NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2 Interface

12/02/03

NENA-05-001 December 2003 (Original)

NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2 Interface

Prepared by:

National Emergency Number Association (NENA) Technical Committee Chairs

Published by NENA

Printed in USA

NENA STANDARDS

NOTICE

This NENA STANDARD is published by National Emergency Number Association (**NENA)** as a guide for the designers and manufacturers of systems that are used for the purpose of processing emergency calls. It is not intended to provide complete design specifications or parameters nor to assure the quality of performance of such equipment.

NENA reserves the right to revise this NENA STANDARD for any reason including, but not limited to, conformity with criteria or standards promulgated by various agencies, utilization of advances in the state of the technical arts or to reflect changes in the design of equipment or services described herein.

It is possible that certain advances in technology will precede these revisions. Therefore, this NENA STANDARD should not be the only source of information used. **NENA** members are advised to contact their Telecommunications Carrier representative to ensure compatibility with the 9-1-1 network.

Patents may cover the specifications, techniques or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document is not to be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

This document has been prepared solely for the voluntary use of E9-1-1 Service System Providers, network interface and system vendors, participating telephone companies, etc..

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Technical Committee has developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association

1700 Diagonal Rd, Suite 500

Alexandria, VA 22314

202.466.4911

or commleadership@nena.org

Acknowledgments:

This document has been developed by the National Emergency Number Association (NENA) Wireless Technical Committee (and the Network Technical Committee).

The following industry experts and their companies are recognized for their contributions in development of this document.

Members:	**Company**
Tom Breen – NTC Chair	Bell South
Bob Sherry	Intrado
Pete Schmidt	Intrado
Tim Dunn	Openwave
Atul Thaper	Telcordia
Terry Reese	Telcordia
Ketan Parekh	Intrado

TABLE OF CONTENTS

1 Executive Overview

1.1 Purpose and Scope of Document

This "NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2 Interface" document provides explicit protocols and parameters for interoperable operation of the E2 interface over TCP/IP. [1]This interface is between the MPC/GMLC and the EMSE as defined in TR45.2's TIA/EIA/J-STD-036-A . This document defines the methods that MPC/GMLC and ESME use to interact, allowing for the concept of geographically redundant nodes and the inherent link management. It defines how the TCAP-based application protocol is to be encapsulated upon the TCP/IP stack.

1.2 Reason to Implement

While TIA/EIA/J-STD-036-A defined parameters for the E2 interface, it did not provide sufficient detail to allow vendors to implement the E2 interface and assure interoperability. This interface is required for the implementation of Wireless Phase 2, and, with the addition of the Location Description parameter, supports the necessary fall back to Phase 1 when Phase 2 data is unavailable.

1.3 Benefits

The use of this standard by equipment vendors will facilitate the implementation of the E2 interface between the wireless network and an ESME. It assures that vendors implement the parameters, TCAP, TCP/IP and link management in a consistent manner which will aide in the interoperability of the network elements as each vendor and their associated carriers roll out Wireless Phase 2. This document specifies implementation details not specified in TIA/EIA/J-STD-036-A down to explicit elements so that there can be no confusion regarding how parameters are to be implemented.

1.4 Operational Impacts Summary

This standard must be implemented on each associated network element (MPC, GMLC and ESME) and provisioned by the hosting carrier. TCP/IP connectivity between the network elements should be accomplished based upon best practices for network interconnection and in line with specific guidelines adopted by each carrier.

[1] In this document the use of the term E2 is in most ways synonymous with the defacto term E2+, although E2+ is not yet documented in TR45.2's TIA/EIA/J-STD-036-A.

1.5 Document Terminology

The terms "shall ", "must " and "required" are used throughout this document to indicate required parameters and to differentiate from those parameters that are recommendations. Recommendations are identified by the words "desirable" or "preferably".

1.6 Reason for Issue

This document was developed by NENA to assure that vendors who develop to TR45.2's E2 interface have a reference document for implementation.

1.7 Reason for Reissue

NENA reserves the right to modify this document. Whenever it is reissued, the reason(s) will be provided in this paragraph.

This is the first release of this document.

1.8 Date Compliance

All systems that are associated with the 9-1-1 process shall be designed and engineered to ensure that no detrimental, or other noticeable impact of any kind, will occur as a result of a date/time change up to 30 years subsequent to the manufacture of the system. This shall include embedded application, computer based or any other type application.

To ensure true compliance the manufacturer shall upon request provide verifiable test results to an industry acceptable test plan such as Telcordia GR-2945 or equivalent.

1.9 Anticipated Timeline

The implementation of this standard is currently completed or underway by the major vendors. In order to assure timely deployment this standard has been distributed to the vendor community in draft form and vendors have provided significant input into the completion of the document. Each vendor is expected to provide their own schedule for implementation but it is anticipated that this interface is a significant component to the roll out of Wireless Phase 2.

1.10 Costs Factors

The implementation of the E2 interface is an incremental component to the network elements used in Phase 2. In order to implement this interface, appropriate steering links are required between the associated network elements along with associated TCP/IP routers and affiliated equipment.

1.11 Cost Recovery Considerations

Normal business practices shall be assumed to be the cost recovery mechanism.

1.12 Acronyms/Abbreviations

See NENA Master Glossary of 9-1-1 Terminology located on the NENA web site for a complete listing of terms used in NENA documents.

2 Technical Description

While the TIA/EIA/J-STD-036-A Emergency Services Position Request and Response uses a TCAP message format, this implies to some that SS7 is the transport and interconnection methodology. However, this does not appear to be viable (or what was intended by the 9-1-1 industry during the standards development) given that virtually none of the 9-1-1 ALI systems in place today are SS7 capable and that TCP/IP is a more appropriate transport protocol.

While SS7 is in limited use today for routing E9-1-1 voice traffic, it is not in use for the purpose of retrieving data from an Automatic Location Identification (ALI) database to get address or position data about the 9-1-1 caller. Because of this, the ALI systems have not had a need to support a message directly from the SS7 network and do not incorporate the hardware or software to support SS7 messaging. Most of the ALI/(Emergency Services Message Entity) ESME systems in the field today do not have the capability of being upgraded to support SS7 connectivity.

ALI hosts do, however, have redundant, high availability TCP/IP connectivity available today in almost all cases. TCP/IP connections are in use today for connectivity to the Public Safety Answering Point (PSAP), interconnection with peer ALI hosts, remote monitoring, administration and provisioning.

Given this situation, the E2 interface connectivity should be TCP/IP based, utilizing a Transaction Capability Application Part (TCAP)-based application protocol.

The ESMEs normally operate in a redundant, geographically distributed configuration. The MPCs (Mobile Positioning Centers) (may or may not be configured as redundant nodes. Note that this interface specification also applies to Global Mobile Location Centers (GMLC), however, MPC is used in this document for simplicity. This E2 interface must be able to handle queries and responses for these various network configurations. That is, both ESMEs must be capable of querying both MPCs in a network configuration where both operate as redundant nodes.

3 TCP/IP Protocol Stack

Figure 1 replicates the TCP/IP protocol stack for the E2 interface described in Figure G-2 of TIA/EIA/J-STD-036-A-A. This figure illustrates the direct encapsulation of the TCAP ASN.1 encoded messages described in Chapter 7 of TIA/EIA/J-STD-036-A-A within TCP/IP packets, without additional layers of encoding. IP provides the capability to route the message, which replaces the need for the Signaling Connection Control Part (SCCP) portion of the standard SS7 message. The intervening network elements (e.g. routers and firewalls) need only use IP to correctly route the session set up message and subsequent packets.

IP provides a connectionless, “best-effort” delivery service. IP’s responsibilities include the transmission of a block of data received from upper layers as well as the message addressing. The combination of an IP header preceding a block of data constitutes a datagram. If a link layer failure occurs during datagram transmission, IP's behavior rules do not specify that the datagram be resent.

The transport layer (e.g., TCP) is responsible for this datagram retransmission functionality. TCP provides a reliable, connection-oriented, byte stream, transport layer service. It provides the reliability by performing the following functions:

1. Resizing application layer packets into the proper buffers for the network layer,
2. Sending acknowledgments for each block of data received,
3. Retransmitting unacknowledged data blocks,
4. Making sure that the transmitted packets are received through the use of acknowledgement timers,
5. Maintaining a checksum for the header and data,
6. Discarding duplicate blocks of data, and
7. Providing flow control that prevents a faster host from overrunning a slower one.

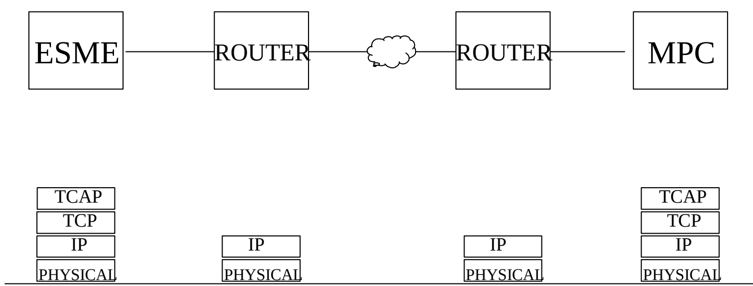

Figure 1

4 Network Architecture

Figure 2 below, represents the data network architecture between the wireless network and the wireline network to allow the caller's location to be returned to the PSAP. Each PSAP has links to both of the mated, geographically distributed ESMEs. For the interconnection between the MPC and ESME, three different configurations are anticipated.

The first is the Simplex Node configuration. In this configuration the MPC is a Simplex Node. Both ESMEs connect to a high availability MPC deployed in the wireless network over Links A and C. Both ESMEs will steer queries to the single MPC.

The second is the Redundant Node configuration. In this configuration each ESME will have a companion MPC with which it communicates (Links A and D). Each ESME will steer queries to its companion MPC.

The third is the Full Redundancy configuration. In this configuration, the ESME complex and the MPC complex are fully connected (Links A, B, C, D). Therefore, each ESME has a logical TCP/IP connection to both MPCs. The ESMEs will have an alternate destination to query if the query to the primary destination fails.

The network connection between the Emergency Service Provider and the Wireless Carrier is expected to be either a private packet-based network or a dedicated point-to-point environment.

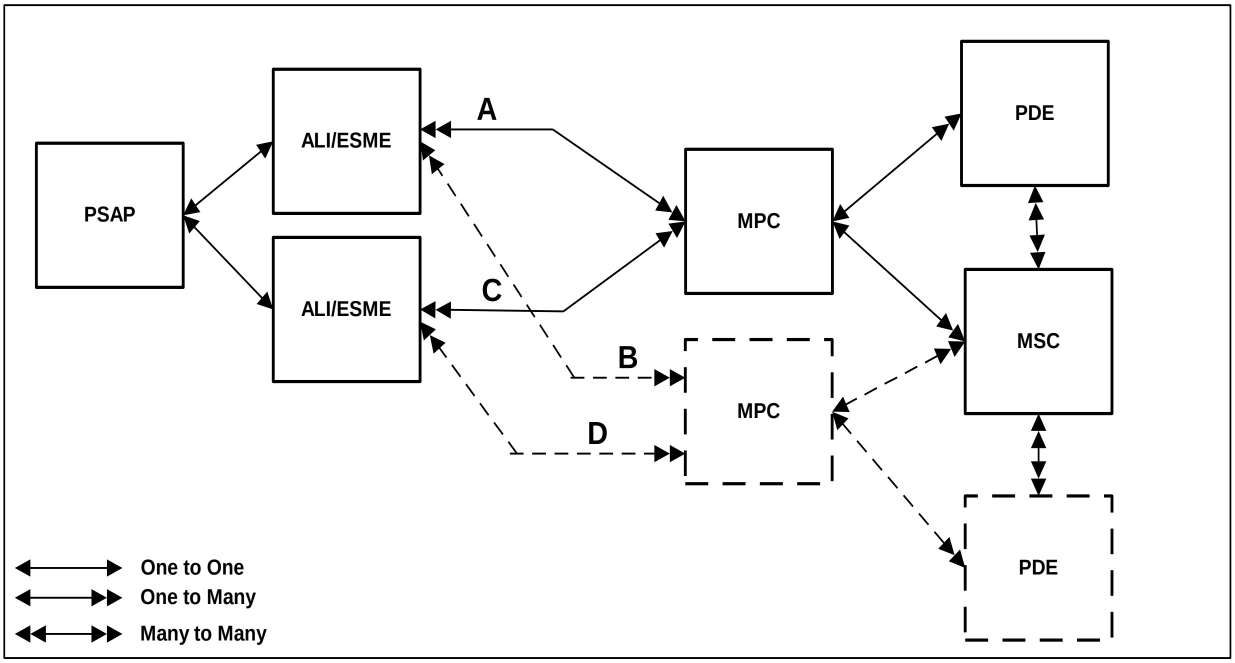

Figure 2: Wireless E9-1-1 Entities Diagram

4.1 Simplex Node

In the simplex node configuration (links A, C in Figure 2), the MPC Node processes all origination requests from the MSC. It coordinates the process of locating the mobile subscriber through a sequence of messages to the PDEs. The ESMEs, always assumed to operate in a mated configuration, will have TCP/IP sessions to this MPC Node.

As described in the call flows in Section 6, either one or both ESMEs will query this MPC Node. If the query is for Selective Routing instructions, only one ESME may query the MPC node. If the query is originated by a PSAP, both ESMEs may query the one MPC. If a single MPC receives the same query from two different ESMEs, the MPC will either a) return the Position Information to the ESME that it received the query from first and ignore the second query; or b) process both queries as if they are separate requests. If the MPC processes both queries as if they are separate requests, the PSAP may see duplicate responses.

In this configuration, if the MPC is out of service, the ESMEs will not receive a response to their queries. If one link is out of service, and both ESMEs queried the MPC Node, the ESME that receives the response will process it, and the PSAP will receive a single response. If only one ESME attempts to query the MPC Node and the link between it and the MPC Node is not available, the ESME will receive no response. This will result in the PSAP not receiving the Position Information, or the Selective Router routing the call based on an ESRD.

4.2 Redundant Node

In the Redundant Node configuration (links A, D in Figure 2) the MPC operates in a dual node configuration. The nodes may operate load sharing where they alternately service requests from the MSC or in a active standby configuration where one MPC Node services all requests from the MSC and the other node is activated only when there is a problem with the primary node. The ESMEs and MPCs have a one to one relationship. ESME A is connected to MPC A and ESME B is connected to MPC B.

As described in the call flows in Section 6 either one or both ESMEs will query its companion MPC Node. If the query is for Selective Routing instructions, only one ESME may query its companion MPC Node. If the query is originated by a PSAP, both ESMEs may query their companion MPC Node. If both MPCs receive the same query, the MPCs may negotiate to determine which MPC will send the response to the query and that system returns the Position Information to the ESME, or both queries will be processed as separate requests.

In this configuration, if one MPC Node is out of service, the ESME communicating with that node will not receive a response to its query. This is also true if the link between the ESME and its companion MPC Node is not available. If both ESMEs queried the associated MPC Nodes, and only one node responds, the ESME that receives the response will process it. If only one ESME attempts to query the MPC Node and the link between it and the MPC Node is not available the ESME will receive no response. This will result in the PSAP not receiving the Position Information or the Selective Router routing a call based on an ESRD.

4.3 Full Redundancy

In the Full Redundancy configuration (links A, B, C and D in Figure 2) there is a link between each ESME and each MPC. The MPC operates in a dual node configuration. The nodes may operate load sharing where they alternately service requests from the MSC or in a active standby configuration where one MPC Node services all requests from the MSC and the other node is activated only when there is a problem with the primary node.

As described in the call flows in Section 6 either one or both ESMEs will query the MPC Nodes. If the query is for Selective Routing instructions, only one ESME may query both MPC Nodes. If the query is originated by a PSAP, both ESMEs may query both MPC Nodes. If the MPC responds on one link, the ESME that receives the response will respond to the PSAP. If both ESMEs receive responses they will each respond with one response.

In this configuration, if one MPC Node is out of service, both ESME still have connections to the mated MPC Node. Therefore, it would require two failures in the network before the ESME complex would not receive a response to a query.

5 Session Establishment

In this configuration, the TCP/IP address and port are agreed upon between the owners of the ESME and the MPC. By convention, the ESME is the TCP/IP server and the MPC is the TCP/IP client. The sessions are established via sockets where the MPC establishes the connection to the ESME. Upon system start up, the ESME will listen to the designated port and the MPC will initiate session set up to the designated TCP/IP address and port. Once the socket session is established, the application may begin the query and response handshake.

6 Emergency Service Protocol (ESP) Messages

The ESP query has two formats, identified here as Format A and Format B. For Format A, the Emergency Service Routing Key (ESRK) is passed in the query. For a Format B message the Callback Number (CBN) and, optionally, the Emergency Service Routing Digits (ESRD) are passed. Parameters of ESME Identification and Position Request Type are sent for both formats of messages. For the ESP response, the salient information is the CBN and Location. Once the ESME receives these, it will format them with a local ALI record associated with the ESRK/ESRD and return the information to the PSAP.

In addition to query and response, there will be heartbeat messages between the ESME and the MPC to verify the integrity of the links. These will be initiated by the ESME and responded to by the MPC. The ESME will query with the PositionRequestType=4 (Test) and the EmergencyServiceRoutingKey=0. The MPC should respond with the PositionResult=0A (Test). These messages only will be sent during periods of inactivity of 60 seconds (a configurable parameter) on a link to verify the integrity of the application and socket connection.

7 ESP Queries and Responses

The MPC may expect queries from the ESME for two situations. The first is when the Selective Router queries the ESME and the second is when the PSAP queries the ESME.

Some ESME systems have specific software to aid the Selective Router in routing the call to the correct PSAP. In this situation, the ESME may query the MPC for position prior to returning routing instructions to the Selective Router. The Selective Router treats the links to the mated ESME systems as active/standby. That is, the Selective Router only queries one ESME for routing instructions. Therefore, only the ESME that receives the request from the Selective Router may query the MPC complex. The query may be either a Format A or Format B query, but the most likely case is a Format B query with both Callback Number and ESRD.

An example of this scenario is shown in Figure 3 below. This flow follows that of Figure 4-5 in TIA/EIA/J-STD-036-A. The sequence of locating the Mobile Station (MS or handset) position is not shown in this flow. The MSC queries the MPC with the Cell Site and Sector (CS&S) and Callback Number (CBN) to retrieve the Emergency Services Routing Digit (ESRD) associated with the Cell Site and Sector of where the call originated (1). The MPC returns the ESRD to the MSC (2). The MSC routes the call toward the Emergency Service Network Entity (ESNE or Selective Router) selected by the ESRD and passes CBN and ESRD (3). The ESNE queries one of the ESMEs (ESME B) for routing instructions using CBN and ESRD (4). ESME B queries both MPCs for which it has TCP/IP sessions established with a Format B query (CBN and ESRD) (5). One MPC responds to ESME B with the Position Information (6). The ESME uses the Position Information to determine routing instructions for the ESNE and passes back to the ESNE an Emergency Service Number (ESN) (7). The ESNE delivers the call to the PSAP passing the CBN and potentially the ESRD (8). The PSAP queries both ESMEs with the CBN (9). ESME B, having the Position Information, returns it in the response to the PSAP

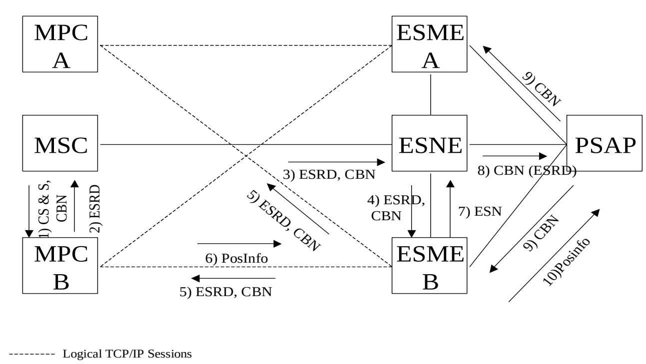

Figure 3 Query for Selective Routing

The second situation is when the PSAP queries the ESME based upon the delivery of the Emergency Service Call to that PSAP. The PSAP queries the ESME and in turn the ESME queries the MPC for the location data. The ESME may query the MPC with either a Format A or Format B query depending upon what information is available to the ESME. For example, if the MSC sent both CBN and ESRD in the SS7 Initial Address Message (IAM) message to the ESNE, it is likely that the ESME will query the MPC with both. If the MSC sent only ESRK in the call set up to the ESNE, the ESME will query with Emergency Service Routing Key (ESRK).

For the first query, called (initial) query, from the PSAP, the ESME will query the MPC with request type of initial. If the ESME can discern that the PSAP has issued a repeat (update) query, the ESME will query the MPC with either the request type of updated or updated or last. The most likely case is "updated or last" to allow the PSAP to receive the last known location if a new location cannot be provided by the location equipment.

An example of this flow is shown in Figure 4 below. This flow follows that of Figure 4-8 in TIA/EIA/J-STD-036-A where ESRK is passed. The MSC queries the MPC with the Cell Site and Sector (CS&S) and Callback Number (CBN) to retrieve the Emergency Services Routing Key (ESRK) assigned to this call (1). The MPC returns the ESRK to the MSC (2). The MSC routes the call toward the PSAP via the ESNE selected by the ESRK (3). Using the ESRK as an index into static tables to determine routing, the ESNE routes the call to the PSAP [These tables may be resident in the ESNE or the ESNE may query the ESME.] (4). It passes only ESRK to the PSAP. The PSAP queries both ESMEs with the ESRK (5).

There are two options as to how the ESMEs query the MPC Complex (6).

1. Both Mode. Both ESMEs query the MPCs to which it has a TCP/IP session established (6). (Figure 4)
2. Primary Mode. ESME A queries the MPC to which it has a TCP/IP session established (6). (Figure 5) If there is a failure, ESME A queries the other mated MPC to which it has a TCP/IP session established (6).

There are three options for the MPC to respond to the ESME with the Position information (7).

1. When both MPCs receive queries from the ESMEs , the MPCs may negotiate to determine which MPC will send a single response to the queries and that system returns the Position Information to the ESME (7). The MPCs acknowledge the other queries by responding with the PositionResult=07 (Inactive)(8). If the MPCs do not negotiate then each MPC will treat each query as a separate request (not shown in the figure).
2. When only one MPC receives the query, the MPC that receives the request from an ESME, responds with the Position Information to the ESME (7).
3. When a single MPC receives the same query from two different ESMEs, the MPC may return the Position Information to the ESME that it received the query from first. The query from the second ESME may be ignored. The MPC acknowledges the other query

by responding to the other ESME with the PositionResult=07 (Inactive)(8). Alternatively the MPC may treat each request as separate query and processes it as such.

In the example of Figure 4, the ESME that received the response from the MPC returns the Position Information to the PSAP (9). If both ESMEs receive a Position Information response from an MPC, there is a potential that both ESMEs may respond to the PSAP.

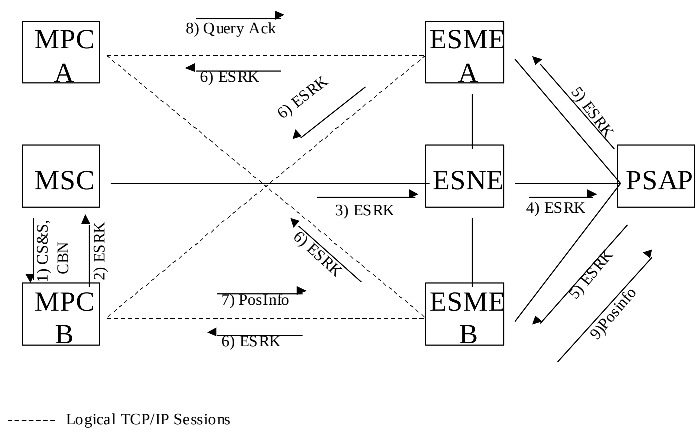

Figure 4 Both Mode Query

An example of Primary Mode query is shown in Figure 5 below. This follows that of Figure 4-8 in TIA/EIA/J-STD-036-A where ESRK is passed.

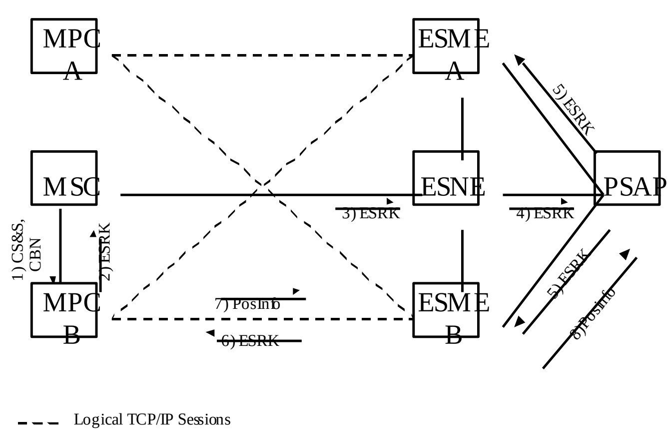

Figure 5 – Primary Mode Query

When installing Phase II functionality at the PSAP, the PSAP may request to test the path between the PSAP and the MPC as well as having test coordinates returned from the MPC to project on the PSAP's boundary map. The PSAP can do this by doing a manual query and sending the test ESRK to both ESMEs (1). The ESME will query the MPC with Format A message with the ESMEIdentification, PositionRequestType=4 (test), a test ESRK specifically configured on the MPC for the PSAP.

If there is no query and response activity between the ESME and the MPC for a period of time, the ESME will send a heartbeat over that link (session) and expect the MPC to respond. This assures that, at the application level, the session is still established. A lack of heartbeat response will cause the ESME to take recovery actions.

An example of the heartbeat is shown in Figure 6 below. This flow follows that of Figure 4-7 in TIA/EIA/J-STD-036-A. The ESME formats and sends an Emergency Services Protocol message with the PositionRequestType=4 and EmergencyServiceRoutingKey=0 (1). The MPC response contains a PositionResult=0A(test)(2).

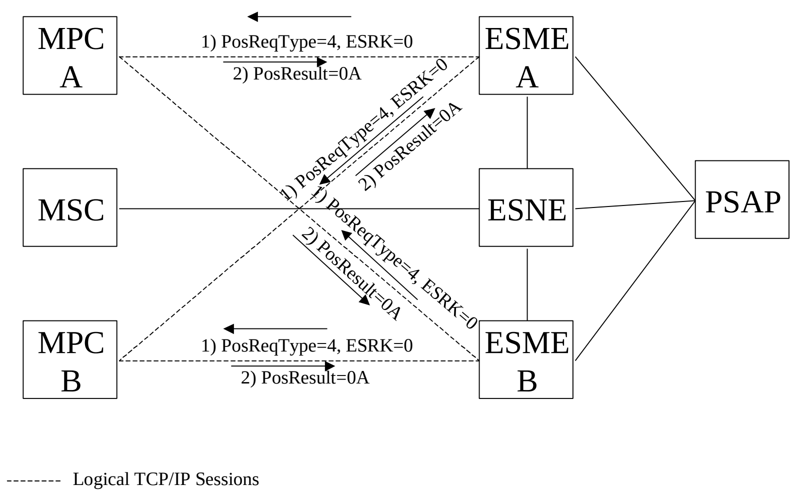

Figure 6

8 Emergency Services Protocol (ESP) Message Formats

ESP messages are formatted using many of the formatting principles of the ANSI TCAP protocol, as described in ANSI T1.114.1 – T1.114.4, with the following clarifications. The encoding of the Transaction Portion of an ESP message, which consists of the Package Type, Transaction ID, and Component Sequence, is as described in ANSI T1.114.3. The encoding of certain elements of the Component Portion, namely the Component Type, Component ID, Operation Code and Parameter Set data elements, are also formatted according to ANSI TCAP. However, the coding of the ESP parameters within the Parameter Set diverge from ANSI TCAP with regard to the coding of the various parameter identifiers. Although the Emergency Services Protocol uses identifiers from the National TCAP codespace, as defined in ANSI T1.114.3, the ESP parameters are not defined within the ANSI TCAP standard. Because of the potential for code conflicts between the ESP parameter identifier values and those assigned to existing or future TCAP data elements defined in ANSI T1.114, caution should be exercised in using the ESP protocol with network nodes that also support the ANSI TCAP protocol. The tables below define the sequence of message elements and parameters within each ESP message type. Note that parameters in the Parameter Set may occur in any order. Other element ordering is mandatory.

8.1 Emergency Services Position Request

This message is sent from the ESME to MPC to request the initial, updated or last known position of an MS.

Element /Parameter	Reference	Type
Package Type = Query With Permission	9.1.1	M
Transaction ID	9.1.2	M
Component Sequence	9.2.1	M
Component Type = Invoke(Last)	9.2.2	M
Component ID	9.2.3	M
Operation Code = Private TCAP	9.2.4	M
Parameter Set	9.2.7	M
ESMEIdentification	9.3.1	M
PostionRequestType	9.3.2	M
EmergencyServicesRoutingKey (esprKey)	9.3.3	O
CallbackNumber (esprKey)	9.3.4	O

EmergencyServiceRoutingDigits (esprKey)	9.3.6	O

Please Note: The esprKey is a CHOICE of either the EmergencyServicesRoutingKey (ESRK), or the CallbackNumber and the optional EmergencyServiceRoutingDigit (ESRD). CallbackNumber is mandatory only if ESRK is not provided.

8.2 Emergency Services Position Request Response

This message is sent from MPC to the ESME to inform the ESME interface of the position of the MS.

Element /Parameter	Reference	Type
Package Type = Response	9.1.1	M
Transaction ID	9.1.2	M
Component Sequence	9.2.1	M
Component Type = Return Result(Last)	9.2.2	M
Component ID	9.2.3	M
Parameter Set	9.2.7	M
PositionResult	9.3.8	M
PostionInformation	9.3.9	O
CallbackNumber	9.3.5	O
EmergencyServiceRoutingDigits	9.3.7	O
GeneralizedTime	9.3.11	O
MobileIdentificationNumber	9.3.12	O
InternationalMobileSubscriberIdentit y	9.3.13	O
MobileCallStatus	9.3.14	O
CompanyID	9.3.15	O
Location Description	9.3.16	O

8.3 Emergency Services Position Request Response Return Error

This message is sent from the MPC to the ESME to inform the ESME that the requested action was not performed. The Error Code contains the reason for the failure.

Element /Parameter	Reference	Type
Package Type = Response	9.1.1	M

Transaction ID	9.1.2	M
Component Sequence	9.2.1	M
Component Type = Return Error	9.2.2	M
Component ID	9.2.3	M
Error Code	9.2.5	M
Parameter Set	9.2.7	M

8.4 Emergency Services Position Request Response Reject

This message is sent from the MPC to the ESME to inform the ESME that the invoke message contains a Transaction or Component Level protocol error. The problem code describes the nature of the protocol error.

Element /Parameter	Reference	Type
Package Type = Response	9.1.1	M
Transaction ID	9.1.2	M
Component Sequence	9.2.1	M
Component Type = Reject	9.2.2	M
Component ID	9.2.3	M
Problem Code	0	M
Parameter Set	9.2.7	M

9 Emergency Services Protocol (ESP) Message Element Descriptions

9.1 Transaction Portion Information Elements

9.1.1 Package Type

The Package Type is used to control the state of the transaction.

Octet	H	G	F	E	D	C	B	A
1	Package Type Identifier							
2	Package Length							

The Package Type identifier is coded as defined in ANSI T1.114.3 – 1996, Section 3.1.The subset of Package Types that will be supported are shown below.

H	G	F	E	D	C	B	A	Hex	Meaning
1	1	1	0	0	0	1	0	E2	Query With Permission
1	1	1	0	0	1	0	0	E4	Response

9.1.2 Transaction ID

The Transaction ID used to identify messages that belong to the same transaction. It is unique for each transaction. The Transaction ID identifier is coded as defined in ANSI T1.114.3 – 1996, Section 3.3. All TCAP messages require a Transaction ID field. Each Transaction ID has a length of 4 octets. In messages that have a Package Type of Query with Permission, there is only one Transaction ID, which is the Originating Transaction ID. In messages that have a Package Type of Response, there is a single Transaction ID, the Responding Transaction ID (which reflects the Originating Transaction ID).

Octet	H	G	F	E	D	C	B	A
1(=C7)	1	1	0	0	0	1	1	1
2	Transaction ID Length = 4							
3	Transaction ID (most significant octet)							
4	Transaction ID (octet 2)							
5	Transaction ID (octet 3)							
6	Transaction ID (least significant octet)							

9.2 Component Portion Information Elements

9.2.1 Component Sequence

The Component Sequence indicates that a sequence of one or more components follows. The Component Sequence Identifier is coded as in ANSI T1.114.3, Section 5.1. The Component Sequence Length is the length of the entire component.

Octet	H	G	F	E	D	C	B	A
1(=E8)	1	1	1	0	1	0	0	0
2	Component Sequence Length							

9.2.2 Component Type

The Component Type indicates the type of component that follows.

Octet	H	G	F	E	D	C	B	A
1	Component Type Identifier							
2	Component Length							

The Component Type Identifier is coded as defined in ANSI T1.114.3-1996, Section 5.3.The subset of Component Types that will be supported are shown below.

H	G	F	E	D	C	B	A	Hex	Meaning
1	1	1	0	1	0	0	1	E9	Invoke (last)
1	1	1	0	1	0	1	0	EA	Return Result (last)
1	1	1	0	1	0	1	1	EB	Return Error
1	1	1	0	1	1	0	0	EC	Reject

9.2.3 Component ID

The Component ID is used to identify components within a transaction. The Component ID identifier is coded as defined in ANSI T1.114.3-1996, Section 5.5. In the ESP, the Component ID Length is always 1, meaning that there is only one Component ID in the Component. Since the component in the Emergency Services Position Request is an Invoke component, and the Package Type is a query, this message will contain an Invoke ID. Since the Emergency Services Position Request Response contains a Return Result component, it will contain a Correlation ID (which reflects the Invoke ID).

Octet	H	G	F	E	D	C	B	A
1(=CF)	1	1	0	0	1	1	1	1
2	Component ID Length = 1							
3	Component ID							

9.2.4 Operation Code

The Operation Code defines the operation to be invoked in an Invoke component. The Operation Code identifier is coded as defined in ANSI T1.114.3-1996, Section 5.8 and is Private TCAP. The Operation Code consists of 2 octets: the Operation Family and the Operation Specifier.

Octet	H	G	F	E	D	C	B	A
1(=D1)	1	1	0	1	0	0	0	1
2	Operation Code Length = 2							
3	Operation Family (= 1 decimal)							
4	Operation Specifier = 1							

The Operation Specifier value for Emergency Services Position Request is 1.

9.2.5 Error Code

The Error Code defines an Application Level error that occurred and is being returned in a Return Error component. The Error Code Identifier is coded as defined in ANSI T1.114.3-1996, Section 5.11, and is Private TCAP.

Octet	H	G	F	E	D	C	B	A
1(=D4)	1	1	0	1	0	1	0	0
2	Error Code Length = 1							
3	Error Code							

The following table lists the values for Error Code and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	System Failure
0	0	0	0	0	0	1	0	02	Unauthorized Request
0	0	0	0	0	0	1	1	03	Unexpected Data Value
0	0	0	0	0	1	0	0	04	Unrecognized Key

9.2.6 Problem Code

The Problem Code defines the reason that the Transaction or Component Portion of the message was rejected. The Problem Code identifier is coded as defined in ANSI T1.114.3-1996, Section 5.14.

Octet	H	G	F	E	D	C	B	A
1(=D5)	1	1	0	1	0	1	0	1
2	Problem Code Length = 2							
3	Problem Type							
4	Problem Specifier							

The Problem Type is coded as defined in ANSI T1.114.3-1996, Section 5.16.1.The subset of Problem Types that will be supported are shown below.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	General
0	0	0	0	0	0	1	0	02	Invoke
0	0	0	0	0	1	0	1	05	Transaction Portion

The Problem Specifier is coded as defined in ANSI T1.114.3-1996, Section 5.16.2.The subset of Problem Specifiers that will be supported are shown below. Note that each Problem Type value corresponds to a specific set of Problem Specifier values.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	General: Unrecognized Component Type
0	0	0	0	0	0	1	0	02	General: Incorrect Component Portion
0	0	0	0	0	0	1	1	03	General: Badly structured component portion
0	0	0	0	0	1	0	0	04	General: Incorrect component coding
0	0	0	0	0	0	0	1	01	Invoke: Duplicate Invoke Id
0	0	0	0	0	0	1	0	02	Invoke: Unrecognized Operation code
0	0	0	0	0	0	1	1	03	Invoke: Incorrect Parameter
0	0	0	0	0	0	0	1	01	Transaction Portion: Unrecognized Package Type

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	1	0	02	Transaction Portion :Incorrect Transaction Portion
0	0	0	0	0	0	1	1	03	Transaction Portion: Badly Structured Transaction Portion
0	0	0	0	0	1	0	0	04	Transaction Portion: Unassigned Responding Transaction ID
0	0	0	0	0	1	0	1	05	Transaction Portion: Permission to Release Problem
0	0	0	0	0	1	1	0	06	Transaction Portion: Resource Unavailable

9.2.7 Parameter Set

The Parameter Set indicates that a set of zero or more parameters follows. The Parameter Set Identifier is coded as defined in ANSI T1.114.3-1996 Section 5.17

Octet	H	G	F	E	D	C	B	A
1(=F2)	1	1	1	1	0	0	1	0
2	Parameter Set Length							

9.3 Emergency Services Protocol (ESP) Parameters

The order of the parameters within the Parameter Set is not significant. . Note that the Parameter Identifier value assignments provided in this document are not defined in ANSI T1.114..

9.3.1 ESME Identification

This parameter identifies the ESME system initiating the request (i.e. ESME).

Octet	H	G	F	E	D	C	B	A
1(=C0)	1	1	0	0	0	0	0	0
2	ESME Identification Length is variable							

3	ESME Identification String (most significant octet)
4	ESME Identification String
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	ESME Identification String (least significant octet)

Max 15 alpha/numeric that defines unique name of ESME that is originating the query. Agreement between TR45 and NENA is that NENA will maintain the nationwide list.

9.3.2 Position Request Type

This parameter indicates the type of position requested.

Octet	H	G	F	E	D	C	B	A
1(=C1)	1	1	0	0	0	0	0	1
2	Position Request Type length=1							
3	Position Request Type							

This table identifies the legal values for Position Request Type and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	Initial
0	0	0	0	0	0	1	0	02	Updated
0	0	0	0	0	0	1	1	03	Updated or Last known
0	0	0	0	0	1	0	0	04	Test

Undefined values are treated as value 1(Initial).

9.3.3 Emergency Services Routing Key

This parameter uniquely identifies an ongoing Emergency Services Call.

Octet	H	G	F	E	D	C	B	A
1(=C2)	1	1	0	0	0	0	1	0
2	Emergency Service Routing Key Length = 9							
3	Type of Digits (Routing Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

This table identifies the legal values for Type of Digits and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	Called Party Number
0	0	0	0	0	0	1	0	02	Calling Party Number
0	0	0	0	0	0	1	1	03	Caller Interaction
0	0	0	0	0	1	0	0	04	Routing Number
0	0	0	0	0	1	0	1	05	Billing Number
0	0	0	0	0	1	1	0	06	Destination Number
0	0	0	0	0	1	1	1	07	LATA
0	0	0	0	1	0	0	0	08	Carrier
0	0	0	0	1	0	0	1	09	Last Calling Party
0	0	0	0	1	0	1	0	0A	Last Party Called

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	1	0	1	1	0B	Calling Directory Number
0	0	0	0	1	1	0	0	0C	VMSR Identifier
0	0	0	0	1	1	0	1	0D	Original Called Number
0	0	0	0	1	1	1	0	0E	Redirecting Number
0	0	0	0	1	1	1	1	0F	Connected Number

This table identifies the legal values for Nature of Number and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	0	00	National/No Presentation Restricted
0	0	0	0	0	0	0	1	01	International/No Presentation Restricted
0	0	0	0	0	0	1	0	02	National/Presentation Restricted
0	0	0	0	0	0	1	1	03	International/Presentation Restricted

This table identifies the legal values for Encoding scheme and their meanings.

D	C	B	A	Hex	Meaning
0	0	0	1	01	BCD
0	0	1	0	02	IA5

This table identifies the legal values for Numbering Plan and their meanings.

H	G	F	E	Hex	Meaning
0	0	0	1	01	ISDN Numbering
0	0	1	0	02	Telephony Numbering
0	0	1	1	03	Data Numbering
0	1	0	0	04	Telex Numbering
0	1	0	1	05	Maritime Mobile Numbering

0	1	1	0	06	Land Mobile Number
0	1	1	1	07	Private Numbering Plan

9.3.4 Callback Number – Request

This parameter is MDN/MSISDN that identifies the emergency service caller.

Octet	H	G	F	E	D	C	B	A
1(=C3)	1	1	0	0	0	0	1	1
2	Callback Number Length = 9							
3	Type of Digits (Calling Party Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.5 Callback Number – Request Response

This parameter is MDN/MSISDN that identifies the emergency service caller.

Octet	H	G	F	E	D	C	B	A
1(=C2)	1	1	0	0	0	0	1	0
2	Callback Number Length = 9							
3	Type of Digits (Calling Party Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.6 Emergency Services Routing Digits – Request

This parameter uniquely identifies a base station, cell site or sector.

Octet	H	G	F	E	D	C	B	A
1(=C4)	1	1	0	0	0	1	0	0
2	Emergency Services Routing Digits Length = 9							
3	Type of Digits (Routing Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			

Octet	H	G	F	E	D	C	B	A
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.7 Emergency Services Routing Digits – Request Response

This parameter uniquely identifies a base station, cell site or sector.

Octet	H	G	F	E	D	C	B	A
1(=C3)	1	1	0	0	0	0	1	1
2	Emergency Services Routing Digits Length = 9							
3	Type of Digits (Routing Number)							
4	Nature of Number (National/International, No Presentation Restrictions)							
5	Numbering Plan (Telephony Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.8 Position Result

This parameter indicates the type of position returned or the reason for not providing position information.

Octet	H	G	F	E	D	C	B	A
1(=C0)	1	1	0	0	0	0	0	0
2	Position Result length=1							
3	Position Result							

The table below identifies the legal values for Position Result and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	1	01	Initial Position Returned
0	0	0	0	0	0	1	0	02	Updated Position Returned
0	0	0	0	0	0	1	1	03	Last known Position Returned
0	0	0	0	0	1	0	0	04	Req Position Not Avail
0	0	0	0	0	1	0	1	05	Caller Disconnected
0	0	0	0	0	1	1	0	06	Caller Has Handed Off
0	0	0	0	0	1	1	1	07	Inactive
0	0	0	0	1	0	0	0	08	Unresponsive
0	0	0	0	1	0	0	1	09	Refused
0	0	0	0	1	0	1	0	0A	Test

If undefined values are received they are treated as value 4 was received.

9.3.9 Position Information

This parameter contains the geographic position estimate of the mobile and the time of the position determination. This parameter may also contain information regarding the method used to obtain the geographic position.

Octet	H	G	F	E	D	C	B	A
1(=E1)	1	1	1	0	0	0	0	1
2	Length of Position Information							
3	Position Information Parameters							

9.3.10 Position Information Parameters:

9.3.10.1 Generalized Time (Mandatory)

This parameter contains time of position determination. This timestamp is specified in Universal Coordinated Time (UTC).

Octet	H	G	F	E	D	C	B	A
1(=C0)	1	1	0	0	0	0	0	0
2	Length of Generalized Time = 6							
3	Year – 2000							
4	Month							
5	Day of Month							
6	MSB Time of Day							
7								
8	LSB							

9.3.10.2 Geographic Position (Mandatory)

Latitude and longitude of the wireless caller's position are carried in this parameter. The format and coding of the elements in the shape description are described in the sub clauses.

Octet	H	G	F	E	D	C	B	A
1(=C1)	1	1	0	0	0	0	0	1
2	Length of Geographic Position							
3	Spare				LPRI		Screening	
4	Ext	Type of Shape						
5	Shape description							
6								
N								

The following codes are used in the sub fields of Geographic Position parameter:

Location Presentation Restricted Indicator (LPRI)

D	C	Hex	Meaning
0	0	00	Presentation Allowed
0	1	01	Presentation Restricted
1	0	02	Location not Available
1	1	03	Spare

Screening Indicator (Screening)

B	A	Hex	Meaning
0	0	00	User provided, not verified
0	1	01	User provided, verified and passed
1	0	02	User provided, verified and failed
1	1	03	Network provided

Extension Indicator (Ext)

H	Hex	Meaning
0	00	Info continues thru the next octet
1	01	Last octet

Type of Shape and Shape descriptions:

1. Ellipsoid Point

	H	G	F	E	D	C	B	A
4		0	0	0	0	0	0	0
5	Lat sign	MSB						
6				Degrees of Latitude				
7								LSB
8	MSB							
9					Degrees of Longitude			
10								LSB

These values are further defined in ANSI T1.628-2000 as:

i) Lat Sign

0 North
1 South

ii) Degrees of latitude

The relation between the binary coded number N and the range of latitudes X ($0 \leq X < 90$), where X is in degrees but not necessarily an integral number of degrees it encodes, is described by the following equation:

$$N \leq \frac{2^{23}}{90} X < N + 1$$

except for $N=2^{23}-1$, for which the range is extended to include N+1

iii) Degrees of longitude

The longitude, expressed in the range (-180, +180) is coded as a number between -2^{23} and $2^{23}-1$, coded in 2's complement binary. The relation between the binary coded number N and the range of longitudes X (-180 ≤ X < 180), where X is in degrees but not necessarily an integral number of degrees it encodes, is described by the following equation:

$$N \leq \frac{2^{24}}{360} X < N + 1$$

2. Ellipsoid point with uncertainty

	H	G	F	E	D	C	B	A
4		0	0	0	0	0	0	1
5	Lat sign	MSB						
6					Degrees of Latitude			
7								LSB
8	MSB							
						Degrees of Longitude		
								LSB
11	Spare				Uncertainty code			
12	Spare				Confidence			

These values are further defined in ANSI T1.628-2000 as:

i) Lat Sign
Same as above

ii) Degrees of latitude
Same as above

iii) Degrees of longitude
Same as above

iv) Uncertainty code
The uncertainty *r*, expressed in meters (in the range 1m to 1800km), is mapped from

$$r = C\left(\left(1 + x\right)^{K} - 1\right)$$

the binary number K, with the following formula:

with C = 10 and x = 0.1.

v) Confidence
The confidence by which the location is known to be within the shape description, C (expressed as a percentage) is directly mapped from the binary number K, except for K=0 which is used to indicate ‘no information’, and 100 < K ≤127 which are not used.

3. Point with altitude and uncertainty

	H	G	F	E	D	C	B	A
4		0	0	0	0	0	1	0
5	Lat sign	MSB						
6	Degrees of Latitude							
7								LSB
8	MSB							
	Degrees of Longitude							
								LSB
11	Spare	Uncertainty code						
12	Alt sign	MSB	Altitude					
13								LSB
14	Spare	Altitude Uncertainty code						
15	Spare	Confidence						

These values are further defined in ANSI T1.628-2000 as:

i) Lat Sign
Same as above

ii) Degrees of latitude
Same as above

iii) Degrees of longitude
Same as above

iv) Uncertainty code
Same as above

v) Confidence
Same as above

vi) Alt Sign
0 Above the ellipsoid
1 Below the ellipsoid

vii) Altitude

The relation between the binary coded number N and the range of altitudes *a* (in meters) it encodes is described by the following equation;

$$N \leq a < N+1$$

except for N=2^{15} for which the range is extended to include all greater values of *a*.

viii) Altitude uncertainty code

Altitude uncertainty *h*, expressed in meters (in the range 0m to ≈1000m), is mapped from the binary number K, with the following formula:

$$h = C\left((1+x)^{K} - 1\right)$$

with C = 45 and x = 0.025.

9.3.10.3 Position Source (Optional)

This parameter specifies how particular position information was obtained to help assess its credibility.

Octet	H	G	F	E	D	C	B	A
1(=C2)	1	1	0	0	0	0	1	0
2	Length of Position Source=1							
3	Value of Position Source							

The table below identifies the legal values for Position Source and their meanings.

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	0	0	0	0	0	00	Unknown
0	0	0	0	0	0	0	1	01	Network Unspecified
0	0	0	0	0	0	1	0	02	Network AOA
0	0	0	0	0	0	1	1	03	Network TOA
0	0	0	0	0	1	0	0	04	Network TDOA
0	0	0	0	0	1	0	1	05	Network RF Fingerprinting
0	0	0	0	0	1	1	0	06	Network Cell Sector
0	0	0	0	0	1	1	1	07	Network Cell Sector with Timing
0	0	0	1	0	0	0	0	10	Handset Unspecified
0	0	0	1	0	0	0	1	11	Handset GPS

H	G	F	E	D	C	B	A	Hex	Meaning
0	0	0	1	0	0	1	0	12	Handset AGPS
0	0	0	1	0	0	1	1	13	Handset EOTD
0	0	0	1	0	1	0	0	14	Handset AFLT
0	0	0	1	0	1	0	1	15	Handset EFLT

Undefined values in the range 1-15 are treated as if value 1(Network Unspecified)

Undefined values in the range 16-31 are treated as if value 1(Handset Unspecified)

Other undefined values are treated as if value 0(unknown)

9.3.11 Generalized Time

This parameter contains time of position determination. This timestamp is specified in Universal Coordinated Time (UTC).

<table>
<tr><th>Octet</th><th>H</th><th>G</th><th>F</th><th>E</th><th>D</th><th>C</th><th>B</th><th>A</th></tr>
<tr><td>1(=C4)</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td></tr>
<tr><td>2</td><td colspan="8">Length of Generalized Time = 6</td></tr>
<tr><td>3</td><td colspan="8">Year – 2000</td></tr>
<tr><td>4</td><td colspan="8">Month</td></tr>
<tr><td>5</td><td colspan="8">Day of Month</td></tr>
<tr><td>6</td><td colspan="8" rowspan="3">MSB Time of Day
LSB</td></tr>
<tr><td>7</td></tr>
<tr><td>8</td></tr>
</table>

9.3.12 Mobile Identification Number

Octet	H	G	F	E	D	C	B	A
1(=C5)	1	1	0	0	0	1	0	1
2	Mobile Identification Number Length = 9							
3	Type of Digits (Not Used)							
4	Nature of Number (International, No Presentation Restrictions)							
5	Numbering Plan (Not Applicable)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.13 International Mobile Subscriber Identity

Octet	H	G	F	E	D	C	B	A
1(=C6)	1	1	0	0	0	1	1	0
2	IMSI Length = 12							
3	Type of Digits (Not Used)							
4	Nature of Number (International, No Presentation Restrictions)							
5	Numbering Plan (Land Mobile Numbering)				Encoding (BCD)			
6	Number of Digits							
7	Digit 2				Digit 1			
8	Digit 4				Digit 3			
9	Digit 6				Digit 5			
10	Digit 8				Digit 7			
11	Digit 10				Digit 9			

Octet	H	G	F	E	D	C	B	A
12	Digit 12				Digit 11			
13	Digit 14				Digit 13			
14	Filler				Digit 15			

See Section 9.3.3 for how to encode type of digits, nature of number, numbering plan and encoding fields.

9.3.14 Mobile Call Status

This parameter identifies the validation status of the MS's subscription or the access status of an MS for a particular call origination.

Octet	H	G	F	E	D	C	B	A
1(=C7)	1	1	0	0	0	1	1	1
2	Length of Mobile call status = 1							
3	←	Authori zation	-	→	←	Authen tication	-	→

The table below identifies the legal values for Authentication and their meanings.

D	C	B	A	Hex	Meaning
0	0	0	0	00	Authentication not performed
0	0	0	1	01	Authentication successful
0	0	1	0	02	Authentication failure

The table below identifies the legal values for Authorization and their meanings.

H	G	F	E	Hex	Meaning
0	0	0	0	00	Authorization not performed
0	0	0	1	01	Authorization successful
0	0	1	0	02	Invalid Electronic Serial Number
0	0	1	1	03	Unassigned Directory Number
0	1	0	0	04	Duplicate Unit
0	1	0	1	05	Delinquent Account
0	1	1	0	06	Stolen Unit
0	1	1	1	07	Not Authorized for MSC

H	G	F	E	Hex	Meaning
1	0	0	0	08	Unspecified
				09-15	Reserved. Treat the same as value 0. Authorization not performed.

9.3.15 Company ID

This parameter carries a unique identifier for the wireless service provider.

Octet	H	G	F	E	D	C	B	A
1(=C8)	1	1	0	0	1	0	0	0
2	Company ID Length is Variable (up to 15 octets)							
3	Company ID String (most significant octet)							
4								
	…..							
n-1								
N	Company ID String (least significant octet)							

9.3.16 Location Description

This parameter provides descriptive location information to the PSAP. This parameter will be used to provide general location information of the caller. It can also be used to deliver Phase I data if the Phase II information is not available.

Octet	H	G	F	E	D	C	B	A
1(=CE)	1	1	0	0	1	1	1	0
2	Location Description Length is Variable (up to 512 octets)							
3	Location Description (most significant octet)							
4								
	…..							
n-1								
N	Location Description (least significant octet)							

The data in this field is tagged using the NENA version 4 XML tags as defined in the NENA 02-010, Standards for Recommended Formats & Protocols For Data Exchange. All fields are optional. This field supports the following tags (type values are: A=Alphabetic, N=Numeric, V=Variable Length):

Name	Tag	Max Chars	Type	Description
Cell ID	<CEL></CEL>	6	ANV	Identification number indicating a geographic region of wireless coverage. i.e. the cell site where the call is received. Valid Values: 0-2047
Company ID 1	<CPF></CPF>	5	ANV	NENA registered Company Identification code for Service Provider providing wireline or wireless service to the customer.
County ID	<COI></COI>	5	ANV	County Identification Code
Customer Name	<NAM></NAM>	32	ANV	Subscriber Name
Emergency Medical Service Responder	<EMS></EMS>	25	ANV	Name of Emergency Medical Service Responder associated with the ESN of the caller.
Emergency Services Number	<ESN></ESN>	5	ANV	Emergency Service Number associated with the House Number and Street Name and Community Name. *Note: The Service Provider, providing the E9-1-1 Selective Routing will assign ESN's.*
Fire Department Service Responder	<FIR></FIR>	25	ANV	Name of Fire Department Service Responder associated with the ESN of the caller.
House Number	<HNO></HNO>	10	ANV	House Number

Name	Tag	Max Chars	Type	Description
House Number Suffix	<HNS></HNS>	4	ANV	House Number Extension (e.g. ½)
Law Enforcement Service Responder	<LAW></LAW>	25	ANV	Name of Law Enforcement Service Responder associated with the ESN of the caller.
Location	<LOC></LOC>	60	ANV	Additional location information (free formatted) describing the exact location of the Calling Party Number. (e.g., “Apt 718” or “cell sector A”) Emergency Response Location (ERL) - A Location to which a 9-1-1 emergency response team may be dispatched. The location should be specific enough to provide a reasonable opportunity for the emergency response team to quickly locate a caller anywhere within it. *This information may be displayed at the PSAP*
MSAG Community	<MCN></MCN>	32	AV	Valid service community name as identified by the MSAG
Post Directional	<POD></POD>	2	AV	Directional Trailing street direction suffix. Valid Entries: N S E W NE NW SE SW
Prefix Directional	<PRD></PRD>	2	AV	Directional Leading street direction prefix. Valid Entries: N S E W NE NW SE SW
Sector ID	<SEC></SEC>	2	AN	Sub set/section of a cell. Valid Values: 1-15

Name	Tag	Max Chars	Type	Description
State	<STA></STA>	2	A	Alpha U.S. state or Canadian province abbreviation, i.e. TX (Texas), ON (Ontario)
Street Name	<STN></STN>	60	ANV	Valid service address of the Calling Party Number
Street Name Suffix	<STS></STS>	4	AV	Valid street abbreviation, as defined by the U S Postal Service Publication 28. (e.g. AVE)

10 References

- American National Standard for Telecommunications – Signaling System Number 7 (SS7) – Transaction Capabilities Transaction Part (TCAP), T1.114-1996, Standards Committee T1 – Telecommunications
- ANSI T1.628-2000 for Telecommunications – Emergency Calling Service
- TIA/EIA-41-D – Cellular Radiotelecommunications Intersystem Operations, December 1997.
- TIA/EIA/IS-TIA/EIA/J-STD-036-A-A – Enhanced Wireless 9-1-1 Phase 2, March 2002.
- TIA/EIA/IS-TIA/EIA/J-STD-036-A-A Addendum 1 – Enhanced Wireless 9-1-1 Phase 2, In Ballot.
- NENA 02-010, Standards for Recommended Formats & Protocols For Data Exchange, February 2002.