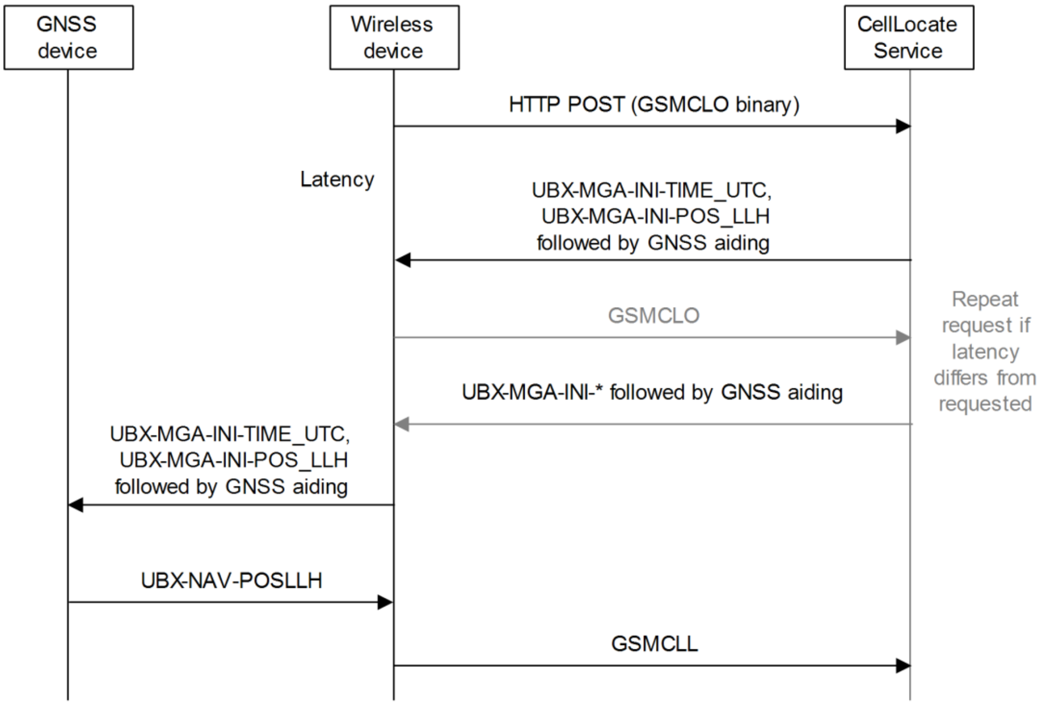
3 Binary Protocol Definition

3.1 Overview

The protocol consists of binary messages posted over an HTTP interface between the wireless module and the CellLocate Service. All actions are initiated from the wireless module, and messages are only sent from the service in response to request from the wireless module. All messages are encapsulated in single binary payload and sent to the CellLocate Service via an HTTP POST, with the binary message provided as the content of the POST. The device must respond accordingly in the event of connection failure, and the loss of one or more messages.

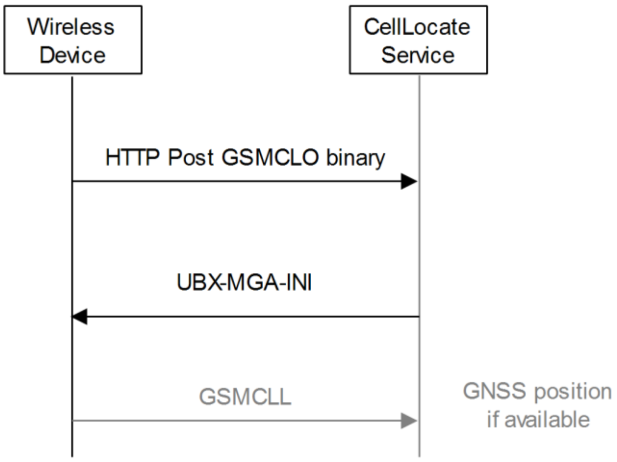
An example message sequence for the GNSS aiding case (UBX-MGA-* u-blox M8 onwards) together with a position estimate is shown below:

Protocol diagram for GNSS aiding


GNSS device
Wireless device
CellLocate Service
HTTP POST (GSMCLO binary)
Latency
UBX-MGA-INI-TIME_UTC, UBX-MGA-INI-POS_LLH followed by GNSS aiding
GSMCLO
Repeat request if latency differs from requested
UBX-MGA-INI-* followed by GNSS aiding
UBX-MGA-INI-TIME_UTC, UBX-MGA-INI-POS_LLH followed by GNSS aiding
UBX-NAV-POSLLH
GSMCLL

An example of a simpler, position estimation mode of operation is shown below:

Protocol diagram for position estimation



3.2 Wireless Module (Uplink) Message Format

All messages sent from the wireless module to the CellLocate Service have a common structure consisting of a Message Header followed by a variant sequence of Tag Structures:

Message Header
Tag Structure
Tag Structure
…
Null Tag

Multi-byte integer values are in little-endian order (i.e. least significant byte first). All fields are unsigned integers unless otherwise specified. Signed integers are in 2's complement format.

Each message along with all its tags is transmitted in a single binary packet.

3.2.1 Message Header Format

A Message Header consists of a 6 byte message identifier (whose first four bytes are the ASCII characters 'GSMC'), followed by an 8 byte device identifier, followed by individual message specific fields.

Offset	Field	Size	Value	Description
0	MessageID	6	ASCII chars	Message Identifier. 6 ASCII characters starting with 'GSMC'. The final 2 characters select the message type.
6	DeviceID	8	Any	Identifier for the originating device. Typically obtained by XOR combination of IMEI and IMSI identifiers.
7	Header fields	N	-	Header contents. Varies according to MessageID

Table 1: GSMCxx Header structure

3.2.2 Tag Structure Format

The Tag Structures start at the first byte after the Message Header.

The first byte of each Tag Structure is a Tag ID which identifies the Tag Structure. The most significant bit of the Tag ID indicates if the structure has a variable size, in which case the byte following the Tag ID is the length of the structure.

Offset	Field	Size	Value	Description
0	TagID	1	See below	Tag Identifier. 0 for message terminator. 1-127 for fixed length tag fields. 128-255 for variable-length tag fields.
[1	Length	1	N	Length field of following structure for variable length tag fields only.]
1 or 2	Fields	[N]	-	Tag contents. Varies according to tagID.

Table 2: GSMCxx tag structure

Tags are processed in transmission order. An unexpected Tag ID or an incomplete tag structure causes the service to discard the entire message.

GSMC messages shall be terminated either by a special Null Tag or the end of the UDP packet.

Offset	Field	Size	Value	Description
0	TagID	1	0	Null Tag Identifier. Terminates the message.

Table 3: Null Tag structure

Any GSMCxx message may include one or more padding tags, which carry no information:

Offset	Field	Size	Value	Description
0	TagID	1	128	Padding Tag Identifier.
1	Length	1	N	Length field of padding field
2	Padding	N	0	Padding bytes.

Table 4: Padding tag structure

3.2.3 Message Format with Encryption

If a message is encrypted, it will contain two parts – the Header and the Content, which will be encrypted using different keys.

The Header will consist of 14 bytes of binary payload consisting of the MessageID and the DeviceID. This will be encrypted using a Header Key.

The Content will comprise of the rest of the binary payload (i.e. excluding the MessageID and DeviceID). This will be encrypted using another chosen Content Key. In future, the Content Key may be device specific i.e. each device will have its own Content Key.

For now, only EncryptionID version E00 is defined and will encrypt both header and content using Authenticated Encryption with Associated Data (AEAD) with the Encrypt-then-MAC (EtM) approach. It will use the Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) with a 128 bit key. This cipher is usually referred to as AEAD_AES_128_GCM. Refer to https://tools.ietf.org/html/rfc5116 for more information.

AEAD is chosen as it simultaneously provides Confidentiality, Integrity and Authenticity assurances on the data.

- Confidentiality: provides assurance that only u-blox is able to understand (decipher) the data.
- Integrity: provides assurance of the accuracy and consistency of the data throughout its entire life-cycle.
- Authenticity: provides the assurance that the data has been created by u-blox and not modified by a MiM.

AEAD with Encrypt-then-MAC (EtM) is more secure than other options such as Encrypt-and-MAC (E&M)/ MAC-then-Encrypt (MtE).

GCM symmetric key cryptographic block ciphers have been widely adopted because of its efficiency and performance.

The procedure to encrypt the binary payload is described as follows:

1. Split the payload into Header and Content, with the first 14 bytes of the payload as Header and the rest as Content.

   Note: The Header includes the DeviceID and MessageID (14 bytes).
2. Encrypt the Header using AEAD with chosen ‘Cipher Algorithm’ and ‘Header Key’ where the EncryptionID is used as the Additional Data (AD).

   Note: The Cipher algorithm and Header Key are selected based on EncryptionID.

   For example: E00 uses AEAD_AES_128_GCM as its cipher mode. In this case, the size of the Encrypted Header will be 23 bytes (3 bytes EncryptionID + 14 bytes Header + 2 bytes Nonce + 4 bytes MAC).
3. Encrypt the Content using AEAD with chosen ‘Cipher Algorithm’ and ‘Content Key’ where the ‘Encrypted Header’ calculated in Step 2 is used as the Additional Data (AD).

   Note: The Cipher algorithm and Content Key are selected based on EncryptionID. For different EncryptionIDs, the cipher mode and keys can vary.

   For example: E00 uses AES_128_GCM as its cipher mode. In this case, the EncryptionID E00 uses AEAD_AES_128_GCM cipher. The Encrypted Header (23 bytes inclusive of EncryptionID) calculated above will be used as Additional. For a binary payload of size N, the encrypted binary size will be N + 15 bytes (3 bytes EncryptionID + 2 bytes Nonce * 2 + 4 bytes MAC * 2).

Offset	Field	Size	Value	Description
0	EncryptionID	3	E[00-99]	Encryption Identifier. 3 ASCII characters starting with E followed by version number [00-99].
3	Encrypted Header	N	Any	Encrypted value of the header.
3+N	Encrypted Content	N	Any	Encrypted value of the content.

Table 5: Encrypted GSMCxx Message structure

3.3 Available Messages (for Uplink)

This section of the specification defines the available messages along with the Message Header format for each message sent by the device to the CellLocate Service.

3.3.1 GSMCEL Message (Ephemeris and Location request message)

The GSMCEL message is used to request both GNSS aiding data and a location estimate from the CellLocate service. This message is sent along with appropriate tags that supply information to the CellLocate service about the wireless networks that can be observed, and the CellLocate service uses this information in order to estimate a location.

On receiving a GSMCEL message the CellLocate service will always respond with a response message using the (see Section **Error! Reference source not found. Error! Reference source not found.**) and will provide the following aiding data if the 'Multi GNSS Assistance Tag' is not set: a single UBX-AID-INI message which includes the location estimate, a single UBX-AID-HUI message and one UBX-AID-EPH message for each satellite currently in view of the estimated location or for every satellite if a location estimate could not be determined.

If the 'Multi GNSS Assistance Tag' is defined, then based on the GNSS[s] requested: a UBX-MGA-INI-TIME_UTC, UBX-MGA-INI-POS_LLH message which includes the location estimate, followed by assistance data for one or more GNSS is returned as shown below.

GPS - UBX-MGA-GPS-HEALTH, UBX-MGA-GPS-IONO, UBX-MGA-GPS-UTC, [UBX-MGA-GPS-EPH] x N

GLONASS - UBX-MGA-GLO-TIMEOFFSET, [UBX-MGA-GLO-EPH] x N

QZSS - UBX-MGA-QZSS-HEALTH, [UBX-MGA-QZSS-EPH] x N

The response could optionally contain some additional response message tags [2.4.2].

The GSMCEL Message Header is defined below:

Offset	Field	Size	Value	Description
0	MessageID	6	'GSMCEL'	Estimate Location Message Identifier
6	DeviceID	8	Any	Identifier for the originating device. Typically obtained by XOR combination of IMEI and IMSI identifiers.
14	Home PLMN	3	0- 0x999999	Home PLMN for the wireless module. Combines the MCC and MNC identifiers in a single 6 digit identifier. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The Home PLMN is the PLMN for following cell tags until a new PLMN tag occurs. If the MCC and MNC values are not known, then it should be set to 0-0. In case of CDMA, many serving networks broadcast a wildcard value of '1111111111' (decimal 1023) for MCC and wildcard value of '1111111' (decimal 127) for MNC (IMSI_11_12). In such cases, the MCC and MNC should be also be set to 0.
17	Latency	2		Latency of communication channel in milliseconds. The timestamp on the returned aiding message is adjusted by this value.

Table 6: GSMCEL (Ephemeris and Location Request) Message Header structure

3.3.2 GSMCLO message (Location Only request message)

The GSMCLO message is a variant of the GSMCEL message which is used to request a location estimate only, without GPS satellite aiding data. This may be used for devices with no GPS device available, when a GPS fix is not required, or when an update of the aiding data (i.e. current satellite ephemeris data) is not needed. Again this message is sent along with the appropriate tags to supply the network cell information currently detected by the wireless module.

On receiving a GSMCLO message the CellLocate service will always respond with a response message using the (see Section **Error! Reference source not found. Error! Reference source not found.**) and will provide the following aiding data if the 'Multi GNSS Assistance Tag' is not set: a single UBX-AID-INI message which includes the location estimate, a single UBX-AID-HUI message and one UBX-AID-EPH message for each satellite currently in view of the estimated location or for every satellite if a location estimate could not be determined.

If the 'Multi GNSS Assistance Tag' is defined, then based on the GNSS[s] requested: a UBX-MGA-INI-TIME_UTC, UBX-MGA-INI-POS_LLH message which includes the location estimate, followed by assistance data for one or more GNSS is returned as shown below.

GPS - UBX-MGA-GPS-HEALTH, UBX-MGA-GPS-IONO, UBX-MGA-GPS-UTC, [UBX-MGA-GPS-EPH] x N

GLONASS - UBX-MGA-GLO-TIMEOFFSET, [UBX-MGA-GLO-EPH] x N

QZSS - UBX-MGA-QZSS-HEALTH, [UBX-MGA-QZSS-EPH] x N

The GSMCLO Message Header is defined below:

Offset	Field	Size	Value	Description
0	MessageID	6	'GSMCLO'	Location Only Message Identifier
6	DeviceID	8	Any	Identifier for the originating device. Typically obtained by XOR combination of IMEI and IMSI identifiers.
14	Home PLMN	3	Any	Home PLMN for the wireless module. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The Home PLMN is the PLMN for following cell tags until a new PLMN tag occurs. If the MCC and MNC values are not known, then it should be set to 0-0. In case of CDMA, many serving networks broadcast a wildcard value of '1111111111' (decimal 1023) for MCC and wildcard value of '1111111' (decimal 127) for MNC (IMSI_11_12). In such cases, the MCC and MNC should be also be set to 0.

Table 7: GSMCLO Message Header structure

3.3.3 GSMCLL Message (GNSS fix message)

The GSMCLL message contains a GNSS fix obtained on the wireless module to be associated with previously transmitted cell information. The position is in WGS-84 geodetic co-ordinates. This message is used to provide contributions to the CellLocate database in latitude and longitude coordinates.

The CellLocate Service does not send any form of response to this message at all.

The CellLocate Service acts upon this message in two distinct ways and dependent on whether the message also includes any Cell Observation Tags or not, thus:

No Cell Observation Tags supplied with the GSMCLL Message

The CellLocate Service will find the last message received from the same device (i.e. with the same DeviceID as the one supplied in this message), and if that message is a GSMCLO message it will associate the position supplied in this message with the Cell Observations in the GSMCLO message and add them to the CellLocate database. If the previous message from the same device is not a GSMCLO, then the location provided in this message is discarded and not used.

Cell Observation Tags are supplied with the GSMCLL Message – "Harvesting Mode"

The CellLocate Service will associate the position and Cell Observations supplied in this message and add them to the CellLocate database.

The GSMCLL Message Header is defined below:

Offset	Field	Size	Value	Description
0	MessageID	6	'GSMCLL'	Latitude/Longitude Message Identifier
6	DeviceID	8	Any	Identifier for the originating device. Typically obtained by XOR combination of IMEI and IMSI identifiers.
14	Latitude	4	Any	Signed latitude coordinate in degree*1e-7.
18	Longitude	4	Any	Signed longitude coordinate in degree*1e-7.
22	Altitude	4	Any	Signed altitude coordinate in cm.
26	Accuracy	4	Any	Position accuracy in cm
30	TTF	4	Any	Time to fix in seconds.
34	NumSV	1	0-32	Number of satellites used in the position fix

Table 8: GSMCLL structure

3.3.4 Autonomous Solution

The device could optionally notify the CellLocate service, its previous solution with the corresponding uncertainty as part of any of the GSMCxx messages.

The autonomous solution structure can be constructed by combining the Version Tag (3.5.3.3), Position Tag (3.5.3.14), Uncertainty Tag (3.5.3.16) and Relative Time Tag (3.5.3.9). The Velocity Tag (3.5.3.10) can be optionally inserted.

3.4 Message structure for down-link

In response, all messages originating from the CellLocate service and sent to the device are packaged in an HTTP-like structure, with a text header identifying the content type and length. The content of a successful response is a sequence of UBX format messages. This format is described in detail in [1][2].

The UBX aiding messages (containing aiding position) are optionally followed by UBX-CEL-TUN which wraps the multiple positions & ellipsoidal uncertainties if requested.

The structure of the UBX responses is listed below:

3.4.1 Response Message Header

The text of the header for a successful response is:

```
u-blox a-gps server (c) 1997-2010 u-blox AG\r\n
Content-Length: %i\r\n
Content-Type: application/ubx\r\n
\r\n
```

Where '%i' is the decimal length of the content in bytes, '\r' is ASCII CR (value 0x0D), and '\n' is ASCII LF (value 0x0A). The header is terminated by an empty line.

The error response is distinguished from a successful response by content type. Error responses have no UBX content, but may have some (optionally empty) plain text error content. The first line of the response is not defined, but may take the form of a successful HTTP response in order to allow connectivity to the service to be checked simply by a web browser. The text of the header for an error response is:

```
HTTP/1.1 2c00 OK\r\n
Content-Length: %i\r\n
Content-Type: text/plain\r\n
\r\n
```

3.4.2 Response Message Tags

The response message Tags follow the UBX format messages as shown below.

- UBX-AID-INI/ UBX-MGA-INI - Contains GNSS Aiding messages
- [UBX-TUN-CEL] - Contains multiple positions and their ellipsoidal uncertainties in the format

  UBX-TUN-CEL**({**Position, Ellipsoidal Uncertainty 1 **[**, 2**]** **[**, Supplementary reverse geocode**]}}** x N**)** where the curly braces **{ }** denote that the fields are grouped.

  - At least one uncertainty ellipse has to be provided. The second ellipse is optional.
  - Only uncertainty ellipses with 50%(or 1sigma) or 95%(or 2 sigmas) confidence levels have to be provided.

Note: The square brackets [ ] denote that the response is optional. The curly braces { } denote that the fields are grouped.

The tags used for the Ellipsoidal uncertainty, the Position and the Reverse-geocode are defined in paragraphs (3.5.3.16), (3.5.3.14) and (3.5.3.18).

3.4.3 Version handling

The server will report different set of information to different firmware versions in order to maintain the compatibility with old devices.

If the up-link message from the device will not contain the Supplementary Position Request Tag (3.5.3.12), the modem will be considered by default of version 1 (legacy).

The following paragraphs contain the content of the down-link for different versions.

Version 1

This approach is the one used for legacy devices (Position Detail Request Tag not present).

The server sends to the devices a UBX-AID-INI/ UBX-MGA-INI-POS message containing the 1sigma confidence level uncertainty.

The module will extract the position from the UBX-AID-INI/ UBX-MGA-INI-POS message. The 1sigma confidence
3.4.3.1 will be reported to the user.

The module will then forward the aiding messages also to the GNSS device after correcting it for the network delays.

Version 2

Newer devices will always receive:

- One aiding message (UBX-AID-INI/ UBX-MGA-INI-POS) with 95% (2sigma) confidence level

3.4.3.2

- The UBX-TUN-CEL message with at least a solution in it.

The module will extract the position/positions from the UBX_TUN_CEL message.

The module will forward the aiding messages as they are to the GNSS device.

3.4.4 Encrypted Response Message

Only response messages received with content type "application/ubx" will have been encrypted.

If the response message is encrypted, it will consist of a prepended EncryptionID (E[00-99).

The binary response content will be encrypted using chosen Content Key. In future, the Content Key may be device specific i.e. each Device will have its own Content Key.

Offset	Field	Size	Value	Description
0	EncryptionID	3	E[00-99]	Encryption Identifier. 3 ASCII characters starting with E followed by version number [00-99].
3	Encrypted Binary Response	N	Any	Encrypted value of the binary response payload.

Table 9: Encrypted Response Message structure

Refer to section 3.2.3 Uplink Message Format with Encryption to learn more about the chosen/defined encryption algorithm and cipher.

The procedure to decrypt the binary payload is described as follows:

1. Decrypt the binary response payload using AEAD with chosen 'Cipher Algorithm' and 'Content Key' where the EncryptionID is used as the Additional Data (AD).

   Note: The Cipher algorithm and Content Key are selected based on EncryptionID. For different EncryptionIDs, the cipher mode and keys can vary.

   For example: E00 uses AEAD_AES_128_GCM as its cipher mode. In this case, the encrypted content can be decrypted using the Content Key with EncryptionID 'E00' as Additional Data (AD).

   For an E00 encrypted binary of size N, the decrypted message size should be N - 9(where 9 bytes consist of 3 bytes EncryptionID + 2 bytes Nonce + 4 bytes MAC).

3.5 Available Tags

Immediately following the Message Header, there may be a sequence of Tag Structures. The tags that may be supplied with each of the available messages are given along with the messages in section 3.3 (Available Messages) above. Typical examples of usage are illustrated in section 0.

3.5.1 Cell Observation Tags

The following section defines the Cell Observation tags which provide information relating to the 2G, 3G, LTE or CDMA cells that are currently observed or have been observed.

General

3.5.1.1.1 PLMN Tag

3.5.1.1 The PLMN tag is used to change the PLMN (MCC and MNC) used for subsequent Cell Observation Tags. Any number of PLMN Tags can be supplied e.g. in the case where cells from several different networks operators are observed. In the case of Message Headers that do not include a HomePLMN field, the PLMN tag must be used before any Cell Observation Tags are given.

Offset	Field	Size	Value	Description
0	TagID	1	3	PLMN Tag Identifier.
1	PLMN	3	0-0x999999	New PLMN. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The new PLMN is the PLMN for any following cell tags. If the MCC and MNC values are not known, then it should be set to 0-0. In case of CDMA, many serving networks broadcast a wildcard value of '1111111111' (decimal 1023) for MCC and wildcard value of '1111111' (decimal 127) for MNC (IMSI_11_12). In such cases, the MCC and MNC should be also be set as 0-0.

Table 10: PLMN Cell Tag

3.5.1.1.2 PLMN Shared Tag

The PLMN Shared tag is used to provide the list of extra-PLMNs (excluding the main PLMN already provided with PLMN Tag) that may be associated to a LTE cell. The number of PLMN is variable. The maximum number of shared PLMN allowed is 5.

Each PLMN shared tag contains the list of MNC for a single MCC. If more than one MCC is present, more PLMN shared tags should be used.

Offset	Field	Size	Value	Description
0	TagID	1	146	PLMN Tag Identifier.
1	Number of PLMNs	1	1-5	Number of PLMNs broadcast by the cell and present in PLMN Identity list.
2	MCC	2	0-0x0999	MCC forms the least significant digits.
4	MNC1	2	0-0x0999	The MNC forms the 2 or 3 least significant digits. The most significant digit is 0 if not used.
3.5.1.2 6	MNC2	2	0-0x0999	The MNC forms the 2 or 3 least significant digits. The most significant digit is 0 if not used.
…	…	…		
2+n*2	MNCn	2	0-0x0999	The MNC forms the 2 or 3 least significant digits. The most significant digit is 0 if not used.

Table 11: PLMN Shared Tag

2G

This section defines the tags used to provide information to the CellLocate Service about the 2G cells observed.

3.5.1.2.1 GSM Serving Cell Tag

This tag is used to supply the description of the 2G serving Cell. Note that if present only one such tag should be supplied with any message.

Offset	Field	Size	Value	Description
0	TagID	1	1	GSM Serving Cell Tag Identifier.
1	LAC	2	1-0xFFFD	Location Area Code. 0xFFFF if unknown.
3	CI	2	0-0xFFFF	Cell Identity. 0xFFFF if unknown.
5	Rx Level	1	0-63	RXLEV. Receiving level of the cell signal
6	BSIC	1	0-0x3F	Base Station Identity Code.
7	ARFCN	2	0-1023	Absolute Radio Frequency Channel Number
9	TA	1	0-63	Timing Advance
10	RAC	1	0-0xFF	Routing Area Code (set for GPRS connections; 0 if unused)

Table 12: GSM Serving Cell Tag

3.5.1.2.2 GSM Neighbouring Cell Tag

This tag is used to supply the 2G neighbouring cells observed by the device.

Where neighbouring cells are observed with different PLMN (MCC / MNC) to that in previous tags then the PLMN Tag is used to change this (for this cell and any subsequent cells).

Any number (zero or more) of these tags may be supplied as part of a message.

Offset	Field	Size	Value	Description
0	TagID	1	2	GSM Neighbouring Cell Tag Identifier.
1	LAC	2	1-0xFFFD	Location Area Code. 0xFFFF if unknown. (In 3G only known in Full Scan mode)
3	CI	2	0-0xFFFF	Cell Identity. 0xFFFF if unknown. (In 3G only known in Full Scan mode)
5	Rx Level	1	0-63	RXLEV. Receiving level of the cell signal
6	BSIC	1	0-0x3F	Base Station Identity Code.
7	ARFCN	2	0-1023	Absolute Radio Frequency Channel Number

Table 13: GSM Neighbouring Cell Tag

3G

This section defines the tags used to provide information to the CellLocate Service about the 3G cells observed.

3.5.1.3.1 UTRAN Serving Cell Tag (Radio IDLE)

This tag is used to supply the 3G serving Cell observed by the device when the wireless radio is in IDLE mode (note a separate tag is used when the radio is in connected mode since there is far less information about each cell available when connected).

3.5.1.3 Note that if present only one such tag should be supplied as part of any message.

Offset	Field	Size	Value	Description
0	TagID	1	4	UTRAN Serving Cell Tag Identifier
1	LAC	2	1-0xFFFD	Location Area Code. 0xFFFF if unknown.
3	CI	4	0-0x0FFFFFFF	Cell Identity. 0xFFFFFFFF if unknown
7	Rscp	1	0-91	1 byte unsigned integer giving Received Signal Code Power in dBm levels. 0XFF if not available
8	ScramblingCode	2	0-0x01FF	Scrambling code. 0xFFFF if not applicable
10	dlFrequency	2	0-0x3FFF	Download frequency. 0xFFFF if not applicable
12	RTT	2	768-1280	Round Trip Time in chips. 0xFFFF if invalid
14	RAC	1	0-0xFF	Routing Area Code (set for GPRS connections; 0 if unused)
15	ECN0	1	0-49	Energy per Chip / Noise in dB levels. 0xFF if not available
16	CPICH_tx_pow	1	-10 to +50 or +127	1 byte signed integer giving Pilot channel transmission power in dBm. +127 is invalid

Table 14: UTRAN Serving Cell Tag (Radio IDLE)

3.5.1.3.2 UTRAN Neighbouring Cell Tag (Radio IDLE)

This tag is used to supply the 3G neighbouring cells observed by the device when the wireless radio is in IDLE mode (note a separate tag is used when the radio is in connected mode since there is far less information about each cell available when connected).

Where neighbouring cells are observed with different PLMN (MCC / MNC) to that in previous tags then the PLMN Tag is used to change this (for this cell and any subsequent cells).

Notes:

- Even when the wireless radio is in IDLE mode certain fields are only valid if a Full Scan is performed.
- The tag is identical in structure to both the Last UTRAN Serving Cell Before Radio Connected Tag with just the tag number changing.
- Any number (zero or more) of these tags may be supplied as part of a message.

Offset	Field	Size	Value	Description
0	TagID	1	5	UTRAN Neighboring Cell Tag Identifier (Radio IDLE)
1	LAC	2	1-0xFFFD	Location Area Code, 0xFFFF if unknown ***(Only known in Full Scan mode)***
3	CI	4	0-0x0FFFFFFF	Cell Identity. 0xFFFFFFFF if unknown. ***(Only known in Full Scan mode)***
7	Rscp	1	0-91	1 byte unsigned integer giving Received Signal Code Power in dBm levels. 0XFF if not available
8	ScramblingCode	2	0-0x01FF	Scrambling code. 0xFFFF if not applicable
10	dlFrequency	2	0-0x3FFF	Download frequency. 0xFFFF if not applicable
12	RAC	1	0-0xFF	Routing Area Code (set for GPRS connections; 0 if unused or unknown) ***(Only known in Full Scan mode)***
13	ECN0	1	0-49	Energy per Chip / Noise in dB levels. 0xFF if not available

Table 15: UTRAN Neighbouring Cell Tag (Radio IDLE)

3.5.1.3.3 UTRAN Neighbouring Cell in Report Tag

This tag is used to supply the 3G neighbouring cells part of the report from the serving cell. This tag may be used both in IDLE and in CONNECTED mode.

Where neighbouring cells are observed with different PLMN (MCC / MNC) to that in previous tags then the PLMN Tag is used to change this (for this cell and any subsequent cells).

Notes:

- LAC, CI and RAC are not provided from the report of the serving cell, therefore the corresponding fields are generally empty. They may be known if the specific cell was observed also in the full scan
- Any number (zero or more) of these tags may be supplied as part of a message.

Offset	Field	Size	Value	Description
0	TagID	1	147	UTRAN Neighboring Cell Tag Identifier (Radio IDLE)
1	LAC	2	1-0xFFFD	Location Area Code, 0xFFFF if unknown ***(Only known if observed also in Full Scan)***
3	CI	4	0-0x0FFFFFFF	Cell Identity. 0xFFFFFFFF if unknown. ***(Only known if observed also in Full Scan)***
7	Rscp	1	0-91	1 byte unsigned integer giving Received Signal Code Power in dBm levels. 0XFF if not available
8	ScramblingCode	2	0-0x01FF	Scrambling code. 0xFFFF if not applicable
10	dlFrequency	2	0-0x3FFF	Download frequency. 0xFFFF if not applicable
12	RAC	1	0-0xFF	Routing Area Code (set for GPRS connections; 0 if unused or unknown) ***(Only known if observed also in Full Scan)***
13	ECN0	1	0-49	Energy per Chip / Noise in dB levels. 0xFF if not available

Table 16: UTRAN Neighbouring Cell in Report Tag

3.5.1.3.4 Last UTRAN Serving Cell Before Radio Connected Tag

This tag is used to supply the 3G serving Cell that was previously observed by the device immediately before the wireless radio went in to connected mode.

This tag is unusual to other tags in the respect that it gives information about a cell that was observed at some unspecified earlier point in time. The CellLocate Service will not directly link a subsequent GNSS fix (GSMCLL message) with this observations provided in this tag, it will be used however to assist in the location estimation.

Notes:

- The tag is identical in structure to both the UTRAN Neighbouring Cell Tag (Radio IDLE) with just the tag number changing.
- If present only one such tag should be supplied with any message.

Offset	Field	Size	Value	Description
0	TagID	1	6	Last UTRAN Serving Cell Before Radio Connected Tag Identifier
1	LAC	2	1-0xFFFD	Location Area Code. 0xFFFF if unknown.
3	CI	4	0-0x0FFFFFFF	Cell Identity. 0xFFFFFFFF if unknown
7	Rscp	1	0-91	1 byte unsigned integer giving Received Signal Code Power in dBm levels. 0XFF if not available
8	ScramblingCode	2	0-0x01FF	Scrambling code. 0xFFFF if not applicable
10	dlFrequency	2	0-0x3FFF	Download frequency. 0xFFFF if not applicable
12	RAC	1	0-0xFF	Routing Area Code (set for GPRS connections; 0 if unused)
13	ECN0	1	0-49	Energy per Chip / Noise in dB levels. 0xFF if not available

Table 17: Last UTRAN Serving Cell Before Radio Connected Tag

3.5.1.3.5 Last UTRAN Neighbouring Cell Before Radio Connected Tag

This tag is used to supply the 3G neighbouring cells that were previously observed by the device immediately before the wireless radio went in to connected mode.

This tag is unusual to other tags in the respect that it gives information about a cell that was observed at some unspecified earlier point in time. The CellLocate Service will not directly link a subsequent GNSS fix (GSMCLL message) with this observations provided in this tag, it will be used however to assist in the location estimation.

Where neighbouring cells were observed with different PLMN (MCC / MNC) to that in previous such tags then the PLMN Tag is used to change this (for this cell and any subsequent cells).

Notes:

- The tag is identical in structure to the UTRAN Connected Set Cell Tag with just the tag number changing.
- Any number (zero or more) of these tags may be supplied as part of a message.

Offset	Field	Size	Value	Description
0	TagID	1	7	Last UTRAN Neighbouring Cell Before Radio Connected Tag Identifier
1	ScramblingCode	2	0-0x01FF	Scrambling code. 0xFFFF if not applicable
3	dlFrequency	2	0-0x3FFF	Download frequency. 0xFFFF if not applicable

Table 18: Last UTRAN Neighbouring Cell Before Radio Connected Tag

3.5.1.3.6 UTRAN Connected Set Cell Tag (Radio CONNECTED)

This tag is used to supply the 3G cells (either neighbouring or serving) observed by the device when the wireless radio is in CONNECTED mode.

Where cells are observed with different PLMN (MCC / MNC) to that in previous tags then the PLMN Tag is used to change this (for this cell and any subsequent cells).

Notes:

- There is very limited information available on each cell when the wireless radio is in CONNECTED mode hence the tag only has a few fields.
- There is no distinction between the serving cell / neighbouring cell or whether the cell belongs to any of the cell sets maintained by the device, the tag is simply used to identify the cells which are currently detected / observed.
- Any number (zero or more) of these tags may be supplied as part of a message.

Offset	Field	Size	Value	Description
0	TagID	1	8	UTRAN Connected Set Cell Tag Identifier (Radio CONNECTED). This can belong to Active Set, Virtual Active Set, Monitored Set, Detected Set and 3G neighbours.
1	Rscp	1	0-91	1 byte unsigned integer giving Received Signal Code Power in dBm levels. 0XFF if not available
2	ScramblingCode	2	0-0x01FF	Scrambling code. 0xFFFF if not applicable
4	dlFrequency	2	0-0x3FFF	Download frequency. 0xFFFF if not applicable
6	ECN0	1	0-49	Energy per Chip / Noise in dB levels. 0xFF if not available

Table 19: UTRAN Connected Set Cell Tag (Radio CONNECTED)

3.5.1.3.7 Last GSM Neighbouring Cell Before Radio Connected Tag

This tag is used to supply the 2G neighbouring cells that were previously observed by the device immediately before the wireless radio went in to connected mode.

This tag is unusual to other tags in the respect that it gives information about a cell that was observed at some unspecified earlier point in time. The CellLocate Service will not directly link a subsequent GNSS fix (GSMCLL message) with this observations provided in this tag, it will be used however to assist in the location estimation.

Where neighbouring cells were observed with different PLMN (MCC / MNC) to that in previous such tags then the PLMN Tag is used to change this (for this cell and any subsequent cells).

Notes:

- Any number (zero or more) of these tags may be supplied as part of a message.

Offset	Field	Size	Value	Description
0	TagID	1	9	Last seen GSM Neighbouring Cell Tag Identifier.
1	BSIC	1	0-0x3F	Base Station Identity Code.
2	ARFCN	2	0-1023	Absolute Radio Frequency Channel Number

Table 20: Last GSM Neighbouring Cell Before Radio Connected Tag

CDMA

This section defines the tags used to provide information to the CellLocate Service about the CDMA Pilots observed.

3.5.1.4 3.5.1.4.1 CDMA Active Set Pilot Tag (Radio IDLE & CONNECTED)

This tag is used to supply the CDMA Pilot information for an Active set when device radio is in Idle or Connected mode.

Note that multiple tags could be supplied as a part of the message while a handoff is in progress.

Offset	Field	Size	Value	Description
0	TagID	1	10	CDMA Active Pilot Tag Identifier in IDLE or CONNECTED mode.
1	SID	2	0-0x7FFF	System Identifier. 0xFFFF if unknown
3	NID	2	0-0xFFFF	Network Identifier. 0xFFFF if unknown.
5	BSID	2	0-0xFFFF	Base Station Identifier. 0xFFFF if unknown.
7	LTMOffset	1	-95 to +95	Local Time Offset in units of 15 minutes. 0x7F if not available.
8	DaylightSaving	1	0 or 1	Daylight saving indicator. 1 if daylight savings is in effect else 0. 255 if not known. This field should also be ignored if LTM Offset is set to unknown (0xFF).
9	BSLatitude	4	Any	Signed latitude coordinate of Base Station in degree*1e-7. 0 if not known.
13	BSLongitude	4	Any	Signed latitude coordinate of Base Station in degree*1e-7. 0 if not known.
17	RoamState	1	0-2	The roaming state of the device. 0 – Home, 1 – Roam (same network) and 2- Roam (different network). 255 if not known.
18	RSSI	2	-50 to -130	The Received Signal Strength Indication in dBm for the active set of pilots. 255 if not known.
20	Channel	2	0-0x07FF	CDMA Channel Number. 0xFFFF if unknown.
22	BandClass	1	0-10	A numbering scheme for frequency channels. Example: Band Class 0 (800 MHz Band), Band Class 1 (1900 MHz Band), etc. 255 if not known.
23	PilotPN	2	0-0x01FF	The active pilot PN Offset (PN – Pseudo Noise) is short code sequences used to differentiate base stations. 0xFFFF if unknown.
25	EcIo	1	0-0x3F	The Ec/Io (in dB) which is the ratio of received pilot energy, Ec, to total received energy, Io per pilot. It is the highest energy of this pilot and is represented in 0.5dB steps from 0dB (value=0) to 31.5dB (value=63). 0XFF if not known.

Table 21: CDMA Active Set Pilot Tag (Radio IDLE & CONNECTED)

3.5.1.4.2 CDMA Candidate Set Pilot Tag (Radio IDLE)

This tag is used to supply the CDMA Pilot information in Candidate set which is not a part of the Active set but with enough signal power level to become an Active Pilot. Here the device radio is in IDLE mode.

Note that multiple tags could be supplied as a part of the message.

Offset	Field	Size	Value	Description
0	TagID	1	11	CDMA Candidate Pilot Tag Identifier in IDLE mode.
1	Channel	2	0-0x07FF	CDMA Channel Number. 0xFFFF if unknown.
3	BandClass	1	0-10	A numbering scheme for frequency channels. Example: Band Class 0 (800 MHz Band), Band Class 1 (1900 MHz Band), etc. 255 if not known.
4	PilotPN	2	0-0x01FF	The active pilot PN Offset (PN – Pseudo Noise) is short code sequences used to differentiate base stations. 0xFFFF if unknown.
6	EcIo	1	0-0x3F	The Ec/Io (in dB) which is the ratio of received pilot energy, Ec, to total received energy, Io per pilot. It is the highest energy of this pilot and is represented in 0.5dB steps from 0dB (value=0) to 31.5dB (value=63).

Table 22: CDMA Candidate Set Pilot Tag (Radio IDLE)

3.5.1.4.3 CDMA Neighbour Set Pilot Tag (Radio IDLE)

This tag is used to supply the CDMA Pilot information in Neighbour set which are not a part of the Active or Candidate set but may also be considered candidates for a handoff process. Here the device radio is in IDLE mode.

Note that multiple tags could be supplied as a part of the message.

Offset	Field	Size	Value	Description
0	TagID	1	12	CDMA Neighbour Pilot Tag Identifier in IDLE mode.
1	Channel	2	0-0x07FF	CDMA Channel Number. 0xFFFF if unknown.
3	BandClass	1	0-10	A numbering scheme for frequency channels. Example: Band Class 0 (800 MHz Band), Band Class 1 (1900 MHz Band), etc. 255 if not known.
4	PilotPN	2	0-0x01FF	The active pilot PN Offset (PN – Pseudo Noise) is short code sequences used to differentiate base stations. 0xFFFF if unknown.
6	EcIo	1	0-0x3F	The Ec/Io (in dB) which is the ratio of received pilot energy, Ec, to total received energy, Io per pilot. It is the highest energy of this pilot and is represented in 0.5dB steps from 0dB (value=0) to 31.5dB (value=63).

Table 23: CDMA Neighbour Set Pilot Tag (Radio IDLE)

3.5.1.4.4 CDMA Candidate Set Pilot Tag (Radio CONNECTED)

This tag is used to supply the CDMA Pilot information in Candidate set which is not a part of the Active set but with enough signal power level to become an Active Pilot. Here the device radio is in CONNECTED mode.

Note that multiple tags could be supplied as a part of the message.

Offset	Field	Size	Value	Description
0	TagID	1	13	CDMA Candidate Pilot Tag Identifier in CONNECTED mode.
1	Channel	2	0-0x07FF	CDMA Channel Number. 0xFFFF if unknown.
3	BandClass	1	0-10	A numbering scheme for frequency channels. Example: Band Class 0 (800 MHz Band), Band Class 1 (1900 MHz Band), etc. 255 if not known.
4	PilotPN	2	0-0x01FF	The active pilot PN Offset (PN – Pseudo Noise) is short code sequences used to differentiate base stations. 0xFFFF if unknown.
6	EcIo	1	0-0x3F	The Ec/Io (in dB) which is the ratio of received pilot energy, Ec, to total received energy, Io per pilot. It is the highest energy of this pilot and is represented in 0.5dB steps from 0dB (value=0) to 31.5dB (value=63).

Table 24: CDMA Candidate Set Pilot Tag (Radio CONNECTED)

3.5.1.4.5 CDMA Neighbour Set Pilot Tag (Radio CONNECTED)

This tag is used to supply the CDMA Pilot information in Neighbour set which are not a part of the Active or Candidate set but may also be considered candidates for a handoff process. Here the device radio is in CONNECTED mode.

Note that multiple tags could be supplied as a part of the message.

Offset	Field	Size	Value	Description
0	TagID	1	14	CDMA Neighbour Set Pilot Tag Identifier in CONNECTED mode.
1	Channel	2	0-0x07FF	CDMA Channel Number. 0xFFFF if unknown.
3	BandClass	1	0-10	A numbering scheme for frequency channels. Example: Band Class 0 (800 MHz Band), Band Class 1 (1900 MHz Band), etc. 255 if not known.
4	PilotPN	2	0-0x01FF	The active pilot PN Offset (PN – Pseudo Noise) is short code sequences used to differentiate base stations. 0xFFFF if unknown.
6	EcIo	1	0-0x3F	The Ec/Io (in dB) which is the ratio of received pilot energy, Ec, to total received energy, Io per pilot. It is the highest energy of this pilot and is represented in 0.5dB steps from 0dB (value=0) to 31.5dB (value=63).

Table 25: CDMA Neighbour Set Pilot Tag (Radio CONNECTED)

LTE

3.5.1.5This section defines the tags used to provide information to the CellLocate service about the LTE cells observed.

3.5.1.5.1 LTE Cell identity

This tag is used only if the cell is part of a close subscription group (CSG) or is a hybrid cell. If a cell is not preceded by this tag, the cell is recognised by default as a normal cell.

Offset	Field	Size	Value	Description
0	TagID	1	15	Cell Type item Tag Identifier.
1	Cell Type	1	1-2	1 = CSG cell 2 = hybrid cell
2	CSG Identity	4	0-0x07FFFFFF	This field is present and has a valid value only if Cell type is set to CSG or Hybrid.

Table 26: LTE Cell Identity Tag

3.5.1.5.2 LTE Serving Cell Tag (Radio IDLE)

This tag is used to supply the LTE serving Cell observed by the device when the wireless radio is in IDLE mode (note a separate tag is used when the radio is in connected mode).

When the serving cell is part of a CSG or is a hybrid cell, this tag is preceded by the LTE cell identity tag.

Note that if present only one such tag should be supplied as part of any message.

Offset	Field	Size	Value	Description
0	TagID	1	16	LTE Serving Cell Tag Identifier
1	TAC	2	1-0xFFFF	Tracking Area Code.
3	CI	4	0-0x0FFFFFFF	Cell Identity. 0xFFFFFFFF if unknown
7	RSRP	2	-40 to -140	Reference Signal Received Power
9	PCI	2	0-0x01F7	Physical Cell ID. 0xFFFF if not applicable
11	EARFCN	2	0-0xFFFF	Download frequency. 0xFFFF if not applicable
13	CRS tx_pow	1	-60 to +50	1 byte signed integer giving Pilot channel transmission power in dBm. +127 is invalid
14	Cell downlink Bandwidth	1	1-0xFF	0xFF if not applicable
15	Rx-Tx time difference	2	1-0xFFFF	0xFFFF if not applicable

Table 27: LTE Serving Cell Tag (Radio IDLE)

3.5.1.5.3 LTE Neighbouring Cell Tag (Radio IDLE)

This tag is used to supply the LTE neighbouring cells observed by the device when the wireless radio is in IDLE mode (note a separate tag is used when the radio is in connected mode since there is far less information about each cell available when connected).

Where neighbouring cells are observed with different PLMN (MCC / MNC) to that in previous tags then the PLMN Identity Tag is used to change this (for this cell and any subsequent cells).

When neighbouring cells are part of a CSG or are hybrid cells, this tag is preceded by the LTE cell identity tag.

Notes:

- Any number (zero or more) of these tags may be supplied as part of a message.

Offset	Field	Size	Value	Description
0	TagID	1	17	LTE Neighboring Cell Tag Identifier (Radio IDLE)
1	TAC	2	1-0xFFFF	Tracking Area Code.
3	CI	4	0-0x0FFFFFFF	Cell Identity. 0xFFFFFFFF if unknown
7	RSRP	2	-40 to -140	Reference Signal Received Power
9	PCI	2	0-0x01F7	Physical Cell ID. 0xFFFF if not applicable
11	EARFCN	2	0-0xFFFF	Download frequency. 0xFFFF if not applicable
13	Cell downlink Bandwidth	1	1-0xFF	0xFF if not applicable
14	OTDA to serving cell	2	1-0xFFFF	0xFFFF if not applicable

Table 28: UTRAN Neighbouring Cell Tag (Radio IDLE)

3.5.1.5.4 LTE Connected Set Cell Tag (Radio CONNECTED)

This tag is used to supply the LTE cells (either neighbouring or serving) observed by the device when the wireless radio is in CONNECTED mode.

Where cells are observed with different PLMN (MCC / MNC) to that in previous tags then the PLMN Tag is used to change this (for this cell and any subsequent cells).

Notes:

- There is very limited information available on each cell when the wireless radio is in CONNECTED mode hence the tag only has a few fields.
- Any number (zero or more) of these tags may be supplied as part of a message.

Offset	Field	Size	Value	Description
0	TagID	1	18	LTE Neighboring Cell Tag Identifier (Radio IDLE)
1	TAC	2	1-0xFFFF	Tracking Area Code.
3	CI	4	0-0x0FFFFFFF	Cell Identity. 0xFFFFFFFF if unknown
7	RSRP	2	-40 to -140	Reference Signal Received Power
9	PCI	2	0-0x01F7	Physical Cell ID. 0xFFFF if not applicable
11	EARFCN	2	0-0xFFFF	Download frequency. 0xFFFF if not applicable
13	Cell downlink Bandwidth	1	1-0xFF	0xFF if not applicable
14	OTDA to serving cell	2	1-0xFFFF	0xFFFF if not applicable

Table 29: LTE Connected Set Cell Tag (Radio CONNECTED)

3.5.2 WiFi Tags

Device ID

This section defines the tags used to provide information to the CellLocate service about the Device ID in the WiFi domain (the MAC address ?).

Offset	Field	Size	Value	Description
0	TagID	1	19	WiFi Device ID Tag Identifier
1	WiFiDeviceID	48	0-0xFFFFFFFFFFFF	WiFi Device ID (MAC address?)

3.5.2.1

Table 30: WiFi Device ID Tag

Access Points (AP)

This section defines the tags used to provide information to the CellLocate service about the WiFi Access Points observed.

3.5.2

Offset	Field	Size	Value	Description
0	TagID	1	20	WiFi Access Point Tag Identifier
1	BSSID	6	0-0xFFFFFFFFFFFF	Access Point MAC address
7	RSSI	3	0-0xFFFFFF	Measured signal strength in dBm
10	Channel	3	0-0xFFFFFF	Channel used by the network
13	OpMode	1	1-2	Operator Mode: 1 = Infrastructure, 2 = Ad-hoc
14	AuthSuites	1	0-0xF	Authentication suites: Bit 0 = Shared secret, Bit 1 = PSK, Bit 2 = EAP, Bit 3 = WPA, Bit 4 = WPA2
15	UniCiphers	1	0-0xF	Unicast ciphers: Bit 0 = WEP64, Bit 1 = WEP128, Bit 2 = TKIP, Bit 3 = AES/CCMP
16	GroupCiphers	1	0-0xF	Group ciphers: Bit 0 = WEP64, Bit 1 = WEP128, Bit 2 = TKIP, Bit 3 = AES/CCMP
17	Length	1	N	Length field of SSID field
18	SSID	N	ASCII	SSID name of the network

Table 31: WiFi Access Point Tag

3.5.3.1

3.5.3 General Data Tags

SessionID Tag

A session is defined as the interaction between a device and the service where the device may submit a network scan and a GNSS fix to the service.

The session may be formed by:

- Single interaction (position request based on a network scan or a network scan together with a GNSS fix)
- Two interactions (a network scan first followed by a GNSS fix message)

The SessionID is an identifier that, together with the DeviceID, guarantees the unique identification of the device during a session.

Offset	Field	Size	Value	Description
0	TagID	1	148	SessionID Tag Identifier.
1	SessionID	4	0-4294967295	SessionID

Table 32: DeviceDescriptor Tag

DeviceDescriptor Tag

Offset	Field	Size	Value	Description
0	TagID	1	129	Device Descriptor Tag Identifier.
1	Length	1	N	Length field of DeviceDescriptor field
2	DeviceDescriptor	N	ASCII	A descriptor that defines the actual u-blox module type (e.g. LISA or LEON) and details of the firmware running on the module.

3.5.3.2 Table 33: DeviceDescriptor Tag

Version tag structure

Version of the device as defined in section 3.4.3.

Offset	Field	Size	Value	Description
0	TagID	1	142	Version Tag Identifier.
1	Version	1	1-2	Version of modem

3.5.3.3

Table 34: Version tag structure

CustomerData tag structure

Offset	Field	Size	Value	Description
0	TagID	1	131	CustomerData Tag Identifier.
1	Length	1	N	Length field of CustomerData field
2	CustomerData	N	ASCII	Customer Data. This is data passed to the module directly via the AT interface and then passed over the interface to the CellLocate Service. Used as a means to supply additional information to the service directly from the customer application.

3.5.3.4

Table 35: CustomerData tag structure

Note that this tag is used for FAE support, whereby when the value of the tag is a TwikiName of a u-blox employee, additional logging of the device will be performed in order to make information available to FAE's on the device usage for support purposes.

3.5.3.5

DCU Tag structure

The tag ID 132 is reserved for Data Collection Units (DCU). DCU are devices used in the field by FAEs to seed CellLocate database. This tag has no content. The presence of this tag indicates that the request is not required to be processed by the commercial 3rd party database.

Offset	Field	Size	Value	Description
0	TagID	1	133	DCU Mode Tag Identifier. This request if from a DCU (Data Collection Unit).

3.5.3.6

Table 36**: DCU tag structure**

Carrier Tag structure

The Carrier tag is used to update the Carrier of the device.

Offset	Field	Size	Value	Description
0	TagID	1	134	Carrier Tag Identifier.
1	Length	1	N	Length field of Carrier name field.
2	Carrier	N	ASCII	The Carrier name. Example: Cellular One, AT&T, Cingular, Sprint, Verizon Wireless, etc.

Table 37: Carrier Tag structure

3.5.3.7 PRL Tag structure

The PRL tag is used to update the PRL Identifier of the device. If there have been any changes to the PRL Identifier on the device, then this tag can be used to indicate the changes.

Offset	Field	Size	Value	Description
0	TagID	1	135	PRL Tag Identifier.
1	PRLId	2	0-0xFFFF	The Preferred Roaming List Identifier.

Table 38: PRL Tag structure

3.5.3.8 Time Tag

The Time tag is used inform the service about the epoch in which the information following has been taken

Offset	Field	Size	Value	Description
0	TagID	1	143	PLMN Tag Identifier.
1	Year	1	17-99	Year (UTC)
3	Month	1	1-12	Month (UTC)
4	Day	1	1-31	Day (UTC)
5	Hour	1	0-24	Hour (UTC)
6	Min	1	0-60	Minutes (UTC)
7	Second	1	0-60	Seconds (UTC)

Table 39: Time Tag

3.5.3.9 Relative Time Tag structure

The request message has to contain this optional tag if the velocity and/or position tags are used in order to provide the corresponding time reference.

❖ Time offset in seconds is expressed with an exponential parametric coding:

$$offset = C((1 + x)^k - 1)$$

where C=1 and x=0.05.

8bits are used to express the exponent k. k has the rage 0-255, the time difference range is 0-250000s (about 3days).

To recover the absolute time, the server will subtract the time offset from the current time.

Offset	Field	Size	Value	Description
0	TagID	1	200	Time Tag Identifier.
1	timeOffset	1	0-255	time offset expressed with exponential coding: C=1, x=0.05

Table 5: Time Tag structure

3.5.3.10 Velocity Tag structure

The device could optionally notify the CellLocate service, the average speed and direction using the Velocity tag.

This tag could also be additionally used with the GSMCLL and GSMCNF message (including the GSMCEL/GSMCLO).

Offset	Field	Size	Value	Description
0	TagID	1	136	Velocity Tag Identifier.
1	Speed	1	0-254	Speed over ground m/s. 255 if unknown.
2	Direction	2	0-360	Course over ground in degrees relative to North clockwise. 65535 if unknown.

Table 40: Velocity Tag structure

Motion detection Tag structure

The new FW devices can notify the CellLocate service with its dynamic status.

The presence of this tag means that the motion detection algorithms were active on the modem. The absence of this tag may indicate an old FW or that the motion detection was disabled.

3.5.3. . .

Offset	Field	Size	Value	Description
0	TagID	1	144	Motion detection Tag Identifier.
1	status	1	0-100	Confidence of the motion detection. Percentage ranging from 0 (no match = motion) to 100 (perfect match = static conditions)

Table 41: Motion detection Tag structure

Network scan status Tag structure

The modem can notify the CellLocate service with the status of the network scan.

The network scan may not be complete because of many reasons.

3.5.3.12

Offset	Field	Size	Value	Description
0	TagID	1	145	Netwrok scan status Tag Identifier.
1	status	1	0-255	Unsigned integer indicating the scan status. Following are the codes 0 – Scan complete 1 – scan interrupted because of buffer size settings 2 – scan interrupted because of timeout 3 – scan suspended and not resumed because of data traffic
2	limits	2	0-65535	Applicable only to status 1 or 2: 1 – max size of the buffer in bytes 2 – timeout of the scan in seconds

Table 42: Motion detection Tag structure

3.5.3.13

Supplementary Position Request Tag structure

This tag allows the device to request for multiple position estimates from the CellLocate service. This is in addition to the nominal position estimate sent in the UBX-AID-INI message.

Offset	Field	Size	Value	Description
0	TagID	1	137	Supplementary Position Request Tag Identifier.
1	NumReports	1	0-255	The maximum number of supplementary position estimates to be returmed. The service would limit the number of positions returned to this value. If the value of NumReports is greater than what the service can actually provide, the service only returns what it can provide.

3.5.3.14

Table 43: Supplementary Position Request Tag structure

Position Tag structure

This tag contains a position estimate and can be used in the following scenarios:

- The device can inform the CellLocate Service about its autonomous position using this tag.

  When the device sends its autonomous position to the Service, it will use the appropriate value to indicate the source of its autonomous position. For example, if the autonomous solution is based on a GNSS solution, then the location source will be set to 10.

- If the device has requested for multiple positions, then the CellLocate Service responds with multiple position tags. There may be multiple position tags up to the 'NumReports' field specified by the device.

  The Service will include the source of its location in the position tags to the device. This will not be exposed to the application using AT commands.

Offset	Field	Size	Value	Description
0	TagID	1	138	Position Tag Identifier.
1	Latitude	4	Any	Signed latitude coordinate of position in degree*1e-7. The Latitude and Longitude is set to 0 if unknown.
5	Longitude	4	Any	Signed latitude coordinate of position in degree*1e-7. The Latitude and Longitude is set to 0 if unknown.
9	Source	1	0-255	Unsigned integer indicating the source of position. Following are the codes to indicate the source of position 1 – CelllLocate solution without fallback 2 – OpenCellID 3 – GNSS solution from device 5 – User location 6 – Combain Cache 7 – Combain Web 8 – CellLocate solution using fallback 9 – CDMA Basestation location 10 – CDMA CellLocate location

Table 44: Position Tag structure

3.5.3.15 Uncertainty Ellipse Request Tag structure

The default uncertainty provided by the service is in the form of a radius. The device could also request for the uncertainty as an ellipse for the position estimate. This tag has no content.

If this tag is set in the request, then the ellipsoidal uncertainty for the nominal position estimate and the supplementary positions (if requested) will be sent to the device.

The ellipsoidal uncertainty for the nominal position estimate will follow the UBX messages. If multiple position reports are requested, then the ellipsoidal uncertainty will follow each supplementary position estimate.

Offset	Field	Size	Value	Description
0	TagID	1	139	Uncertainty Ellipse Request Tag Identifier.

Table 45: Uncertainty Ellipse Request Tag structure

3.5.3.16 Uncertainty Ellipsoid Tag structure

This tag identifies the uncertainty of a position estimate as an ellipse.

The ellipsoidal uncertainty includes the offset of the centre point of the ellipse, semi-major axis, semi-minor axis, orientation of the major axis and the confidence level of the uncertainty.

This tag can be used in the following scenarios:

- It can be used by the device to inform the Server about its autonomous position uncertainty.
- If the device requests for Multiple Position(s), then for each instance of the multiple position reports; one or more of the Uncertainty Ellipsoid Tag (with 95 and/or 50 percent confidence) will always follow its respective Position Tag. This response tag will be sent to the device, wrapped as part of the UBX-TUN-CEL message.
- Latitude and longitude offsets in degrees are expressed with an exponential parametric coding:

  $$angle = C((1+x)^k - 1$$

  where C=0.00035 and x=0.025.

  Latitude and longitude offsets are expressed in 8bits: 1 bit for the sign and 7bits to express the exponent k. k has the rage 0-512, the angle offset of ±108° (about ±6000km at 60° latitude).
- Semi-major and semi-minor axis are expressed in meters using the same exponential coding used for the angle offsets but with parameters C=25 and x=0.05.

  8bits are used to express the exponent k. k has the rage 0-255, the axis range is 0-6300km.

Offset	Field	Size	Value	Description
0	TagID	1	139	Uncertainty Ellipsoid Response Tag Identifier.
1	latOffset	2	-512 – 512	Exponential parameters to compute the latitude offset in degrees from the position. Exponential coding: C=0.00035, x=0.025
3	lonOffset	2	-512 – 512	Exponential parameters to compute the longitude offset in degrees from the position. Exponential coding: C=0.00035, x=0.025
5	SemiMajor	1	0-255	Exponential parameters to compute the semi-major axis of the uncertainty ellipse in metres. Exponential coding: C=25, x=0.05
6	SemiMinor	1	0-255	Exponential parameters to compute the semi-minor axis of the uncertainty ellipse in metres. Exponential coding: C=25, x=0.05
7	Orientation	1	0-179	The orientation of the major axis in degrees computed clockwise from North.
8	Confidence	1	0-100	The confidence level of the uncertainty in percent.

Table 4: Uncertainty Ellipsoid Response Tag structure

Reverse Geocoding Request Tag structure

The device could request for reverse geocoded information for the position estimate using this tag. It has no content.

3.5.3.17 If this tag is set in the request, then the nominal position estimate and the supplementary positions (if requested for) will be reverse geocoded.

The reverse gecoded information of the nominal position will follow the UBX Messages. If multiple position reports are requested, then the ellipsoidal uncertainty will follow each of it supplementary position.

Offset	Field	Size	Value	Description
0	TagID	1	140	Reverse-Geocoding Request Tag Identifier.

Table 46: Reverse Geocoding Request Tag structure

3.5.3.18 Reverse Geocode Response Tag structure

If the device has requested for reverse geocoding information, this tag contains the reverse geocoded details sent back to the device.

The first Reverse Geocode Response Tag will belong to the nominal position.

If supplementary positions are requested, then this tag will follow each instance of the Supplementary Position Reports.

Offset	Field	Size	Value	Description
0	TagID	1	140	Reverse-Geocode Response Tag Identifier.
1	Category	1	0-6	cycleway, highway, tracktype, waterway, railway
2	Subcategory	1	0-255	TBD
3	Length	2	N	Length of reverse geocoded field.
5	Address	N	ASCII	Comma separated reverse geocoded information containing Street, Town and Country, etc.

3.5.3.19

Table 47: Reverse Geocode Response Tag structure

Multi GNSS Assistance (MGA) Support

The tag ID 141 is reserved for Multi GNSS Assistance support to request assistance data for one or more GNSS.

The GNSS types supported currently are GPS, GLONASS and QZSS.

The data can be requested for a specific GNSS or a combination of GNSS as shown in the table below.

Offset	Field	Size	Value	Description
0	TagID	1	141	Multi GNSS Assistance Tag Identifier.
1	GNSS	1	1-32	GNSS data requested where the following values indicates the GNSS type in binary 0000 0001 GPS 0000 0010 GLONASS (GLO) 0000 0100 QZSS 0000 1000 BeiDou (BDS) 0001 0000 SBAS A combination of GNSS can be requested as follows 0000 0011 GLO + GPS 0000 0101 QZSS + GPS 0000 0110 QZSS + GLO 0000 1001 BDS + GPS 0000 1010 BDS + GLO 0000 1100 BDS + QZSS 0001 0001 SBAS + GPS 0001 0010 SBAS + GLO 0001 0100 SBAS + QZSS 0001 1000 SBAS + BDS 0000 0111 QZSS + GLO + GPS 0000 1011 BDS + GLO + GPS 0000 1101 BDS + QZSS + GPS 0000 1110 BDS + QZSS + GLO 0001 0011 SBAS + GLO + GPS 0001 0101 SBAS + QZSS + GPS 0001 0110 SBAS + QZSS + GLO 0001 1001 SBAS + BDS + GPS 0001 1010 SBAS + BDS + GLO 0001 1100 SBAS + BDS + QZSS 0000 1111 BDS + QZSS + GLO + GPS 0001 0111 SBAS + QZSS + GLO + GPS 0001 1011 SBAS + BDS + GLO + GPS 0001 1101 SBAS + BDS + QZSS + GPS 0001 1110 SBAS + BDS + QZSS + GLO 0001 1111 SBAS + BDS + QZSS + GLO + GPS Please note that SBAS and BeiDou is not currently supported.

Table 48: Multi GNSS Assistance tag structure

4 Usage Models

There are a number of expected use cases for this protocol. The following is a representative, but not exhaustive, list of these typical use cases and the message structures appropriate for these cases.

Also refer to Appendix A for full examples of the GSMCxx messages.

4.1 GPS aiding request (aid format) with location estimate based on existing cell information

The wireless module is currently registered to the GSM network and has current information on visible cells in the home network. The device is commanded to perform a GPS fix using CellLocate aiding, and the device does not have current aiding information present. The service provides a set of aiding data appropriate to the location estimated from the cell information. If the service can provide no position estimate then it will provide the complete set of aiding information.

Direction	**Message Structure (example)**
Device->Service	[GSMCLO, ServingCell, NeighbourCell x5, Null]
Service->Device	[UBX-AID-EPH x12, UBX-AID-HUI, UBX-AID-INI]
Device->Service	[GSMCLL, Null]

4.2 Multi-GNSS aiding request (gnss=gps,glo) following a full network scan for enhanced position estimate

The wireless module is commanded to perform a GNSS fix using CellLocate aiding, and the device does not have current aiding information present. The wireless module has been configured to allow a scan for available networks when requesting aiding (datatype=eph,aux,pos). The scan produces cell information from a number of PLMNs. The service provides a set of aiding data appropriate to the location estimated from the cell information.

Direction	**Message Structure (example)**
Device->Service	[GSMCLO, ServingCell, NeighbourCell x6, PLMN, NeighbourCell x4, PLMN, NeighbourCell x1, PLMN, NeighbourCell x2, Null]
Service->Device	[UBX-MGA-INI-TIME_UTC, UBX-MGA-INI-POS_LLH, UBX-MGA-GPS-EPH x12, UBX-MGA-GPS-HEALTH, UBX-MGA-GPS-UTC , UBX-MGA-GPS-IONO, UBX-MGA-GLO-EPH x12, UBX-MGA-GLO-TIMEOFFSET]
Device->Service	[GSMCLL, Null]

4.3 Location estimate request with GPS present and no aiding needed

The wireless module is currently registered to the GSM network and has current information on visible cells in the home network. The device is commanded to perform a GPS fix using CellLocate aiding, and the device already has current aiding information. The service provides aiding data specifying the location estimated from the cell information.

Direction	**Message Structure (example)**
Device->Service	[GSMCLO,ServingCell,NeighbourCell x 5,Null]
Service->Device	[UBX-AID-INI]
Device->Service	[GSMCLL, Null]

4.4 Location estimate request with no GNSS present

The wireless module is currently registered to the GSM network and has current information on visible cells in the home network. There is no GNSS device available to the wireless module. The device is commanded to obtain a location estimate cell fix. The service provides the location estimated from the cell information.

Direction	Message Structure (example)
Device->Service	[GSMCLO,ServingCell,NeighbourCell x5,Null]
Service->Device	[UBX-MGA-INI-POS_LLH, UBX-MGA-INI-TIME_UTC]

4.5 GNSS aiding with multi-hypothesis and uncertainty ellipse

As in (4.1) except that the Modem requires at least one position estimate with uncertainty ellipse.

The modem has to select the best solution from the multiple positions returned and modify the UBX-AID-INI/UBX-MGA-INI to GNSS

Direction	Message Structure (example)
Modem->Service	[GSMCEL, ServingCell, NeighbourCell x6, PLMN, NeighbourCell x4, PLMN, NeighbourCell x1, PLMN, NeighbourCell x2, MultiHypotesisReq, UncEllipseReq, Null]
Service->Modem	[UBX-AID-EPH x10, UBX-AID-HUI, UBX-AID-INI, UBX-TUN-CEL]
Modem->GNSS	[UBX-AID-EPH x10, UBX-AID-HUI, UBX-AID-INI(modified by the modem)]
GNSS->Modem	GPS fix
Modem->Service	[GSMCLL, Null]

5 Future Extensions

5.1 Extending Message Types

Additional message types may be defined in the future. The preamble 'GSMC' shall be interpreted to indicate the message is structured as defined in 3.2. Messages that differ in structure must use a distinct preamble.

A future version of the service may be extended to support additional message types, but it shall also maintain backward compatibility with devices using the interface defined in this version of the specification. That is, it shall continue to accept the messages defined in this release of the interface specification, and shall continue to respond to such messages in the response message format defined.

5.2 Extending Tags

Further Tag IDs may be defined in the future for new classes of information. New tags may be defined to be optionally present for the existing message type.

As the service rejects messages with unrecognized tag IDs, the deployment of the update to the service to support new tags shall precede implementation on devices.

To retain backward compatibility, the response to devices that do not utilize the extended tags shall continue to be in the format defined in this release of the interface specification. New devices must send the new tags in order to request additional enhanced response information.

5.3 Extending Response Format

The response format to messages with the preamble 'GSMC' shall continue to be of content type 'application/ubx'. New UBX message types may be emitted in response to new message types or tags.

Appendix

A Examples

A.1 GSMCLO Home PLMN example

Serving cell and a number of neighbouring cells in the home PLMN are detected. Some neighbours have missing CI field (FFFF is used). Cells seen (as MCC-MNC-LAC-CI-BSIC-ARFCN RXLEV):

234-15-008e-6172-15-0099 63
234-15-008e-6173-05-0075 57
234-15-008e-159b-23-0077 27
234-15-008e-0de5-24-0079 25
234-15-008e-ffff-32-0553 29
234-15-008e-ffff-04-0065 44

Offset	Hex	Text	Description
0	47	G	Cell Information Message Identifier
1	53	S	
2	4D	M	
3	43	C	
4	4C	L	
5	4F	O	
6	24	-	Identifier for the originating device. Typically obtained by XOR combination of IMEI and IMSI identifiers.
7	78	-	
8	30	-	
9	56	-	
10	26	-	
11	46	-	
12	1B	-	
13	F3	-	
14	15	-	Home PLMN for the wireless module. Combines the MCC and MNC identifiers in a single 6 digit identifier. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The Home PLMN is the PLMN for following cell tags until a new PLMN tag occurs. MCC=234, MNC=15
15	34	-	
16	02	-	
17	01	-	Serving Cell Tag Identifier.
18	8E	-	Location Area Code. LAC=008E
19	00	-	
20	72	-	Cell Identity. CI=6172
21	61	-	
22	49	-	RXLEV. Receiving level of the cell signal rxlev=63
23	15	-	Base Station Identity Code. BSIC=15
24	63	-	Absolute Radio Frequency Channel Number. ARFCN=99
25	00	-	
26	14	-	Timing Advance. TA=20
27	00	-	Routing Area Code (unused). RAC=0
28	02	-	Neighbouring Cell Tag Identifier
29	8E	-	Location Area Code. LAC=008E
30	00	-	
31	73	-	Cell Identity. CI=6173
32	61	-	

33	39	-	RXLEV. Receiving level of the cell signal. Rxlev=57
34	05	-	Base Station Identity Code. BSIC=05
35	48	-	Absolute Radio Frequency Channel Number. ARFCN=75
36	00	-	
37	02	-	Neighbouring Cell Tag Identifier
38	8E	-	Location Area Code. LAC=008E
39	00	-	
40	9B	-	Cell Identity. CI=159b
41	15	-	
42	1B	-	RXLEV. Receiving level of the cell signal. Rxlev=27
43	23	-	Base Station Identity Code. BSIC=23
44	4D	-	Absolute Radio Frequency Channel Number. ARFCN=77
45	00	-	
46	02	-	Neighbouring Cell Tag Identifier
47	8E	-	Location Area Code. LAC=008E
48	00	-	
49	E5	-	Cell Identity. CI=0de5
50	0D	-	
51	19	-	RXLEV. Receiving level of the cell signal. Rxlev=25
52	24	-	Base Station Identity Code. BSIC=24
53	4F	-	Absolute Radio Frequency Channel Number. ARFCN=79
54	00	-	
55	02	-	Neighbouring Cell Tag Identifier
56	8E	-	Location Area Code. LAC=008E
57	00	-	
58	FF	-	Cell Identity. CI=ffff
59	FF	-	
60	1D	-	RXLEV. Receiving level of the cell signal. Rxlev=29
61	32	-	Base Station Identity Code. BSIC=32
62	29	-	Absolute Radio Frequency Channel Number. ARFCN=553
63	02	-	
64	02	-	Neighbouring Cell Tag Identifier
65	8E	-	Location Area Code. LAC=008E
66	00	-	
67	FF	-	Cell Identity. CI=ffff
68	FF	-	
69	2C	-	RXLEV. Receiving level of the cell signal. Rxlev=44
70	04	-	Base Station Identity Code. BSIC=04
71	41	-	Absolute Radio Frequency Channel Number. ARFCN=65
72	00	-	
73	00	-	Null Tag Identifier

A.2 GSMCLL example

Following receipt of aiding, when a first fix is achieved by the GNSS device, a second message is sent to the service (Lat/Lon format):

Offset	Hex	Text	Description
0	47	G	Lat/Lon Message Identifier
1	53	S	
2	4D	M	
3	43	C	
4	4C	L	
5	4C	L	
6	24	-	Identifier for the originating device. Typically obtained by XOR combination of IMEI and IMSI identifiers.
7	78	-	
8	30	-	
9	56	-	
10	26	-	
11	46	-	
12	1B	-	
13	F3	-	
14	60	-	Signed latitude coordinate in degree*1e-7. lat= +512415840
15	D8	-	
16	8A	-	
17	1E	-	
18	C0	-	Signed longitude coordinate in degree*1e-7. lon = -2047040
19	C3	-	
20	E0	-	
21	FF	-	
22	EC	-	Signed altitude coordinate in cm. alt = 14060
23	36	-	
24	00	-	
25	00	-	
26	E8	-	Position accuracy in cm. 10m
27	03	-	
28	00	-	
29	00	-	
30	10	-	Time to fix in seconds. 16sec
31	00	-	
32	00	-	
33	00	-	
34	05	-	Number of satellites used in the position fix. SVs=5
35	00	-	Null Tag Identifier

A.3 GSMCLO Multiple PLMN example

Serving cell and a number of neighbouring cells in the various PLMNs are detected. Cells seen (as MCC-MNC-LAC-CI-BSIC-ARFCN RXLEV):

234-15-008e-6172-15-0099 63
234-33-0076-05c8-2b-0804 39
234-33-0076-4778-28-0839 36
234-30-02aa-1391-29-0642 38
234-10-331a-4e3b-0c-0119 50

Offset	Hex	Text	Description
0	47	G	Cell Information Message Identifier
1	53	S	
2	4D	M	
3	43	C	
4	4C	L	
5	4F	O	
6	24	-	Identifier for the originating device. Typically obtained by XOR combination of IMEI and IMSI identifiers.
7	78	-	
8	30	-	
9	56	-	
10	26	-	
11	46	-	
12	1B	-	
13	F3	-	
14	15	-	Home PLMN for the wireless module. Combines the MCC and MNC identifiers in a single 6 digit identifier. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The Home PLMN is the PLMN for following cell tags until a new PLMN tag occurs. MCC=234, MNC=15
15	34	-	
16	02	-	
17	01	-	Serving Cell Tag Identifier.
18	8E	-	Location Area Code. LAC=008E
19	00	-	
20	72	-	Cell Identity. CI=6172
21	61	-	
22	3F	-	RXLEV. Receiving level of the cell signal rxlev=63
23	15	-	Base Station Identity Code. BSIC=15
24	63	-	Absolute Radio Frequency Channel Number. ARFCN=99
25	00	-	
26	14	-	Timing Advance. TA=20
27	00	-	Routing Area Code (unused). RAC=0
28	03	-	PLMN Tag Identifier.
29	33	-	New PLMN. Combines the MCC and MNC identifiers in a single 6 digit identifier. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The new PLMN is the PLMN for any following cell tags. MCC=234 MNC=33
30	34	-	
31	02	-	
32	02	-	Neighbouring Cell Tag Identifier
33	76	-	Location Area Code. LAC=0076
34	00	-	
35	C8	-	Cell Identity. CI=05c8
36	05	-	
37	27	-	RXLEV. Receiving level of the cell signal. Rxlev=39

38	2B	-	Base Station Identity Code. BSIC=2B
39	24	-	Absolute Radio Frequency Channel Number. ARFCN=804
40	03	-	
41	02	-	Neighbouring Cell Tag Identifier
42	76	-	Location Area Code. LAC=0076
43	00	-	
44	78	-	Cell Identity. CI=4778
45	47	-	
46	24	-	RXLEV. Receiving level of the cell signal. Rxlev=36
47	28	-	Base Station Identity Code. BSIC=28
48	47	-	Absolute Radio Frequency Channel Number. ARFCN=839
49	03	-	
50	03	-	PLMN Tag Identifier
51	30	-	New PLMN. Combines the MCC and MNC identifiers in a single 6 digit identifier. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The new PLMN is the PLMN for any following cell tags. MCC=234 MNC=30
52	34	-	
53	02	-	
54	02	-	Neighbouring Cell Tag Identifier
55	AA	-	Location Area Code. LAC=02aa
56	02	-	
57	91	-	Cell Identity. CI=1391
58	13	-	
59	26	-	RXLEV. Receiving level of the cell signal. Rxlev=38
60	29	-	Base Station Identity Code. BSIC=29
61	82	-	Absolute Radio Frequency Channel Number. ARFCN=642
62	02	-	
63	03	-	PLMN Tag Identifier
64	10	-	New PLMN. Combines the MCC and MNC identifiers in a single 6 digit identifier. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The new PLMN is the PLMN for any following cell tags. MCC=234 MNC=10
65	34	-	
66	02	-	
67	02	-	Neighbouring Cell Tag Identifier
68	1A	-	Location Area Code. LAC=331a
69	33	-	
70	3B	-	Cell Identity. CI=4e3b
71	4E	-	
72	32	-	RXLEV. Receiving level of the cell signal. Rxlev=50
73	0C	-	Base Station Identity Code. BSIC=0c
74	77	-	Absolute Radio Frequency Channel Number. ARFCN=0119
75	00	-	
76	00	-	Null Tag Identifier

A.4 GSMCLO PLMN with 3 digit MNC example

Serving cell with 3 digit PLMN is detected. Cells seen (as MCC-MNC-LAC-CI-BSIC-ARFCN RXLEV):

234-153-008e-6172-15-0099 63

Offset	Hex	Text	Description
0	47	G	Cell Information Message Identifier
1	53	S	
2	4D	M	
3	43	C	
4	4C	L	
5	4F	O	
6	24	-	Identifier for the originating device. Typically obtained by XOR combination of IMEI and IMSI identifiers.
7	78	-	
8	30	-	
9	56	-	
10	26	-	
11	46	-	
12	1B	-	
13	F3	-	
14	53	-	Home PLMN for the wireless module. Combines the MCC and MNC identifiers in a single 6 digit identifier. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The Home PLMN is the PLMN for following cell tags until a new PLMN tag occurs. MCC=234, MNC=153
15	41	-	
16	23	-	
17	64	-	Latency of communication channel in milliseconds. The timestamp on the returned aiding message is adjusted by this value. 100ms
18	00	-	
19	01	-	Serving Cell Tag Identifier.
20	8E	-	Location Area Code. LAC=008E
21	00	-	
22	72	-	Cell Identity. CI=6172
23	61	-	
24	3F	-	RXLEV. Receiving level of the cell signal rxlev=63
25	15	-	Base Station Identity Code. BSIC=15
26	63	-	Absolute Radio Frequency Channel Number. ARFCN=99
27	00	-	
28	14	-	Timing Advance. TA=20
29	00	-	Routing Area Code (unused). RAC=0
30	00	-	Null Tag Identifier

A.5 GSMCLO non-home PLMN example

Serving cell and a number of neighbouring cells in the same non-home PLMN are detected. A CustomerData field is transmitted to access premium service. Cells seen (as MCC-MNC-LAC-CI-BSIC-ARFCN RXLEV):

222-88-55fa-1d0d-39-0761 34

222-88-55fa-12eb-3d-0102 29

Offset	Hex	Text	Description
0	47	G	Cell Information Message Identifier
1	53	S	
2	4D	M	
3	43	C	
4	4C	L	
5	4F	O	
6	24	-	Identifier for the originating device. Typically obtained by XOR combination of IMEI and IMSI identifiers.
7	78	-	
8	30	-	
9	56	-	
10	26	-	
11	46	-	
12	1B	-	
13	F3	-	
14	15	-	Home PLMN for the wireless module. Combines the MCC and MNC identifiers in a single 6 digit identifier. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The Home PLMN is the PLMN for following cell tags until a new PLMN tag occurs. MCC=234, MNC=15
15	34	-	
16	02	-	
17	03	-	PLMN Tag Identifier.
18	88	-	New PLMN. Combines the MCC and MNC identifiers in a single 6 digit identifier. The identifiers are represented as BCD digits, as in the GSM transmission. The MNC forms the 2 or 3 least significant digits, and the MCC forms the next 3 digits. The most significant digit is 0 if not used. The new PLMN is the PLMN for any following cell tags. MCC=222 MNC=88
19	22	-	
20	02	-	
21	01	-	Serving Cell Tag Identifier.
22	FA	-	Location Area Code. LAC=55fa
23	55	-	
24	0D	-	Cell Identity. CI=1d0d
25	1D	-	
26	22	-	RXLEV. Receiving level of the cell signal rxlev=34
27	39	-	Base Station Identity Code. BSIC=39
28	F9	-	Absolute Radio Frequency Channel Number. ARFCN=761
29	02	-	
30	14	-	Timing Advance. TA=20
31	00	-	Routing Area Code (unused). RAC=0
32	02	-	Neighbouring Cell Tag Identifier
33	FA	-	Location Area Code. LAC=55fa
34	55	-	
35	EB	-	Cell Identity. CI=12eb
36	12	-	
37	1D	-	RXLEV. Receiving level of the cell signal. Rxlev=29
38	3D	-	Base Station Identity Code. BSIC=3d
39	66	-	Absolute Radio Frequency Channel Number. ARFCN=102
40	00	-	

41	81	-	Customer ID Tag Identifier
42	03	-	Length field of customer ID field. 3 bytes
43	56	V	Customer data
44	49	I	
45	50	P	
46	83	-	Customer Password Tag Identifier
47	07	-	Length field of customer password field. 7 bytes
48	70	P	Customer data
49	61	A	
50	73	S	
51	73	S	
52	6B	K	
53	65	E	
54	79	Y	
55	00	-	Null Tag Identifier

B Informative - Reserved Functions

This section is for informative purposes only.

The protocol may support auxiliary functions for internal u-blox use only. These functions are not intended to be implemented on devices available to end-users, and are documented here to reserve their use.

B.1 Cell Harvesting using GSMCLL

Devices containing both a GPS receiver and a wireless module can directly associate a GPS position fix with a set of cell observations. Such devices can perform a survey of a geographic area, providing bulk data for the database. The upload of this data is enabled by extending the capabilities of the GSMCLL message.

The message tags ‘PLMN’, ‘GSM Serving Cell’, and ‘GSM Neighbouring Cell’ are reserved, in these messages, for this purpose. For these messages, the cell information tags are defined to be the visible cells at the device position reported.

The PLMN tag defines the PLMN fields for subsequent Cell tags. Note that, as there is no default PLMN in the header structure for these messages, the value of the PLMN for cells declared before the first PLMN tag is undefined.

This extension to the GSMCLL function does not affect their other semantics. For example, processing this message after previous reception of a GSMCLO message from the same device will cause the reported position to be associated with the previous cell report as usual.

C Test Support

The tag ID 127 is reserved for testing purposes. The tag has no content. The presence of this tag indicates that the request is not required to processed by the service, and the response (if any) to requests marked in this way is not defined.

Offset	Field	Size	Value	Description
0	TagID	1	127	Test Tag Identifier. The request is a test.

Table 49: Test tag structure

Glossary

- MCC - Mobile Country Code. 3 digit identifier.
- MNC – Mobile Network Code. 2 or 3 digit identifier.
- PLMN - Public Land Mobile Network. A PLMN is identified by combination of MCC and MNC.
- LAC - Location Area Code used for a small region by the network operator. 4 digit identifier.
- CI - Cell Identity. Identifier allocated for a BTS by the network operator. 4 digit identifier.
- BSIC - Base Station Identity Code. The short form identifier allocated by the network operator. 6 bit code.
- ARFCN - Absolute Radio Frequency Channel Number. For cell identity, the ARFCN is the frequency being used for the BCCH transmission.
- BCCH - Broadcast common control channel. The beacon of every BTS.
- BTS - Base transceiver station. i.e. a cell base station.
- Digit - in GSM, 1digit=4bits. May contain a single hex or BCD digit.
- RXLEV – measurement of the receiving level of the GSM Air-interface. 5bit code mapping to -110dBm to -48dBm.
- RSCP - Received Signal Code Power.
- dlFrequency - Download frequency.
- RAC - Routing Area Code.
- ECN0 - Energy per Chip / Noise in dB levels.
- SID - CDMA System Identifier.
- NID – CDMA Network Identifier.
- BSID - Base Station Identifier
- LTMOffset - Local Time Offset.
- RSSI - Received Signal Strength Indication.
- Channel - CDMA Channel Number.
- BandClass - A numbering scheme for frequency channels in CDMA network.
- PilotPN - The active pilot PN Offset (PN – Pseudo Noise) is short code sequences used to differentiate base stations
- EcIo - The Ec/Io (in dB) which is the ratio of received pilot energy, Ec, to total received energy, Io per pilot. Related documents
- UBX – binary protocol format used for communication with u-blox GNSS devices.
- UBX-AID – UBX protocol message class used for GPS aiding data.
- UBX-AID-INI – message type containing position, time and clock drift.
- UBX-AID-EPH – message type containing ephemeris data for a single GPS satellite.
- UBX-AID-HUI – message type containing satellite health, UTC correction terms, and ionospheric correction terms.
- UBX-MGA-INI - UBX protocol message class used for Multi-GNSS aiding data.
- UBX-MGA-INI-POS_LLH – message type containing position information in WGS84 lat/long/alt coordinates.

☞ UBX-MGA-INI-TIME_UTC - message type containing UTC time.

☞ UBX-MGA-GPS-EPH - message type containing ephemeris data for a single GPS satellite in Multi-GNSS format.

☞ UBX-MGA-GPS-HEALTH - message type containing satellite health in Multi-GNSS format.

☞ UBX-MGA-GPS-UTC - message type containing GPS UTC time correction in Multi-GNSS format.

☞ UBX-MGA-GPS-IONO - message type containing ionospheric correction terms in Multi-GNSS format.

☞ UBX-MGA-GLO-EPH - message type containing GLONASS ephemeris data for a single satellite in Multi-GNSS format.

☞ UBX-MGA-GLO-TIMEOFFSET - message type containing GLONASS Auxiliary Time Offset in Multi-GNSS format.

[1] GNSS Implementation and Aiding Features in u-blox wireless modules - UBX-13001849

[2] UBX Protocol Specification -

All these documents are available on our homepage (http://www.u-blox.com).

☞ For regular updates to u-blox documentation and to receive product change notifications please register on our homepage.

Revision history

Revision	Date	Name	Status / Comments
-	28/09/2010	rhou	Initial draft
	1/12/2010	rhou	Updated customer tags, added LLH coordinate support.
	13/12/2010	rhou	Informative appendix on harvesting function added.
	17/2/2010	rhou	UTRAN serving cell tag added. Informative appendix for testing added.
	5/08/2011	nhan	Major rework of document and additions for support of LISA 3G platform.
	19/08/2011	rrao	Updated interface for Last UTRAN Neighbouring Cell Before Radio Connected Tag and Last GSM Neighbouring Cell Before Radio Connected Tag
	26/09/2011	rrao	Added an GSMCLO example for 3 digit PLMN
	11/01/2013	rrao	Additions to support CDMA platform.
	25/09/2014	rrao	Major rework of the document. Inclusion of Multi-GNSS support and HTTP interfaces.
	25/09/2015	anda	Multi-hypothesis and elliptical uncertainty tags. LTE extension.
	21/04/2015	rrao	Details on Encryption of binary payload.
	17/05/2015	rrao	Updated encryption key size from 256 to 128, updated encryption procedure for uplink messages and added decryption of downlink response messages.

Contact

For complete contact information visit us at http://www.u-blox.com/en/contact-us.html