Harris Corporation
44965 Aviation Dr., Suite 400
Dulles, VA 20166

SBD DirectIP Specification

For use with the Enhanced Mobile Satellite Services Department of Defense Gateway

Version 3.0

1 February 2017

Revision History

Revision Number	*Release Date*	*Principal Contributors*	*Description*
1.0	**7/3/2006**	**SBD Design Group**	**Initial Release**
2.0	**5/24/2010**	**SBD Design Group**	**Assign MTMSN Disposition, MT LAC / Cell ID IE**
2.1	**5/24/2011**	**SBD Design Group**	**MO Confirmation Acknowledgement**
3.0	**2/1/2017**	**SBD Design Group**	**Document markings, MT Filter error codes**

Table of Contents

List of Tables

1 Introduction

1.1 Purpose

This document lays out the specification of how the DirectIP service is to be implemented. DirectIP is a socket-based delivery mechanism. The name references the basic concept used of directly connecting to a distant IP address for data delivery and reception.

1.2 Scope

This document is intended to serve as an interface control document between the GSS and the vendor applications. It is not intended to provide details of the DirectIP processing within the GSS.

1.3 Audience

This document is primarily intended for use by the engineers who are interfacing to the SBD service through the Department of Defense EMSS gateway.

1.4 Definitions

Message – The complete data transfer between the vendor application and GSS including a header, optional sets of information, and the payload to be transmitted over the air.

Payload – The actual data payload to be transmitted over the air.

2 DirectIP Concept of Operation

2.1 DirectIP Overview

DirectIP is the most efficient SBD data delivery option and provides the lowest delivery latency. It consists of a specialized socket-oriented communications protocol that utilizes direct connections between the DoD gateway SBD subsystem (GSS) and vendor server/client applications.

Like SBD processing of MO and MT e-mail messages, DirectIP is composed of separate MO and MT gateway components. The MO DirectIP component acts as a client to the vendor MO DirectIP server application. The MT DirectIP component acts as a server to the vendor MT DirectIP clients. In other words, the GSS MO component seeks to establish a connection to the vendor server for MO transfers while the GSS MT component actively listens for connections from the vendor clients for MT transfers. In either direction, clients only attach to the server when they are delivering data.

Both MO DirectIP and MT DirectIP protocols utilize bi-directional TCP/IP socket connections. These connections are unencrypted by default, but can use SSL/TLS when configured by vendor. The MO DirectIP protocol only delivers SBD MO messages from the GSS client to the vendor server, and no acknowledgement is expected from the server. In contrast, the MT DirectIP protocol delivers SBD MT messages from the vendor client to the GSS server, and a confirmation is passed from the server back to the client indicating the success or failure of the processing of the message.

The well-known unencrypted port on which the GSS MT server listens is 10800. The well-known unencrypted port to which the GSS MO client attempts to connect is also 10800. Therefore, the vendor MO server must listen on port 10800. The well-known SSL/TLS encrypted port on which the GSS MT server listens is 10900. The well-known SSL/TLS encrypted port to which the GSS MO client attempts to connect is also 10900. Therefore, the vendor MO server must listen on port 10900.

2.2 MO DirectIP Deliveries

Upon the completion of an SBD session between the SSD and the GSS, the GSS opens a socket, connects to the vendor application, and delivers the MO message including SBD session descriptors. Messages to the same vendor application are delivered in a first-in-first-out (FIFO) manner so that they are delivered in the same sequence that they are received. All other messages destined for the same vendor application will be queued behind the first message while it is being delivered. Only one message is delivered per socket connection. Once a socket connection is established, one MO message is delivered, and then the socket is closed. This sequence is repeated for every MO message queued for delivery to the vendor server.

SSDs delivering to a vendor server may be provisioned in the GSS to require an application layer acknowledgement, or confirmation message, from the server back to the gateway before the delivery is marked as Delivered. While extremely rare, it is possible that a message could be marked as Delivered in the SBD system, but the message was not received by the vendor. They may occur due to how operating systems and other network elements pass messages over TCP/IP. If a vendor uses the application layer acknowledgement, the SBD system connects and sends a message to the vendor server and waits for a timeout period for an confirmation message. If a confirmation message is received indicating success, the message is marked as Delivered. If the confirmation message is not received, is invalid, or indicates failure, the message is re-queued for delivery. The SSD must be provisioned to require confirmation

2.2.1 Vendor Application Server Unavailable

If the initial attempt to connect to the vendor application times out, the subsequent MO message delivery will not take place and subsequent connection attempts will be made. A retry scheme has been implemented to back off delivery attempts to unreachable servers. Retries will occur after 1, 5, 10, 20, 30, 60, 120, 240, and 360 seconds with the maximum of 360 seconds used for every retry thereafter. Connection attempts continue to be made for up to 12 hours. Each individual message has a lifetime of 12 hours starting at the time that the payload was received at the GSS. If it is not able to be delivered within this lifetime, it will be marked as "DirectIP_Timeout" in the SBD database and removed from the delivery queue.

As of the date of this document, up to 10,000 messages may be queued for a specific vendor application. If this limit is exceeded, payloads will be deleted from the front of the queue (the "oldest" payloads) and will be marked as "DirectIP_QueueOverflow" in the SBD database.

2.3 MT DirectIP Deliveries

When an MT message is to be delivered, the vendor application client opens a socket, connects to the GSS server, and delivers the MT message with disposition (see section 2.4). The GSS server then parses the message, inserts the payload into the database, and sends a confirmation message back to the vendor.

Once the GSS server has inserted the payload into the database, a different process within the GSS queues the payload for delivery and assigns an MTMSN to each. If the payload is the first in the queue, it is marked as "Queued" and is ready for immediate delivery. Otherwise, it is marked as "Pending".

2.4 MT Disposition Flags

Additional features related to MT deliveries have been introduced using MT DirectIP. These features are not intended to be made available through other means of receiving MT messages such as email. They are flagged using the MT disposition field in the MT header and are described in the following sections. The disposition field itself is a 2-byte bit map with 16 available flags. Those flags defined are shown in Table 5-9.

2.4.1 Flush MT Queue

When this flag is set, all payloads in the MT queue for the given IMEI will be deleted. This provides another means for a vendor to administer their MT queue.

When a payload is included in the MT message, it will be queued after the currently queued payloads, if any, are deleted. This enables a vendor to maintain a queue depth of one, overwriting any previous payload queued. Functionally, the GSS server will mark the currently queued payloads in the Downloads table as "Delete" and insert the new payload, if any, as "New".

2.4.2 Send Ring Alert – No MT Payload

When this flag is set, the GSS is directed to send a ring alert to the given SSD within the bounds of normal ring alert processing even though no new MT payload is being queued. The bounds refer to the SSD's ring alert enable flag and attach/detach status. If the ring alerts are enabled for this SSD, and it is attached (location is known), a ring alert will be triggered. If either of these conditions is not met, no ring alert will be sent, and the vendor will be notified via a status flag in the confirmation message. If a ring alert is sent, and an MT payload is already queued, that payload will be delivered. If an MT payload is included, the MT delivery will fail with a protocol error.

2.4.3 Update SSD Location (partially supported)

When this flag is set, the location of the SSD is updated in the SSD table of the database. A lat/lng pair or LAC/Cell ID pair must be included in the inbound message. If a lat/lng pair is provided, the LAC and Cell ID values must then be derived (this is not yet supported). When coupled with another flag triggering a ring alert, forced or not, the location will be updated first so that the ring alert is sent as directed.

2.4.4 High Priority Message (not yet supported)

When this flag is set, the delivered payload will be placed at the front of the MT queue for the given SSD. Any payload currently queued will be superseded, though not deleted.. If the SSD's queue is full at the time that the MT message is received (maximum queue depth is 50 payloads), the new payload will be rejected.

2.4.5 Assign MTMSN

When this flag is set, the GSS will use the value in the Unique ID field in the message header as the MTMSN for the associated MT message payload. Because the MTMSN is a 16-bit field, the Unique ID (a 32-bit field) must be between 1 to 65,535. Any value not in this range will cause the MT delivery to fail with an MTMSN out-of-range error.

The MTMSN normally used is an internally maintained value for each IMEI independent of all other IMEIs. When the assign MTMSN flag is not used, the GSS will use this value for the given IMEI incremented by one. When this flag is used, the assigned MTMSN only affects the associated MT message. The internally tracked value remains unchanged and will be used for all subsequent messages when the flag is not set.

3 MT and MO DirectIP Application Requirements

3.1 MO DirectIP Server/Client Requirements

3.1.1 MO GSS Client Requirements (No Application Layer Acknowledgement)

1. The client will seek to establish a TCP/IP socket connection to the IP address and port provisioned for the originating SSD. The connection will either be encrypted (SSL/TLS) or unencrypted based on the stored provisioning of the originating SSD.
2. If no connection is established, the client will implement the retry scheme outlined in section 0.
3. Once connected, the client will transmit the MO payload and close the socket connection.
4. Once the message has been transmitted, the client will close the socket connection. No acknowledgement from the server will be expected.

3.1.2 MO GSS Client Requirements (with Application Layer Acknowledgement)

1. The client will seek to establish a TCP/IP socket connection to the IP address and port provisioned for the originating SSD. The connection will either be encrypted (SSL/TLS) or unencrypted based on the stored provisioning of the originating SSD.
2. If no connection is established, the client will implement the retry scheme outlined in section 0.
3. Once connected, the client will transmit the MO payload.
4. Once the message has been transmitted, the client will wait for the server to send a confirmation message.
5. If the confirmation message is not received, is invalid, or indicates a failure, the client will implement the retry scheme outlined in section 0.
6. Upon receipt or timeout, the client will close the socket connection.

3.1.3 MO Vendor Server Requirements (No Application Layer Acknowledgement)

1. The server will listen for TCP/IP socket connections on port 10800 or the port set when the SSD is provisioned.
2. If the SSD was provisioned to use encryption, the server will need to employ SSL/TLS over the socket to perform the SSL handshake. This would be on a separate port form the unencrypted connection.
3. Once connected, the server will receive the entire MO message before parsing.
4. The server will allow the GSS client to close the socket connection.

3.1.4 MO Vendor Server Requirements (with Application Layer Acknowledgement)

1. The server will listen for TCP/IP socket connections on port 10800 (default) or the port set when the SSD is provisioned.
2. If the SSD was provisioned to use encryption, the server will need to employ SSL/TLS over the socket to perform the SSL handshake. This would be on a separate port form the unencrypted connection.
3. Once connected, the server will receive the entire MO message before parsing.
4. The server will transmit a confirmation message indicating success or failure.
5. The GSS client or server will close the socket connection. After sending the confirmation message, it is recommended that the server closes the connection.

3.2 MT DirectIP Server/Client Requirements

3.2.1 MT GSS Server Requirements

1. The server will listen for TCP/IP socket connections on port 10800.
2. If the SSD was provisioned to use encryption, the server will need to employ SSL/TLS over the socket to perform the SSL handshake. This would be on a separate port form the unencrypted connection.
3. Once connected, the server will receive the entire MT message before parsing.
4. The server will validate the message to ensure it meets the following criteria:
    a. IMEI is of a valid format and is provisioned
    b. All other input values in the MT header are valid
    c. Payload length does not exceed the prescribed maximum
    d. GSS resources are available (given SSDs MT queue, overall number of active MT users)
5. The server will send a confirmation message indicating the success or failure of processing the message.
6. The server will terminate the socket connection once the confirmation message is sent.
7. If the connection fails at any point prior to sending the confirmation message, the MT message will be dropped.

3.2.2 MT Vendor Client Requirements

1. The client will seek to establish a TCP/IP socket connection to the IP address of the GSS MT DirectIP server on port 10800.
2. If the SSD was provisioned to use encryption, the client will need to employ SSL/TLS over the socket to perform the SSL handshake. This would be on a separate port form the unencrypted connection.
3. Once connected, the client will transmit the MT payload and wait for the confirmation message.
4. Once the confirmation message has been received, the client will allow the server to close the socket connection.

4 MO and MT Message Specifications

4.1 Overall Message Structure

The overall message structure for both MO and MT DirectIP is shown in Table 4-1. When a connection is first established, the receiving application will receive three bytes. The first is a general DirectIP protocol revision number (this document describes revision 1). The following two bytes indicate the number of bytes that make up the body of the message that is made up of some number of information elements.

Table 4-1 Overall Message Format

Field Name	Length (bytes)	Range of Values
Protocol Revision Number	1	1
Overall Message Length	2	N
Information Elements Related to Message	N	See Section 5

4.1.1 Message Length

The message length value indicates the number of bytes that make up the body of the message being transferred following the initial three bytes. This enables the receiving end to know deterministically when all bytes transferred have been received. This is particularly relevant when multiple receives over the socket are required to read in the entire message.

4.1.2 Byte Alignment

The entire message transfer will be treated as a byte stream. Multi-byte fields are transmitted in network byte order (big-endian). For example, the four-byte field 0x0a0b0c0d will be transmitted as follows:

```
byte address     0        1        2        3
bit   offset  01234567 01234567 01234567 01234567
      binary  00001010 00001011 00001100 00001101
         hex     0a       0b       0c       0d
```

4.2 Information Elements

To maintain maximum flexibility within the protocol, all data to be transferred has been segmented into information elements (IEs). Those IEs currently defined are shown in detail in section 5. The general format of each IE is the same and is shown in Table 4-2.

Table 4-2 Information Element General Format

Field Name	Length (bytes)	Range of Values
Information Element ID (IEI)	1	See Table 5-1
Information Element Length	2	Variable
Information Element Contents	N	See Section 5

4.2.1 Information Element Identifiers

Each IE begins with a 1-byte information element identifier (IEI) that uniquely defines the following 2+N bytes. A complete list of the IEs and their associated IEIs is shown in Table 5-1.

4.2.2 Information Element Length

The two bytes following the IEI give the length of the IE in bytes following the initial three bytes. While the length for all currently defined IEs other than the MO and MT payloads may be represented with a 1-byte field, a 2-byte field is used for consistency across all IEs.

The primary goal for including the length field in every IE as a standard is to allow for new IEs in the future that may or may not be recognized by a vendor application based the vendor's upgrade path. If the application does not recognize an IE, it will know that it can read the next two bytes as a length and then skip that number of bytes before checking for the next IEI.

4.2.3 Parsing Information Elements

Once an entire message has been received, a parser will step through the bytes. The first will be an IEI followed by two bytes representing the number of bytes in the IE following the length. How to interpret these bytes is dictated by the IE type as indicated by the IEI. Once they are parsed, and if there are additional bytes received in the overall message, the next IEI may be checked, etc. If there are too many or too few bytes received as determined by the parser, the overall message will be dropped. For MT message processing, an error will be returned in the confirmation message.

4.3 Successful MO Message Delivery Example

Table 4-3 gives an example of a byte stream for a typical MO DirectIP message following a successful SBD session. Note that the SSD has been provisioned such that the geolocation information is not included in the message.

Table 4-3 MO DirectIP Message Delivery Example – Successful SBD Session

Field Name	Length (bytes)	Value
Protocol Revision Number	1	1
Overall Message Length	2	104
MO Header IEI	1	0x01
MO Header Length	2	28
CDR Reference (Auto ID)	4	1234567
IMEI	15	300034010123450
Session Status	1	0 (Transfer OK)
MOMSN	2	54321
MTMSN	2	12345
Time of Session	4	1135950305 (12/30/05 13:45:05)
MO Payload IEI	1	0x02
MO Payload Length	2	70
MO Payload	70	Payload Bytes

4.4 Failed MO Message Delivery Example

Table 4-4 gives an example of a byte stream for an MO DirectIP message following a failed SBD session due to an incomplete transfer. Note that no payload is included.

Table 4-4 MO DirectIP Message Delivery Example – Failed SBD Session

Field Name	Length (bytes)	Value
Protocol Revision Number	1	1
Overall Message Length	2	31
MO Header IEI	1	0x01
MO Header Length	2	28
CDR Reference (Auto ID)	4	1301567
IMEI	15	300034010123450
Session Status	1	13 (Incomplete Transfer)
MOMSN	2	54322
MTMSN	2	0
Time of Session	4	1135950325 (12/30/05 13:45:25)

4.5 MO Message Delivery Confirmation Example

Table 4-5 gives an example of an application layer acknowledgement, or confirmation, from the MO DirectIP vendor server.

Table 4-5 MO DirectIP Message Confirmation Example

Field Name	Length (bytes)	Value
Protocol Revision Number	1	1
Overall Message Length	2	4
MO Confirmation IEI	1	0x05
MO Confirmation Length	2	1
Confirmation Status	1	1

4.6 MT Message Delivery Example

Table 4-6 gives an example of a byte stream for a typical MT DirectIP message delivery.

Table 4-6 MT DirectIP Message Delivery Example

Field Name	Length (bytes)	Value
Protocol Revision Number	1	1
Overall Message Length	2	97
MT Header IEI	1	0x41
MT Header Length	2	21
Unique Client Message ID	4	“Msg1”
IMEI (User ID)	15	300034010123450
MT Disposition Flags	2	0x0000
MT Payload IEI	1	0x42
MT Payload Length	2	70
MT Payload	70	Payload Bytes

Table 4-7 shows one potential confirmation response. This example assumes that the given IMEI already had 49 MT message queued (max of 50).

Table 4-7 MT DirectIP Message Confirmation Example

Field Name	Length (bytes)	Value
Protocol Revision Number	1	1
Overall Message Length	2	28
MT Confirmation Message IEI	1	0x44
MT Confirmation Msg Length	2	25
Unique Client Message ID	4	“Msg1”
IMEI (User ID)	15	300034010123450
Auto ID Reference	4	58473
MT Message Status	2	50

5 Information Element Specifications

5.1 Information Element Identifiers

Table 5-1 summarizes the IEIs for the information elements passed within the DirectIP protocol.

Table 5-1 Information Elements

Information Element	IEI Value	Described In
MO Header IEI	0x01	Section 5.2
MO Payload IEI	0x02	Section 5.3
MO Lat / Lng Location Information IEI	0x03	Section 5.4
MO Confirmation IEI	0x05	Section 5.5
MT Header IEI	0x41	Section 5.6
MT Payload IEI	0x42	Section 5.7
MT Lat / Lng Location Information IEI	0x43	Section 5.8
MT Confirmation Message IEI	0x44	Section 5.10
MT LAC / Cell ID Location Information IEI	0x45	Section 5.9

5.2 MO DirectIP Header

The information in this header is required as part of every DirectIP MO message delivery. It includes all of the information necessary to uniquely identify the SBD MO message. It also includes the overall SBD session status and identifier (MTMSN) for the associated MT message delivery, if any.

Table 5-2 MO DirectIP Header IE

Field Name	Length (bytes)	Range of Values
MO Header IEI	1	See Table 5-1
MO Header Length	2	28
CDR Reference (Auto ID)	4	0 - 4294967295
IMEI	15	ASCII Numeric Characters
Session Status	1	See Table 5-3
MOMSN	2	1 – 65535
MTMSN	2	0 – 65535
Time of Session	4	Epoch Time

5.2.1 MO Header Length

This field specifies the number of bytes in the IE following this byte. Even though the length is fixed, the field is included as a standard across all IEs and to allow for maximum flexibility for future enhancements.

5.2.2 CDR Reference

Each call data record (CDR) maintained in the GSS Database is given a unique value independent of all other information in order to absolutely guarantee that each CDR is able to be differentiated from all others. This reference number, also called the auto ID, is included should the need for such differentiation and reference arise.

5.2.3 IMEI

The IMEI is the equipment identifier, unique to each Iridium field device, of the SSD originating the MO message. It is a 15-digit number represented here in ASCII format.

5.2.4 Session Status

This field provides an indication of success of the SBD session between the SSD and the GSS associated with the over-the-air payload delivery. The possible values are shown in Table 5-3. If the status was unsuccessful, no payload will be included in the MO message.

Table 5-3 SBD Session Status Values

Value	Description
0	The SBD session completed successfully.
1	The MO message transfer, if any, was successful. The MT message queued at the GSS is too large to be transferred within a single SBD session.
2	The MO message transfer, if any, was successful. The reported location was determined to be of unacceptable quality. This value is only applicable to SSDs using SBD protocol revision 1.
10	The SBD session timed out before session completion.
12	The MO message being transferred by the SSD is too large to be transferred within a single SBD session.
13	An RF link loss occurred during the SBD session.
14	An SSD protocol anomaly occurred during SBD session.
15	The SSD is prohibited from accessing the GSS.

5.2.5 MOMSN

This is the mobile-originated message sequence number (MOMSN) associated with the SBD session. This value is set by the SSD and transmitted to the GSS as part of every SBD session. It is incremented by the SSD after every successful session.

5.2.6 MTMSN

This is the mobile-terminated message sequence number (MTMSN) associated with the SBD session. This value is set by the GSS at the time that an MT message is queued for delivery and is unique to each SSD. It is then sent to the SSD as part of the MT payload transfer. If an MT payload transfer was attempted, the MTMSN will be included in the header regardless of the success of the session. If the session failed, the payload is still queued for delivery. If no MT delivery attempt was made in the session, this value will be zero.

5.2.7 Time of Session

This field provides a UTC timestamp of the SSD session between the SSD and the GSS in the format of an epoch time integer. The epoch time is the number of seconds since the start of the epoch at 1/1/1970 00:00:00.

Format: epoch time integer
Resolution: 1 second

5.3 MO Payload

This information element includes the actual MO payload delivered from the SSD to the GSS during the SBD session identified in the header. In an MO message delivery related to an empty mailbox check (EMBC) session or a failed session, no payload will be included.

Table 5-4 MO Payload IE

Field Name	Length (bytes)	Range of Values
MO Payload IEI	1	See Table 5-1
MO Payload Length	2	1 – 1960
MO Payload	1 – 1960	Payload Bytes

5.3.1 MO Payload Length

This field indicates the number of the bytes in the MO payload.

5.3.2 MO Payload

This is the actual content of the MO payload. The MO payload size is generally limited to 1960 bytes and is limited to 340 bytes on some SBD-only devices (e.g. commercial 9601).

5.4 MO Latitude / Longitude Location Information

The location values included in this IE provide an estimate of the originating SSD's location in latitude and longitude coordinates. The inclusion of this information in an MO message delivery is optional. Whether or not it is included is established when the SSD is provisioned and may be changed at any time via the SBD Web Pages. The CEP radius provides the radius around the center point within which the unit is 90% probable to be located.

Table 5-5 MO Location Information IE

Field Name	Length (bytes)	Range of Values
MO Location Information IEI	1	See Table 5-1
MO Location Info Length	2	11
Latitude / Longitude	7	See Table 5-6
CEP Radius	4	1 – 2000

5.4.1 MO Location Information Length

This field specifies the number of bytes in the IE following this byte. Even though the length is fixed, the field is included as a standard across all IEs and to allow for maximum flexibility for future enhancements.

5.4.2 Latitude / Longitude

The latitude and longitude provide a center point of the estimated location and are derived from the LGC coordinates output from the CPLD exchange during the SBD session. The coordinates are sent using the format shown in Table 5-6.

Table 5-6 Location Data Format

Location Data Format									
MSB Bit Position LSB								Byte Number	Description & Allowed Values
0	1	2	3	4	5	6	7		
Reserved				Format Code		NSI	EWI	1	Reserved & Format Code: 0 (all other values are reserved) NSI: North/South Indicator (0=North, 1=South) EWI: East/West Indicator (0=East, 1=West)
Latitude (degrees)								2	Decimal Range: 0 to 90 Hex Range: 0x00 to 0x5A
Latitude (thousandths of a minute, MS-Byte)								3	Decimal Range: 0 to 59,999 (unsigned integer, American notation) Hex Range: 0x0000 to 0xEA5F
Latitude (thousandths of a minute, LS-Byte)								4	
Longitude (degrees)								5	Decimal Range: 0 to 180 Hex Range: 0x00 to 0xB4
Longitude (thousandths of a minute, MS-Byte)								6	Decimal Range: 0 to 59,999 (unsigned integer, American notation) Hex Range: 0x0000 to 0xEA5F
Longitude (thousandths of a minute, LS-Byte)								7	

5.4.3 CEP Radius

The CEP radius provides the radius around the center point within which the SSD is located with a 90% probability of accuracy.

Resolution: 1 km

5.5 MO Confirmation Message

This IE forms the application layer acknowledgement, or confirmation, that may optionally be returned from the MO DirectIP vendor server to the GSS. If the SSD is provisioned to enable confirmation, this message must be returned to the GSS for the delivery to be successful. See section 2.2 for more information and section 4.5 for an example message.

Table 5-7 MO DirectIP Confirmation Message

Field Name	Length (bytes)	Range of Values
MO Confirmation IEI	1	See Table 5-1
MO Confirmation Length	2	1
Confirmation Status	1	1 (Success) or 0 (Failure)

5.6 MT DirectIP Header

The information in this header is required as part of every DirectIP MT message delivery.

5.6.1 MT Header Length

This field specifies the number of bytes in the IE following this byte. Even though the length is fixed, the field is included as a standard across all IEs and to allow for maximum flexibility for future enhancements.

Table 5-8 MT Header IE

Field Name	Length (bytes)	Range of Values
MT Header IEI	1	See Table 5-1
MT Header Length	2	21
Unique Client Message ID	4	From client (not MTMSN)
IMEI (User ID)	15	ASCII Numeric Characters
MT Disposition Flags	2	See Table 5-9

5.6.2 Unique Client Message ID

The vendor client will include a 4-byte message ID unique within its own application. If the Assign MTMSN disposition flag is not set, this value is not used in any way by the GSS server except to include it in the confirmation message sent back to the client. If the Assign MTMSN flag is set, the value will be used as the MTMSN for the associated MT message payload. See section 2.4.5 for details..

5.6.3 IMEI

The IMEI is the equipment identifier, unique to each Iridium field device, of the MT message destination SSD. It is a 15-digit number represented here in ASCII format.

5.6.4 MT Disposition Flags

These flags are set by the vendor client to trigger particular actions by the GSS. Combinations of flags are allowed. The field is a 2-byte bit map with 16 available flags. Those defined are shown in Table 5-9. Each defined flag is described in detail in section 2.4.

Table 5-9 MT Disposition Flags

Disposition Flag	Value	Description
Flush MT Queue	1	Delete all MT payloads in the SSD's MT queue
Send Ring Alert – Mo MTM	2	Send ring alert with no associated MT payload (normal ring alert rules apply)
Update SSD Location	8	Update SSD location with given lat/lng values
High Priority Message	16	Place the associated MT payload in front of queue
Assign MTMSN	32	Use the value in the Unique ID field as the MTMSN

5.7 MT Payload

This information element includes the actual MT payload to be queued and delivered over the air to the destination SSD. This inclusion of this IE in the MT delivery is optional based on the disposition flags included in the header.

Table 5-10 MT Payload IE

Field Name	Length (bytes)	Range of Values
MT Payload IEI	1	See Table 5-1
MT Payload Length	2	1 – 1890
MT Payload	1 – 1890	Payload Bytes

5.7.1 MT Payload Length

This field indicates the number of the bytes in the MT payload.

5.7.2 MT Payload

This is the actual content of the MT payload. The MT payload size is limited to 1890 bytes for 9505[A] and 9522[A] SSDs. The size is limited to 270 bytes for non-customized SBD-only devices (e.g. 9601).

5.8 MT Latitude / Longitude Location Information (not yet supported)

The location values included in this IE provide the location of the destination SSD in latitude and longitude coordinates. The inclusion of this information in an MT message delivery is optional, but is expected when the Update SSD Location disposition flag is set in the MT header. When this flag is set and the location is included, the location of the SSD in the SBD database is updated based on the given values. If the location is included, but the flag is not set, the location will be ignored.

The location is given as a pair of latitude and longitude coordinates. These must be converted to LAC and Cell ID values before updating the SBD database.

Table 5-11 MT Location Information IE

Field Name	Length (bytes)	Range of Values
MT Location Information IEI	1	See Table 5-1
MT Location Info Length	2	7
Latitude / Longitude	7	See Table 5-6

5.8.1 MT Location Information Length

This field specifies the number of bytes in the IE following this byte. Even though the length is fixed, the field is included as a standard across all IEs and to allow for maximum flexibility for future enhancements.

5.8.2 Latitude / Longitude

The latitude and longitude provide the location of the SSD from which the LAC and Cell ID will be derived. The coordinates are sent using the format shown in Table 5-6.

5.9 MT LAC / Cell ID Location Information

The location values included in this IE provide the location of the destination SSD by LAC and Cell ID. The inclusion of this information in an MT message delivery is optional, but is expected when the Update SSD Location disposition flag is set in the MT header. When this flag is set and the location is included, the location of the SSD in the SBD database is updated based on the given values. If the location is included, but the flag is not set, the MT delivery will fail with a protocol error.

Table 5-12 MT LAC / Cell ID Location Information IE

Field Name	Length (bytes)	Range of Values
MT Lat/Lng Location Infor IEI	1	See Table 5-1
MT Lat/Lng Location Info Length	2	4
LAC (Location Area Code)	2	0 – 65,535
Cell ID	2	0 – 65,535

5.9.1 MT Location Information Length

This field specifies the number of bytes in the IE following this byte. Even though the length is fixed, the field is included as a standard across all IEs and to allow for maximum flexibility for future enhancements.

5.9.2 LAC

The LAC (location area code) is a value that provides an unambiguous identification of geographic location on a worldwide basis. It is an estimate of where the subscriber is actually located and is used in the ring request message which in turn prompts an over-the-air ring alert notification.

5.9.3 Cell ID

The Cell ID is a value that provides refinement of the location given in the LAC. Essentially, it is a sub-LAC value and is used in the ring request message which in turn prompts an over-the-air ring alert notification.

5.10 MT Message Confirmation Message

A confirmation message indicating the status of the processing of the MT message is sent to the vendor client from the GSS for every MT message received.

Table 5-13 MT Confirmation Message IE

Field Name	Length (bytes)	Range of Values
MT Confirmation Message IEI	1	See Table 5-1
MT Confirmation Msg Length	2	25
Unique Client Message ID	4	From Client (not MTMSN)
IMEI (User ID)	15	ASCII Numeric Characters
Auto ID Reference	4	0 – 4294967295
MT Message Status	2	Order of message in SSD's queue or error reference (see Table 5-14)

5.10.1 MT Confirmation Message Length

This field specifies the number of bytes in the IE following this byte. Even though the length is fixed, the field is included as a standard across all IEs and to allow for maximum flexibility for future enhancements.

5.10.2 Unique Client Message ID

This field is the unique client IE sent in the MT header in the message sent to the GSS. This is intended to serve as a form of validation and reference for the client application.

5.10.3 IMEI

The IMEI is the equipment identifier, unique to each Iridium field device, of the MT message destination SSD. It is a 15-digit number represented here in ASCII format.

5.10.4 Auto ID Reference

This value provides a unique reference for identifying the MT payload within the SBD database. It is assigned at the time that the payload is inserted into the database as a new record, but prior to the record being queued for delivery and the MTMSN is assigned. This reference is passed instead of the MTMSN in order for the GSS server to remain independent of all other GSS processes and to allow the socket connection to be closed as soon as possible. This value will be zero when there is an error in processing the message.

5.10.5 MT Message Status

This field is the status value that is returned with every confirmation indicating that the overall MT message was received and validated and that the payload was queued successfully or that a failure occurred. If successful, the value is a positive number indicating the order of the received payload in the associated SSD's MT message queue. If not successful, the value will be a negative number serving as an error code specifying the problem detected. Table 5-14 shows the possible status values including the error codes. Note that the last two error values (-8 and -9) only apply when the "Send Ring Alert" disposition flag has been set.

Table 5-14 MT Message Status

Status	Description
1 – 50	Successful, order of message in the MT message queue
0	Successful, no payload in message
-1	Invalid IMEI – too few characters, non-numeric characters
-2	Unknown IMEI – not provisioned on the GSS
-3	Payload size exceeded maximum allowed
-4	Payload expected, but none received
-5	MT message queue full (max of 50)
-6	MT resources unavailable
-7	Violation of MT DirectIP protocol
-8	Ring alerts to the given SSD are disabled
-9	The given SSD is not attached (not set to receive ring alerts)
-10	Source address rejected by MT filter
-11	MTMSN value is out of range (valid range is 1 – 65,535)
-12	Client SSL/TLS certificate rejected by MT filter

6 Acronyms

The following is a list of SBD and iridium-related acronyms.

CDR	Call Detail Record
CEP	Circular Error Probability
CIOSD	Change ISU Outbound Signaling Destination
CPLD	Call Processing Location Determination
CRC	Cyclical Redundancy Check
DMO	MO DirectIP Process (DirectMO)
DMT	MT DirectIP Process (DirectMT)
GSS	Gateway SBD Subsystem
GW	Gateway
ICD	Interface Control Document
IE	Information Element
IEI	Information Element Identifier
IMEI	International Mobile Equipment Identifier
IP	Internet Protocol
ISU	Iridium Subscriber Unit
LAC	Location Area Code
LBT	L-Band Transceiver
LGC	Location Grid Code
MO	Mobile Originated
MOMSN	Mobile Originated Message Sequence Number
MT	Mobile Terminated
MTMSN	Mobile Terminated Message Sequence Number
SBD	Short Burst Data
SMTP	Simple Mail Transfer Protocol
SSD	SBD Subscriber-Device
SSL	Secure Socket Layer
TAC	Type Acceptance Code
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
VA	Vendor Application