ATIS-0700028.v002

ATIS Standard on -

Location Accuracy Improvements for Emergency Calls (version 2)

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0700028.v002

ATIS Standard on

Location Accuracy Improvements for Emergency Calls (version 2)

Alliance for Telecommunications Industry Solutions

Approved December 6, 2018

Abstract

A voluntary agreement for improving location accuracy for emergency calls was developed and signed on November 14, 2014, by APCO, NENA, AT&T, Sprint, T-Mobile, and Verizon Wireless. This voluntary agreement included a roadmap for technology changes that was submitted to the FCC in response to an FCC initiative (proceeding 07-114) to provide a number of improvements to emergency location capabilities including providing a Dispatchable Location for emergency calls to PSAPs.

This Standard specifies the requirements, architecture, and interfaces required to support the commitments defined in the roadmap described above as well as the rules as outlined within the FCC CFR [Ref 37].

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Wireless Technologies and Systems Committee (WTSC) develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies. The Emergency Services Interconnection Forum (ESIF) develops Next Generation 911 (NG911) and location accuracy requirements and solutions and is where the industry comes together in a voluntary open forum to identify and resolve technical and operational issues to facilitate interconnection of emergency services networks with other networks (e.g., wireline, cable, satellite, Internet, etc.). ESIF members comprise industry, government, standards, and public safety organizations.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, WTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

The Emergency Location (ELOC) Task Force (TF), a joint Task Force comprised of WTSC and ESIF, was responsible for the development of this document. At the time of consensus on this document, the leadership was comprised of:

D. Zelmer, WTSC Chair (AT&T)

M. Younge, WTSC Vice Chair (T-Mobile)

R. Marshall, ESIF Chair (Comtech Telecommunications)

J. Green, ESIF 1st Vice Chair (Sprint)

R. Muscat, ESIF 2nd Vice Chair (Bexar Metro 911)

P. Musgrove, ELOC TF Co-Chair (AT&T)

C. Militeau, ELOC TF Co-Chair (West Corporation)

R. Sherry, Technical Editor (West Corporation)

Table of Contents

Table of Figures

Table of Tables

ATIS Standard on –

Location Accuracy Improvements for Emergency Calls (version 2)

1 Scope & Purpose

1.1 Scope

A voluntary agreement for improving location accuracy for emergency calls was developed and signed on November 14, 2014 by APCO, NENA, AT&T, Sprint, T-Mobile, and Verizon Wireless. This voluntary agreement included a roadmap for technology changes that was submitted to the FCC in response to an FCC initiative (proceeding 07-114) to provide a number of improvements to emergency location capabilities including providing a Dispatchable Location for emergency calls to Public Safety Answering Points (PSAPs) (http://apps.fcc.gov/ecfs/document/view?id=60000988441). Standards development is needed to support the goals stated in the roadmap.

In addition to the roadmap submitted, the FCC created new requirements to address Location Accuracy. These rules are discussed in the FCC 4th Report & Order [Ref 36] and codified within the published Code of Federal Regulations (CFR) [Ref 37].

This specification describes the standards needed to support the commitments defined in the roadmap described above as well as the rules as outlined within the FCC CFR.

The standard also provides a platform to develop input (liaisons and reference specifications) into 3GPP based on 3GPP release development schedules. It also enables interaction, input, and coordination with other SDOs and related organizations, including NENA and APCO requirements and standards.

Version 2 of this Standard extends the architecture to include an interface to an External Location Server that allows retrieving UE location based on Access Points or Bluetooth beacons managed and hosted by an external service on behalf of one or more enterprises.

1.2 Purpose

The purpose of this standard is to develop specifications for location accuracy improvements for emergency calls specific to North American regulatory policies and practices.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] FCC 07-114, *Federal Communications Commission Fourth Report and Order In the Matter of Wireless E911 Location Accuracy Requirements*; February 3, 2015.[1]

[Ref 2] 3GPP TS 23.167, *IP Multimedia Subsystem (IMS) emergency sessions*.[2]

[1] This document is available from the Federal Communications Commission at: < http://www.fcc.gov/ >.

[2] This document is available from the Third Generation Partnership Project (3GPP) at:
< http://www.3gpp.org/specs/specs.htm >.

[Ref 3] ATIS/TIA J-STD-036-C-2, *Enhanced Wireless 9-1-1 Phase II*, July 2017.[3]

[Ref 4] ATIS-0700015, *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination.*[4]

[Ref 5] 3GPP TS 36.355, *LTE Positioning Protocol (LPP).*[2]

[Ref 6] OMA TS OMA-TS-LPPe-V1_0, *LPP Extensions Specification*.[5]

[Ref 7] 3GPP TS 23.271, *Functional stage 2 description of Location Services (LCS)*.[2]

[Ref 8] 3GPP TS 36.305, *Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN.*[2]

[Ref 9] 3GPP TS 29.171, *LCS Application Protocol (LCS-AP) between the Mobile Management Entity (MME) and Evolved Serving Mobile Location Centre (E-SMLC); SLs interface*.[2]

[Ref 10] 3GPP 29.172, *Evolved Packet Core (EPC) LCS Protocol (ELP) between the Gateway Mobile Location Centre (GMLC) and the Mobile Management Entity (MME); SLg interface*.[2]

[Ref 11] OMA-TS-MLP-V3_5, *Mobile Location Protocol 3.5*.[5]

[Ref 12] IETF RFC 6753, *A Location Dereferencing Protocol Using HELD*, October 2012.[6]

[Ref 13] ATIS-0700039, Guidelines for Emergency Call Location Selection and Reporting by Originating Networks.[7]

[Ref 14] IETF RFC 3265, *Session Initiation Protocol (SIP)-Specific Event Notification*.[6]

[Ref 15] OMA-AD-SUPL-V2_0, *Secure User Plane Location Architecture*.[5]

[Ref 16] OMA-TS-ULP-V2_0_3, *UserPlane Location Protocol*.[5]

[Ref 17] OMA-TS-ILP-V2_0_3, *Internal Location Protocol*.[5]

[Ref 18] 3GPP TS 36.455, *LTE Positioning Protocol A (LPPa)*.[2]

[Ref 19] 3GPP TS 23.401, *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*.[2]

[Ref 20] OMA-ERELD-SUPL-V2_0_3, SUPL 2.0, *UserPlane Location Protocol*.[5]

[Ref 21] 3GPP TS 23.060, *General Packet Radio Service (GPRS); Service description; Stage 2*.[2]

[Ref 22] 3GPP TS 25.305, Stage 2 functional specification of User Equipment (UE) positioning in UTRAN.[2]

[Ref 23] OMA-TS-ULP-V2_0_3, SUPL 2.0, *UserPlane Location Protocol.*[5]

[Ref 24] 3GPP TS 23.272, *Circuit Switched (CS) fallback, Evolved Packet System (EPS); Stage 2*.[2]

[Ref 25] 3GPP 25.331, *Radio Resource Control (RRC); Protocol specification*.[2]

[Ref 26] 3GPP 24.008, *Mobile radio interface Layer 3 specification; Core network protocols; Stage 3*.[2]

[Ref 27] 3GPP 23.018, *Basic call handling; Technical realization*.[2]

[Ref 28] IETF RFC 5985, *HTTP-Enabled Location Delivery (HELD)*, September 2010.[6]

[Ref 29] IETF RFC 6155, *Use of Device Identity in HTTP-Enabled Location Delivery (HELD)*, March 2012.[6]

[Ref 30] IETF RFC 4119, *A Presence-based GEOPRIV Location Object Format*, December 2005.[6]

[Ref 31] IETF RFC 5139, *Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)*, February 2008.[6]

[Ref 32] IETF RFC 5491, *GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations*, March 2009.[6]

[Ref 33] IETF RFC 7540, *Hypertext Transfer Protocol Version 2 (HTTP/2)*, May 2015.[6]

---

[3] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005, at: < https://www.atis.org/docstore/product.aspx?id=26080 >.

[4] This document is available from ATIS, 1200 G Street N.W., Suite 500, Washington, DC 20005 at: < https://www.atis.org/docstore/product.aspx?id=28140 >.

[5] This document is available from the Open Mobile Alliance (OMA) at: < http://openmobilealliance.org/ >.

[6] This document is available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

[7] This document is available from ATIS at, 1200 G Street N.W., Suite 500, Washington, DC 20005: < https://www.atis.org/docstore/product.aspx?id=28383 >.

[Ref 34] Bluetooth Special Interest Group, *Bluetooth® Core Specification v4.2*, December 2014.[8]

[Ref 35] NENA-STA-004.1.1-2014, *NENA Next Generation 9-1-1 (NG9-1-1) United States Civic Location Data Exchange Format (CLDXF) Standard*, March 2014. [9]

[Ref 36] FCC 4th Report and Order on Location Accuracy.[10]

[Ref 37] FCC Code of Federal Regulations (CFR) 47CFR20.18, *911 Service*.[11]

[Ref 38] IETF RFC 6848, *Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)*, January 2013.[6]

[Ref 39] 3GPP 25.413, *UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling*.[2]

[Ref 40] 3GPP 25.453, *UTRAN Iupc interface Positioning Calculation Application Part (PCAP) signalling*.[2]

[Ref 41] 3GPP 29.002, *Mobile Application Part (MAP) specification*.[2]

[Ref 42] IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*, July 2005.[6]

[Ref 43] 3GPP 33.310, *Network Domain Security (NDS); Authentication Framework (AF)*[2]

[Ref 44] IETF RFC 2818 *HTTP Over TLS,* May 2000[6]

3 Informative References

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this ATIS Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 100] NENA-STA-010.2, *Detailed Functional and Interface Standards for the NENA i3 Solution*, September 10, 2016.[12]

[Ref 101] NENA-ADM-000.22-2018, *NENA Master Glossary of 9-1-1 Terminology.*[13]

[Ref 102] IEEE 802.11-2016, Wireless LANs, 2016[14]

4 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

4.1 Definitions

Bluetooth Public Device Address (BT-PDA): Forty-eight (48) bit globally unique address used to identify a Bluetooth device.

Dispatchable Location: Appendix D, (i) (1) iii of the FCC Report and Order [Ref 1] (Also see Annex A) defines Dispatchable Location as follows:

---

[8] This document is available from Bluetooth Special Interest Group at: < https://www.bluetooth.org/en-us/specification/adopted-specifications >.

[9] This document is available from National Emergency Numbering Association (NENA) at: < http://www.nena.org/?page=Standards >.

[10] This document is available from the FCC at: < https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-9A1.pdf >.

[11] This document is available at < http://www.ecfr.gov/cgi-bin/text-idx?SID=d111e6a56b3786c1bc935ee861af37d8&mc=true&node=se47.2.20_118&rgn=div8 >

[12] This document is available from NENA at: < http://www.nena.org/?page=Standards >.

[13] This document is available from NENA at: < http://www.nena.org/standards/master-glossary >.

[14] This document is available from the Institute of Electrical and Electronics Engineers (IEEE) at: < https://www.ieee.org/ >.

> *Dispatchable location: A location delivered to the PSAP by the CMRS provider with a 911 call that consists of the street address of the calling party, plus additional information such as suite, apartment or similar information necessary to adequately identify the location of the calling party. The street address of the calling party must be validated and, to the extent possible, corroborated against other location information prior to delivery of dispatchable location information by the CMRS provider to the PSAP*.

Emergency Services (ES) Network: ES Network signifies the NENA i3 ESInet and associated functional elements or the legacy Selective Router and ALI.

Geocoding Process: The geocoding process is the process that converts a street address to geographic coordinates and may or may not result in an indication of the geocoded location accuracy.

Heightened Location Accuracy: A specific form of location according to FCC Report and Order [Ref 1] either a Dispatchable location or a position estimate accurate to within 50 m (horizontal).

Heightened Location Accuracy Technologies: Paragraph 25 of the FCC Report and Order [Ref 1] refers to the definition of Heightened Location Accuracy Technologies presented in the Roadmap:

> *25. As originally proposed, the Roadmap contained the following horizontal location accuracy performance benchmarks:*
>
> *… "Heightened location accuracy technologies" consist of: (1) satellite-based (A-GNSS) location, (2) dispatchable location, or (3) "any other technology or hybrid of technologies capable of location accuracy performance of 50 meters." …*

Indoor Location: A type of location information that means that the caller's device is within a structure that may be represented by a home, apartment, high-rise, enterprise, etc. Indoor location may be represented as a Dispatchable Location as defined above. Indoor location may also be represented by a geodetic location that includes the latitude and longitude and may potentially include vertical location information (e.g., z-axis).

Medium Access Control (MAC) Address: Forty-eight (48) bit globally unique address used to identify a Wi-Fi access point. In the context of this standard, the term MAC address (see [Ref 1]) is equivalent to a Wireless MAC address. The wireless MAC address of an Access Point is also known as a Basic Service Set Identifier (BSSID). Other common usages of the term MAC address may exist such as the Ethernet MAC address of the Access Point, but such usages are not applicable within this standard. Note that a single Access Point may have multiple BSSIDs.

National Emergency Address Database (NEAD) : Appendix D, (i) (1) iii of the FCC Report and Order [Ref 1] (also see Annex A) defines the NEAD (pronounced nee-ad) as follows.

> *National Emergency Address Database (NEAD). A database that utilizes MAC address information to identify a dispatchable location for nearby wireless devices within the CMRS provider's coverage footprint.*

This standard also supports the use of BT-PDA to identify the dispatchable location for nearby Bluetooth beacons.

Reference Point: A Wi-Fi access point whose Media Access Control (MAC) address or a Bluetooth device whose Public Device Address (BT-PDA) is detectable by the user's end device during an emergency call. A Reference Point identifier may be associated with a candidate Dispatchable Location in the NEAD. In this standard, Reference Point is also used to indicate a Reference Point identifier.

Vertical Location Information: Appendix D, (2) ii of the FCC Report and Order [Ref 1] (Also see Annex A) defines vertical location as one of 1) the floor component of a Dispatchable Location, 2) barometric pressure, or 3) z-axis methods to be defined through the evaluation of technologies in the test bed.

External Location Services: External Location Services allow the NEAD Platform to retrieve the UE location information from an external source. Address information may be contained within an Enterprise or another source. For these Access Points or Bluetooth beacons, when the LS queries the NEAD, the NEAD will query the ELS and return the acquired location to the LS.

4.2 Acronyms & Abbreviations

3GPP	Third Generation Partnership Project

AP	Access Point
APCO	Association of Public Safety Communications Officials
ATIS	Alliance for Telecommunications Industry Solutions
BSSID	Basic Service Set Identifier
BLE	Bluetooth Low Energy
BT	Bluetooth®
BT-PDA	Bluetooth – Public Device Address
CM	Connection Management
CLDXF	Civic Location Data Exchange Format
CS	Circuit Switched
CMRS	Commercial Mobile Radio Service
CSCF	Call Session Control Function
CSFB	Circuit Switched Fallback
DIS	Data Integrity Specialist
DL	Dispatchable Location
EATF	Emergency Access Transfer Function
E-CSCF	Emergency CSCF
FQDN	Fully Qualified Domain Name
eNB	Evolved Node B
EPC	Evolved Packet Core
ELC	External Location Controller
ELP	EPC LCS Protocol
ELS	External Location Server
ES	Emergency Services
ESInet	Emergency Services IP network
E-SLP	Emergency SLP
E-SMLC	Enhanced Serving Mobile Location Center
ESRD	Emergency Service Routing Digits
ESRK	Emergency Service Routing Key
ESRP	Emergency Services Routing Proxy
GGSN	Gateway GPRS Support Node
GL	Geodetic Location
GMLC	Gateway Mobile Location Center

GPRS	General Packet Radio Service
GRUU	Global Routable User Agent URI
HALI	Heightened Accuracy Location Information
HELD	HTTP-Enabled Location Delivery
HTTP	HyperText Transfer Protocol
HLR	Home Location Register
HSS	Home Subscriber Server
ILP	Internal Location Protocol
IANA	Internet Assigned Numbers Authority
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
LCS	Location Services
LM	Location Measurements
LPG	Legacy PSAP Gateway
LPP	LTE Positioning Protocol
LPPa	LTE Positioning Protocol A
LPPe	LTE Positioning Protocol Extensions
LRF	Location Retrieval Function
MAC	Media Access Control
LTE	Long Term Evolution
M2M	Machine to Machine
MAP	Mobile Application Part
MSC	Mobile Switching Center
MGCF	Media Gateway Control Function
MME	Mobility Management Entity
MLP	Mobile Location Protocol
MSISDN	Mobile Station International Subscriber Directory Number
NEAD	National Emergency Address Database
NEAM	National Emergency Address Manager
NENA	National Emergency Number Association
OMA	Open Mobile Alliance
PCAP	Positioning Calculation Application Part

P-CSCF	Proxy CSCF
PDG	PDN Gateway
PDP	Packet Data Protocol
PIDF-LO	Presence Information Data Format – Location Object
PDN	Packet Data Network
PDU	Protocol Data Unit
PS	Packet Switched
PSAP	Public Safety Answering Point
QoS	Quality of Service
RANAP	Radio Access Network Application Part
RDF	Routing Determination Function
RNC	Radio Network Controller
RP	Reference Point
RRC	Radio Resource Control
RRLP	Radio Resource LCS Protocol
RTLS	Real Time Location System
RTT	Round Trip Time
RSSI	Received Signal Strength Indicator
SAI	Service Area Identifier
SAS	Standalone SMLC
SET	SUPL Enabled Terminal
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIM	Subscriber Identity Module
SLC	SUPL Location Center
SLP	SUPL Location Platform
SMLC	Serving Mobile Location Center
SPC	SUPL Positioning Center
SPM	Source Position Method(s)
SUPL	Secure User Plane Location
TMSI	Temporary Mobile Subscriber Identity
UBP	Uncompensated Barometric Pressure
UE	User Equipment

ULP	User plane Location Protocol
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
USIM	Universal SIM
VLR	Visitor Location Register
WLAN	Wireless Local Area Network

5 Introduction

A voluntary agreement for improving location accuracy for emergency calls was developed and signed on November 14, 2014 by APCO, NENA, AT&T, Sprint, T-Mobile, and Verizon Wireless. This voluntary agreement included a roadmap for technology changes that was submitted to the FCC in response to an FCC initiative (proceeding 07-114) to provide a number of improvements to emergency location capabilities including providing a Dispatchable Location for emergency calls to PSAPs.

This Standard specifies the requirements, architecture, and interfaces required to support the commitments defined in the roadmap described above as well as the rules as outlined within the FCC CFR [Ref 37].

This revision describes optional additional technology to support the acquisition of indoor location from external location services. This technology is specifically designed to help meet the need of accurate indoor location for certain entities, such as enterprises, that have reasons to provide their campus Wi-Fi AP or BLE beacon location information as an alternative to provisioning the location information in the NEAD. In addition, this revision allows technologies other than the NEAD to support determination of indoor location.

6 Assumptions & Requirements

This clause lists the basic assumptions and requirements.

6.1 Basic Assumptions

The following assumptions may be used to develop requirements and architecture(s) for improved location accuracy.

6.1.1 User Equipment (UE)

The following assumptions are for the User Equipment (UE):

1. User equipment may be one of the following:
    a. A mobile registered with a U.S. CMRS provider.
    b. A Non Service Initialized (NSI) mobile.
    c. A mobile that may have roamed into the U.S. based upon roaming agreements. A roaming mobile may not support the heightened accuracy location capabilities in the serving network, but there are fallback options such as coarse location.
2. A smart phone does not have to install a third-party app in order to support indoor location acquisition.
3. Heightened location accuracy applies to both feature phones and smart phones.
4. Heightened location accuracy applies to emergency calls originated using Universal Mobile Telecommunications System (UMTS) Circuit Switched (CS) and Long Term Evolution (LTE) access networks.
5. In support of external location services, the UE may convey its own WLAN MAC address along with the visible reference points over the LPPe protocol. This capability is based on UE support of the LPPe protocol for UE WLAN MAC address conveyance.

6.1.2 Emergency Services Networks

The following assumptions are for the Emergency Services Networks:

1. Heightened location accuracy is made available to legacy Emergency Services Networks and PSAP CPE.

   NOTE: May require new screen character mapping to take advantage of new information provided.

2. Heightened location accuracy is made available to NG9-1-1 Emergency Services IP Networks (ESInets) and PSAPs.
3. In support of external location services, PSAPs that have a method of accessing HTTP content may be able to take advantage of future enhancements to receive available rich data such as a floor map and more definitive position data from the external location services complex.
4. In support of external location services, PSAPs that do not access HTTP content will receive an external location service-supplied dispatchable address via an ALI system of Legacy PSAP Gateway that supports an E2/ESP or MLP interface.

6.1.3 Location Accuracy

The following assumptions are for location accuracy:

1. The location presented to the PSAP is in the same format as it was acquired. For example, if the location is in the form of latitude and longitude it will not be converted to civic, which would require reverse geocoding that may introduce errors.
2. Heightened location accuracy is not required for call routing.
3. An LS (e.g., E-SMLC) can make a distinction between an ELS (Wi-Fi WLAN or Bluetooth)-derived location vs. NEAD-provisioned location.
4. Results from an ELS can be used by a downstream location server as an additional input to the location selection process.

6.1.4 NEAM Assumptions

The following assumptions are for the National Emergency Address Manager (NEAM):

1. External Data Sources will have a secure method to provision Reference Points into the NEAM (e.g., via web services).
2. External Data Sources will be uniquely identified to enable the NEAM to include unique source IDs in its database (e.g., to allow all Reference Points provisioned by a particular External Data Source to be identified at a later date).
3. Reference Points provisioned into the NEAM will include a single correlation between the Reference Point and a civic address or ELS URI.
4. External Data Sources may add, modify, or delete Reference Points into the NEAM. Addition, deletion, and modification are restricted to Reference Points belonging to owners that an External Data Source has been authorized by the owner to support.
5. All civic addresses will be validated against appropriate 9-1-1 addressing databases and geocoded prior to the NEAM pushing them to the NEAD.
6. If validation fails, the NEAM will provide that indication to the External Data Source.
7. When pushing Reference Point information to the NEAD, the NEAM will indicate whether the information is new and to be added, is existing information that is to be modified, or whether an association is to be deleted.
8. The NEAM will have full OA&M capabilities to include logging, reporting, alarming, etc.
9. There may be multiple NEAM elements connected to a single NEAD. The procedures used to manage the NEAD entry when multiple NEAMs are connected is for future study.
10. The NEAM may employ additional methods to validate NEAD entries at the time of provisioning and/or at a later date. The methods may include re-verification with External Data Sources and verification using other sources of Reference Point data.

11. It is assumed that input data received via the Np interface may be in a variety of address forms.
12. The NEAM supports provisioning interface Np' to accept reference identifiers with a URI from the ELS.
    a. Each entry includes a FIPS county code to indicate the Cellular Market Area (CMA)
    b. A certification process is in place to confirm the External Location Server provider has performed the required civic address validation.

6.1.5 NEAD Assumptions

The following assumptions are for the NEAD:

1. The NEAD is queried by or on behalf of the serving CMRS Network.
2. NEAD hosting is carrier-independent.
3. The NEAD enables a serving CMRS network to query for civic addresses during an emergency call based on globally unique identifiers (e.g., MAC of a WLAN Access Point visible to the calling UE).
4. The NEAD returns a civic address and an associated geocoded location determined by the NEAM or ELS based on the civic address. The geocoded location is provided to allow cross checking of the civic location and shall not be provided to a PSAP.
5. If the query cannot resolve to a civic address, the NEAD will return an error.
6. All civic addresses will be validated and geocoded by the NEAM prior to being provisioned into the NEAD.
7. The NEAD could be a single national database or a distributed database. The latter implies the need for a discovery or routing mechanism.
8. If the NEAD is a distributed database, there will be a mechanism to synchronize any duplicate data among the elements.
9. The NEAD will perform the addition, deletion, and modification of entries as directed by the NEAM.
10. The NEAD will have full OA&M capabilities to include logging, reporting, alarming, etc.
11. Crowdsourced geodetic location is not expected to be initially available as part of the NEAD.
12. The NEAD will be able to accept multiple Reference Points from a CMRS network for any call and return multiple civic addresses and geocoded locations in the response(s).
13. The response to a query from a CMRS network may include either a location or an error code.
14. The civic address(es) returned by the NEAD may or may not include the actual Dispatchable Location of the UE as determined by the CMRS network.
15. The NEAD will deliver over the Nq interface whatever form of candidate Dispatchable Location it has been provisioned with or has received from the ELS.
16. The NEAD supports the entry and storage of ELS-managed Reference Point identifiers mapped to URLs rather than civic addresses, provisioned via the NEAM.
17. The Nq query interface may include the UE WLAN MAC address along with the Reference Point identifier as separate parameters.
18. The Nq interface supports the return of an ELS-provided candidate dispatchable location and geocoded position representing the associated civic address to the LS.
19. The Na interface to the ELS is used only for emergency calls.
20. When used as a proxy for ELS queries, the NEAD will not perform any type of validation on the URI or returned civic location information.

6.2 Requirements

6.2.1 NEAM Requirements

1. The NEAM must develop mechanisms to establish trust levels for External Data Sources including an ability to verify whether an External Data Source has been authorized by an owner.
2. For each Reference Point submitted, the NEAM shall accept only one civic address (via the Np interface) or one URI (via the Np' interface).
3. If the External Data Source requests to add a Reference Point, the NEAM must validate the civic address and invoke a geocoding process, and if the validation passes, it must forward the association to the NEAD.

4. If the External Data Source requests to add a Reference Point, the NEAM must validate the civic address and invoke a geocoding process, and if the validation fails, it must return an error indication.
5. If the External Data Source requests to add a Reference Point via the Np, and the Reference Point already exists within the NEAD, the NEAM must return an error indication.
6. If the ELS requests to add a Reference Point via the Np', and the Reference Point already exists within the NEAD, the NEAM must return an error indication.
7. The NEAM must be able to accept multiple Reference Points within the add request.
8. If the External Data Source requests to modify an existing Reference Point, the NEAM must validate the modified civic address and invoke a geocoding process, and if the validation fails it must return a rejection error indication.
9. If the External Data Source requests to modify or delete an existing Reference Point on behalf of an owner different than the owner of the Reference Point, a rejection error indication must be returned.
10. If the External Data Source requests to modify an existing Reference Point, the NEAM must validate the civic address and invoke a geocoding process, and if the validation passes, it must forward the modified association to the NEAD.
11. The NEAM must be able to accept multiple Reference Points within the modification request.
12. If the External Data Source requests the deletion of a Reference Point on behalf of the owner of the Reference Point, the NEAM must send the deletion request to the NEAD.
13. The NEAM must be able to accept a request to delete one, multiple, or all Reference Points for a particular owner in the deletion request.
14. A query on behalf of an owner shall return the record for the owner. However, a query on behalf of a non-owner shall return an error.
15. The system administrator of the NEAM shall have the capability to add, delete, modify, or query a Reference Point and associated address or URI in the NEAD.
16. The NEAM shall ensure the security and privacy of the data input by External Data Sources.
17. The NEAM shall allow the address information that is input via the Np interface to be in a form that is familiar to the end user.

6.2.2 NEAD Requirements

1. When the NEAD receives a request from the NEAM to add a Reference Point, it must put the association in its internal database.
2. When the NEAD receives a request from the NEAM to modify an existing a Reference Point, it must update the association within its internal database.
3. When the NEAD receives a request from the NEAM to delete a Reference Point, it must delete the association in its internal database.
4. A Location Server that accesses the NEAD shall be authenticated and authorized when accessing the NEAD.
5. When the Location Server queries the NEAD with one or more Reference Points, the NEAD shall return the associated civic address(es) and geocoded location(s) in the response.
6. If the NEAD is queried by the Location Server and it does not contain a Reference Point record, it must return an indication that the record was not found.
7. The NEAD shall have the capability to flag suspicious location records. How those suspicious records are determined and how they are resolved are for future study.
8. The NEAD shall ensure the security and privacy of the data provisioned by the NEAM and shall endeavor to provide access to CMRS networks at all times.

6.2.3 UE Requirements

When the UE detects that an emergency call is being attempted it shall perform the following:

1. If the UE supports a Wi-Fi interface, it shall activate the Wi-Fi interface if not already active.
2. If the UE supports a Bluetooth interface, it shall activate the Bluetooth interface if not already active.
3. If the UE supports a barometric pressure sensor, it shall activate the barometric pressure sensor if not already active.

6.2.4 ELS Requirements

1. All civic addresses under the control of the ELS shall be validated against appropriate 9-1-1 addressing databases prior to provisioning the corresponding URI in the NEAM.

7 Architecture

This clause defines architectural support for heightened accuracy location including identification and definition of relevant network elements and interfaces. The architecture enables use of a NEAD to support Dispatchable Location as referred to in Annex A.

This revision defines architectural support for external location services including identification and definition of relevant functional elements, the network architecture, and interfaces. The architecture enables the use of a NEAD to query the ELS over the Na interface.

7.1 Overview

Figure 7.1 shows an overview of the NEAD Service architecture that includes support for an External Location Server for UE-initiated emergency calls.

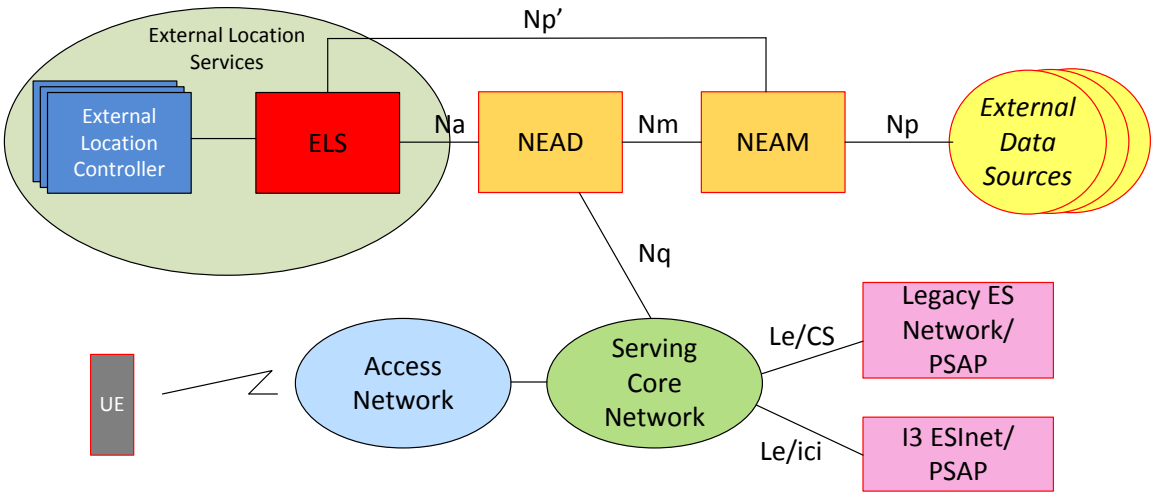


Figure 7.1 – High Level NEAD Service Architecture Including External Location Server

7.1.1 User Equipment (UE)

User Equipment is used here as defined in 3GPP TS 23.167 [Ref 2]. The UE initiates the emergency session establishment request.

7.1.2 National Emergency Address Database (NEAD)

The National Emergency Address Database stores Dispatchable Location information comprising civic location and geocoded location for Reference Points. The NEAD responds to queries for Dispatchable Location information from a serving core network in support of individual emergency calls.

In support of external location services, the NEAD may store a URL that identifies the ELS instead of a provisioned candidate dispatchable location. The NEAD queries the ELS over the Na interface as a result of receiving a query from the LS over the Nq interface. The NEAD returns the candidate dispatchable location information along with geocoded position information it received from the ELS to the LS. The NEAD mutually authenticates with the ELS.

NOTE: It is considered an operational detail to verify the NEAD's ability to connect to an ELS via each URI loaded, making sure that it is well-formed and results in access to the ELS (examples include firewall rules, mutual authentication credentials, etc.).

7.1.3 National Emergency Address Manager (NEAM)

The National Emergency Address Manager supports OAM&P functions for the NEAD and is the recipient of civic location information for Reference Points from External Data Sources. The NEAM supports identification and authentication of External Data Sources, validation of received civic location information, and provisioning of civic location information in the NEAD. The NEAM also determines a geocoded location for each civic location that represents the approximate geodetic location for the civic location. The geocoded location allows cross checking of a civic location by a CMRS network and shall not be provided to a PSAP.

In support of external location services, the NEAM receives Reference Point identifier information (MAC address or BT-PDA) and the URL of the ELS over the Np' provisioning interface. The NEAM in turn provisions the NEAD over the Nm interface. A CMA identifier is also supplied over the Np' interface designating the general geographic area in which the associated reference identifier is located. The CMA identifier is a FIPS county code value. The NEAM mutually authenticates with the ELS.

7.1.4 Access Network

The access network provides wireless access to a UE that is initiating an emergency call. The access network may belong to the operator for the serving core network or may belong to an operator with a business relationship with the operator for the serving core network.

7.1.5 Serving Core Network

The serving core network supports establishment of an emergency call from a UE to a legacy or NENA i3-capable Emergency Services Network and its PSAPs. Functions supported by the serving core network include emergency call detection, call routing, and acquisition and delivery of a Dispatchable Location. For a UE with a valid subscription, the serving core network also supports callback from a PSAP. However, for PSAP callback, the network elements of the home network of a roaming UE are also involved.

7.1.6 External Data Sources

External Data Sources provide Dispatchable Location information to the NEAM. An External Data Source may correspond to an operator, user, or organization that owns or operates one or more Reference Points that may form one or more access networks. The civic location information that is provided may correspond to civic location information for the Reference Points that are owned or operated. External Data Sources have unique identities that can be authenticated by the NEAM and may need to establish some minimum level of trust in order to receive authorization to provide Dispatchable Location information. Internal structure and other details of an External Data Source are outside the scope of this document. To improve flexibility, External Data Sources are classified as OWNERs, users, or both. An OWNER owns or operates Reference Points, whereas a user administers Reference Points in the NEAM on behalf of one or more OWNERs.

7.1.7 Legacy Emergency Services (ES) Network

A legacy Emergency Services Network receives emergency calls and associated Dispatchable Location information from a serving core network using means associated with E9-1-1 Phase 2 and as defined in J-STD-036-C-2 [Ref 3]. Provision of heightened accuracy location is supported to a legacy Emergency Services Network.

7.1.8 NENA i3 ESInet

A NENA i3 ESInet receives emergency calls and Dispatchable Location information from a serving core network using Next Generation means as defined in NENA i3 [Ref 100] and ATIS-0700015 [Ref 4]. Provision of

heightened accuracy location is supported to a NENA i3 ESInet. Note that the NENA i3 PSAPs receive the Dispatchable Location from the serving core network through a direct query.

7.1.9 External Location Server (ELS)

The External Location Server is a function that interconnects, for example, to enterprises represented as an External Location Controller in Figure 7.1. The ELS manages the association of a reference identifier (i.e., Wi-Fi access point and/or Bluetooth beacon) with the External Location Controller in order to deliver indoor location representing a UE involved in an emergency call. The ELS is queried from the NEAD over the Na interface. Each query to the ELS includes the URI that is stored in the NEAD as the target address and either one or two parameters that are conveyed through the NEAD at the time of an emergency call. The first of these two parameters includes the Reference Point identifier of a specific Wi-Fi AP or Bluetooth beacon, and is required. The second parameter, the UE's own Wi-Fi MAC address is optional. The NEAD queries the ELS as a result of the NEAD receiving a query from the LS and the Reference Point identifier in the query being mapped to a URI. The ELS returns location information in the form of a civic address (candidate dispatchable address) including sub-address information, if available, along with geocoded position information back to the NEAD. The response will also contain an IANA registered method token value as referenced in RFC 4119 [Ref 30] and defined in Table 7.1.

7.1.10 External Location Controller

The External Location Controller is, by example, a commercial enterprise that manages Reference Point identifiers (either Wi-Fi Access Points or Bluetooth beacons) for use in providing indoor location associated with the UE to the ELS. The interface between the ELS and the External Location Controller is out of scope for this document.

7.2 Support for Bluetooth

This clause identifies unique characteristics of Bluetooth that are relevant to this standard.

According to the Bluetooth Core Specification [Ref 34] Vol 6, Part B, Section 1.3:

> *Devices are identified using a device address. Device addresses may be either a public device address or a random device address. A public device address and a random device address are both 48 bits in length.*

Refer to the advertising channel PDU header as specified in [Ref 34] Vol 6, Part B, Section 2.3, Figure 2.3 for further details related to address encoding. When the field TxAdd is set to zero, the device address in the advertising PDU is the public address (IEEE-assigned MAC address); when it is set to one, it is a random address (static, non-resolvable private, or resolvable private address). For beacons, the advertiser's address should always be a public address (TxAdd = 0).

In Bluetooth Low Energy (BLE), the total length of the device address is considered 49 bits because one of the bits that describes the type of the address is located within the PDU header as described above (separate from the device address).

In this Standard, only public device addresses are considered which require 48 bits.

7.3 Interfaces

This clause defines interfaces to the NEAD and NEAM.

> NOTE: Np, Nm, Np', Na and Nq interfaces defined in this standard are specifically to be associated with the architecture of heightened accuracy location for indoor E9-1-1 calls in North America and as such are not related to interfaces/Reference Points having the same name specified in 3GPP specifications (e.g., Nq Reference Point between MME and RCAF or Np Reference Point between RCAF and PCRF (see 3GPP TS 23.401 [Ref 19]).

7.3.1 NEAD Query (Nq) Interface

The Nq interface is the interface between the NEAD and a serving core network. The Nq interface supports individual queries by a serving core network element (e.g., Location Server) to retrieve a candidate Dispatchable Location with each potential response. Any candidate Dispatchable Location returned includes geocoded location

information that is associated with a Reference Point visible to a UE that has originated an emergency call. The Nq query message will support a single Reference Point as input. The Nq interface supports two modes of NEAD operation, the first mode is the direct retrieval of location (civic address) information that has been provisioned into the NEAD. The second mode relies on a URI in the NEAD to enable the NEAD to operate as a proxy to query an ELS. This URI is provisioned into the NEAD ahead of the emergency call that might use it. In order for the NEAD to successfully query the ELS over the Na interface, it must have the Reference Point identifier and may optionally have an additional parameter, the UE WLAN MAC address present in the Nq query, which is the specific UE WLAN MAC address of the device making the emergency call. Both modes require the Reference Identifier parameter but allow for both parameters to be present. For location that the ELS determines, the ELS requires the first parameter to achieve proximate location to the device but requires both parameters to be present to enable finer grained device location to be returned. The Nq query message is sent with either one or two included input parameters, the first being a Reference Identifier of the Wi-Fi Access Point or Bluetooth beacon, and the second parameter indicating the specific WLAN MAC address of the UE that initiated the emergency call. If multiple Reference Points are sent by the UE, the serving core network will query the NEAD for any Reference Point individually, including one or both input parameters in each query depending on availability of this data. The Nq interface is an inter-domain interface given that the operator of the NEAD is not the same as the serving core network provider. The Nq interface may support VPN or IP direct connect. It is recommended that the connection be persistent TCP/IP. Per RFC 5985 [Ref 28], the connection must support TLS. In this version of the standard, the URI of the NEAD is known at configuration time and does not require discovery.

A successful response message sent from the NEAD provides results according to the number of parameters supplied at input and based on how the NEAD is provisioned. The data provided by the NEAD or via the ELS for a specific Reference Point comprises (i) a civic address plus additional information such as floor, suite, apartment, or similar information (if available); (ii) a geocoded location determined by the NEAM or ELS based on the civic address; or (iii) an error code if no other data can be returned. The NEAD or ELS will provide either (i) and (ii) or (iii). The originator of the query (i.e., a Location Server in the serving core network) is responsible for reconciling disparate location information that may be returned for different Reference Points that are associated with the same emergency call (e.g., by using additional measurements provided by a location service for a target UE) and for selecting the final Dispatchable Location, and/or geodetic location information provided by a location determination technology other than the NEAD or ELS.

The protocol for this interface query mechanism is standard HTTP with the response message using HTTP-Enabled Location Delivery (HELD) (RFC 5985) [Ref 28]. The serving core network will query the NEAD with an HTTP GET message containing the identifier of the Reference Point (single parameter) or will query the NEAD with both parameters (Reference Point and the UE WLAN MAC address) so that the NEAD can access ELS managed location information. The ELS (when used) and NEAD will respond with a HELD locationResponse message providing a candidate Dispatchable Location and derived geocoded location[15].

If the NEAD response includes a civic location, it will be in the form of Presence Information Data Format – Location Object (PIDF-LO) (RFC 4119 [Ref 30], updated by RFC 5139 [Ref 31], RFC 6848 [Ref 38], and RFC 5491 [Ref 32]). The PIDF-LO supplied from the NEAD contains a civic address along with a geocoded location based on the civic address provided. The response will also contain an IANA registered method token value as referenced in RFC 4119 [Ref 30] specific to whether the result is from the NEAD directly or originally from the ELS.

The Nq interface only supports an HTTP GET method in which the identifier of the UE-observed Reference Point is included as a parameter in the request message and the UE-specific MAC address is optionally included as a second parameter to support ELS interaction. There is also an encoded identifier, a UUID according to RFC 4122, that serves as a correlation identifier to associate different queries to the same emergency call in progress. This UUID correlation identifier also gets passed within the query over the Na interface to the ELS. Since an HTTP GET message that contains only a single Reference Identifier may be indistinguishable from a separate emergency call within the same geographic area referencing some or all of the same Reference Points, the LS will create a Correlation Identifier parameter, Corr-ID that will be associated with all of the Access Points and Bluetooth beacons observed by the UE. For those Access Points and Bluetooth beacons, the LS will send the same Corr-ID as a parameter in the GET Request Line to the NEAD. The Corr-ID, will be a UUID of the format '?Corr-ID=457e4567-e89b-12d3-a456-426655328733'. Note that in response to location update requests from the emergency services network, the LS may obtain a new set of Access Point and Bluetooth beacon identifiers and therefore will use a new Corr-ID in subsequent requests to the NEAD.

[15] This document refers to a geodetic position produced via a geocoding process as "geocoded location".

The Corr-ID UUID will be logged within the NEAD and may be used to perform post-query analysis of Access Point and/or Bluetooth beacon addresses. Note that, for example, if an Access Point or Bluetooth beacon is visible to a UE but has a location that is not within some geographic vicinity of the locations of other Access Points and/or Bluetooth beacons also visible to the UE, the Access Point or Bluetooth beacon location is probably incorrect (e.g., perhaps because the Access Point or Bluetooth beacon was moved and not updated within the NEAD).

The Nq interface implements HTTP/2 as defined in RFC 7540 [Ref 33] which allows asynchronous requests and responses. Streams in HTTP/2 allow the ability to 1) interleave multiple requests in parallel without blocking any one and 2) interleave multiple responses in parallel without blocking any one. The Nq interface implements streams to facilitate the advantages of HTTP/2.

locationRequest Parameters

The following request parameters are supported for NEAD provisioned civic address content:

- GetAddress – This parameter represents the identifier of the Reference Point. The Reference Point identifier shall be represented as a string of hexadecimal digit pairs separated by hyphens or colons.
- Corr-ID – This parameter correlates all Access Points and Bluetooth beacons observed by the UE at one positioning instance. The Corr-ID shall be represented as a UUID per RFC 4122 [Ref 42].

The following request parameters are supported for the Nq interface to support ELS content proxied via the NEAD:

- GetAddress – This parameter represents the identifier of the Reference Point. The Reference Point identifier shall be represented as a string of hexadecimal digit pairs separated by hyphens or colons.
- UEMACAddress – This parameter embeds a specific UE WLAN MAC address value of the device that is making the emergency call and is used as input to the ELS system to acquire an associated location for the UE.
- Corr-ID -- This parameter correlates all Access Points and Bluetooth beacons observed by the UE at one positioning instance. The Corr-ID shall be represented as a UUID per RFC 4122 [Ref 42].

locationResponse Parameters (both modes):

The following response parameters are supported:

- Presence parameter – This is the PIDF-LO format that contains the candidate Dispatchable Location and geocoded location.
- Code – For error codes see below.
- Message – The message parameter expands upon the intent of the Code parameter and is free format and not standardized.
- Method element parameter associated with the location included in the PIDF-LO.

The following response parameters are <u>not</u> supported:

None.

Method Element Parameter

The following Method Element Parameter values are supported. The Method Element Parameter, or “token” is defined within the IANA Method Token registry per RFC 4119 [Ref 30] and conveyed in the HELD location response message. It describes the way the location information was derived or discovered.

Table 7.1 – Supported Method Element Parameters – Nq Interface

Token	Description	Reference	Registration Date
NEAD-WiFi	Civic Address representing the provisioned location of a Wi-Fi Access Point to support the dispatching of emergency services.	ATIS/WTSC-ELOC*	TBD
NEAD-BLE	Civic Address representing the provisioned location of a Bluetooth beacon to support	ATIS/WTSC-ELOC*	TBD

	the dispatching of emergency services.		
ELS-WiFi	Civic Address representing the associated location of the UE based upon the referenced Wi-Fi Access Point from ELS	ATIS/WTSC-ELOC*	TBD
ELS-BLE	Civic Address representing the associated location of the UE based upon the Bluetooth beacon from ELS	ATIS/WTSC-ELOC*	TBD

An xml example of method token value:

<method> ELS-WiFi </method>

* NOTE: Reference IANA registry URL for location method token values:

https://www.iana.org/assignments/method-tokens/method-tokens.xhtml#method-tokens-1

This registry value is added on a first-come, first-served basis.

Error Response Messages

HELD errors are application level errors and returned in a HTTP 200 OK response. The following table describes the error codes from RFC 5985 [Ref 28] (except as noted) applicable to this standard.

Table 7.2 – Applicable Error Codes from RFC 5985 – Nq Interface

Error Code	Description	Comment
RequestError	“This code indicates that the request was badly formed in some fashion (other than the XML content).”	
xmlError	“This code indicates that the XML content of the request was either badly formed or invalid.”	Not used in this standard.
generalLisError	“This code indicates that an unspecified error occurred at the LIS.”	LIS in this context corresponds to the NEAD or ELS.
locationUnknown	“This code indicates that the LIS could not determine the location of the Device. The same request can be sent by the Device at a later time. Devices MUST limit any attempts to retry requests.”	This error code is not used in this standard. It implies that the requestor may re-query for location.
unsupportedMessage	“This code indicates that an element in the XML document for the request was not supported or understood by the LIS. This error code is used when a HELD request contains a document element that is not supported by the receiver.”	LIS in this context corresponds to the NEAD or ELS.
Timeout	“This code indicates that the LIS could not satisfy the request within the time specified in the "responseTime" parameter.”	As this standard does not support the request parameter "responseTime”, a configurable processing timeout will be used by the NEAD or ELS.

Error Code	Description	Comment
cannotProvideLiType	“This code indicates that the LIS was unable to provide LI of the type or types requested. This code is used when the "exact" attribute on the "locationType" parameter is set to "true".”	Not used in this standard.
notLocatable	“This code indicates that the LIS is unable to locate the Device and that the Device MUST NOT make further attempts to retrieve LI from this LIS. This error code is used to indicate that the Device is outside the access network served by the LIS, for instance, the VPN and NAT scenarios discussed in Section 4.1.2.”	This error code should be used when the Reference Point is not found in the NEAD or ELS. This code indicates that the NEAD or ELS do not have an entry for the Reference Point and the serving core network must not make further attempts to retrieve location information from the NEAD or ELS.
badIdentifier	“This error code indicates that a Device identifier used in the HELD request was either: not supported by the LIS, badly formatted, or not one for which the requestor was authorized to make a request.”	From RFC 6155 [Ref 29] and denotes that the MAC address is malformed. There should be no cases where the requestor is not authorized to request location for a Reference Point. This error code indicates that the Reference Point identifier (e.g., MAC address) used in the HELD request was either not supported by the NEAD or ELS or was badly formatted.

Nq Message examples

The examples in this clause are informative.

The following illustrates two examples of an Nq client message request using HTTP GET (REST type), each one including the identifier of either a Bluetooth beacon or Wi-Fi Access Point. The Corr-ID parameter is used to associate all Access Points and Bluetooth beacons observed by the UE at the same location and within the same location transaction.

The Nq interface as specified within this document utilizes HTTP/2 from the IETF HTTP 2.0 specification [RFC 7540]. Refer to Section 9 regarding TLS requirements.

Message query examples:

Wi-Fi Example of Nq Request with Reference Point Identifier as a Wi-Fi access point MAC Address:

HTTPS://NEAD-LLC-WiFi.example.com/GetAddress/A0-12-34-56-78-90?Corr-ID=457e4567-e89b-12d3-a456-426655328733

Bluetooth Example Nq Request with Reference Point Identifier as a Bluetooth beacon BT-PDA:

HTTPS://NEAD-LLC-BT.example.com/GetAddress/A0:12:34:56:78:91?Corr-ID=457e4567-e89b-12d3-a456-426655328733

Wi-Fi Example Nq Request with both parameters, Reference Point Identifier as a Wi-Fi access point MAC Address and UE WLAN MAC Address:

HTTPS://NEAD-LLC-WiFi.example.com/GetAddress/A0-12-34-56-78-90?UEMACAddress=D2-A3-F0-B8-C5?Corr-ID=457e4567-e89b-12d3-a456-426655328733

Bluetooth Example Nq Request with both parameters, Reference Point Identifier as a Bluetooth beacon BT-PDA and UE WLAN MAC Address:

HTTPS://NEAD-LLC-BT.example.com/GetAddress/A0:12:34:56:78:91?UEMACAddress=D2-A3-F0-B8-C5?Corr-ID=457e4567-e89b-12d3-a456-426655328733

Message response examples:

Example Wi-Fi Response from the NEAD:

The following example illustrates a HELD response as described in RFC 5985 [Ref 28] that contains both the civic address of the Wi-Fi Access Point and a geocoded location related to the validated address.

Response with candidate Dispatchable Location information:

```
<?xml version="1.0"?>
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
        <presence xmlns="urn:ietf:params:xml:ns:pidf"
        entity="pres:ae3be8585902e2253ce2@ NEAD-LLC-WiFi.example.com">
                <tuple id="neadLocation">
                <status>
                        <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
                        <location-info>
                                <gs:Point xmlns:gs="http://www.opengis.net/pidflo/1.0"
                                 xmlns:gml="http://www.opengis.net/gml"
                                srsName="urn:ogc:def:crs:EPSG::4326">
                                <gml:pos>41.80882 -88.11135</gml:pos>
                                </gs:Point>
                                <ca:civicAddress
                                 xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
                                 xml:lang="en-au">
                                <ca:country>US</ca:country>
                                <ca:A1>IL</ca:A1>
                                <ca:A2>DuPage</ca:A2>
                                <ca:A3>Lisle</ca:A3>
                                <ca:RD>Warrenville</ca:RD>
                                <ca:STS> Rd</ca:STS>
                                <ca:HNO>3030</ca:HNO>
                                <ca:LOC>Zone=NW</ca:LOC>
                                <ca:FLR>Floor 4</ca:FLR>
                                <ca:PC>60532</ca:PC>
                                <ca:ROOM>254</ROOM>
                                </ca:civicAddress>
                        </location-info>
                        <method>NEAD-WiFi</method>
                        </geopriv>
                </status>
                <timestamp>2015-10-19T12:35:02+10:00</timestamp>
                </tuple>
        </presence>
</locationResponse>
```

The following example illustrates the NEAD returning an error indicating that the Reference Identifier (i.e., MAC Address) is not provisioned in the NEAD.

```
<error xmlns="urn:ietf:params:xml:ns:geopriv:held"
        code=" notLocatable ">
        <message xml:lang="en">MAC address not available</message>
        <method>NEAD-WiFi</method>
</error>
```

Example Wi-Fi Response via the NEAD with data from the ELS:

The following example illustrates a HELD response as described in RFC 5985 [Ref 28] that contains both the civic address of the Wi-Fi Access Point and a geocoded location related to the validated address.

Response with candidate Dispatchable Location information:

```
<?xml version="1.0"?>
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
        <presence xmlns="urn:ietf:params:xml:ns:pidf"
        entity="pres:ae3be8585902e2253ce2@ NEAD-LLC-WiFi.example.com">
                <tuple id="elsLocation">
                <status>
                        <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
                        <location-info>
                                <gs:Point xmlns:gs="http://www.opengis.net/pidflo/1.0"
                                 xmlns:gml="http://www.opengis.net/gml"
                                srsName="urn:ogc:def:crs:EPSG::4326">
                                <gml:pos>41.80882 -88.11135</gml:pos>
                                </gs:Point>
                                <ca:civicAddress
                                 xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
                                 xml:lang="en-au">
                                <ca:country>US</ca:country>
                                <ca:A1>IL</ca:A1>
                                <ca:A2>DuPage</ca:A2>
                                <ca:A3>Lisle</ca:A3>
                                <ca:RD>Warrenville</ca:RD>
                                <ca:STS> Rd</ca:STS>
                                <ca:HNO>3030</ca:HNO>
                                <ca:LOC>Zone=NW</ca:LOC>
                                <ca:FLR>Floor 4</ca:FLR>
                                <ca:PC>60532</ca:PC>
                                <ca:ROOM>254</ROOM>
                                </ca:civicAddress>
                        </location-info>
                        <method>ELS-WiFi</method>
                        </geopriv>
                </status>
                <timestamp>2015-10-19T12:35:02+10:00</timestamp>
                </tuple>
        </presence>
</locationResponse>
```

The following example illustrates the NEAD returning an error indicating that the ELS was unable to determine location information associated with the Reference Identifier (i.e., MAC Address)/UE WLAN MAC Address provided in the query sent by the NEAD.

```
<error xmlns="urn:ietf:params:xml:ns:geopriv:held"
        code=" notLocatable ">
        <message xml:lang="en">MAC address not available</message>
        <method>ELS-WiFi</method>
</error>
```

7.3.2 NEAD-to-ELS Query (Na) Interface

The Na interface is the interface between the NEAD and the ELS. The Na interface supports individual queries initiated by the NEAD when it operates as a proxy for queries from a serving core network element in the case where the NEAD maps a Reference Point identifier to a pointer (URI). Once queried, the ELS returns a candidate Dispatchable Location if available, or otherwise returns an error. Any candidate Dispatchable Location returned by

the ELS also includes geocoded location information in the form of a Lat/Long. Since the Na interface is only used when the NEAD contains a provisioned URI for an associated Reference Identifier, not every query over the Nq interface will result in a proxied query over the Na. When an Na query is initiated, it requires a Reference Identifier, and optionally may include a second input parameter in the query message. The first, parameter identifies the Wi-Fi Access Point or Bluetooth beacon, and the second parameter identifies the specific WLAN MAC address of the UE that initiated the emergency call. If multiple Reference Points (that the ELS manages) are observed by the UE at the start of an emergency call, they will be sent to the serving core network, and handled individually, combining both input parameters in each query. It is assumed that the Na interface will span different operational domains, where an operator of the NEAD is not the same as the ELS provider, requiring a mutually agreeable and secure connection between the separate domains. The Na interface may be supported over a dedicated network connection. Per RFC 5985 [Ref 28], the HTTP transport must support TLS. It is assumed the URI of the ELS is configured ahead of time and does not require discovery.

The NEAD is responsible for constructing an Na query message in the case where a URI was found based on the Reference Point identifier being queried in the NEAD. The NEAD then assembles an HTTP GET message, reusing the input parameters it received via the Nq interface.

An Na response message sent from the ELS during normal processing, provides results to the NEAD. The data provided by the ELS for a specific Reference Point and UE WLAN MAC address being queried comprises (i) a civic address plus additional information such as floor, suite, apartment, or similar information (if available); (ii) a geocoded location determined by the ELS based on the civic address; or (iii) an error code if no other data can be returned. The ELS will provide either (i) and (ii) or (iii) over the Na interface. The Location Server (the initiator of the original query to the NEAD) is responsible for reconciling sets of location information that may be received as a result of multiple queries for different Reference Point identifiers that are associated with the same emergency call and for selecting the final Dispatchable Location, and/or geodetic location information that would be provided by a location determination technology other than the ELS in this case.

The transport protocol specified for this interface query mechanism is standard HTTP with the response message using HTTP-Enabled Location Delivery (HELD) (RFC 5985) [Ref 28]. The NEAD will query the ELS with an HTTP GET message containing the identifier of the Reference Point plus the UE WLAN MAC address to access ELS managed location information. The ELS will respond with a HELD locationResponse message providing a candidate Dispatchable Location and derived geocoded location[16].

If the ELS returns a successful response with a civic location it will be in the form of PIDF-LO. The PIDF-LO supplied from the ELS contains a civic address along with a geocoded location associated with the civic address. The response will also contain an IANA registered method token value as referenced in RFC 4119 [Ref 30] specific to the fact that the result is from the ELS.

It is expected that a small number of ELS elements will exist over time to support the Na interface. There is no requirement that IP connections need to be persistent but can be on demand. The Na interface supports an HTTP GET method for which the identifier of the UE-observed Reference Point is included as a parameter in the request message along with the UE-specific MAC address as a second parameter and the Correlation Identifier parameter (Corr-ID) from the Nq query.

The Corr-ID UUID will be logged within the ELS (as well as the NEAD) and may be used to perform post-query analysis of Access Point and/or Bluetooth beacon addresses.

The Na interface implements HTTP/2 as defined in RFC 7540 [Ref 33] which allows asynchronous requests and responses. Streams in HTTP/2 allow the ability to 1) interleave multiple requests in parallel without blocking any one and 2) interleave multiple responses in parallel without blocking any one. The Na interface implements streams to facilitate the advantages of HTTP/2.

locationRequest Parameters

The following request parameters are supported for ELS queries from the NEAD over the Na:

- GetAddress – This parameter represents the identifier of the Reference Point. The Reference Point identifier shall be represented as a string of hexadecimal digit pairs separated by hyphens or colons.

[16] This document refers to a geodetic position produced via a geocoding process as a “geocoded location”.

- UEMACAddress – This parameter embeds a specific UE WLAN MAC address value attributed to the device's Wi-Fi radio interface of the device that is making the emergency call and is used as input to the ELS system (when available over the Nq) to acquire an associated candidate dispatchable location associated with the UE actual location.
- Corr-ID – This parameter correlates all Access Points and Bluetooth beacons observed by the UE at one positioning instance. The Corr-ID shall be represented as a UUID per RFC 4122 [Ref 42].

locationResponse Parameters

The following response parameters are supported over Na:

- Presence parameter – This is the PIDF-LO format that contains the candidate Dispatchable Location and geocoded location.
- Code – For error codes see below.
- Message – The message parameter expands upon the intent of the Code parameter and is free format and not standardized.
- Method element parameter associated with the ELS input type (Wi-Fi or Bluetooth) that provided the candidate dispatchable civic location and geocoded location included in the PIDF-LO.

The following response parameters are not supported:

None.

Method Element Parameter

The following Method Element Parameter values are supported. The Method Element Parameter, or "token" is defined within the IANA Method Token registry per RFC 4119 [Ref 30] and conveyed in the HELD location response message. It describes the way the location information was derived or discovered.

Table 7.3 – Supported Method Element Parameters– Na Interface

Token	Description	Reference	Registration Date
ELS-WiFi	Civic Address representing the associated location of the UE based upon the referenced Wi-Fi Access Point from ELS	ATIS/WTSC-ELOC*	TBD
ELS-BLE	Civic Address representing the associated location of the UE based upon the Bluetooth beacon from ELS	ATIS/WTSC-ELOC*	TBD

An xml example:

<method>ELS-WiFi</method>

* NOTE: Reference IANA registry URL for location method token values:

https://www.iana.org/assignments/method-tokens/method-tokens.xhtml#method-tokens-1

This registry value is added on a first-come, first-served basis.

Error Response Messages

HELD errors are application level errors and returned in a HTTP 200 OK response. The following table describes the error codes from RFC 5985 [Ref 28] (except as noted) applicable to this standard.

Table 7.4 – Applicable Error Codes from RFC 5985 – Na Interface

Error Code	Description	Comment
RequestError	"This code indicates that the request was badly formed in some fashion (other than the XML content)."	This error is used by the ELS if the Na query message is mal-formed or did not include both Reference ID and UE WLAN MAC address.
xmlError	"This code indicates that the XML content of the request was either badly formed or invalid."	Not used in this standard.
generalLisError	"This code indicates that an unspecified error occurred at the LIS."	LIS in this context corresponds to the ELS.
locationUnknown	"This code indicates that the LIS could not determine the location of the Device. The same request can be sent by the Device at a later time. Devices MUST limit any attempts to retry requests."	This error code is not used in this standard. It implies that the requestor may re-query for location.
unsupportedMessage	"This code indicates that an element in the XML document for the request was not supported or understood by the LIS. This error code is used when a HELD request contains a document element that is not supported by the receiver."	LIS in this context corresponds to the ELS.
Timeout	"This code indicates that the LIS could not satisfy the request within the time specified in the "responseTime" parameter."	As this standard does not support the request parameter "responseTime", a configurable processing timeout will be used by the ELS.
cannotProvideLiType	"This code indicates that the LIS was unable to provide LI of the type or types requested. This code is used when the "exact" attribute on the "locationType" parameter is set to "true"."	Not used in this standard.
notLocatable	"This code indicates that the LIS is unable to locate the Device and that the Device MUST NOT make further attempts to retrieve LI from this LIS. This error code is used to indicate that the Device is outside the access network served by the LIS, for instance, the VPN and NAT scenarios discussed in Section 4.1.2."	This error code should be used when the Reference Point is not found in the ELS. This code indicates that the ELS does not have an entry for the Reference Point and the serving core network must not make further attempts to retrieve location information from the ELS (via the NEAD).
badIdentifier	"This error code indicates that a Device identifier used in the HELD request was either: not supported by the LIS, badly formatted, or not one for which the requestor was authorized to make a request."	From RFC 6155 [Ref 29] and denotes that the MAC address is malformed. There should be no cases where the requestor is not authorized to request location for a Reference Point. This error code indicates that the Reference Point identifier (e.g., MAC address) used in the request was either not supported by the ELS, or was badly formatted.

Na Message examples

The examples in this clause are informative.

The following illustrates two examples of a Na client message request using HTTP GET (REST type), each one including the identifier of either a Bluetooth beacon or Wi-Fi Access Point. The Corr-ID parameter is used to associate all Access Points and Bluetooth beacons observed by the UE at the same location and within the same location transaction.

The Na interface as specified within this document utilizes HTTP/2 from the IETF HTTP 2.0 specification [RFC 7540]. Refer to Section 9 regarding TLS requirements.

Wi-Fi Example Na request message with both parameters shown. The first parameter relates to the Wi-Fi AP MAC address and the second parameter relates to the individual UE WLAN MAC address. The request message is constructed using the URI that is provisioned within the NEAD, the xml GetAddress message, followed by the WLAN Reference Point identifier, the UE WLAN MAC Address, and the Correlation Id:

HTTPS://ELS-ENT-WiFi.example.com/GetAddress/A0-12-34-56-78-90?UEMACAddress=D2-A3-F0-B8-C5?Corr-ID=457e4567-e89b-12d3-a456-426655328733

Bluetooth Example Na Request with both parameters, where the first parameter relates to the Bluetooth beacon BT-PDA and the second parameter relates to the same UE WLAN MAC address:

HTTPS://ELS-ENT-BT.example.com/GetAddress/A0:12:34:56:78:91?UEMACAddress=D2-A3-F0-B8-C5?Corr-ID=457e4567-e89b-12d3-a456-426655328733

Example Wi-Fi Response from the ELS over the Na interface:

The following example illustrates a HELD response as described in RFC 5985 [Ref 28] that contains both the civic address of the Wi-Fi Access Point and a geocoded location related to the validated address.

Response with candidate Dispatchable Location information:

```
<?xml version="1.0"?>
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
        <presence xmlns="urn:ietf:params:xml:ns:pidf"
        entity="pres:ae3be8585902e2253ce2@ELS-ENT-WiFi.example.com">
                <tuple id="elsLocation">
                <status>
                        <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
                        <location-info>
                                <gs:Point xmlns:gs="http://www.opengis.net/pidflo/1.0"
                                 xmlns:gml="http://www.opengis.net/gml"
                                srsName="urn:ogc:def:crs:EPSG::4326">
                                <gml:pos>41.80882 -88.11135</gml:pos>
                                </gs:Point>
                                <ca:civicAddress
                                 xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
                                 xml:lang="en-au">
                                <ca:country>US</ca:country>
                                <ca:A1>IL</ca:A1>
                                <ca:A2>DuPage</ca:A2>
                                <ca:A3>Lisle</ca:A3>
                                <ca:RD>Warrenville</ca:RD>
                                <ca:STS>Rd</ca:STS>
                                <ca:HNO>3030</ca:HNO>
                                <ca:LOC>Zone=NW</ca:LOC>
                                <ca:FLR>Floor 4</ca:FLR>
                                <ca:PC>60532</ca:PC>
                                <ca:ROOM>254</ROOM>
                                </ca:civicAddress>
```

```
                    </location-info>
                    <method>ELS-WiFi</method>
                    </geopriv>
                </status>
                <timestamp>2015-10-19T12:35:02+10:00</timestamp>
                </tuple>
        </presence>
</locationResponse>
```

The following example illustrates the ELS returning an error indicating that the UE's WLAN MAC address is not found, and therefore location is not available from the ELS:

```
<error xmlns="urn:ietf:params:xml:ns:geopriv:held"
        code=" notLocatable ">
        <message xml:lang="en">UE's WLAN MAC address not available</message>
        <method>ELS-WiFi</method>

</error>
```

7.3.3 NEAD Management (Nm) Interface

Nm is the interface between the NEAD and the NEAM. The Nm interface supports OAM&P management of the NEAD by the NEAM, including provisioning of validated address information and event, alarm, and report logging by the NEAD to the NEAM. This interface is out of scope and therefore not defined in this standard.

7.3.4 NEAM Provisioning (Np) Interface

The Np interface is between the NEAM and External Data Sources. The Np interface supports identification and authentication of External Data Sources by the NEAM and the provisioning of source address information by External Data Sources to the NEAM.

The Np interface at the NEAM is implemented using two methods. The first is a web service implementation where the user logs in and fills out an electronic form to manage their Reference Points. The second method is a Machine-to-Machine (M2M) capability that implements an XML-based web interface between the External Data Sources and the NEAM. Each of these methods allows the user to query, add, modify, or delete information about a Reference Point (e.g., a MAC address) for which they are responsible. The two methods are functionally identical in the sense that changing or querying a configuration state of the NEAD is equally possible using either method.

An Np client may query the NEAM for a specific Reference Point or all Reference Points for a particular owner. The client may add new Reference Points which have not been previously included in the NEAM. The Np client, when authorized by (or the same as) a particular owner, may modify information about a Reference Point for this owner. The user may only modify Reference Points that he is authorized to change. The Np client may delete a Reference Point and its associated validated address. The user may only delete Reference Points that he is authorized to delete.

The term OWNER is used here to designate the entity that is ultimately responsible for the Reference Point. The term authorized user denotes an entity that acts on authority of the OWNER for NEAM access. That means that only an authorized user can query for or manage a specific Reference Point. When a user logs in with a user ID and password or has been authenticated for M2M access, he is associated with one or more OWNER(s). He can therefore manage specific Reference Points on behalf of the associated OWNER(s).

7.3.5 NEAM Web Service Implementation

As mentioned above, the web service implementation must support the ability of a user to query for Reference Points and add, modify, or delete Reference Points for which he is responsible.

When a user logs in, he should be provided with an option to query, add, modify, or delete specific Reference Points. This clause does not define the human interface but specifies the attributes that should be available for each action. This interface may also be applicable for the Data Integrity Specialist (DIS) of the entity managing the NEAM. The DIS may have additional capabilities beyond those available to a user, e.g., the ability to handle changes related to any MAC or Bluetooth Public Device Address (BT-PDA) and its information. The Np interface supports HTTP 1.1 and optionally supports HTTP/2, since most browsers support HTTP 1.1, and only some browsers support HTTP/2.

Querying Reference Points

The user must be able to query for Reference Points for the responsible OWNER. The query may be for a specific Reference Point or for all Reference Points that the OWNER is responsible for, or for all Reference Points that the OWNER is responsible for that include particular civic location parameters. The user should be able to fill in the appropriate electronic form attributes and execute the command to query for Reference Points.

Table 7.5 illustrates the attributes for the query. OWNER is mandatory and MAC, BT-PDA, and CIVIC-LOCATION are optional. If MAC, BT-PDA, and CIVIC-LOCATION are not specified, the query response will return a list of all MAC addresses that the OWNER is responsible for. If MAC or BT-PDA is specified, only information related to that MAC or BT-PDA will be returned. If CIVIC-LOCATION is specified, the query response will return a list of all MAC addresses that the OWNER is responsible for that are associated with civic locations that contain all fields for the CIVIC-LOCATION.

If the user attempts to query for a MAC or BT-PDA that the OWNER is not responsible for, an error indication will be returned with information on how to correct the error. If the user queries for a CIVIC-LOCATION that is not part of the civic location for any Reference Point that the OWNER is responsible for, an error indication will be returned.

The tables use the following convention:

M – Attribute or element is mandatory.

O – Attribute or element is optional.

C – Attribute or element is conditional based upon its use.

Table 7.5 – Query Attributes

Attribute	Mandatory/Optional	Description	Example
OWNER	M	Identifies the OWNER	MYCO
MAC*	O	Specifies the Wi-Fi MAC address to be queried.	A0-12-34-56-78-90
BT-PDA*	O	Specifies the Bluetooth Public Device Address to be queried.	DE:30:5D:54:75:B4
CIVIC-LOCATION*	O	Specifies one or more civic location fields as defined in Table 7.6 that are to be queried.	State=CA, City=San Diego

***** NOTE: The query may include a MAC only, BT-PDA only, CIVIC-LOCATION only, or none.

Adding Reference Point Information

The user may add Reference Point information on behalf of the OWNER. It is anticipated that an electronic form will be provided consisting of the attributes in Table 7.6 if a Dispatchable Location is to be added. The user will fill out the appropriate form and submit it.

If the information is successfully validated, the user will be given an indication that the information has been accepted. If the information does not validate, the user will be given an error indication. If the MAC or BT-PDA information already exists, the user will be given an error indication with information that the record already exists and has not been added.

Table 7.6 – Attributes for Adding Reference Points with Location

Attribute[17]	Mandatory/Optional	Description	Example
OWNER	M	Entity responsible for the MAC or BT-PDA address.	MYCO
MAC*	C	MAC address to be entered.	A0-12-34-56-78-90
BT-PDA*	C	BT-PDA address to be entered.	DE:30:5D:54:75:B4
Country	M	Country	US
State[18]	M	Two-character designation for state.	IL
County[19]	M	County	DuPage
Incorporated Municipality[20]	M	City, Town	Lisle
Unincorporated Community[21]	O	The name of an *Unincorporated Community*, either within an incorporated municipality or in an unincorporated portion of a county, or both.	Poquito Valley (residential area and road improvement district in unincorporated Yavapai County, AZ)
Postal Community Name[22]	O	A city name for the ZIP Code of an address, as given in the USPS City State file.	Stanton *(a post office name in KY)*; Bowen *(a town name shown in the USPS database for KY served by the Stanton PO)*.
Postal Code[23]	O	A system of 5-digit codes that identifies the individual USPS Post Office or metropolitan area delivery station associated with an address, which may optionally be enhanced by four additional digits that identify a specific range of USPS delivery addresses.	1.0.8.3 Examples: 02109 (ZIP Code for Boston, MA); 02109-0001 (portion of a 02109 carrier route).
Neighborhood Community[24]	O	Neighborhood, borough, etc.	Queens

[17] Note since the Nq interface returns Dispatchable Location and geographic information in the format of PIDF-LO, the attributes in this table mimic the PIDF-LO elements.

[18] PIDF-LO A1.

[19] PIDF-LO A2.

[20] PIDF-LO A3, Incorporated Municipality, CLDXF NENA STA-004.1.1.

[21] PIDF-LO A4, Unincorporated Community, CLDXF NENA STA-004.1.1.

[22] PIDF-LO PCN, Postal Community Name, CLDXF NENA STA-004.1.1.

[23] PIDF-LO PC, Postal Code, CLDXF NENA STA-004.1.1.

[24] PIDF-LO A5, Neighborhood Community, CLDXF NENA STA-004.1.1.

Attribute[17]	Mandatory/Optional	Description	Example
Street Name[25]	M	The element of the complete street name that identifies the particular street (as opposed to any street pre-types, suffixes, directionals, and modifiers).	Warrenville
Street Name Pre Directional[26]	C	A word preceding the *Street Name* that indicates the direction taken by the street from an arbitrary starting point or line, or the sector where it is located.	'North' in North Fairfax Drive.
Street Name Pre Modifier[27]	C	Precedes and modifies the Street Name element.	"Old" in Old North First Street.
Street Name Pre Type[28]	C	A word or phrase that precedes the Street Name element and identifies a type of thoroughfare.	"Avenue" in Avenue A.
Street Name Pre Type Separator[29]	C	A preposition or prepositional phrase between the Street Name Pre Type and the Street Name.	"of the" in Avenue of the Americas.
Street Name Post Directional[30]	C	A word following the Street Name element that indicates the direction taken by the street from an arbitrary starting point or line, or the sector where it is located.	“East” in Seventh Street East.
Street Name Post Type[31]	C	A word or phrase that follows the Street Name element and identifies a type of thoroughfare in a complete street name.	"Avenue" in North Fairfax Avenue.
Street Name Post Modifier[32]	C	A word or phrase that follows and modifies the Street Name element, but is separated from it by a Street Name Post Type or a Street Name Post Directional or both.	“Extension” in Market Street North Extension (because “North” separates “Extension” from the Street Name Post Type).

[25] PIDF-LO RD, Condition: A Street Name is required except for landmarks that have no street address (e.g., United States Capitol Building, Brooklyn Bridge), in which case a Landmark Name is required, [Ref. CLDXF NENA STA-004.1.1]

[26] PIDF-LO PRD, Condition: A primary Street Name is required before a Street Name Pre Directional can be given.

[27] PIDF-LO PRM, Condition: A Street Name is required before a Street Name Pre Modifier can be given.

[28] PIDF-LO STP, Condition: A Street Name is required before a Street Name Pre Type can be given.

[29] PIDF-LO STPS, Condition: A Street Name Pre Type must be given before a Street Name Pre Type Separator is permitted. [Ref. CLDXF NENA STA-004.1.1]

[30] PIDF-LO POD, Condition: A Street Name is required before a Street Name Post Directional can be given.

[31] PIDF-LO STS, Condition: A Street Name is required before a Street Name Post Type can be given.

[32] PIDF-LO POM, Condition: A Street Name is required before a Street Name Post Modifier can be given. [Ref. CLDXF NENA STA-004.1.1]

Attribute[17]	Mandatory/Optional	Description	Example
Address Number Prefix[33]	C	An extension of the Address Number that precedes it and further identifies a location along a thoroughfare or within a defined area.	“194-0” in 194-03 1/2 50th Avenue, New York, NY 11365.
Address Number[34]	C	The numeric identifier of a location along a thoroughfare or within a defined community.	"123" in 123 Main Street.
Address Number Suffix[35]	C	An extension of the Address Number that follows it and further identifies a location along a thoroughfare or within a defined area.	“A” in 123A Main Street.
Milepost[36]	C	A distance travelled along a route such as a road or highway, typically indicated by a milepost sign.	“Post 15” in East Bay Bridge Tunnel.
Landmark Name Part[37]	C	The name or collection of names by which a prominent feature is publicly known.	“University of South Florida” and “Sun Dome” in University of South Florida Sun Dome.
Complete Landmark Name[38]	C	The name by which a prominent feature is publicly known.	University of South Florida Sun Dome.

* NOTE**:** The Reference Point may either be a MAC or BT-PDA.

Subaddress Elements

In addition to regular location elements conveyed within the PIDF-LO, there are additional location subaddress elements that provide more granular information associated with a Dispatchable Location. The following paragraph, taken from the NENA CLDXF (NENA-STA-004.1.1) standard [Ref 35] describes how subaddress elements are listed, and because of this, it illustrates how useful they could be in emergency services, if included as part of the civic address data.

[From NENA-STA-004.1.1, Section 3.6.1] “Subaddresses occur within a wide variety of residential and commercial buildings, from single basement apartments to multi-structure office parks, as well as countless specialized structures such as airports, piers, warehouses, manufacturing plants, parking garages, and stadiums. The CLDXF follows the PIDF-LO in providing a structured set of six elements to hold subaddress information: Building, Floor, Unit, Room, Seat, and Additional Location Information. This hierarchy has some limitations: not all site and building subaddress components fit easily into this set of six elements, and the elements can be difficult to distinguish in

[33] PIDF-LO HNP, Condition: An Address Number is required before an Address Number Prefix can be given.

[34] PIDF-LO HNO, Condition: A Street Name is required before an Address Number can be given.

[35] PIDF-LO HNS, Condition: An Address Number is required before an Address Number Suffix can be given.

[36] PIDF-LO MP, Condition: A Street Name is required before a Milepost can be given.

[37] PIDF-LO LMKP, Condition: A Landmark Name Part is optional unless the landmark has no corresponding street address (e.g., United States Capitol Building), in which case a Landmark Name Part is required.

[38] PIDF-LO LMK, Condition: A Complete Landmark Name is required if one or more Landmark Name Parts are given. A Landmark Name Part is required before a Complete Landmark Name can be given.

practice. Although the IETF does not make recommendations on the contents of these fields, NENA recommends that a type and identifier be included. Each element has notes describing its usage."

Table 7.7 – Subaddress Elements for Heightened Location

Attribute	Mandatory/Optional	Description	Example
Building[39]	O	One among a group of buildings that have the same address number and complete street name.	"Building A" in 456 Oak Street, Building A, Apartment 206.
Additional Location[40] Information	O	Zone within a building (NW, SW, NE, SE) <=50 Meters	Zone=NW
Floor[41]	O	A floor, story, or level within a building.	"5th Floor" in 800 Jefferson Street, 5th Floor.
Unit[42]	O	A group or suite of rooms within a building that are under common ownership or tenancy, typically having a common primary entrance.	"Apartment 12" in 422 Via Casitas, Apartment 12.
Room[43]	O	A single room within a building.	"Room 137" in 123 Main Street, Room 137.
Seat[44]	O	A place where a person might sit within a building.	"Cubicle 23" in 2500 Seventh Street, Room 105, Cubicle 23.
Place Type[45]**	O	The type of feature identified by the address.	RSS (*meaning Single Family Residential – Single Story*).

[39] PIDF-LO BLD, Note since the Nq interface returns candidate Dispatchable Location and geographic information, in the format of PIDF-LO, the attributes in this table closely align with the NENA defined CLDXF PIDF-LO element profile.

[40] PIDF-LO LOC

[41] PIDF-LO FLR

[42] PIDF-LO UNIT

[43] PIDF-LO ROOM

[44] PIDF-LO SEAT

[45] PIDF-LO PLC

** If present, the Place Type element shall be populated with the three-character notation as follows:

Table 7.8 – Place Types

Code	Description	Examples
RSS	Single Family Residential – Single story	A one-story private home, no matter how large in square footage. (NOTE: It may be attached to another dwelling, but they are independent living units)
RMS	Single Family Residential – Multi-story	A multi-story private home, no matter how large in square footage. (NOTE: It may be attached to another dwelling, but they are independent living units)
MTS	Multi-Tenant Residential – Single story	One building, subdivided into apartments, condos, suites, hotel rooms, or other living spaces on one floor.
MTM	Multi-Tenant Residential – Multi-story	One building, subdivided into apartments, condos, suites, hotel rooms, or other living spaces on two or more floors.
CMS[46]	Commercial – Single story	A one-story building with no residential use. Includes office buildings, schools, government buildings, churches, libraries, stores, malls, museums, aquariums, factories, stadiums, warehouses, shipping terminals, public transportation buildings, or other similar facilities.
CMM[46]	Commercial – Multi-story	A multi-story building with no residential use. Includes office buildings, schools, government buildings, churches, libraries, stores, malls, museums, aquariums, parking structures, factories, stadiums, warehouses, shipping terminals, public transportation buildings, or other similar facilities.
MUM	Multi-Use – Multi-story (building with both commercial & residential occupants)	A multi-story, multi-use building featuring residential and commercial uses.

[46] In this context, Commercial refers to non-residential.

Code	Description	Examples
MUS	Multi-Use – Single story (building with both commercial & residential occupants)	A single-story, multi-use building featuring residential and commercial uses.

NOTE: Reference IANA registry URL for Place Type values:

http://www.iana.org/assignments/location-type-registry/location-type-registry.xhtml#location-type-registry-1

This registry value is added on a first-come, first-served basis.

Modifying Reference Point Information

The user may modify Reference Point information on behalf of the OWNER.

This may be performed by using an implicit query that obtains the MAC or BT-PDA information, then having the user edit the information and resubmit it. Table 7.13 should be used for modifying MAC or BT-PDA information.

If the MAC or BT-PDA does not exist, the user will be given an error indication with information on how to correct the error. If the information does not successfully validate, the user will be given an error indication with information on how to correct the error.

Deleting Reference Point Information

The user may delete Reference Point information on behalf of the OWNER. The user may delete a specific Reference Point or all Reference Points for which the OWNER is responsible.

Table 7.9 illustrates the attributes for the deletion capability. OWNER is mandatory and MAC or BT-PDA is optional. If MAC or BT-PDA is not specified, the system will delete all MAC or BT-PDA addresses associated with the OWNER. If MAC or BT-PDA is specified, only information related to that MAC or BT-PDA will be deleted. To avoid erroneous deletion, the NEAM shall request a user to confirm any deletion and shall provide a warning in case all Reference Points are to be deleted.

If the OWNER is not responsible for the MAC or BT-PDA, an error indication will be returned with information on how to correct the error.

Table 7.9 – Attributes for MAC Deletion

Attribute	Mandatory/Optional	Description	Example
OWNER	M	Identifies the OWNER	MYCO
MAC*	O	Specifies the MAC address to be deleted	A0-12-34-56-78-90
BT-PDA*	O	Specifies the Bluetooth Public Device Address to be deleted.	DE:30:5D:54:75:B4

***** NOTE**:** The deletion request may contain either a MAC or BT-PDA or neither.

7.3.5.1 NEAM Np M2M Interface

External Data Sources may use the Np interface as an XML-based M2M interface to communicate Access Point or BT-PDA location information to the NEAM. Request messages must be included in a HTTP POST. Responses will be returned in an HTTP 200 OK message. Errors are application level errors and returned in the body of an HTTP 200 OK response. The Np interface supports HTTP 1.1, and optionally supports HTTP/2.

The Np M2M interface supports sending multiple MAC or beacon addresses and associated location in a single request (i.e., an HTTP POST). The response will indicate the success or failure of each in the response (HTTP 200 OK). This exchange is shown in Figure 7.2 where the External Data Source submits multiple MAC addresses and their associated locations. The NEAM will attempt to validate and geocode the information and return the results to the External Data Source (e.g., MAC 1 and 2 are successful and MAC 3 contains an error).

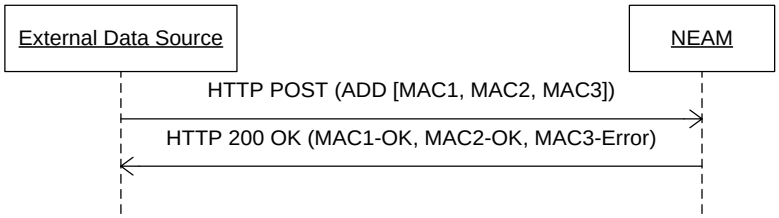


Figure 7.2 – Np M2M Interactions

External Data Sources may query for, add, modify, or delete information associated with an Access Point or Bluetooth device. The following tables identify the XML elements associated with each action. XML schemas for the Np interface are contained within a zip file published along with this standard. If there are any discrepancies between the XML schemas and the tables below, the XML schemas are the authoritative source.

Querying Reference Points

The External Data Source may query for Reference Points for the responsible OWNER. The query may be for 1) a specific Reference Point, 2) all Access Points or all Beacons that the OWNER is responsible for, 3) all Reference Points that the OWNER is responsible for, or 4) all Reference Points that the OWNER is responsible for that have civic locations that contain certain specific field values.

Table 7.10 – Query Request Elements

Element[47]	Mandatory/ Optional/ Conditional	Description	Example
QUERY-REQUEST	M	Root Element	
>OWNER	M	Identifies the OWNER	MYCO
>FILTER	O	Filter based on Reference Point identity or Reference Point civic location.	
--choice--			
>>MAC*	C	Specifies the MAC address to be queried.	A0-12-34-56-78-90 Or “all”
>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be queried.	DE:30:5D:54:75:B4 Or “all”

[47] The format of these tables is intended to represent XML formatting. Therefore an element with double carrots “>>” is the child of an element with a single carrot “>”. Example: parent >element1, child >>element2. “choice” means that only one element is chosen.

Element[47]	Mandatory/ Optional/ Conditional	Description	Example
>>CIVIC-LOCATION*	C	Specifies one or more civic location fields as defined in Table 7.13. NOTE: Matching Reference Points will have civic locations that include all of the provided fields.	State=CA, City=San Diego
--end choice--			

***** NOTE: The Filter element may contain a MAC only, BT-PDA only, or CIVIC-LOCATION only.

Table 7.11 – Query Response Elements

Element	Mandatory/ Optional/ Conditional	Description	Example
QUERY-RESPONSE	M	Root Element	
>RESPONSE	C	This may appear multiple times if multiple location information is returned.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities (may occur multiple times).	
--choice--			
>>>MAC*	C	Specifies the MAC address queried.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address queried.	DE:30:5D:54:75:B4
--end choice--			
--choice--			
>>CIVIC-ADDRESS	M	Location Information represented as defined in NENA CLDXF schema.	
>>ERROR	C	Indicates an error for the action.	
>>CODE	M	Error Code	unavailable
>>MESSAGE	O	Free format error message.	MAC address does not exist.
--end choice--			

***** NOTE: The Identity element may contain a MAC or BT-PDA.

The following error codes are defined:

unauthorized	User not authorized to query for this MAC/BT Public Device Address
unavailable	MAC/BT Public Device Address information or provided CIVIC-LOCATION field(s) does (do) not exist

timeout Request timeout

Adding Reference Point Information

The External Data Source may add information associated with one or more Reference Points on behalf of the OWNER. This is the validated address for the Reference Point.

Table 7.12 – Adding Information Request Elements

Element	Mandatory/ Optional/ Conditional	Description	Example / Comments
ADD-REQUEST	M	Root Element	
>OWNER	M	Entity responsible for the address.	MYCO
>MAC-INFO	M	Parent for IDENTITY and CIVIC-ADDRESS. This may appear multiple times if multiple location information is submitted.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address to be added.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be added.	DE:30:5D:54:75:B4
--end choice--			
>>CIVIC-ADDRESS	M	Location Information as defined in NENA CLDXF schema.	

***** NOTE**:** The Identity element may contain either a MAC or BT-PDA.

Table 7.13 – Adding Information Response Elements

Element	Mandatory/ Optional/ Conditional	Description	Example
ADD-RESPONSE	M	Root Element	
>RESULT	M	Parent for IDENTITY and status. This may appear multiple times if multiple status information is returned.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address added.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address added.	DE:30:5D:54:75:B4
--end choice--			
--choice--			
>>OK	C	Indicates action successfully performed.	
>>INVALID	C	Contains sub-elements identifying the invalid fields (FIELD) and optionally makes recommendations for alternatives (ALTERNATIVIES).	
>>ERROR	C	Indicates there is an error for the action.	
>>>CODE	M	Error Code	702
>>>MESSAGE	O	Free format error message.	Record Already Exists
--end choice--			

***** NOTE**:** The Identity element may contain either a MAC or BT-PDA.

Modifying Reference Point Information

The External Data Source may modify information associated with one or more Reference Points on behalf of the OWNER.

Table 7.14 – Modifying Information Request Elements

Element	Mandatory/Optional/ Conditional	Description	Example
MODIFY-REQUEST	M	Root Element	
>OWNER	M	Entity responsible for the MAC address.	MYCO

Element	Mandatory/Optional/ Conditional	Description	Example
>MAC-INFO	M	Parent for IDENTITY and CIVIC-ADDRESS. This may appear multiple times if multiple location information is modified.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address to be queried.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be queried.	DE:30:5D:54:75:B4
--end choice--			
>>CIVIC-ADDRESS	M	Location Information as defined in NENA CLDXF schema.	

***** Note**:** The Identity element may contain either a MAC or BT-PDA.

Table 7.15 – Modifying Information Response Elements

Element	Mandatory/ Optional/ Conditional	Description	Example
MODIFY-RESPONSE	M	Root Element	
>RESULT	M	Parent for IDENTITY and status. This may appear multiple times if multiple location information is returned.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address to be modified.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be modified.	DE:30:5D:54:75:B4
--end choice--			
--choice--			

Element	Mandatory/ Optional/ Conditional	Description	Example
>>OK	C	Indicates action successfully performed.	
>>ERROR	C	Indicates there is an error for the action.	
>>>CODE	M	Error Code	712
>>>MESSAGE	O	Free format error message.	Record Does Not Exist
>>INVALID	C	Contains sub-elements identifying the invalid fields (FIELD) and optionally makes recommendations for alternatives (ALTERNATIVIES).	
--end choice--			

***** NOTE: The Identity element may contain either a MAC or BT-PDA.

Deleting Reference Point Information

The External Data Source may delete Reference Point information on behalf of the OWNER. The External Data Source may delete a specific Reference Point or all Reference Points for which the OWNER is responsible.

OWNER is mandatory and MAC/BT-PDA is optional. If MAC/BT-PDA is not specified, the system will delete all addresses associated with the OWNER. If MAC/MAC-PDA is specified, only information related to that Reference Point will be deleted.

Table 7.16 – Deleting Information Request Elements

Element	Mandatory/Optional/ Conditional	Description	Example
DELETE-REQUEST	M	Root Element	
>OWNER	M	Entity responsible for the MAC address.	MYCO
>IDENTITY	O	Parent for MAC and BT-PDA identities. May occur multiple times if multiple Access Points or Beacons are deleted. If not specified, all Reference Points will be deleted.	
--choice--			
>>MAC*	C	Specifies the MAC address to be deleted.	A0-12-34-56-78-90
>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be deleted.	DE:30:5D:54:75:B4
--end choice--			

***** NOTE**:** The Identity element may contain either a MAC or BT-PDA.

Table 7.17 – Deleting Information Response Elements

Element	Mandatory/ Optional/ Conditional	Description	Example
DELETE-RESPONSE	M	Root Element	
--choice--			
>OK	C	Indicates Access Point or Beacon not specified and all Reference Points successfully deleted.	
>ERROR	C	Indicates Access Point or Beacon not specified and there is an error for the action.	
>>CODE	M	Error Code	unavailable
>>MESSAGE	O	Free format error message.	MAC address does not exist.
>POINT	C	Indicates one or more Access Points or Beacons were specified. May occur multiple times if multiple addresses were deleted.	
>>IDENTITY	O	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address to be deleted.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be deleted.	DE:30:5D:54:75:B4
--end choice--			
--choice--			
>>OK	C	Indicates action performed.	
>>ERROR	C	Indicates an error for the action.	
>>>CODE	M	Error Code	unavailable
>>>MESSAGE	O	Free format error message.	MAC address does not exist.
--end choice--			
--end choice--			

***** NOTE**:** The Identity element may contain either a MAC or BT-PDA.

The following error codes are defined:

unauthorized	User not authorized to delete information for this MAC/BT Public Device Address
unavailable	MAC/BT Public Device Address information does not exist
timeout	Request timeout

Message Examples for the Np M2M Capabilities

Querying for MAC location information.

The following example illustrates XML content for an HTTP request for the location of a MAC address.

```
<?xml version="1.0"?>
< query-request>
        <OWNER>MYCO</OWNER>
          <IDENTITY>
                <MAC>A0-12-34-56-78-90</MAC>
        </IDENTITY
</ query-request>
```

The following illustrates a response that contains the civic address of the Access Point.

```
<?xml version="1.0"?>
< query-response>
   <RESPONSE>
        <IDENTITY>
                <MAC>A0-12-34-56-78-90</MAC>
        </IDENTITY>

        <CIVIC-ADDRESS>
                                <ca:civicAddress
                                 xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
                                 xml:lang="en-au">
                                <ca:country>US</ca:country>
                                <ca:A1>IL</ca:A1>
                                <ca:A2>DuPage</ca:A2>
                                <ca:A3>Lisle</ca:A3>
                                <ca:RD>Warrenville</ca:RD>
                                <ca:STS> Rd</ca:STS>
                                <ca:HNO>3030</ca:HNO>
                                <ca:LOC>Zone=NW</ca:LOC>
                                <ca:FLR>Floor 4</ca:FLR>
                                <ca:PC>60532</ca:PC>
                                <ca:ROOM>254</ROOM>
                                </ca:civicAddress>
        </CIVIC-ADDRESS>
  </RESPONSE>
</query-response>
```

The following example illustrates an error response where the OWNER is not responsible for the MAC and is not authorized to view information.

```
<?xml version="1.0"?>
< query-response>
        <IDENTITY>
                <MAC>A0-12-34-56-78-90</MAC>
        </IDENTITY>
        <error>
                code=unauthorized
                message=User not authorized to query for this MAC
        </error>
</mac-query-response>
```

7.3.6 ELS-NEAM Provisioning (Np') Interface

The Np' interface is between the NEAM and External Location Server (ELS). The Np' interface supports conveyance of vetted and authenticated Reference ID, CMA, and URI data content from the ELS into the NEAM.

The Np' interface at the NEAM is implemented using a Machine-to-Machine (M2M) method. This M2M capability implements an XML-based web services interface between the ELS and the NEAM. This method allows the client side to query, add, modify, or delete information based on a Reference Point for which they are responsible.

An Np' client may query the NEAM for a specific Reference Point or all Reference Points for a particular owner. The client process may add new Reference Points which have not been previously included in the NEAM. The Np' client, based on authorized policy permissions, may modify information about a Reference Point on behalf of the Reference Point's owner. The user may only modify Reference Points that they are authorized to change. The Np' client may delete a Reference Point and its associated URI. The user may only delete Reference Points that they are authorized to delete.

The term OWNER is used here to designate the entity that is ultimately responsible for the Reference Point. The term authorized user denotes an entity that acts on authority of the OWNER for NEAM access. That means that only an authorized user can query for or manage a specific Reference Point. When a user logs in with a user ID and password or has been authenticated for M2M access, he is associated with one or more OWNER(s). He can therefore manage specific Reference Points on behalf of the associated OWNER(s).

The ELS may use the Np' interface as an XML-based M2M interface to provision Reference Point (e.g., Wi-Fi Access Point MAC address or BT-PDA) key index, CMA and URI information into the NEAM. Request messages must be included in an HTTP POST. Responses will be returned in an HTTP 200 OK message. Errors are application level errors and returned in the body of an HTTP 200 OK response. The Np' interface supports HTTP 1.1, and optionally supports HTTP/2.

The Np' M2M interface supports sending multiple Wi-Fi Access Point MAC addresses or BT-PDAs along with CMA plus URI informatiion in a single request (i.e., an HTTP POST). The response will indicate the success or failure of each in the response (HTTP 200 OK). This exchange is shown in Figure 7-3 where the ELS submits multiple Reference Identifiers and their associated CMA and URI entries. The NEAM will in turn perform scheduled provisioning of the Reference ID and URI into the NEAD based on configuration and will return the results to the ELS (e.g., Reference ID 1 and 2 are successful and Reference ID 3 contains an error).

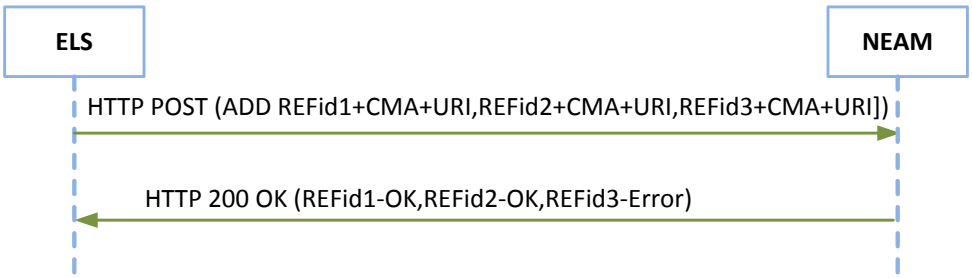


Figure 7.3 – Np' M2M Interactions

The ELS may query for, add, modify, or delete information associated with a Reference Point. The following tables identify the XML elements associated with each action. XML schemas for the Np' interface are contained within a zip file published along with this standard. If there are any discrepancies between the XML schemas and the tables below, the XML schemas are the authoritative source for information related to the Np' interface.

Querying Reference Points

The Np' client may query the NEAM by Reference Point Identifier to find those entries that belong to that OWNER. The query may be for 1) a specific Reference Point, 2) all Access Points or all Beacons that the OWNER is responsible for, 3) all Reference Points that the OWNER is responsible for, 4) all Reference Points that the OWNER is responsible for that have URIs of a certain form or 5) all Reference Points that the OWNER is responsible for that have CMA Identifiers of a specific value.

Table 7.18 – Query Request Elements

Element[48]	Mandatory/ Optional/ Conditional	Description	Example
QUERY-REQUEST	M	Root Element	
>OWNER	M	Identifies the OWNER	MYCO
>FILTER	O	Filter based on Reference Point identity or Reference Point URI.	
--choice--			
>>MAC*	C	Specifies the MAC address to be queried.	A0-12-34-56-78-90 Or “all”
>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be queried.	DE:30:5D:54:75:B4 Or “all”
>>URI*	C	URI Pointer to ELS. NOTE: Matching Reference Points will have the same value for URIs.	https://Ref-ID.els.sp.net
>>CMA	C	Specifies one or more CMA values. NOTE: FIPS code equivalent	TBD
--end choice--			

***** NOTE: The Filter element may contain a MAC only, BT-PDA only, CMA only, or URI only.

Table 7.19 – Query Response Elements

Element	Mandatory/ Optional/ Conditional	Description	Example
QUERY-RESPONSE	M	Root Element	
>RESPONSE	C	This may appear multiple times if multiple location information is returned.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities (may occur multiple times).	
--choice--			
>>>MAC*	C	Specifies the MAC address queried.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address queried.	DE:30:5D:54:75:B4
--end choice--			

[48] The format of these tables is intended to represent XML formatting. Therefore an element with double carrots “>>” is the child of an element with a single carrot “>”. Example: parent >element1, child >>element2. “choice” means that only one element is chosen.

Element	Mandatory/ Optional/ Conditional	Description	Example
--choice--			
>>URI	M	URI Pointer to ELS. NOTE: URI value in the response is the same as in the request	https://Ref-ID.els.sp.net
>>ERROR	C	Indicates an error for the action.	
>>>CODE	M	Error Code	unavailable
>>>MESSAGE	O	Free format error message.	MAC address does not exist.
>>CMA	M	Specifies Cellular Market Area value.	TBD
--end choice--			

***** NOTE: The Identity element may contain a MAC or BT-PDA.

The following error codes are defined:

unauthorized	User not authorized to query for this MAC/BT Public Device Address
unavailable	MAC/BT Public Device Address information or provided URI field(s) does (do) not exist
timeout	Request timeout

Adding Reference Point Information

The ELS may add information associated with one or more Reference Points on behalf of the OWNER. This is the URI and CMA that is associated with a validated address in the ELS that represents the Reference Point.

Table 7.20 – Adding Information Request Elements

Element	Mandatory/ Optional/ Conditional	Description	Example / Comments
ADD-REQUEST	M	Root Element	
>OWNER	M	Entity responsible for the address.	MYCO
>MAC-INFO	M	Parent for IDENTITY and CIVIC-ADDRESS. This may appear multiple times if multiple location information is submitted.	

Element	Mandatory/ Optional/ Conditional	Description	Example / Comments
>>IDENTITY	M	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address to be added.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be added.	DE:30:5D:54:75:B4
--end choice--			
>>URI	M	URI Pointer to ELS.	https://Ref-ID.els.sp.net
>>CMA	M	Specifies Cellular Market Area value	TBD

***** NOTE**:** The Identity element may contain either a MAC or BT-PDA.

Table 7.21 – Adding Information Response Elements

Element	Mandatory/ Optional/ Conditional	Description	Example
ADD-RESPONSE	M	Root Element	
>RESULT	M	Parent for IDENTITY and status. This may appear multiple times if multiple status information is returned.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address added.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address added.	DE:30:5D:54:75:B4
--end choice--			
--choice--			
>>OK	C	Indicates action successfully performed.	
>>INVALID	C	Contains invalid value, either URI or CMA	https://Ref-IDk.els.sp.net or TBD
>>ERROR	C	Indicates there is an error for the action.	

Element	Mandatory/ Optional/ Conditional	Description	Example
>>>CODE	M	Error Code	702
>>>MESSAGE	O	Free format error message.	Record Already Exists
--end choice--			

***** NOTE**:** The Identity element may contain either a MAC or BT-PDA.

Modifying Reference Point Information

The ELS may modify information associated with one or more Reference Points on behalf of the OWNER.

Table 7.22 – Modifying Information Request Elements

Element	Mandatory/Optional/ Conditional	Description	Example
MODIFY-REQUEST	M	Root Element	
>OWNER	M	Entity responsible for the MAC address.	MYCO
>MAC-INFO	M	Parent for IDENTITY and URI. This may appear multiple times if multiple location information is modified.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address to be queried.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be queried.	DE:30:5D:54:75:B4
--end choice--			
>>URI	M	URI Pointer to ELS.	https://Ref-ID.els.sp.net
>>CMA	M	Specifies CMA value (FIPS code equivalent)	TBD

* Note: The Identity element may contain either a MAC or BT-PDA.

Table 7.23 – Modifying Information Response Elements

Element	Mandatory/ Optional/ Conditional	Description	Example
MODIFY-RESPONSE	M	Root Element	
>RESULT	M	Parent for IDENTITY and status. This may appear multiple times if multiple location information is returned.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address to be modified.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be modified.	DE:30:5D:54:75:B4
--end choice--			
--choice--			
>>OK	C	Indicates action successfully performed.	
>>ERROR	C	Indicates there is an error for the action.	
>>>CODE	M	Error Code	712
>>>MESSAGE	O	Free format error message.	Record Does Not Exist
>>INVALID	C	Contains invalid value. Either URI or CMA	https://Ref-IDk.els.sp.net or TBD
--end choice--			

* NOTE: The Identity element may contain either a MAC or BT-PDA.

Deleting Reference Point Information

The ELS may delete Reference Point information on behalf of the OWNER. The ELS may delete a specific Reference Point or all Reference Points for which the OWNER is responsible.

OWNER is mandatory and MAC/BT-PDA is optional. If MAC/BT-PDA is not specified, the system will delete all addresses associated with the OWNER. If MAC/BT-PDA is specified, only information related to that Reference Point will be deleted.

Table 7.24 – Deleting Information Request Elements

Element	Mandatory/Optional/ Conditional	Description	Example
DELETE-REQUEST	M	Root Element	
>OWNER	M	Entity responsible for the MAC address.	MYCO

Element	Mandatory/Optional/ Conditional	Description	Example
>IDENTITY	O	Parent for MAC and BT-PDA identities. May occur multiple times if multiple Access Points or Beacons are deleted. If not specified, all Reference Points will be deleted.	
--choice--			
>>MAC*	C	Specifies the MAC address to be deleted.	A0-12-34-56-78-90
>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be deleted.	DE:30:5D:54:75:B4
--end choice--			

***** NOTE**:** The Identity element may contain either a MAC or BT-PDA.

Table 7.25 – Deleting Information Response Elements

Element	Mandatory/ Optional/ Conditional	Description	Example
DELETE-RESPONSE	M	Root Element	
--choice--			
>OK	C	Indicates Access Point or Beacon not specified and all Reference Points successfully deleted.	
>ERROR	C	Indicates Access Point or Beacon not specified and there is an error for the action.	
>>CODE	M	Error Code	unavailable
>>MESSAGE	O	Free format error message.	MAC address does not exist.
>POINT	C	Indicates one or more Access Points or Beacons were specified. May occur multiple times if multiple addresses were deleted.	
>>IDENTITY	M	Parent for MAC and BT-PDA identities.	
--choice--			
>>>MAC*	C	Specifies the MAC address to be deleted.	A0-12-34-56-78-90
>>>BT-PDA*	C	Specifies the Bluetooth Public Device Address to be deleted.	DE:30:5D:54:75:B4
--end choice--			
--choice--			
>>OK	C	Indicates action performed.	

Element	Mandatory/ Optional/ Conditional	Description	Example
>>ERROR	C	Indicates an error for the action.	
>>>CODE	M	Error Code	unavailable
>>>MESSAGE	O	Free format error message.	MAC address does not exist.
--end choice--			
--end choice--			

***** NOTE**:** The Identity element may contain either a MAC or BT-PDA.

The following error codes are defined:

unauthorized	User not authorized to delete information for this MAC/BT Public Device Address
unavailable	MAC/BT Public Device Address information does not exist
timeout	Request timeout

Message Examples for the Np' M2M Capabilities

Querying for MAC location information between the ELS and NEAM.

The following example illustrates XML content for an HTTP request for the data contents associated with a MAC address.

```
<?xml version="1.0"?>
< query-request>
        <OWNER>MYCO</OWNER>
          <IDENTITY>
                <MAC>A0-12-34-56-78-90</MAC>
        </IDENTITY
</ query-request>
```

The following illustrates a response that contains the Reference ID of the Access Point.

```
<?xml version="1.0"?>
< query-response>
    <RESPONSE>
        <IDENTITY>
                <MAC>A0-12-34-56-78-90</MAC>
        </IDENTITY>

        <CMA>
                <011>
        </CMA>

        <URI>
                https://Ref-ID.els.sp.net
        </URI>
   </RESPONSE>
</query-response>
```

The following example illustrates an error response where the OWNER is not responsible for the MAC and is not authorized to view information.

```
<?xml version="1.0"?>
< query-response>
        <IDENTITY>
                <MAC>A0-12-34-56-78-90</MAC>
        </IDENTITY>
        <error>
                code=unauthorized
                message=User not authorized to query for this MAC
        </error>
</mac-query-response>
```

7.4 Support for LTE Access

This clause defines architectural support for heightened accuracy location with LTE access.

7.4.1 Architecture

Figure 7.3 shows details of architectural support for a UE that originates an IMS emergency call via LTE access when heightened accuracy location is supported by a NEAD.

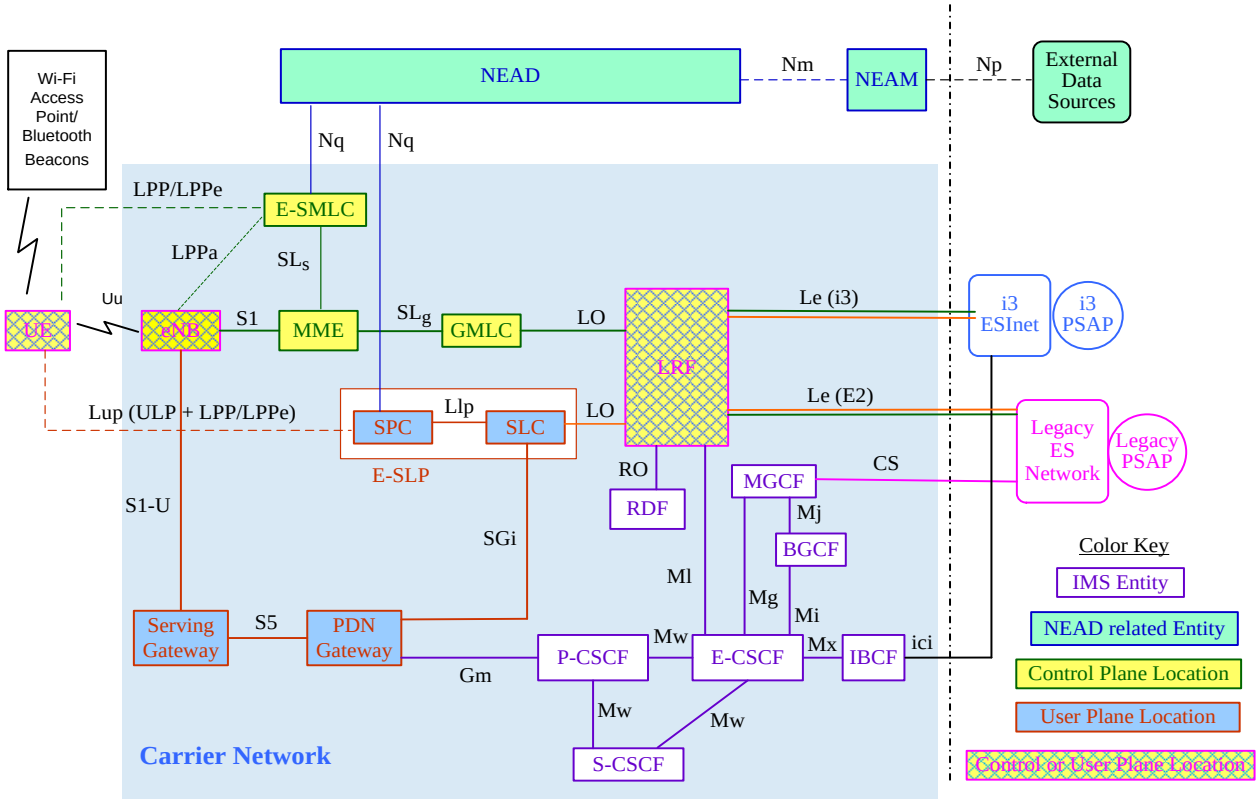


Figure 7.3 – Architecture for Heightened Accuracy Location with LTE Access

For LTE access, and as shown in Figure 7.3, the interface to the NEAD from the serving core network occurs at the E-SMLC when a UE is located using the 3GPP control plane solution and at the E-SPC when the UE is located using the SUPL user plane solution. In the case that the SPC and SLC functions of an E-SLP are combined (e.g.,

the Llp interface is either missing or internal to an E-SLP), the NEAD interface for SUPL location may occur at the E-SLP.

7.4.2 Interfaces & Protocols for Control Plane Location

This clause summarizes impacts to interfaces and protocols within and to a serving LTE core network (EPC) to support heightened accuracy location in the case of control plane location where location delivery to an Emergency Services Network occurs over the Le interface. Figure 7.4 shows the subset of the architecture in Figure 7.3 that applies to control plane location.

NOTE: Information related to heightened accuracy location is referred to generically here as "heightened accuracy location information" (HALI). This information may include one or more of a Dispatchable Location (DL), a geodetic location (GL), details on source position methods (SPM) that were used to obtain a geodetic location and uncompensated barometric pressure (UBP) for a suitably capable UE.

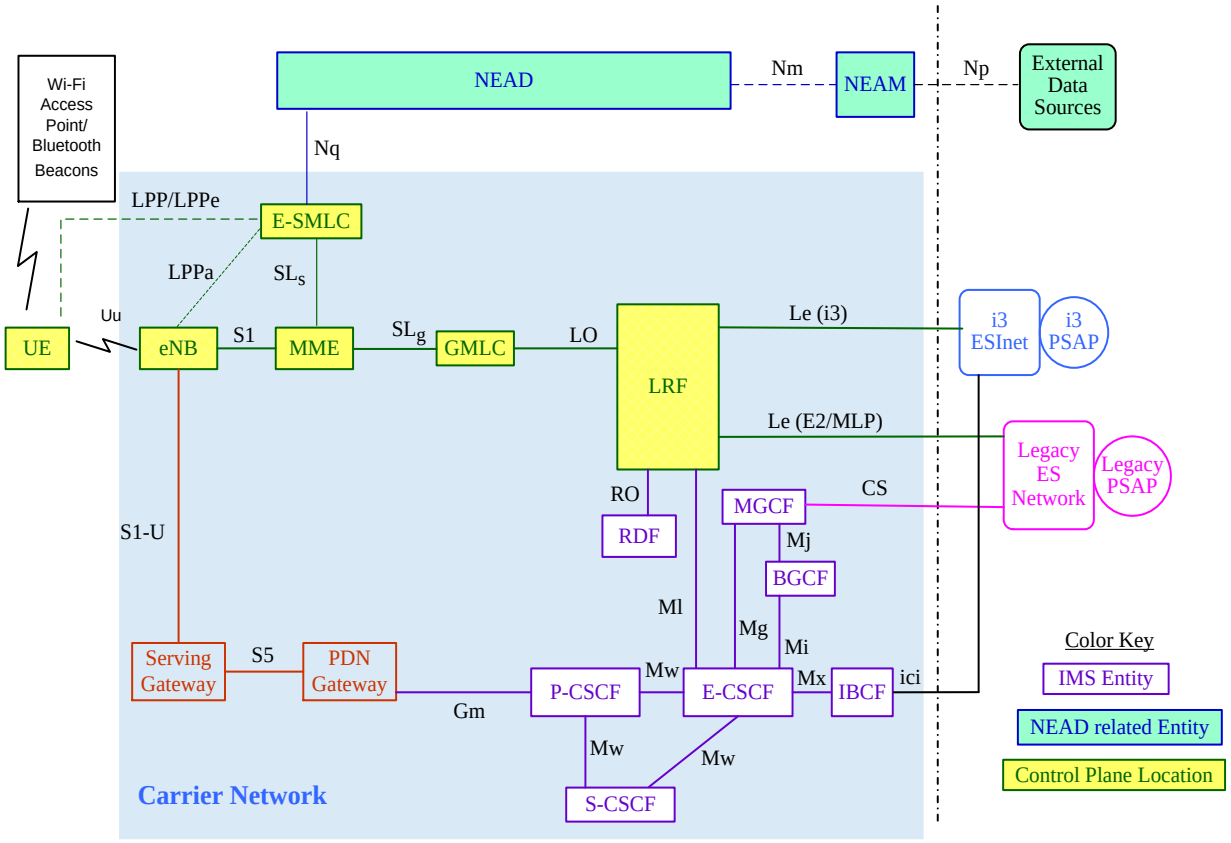


Figure 7.4 – Architecture for Heightened Accuracy Location with LTE Access and Control Plane Location

7.4.2.1 Uu, S1, & SLs Interfaces (LPP/LPPe Protocols)

The LPP protocol defined in 3GPP TS 36.355 [Ref 5] combined with the OMA LPPe protocol [Ref 6] may be used over the Uu, S1, and SLs interfaces for positioning of a UE by an E-SMLC. LPP/LPPe messages are transferred between a UE and E-SMLC via the serving MME and serving eNB for the UE as partially specified in 3GPP TSs 23.271 [Ref 7] and 36.305 [Ref 8]. To support heightened accuracy location, an E-SMLC must be able to request and a UE must be able to provide the following information:

- Identities of visible Reference Points (e.g., including Wi-Fi APs and/or Bluetooth beacons).
- Signal measurements of visible Reference Points (e.g., RSSI, RTT).
- Uncompensated barometric pressure (UBP) (if supported by the UE).

The information identified above is supported in LPPe 1.0 [Ref 6] and in LPP [Ref 5].

7.4.2.2 SLs Interface (LCS-AP Protocol)

The LCS-AP protocol defined in 3GPP TS 29.171 [Ref 9] is used over the SLs interface between the serving MME for a UE and an E-SMLC to enable an MME to request location information for a UE from an E-SMLC using the 3GPP control plane solution. To support heightened accuracy location, the LCS-AP protocol must enable an E-SMLC to return HALI to the MME. As of Release 13, the LCS-AP protocol [Ref 9] supports conveyance of UBP, DL, GL, and SPM.

7.4.2.3 S1 and SLs Interfaces (LPPa Protocol)

The LPPa protocol defined in 3GPP TS 36.455 [Ref 18] is used over the S1 and SLs interfaces between the serving eNB for a UE and an E-SMLC to enable the E-SMLC to request location information for a UE from the serving eNB using the 3GPP control plane solution. As of Release 13, LPPa [Ref 18] supports conveyance of information that may be used by an E-SMLC to determine or help determine a GL.

7.4.2.4 SLg Interface (ELP Protocol)

The ELP protocol defined in 3GPP TS 29.172 [Ref 10] is used over the SLg interface between the serving MME for a UE and a GMLC to enable the GMLC to request and obtain location information for a UE using the 3GPP control plane solution. To support heightened accuracy location, the ELP protocol must enable a serving MME to return HALI to the GMLC. As of Release 13, the ELP protocol [Ref 10] supports conveyance of UBP, DL, GL, and SPM.

7.4.2.5 L0 Interface (MLP, HELD, E2 Protocols)

The L0 interface is used between an LRF and a GMLC to enable an LRF to request location information for a UE from the GMLC in the case that the UE is establishing or has established an IMS emergency call to a PSAP. To support heightened accuracy location, the L0 interface must enable a GMLC to return HALI to the LRF. Possible protocols defined for the L0 interface in ATIS-0700015 [Ref 4] comprise MLP [Ref 11], HELD [Ref 12], and the E2 interface protocol defined in J-STD-036-C-2 [Ref 3]. MLP [Ref 11] and E2 [Ref 3] support conveyance of UBP, DL, GL, and SPM.

7.4.2.6 Le Interface (E2, MLP Protocols)

The Le interface is used between an LRF and the ALI in a legacy Emergency Services Network to enable the ALI to request location information for a UE from an LRF in the case that the UE has established an emergency call to a legacy PSAP that is served by a legacy Emergency Services Network. The Le E2 interface is defined in J-STD-036-C-2 [Ref 3] and needs to enable return of HALI to ALI. The Le MLP interface is defined in OMA-TS-MLP-V3_5-20130220-D [Ref 11] and must support return of HALI to the ALI. MLP [Ref 11] and E2 [Ref 3] support conveyance of UBP, DL, GL, and SPM.

7.4.2.7 Le i3 Interface (HELD, SIP Protocols)

The Le i3 interface is used between an LRF and an Emergency Services IP network (ESInet) to enable an entity in the ESInet (e.g., an ESRP or an i3 PSAP) to request location information for a UE from an LRF in the case that the UE is establishing or has established an emergency call to the ESInet. According to ATIS-0700015 [Ref 4], the Le i3 interface may use HELD [Ref 12] or SIP SUBSCRIBE/NOTIFY [Ref 14]. Each of these protocols therefore needs to enable return of HALI.

7.4.3 Interfaces & Protocols for SUPL User Plane Location

This clause summarizes impacts to interfaces and protocols within and to a serving LTE core network (EPC) to support heightened accuracy location in the case of user plane location where location delivery to an Emergency Services Network occurs over the Le interface. Figure 7.5 shows the subset of the architecture in Figure 7.3 that applies to user plane location.

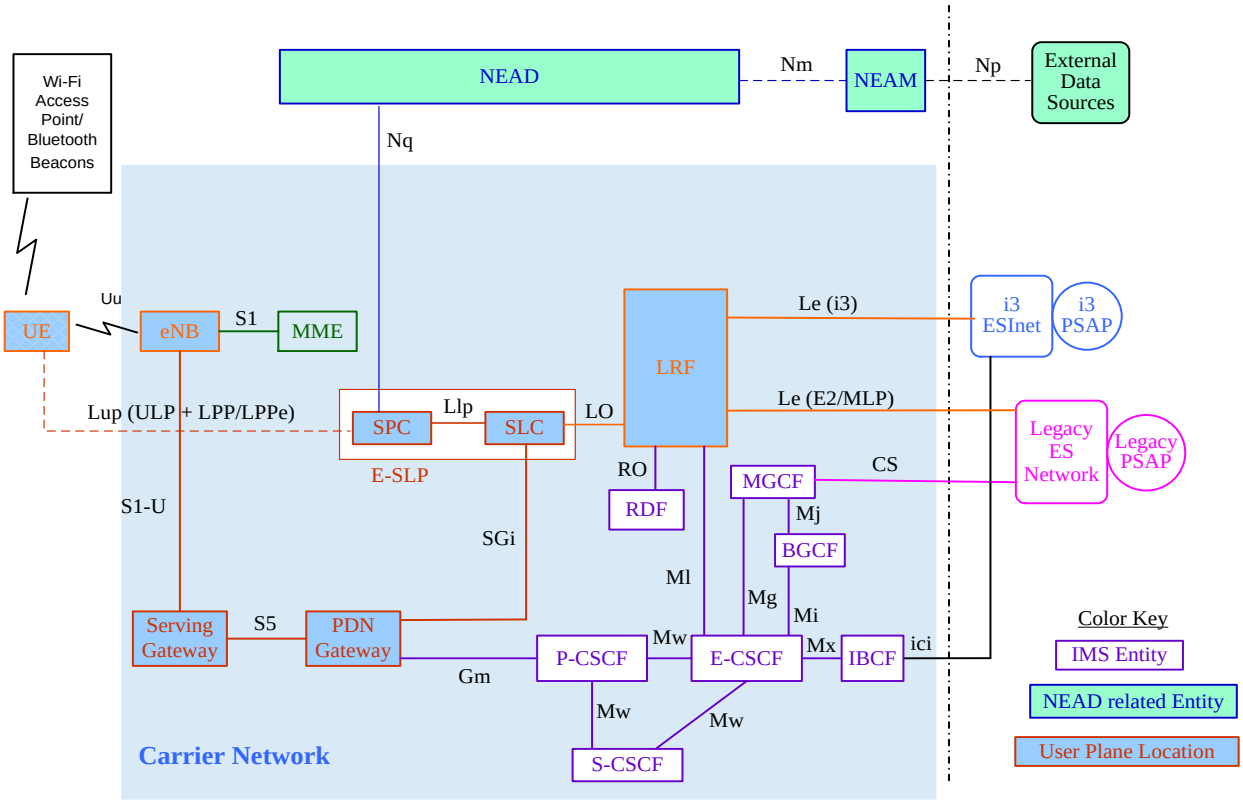


Figure 7.5 – Architecture for Heightened Accuracy Location with LTE Access and User Plane Location

7.4.3.1 Lup Interface (ULP & LPP/LPPe Protocols)

The Lup interface is defined in OMA-AD-SUPL-V2_0 [Ref 15] and is used between a UE (referred to as a SET) and an SLP to support positioning of a UE using the OMA SUPL user plane solution. In the case of location in association with an emergency call, an E-SLP is used in the serving core network. The Lup interface enables exchange of ULP messages, defined in OMA-TS-ULP-V2_0_3 [Ref 16], between the UE being positioned and the SLP. The SLP is split into an SLC and an SPC with the SLC being used to establish and control a SUPL session with a UE and the SPC being used to obtain a location of the UE. The endpoint for any ULP message is then either the SLC or the SPC depending on whether the ULP message is used for control and service provision or for positioning. In the case of a UE with LTE access, ULP messages used for positioning typically encapsulate one or more LPP messages. Each encapsulated LPP message can further encapsulate one LPPe message. To support heightened accuracy location, LPP/LPPe or LPP may be used to enable an SPC to request and a UE to return the same information as described for control plane location in clause 7.4.2.1. This information is supported in LPPe 1.0 and in LPP.

7.4.3.2 Llp Interface (ILP Protocol)

The ILP protocol defined in OMA-TS-ILP-V2_0_3 [Ref 17] is used over the Llp interface between an SLC and SPC to enable an SLC to initiate positioning of a UE using the SPC and to obtain location information for the UE from the SPC. To support heightened accuracy location, the ILP protocol must enable an SPC to return HALI to the SLC. ILP [Ref 17] supports conveyance of GL.

7.4.3.3 L0 Interface (MLP, HELD, E2 Protocols)

The L0 interface is used between an LRF and an E-SLP to enable an LRF to request location information for a UE from the E-SLP in the case that the UE is establishing or has established an IMS emergency call to a PSAP. To support heightened accuracy location, the L0 interface must enable an E-SLP to return heightened accuracy location information to the LRF. Possible protocols defined for the L0 interface in ATIS-0700015 [Ref 4] comprise MLP [Ref 11], HELD [Ref 12], and the E2 interface protocol defined in J-STD-036-C-2 [Ref 3]. MLP [Ref 11] and E2 [REF 3] support conveyance of UBP, DL, GL, and SPM.

7.4.3.4 Le Interface

The impacts for the Le interface are the same as those described for control plane location in clause 7.4.2.6.

7.4.3.5 Le i3 Interface

The impacts for the Le i3 interface are the same as those described for control plane location in clause 7.4.2.7.

7.5 Support for UMTS Access

This clause defines architectural support for heightened accuracy location with UMTS access.

7.5.1 Architecture

Figure 7.6 shows details of architectural support for a UE that originates an emergency call via UMTS access with heightened accuracy location supported by a NEAD.

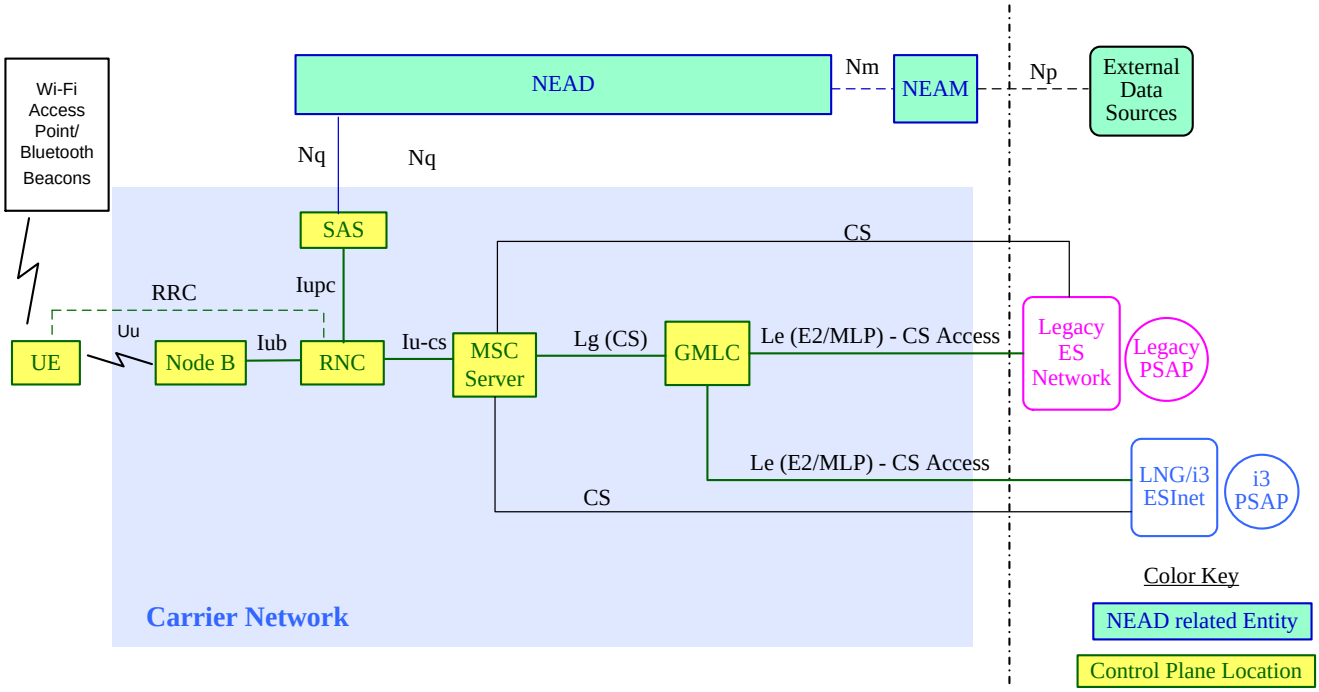


Figure 7.6 – Architecture for Heightened Accuracy Location with UMTS Access

For UMTS access, and as shown in Figure 7.6, the interface to the NEAD from the serving network occurs at the SAS when a UE is located using the 3GPP control plane solution (for access via the CS domain).

7.5.2 Interfaces & Protocols with Control Plane Location for CS Access

This clause summarizes impacts to interfaces and protocols within and to a serving UMTS network to support heightened accuracy location in the case of CS access and control plane location where location delivery to an Emergency Services Network occurs over the Le interface.

NOTE: Information related to heightened accuracy location is referred to generically here as “heightened accuracy location information” (HALI). This information may include one or more of a Dispatchable Location (DL), a geodetic location (GL), details on source position methods (SPM) that were used to obtain a geodetic location, and uncompensated barometric pressure (UBP) for a suitable capable UE.

7.5.2.1 Uu Interface (RRC Protocol)

The RRC protocol defined in 3GPP TS 25.331 [Ref 25] is used over the Uu interface for positioning of a UE by an RNC in the case of control plane location with CS access. To support heightened accuracy location, an RNC must be able to request and a UE must be able to provide the following minimal additional information.

Identities of visible Reference Points (e.g., Wi-Fi APs and/or Bluetooth beacons)

Uncompensated barometric pressure (if supported by the UE)

The information identified above is supported in RRC [Ref 25] as of Release 13.

7.5.2.2 Iupc Interface (PCAP Protocol)

The PCAP protocol defined in 3GPP TS 25.453 [Ref 40] is used over the Iupc interface between the serving RNC for a UE and an SAS to enable an RNC to request location information for a UE from an SAS using the 3GPP control plane solution. The RNC and SAS can interact using PCAP in either SAS centric mode, where the SAS controls the use of different position methods and all interaction with the UE, or in RNC centric mode where the RNC controls the use of different position methods and all interaction with the UE and invokes the SAS only to provide assistance data for the UE or to compute a location from location related measurements provided by the UE to the RNC. To support heightened accuracy location, the PCAP protocol must enable an RNC to transfer the additional location information provided by a UE using RRC, as described in clause 7.5.2.1, to the SAS and must enable the SAS to return HALI comprising DL, GL, UBP, and SPM to the RNC. These requirements apply for both SAS centric and RNC centric modes. This capability is supported by PCAP [Ref 40] as of Release 13.

7.5.2.3 Iu-cs Interface (RANAP Protocol)

The RANAP protocol defined in 3GPP TS 25.413 [Ref 39] is used over the Iupc interface between the serving MSC server for a UE and a serving RNC to enable a serving MSC server to request location information for a UE from a serving RNC using the 3GPP control plane solution. To support heightened accuracy location, the RANAP protocol must enable a serving RNC to return HALI comprising DL, GL, UBP, and SPM to the serving MSC server. This information is supported by RANAP [Ref 39] as of Release 13.

7.5.2.4 Lg Interface (MAP Protocol)

The MAP protocol defined in 3GPP TS 29.002 [Ref 41] is used over the Lg interface between the serving MSC server for a UE and a GMLC to enable the GMLC to request and obtain location information for a UE using the 3GPP control plane solution. To support heightened accuracy location, the MAP protocol must enable a serving MSC server to return heightened accuracy location information comprising DL, GL, UBP, and SPM to the GMLC. This information is supported by MAP [Ref 41] as of Release 13.

7.5.2.5 Le Interface (E2, MLP Protocols)

The Le interface is used between a GMLC and the ALI in a legacy Emergency Services Network or a Legacy Network Gateway on the ingress side of an i3 ESInet to enable the ALI/Legacy Network Gateway to request location

information for a UE from a GMLC in the case that the UE has established an emergency call to a legacy PSAP or to a PSAP that is served by an i3 ESInet, using the CS domain. The Le E2 interface is defined in J-STD-036-C-2 [Ref 3] and needs to enable return of HALI to the ALI or Legacy Network Gateway. The Le MLP interface is defined in OMA-TS-MLP-V3_5 [Ref 11] and must support return of HALI to the ALI or Legacy Network Gateway. MLP [Ref 11] and E2 [REF 3] support conveyance of UBP, DL, GL, and SPM.

7.6 High Level Signaling Flows

This clause provides high level signaling flows at a stage 2 level describing heightened accuracy location support for LTE and UMTS accesses using control plane and user plane location solutions.

7.6.1 LTE Access with Control Plane Location

This clause provides a high level signaling flow description showing heightened accuracy location support for an emergency call from a UE with LTE access and using control plane location. The signaling is shown in Figure 7.7 and described step by step below. Signaling that is related to location support is distinguished in violet.

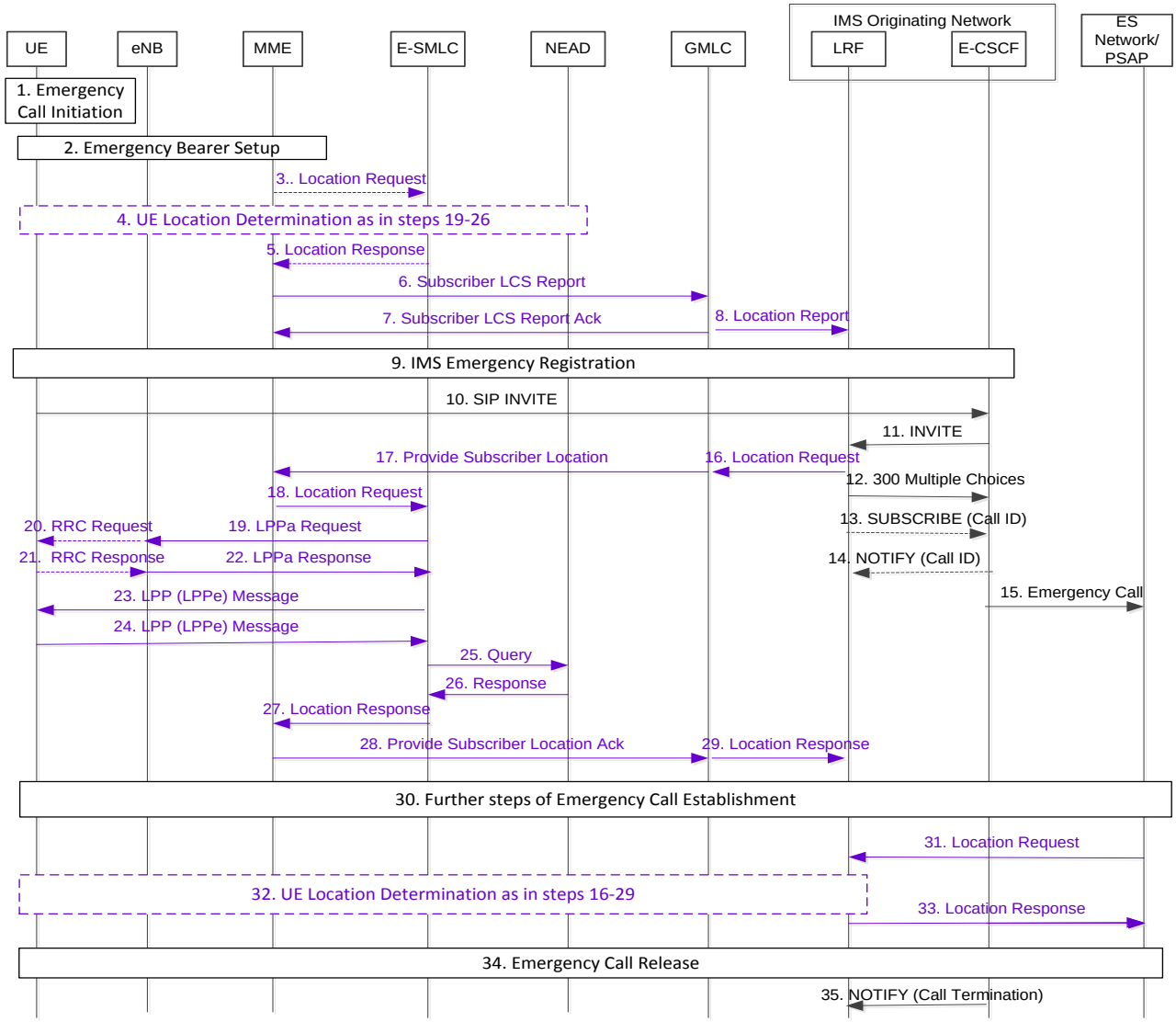


Figure 7.7 – Heightened Accuracy Location with LTE Access and Control Plane Location

Step 1. The user dials an emergency call.

Step 2. If not already attached for LTE access, the UE performs a normal LTE Attach or an Emergency LTE Attach. The UE then obtains an emergency PDN connection and a default signaling bearer as described in 3GPP TS 23.401 [Ref 19].

Step 3. Optionally, the MME sends a location request for the UE to an E-SMLC. Otherwise, the MME skips steps 3-5.

Step 4. The E-SMLC obtains the location of the UE as in steps 19-26. Steps 25-26 may not be performed in this case – e.g., if the MME did not specify high location accuracy in the location request sent in step 3.

Step 5. The E-SMLC returns the UE location to the MME.

Step 6. The MME determines a GMLC using the serving cell identity, any location obtained in step 5 or using a fixed association for the MME. The MME sends a Subscriber Location Report to the GMLC carrying the IMEI and if available the IMSI and MSISDN of the UE, the event causing the message, and, if obtained in step 5, the location estimate and its age. The serving cell identity of the UE may also be sent if available. The MME shall include its own address.

Step 7. The GMLC returns an acknowledgment to the MME.

Step 8. The GMLC forwards the information received in step 5 to the LRF.

Step 9. If the UE is normally attached to the originating network (i.e., not emergency attached), the UE performs an IMS emergency registration with the IMS originating network and with the Home network if different to the originating network.

Step 10. The UE sends a SIP INVITE to the IMS in the originating network. The SIP INVITE is first received by a P-CSCF (not shown in Figure 7.7) and then transferred to an E-CSCF. The UE includes the UE identity (the registered public user ID, MSISDN, or IMEI if the UE is not IMS emergency registered in step 9) and the serving cell ID in the SIP INVITE and may include a location estimate.

Step 11. The E-CSCF may first forward the SIP INVITE to an EATF which returns the SIP INVITE to the E-CSCF (not shown in Figure 7.7) if session continuity is supported. The E-CSCF then forwards the SIP INVITE to the LRF.

Step 12. The LRF determines routing information for the call using one or more of the information received at step 8, information in the SIP INVITE received at step 11, and any location obtained at step 29 if steps 16-29 are completed prior to step 12. The LRF uses an RDF to help determine the routing information (not shown in Figure 7.7). The LRF returns a route URI containing the routing information to the E-CSCF in a SIP 300 Multiple Choices. The LRF also includes a reference identifier identifying the LRF and possibly the UE in the 300 Multiple Choices. ATIS-0700015 [Ref 4] contains more details of LRF routing support.

Step 13. The LRF may send a SUBSCRIBE message to the E-CSCF to receive notification of future call events. As an alternative, step 13 may occur separately, once only at startup, for all emergency calls.

Step 14. The E-CSCF acknowledges any request at step 13.

Step 15. The E-CSCF uses the routing information received at step 12 to route the emergency call toward the destination PSAP through the NENA i3 ESInet or legacy Selective Router. The call related information that is provided to the PSAP includes the reference identifier from step 12 identifying the LRF and possibly the UE, and a UE identifier for location retrieval and/or for PSAP callback (if the UE is IMS emergency registered in step 9). More details of emergency call setup are provided in ATIS-0700015 [Ref 4].

Step 16. At any time after step 11, the LRF may initiate steps 16-29 to obtain high accuracy location information (HALI) for the UE. Steps 16-29 may occur in parallel to steps 12-15 and step 30. Typically, step 29 will not occur until after step 12 and possibly after steps 30 and 31. However, if the LRF specifies low accuracy QoS at step 16 and waits for completion of step 29, the UE location may be used at step 12 to assist call routing. The LRF starts the location procedure by identifying the GMLC from information received at step 8 and forwards the location request to the GMLC and includes a QoS indicating either high accuracy location if location is needed for dispatch, or low accuracy location if the location is needed only for

call routing at step 12, the address of the MME from step 8, the identity of the UE, and an indication that location is needed for an emergency call.

Step 17. The GMLC forwards the location request to the MME using a Provide Subscriber Location request.

Step 18. The MME forwards the location request to an E-SMLC.

Step 19. The E-SMLC may request location information for the UE by sending an LPPa location request to the serving eNB via the MME.

Step 20. The serving eNB may request some location information from the UE using RRC.

Step 21. The UE returns any requested location information to the serving eNB.

Step 22. The serving eNB returns any location information obtained in step 21 and/or other location information available to the serving eNB. Steps 19-22 may be repeated to request and/or provide additional location information.

Step 23. The E-SMLC may request location information for the UE by sending an LPP message to the UE via the MME and serving eNB. The LPP message may include an LPPe message.

Step 24. The UE returns any requested location information to the E-SMLC. Step 23 may be repeated to request more location information, to provide assistance data to the UE and/or to request the positioning capabilities of the UE. Step 24 may be repeated to respond to any additional request in a repetition of step 23 (e.g., to provide additional location information or the UE positioning capabilities) and/or to request assistance data from the E-SMLC. The order of the LPP (and LPPe) messages may be different in different implementations – e.g., step 23 may be used first to request the UE's positioning capabilities and then to provide assistance data to the UE or request location information.

Step 25. The location information obtained by the E-SMLC at step 22 and/or step 24 may include the identities of one or more Reference Points near the UE and UBP if supported by the UE. Based on an indication of a location request for an emergency call at step 18 and possibly based also on a request for high accuracy location (if high accuracy location is requested by the LRF at step 16), the E-SMLC may send a query to the NEAD and may include in the Query the identity of a Reference Point provided by the UE at step 24.

Step 26. The NEAD retrieves any civic location and geocoded location associated with the Reference Point provided at step 25 and returns this to the E-SMLC. Steps 25-26 may be repeated for additional Reference Points.

Step 27. The E-SMLC determines a geodetic location and/or a Dispatchable Location for the UE based on any location information received at steps 22, 24, and 26 and returns the geodetic location and/or Dispatchable Location along with any UBP in the form of HALI to the MME.

Step 28. The MME returns the HALI to the GMLC.

Step 29. The GMLC returns the HALI to the LRF. The LRF stores the HALI for future use – e.g., at step 33.

Step 30. The rest of the emergency call establishment occurs including establishment of voice and/or data media paths as described in ATIS-0700015 [Ref 4].

Step 31. The i3 PSAP or LPG or ALI sends a location request to the LRF for an initial Dispatchable Location for the UE using information received at step 15 to route the request to the LRF and to identify the UE.

Step 32. If the LRF initiated steps 16-29 to obtain high accuracy location, the LRF waits for step 29 to complete if needed and skips step 32. Otherwise (e.g., if steps 16-29 were not performed or performed only to obtain low accuracy location for call routing), the LRF initiates a request for HALI for the UE by performing steps identical to steps 16-29 as described above where high accuracy QoS is requested at step 16.

Step 33. The LRF returns the HALI obtained either at step 29 or step 32 to the i3 PSAP or LPG or ALI. Steps 31-33 may be repeated by the i3 PSAP, or legacy PSAP via LPG, or legacy PSAP via ALI at a later time to obtain updated location information. In that case, the LRF will perform step 32 to obtained updated HALI.

Step 34. The PSAP (or possibly the UE) releases the emergency call.

Step 35. The E-CSCF notifies the LRF that the emergency call was released. The LRF may then release any resources for the emergency call.

7.6.2 LTE Access with User Plane Location

This clause provides a high-level signaling flow showing heightened accuracy location support for an emergency call from a UE with LTE access and using user plane location according to OMA SUPL. The signaling is shown in Figure 7.8 and described step by step below. Signaling that is related to location support is distinguished in violet.

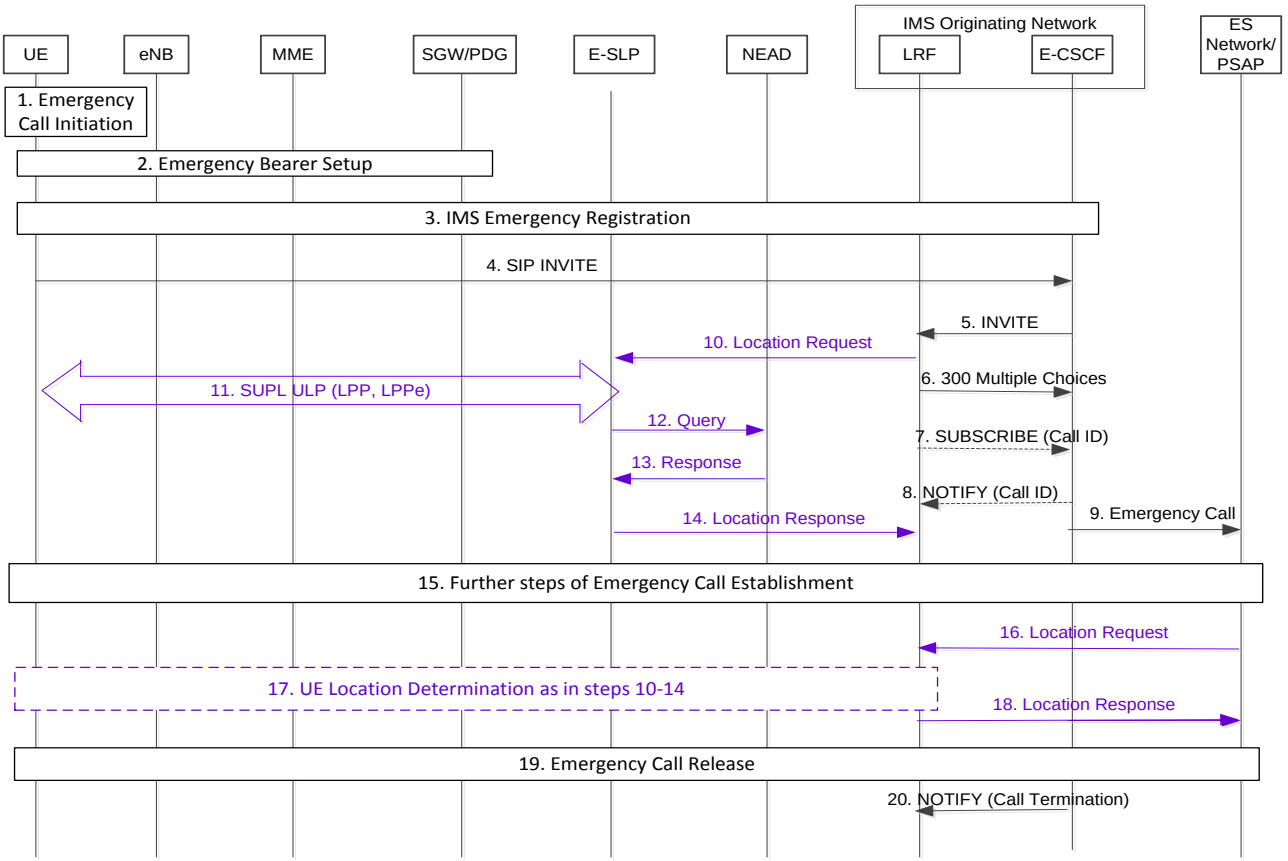


Figure 7.8 – Heightened Accuracy Location with LTE Access and User Plane Location

Step 1. The user dials an emergency call.

Step 2. If not already attached for LTE access, the UE performs a normal LTE Attach or an Emergency LTE Attach. The UE then obtains an emergency PDN connection, an IP address and a default signaling bearer as described in 3GPP TS 23.401 [Ref 19]. The default signaling bearer is supported by an SGW and PDG and enables IP based signaling in later steps between the UE and other entities in the originating PLMN such as the E-SLP and IMS.

Step 3. If the UE is normally attached to the originating network (i.e., not emergency attached), the UE performs an IMS emergency registration with the IMS originating network and with the Home network if different from the originating network.

Step 4. The UE sends a SIP INVITE to the IMS in the originating network via the SGW and PDG. The SIP INVITE is first received by a P-CSCF (not shown in Figure 7.8) and then transferred to an E-CSCF. The UE includes the UE identity (the registered public user ID, MSISDN, or IMEI if the UE is not IMS emergency registered in step 3), the UE Contact address containing the IP address obtained in step 1 or a GRUU if a GRUU is supported by the UE and was assigned by the IMS in step 3, and the serving cell ID in the SIP INVITE and may include a location estimate.

Step 5. The E-CSCF may first forward the SIP INVITE to an EATF which returns the SIP INVITE to the E-CSCF (not shown in Figure 7.8) if session continuity is supported. The E-CSCF then forwards the SIP INVITE to the LRF.

Step 6. The LRF determines routing information for the call using one or more of the information in the SIP INVITE received at step 5 and any location obtained at step 14 if steps 10-14 are completed prior to step 6. The LRF may use an RDF to help determine the routing information (not shown in Figure 7.8). The LRF returns a route URI containing the routing information to the E-CSCF in a SIP 300 Multiple Choices. The LRF also includes a reference identifier identifying the LRF and possibly the UE in the 300 Multiple Choices. ATIS-0700015 [Ref 4] contains more details of LRF routing support.

Step 7. The LRF may send a SUBSCRIBE message to the E-CSCF to receive notification of future call events. As an alternative, step 7 may occur separately, once only at startup, for all emergency calls.

Step 8. The E-CSCF acknowledges any request at step 7.

Step 9. The E-CSCF uses the routing information received at step 6 to route the emergency call toward the destination PSAP through the NENA i3 ESInet or legacy Selective Router. The call related information that can be provided to the PSAP includes the reference identifier from step 6 identifying the LRF and possibly the UE, and a UE identifier for location retrieval and/or for PSAP callback (if the UE is IMS emergency registered in step 3). More details of emergency call setup are provided in ATIS-0700015 [Ref 4].

Step 10. At any time after step 5, the LRF may initiate steps 10-14 to obtain high accuracy location information (HALI) for the UE. Steps 10-14 may occur in parallel to steps 6-9 and step 15. Typically, step 14 will not occur until after step 6 and possibly after steps 15 and 16. However, if the LRF specifies low accuracy QoS at step 10 and waits for completion of step 14, the UE location may be used at step 6 to assist call routing. The LRF starts the location procedure by sending a location request to an E-SLP and includes a QoS indicating either high accuracy location if location is needed for PSAP dispatch or low accuracy location if the location is needed only for call routing at step 6, the identity of the UE, the IP address of the UE if received at step 5, and an indication that location is needed for an emergency call.

Step 11. The E-SLP initiates a network initiated SUPL session with the UE by transferring an initial SUPL ULP message (typically a SUPL INIT message) to the UE. The initial SUPL ULP message may be transferred to the UE via the SGW and PDG using UDP/IP if the UE IP address is provided at step 10. The UE responds to the initial SUPL ULP message by establishing a secure IP connection to the E-SLP using the signaling bearer established at step 1 and then returns a SUPL ULP message that may contain some initial location information. The E-SLP and UE may then exchange additional SUPL ULP messages to enable the E-SLP to obtain further location information for the UE. The SUPL ULP messages that are exchanged may each include one or more embedded LPP messages. Each embedded LPP message may contain an embedded LPPe message. The embedded LPP and LPPe messages may enable the E-SLP to request and the UE to provide location related information. The E-SLP terminates the SUPL session when sufficient location information has been obtained. Further details of support of a SUPL positioning session for an emergency call are provided in SUPL 2.0 [Ref 20].

Step 12. The location information obtained by the E-SLP at step 11 may include the identities of one or more Reference Points nearby to the UE and UBP if supported by the UE. Based on indication of an emergency call at step 10 and possibly based also on a request for high accuracy location (if high accuracy location is requested by the LRF at step 10), the E-SLP may send a query to the NEAD and may include in the query the identity of a Reference Point provided by the UE at step 11.

Step 13. The NEAD retrieves any civic location and geocoded location associated with the Reference Point provided at step 12 and returns this to the E-SLP. Steps 12-13 may be repeated for additional Reference Points.

Step 14. The E-SLP determines a geodetic location and/or a Dispatchable Location for the UE based on any location information received at steps 11 and 13 and returns the geodetic location

and/or Dispatchable Location along with any UBP in the form of HALI to the LRF. The LRF stores the HALI for future use – e.g., at step 18.

Step 15. The rest of the emergency call establishment occurs including establishment of voice and/or data media paths as described in ATIS-0700015 version 3 [Ref 4].

Step 16. The i3 PSAP or LPG or ALI sends a location request to the LRF for an initial Dispatchable Location for the UE using information received at step 9 to route the request to the LRF and to identify the UE.

Step 17. If the LRF initiated steps 10-14 to obtain high accuracy location, the LRF waits for step 14 to complete if needed and skips step 17. Otherwise (e.g., if steps 10-14 were not performed or performed only to obtain low accuracy location for call routing), the LRF initiates a request for HALI for the UE by performing steps identical to steps 10-14 as described above where high accuracy QoS is requested at step 10.

Step 18. The LRF returns the HALI obtained either at step 14 or step 17 to the i3 PSAP or LPG or ALI. Steps 16-18 may be repeated by the i3 PSAP, or legacy PSAP via LPG, or legacy PSAP via ALI at a later time to obtain updated location information. In that case, the LRF will perform step 17 to obtain updated HALI.

Step 19. The PSAP (or possibly the UE) releases the emergency call.

Step 20. The E-CSCF notifies the LRF that the emergency call was released. The LRF may then release any resources for the emergency call.

7.6.3 UMTS Access with CS Access & Control Plane Location

This clause provides a high-level signaling flow showing heightened accuracy location support for an emergency call from a UE with UMTS CS access and using control plane location. The signaling is shown in Figure 7.9 and described step by step below. Signaling that is related to location support is distinguished in violet.

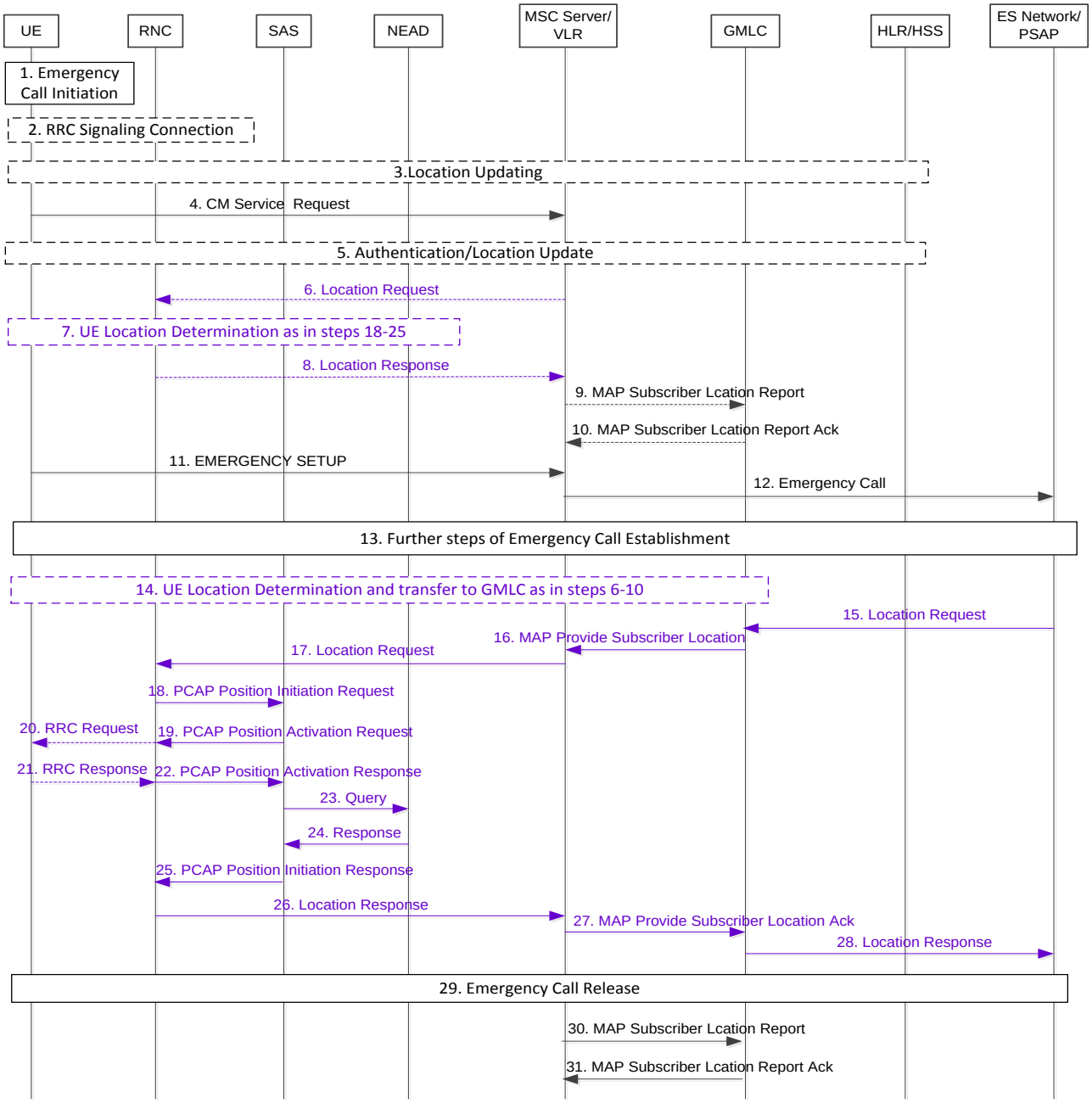


Figure 7.9 – Heightened Accuracy Location with UMTS CS Access and Control Plane Location

Step 1. The user dials an emergency call.

Step 2. If the UE has no UMTS signaling connection (e.g., the UE is initially idle or attached to LTE), the UE obtains an RRC signaling connection as described in 3GPP TS 25.331 [Ref 25]. If the UE was combined attached to LTE and UMTS with CSFB allowed to UMTS, the UE initiates CSFB on the LTE side as described in 3GPP TS 23.272 [Ref 24] before obtaining the RRC signaling connection.

Step 3. The UE may perform a Location Update with the MSC Server/VLR and HLR/HSS in the HPLMN if not registered in the current UMTS Location Area. This step is optional for an emergency call.

Step 4. The UE sends a CM Service Request to the MSC Server indicating an emergency call and includes an identifier for the UE – consisting of a TMSI if already assigned by the MSC Server/VLR, otherwise an IMSI if available, or the IMEI.

Step 5. For a UE identified by an IMSI or TMSI, the MSC Server may perform authentication of the UE. As an option for CSFB where location update did not occur in step 3 and the IMSI is unknown to the MSC Server/VLR, the MSC Server/VLR may perform a location update on behalf of the UE. The MSC Server returns a CM Service Accept to the UE if authentication is not successfully performed. Further details of steps 3-5 are provided in 3GPP TS 24.008 [Ref 26], 3GPP TS 23.272 [Ref 24], and 3GPP TS 23.018 [Ref 27].

Step 6. Steps 9-10 are optional and are performed only if the MSC Server makes use of a GMLC to obtain routing information for the emergency call. When steps 9-10 are performed, the MSC Server may first send a location request for the UE to the serving RNC. Otherwise, the MSC Server skips steps 6-8.

Step 7. The serving RNC obtains the location of the UE as in steps 18-25. Steps 23-24 may not be performed in this case – e.g., if the MSC Server did not specify high location accuracy in the location request sent in step 6.

Step 8. The serving RNC returns the UE location to the MSC Server

Step 9. The MSC Server determines a GMLC based on the serving cell identity, SAI, any location obtained in step 8, advance knowledge of the PSAP toward which the emergency call will be routed, or using a fixed association for the MSC Server. The MSC Server sends a MAP Subscriber Location Report to the GMLC carrying any location estimate returned in step 8, the age of this estimate, the MSISDN, IMSI and/or IMEI of the calling UE, the information about the positioning method used, and the serving cell identity or SAI of the UE. In case of a (U)SIM-less emergency call, or a non-registered (U)SIM emergency call, the IMEI shall always be sent and the MSISDN shall be populated with a non-dialable callback number. The message shall also indicate the event that triggered the location report. The MSC Server may also include an ESRD or ESRK if assigned by the MSC server.

Step 10. The GMLC translates the location estimate, cell identity, or SAI into a PSAP zone identity and assigns either an ESRK or ESRD indicating a PSAP routing destination. The GMLC returns the ESRK or ESRD to the MSC Server. The GMLC stores the assigned ESRD or ESRK and the information received in step 9.

Step 11. The UE sends an EMERGENCY SETUP message to the MSC Server.

Step 12. If steps 9-10 are performed, the MSC Server waits for step 10 to complete and then routes the emergency call toward the destination PSAP through the NENA i3 ESInet or legacy Selective Router indicated by the ESRK or ESRD received from the GMLC in step 10. The MSC Server includes the UE identification (e.g., MSISDN, non-dialable callback number, or ESRK) in call information forwarded toward the PSAP. If steps 9-10 are not performed, the MSC Server routes the emergency call toward a destination PSAP based on the serving cell or SAI. As an option in this case, steps 6-8 (but not steps 9-10) could be performed to obtain a UE location and route the call based on the UE location. The MSC Server may also assign an ESRD or ESRK based on the PSAP destination and include this in information sent toward the PSAP along with an MSISDN or non-dialable callback number. More details of emergency call setup are provided in J-STD-036-C-2 [Ref 3] and NENA-STA-010.2 [Ref 100].

Step 13. The remainder of emergency call establishment takes place.

Step 14. If steps 9-10 are not performed, the MSC Server performs steps similar to steps 6-8 and identical to steps 17-26 to obtain high accuracy location information (HALI) for the UE and then performs steps identical to steps 9-10 with one exception to transfer UE information to the GMLC including the UE identity (MSISDN, IMSI, non dialable callback number, and/or IMEI), the HALI, the serving cell ID or SAI. The MSC Server also includes any ESRD or ESRK assigned at step 12. The GMLC stores the received information and returns an ack. The one exception to steps 9-10 is that the GMLC does not assign and return an ESRK or ESRD to the MSC Server at step 10.

Step 15. The i3 PSAP or LPG or ALI sends a location request to the GMLC for an initial Dispatchable Location for the UE using information received at step 12 to route the request to the GMLC and to identify the UE.

Step 16. If steps 9-10 were not performed, the GMLC skips steps 16-27 and waits for step 14 to occur if step 14 did not yet occur. The GMLC then returns the HALI received at step 14 to the ALI at step 28. If steps 9-10 were performed and the GMLC received HALI at step 10, the GMLC skips steps 16-27 and returns the HALI received at step 10 to the ALI at step 28. Otherwise, if steps 9-10 were performed but the GMLC did not receive HALI at step 10, the GMLC forwards the location request received at step 15 to the MSC Server indicated at step 9 and indicates a location request for an emergency call and high accuracy location.

Step 17. The MSC Server forwards the location request to the serving RNC.

Step 18. If SAS centric location is supported, the serving RNC forwards the location request to an SAS in a PCAP Position Initiation Request. In the case of RNC centric location (not shown in Figure 7.9), steps 18, 19, 22, and 25 are not present and steps 23 and 24 may be performed by the RNC rather than SAS.

Step 19. The SAS sends a PCAP Position Activation Request to the RNC to request location information for the UE.

Step 20. The RNC may request location information from the UE using RRC and may then provide to the UE any assistance data provided by the SAS in step 19.

Step 21. The UE returns any requested location information to the RNC.

Step 22. The serving RNC returns any location information obtained in step 21 and/or other location information available to the serving RNC and/or obtained from the serving Node B or other nearby Node Bs. Steps 19-22 may be repeated to obtain additional location information. Additional details of SAS centric and RNC centric location are provided in 3GPP TS 25.305 [Ref 22].

Step 23. The location information obtained by the SAS at step 22 may include the identities of one or more Reference Points near the UE and UBP if supported by the UE. Based on an indication of a location request for an emergency call at step 18 and based on any request for high accuracy location, the SAS may send a query to the NEAD and may include in the Query the identity of a Reference Point provided by the RNC at step 22.

Step 24. The NEAD retrieves any civic location and geocoded location associated with the Reference Point provided at step 23 and returns this to the SAS. Steps 23-24 may be repeated for additional Reference Points.

Step 25. The SAS determines a geodetic location and/or a Dispatchable Location for the UE based on any location information received at steps 22 and 24 and returns the geodetic location and/or Dispatchable Location along with any UBP in the form of HALI to the serving RNC in a PCAP Position Initiation Response.

Step 26. The serving RNC returns the HALI to the MSC Server.

Step 27. The MSC Server returns the HALI to the GMLC.

Step 28. The GMLC returns the HALI obtained at step 27, step 14, or step 9 to the i3 PSAP or LPG or ALI. Steps 15-28 may be repeated by the i3 PSAP, or by the legacy PSAP via LPG, or by legacy PSAP via ALI at a later time to obtain updated location information. In that case, the GMLC will perform steps 16-27 to obtain updated HALI.

Step 29. The PSAP (or possibly the UE) releases the emergency call.

Step 30. The MSC Server notifies the GMLC that the emergency call has ended.

Step 31. The GMLC returns an ack. And may release any resources assigned to the emergency call.

7.6.4 External Location Services Heightened Accuracy Location with LTE and Control Plane

This clause provides a high level signaling flow showing heightened accuracy location support for an emergency call from a UE with LTE access and using control plane where the Reference Point based location is provided by External Location Services. This figure is extended from Figure 7.7. Additional configurations can be extrapolated from this flow.

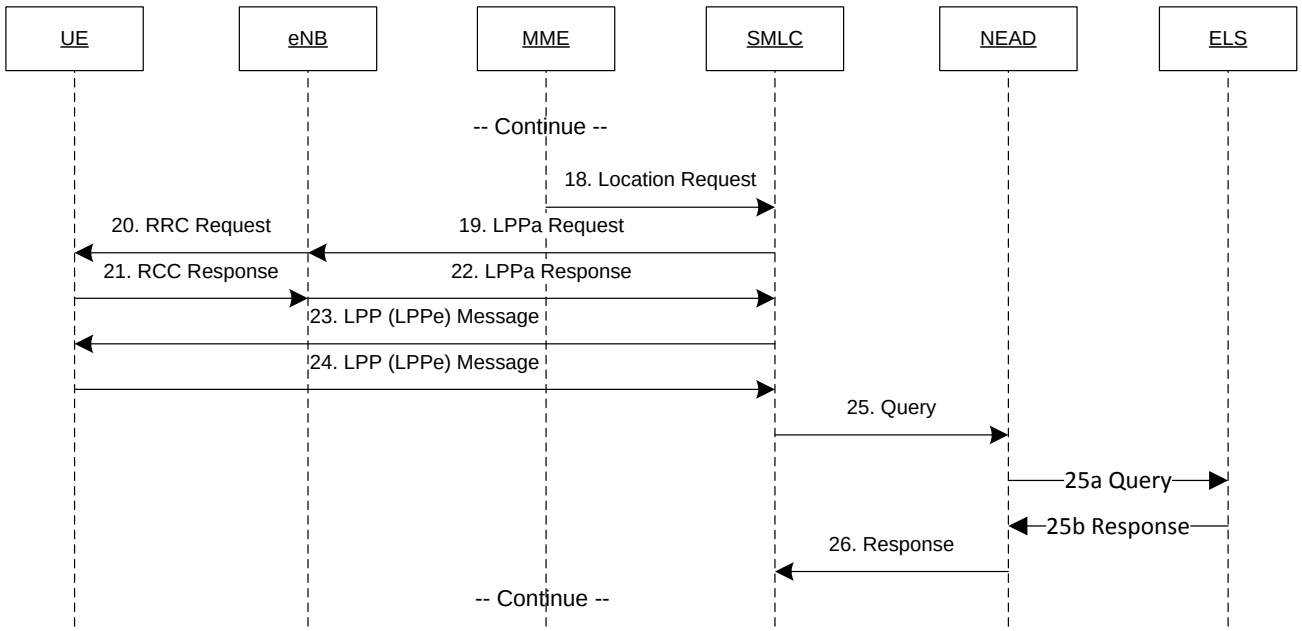


Figure 7.10 – External Location Services Heightened Accuracy Location with LTE and Control Plane

Step 18. The MME forwards the location request to an E-SMLC.

Step 19. The E-SMLC may request location information for the UE by sending an LPPa location request to the serving Enb via the MME.

Step 20. The serving Enb may request some location information from the UE using RRC.

Step 21. The UE returns any requested location information to the serving Enb.

Step 22. The serving Enb returns any location information obtained in step 21 and/or other location information available to the serving Enb. Steps 19-22 may be repeated to request and/or provide additional location information.

Step 23. The E-SMLC may request location information for the UE by sending an LPP/LPPe message to the UE via the MME and serving Enb. The LPP message includes an embedded LPPe message.

Step 24. The UE returns any requested location related information to the E-SMLC. This related information, in the case of Wi-Fi location, would include a list of identifiers (e.g., MAC addresses) of Wi-Fi Aps and BLE BT-PDAs visible to the UE at the time of the request. Also included in the response is the UE's own Wi-Fi MAC address. Step 23 may be repeated to request more location information, to provide assistance data to the UE and/or to request the positioning capabilities of the UE. Step 24 may be repeated to respond to any additional request in a repetition of step 23 (e.g., to provide additional location information or the UE positioning capabilities) and/or to request assistance data from the E-SMLC. The order of the LPP/LPPe messages may be different in different implementations – e.g., step 23 may be used first to request the UE's positioning capabilities, used again to provide assistance data to the UE, or used to request location information.

Step 25. If the location information obtained by the E-SMLC at step 22 and/or step 24 includes the identifiers for one or more Reference Points near the UE (and UBP if supported by the UE), then based on variety of factors, including the marking of an emergency call at step 18, or perhaps based also on a request for high accuracy location (assuming high accuracy location is requested by the LRF at step 16), the E-SMLC may send a query to the NEAD over the Nq interface that includes two separate parameters: a Reference Point identifier and the UE's WLAN MAC address (provided at step 24).

Step 25a. The NEAD attempts to match the identifier received with what is provisioned in its database. If it finds that a matching row's data is a URI, it determines that the Reference Point information must be obtained from the External Location Server. The NEAD then queries the External Location Server over the Na interface with the Identifier of the Reference Point and the UE's Wi-Fi MAC address it received from the Esmlc.

Step 25b. The External Location Server returns a civic address associated with the UE.

Step 26. The NEAD returns the civic location and geocoded location associated with the UE provided at step 25b and returns this to the E-SMLC. Steps 25-26 may be repeated for additional Reference Points.

8 Stage 3

This clause provides the stage 3 support for acquisition and conveyance of high accuracy location information (HALI) for an emergency call. Parts of this support are defined in specifications and standards from other SDOs. In the case of any conflict between this clause and any normative reference to another standard or specification, the latter shall have precedence unless stated explicitly to the contrary here.

8.1 Overview

This clause provides an overview of the acquisition and conveyance of HALI. Detailed impacts to individual entities, interfaces, and protocols are provided in later clauses.

8.2 Procedures for the NEAM, NEAD & Location Server (Informative)

This clause describes procedures within and among the NEAM, NEAD, and the Location Server. It discusses how Dispatchable Location is provisioned into the NEAM, validated and geocoded, and then pushed to the NEAD. It also discusses procedures used by an ELS to provision URI data into the NEAM for subsequent delivery to the NEAD. Interactions between the NEAD and the Location Server and between the NEAD and the ELS are also discussed.

8.2.1 NEAM Procedures

The NEAM supports two interfaces to External Data Sources that provision source location information for their Access Points or Bluetooth beacons. The first interface is a webpage interface where users login with their user IDs and passwords. Once users have been authenticated, they are assigned privileges to perform actions. Specifically, they are associated with one or more OWNERs (as described in Clause 7.3.4). These privileges allow users to perform actions on behalf of the OWNER; such as adding or modifying Access Point or Bluetooth beacon information. Ideally an electronic form will be provided to users that will facilitate the action.

The second interface to External Data Sources is an XML-based web M2M interface. This interface has a defined XML schema that supports standardized interactions between the NEAM and External Data Sources and between the NEAM and an ELS.

Both of these interfaces allow the External Data Sources to query for, add, modify, or delete location information associated with an Access Point or Bluetooth beacon, provided they are authorized to do so. The M2M interface also allows an authorized ELS to add, modify, or delete URI and CMA information associated with an Access Point or Bluetooth beacon. The M2M interface allows the user to specify one or more Access Points or Bluetooth beacons in the request.

When a query request is submitted by an External Data Source, the NEAM will respond with the location information associated with the Access Point or Bluetooth beacon, if the information is found within the NEAM/NEAD complex. When a query request is submitted by an ELS, the NEAM will respond with URI and CMA information associated with the Access Point or Bluetooth beacon, if the information is found within the NEAM/NEAD complex.

When an External Data Source makes a request to add location information for an Access Point or Bluetooth beacon, the NEAM invokes a process to honor the request. First it validates the location information to assure that the location is a valid location. If the location cannot be validated, an error response is returned to the External Data Source. Next the NEAM invokes a geocoding process. The geocoded location is used by the Location Server in the selection process of the location passed toward the PSAP.

The validation process is expected to handle source addresses in a variety of formats. The result of the internal NEAM validation process is to produce an address that can be delivered to a PSAP. This validated address may be different from the source address. The validation process matches incoming addresses with data that is supplied/approved by Public Safety entities for the geographic area within which the address to be validated belongs. Both source and validated address information are stored in the NEAM, since the originally-submitted location may need to be retained for potential user interaction. Only the validated address will be provisioned to the NEAD.

Once the location is successfully validated and geocoded, it is pushed to the NEAD. Once the NEAD indicates that it has successfully loaded the location information, the NEAM responds back to the External Data Source with a success indication.

When an ELS makes a request to add URI and CMA information for an Access Point or Bluetooth beacon, the NEAM verifies that the data is formatted correctly and then provisions the information into the NEAD. Once the NEAD indicates it has successfully loaded the information, the NEAM responds back to the ELS indicating that the process was successful.

It should be noted that if information associated with multiple Access Points or Bluetooth beacons is contained in the request, the NEAM will process all records prior to responding back to the External Data Source or ELS. Therefore, this response may contain a mix, indicating the success or failure to process information associated with specific Access Points or Bluetooth beacons.

When an External Data Source or ELS makes a request to modify location information for an Access Point or Bluetooth beacon, the NEAM invokes a similar process as for adding information. The primary difference is that if the information is not already in the NEAD/NEAM complex, the NEAM will return an error.

When an External Data Source or ELS makes a request to delete location information for an Access Point or Bluetooth beacon, the NEAM first verifies that the information resides in the NEAM/NEAD complex and then deletes the information.

8.2.2 NEAD Procedures

Because of the close relationship between the NEAM and the NEAD, the interface and protocol between them is not defined. When the NEAD receives the Access Point or Bluetooth beacon location from the NEAM, it loads it into its internal database. The location information will contain the relationship between the MAC or Bluetooth Public Device Address (BT-PDA) and a civic address and geocoded location. Likewise, when the NEAD receives a URI associated with an Access Point MAC address or BT-PDA, it loads it into its internal database. Since the NEAD assumes that the NEAM is the master, NEAD makes minimal checks prior to accepting the data. The NEAM must assure that the MAC address is unique within the system.

The NEAD is a common functional element among the participating CMRS providers. That is, it does not reside within any CMRS network, but each CMRS provider has access to it. Access to the NEAD is via secure connections. The CMRS network queries the NEAD with the MAC or BT-PDA. The NEAD returns the Dispatchable Location for that Access Point or Bluetooth beacon and the geocoded location provided by the NEAM or ELS. It is highly likely that the NEAD will be queried with a MAC or BT-PDA that has not been provisioned in the NEAM/NEAD complex. This should not be considered an error condition although the NEAD will return an error code if the information is not present.

8.2.3 Location Server Procedures

The Location Server (e.g., an E-SMLC) is responsible for invoking the location determination methods and analyzing the results from the various positioning methods to make the final determination on the location to be passed toward the PSAP. For example, in addition to the existing procedures for determining geodetic location, the Location Server may select from among one or more candidate Dispatchable Locations provided from a NEAD and pass the Dispatchable Location on toward the PSAP. This clause does not dictate how the Location Server does this but provides some guidelines. See ATIS-0700039 [Ref 13] for further details related to guidelines for selecting the location that is to be passed toward the PSAP.

It is anticipated that there will be multiple Access Points or Bluetooth beacons observable to the UE during the call. When the Location Server interacts with the UE, it obtains a list of MAC or BT-PDA along with associated measurement information. It may not be appropriate for the Location Server to send all MAC or BT-PDA to the NEAD. The Location Server may use measurement information or other means to limit the list of MAC or BT-PDA to send to the NEAD. (See ATIS-0700039 [Ref 13] for further information.)

When the Location Server queries the NEAD with a MAC or BT-PDA, it will get back a candidate Dispatchable Location for that Reference Point along with a geocoded location and a method parameter indicating whether the location information is associated with a Wi-Fi Access Point or Bluetooth beacon, and whether the information was provisioned in the NEAD or provided by an ELS. Since there may be multiple Reference Points observable to the UE, and the Location Server queries the NEAD with each or a subset of them, the Location Server will have to

provide a method to select the most appropriate Dispatchable Location candidate provided by the NEAD. For example, the Location Server may use the geocoded location to determine that a Dispatchable Location is reasonable (e.g., by comparing to a computed geodetic location).

The LS will assign a location method token based upon a quality level rating (as an example, see Annex D). New location method tokens, NEAD-CVC, NEAD-DL1, and NEAD-DL2 associated with location information provisioned in the NEAD, and ELS-CVC, ELS-DL1, and ELS-DL2 are shown below. One of these three location method tokens will be populated in the PIDF-LO that is to be forwarded to the downstream network elements such as the GMLC and LRF.

For Dispatchable Location candidates provided by an ELS the LS will not receive any explicit indication of the uncertainty of the information. For the purpose of selecting the most appropriate candidate and quality level rating, the LS may as an example use a fixed assumption of the uncertainty. This assumption can be based on e.g., Service Level Agreement with External Location Server providers.

Table 8.1 – LS Location Method Tokens

Token	Description	Reference	Registration Date
NEAD-CVC	Civic Location	ATIS/WTSC-ELOC*	TBD
NEAD-DL1	Dispatchable Civic Location – medium-level	ATIS/WTSC-ELOC*	TBD
NEAD-DL2	Dispatchable Civic Location – highest level	ATIS/WTSC-ELOC*	TBD
ELS-CVC	Civic Location	ATIS/WTSC-ELOC*	TBD
ELS-DL1	Dispatchable Civic Location – medium-level	ATIS/WTSC-ELOC*	TBD
ELS-DL2	Dispatchable Civic Location – highest level	ATIS/WTSC-ELOC*	TBD

An XML example:

<method>NEAD-DL2</method>

* NOTE: Reference IANA registry URL for location method token values:

https://www.iana.org/assignments/method-tokens/method-tokens.xhtml#method-tokens-1

This registry value is added on a first-come, first-served basis.

8.3 Protocol Mappings for Dispatchable Location

This clause identifies the protocol capabilities and mapping to support Dispatchable Location. Table 8.8, Table 8.9, Table 8.10, Table 8.11, and Table 8.12 identify potential protocols that may be used to acquire and transport Dispatchable Location toward the PSAP. This clause identifies the capabilities of the specific protocols, identifies any necessary element mapping, and denotes any potential gaps.

8.3.1 Np Interface Using the NENA CLDXF Specification

Table 8.3 and Table 8.4 denote the XML elements that are used to provision civic location from External Data Sources to the NEAM via the Np interface.

The following text from section 1.2 of CLDXF [Ref 35] defines XML elements not used by CLDXF.

“In addition, the NENA NG9-1-1 CLDXF standard restricts IETF PIDF-LO civic address standard by exclusion of the following PIDF-LO elements:

1. A6 – Street (group of streets below the neighborhood level): Not used in the United States.
2. ADDCODE – Address Code: Not used in NG9-1-1 CLDXF.
3. POBOX – Post Office Box: Not used in NG9-1-1 CLDXF.
4. RDSEC – Road section: Not found in US addresses.
5. RDBR – Road Branch: Not found in US addresses.
6. RDSUBBR – Road sub-branch: Not found in US addresses."

The following table contains a list of all XML elements from CLDXF [Ref 35], RFC 4119 [Ref 30], RFC 5139 [Ref 31], and RFC 6848 [Ref 38] that are not used in the Np protocol.

Table 8.2 – XML Elements not used in Np

Mnemonic	Name	RFC	Comment
A6	Street (group of streets below the neighborhood level)	4119	XML element RD is used to denote street.
ADDCODE	Address Code	5139	Not used in NG9-1-1 CLDXF.
NAM	Name	4119	
PN	Post Number	6848	
POBOX	Post Office Box	5139	Not used in NG9-1-1 CLDXF.
RDSEC	Road section	5139	Not found in US addresses.
RDBR	Road Branch	5139	Not found in US addresses.
RDSUBBR	Road sub-branch	5139	Not found in US addresses.

8.3.2 Nq Interface using HELD

The Location Server will query the NEAD via the Nq interface. The XML elements defined in Table 8.3 (except OWNER and MAC or BT-PDA), in addition to the geocoded location, will be returned in the response. Only civic location elements provisioned by the External Data Source via the Np interface or provided by the ELS will be returned in the response.

8.3.3 OMA MLP

MLP version 3.3 and 3.4 provided a finite set of civic location elements (civicloc_element) based upon RFCs 4119 [Ref 30] and 5139 [Ref 31]. They are COUNTRY, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, LMK, LOC, FLR, NAM, PC, BLD, UNIT, ROOM, PLC, PCN, POBOX, ADDCODE, SEAT, RD, RDSEC, RDBR, RDSUBBR, PRM, and POD.

MLP version 3.5 extended the definition of civic location (civicloc_element) by including all of the elements defined in RFCs 4119 [Ref 30], 5139 [Ref 31], and 6848 [Ref 38]. It also added VENUE_NAME, VENUE_ID, and VENUE_SPECIFIC_NAME, which are not to be used in the context of this standard.

Based upon a comparison with Table 8.3, the elements for Dispatchable Location can be mapped into versions 3.3 and 3.4 of MLP with the following exceptions.

1. Mile Post (MP)[49] is not supported in these versions of MLP.

[49] From RFC 6848 [Ref 38].

2. Landmark Name Part (LMKP)[50] is not supported in these versions of MLP.
3. Address Number Prefix (HNP)[49] is not supported in these versions of MLP.
4. Street Name Pre Type Separator (STPS)[51] is not supported in these versions of MLP.
5. Street Name Pre Type (STP)[49] is not supported in these versions of MLP.

Based upon a comparison with Table 8.3, all the elements for Dispatchable Location can be mapped into version 3.5 of MLP.

8.3.4 LCS-AP Location Response Message

TS 29.171 Release 13 [Ref 9] supports civic location via the Civic Address element in the LCS-AP location response message based upon RFCs 4119 [Ref 30], 5139 [Ref 31], and 6848 [Ref 38]. The elements for Dispatchable Location defined in Table 8.3 may be mapped to this element.

8.3.5 PSL Response message & SLR

TS 29.172 Release 13 [Ref 10] supports civic location via the Civic-Address element in the Provide Subscriber Location (PSL) response and the Subscriber Location Report (SLR) based upon RFCs 4119 [Ref 30], 5139 [Ref 31], and 6848 [Ref 38]. The elements for Dispatchable Location defined in Table 8.3 may be mapped to this element.

8.3.6 E2 esposreq

Depending upon the network implementation, either the LRF or the GMLC will have to map the civic address format from the MLP response, the SLR, or PSL response to the E2 Emergency Position Request response message (esposreq) toward the regional ALI or Legacy Network Gateway. The esposreq is defined in J-STD-036-C-2 [Ref 3]. As currently defined, the elements in the Location Description parameter of the esposreq response message are somewhat limited and the regional ALI must map those elements into the legacy PSAP format to be displayed at the PSAP. The Legacy Network Gateway must be able to map those elements into the PIDF-LO and an associated Additional Data structure. The tables below identify mapping of elements in Table 7.4and Table 7.5into the elements defined by NENA in the Location Description field.

If the mapping of XML elements to the E2 elements as described below exceeds the E2 element length, the LRF or GMLC will truncate the string from right to left (left justified). If elements received in the E2 response are longer than can be utilized in the ALI server, the ALI will truncate the string from right to left (left justified).

How the LRF or GMLC maps the Dispatchable Location received in the MLP response, SLR, or PSL response to a PositionSource code is described in Clause 8.3.6.1.

Table 8.3 – Mapping of Table 7.6 to E2 Location Description

Table 7.6 Attribute (XML Element)	E2 Location Description Field (Max Field Length)	E2 Example
Country (Country)	Not mapped	
State (A1)	Not mapped	
County (A2)	Not mapped	

[50] NENA CLDXF Civic Address Extensions [Ref 35].

[51] From RFC 5139 [Ref 31].

Table 7.6 Attribute (XML Element)	E2 Location Description Field (Max Field Length)	E2 Example
Incorporated Municipality (A3)	MCN (32)[52]	<MCN>Lisle</MCN>
Unincorporated Community (A4)	MCN (32)[48]	<MCN>Lisle</MCN>
Postal Community Name (PCN)	MCN (32)[48]	<MCN>Lisle</MCN>
Postal Code (PC)	Not mapped	
Neighborhood Community (A5)	Not mapped	
Street Name (RD)	STN (60)	<STN>Warrenville</STN>
Street Name Pre Directional (PRD)	PRD (2) Street pre-directionals are mapped as shown in Pre/Post Directional Mapping	<PRD>N</PRD>
Street Name Pre Modifier (PRM)	STN (60)	<STN>**Old**[53] Avenue of the Americas</STN >
Street Name Pre Type (STP)	STN (60)	<STN>Old **Avenue** of the Americas</STN>
Street Name Pre Type Separator (STPS)	STN (60)	<STN>Old Avenue **of the** Americas</STN>
Street Name Post Directional (POD)	POD (2) Street post-directionals are mapped as shown in Pre/Post Directional Mapping	<POD>E </POD>
Street Name Post Type (STS)	STN (60)	<STN>Warrenville **Avenue** Extension</STN>
Street Name Post Modifier (POM)	STN (60)	<STN> Warrenville Avenue **Extension** </STN>
Address Number Prefix (HNP)	HNO (10)	<HNO>**A** 123</HNO>
Address Number (HNO)	HNO (10)	<HNO>A **123**</HNO>
Address Number Suffix (HNS)	HNS (4)	<HNS>1/2</HNS>
Milepost (MP)	LOC (60)	<LOC>MP 15</LOC>
Landmark Name Part (LMKP)	LOC (60)[54]	<LOC> LMKP **University of South Florida** LMKP Sun Dome</LOC>

[52] Assumed mutually exclusive. Incorporated Municipality takes precedence over Unincorporated Community, which in turn takes precedence over Postal Community.

[53] **Bold** font represents the segment of the format for that specific row when multiple rows are mapped into a single E2 Location Description element.

[54] If LMK exists, LMKP is not used.

Table 7.6 Attribute (XML Element)	E2 Location Description Field (Max Field Length)	E2 Example
Complete Landmark Name (LMK)	LOC (60)[46]	<LOC> LMK **University of South Florida Sun Dome<**/LOC>

The following table defines the mapping for Street pre-directionals and post-directionals.

Table 8.4 – Pre/Post Directional Mapping

CLDXF Name	E2 Mapping
North	N
Northeast	NE
East	E
Southeast	SE
South	S
Southwest	SW
West	W
Northwest	NW

Table 8.5 – Mapping of Table 7.7 to E2 Location Description

Table 7.7 Attribute	Location Description Field	Example
Building (BLD)	LOC (60)	<LOC>**BLD A** FLR 5 UNIT 12</LOC>
Additional Location Information (LOC)	LOC (60)	<LOC> LOC West Wing</LOC>
Floor (FLR)	LOC (60)	<LOC>BLD A **FLR 5** UNIT 12</LOC>
Unit (UNIT)	LOC (60)	<LOC>FLR 5 **UNIT 12**</LOC>
Room (ROOM)	LOC (60)	<LOC>FLR 5 **ROOM 102** SEAT 23</LOC>
Seat (SEAT)	LOC (60)	<LOC>FLR 5 ROOM 102 **SEAT 23**</LOC>
Place Type (PLC)	LOC (60)	<LOC> PLC MTS</LOC>

The priority of mapping XML elements to the LOC element in the E2 Location Description parameter is as follows:

BLD**|**FLR**|**UNIT**|**ROOM**|**SEAT**|**MP**|**LOC**|**LMK (or LMKP) **|**PLC|UBP

where UBP refers to the UBP field defined in subclause 8.4.

Table 8.6 – Mapping of other LS data to E2 Location Description

LS Data	Location Description Field	Example
Uncompensated Barometric Pressure (UBP)	LOC (60)	<LOC>FLR 5 **UBP 101324**</LOC>

A string longer than 60 characters will be truncated right to left (left justified). A space is inserted between each element. All strings (except UBP) will be preceded by a descriptor that contains the name of the CLDXF element (e.g., BLD).

8.3.6.1 E2 esposreq Position Source Treatment

If the GMLC receives a civic address, and potentially subaddress elements, it will map the appropriate location method token included in the PIDF-LO to a Position Source. Three new Position Source values have been defined in J-STD-036-C-2 [Ref 3] and are shown in the table below.

Table 8.7 – Position Source Values

55	Class of Service – WCVC representing an E9-1-1 civic location.
56	Class of Service – WDL1 representing an E9-1-1 medium -level quality dispatchable civic location.
57	Class of Service – WDL2 representing an E9-1-1 highest level quality dispatchable civic location.

The GMLC will map the location method token of NEAD-CVC and ELS-CVC to Position Source 55, location method token NEAD-DL1 and ELS-DL1 to Position Source 56, and location method token of NEAD-DL2 and ELS-DL2 to Position Source 57.

8.4 Protocol Mappings for Uncompensated Barometric Pressure (UBP)

This clause identifies the protocol mappings to support end-to-end transfer of UBP. The mappings are described separately for each type of access (LTE and UMTS) and for each location solution (control plane and user plane) for transfer of UBP from a UE as far as a gateway location server (GMLC or LRF) responsible for passing location information toward the PSAP. For transfer from a gateway location server (GMLC or LRF) toward the PSAP, a single description is provided as this is common for both LTE and UMTS access and for both control plane and user plane location solutions.

8.4.1 UBP Transfer from a UE to LRF for LTE Access & Control Plane Location

UBP transfer from a UE as far as an LRF for LTE access with control plane location uses the sequence of interfaces shown in Table 8.8, which also shows the source and destination elements for each interface (or interfaces), the applicable protocols, and the encoding of UBP.

Table 8.8 – Transfer of UBP from a UE to LRF with LTE Access and Control Plane Location

Interface(s)	Sender	Receiver	Protocol(s)	UBP encoding
Uu, S1, SLs	UE	E-SMLC	LPP or LPPe	Integer between 30,000 and 115,000 in units of Pascals
SLs	E-SMLC	MME	LCS-AP	Integer between 30,000 and 115,000 in units of Pascals
SLg	MME	GMLC	ELP	Integer between 30,000 and 115,000 in units of Pascals

L0	GMLC	LRF	MLP	Character encoded decimal integer in units of Pascals

NOTE: LPP [Ref 5], LCS-AP [Ref 9], ELP [Ref 10] are for Release 13, MLP [Ref 11] is MLP 3.5, and LPPe [Ref 6] is LPPe 1.0.

8.4.2 UBP Transfer from a UE to LRF for LTE Access & User Plane Location

UBP transfer from a UE as far as an LRF for LTE access with user plane location uses the sequence of interfaces shown in Table 8.9, which also shows the source and destination elements for each interface (or interfaces), the applicable protocols, and the encoding of UBP.

Table 8.9 – Transfer of UBP from a UE to LRF with LTE Access and User Plane Location

Interface(s)	Sender	Receiver	Protocol(s)	UBP encoding
Lup	UE	E-SLP	LPP or LPPe	Integer between 30,000 and 115,000 in units of Pascals
L0	E-SLP	LRF	MLP	Character encoded decimal integer in units of Pascals

NOTE: LPP [Ref 5] is for Release 13, MLP [Ref 11] is MLP 3.5, and LPPe [Ref 6] is LPPe 1.0.

8.4.3 UBP Transfer from a UE to GMLC for UMTS CS Access & Control Plane Location

UBP transfer from a UE as far as a GMLC for UMTS CS access with control plane location uses the sequence of interfaces shown in Table 8.10, which also shows the source and destination elements for each interface (or interfaces), the applicable protocols, and the encoding of UBP.

Table 8.10 – Transfer of UBP from a UE to GMLC with UMTS CS Access and Control Plane Location

Interface(s)	Sender	Receiver	Protocol(s)	UBP encoding
Uu, Iub	UE	RNC	RRC	Integer between 30,000 and 115,000 in units of Pascals
Iupc	RNC	SAS	PCAP	Integer between 30,000 and 115,000 in units of Pascals
Iupc	SAS	RNC	PCAP	Integer between 30,000 and 115,000 in units of Pascals
Iu-cs	RNC	MSC	RANAP	Integer between 30,000 and 115,000 in units of Pascals
Lg	MSC	GMLC	MAP	Integer between 30,000 and 115,000 in units of Pascals

NOTE: RRC [Ref 25], PCAP [Ref 40], RANAP [Ref 39] and MAP [Ref 41] are for Release 13.

8.4.4 UBP Transfer from a GMLC or LRF to the ALI over the E2 Interface

UBP is transferred in the E2 Emergency Position Request response message (esposreq) from a GMLC (for UMTS CS access) toward a regional ALI or Legacy Network Gateway, or from an LRF (for LTE access or UMTS PS access) toward a regional ALI. The esposreq is defined in J-STD-036-C-2 [Ref 3]. UBP is transferred as part of the 60-character location (LOC) field defined in section 9.3.16 of NENA 05-001. The syntax and encoding of the LOC field when carrying UBP and no other information is as follows:

LOC encoding = <LOC>UBP nnnnnn</LOC>

where nnnnnn is the six-digit UBP value in units of Pascals (1 Pa = 0.01 mbar) which has a vertical granularity of approximately 0.083 meters. As an example, if the received UBP is 101324 Pa, nnnnnn is encoded as 101324. If the received UBP is 99870 Pa, nnnnnn is encoded as 099870.

When the LOC field carries other information such as fields for a Dispatchable Location as described in subclause 8.3.6, the UBP field is separated from any adjacent field using a space character and shall be included as the rightmost field in the LOC field prior to any truncation. The UBP field will always be removed if the LOC field is truncated (from right to left) as described in subclause 8.3.6.

8.4.5 UBP Transfer from a GMLC or LRF to the ALI over the MLP Interface

UBP is transferred in the Mobile Location Protocol (Emergency Location Immediate Answer) from a GMLC (for UMTS CS access) toward a regional ALI or Legacy Network Gateway, or from an LRF (for LTE access or UMTS PS access) to a regional ALI. The ELIA message is defined by the Open Mobile Alliance, MLP specification [Ref 11]. The MLP specification transfers UBP information as character encoded decimal integer in units of Pascals. This enhancement serves the needs of both the L0 interface and the MLP-based interface to the ALI where deployed.

8.5 HALI Acquisition & Conveyance

8.5.1 LTE Access with Control Plane Location

Figure 8.1 shows the architecture from Figure 7.4 applicable to use of control plane location for a UE with LTE access. Figure 8.1 highlights the set of interfaces and involved entities that are needed to acquire and/or convey a Dispatchable Location (DL), Geodetic Location (GL), Uncompensated Barometric Pressure (UBP), source position method(s) (SPM) used for a GL, data for Reference Points (RPs), and other location measurements (LM). Note that Figure 8.1 shows the maximum set of information elements for each interface, not all of which may be included for any particular emergency call.

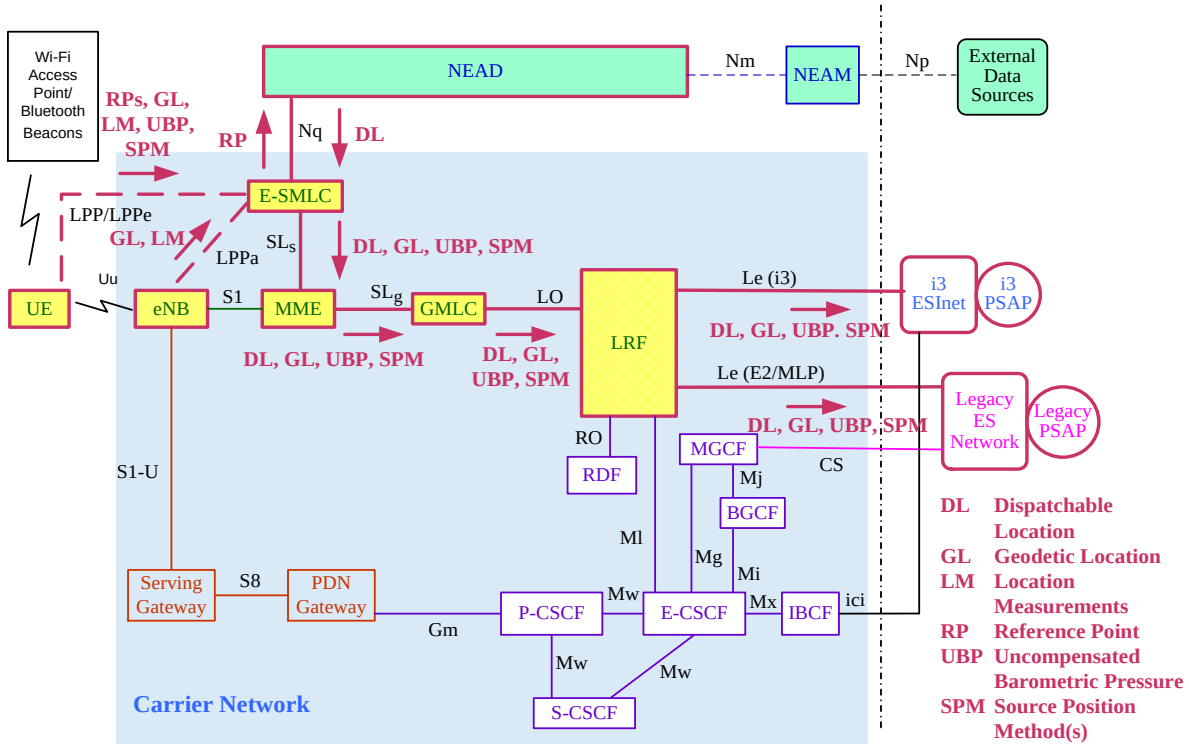


Figure 8.1 – Overview of HALI Acquisition and Conveyance with LTE Access and Control Plane Location

Table 8.11 summarizes the interface and protocol support shown in Figure 8.1 in tabular form. Support for conveyance of any parameter by a particular protocol is indicated by a “Y” entry, while lack of support is indicated by an “N” entry.

Table 8.11 – Interface and Protocol Support of HALI for LTE Access and Control Plane Location

Interface	Sender	Recipient	Protocol(s)	RP Data	GL	DL	LM	UBP	SPM
Uu	UE	E-SMLC	LPP	Y	Y	N	Y	Y	Y
			LPPe	Y	Y	N	Y	Y	Y
S1/SLs	eNB	E-SMLC	LPPa	N	Y	N	Y	N	N
Nq	E-SMLC	NEAD	HTTP	Y	N	N	N	N	N
	NEAD	E-SMLC	HELD (note 1)	N	N	Y	N	N	N
SLs	E-SMLC	MME	LCS-AP	N	Y	Y	N	Y	Y
SLg	MME	GMLC	ELP	N	Y	Y	N	Y	Y
L0	GMLC	LRF	MLP	N	Y	Y	N	Y	Y
			HELD	N	Y	Y	N	N	N
			E2 (note 2)	N	Y	Y	N	Y	Y
Le (i3)	LRF	i3 ESInet	HELD	N	Y	Y	N	N	N
			SIP	N	Y	Y	N	N	N
Le (E2/MLP)	LRF	Legacy ES network	MLP	N	Y	Y	N	Y	Y
			E2 (note 2)	N	Y	Y	N	Y	Y

NOTE 1: The NEAD returns a geocoded location but not a geodetic location.

NOTE 2: E2 in J-STD-036-C-2 [Ref 3] currently supports a subset of DL. E2 has been extended in this standard to support UBP and certain additional DL elements.

8.5.2 LTE Access with User Plane Location

Figure 8.2 shows the architecture from Figure 7.5 applicable to use of user plane location for a UE with LTE access. Figure 8.2 highlights the set of interfaces and involved entities that are needed to acquire and/or convey a Dispatchable Location (DL), Geodetic Location (GL), Uncompensated Barometric Pressure (UBP), source position method(s) (SPM) used for a GL, data for Reference Points (RPs), and other location measurements (LM). Note that Figure 8.2 shows the maximum set of information elements for each interface, not all of which may be included for any particular emergency call.

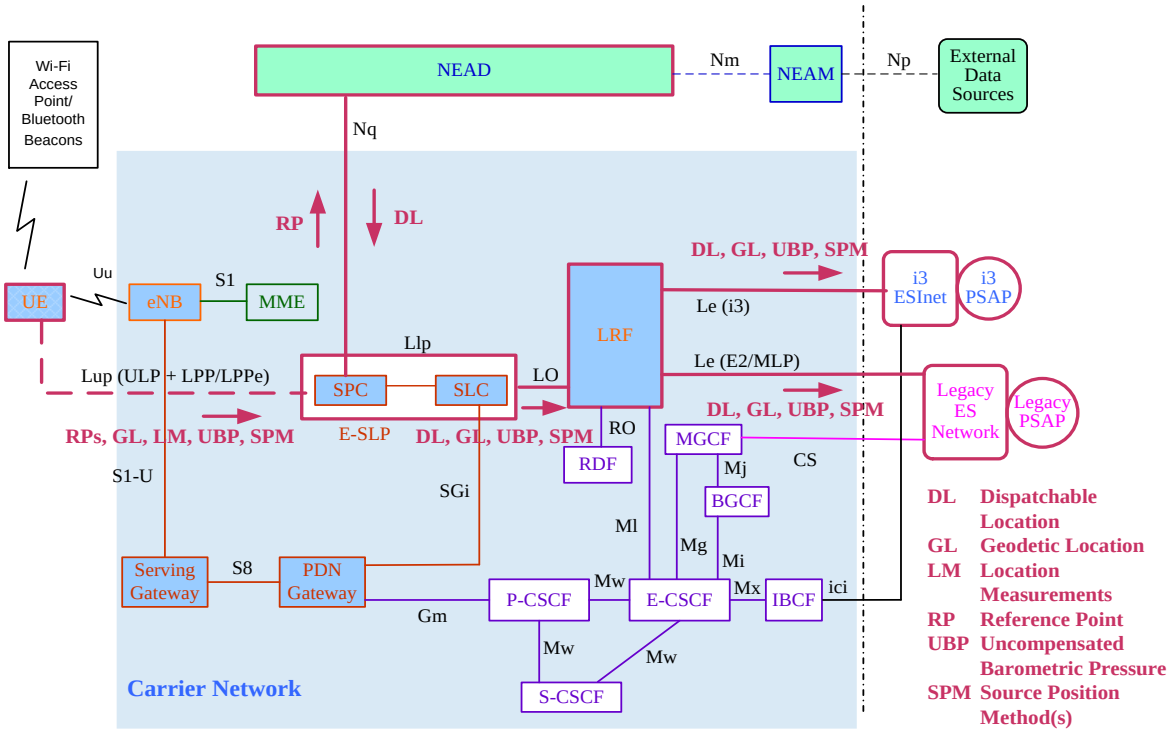


Figure 8.2 – Overview of HALI Acquisition and Conveyance with LTE Access and User Plane Location

Table 8.12 summarizes the interface and protocol support shown in Figure 8.2 in tabular form. Support for conveyance of any parameter by a particular protocol is indicated by a "Y" entry, while lack of support is indicated by an "N" entry.

Table 8.12 – Interface and Protocol Support of HALI for LTE Access and User Plane Location

Interface	Sender	Recipient	Protocol(s)	RP Data	GL	DL	LM	UBP	SPM
Lup	UE	E-SLP	ULP + LPP	Y	Y	N	Y	Y	Y
			ULP + LPP/LPPe	Y	Y	N	Y	Y	Y
Nq	E-SLP	NEAD	HTTP	Y	N	N	N	N	N
	NEAD	E-SLP	HELD (note 1)	N	N	Y	N	N	N
L0	E-SLP	LRF	MLP	N	Y	Y	N	Y	Y
			HELD	N	Y	Y	N	N	N
			E2 (note 2)	N	Y	Y	N	Y	Y
Le (i3)	LRF	i3 ESInet	HELD	N	Y	Y	N	N	N
			SIP	N	Y	Y	N	N	N
Le (E2/MLP)	LRF	Legacy ES network	MLP	N	Y	Y	N	Y	Y
			E2 (note 2)	N	Y	Y	N	Y	Y

NOTE 1: The NEAD returns a geocoded location but not a geodetic location.

NOTE 2: E2 in J-STD-036-C-2 [Ref 3] currently supports a subset of DL. E2 has been extended in this standard to support UBP and certain additional DL elements.

8.5.3 UMTS CS Access with Control Plane Location

Figure 8.3 shows the architecture from Figure 7.7 applicable to use of control plane location for a UE with UMTS CS access. Figure 8.3 highlights the set of interfaces and involved entities that are needed to acquire and/or convey a Dispatchable Location (DL), Geodetic Location (GL), Uncompensated Barometric Pressure (UBP), source position method(s) (SPM) used for a GL, data for Reference Points (RPs), and other location measurements (LM). Note that Figure 8.3 shows the maximum set of information elements for each interface, not all of which may be included for any particular emergency call.

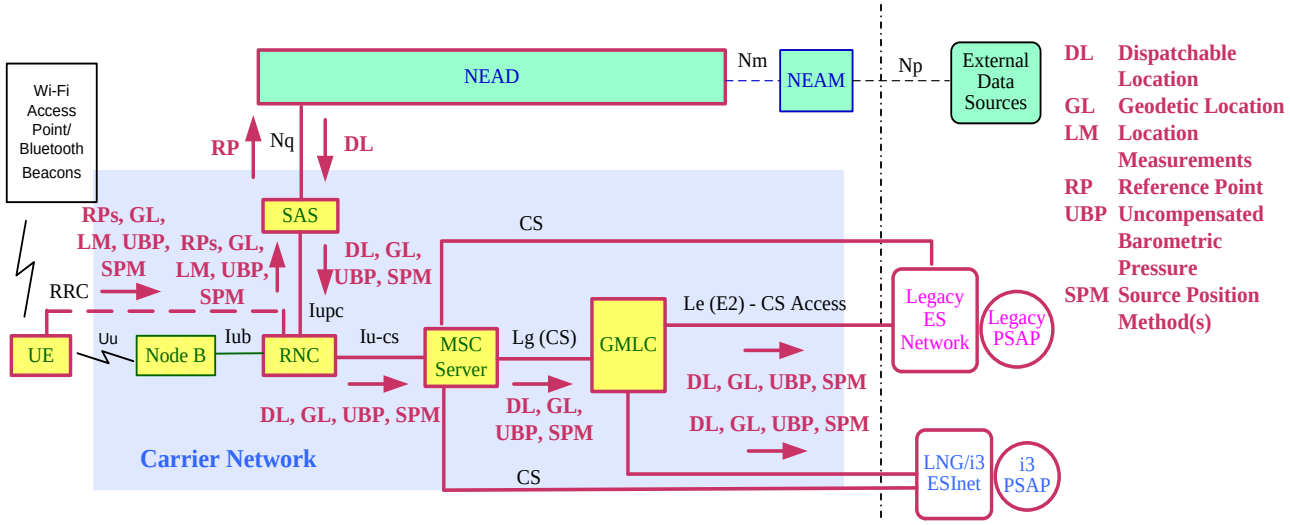


Figure 8.3 – Overview of HALI Acquisition and Conveyance with UMTS CS Access and Control Plane Location

Table 8.13 summarizes the interface and protocol support shown in Figure 8.3 in tabular form. Support for conveyance of any parameter by a particular protocol is indicated by a “Y” entry, while lack of support is indicated by an “N” entry.

Table 8.13 – Interface and Protocol Support of HALI for UMTS CS Access and Control Plane Location

Interface	Sender	Recipient	Protocol(s)	RP Data	GL	DL	LM	UBP	SPM
Uu	UE	RNC	RRC	Y	Y	N	Y	Y	Y
Iupc	RNC	SAS	PCAP	Y	Y	N	Y	Y	Y
	SAS	RNC		N	Y	Y	N	Y	Y
Nq	SAS	NEAD	HTTP	Y	N	N	N	N	N
	NEAD	SAS	HELD (note 1)	N	N	Y	N	N	N
Iu-cs	RNC	MSC Server	RANAP	N	Y	Y	N	Y	Y
Lg	MSC Server	GMLC	MAP	N	Y	Y	N	Y	Y
Le (E2/MLP)	GMLC	Legacy ES Network or LNG	MLP	N	Y	Y	N	Y	Y
			E2 (note 2)	N	Y	Y	N	Y	Y

NOTE 1: The NEAD returns a geocoded location but not a geodetic location.

NOTE 2: E2 in J-STD-036-C-2 [Ref 3] currently supports a subset of DL. E2 has been extended in this standard to support UBP and certain additional DL elements.

9 Security

9.1 Security principles

The scope of this clause is to outline the basic security principles which will guide the following detailed security related clauses. The architecture described in clause 7.1 has been developed with the assumption that the External Location Service; the NEAD and NEAM; the External Data Sources, as well as the Serving Core Network are all components of separate networks, each managed by separate administrative authorities. In each of these networks (or sub-networks) a security domain is established. The security domains generally coincide with the network or sub-network border. The security domain is protected at the border by security gateways (e.g. firewalls, SBCs) which are responsible for enforcing the administrative authorities' security policies.

In this specification, these security principles are applicable to those interfaces defined in clause 7.1: Np', Na, Np, and Nq.

9.2 Security assumptions

The following assumptions apply to the security of the elements providing improved location accuracy:

1. It is assumed that the administrative authority will integrate the security elements defined in this specification into authoritiy-wide security policies and practices.
2. It is assumed that the administrative authority will utilize other security standards, guidelines and best practices for security topics not covered in this specification.
3. It is assumed that this security domain approach can be extended to provide security in depth, but is not described in this specification.
4. It is assumed for network components based on 3GPP specifications, the corresponding 3GPP security specifications are also implemented and deployed.

9.3 Security requirements

The following sub-clauses describe the specific network security domain requirements for the reference points defined in this specification.

9.3.1 Np, Np', Na and Nq interfaces

The following high-level security requirements apply to each interface

1. When the interface crosses security domains (inter-network), security gateways shall be used at least at the edge of the security domain.
2. When the interface does not cross security domains (intra-network) security gateways may be used between network elements within the security domain.
3. Confidentiality protection shall be provided between the security gateways when the interface crosses security domains.
4. Confidentiality protection may be provided between the interface endpoint and security gateway within a single security domain.
5. Integrity protection shall be provided between the security gateways when the interface crosses security domains.
6. Integrity protection may be provided between the interface endpoint and security gateway within a single security domain.
7. Mutual authentication and validation shall be provided between the interface endpoints.
8. When security gateways are deployed in the interface path, mutual authentication shall be provided between the security gateways.

9.3.1.1 TLS requirements

The following requirements apply to the use of TLS on Nq and Na reference points.

1. TLS certificate management shall adhere to TLS aspects in TS 33.310 [Ref 43] for the Za portion of the Nq and Na reference points with the following cavets.
   - Security Gateways are interpreted as the TLS endpoint
   - Cross certification is not supported
   - Mutual TLS is not supported
2. TLS certificate management may adhere to TLS aspects in TS 33.310 [Ref 43] for the Zb portion of the Nq and Na reference points.
3. Nq and Na reference points shall support TLS 1.2 (RFC 2818 [Ref 44] or higher as specified in RFC 7540 [Ref 33]

Annex A: Extract of the Wireless E9-1-1 Location Accuracy Requirements, Fourth Report & Order

(informative)

This informative Annex includes quoted text from Appendix D of the FCC's Wireless E9-1-1 Location Accuracy Requirements, Fourth Report and Order [Ref 1].

Final Rules

Part 20 of the Code of Federal Regulations is amended as follows:

PART 20 – COMMERCIAL MOBILE RADIO SERVICES

1. The authority for Part 20 is revised to read as follows:

Authority: 47 U.S.C. §§ 151, 152(a), 154(i), 157, 160, 201, 214, 222, 251(e), 301, 302, 303, 303(b), 303(r), 307, 307(a), 309, 309(j)(3), 316, 316(a), 332, 615, 615a, 615b, 615c.

2**.** Section 20.18 is amended by amending paragraph (h)(3) and re-designating paragraphs (i) through (n) as paragraphs (o) through (t), adding new paragraphs (i) through (n), and revising paragraph (1) of re-designated new paragraph (n) to read as follows:

* * * * *

(h)(3) *Latency (Time to First Fix)*. For purposes of measuring compliance with the location accuracy standards of this paragraph, a call will be deemed to satisfy the standard only if it provides the specified degree of location accuracy within a maximum latency period of 30 seconds, as measured from the time the user initiates the 911 call to the time the location fix appears at the location information center: Provided, however, that the CMRS provider may elect not to include for purposes of measuring compliance therewith any calls lasting less than 30 seconds.

(i) *Indoor location accuracy for 911 and testing requirements*.

(1) *Definitions:* The terms as used in this section have the following meaning:

i. *Dispatchable location:* A location delivered to the PSAP by the CMRS provider with a 911 call that consists of the street address of the calling party, plus additional information such as suite, apartment or similar information necessary to adequately identify the location of the calling party. The street address of the calling party must be validated and, to the extent possible, corroborated against other location information prior to delivery of dispatchable location information by the CMRS provider to the PSAP.

ii. *Media Access Control (MAC) Address*. A location identifier of a Wi-Fi Access Point.

iii. *National Emergency Address Database (NEAD*). A database that utilizes MAC address information to identify a dispatchable location for nearby wireless devices within the CMRS provider's coverage footprint.

iv. *Nationwide CMRS provider:* A CMRS provider whose service extends to a majority of the population and land area of the United States.

v. *Non-nationwide CMRS provider:* Any CMRS provider other than a nationwide CMRS provider.

vi. *Test Cities*. The six cities (San Francisco, Chicago, Atlanta, Denver/Front Range, Philadelphia, and Manhattan Borough) and surrounding geographic areas that correspond to the six geographic regions specified by the February 7, 2014 ATIS Document, "Considerations in Selecting Indoor Test Regions," for testing of indoor location technologies.

(2) *Indoor location accuracy standards:* CMRS providers subject to this section shall meet the following requirements:

i. *Horizontal location*.

(A) Nationwide CMRS providers shall provide (1) dispatchable location, or (2) x/y location within 50 meters, for the following percentages of wireless 911 calls within the following timeframes, measured from the effective date of the adoption of this rule:

(1) Within 2 years: 40 percent of all wireless 911 calls.

(2) Within 3 years: 50 percent of all wireless 911 calls.

(3) Within 5 years: 70 percent of all wireless 911 calls.

(4) Within 6 years: 80 percent of all wireless 911 calls.

(B) Non-nationwide CMRS providers shall provide (1) dispatchable location or (2) x/y location within 50 meters, for the following percentages of wireless 911 calls within the following timeframes, measured from the effective date of the adoption of this rule:

(1) Within 2 years: 40 percent of all wireless 911 calls.

(2) Within 3 years: 50 percent of all wireless 911 calls.

(3) Within 5 years or within six months of deploying a commercially-operating VoLTE platform in their network, whichever is later: 70 percent of all wireless 911 calls.

(4) Within 6 years or within one year of deploying a commercially-operating VoLTE platform in their network, whichever is later: 80 percent of all wireless 911 calls.

ii. *Vertical location.* CMRS providers shall provide vertical location information with wireless 911 calls as described in this section within the following timeframes measured from the effective date of the adoption of this rule:

(A) Within 3 years: All CMRS providers shall make uncompensated barometric data available to PSAPs with respect to any 911 call placed from any handset that has the capability to deliver barometric sensor information.

(B) Within 3 years: Nationwide CMRS providers shall develop one or more z-axis accuracy metrics validated by an independently administered and transparent test bed process as described in paragraph (i)(3)(a) of this section, and shall submit the proposed metric or metrics, supported by a report of the results of such development and testing, to the Commission for approval.

(C) Within 6 years: In each of the top 25 CMAs, nationwide CMRS providers shall deploy either (1) dispatchable location, or (2) z-axis technology in compliance with any z-axis accuracy metric that has been approved by the Commission,

(1) In each CMA where dispatchable location is used: nationwide CMRS providers must ensure that the NEAD is populated with a sufficient number of total dispatchable location Reference Points to equal 25 percent of the CMA population.

(2) In each CMA where z-axis technology is used: nationwide CMRS providers must deploy z-axis technology to cover 80 percent of the CMA population.

(D) Within 8 years: In each of the top 50 CMAs, nationwide CMRS providers shall deploy either (1) dispatchable location or (2) such z-axis technology in compliance with any z-axis accuracy metric that has been approved by the

Commission.

(E) Non-nationwide CMRS providers that serve any of the top 25 or 50 CMAs will have an additional year to meet each of the benchmarks in paragraphs (i)(2)(ii)(C)-(D) of this section.

iii. *Compliance*. Within 60 days after each benchmark date specified in paragraphs (i)(2)(i) and (ii) of this section, CMRS providers must certify that they are in compliance with the location accuracy requirements applicable to them as of that date. CMRS providers shall be presumed to be in compliance by certifying that they have complied with the test bed and live call data provisions described in paragraph (i)(3) of this section.

(A) All CMRS providers must certify that the indoor location technology (or technologies) used in their networks are deployed consistently with the manner in which they have been tested in the test bed. A CMRS provider must update certification whenever it introduces a new technology into its network or otherwise modifies its network, such that previous performance in the test bed would no longer be consistent with the technology's modified deployment.

(B) CMRS providers that provide quarterly reports of live call data in one or more of the six test cities specified in paragraph (i)(1)(vi) of this section must certify that their deployment of location technologies throughout their coverage area is consistent with their deployment of the same technologies in the areas that are used for live call data reporting.

(C) Non-nationwide CMRS providers that do not provide service or report quarterly live call data in any of the six test cities specified in paragraph (i)(1)(vi) must certify that they have verified based on their own live call data that they are in compliance with the requirements of paragraphs (i)(2)(i)(B) and (ii) of this section.

iv. *Enforcement.* PSAPs may seek Commission enforcement within their geographic service area of the requirements of paragraphs (i)(2)(i) and (ii) of this section, but only so long as they have implemented policies that are designed to obtain all location information made available by CMRS providers when initiating and delivering 911 calls to the PSAP. Prior to seeking Commission enforcement, a PSAP must provide the CMRS provider with [30] days written notice, and the CMRS provider shall have an opportunity to address the issue informally. If the issue has not been addressed to the PSAP's satisfaction within 90 days, the PSAP may seek enforcement relief.

(3) *Indoor location accuracy testing and live call data reporting*.

i. *Indoor location accuracy test bed.* CMRS providers must establish the test bed described in this section within 12 months of the effective date of this rule. CMRS providers must validate technologies intended for indoor location, including dispatchable location technologies and technologies that deliver horizontal and/or vertical coordinates, through an independently administered and transparent test bed process, in order for such technologies to be presumed to comply with the location accuracy requirements of this paragraph. The test bed shall meet the following minimal requirements in order for the test results to be considered valid for compliance purposes:

(A) include testing in representative indoor environments, including dense urban, urban, suburban and rural morphologies;

(B) test for performance attributes including location accuracy (ground truth as measured in the test bed), latency (Time to First Fix), and reliability (yield); and

(C) Each test call (or equivalent) shall be independent from prior calls and accuracy will be based on the first location delivered after the call is initiated.

(D) In complying with paragraph (i)(3)(i)(B) of this section, CMRS providers shall measure yield separately for each individual indoor location morphology (dense urban, urban, suburban, and rural) in the test bed, and based upon the specific type of location technology that the provider intends to deploy in real-world areas represented by that

particular morphology. CMRS providers must base the yield percentage based on the number of test calls that deliver a location in compliance with any applicable indoor location accuracy requirements, compared to the total number of calls that successfully connect to the testing network. CMRS providers may exclude test calls that are dropped or otherwise disconnected in 10 seconds or less from calculation of the yield percentage (both the denominator and numerator).

ii. *Collection and reporting of aggregate live 911 call location data*. CMRS providers providing service in any of the Test Cities or portions thereof must collect and report aggregate data on the location technologies used for live 911 calls in those areas.

(A) CMRS providers subject to this section shall identify and collect information regarding the location technology or technologies used for each 911 call in the reporting area during the calling period.

(B) CMRS providers subject to this section shall report Test City call location data on a quarterly basis to the Commission, the National Emergency Number Association, the Association of Public Safety Communications Officials, and the National Association of State 911 Administrators, with the first report due 18 months from the effective date of rules adopted in this proceeding.

(C) CMRS providers subject to this section shall also provide quarterly live call data on a more granular basis that allows evaluation of the performance of individual location technologies within different morphologies (*e.g.*, dense urban, urban, suburban, rural). To the extent available, live call data for all CMRS providers shall delineate based on a per technology basis accumulated and so identified for: (1) each of the ATIS ESIF morphologies; (2) on a reasonable community level basis; or (3) by census block. This more granular data will be used for evaluation and not for compliance purposes.

(D) Non-nationwide CMRS providers that operate in a single Test City need only report live 911 call data from that city or portion thereof that they cover. Non-nationwide CMRS providers that operate in more than one Test City must report live 911 call data only in half of the regions (as selected by the provider). In the event a non-nationwide CMRS provider begins coverage in a Test City it previously did not serve, it must update its certification pursuant to paragraph (i)(2)(iii)(C) of this section to reflect this change in its network and begin reporting data from the appropriate areas. All non-nationwide CMRS providers must report their Test City live call data every 6 months, beginning 18 months from the effective date of rules adopted in this proceeding.

(E) Non-nationwide CMRS providers that do not provide coverage in any of the Test Cities can satisfy the requirement of paragraph (i)(3)(ii) of this section by collecting and reporting data based on the largest county within its footprint. In addition, where a non-nationwide CMRS provider serves more than one of the ATIS ESIF morphologies, it must include a sufficient number of representative counties to cover each morphology.

iii. *Data retention*. CMRS providers shall retain testing and live call data gathered pursuant to this section for a period of 2 years.

(4) *Submission of plans and reports*. The following reporting and certification obligations apply to all CMRS providers subject to this section, which may be filed electronically in PS Docket No. 07-114:

i. *Initial implementation plan.* No later than 18 months from the effective date of the adoption of this rule, nationwide CMRS providers shall report to the Commission on their plans for meeting the indoor location accuracy requirements of paragraph (i)(2) this section. Non-nationwide CMRS providers will have an additional 6 months to submit their implementation plans.

ii. *Progress reports.* No later than 18 months from the effective date of the adoption of this rule, each CMRS provider shall file a progress report on implementation of indoor location accuracy requirements. Non-nationwide CMRS providers will have an additional 6 months to submit their progress reports. All CMRS providers shall provide an additional progress report no later than 36 months from the effective date of the adoption of this rule. The 36-month reports shall indicate what progress the provider has made consistent with its implementation plan, and the nationwide CMRS providers shall include an assessment of their deployment of dispatchable location

solutions. For any CMRS provider participating in the development of the NEAD database, this progress report must include detail as to the implementation of the NEAD database described in paragraphs (i)(4)(iii)-(iv) of this section.

iii. *NEAD privacy and security plan*. Prior to activation of the NEAD but no later than 18 months from the effective date of the adoption of this rule, the nationwide CMRS providers shall file with the Commission and request approval for a security and privacy plan for the administration and operation of the NEAD. The plan must include the identity of an administrator for the NEAD, who will serve as a point of contact for the Commission and shall be accountable for the effectiveness of the security, privacy, and resiliency measures.

iv. *NEAD use certification*. Prior to use of the NEAD or any information contained therein to meet such requirements, CMRS providers must certify that they will not use the NEAD or associated data for any non-911 purpose, except as otherwise required by law.

(j) *Confidence and uncertainty data.*

(1) Except as provided in paragraphs (j)(2)-(3) of this section, CMRS providers subject to this section shall provide for all wireless 911 calls, whether from outdoor or indoor locations, x- and y-axis (latitude, longitude) confidence and uncertainty information (C/U data) on a per-call basis upon the request of a PSAP. The data shall specify (1) the caller's location with a uniform confidence level of 90 percent, and (2) the radius in meters from the reported position at that same confidence level. All entities responsible for transporting confidence and uncertainty between CMRS providers and PSAPs, including LECs, CLECs, owners of E911 networks, and emergency service providers, must enable the transmission of confidence and uncertainty data provided by CMRS providers to the requesting PSAP.

(2) Upon meeting the 3-year timeframe pursuant to paragraph (i)(2)(i) of this section, CMRS providers shall provide with wireless 911 calls that have a dispatchable location the C/U data for the x- and y-axis (latitude, longitude) required under paragraph (k)(1) of this section.

(3) Upon meeting the 6-year timeframe pursuant to paragraph (i)(2)(b) of this section, CMRS providers shall provide with wireless 911 calls that have a dispatchable location the C/U data for the x- and y-axis (latitude, longitude) required under paragraph (k)(1) of this section.

(k) *Provision of live 911 call data for PSAPs*. Notwithstanding other 911 call data collection and reporting requirements in paragraph (i) of this section, CMRS providers must record information on all live 911 calls, including, but not limited to, the positioning source method used to provide a location fix associated with the call. CMRS providers must also record the confidence and uncertainty data that they provide pursuant to paragraphs (j)(1)-(3) of this section. This information must be made available to PSAPs upon request and shall be retained for a period of two years.

(m) *Reports on Phase II plans*. * * *

(n) * * *

(1) *Generally*. The requirements set forth in paragraphs (d) through (n) of this section shall be applicable only to the extent that the administrator of the applicable designated PSAP has requested the services required under those paragraphs and such PSAP is capable of receiving and utilizing the requested data elements and has a mechanism for recovering the PSAP's costs associated with them.

Annex B: Example Heightened Accuracy Location Use Cases

(informative)

This clause identifies use cases, from a user perspective, for scenarios where the caller expects to obtain assistance from Public Safety. The user places a call to 9-1-1, the call is delivered to the appropriate Public Safety 9-1-1 services system and on to the appropriate PSAP. The Telecommunicator receives the dispatch location with the call or obtains it via a query mechanism. The Telecommunicator then relays the incident information to the Dispatcher, who dispatches the first responders (not included in the use cases). Note that technical solutions discussed elsewhere in this standard may apply to one or more of the use cases. A technical solution is not required to apply to all of the use cases. As a corollary, a use case may be satisfied by one or more technical solutions.

In the following use cases, when available, caller's X, Y coordinates will be provided for use in conjunction with the Dispatchable Location.

B.1 Use Case 1: Wireless User Encounters an Emergency Outdoors

Short Description

A subscriber of a U.S. CMRS provider develops respiratory problems while walking down the street. He dials 9-1-1 to obtain aid.

Actors

- John is the pedestrian with respiratory problems.
- CMRS network.
- Emergency Services Network.
- Pat is the Telecommunicator at the PSAP.

Pre-Conditions

John is in distress.

John's mobile phone is attached to the CMRS network through the CMRS provider's licensed spectrum.

Post Conditions

Pat has received the emergency call and determined that emergency aid is needed. She forwards the incident information to the Dispatcher who dispatches the First Responders.

Normal Flow

1. John feels in distress while walking down the street.
2. John dials 9-1-1 with his mobile phone.
3. The CMRS network initiates the steps to obtain the heightened accuracy location of the caller's device.
4. The call is routed from the CMRS network to the appropriate Emergency Services Network.
5. The call is routed to the appropriate PSAP by the Emergency Services Network.
6. Pat answers the call and obtains the heightened accuracy location of John's mobile device by querying for a heightened accuracy location (PSAP CPE may include an auto location update).
7. Pat assesses the situation and forwards the incident to the Dispatcher who will dispatch First Responders.

B.2 Use Case 2: An Emergency Call from a Mobile Phone in the Proximity Of Registered Wi-Fi Access

Short Description

Master Grand accompanied his Dad on a visit to his Dad's friend Mr. Hand. Mr. Hand happened to have Internet connectivity at his house with Wi-Fi access. Master Grand is able to play on-line games while the two elder statesmen are busy.

During the visit, Master Grand encounters a situation where he has to make an emergency call from his Dad's mobile phone. Master Grand who just accompanied his Dad was not aware of the address of Mr. Hand's house.

However, Mrs. Poland (at the PSAP) responding to the emergency call sees that the emergency situation is at Mr. Hand's house and dispatches the emergency personnel to that address to attend for the emergency cause.

Actors

- Master Grand and his Dad (guests).
- Mr. Hand (host).
- Mrs. Poland (PSAP call taker).
- Emergency personnel.

Pre-Conditions

1. Mr. Hand has Internet connectivity at his house with a registered Wi-Fi access.

   NOTE: Here, the registered Wi-Fi access means that the MAC address of Mr. Hand's Wi-Fi router is registered to his home address and the association between the MAC address and the home address is in the National Emergency Address Database (NEAD). The method used to enter such information to NEAD is outside the scope of this use case description.

2. The wireless signal is quite good at around Mr. Hand's house. Master Grand is able to make calls from his Dad's mobile phone.
3. Master Grand's Dad's mobile phone is a smart phone with the latest software upgrades and hence, is able to handle indoor location enhancement requirements.

   NOTE: Able to handle indoor location requirements means that when an emergency call is made, the Wi-Fi and Bluetooth are automatically enabled on the mobile phone and the mobile phone upon query is able to provide the MAC addresses of all the Wi-Fi Access Points and BT-PDAs of all the Bluetooth beacons that it sees in response to the query. After the emergency call, the Wi-Fi and Bluetooth capabilities on the mobile phone go back to the status they had prior to the call.

4. PSAP-H is handling the emergency calls around the area where Mr. Hand's house is located.
5. Mrs. Poland is one of the call takers at PSAP-H.

Post-Condition

PSAP emergency personnel attend the cause of the emergency at Mr. Hand's house.

Normal Flow

1. An emergency situation occurs while Master Grand and his Dad are visiting Mr. Hand's house.
2. Neither Master Grand's Dad nor Mr. Hand are able to able to make calls.
3. Master Grand, now under panic, dials 9-1-1 from his Dad's locked phone.
4. The emergency call is routed to PSAP-H serving the area where Mr. Hand's house is located.
5. Mrs. Poland at PSAP-H answers the emergency call.
6. Mrs. Poland while trying to find the address from where the emergency call has come from asks Master Grand about the address.

7. Master Grand is not able to tell the address since he is just visiting the place (he is not able to look into the phone for the address they used on the Maps while driving, since the phone is locked).
8. Mrs. Poland who sees that the emergency call is from Mr. Hand's home address advises Master Grand to remain calm and dispatches the emergency personnel to Mr. Hand's home address to attend to the cause.
9. Emergency personnel arrive at Mr. Hand's house and are able to resolve the emergency issue.

Network Functional Flow

1. When an emergency call is made, the network routes the call to the PSAP based on the cell-identity with which the mobile phone is associated.
2. The network queries the mobile device for MAC addresses of Wi-Fi Access Points and/or BT-PDAs of Bluetooth beacons.
3. Mobile device returns the MAC address of the Wi-Fi Access Point that it sees to the network.
4. The network queries the NEAD with the MAC address.
5. NEAD finds a candidate Dispatchable Location (Mr. Hand's home address) associated with the MAC address.
6. NEAD returns the candidate Dispatchable Location (Mr. Hand's home address) back to the network.
7. The network determines and sends the selected Dispatchable Location (Mr. Hand's home address) toward the PSAP.

B.3 Use Case 3: An Emergency Call from a Mobile Phone in the Neighborhood of Registered Wi-Fi Access

Short Description

Mrs. Lee is on a phone call, while also busy cooking in the kitchen. A lightning strike kills the power in the house along with a shock to Mrs. Lee. The sudden shock makes Mrs. Lee collapse, but not before dialing 9-1-1 from her smart phone.

Mr. Parker (at the PSAP) responding to the emergency call is not able to communicate with the caller but finds out that the emergency call is coming from Mr. Nathan's house. Mr. Parker dispatches the emergency personnel to Mr. Nathan's house. The emergency personnel arriving at Mr. Nathan's house finds no trouble there but soon are able to judge that the emergency is in the neighboring Mrs. Lee's house (with no power in the house; palm tree outside burning) and are able to attend to the cause right away.

Actors

- Mrs. Lee (where the lightning strikes).
- Mr. Nathan (neighbor).
- Mr. Parker (PSAP call taker).
- Emergency personnel.

Pre-Condition

1. Mrs. Lee's neighborhood has Internet connectivity in almost all the houses with individual registered Wi-Fi access points. Mr. Nathan happens to be the closest neighbor to Mrs. Lee.

   NOTE: Here, the registered Wi-Fi access points mean that the MAC addresses of Wi-Fi access points are registered to individual home addresses where they are located and the association between the MAC addresses and the corresponding home addresses are in the National Emergency Address Database (NEAD). The method used to enter such information to NEAD is outside the scope of this use case description.
2. The wireless signal is quite good around Mrs. Lee's house. Mrs. Lee is able to make calls from her mobile phone.

3. Mrs. Lee's mobile phone is a smart phone with the latest software upgrades and hence, is able to handle indoor location enhancement requirements.

   NOTE: Able to handle indoor location enhancement requirements means that when an emergency call is made, the Wi-Fi and Bluetooth are automatically enabled on the mobile phone and the mobile phone upon query is able to provide the MAC addresses of all the Wi-Fi Access Points and BT-PDAs of all the Bluetooth beacons that it sees in response to the query. After the emergency call, the Wi-Fi and Bluetooth capabilities on the mobile phone go back to the status they had prior to the call.
4. PSAP-L is handling the emergency calls around the area where Mrs. Lee's house is located.
5. Mr. Parker is one of the call takers at PSAP-L.

Post-Condition

PSAP emergency personnel attend to the cause of the emergency at Mrs. Lee's house.

Normal Flow

1. An emergency situation (lightning strike) occurs in Mrs. Lee's house resulting in the loss of the power.
2. Mrs. Lee who receives an electric shock due to the lightning strike calls 9-1-1 and collapses.
3. The emergency call is routed to PSAP-L serving the area where Mrs. Lee's house is located.
4. Mr. Parker at PSAP-L answers the emergency call.
5. Mr. Parker is not able to talk to the emergency caller but sees that emergency call has come from a location near Mr. Nathan's house.
6. Mr. Parker dispatches the emergency personnel to Mr. Nathan's home address to attend to the cause.
7. Emergency personnel arrive at Mr. Nathan's house and find no trouble.
8. Emergency personnel soon discover that the emergency situation must be in the neighbor's house after observing that the house has lost power and that there is a burning palm tree in front of the house.
9. Emergency personnel arrive at Mrs. Lee's house to attend to the emergency situation.

Network Functional Flow

1. When an emergency call is made, the network routes the call to the PSAP based on the cell-identity with which the mobile phone is associated.
2. The network queries the mobile device for MAC addresses of Wi-Fi Access Points and/or BT-PDAs of Bluetooth beacons.
3. Mobile device returns the MAC addresses of the Wi-Fi Access Points that it sees to the network.
4. The network queries the NEAD with the MAC addresses.
5. NEAD finds candidate Dispatchable Locations (home addresses of houses around Mrs. Lee's house) associated with the MAC addresses.
6. NEAD returns the candidate Dispatchable Locations back to the network.
7. The network determines Dispatchable Location and sends the selected Dispatchable Location (Mr. Nathan's home address) toward the PSAP.

B.4 Use Case 4: An Emergency Call from a Mobile Phone in a Multistory Building

Short Description

This emergency situation happens on the 24th floor of New-Site, a multi-story building, where some remodeling is going on. There are multiple registered Wi-Fi Access Points and a nearby smart vending machine with a registered Bluetooth beacon.

Mr. Worky who cannot speak English, working nearby, encounters an emergency situation and makes an emergency call from his mobile phone. He cannot speak English and hence, cannot answer many of the PSAP call taker's questions.

However, Mr. Poland (at the PSAP) responding to the emergency call sees that the emergency situation is on the 24th floor of New-Site building the address of the building and dispatches the emergency personnel to that location (24th floor of New-Site building) to attend to the emergency cause.

Actors

- Mr. Worky.
- Mr. Poland (PSAP call taker).
- Emergency personnel.

Pre-Conditions

1. 24th floor New-Site building has a smart vending machine with a registered Bluetooth beacon and a registered Wi-Fi access point.

   NOTE 1: Here, the registered Bluetooth beacon means that the Bluetooth Public Device Address (BT-PDA) of the Bluetooth beacon is associated with a certain location (in the example, 24th floor, New-Site building) and the address of the location and the associated BT-PDA are in the National Emergency Address Database (NEAD). The method used to enter such information to NEAD is outside the scope of this use case description.

   NOTE 2: Here, the registered Wi-Fi Access Point means that the MAC Address of the Wi-Fi Access Point is associated with a certain location (in the example, 24th floor, New-Site building) and the address of the location and the associated MAC address are in the National Emergency Address Database (NEAD). The method used to enter such information to NEAD is outside the scope of this use case description.
2. The wireless signal is quite good on the 24th floor of New-Site building. Mr. Worky is able to make calls from his mobile phone.
3. Mr. Worky's mobile phone is able to handle indoor location enhancement requirements.

   NOTE: Able to handle indoor location enhancement requirements means that when an emergency call is made, the Wi-Fi and Bluetooth are automatically enabled on the mobile phone and the mobile phone, upon query, is able to provide the MAC addresses of all the Wi-Fi Access Points and BT-PDAs of the Bluetooth beacons that it sees, in response to the query. After the emergency call, the Wi-Fi and the Bluetooth capabilities on the mobile phone go back to the status they had prior to the call.
4. PSAP-N is handling the emergency calls around the area where the New-Site building is located.
5. Mr. Poland is one of the call takers at PSAP-N.

Post-Condition

PSAP emergency personnel attend to the cause of the emergency on the 24th floor of New-Site building.

Normal Flow

1. An emergency situation occurs where Mr. Worky is working on the 24th floor of New-Site building.
2. Mr. Worky dials 9-1-1 from his mobile phone.
3. The emergency call is routed to PSAP-N serving the area where New-Site building is located.
4. Mr. Poland at PSAP-N answers the emergency call.
5. Mr. Poland while trying to find the address from where the emergency call has come from asks Mr. Worky about the address.
6. Mr. Worky cannot speak English, does not know the address, but says something like New-Site.
7. Mr. Poland does not know what New-Site means but receives the address of New-Site building along with the information that the emergency is happening on the 24th floor of the building through the system. Mr. Poland then dispatches the emergency personnel to the New-Site building to attend to the cause.
8. Emergency personnel arrive at the 24th floor of New-Site building and are able to resolve the emergency cause.

Network Functional Flow

1. When an emergency call is made, the call is routed to the PSAP based on the cell-identity with which the mobile phone is associated.
2. The network queries the mobile device for MAC addresses of Wi-Fi Access Points and/or BT-PDAs of Bluetooth beacons.
3. Mobile device returns the BT-PDA of the Bluetooth beacon and the MAC addresses of the Wi-Fi Access Points that it sees to the network.
4. The network queries the NEAD with the BT-PDA and MAC Addresses.
5. NEAD finds candidate Dispatchable Locations associated with the BT-PDA and the MAC Addresses.
6. NEAD returns the candidate Dispatchable Locations back to the network.
7. The network determines which Dispatchable Location is to be delivered to the PSAP.

   NOTE: The algorithm used to determine the Dispatchable Location is outside the scope of this use case description.
8. The network sends the selected Dispatchable Location toward the PSAP.

B.5 Use Case 5: An Emergency Call from a Mobile Phone in the Proximity Of Registered Bluetooth Beacons

Short Description

The situation of emergency occurs in Birds Jungle amusement park at the Parrot Dancing Show. Mr. Funman who is at the Parrot Dancing Show takes action by dialing 9-1-1. The amusement park has quite a few registered Bluetooth beacons attached to the smart vending machines and sometimes to the sensors at the Shows. There is no Internet access or Wi-Fi Access points around the Parrot Dancing Show in the Birds Jungle.

Mr. Funman knows that he is at the amusement park but does not know the exact address of Birds Jungle.

However, Mr. Holand (at the PSAP) responding to the emergency call sees that the emergency situation is happening in Birds Jungle amusement park at the Parrot Dancing Show and knows the exact address where it is located. Mr. Holland dispatches the emergency personnel to that location to attend to the emergency cause.

Actors

- Mr. Funman.
- Mr. Holand (PSAP call taker).
- Emergency personnel.

Pre-Conditions

1. Birds Jungle amusement park has smart vending machines with the registered Bluetooth beacons and sensors (at the shows), also with registered Bluetooth beacons.

   NOTE: Here, the registered Bluetooth beacon means that the Bluetooth Public Device Address (BT-PDA) of the Bluetooth beacon is associated with a certain location and the address of the location and the associated BT-PDA are in the National Emergency Address Database (NEAD). The method used to enter such information to NEAD is outside the scope of this use case description.
2. The wireless signal is quite good at the Parrot Dancing Show in the Birds Jungle. Mr. Funman is able to make calls from his mobile phone.
3. Mr. Funman's mobile phone is able to handle indoor location enhancement requirements.

   NOTE: Able to handle indoor location enhancement requirements means that when an emergency call is made, the Wi-Fi and Bluetooth are automatically enabled on the phone and the phone, upon query, is able to provide the MAC addresses of all the Wi-Fi access points and BT-PDA of the Bluetooth beacons that it sees, in response to the query. After the emergency call, the Wi-Fi and the Bluetooth capabilities of the mobile phone go back to the status they had prior to the call.
4. PSAP-P is handling the emergency calls around the area where Birds Jungle is located.
5. Mr. Holand is one of the call takers at PSAP-P.

Post-Condition

PSAP emergency personnel attend to the cause of the emergency at the Parrot Dancing Show in Birds Jungle.

Normal Flow

1. An emergency situation occurs at the Parrot Dancing Show in Birds Jungle.
2. Mr. Funman dials 9-1-1 from his mobile phone.
3. The emergency call is routed to PSAP-P serving the area where Birds Jungle is located.
4. Mr. Holand at PSAP-P answers the emergency call.
5. Mr. Holand, while trying to find the address from where the emergency call has come, asks Mr. Funman about the address.
6. Mr. Funman informs Mr. Holand that the situation is happening at Parrot Dancing Show in Birds Jungle but does not know the address of the location.
7. With Birds Jungle being a big amusement park, Mr. Holand cannot determine where to send the dispatch. However, Mr. Holand receives the dispatchable address of Birds Jungle and Parrot Dancing Show and knows how to reach the place quickly. Mr. Holand then dispatches the emergency personnel to the exact location at the Birds Jungle to attend to the cause.
8. Emergency personnel arrive at the Parrot Dancing Show in Birds Jungle to resolve the emergency cause.

Network Functional Flow

1. When an emergency call is made, the network routes the call to the PSAP based on the cell-identity with which the mobile phone is associated.
2. The network queries the mobile device for MAC addresses of Wi-Fi Access Points and/or BT-PDAs of Bluetooth beacons.
3. Mobile device returns the BT-PDAs of the Bluetooth beacons that it sees to the network.
4. The network queries the NEAD with the BT-PDAs.
5. NEAD finds candidate Dispatchable Locations associated with the BT-PDAs.
6. NEAD returns the candidate Dispatchable Locations back to the network.
7. The network determines which one of the Dispatchable Locations has to be sent to PSAP.
   NOTE: The algorithm used to determine the Dispatchable Location is outside the scope of this use case description.
8. The network sends the selected Dispatchable Location toward the PSAP.

B.6 Use Case 6: An Emergency Call from a Mobile Phone in a Multistory Building in the Proximity of Wi-Fi Access Points of a Neighboring Building

Short Description

This emergency situation happens on the 24th floor of New-Site, a multi-story building, where some construction is going on with no electronic equipment on the floor.

Mr. Worky who cannot speak English, working on the floor, encounters an emergency situation and makes an emergency call from his mobile phone. He cannot speak English and hence, cannot answer many of the PSAP call taker's questions.

Mr. Poland (at the PSAP) responds to the emergency call and hears the word "New-Site" from the caller, but nothing more. However, Mr. Poland receives an indication that the incident site is on the 24th floor of Old-Site building. Mr. Poland obtains the address of the Old-Site building and dispatches the emergency personnel to that location (24th floor of Old-Site building) to attend to the emergency cause, noting that the caller has mentioned New-Site building. Upon arrival at the Old-Site building, the emergency personnel find no problem in the Old-Site building. With prior

knowledge of the caller mentioning New-Site building, emergency personnel rush to the 24th floor of New-Site building to attend to the emergency situation.

Actors

- Mr. Worky.
- Mr. Poland (PSAP call taker)
- Emergency personnel.

Pre-Conditions

1. 24th floor of New-Site building has no Wi-Fi access points or Bluetooth beacons.
2. However, the 24th floor of Old-site building, across the street, has registered Wi-Fi Access Points and registered Bluetooth beacons.

   NOTE 1: Here, the registered Bluetooth beacon means that the Bluetooth Public Device Address (BT-PDA) of the Bluetooth beacon is associated with a certain location (in the example, 24th floor, Old-Site building) and the address of the location and the associated BT-PDA are in the National Emergency Address Database (NEAD). The method used to enter such information to NEAD is outside the scope of this use case description.

   NOTE 2: Here, the registered Wi-Fi Access Point means that the MAC Address of the Wi-Fi Access Point is associated with a certain location (in the example, 24th floor, Old-Site building) and the address of the location and the associated MAC address are in the National Emergency Address Database (NEAD). The method used to enter such information to NEAD is outside the scope of this use case description.
3. The wireless signal is quite good on the 24th floor of New-Site building. Mr. Worky is able to make calls from his mobile phone.
4. Mr. Worky's mobile phone is able to handle indoor location enhancement requirements.

   NOTE: Able to handle indoor location enhancement requirements means that when an emergency call is made, the Wi-Fi and Bluetooth are automatically enabled on the mobile phone and the mobile phone, upon query, is able to provide the MAC addresses of all the Wi-Fi Access Points and BT-PDAs of the Bluetooth beacons that it sees, in response to the query. After the emergency call, the Wi-Fi and the Bluetooth capabilities on the mobile phone go back to the status they had prior to the call.
5. PSAP-N is handling the emergency calls around the area where the New-Site building is located.
6. Mr. Poland is one of the call takers at PSAP-N

Post-Condition

PSAP emergency personnel attend to the cause of the emergency on the 24th floor of New-Site building.

Normal Flow

1. An emergency situation occurs where Mr. Worky is working on the 24th floor of New-Site building.
2. Mr. Worky dials 9-1-1 from his mobile phone.
3. The emergency call is routed to PSAP-N serving the area where New-Site building is located.
4. Mr. Poland at PSAP-N answers the emergency call.
5. Mr. Poland, while trying to find the address from where the emergency call has come, asks Mr. Worky about the address.
6. Mr. Worky cannot speak English and does not know the address but says something like New-Site.
7. Mr. Poland does not know what New-Site means but receives the address of Old-Site building along with the information that the emergency is happening on the 24th floor of the building. Mr. Poland then dispatches the emergency personnel to the Old-Site building; however, informing the emergency personnel that caller had said something like New-Site building.
8. Emergency personnel arrive at 24th floor of Old-Site building with some going to the 24th floor of adjacent New-Site building (in case).
9. With no issue in the Old-Site building, all the emergency personnel go to the 24th floor of New-Site building and are able to attend to the emergency cause.

Network Functional Flow

1. When an emergency call is made, the call is routed to the PSAP based on the cell-identity with which the mobile phone is associated.
2. The network queries the mobile device for MAC addresses of Wi-Fi Access Points and/or BT-PDAs of Bluetooth beacons.
3. Mobile device returns the BT-PDA of the Bluetooth beacon and the MAC addresses of the Wi-Fi Access Points that it sees to the network.
4. The network queries the NEAD with the BT-PDA and MAC Addresses.
5. NEAD finds candidate Dispatchable Locations associated with the BT-PDA and the MAC Addresses.
6. NEAD returns the candidate Dispatchable Locations back to the network.
7. The network determines which Dispatchable Location is to be delivered to the PSAP. In this example, the network would determine that the 24th floor of Old-Site building is the most likely Dispatchable Location of the emergency situation.

   NOTE: The algorithm used to determine the Dispatchable Location is outside the scope of this use case description.
8. The network sends the selected Dispatchable Location (24th floor of Old-Site building) toward the PSAP.

Annex C: Location Accuracy Improvements for Emergency Calls XML Schema

(informative)

A ZIP file <**Annex C-ATIS-0700028v2_XML.zip**> has been electronically packaged with this ATIS Standard that provides the Location Accuracy Improvements for Emergency Calls XML schema. In case of any discrepancies between the XML schema descriptions in this document and those in the companion xsd document, the latter shall be normative.

Annex D: Dispatchable Location Concept Agreement

(informative)

Dispatchable Location (DL) is a viable location that carries a high level of assurance that indicates a caller can be located by emergency services based on the information presented. A Public Safety Telecommunicator can then leverage this location to deploy emergency services to a citizen in need of assistance. Emerging 9-1-1 location solutions in handsets, chipsets, networks as well as the NEAD, bring many improvements to the emergency location ecosystem. In order to acknowledge the evolving ecosystem and its progression of emerging solutions and access data points, those known today and those of tomorrow, we recommend the use of a level rating of (2) highest level or (1) mid-level, with all defined 9-1-1 wireless Dispatchable Locations. DL takes 9-1-1 location beyond our current XY horizontal coordinate and horizontal uncertainity. DL provides a civic address and additional information as required to adequately locate the calling party. As a starting point for this evolution given the constraints of current technology, we propose that the DL level will be based on the address and sub-address data along with other parameters that are useful in locating the caller. Examples include place type, serving flag, and RSSI among others.

We believe DL will evolve into greater levels of precision as emerging location solutions enter into the emergency location ecosystem and the NEAD data points grow over time, not limited to but to include external access points and Bluetooth beacons. We expect initially there could be a higher number of DL Level 1 locations than DL Level 2 but believe the evolution of the 9-1-1 location ecosystem will drive the percentage of DL Level 2 to higher percentages than DL Level 1. To encourage this evolution, we recommend aligning development of the NEAD and related location technologies with the FCC 4th Report and Order timeframes and requirements.

Below are recommended baselines to define Dispatchable Location Assurance Levels.

Level 2			
Civic Address of the caller	Floor	Zone (NW, SW, NE, SE) <=50 meters	Room/Suite
Level 1			
Civic Address of the caller	Floor (+/-) 1	Zone (NW, SW, NE, SE) <=50 meters	

It is recommended:

Some place types are eligible for DL Level 2 by default. An example would include, but is not limited to, Residential Single Family Home. Other likely cases include low energy beacons.

Low Coverage RF APs (<=50 meters coverage) with validated civic address are eligible for DL Level 2 classification: (FEMTO, FIXED, PICO).

NEAD DL Quality Level Mapping

The DL level mapping will be a combination of data points located in the NEAD (as illustrated in the table below) and the Location Services process. By combining as much available data as possible, placing it in context (place type), and identifying other relevant descriptors (serving flag, etc.), it should be possible to narrow the search ring for a caller in direct proportion to the data available.

NOTE: DL Level 2 exception – Some place types could be mapped to DL Level 2, even though they do not contain all the defined DL Level 2 data points.

Example Table is shown in Table D.1.

Table D.1 – Data Point Table

	Multi-Story Business	Multi-Family Dwelling	Two Story Office	Sports Arena	Single Family Dwelling	Small Business FEMTO	Multi-Story Business	Multi-Family Dwelling	Two Story Office	Sports Arena
Civic Address	X	X	X	X	X	X	X	X	X	X
Floor	X	X	X	X			X	X	X	X
Room/Suite	X	X	X	X						
Zone	X	X	X	X			X	X	X	X
TBD										

DL Level 2

DL Level 1

Annex E: ELS Supporting Enterprise Wi-Fi/BLE Location

(informative)

This Annex provides a description of acquiring dispatchable location via External Location Server interaction in support of Enterprise Wi-Fi/BLE beacon deployed networks. Several commercial WLAN location systems are available that locate Wi-Fi enabled UE devices within managed Wi-Fi and Bluetooth environments during a 9-1-1 emergency call.

Background:

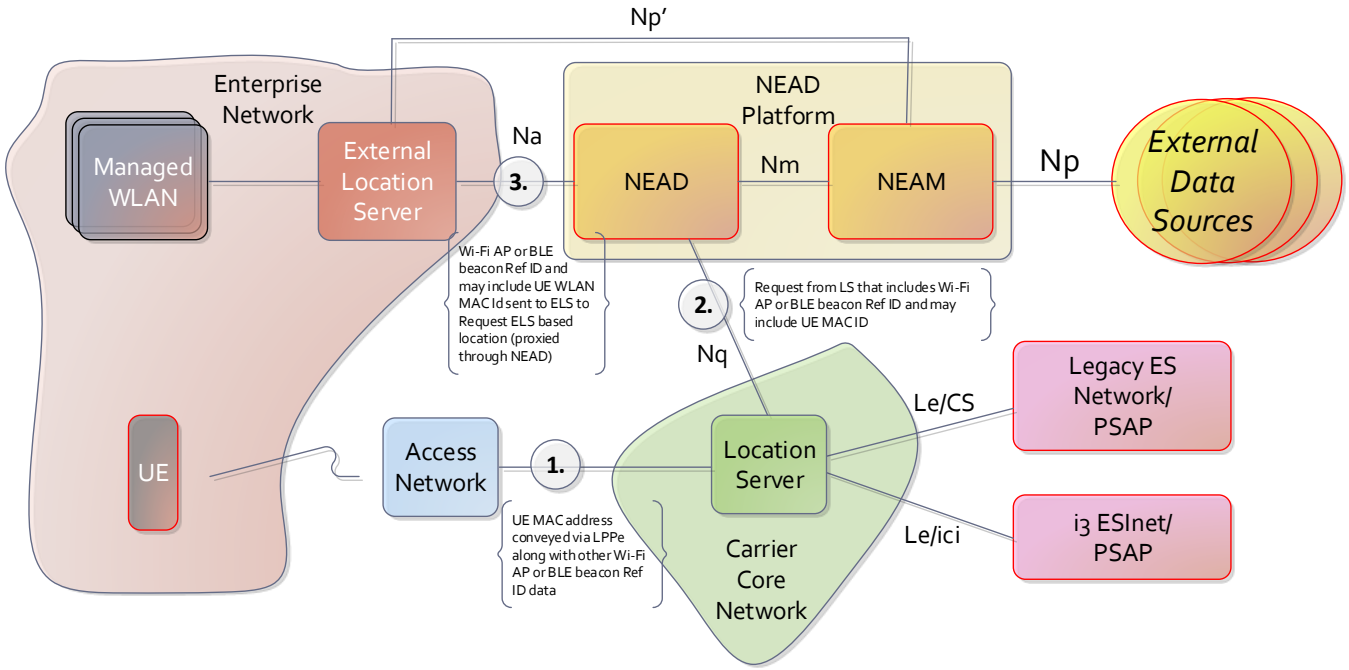
WLAN External Location Server accessed from NEAD (NEAD as a proxy):

In support of emergency calling within the constraints of new rules for Indoor Location accuracy, certain enterprises have unique capabilities to store, access, and maintain Wi-Fi AP location data (as well as for Bluetooth beacons in some cases) from within the enterprise's own managed Wi-Fi location platform environment. For some of these entities, provisioning their AP/BLE location data into the NEAD directly is not an option. External WLAN location platforms exist but require the MAC address of the UE's WLAN interface to be returned over the LPPe protocol, (embedded within the LPP protocol) as input to determine and return location information.

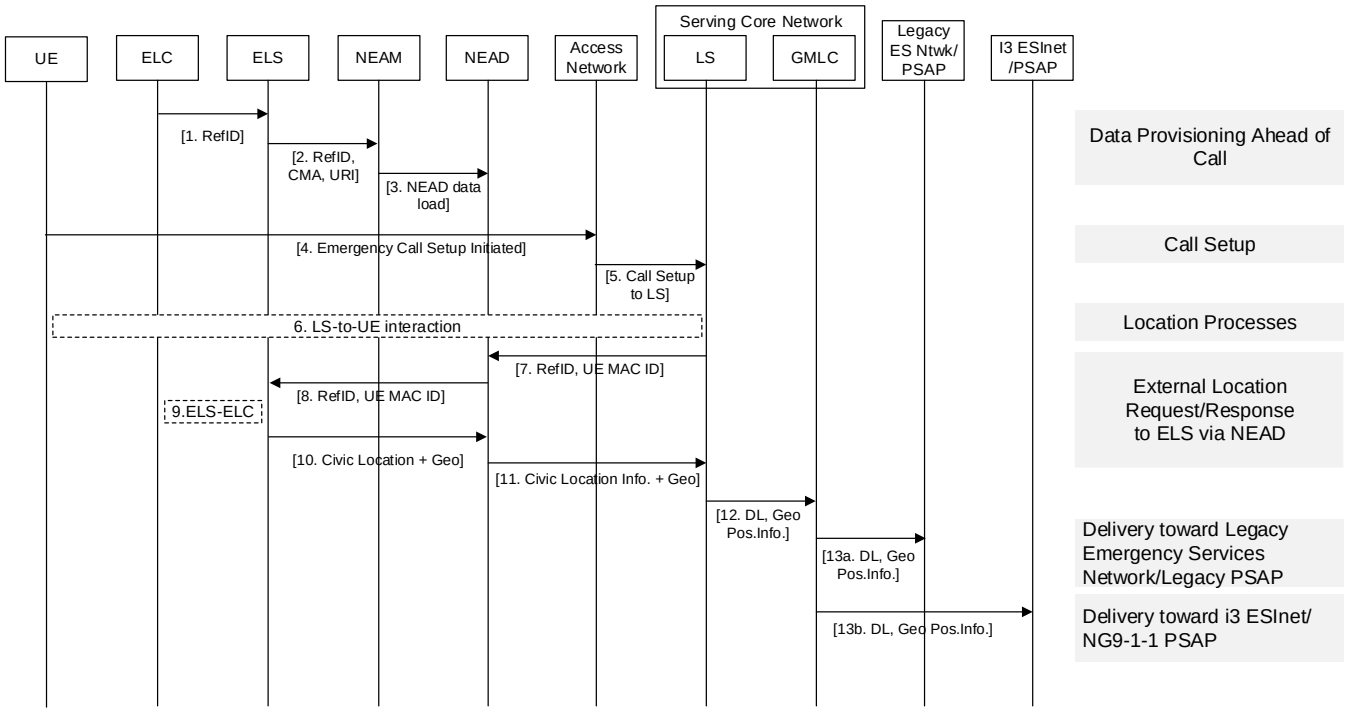
Increasingly, operators have relationships with enterprises that have large managed Wi-Fi networks. More sophisticated than home/residential Wi-Fi networks, they include highly-accurate location positioning systems specifically tuned for enterprise domains. Devices deployed within these domains are identified by their MAC address with other attachment credentials specific to each enterprise network.

The following example is based on current ATIS/ELOC development work around the NEAD and its interaction with the enterprise External Location Server (ELS). The example shows that the Location Server (LS) receives the UE's WLAN MAC address, along with other identifiers from a UE in view of a Wi-Fi network (1). The LS queries the NEAD, the NEAD identifies the WLAN network (via the NEAD provisioning process) (2). It then queries a WLAN External Location Server associated with the enterprise to obtain a current dispatchable location attributed to the UE (3).

Conceptual Diagram:



Call flow diagram:



Call Flow Detail:

1. The Reference ID for any Wi-Fi AP or BT beacon that is deployed within that managed area is sent from the ELC to the ELS. This step happens when a new management domain is created or whenever any new Wi-Fi AP or BT beacon is added or modified within the managed domain.
2. The ELS sends Wi-Fi AP and BT beacon Reference IDs, URIs, and CMA IDs to the NEAM for provisioning into the NEAD. This is done over the Np' interface utilizing an M2M interface.
3. The NEAM pushes the URI data to the NEAD.
4. An emergency 9-1-1 call is initiated in an indoor area served by a Reference ID provisioned in the NEAD.
5. The LS receives the 9-1-1 call.
6. The LS interacts with the UE to retrieve any observed Reference Points and the UE WLAN MAC address.
7. The LS sends a query to the NEAD over the Nq providing Reference Point ID and UE WLAN MAC address. The NEAD finds an entry containing Reference Point ID and a URI that points to the ELS.
8. The NEAD sends a query to the ELS over the Na providing Reference Point ID and UE WLAN MAC address.
9. The ELS interacts with the ELC to obtain a Dispatchable Location representing the area where the UE is located.
10. The ELS returns Dispatchable Location information along with geocoded location to the NEAD.
11. The NEAD sends Dispatchable Location information along with geocoded location to the LS in the Serving Core network.
12. The LS sends Dispatchable Location along with measured geodetic position information (determined by the LS) to the GMLC within the Serving Core network.

13a. [Case Legacy Emergency Services network] The GMLC provides location information that includes Dispatchable Location and geodetic position information (determined by the LS) along with other required ALI data in response to a location request from an ALI system.

13b. [Case NG9-1-1 Emergency Services Network] The PSAP equipment initiates a location request to the LNG. The LNG queries the GMLC for information that includes Dispatchable Location information and geodetic position information and passes the information to the PSAP.

Assumptions for ELS:

1. In order to enable WLAN location for 9-1-1, Wi-Fi access points are “managed”. That is, there is a WLAN location management element. This is referred to as the External Location Controller (ELC). The ELC communicates with each Wi-Fi AP or BLE beacon involved in the WLAN and interoperates with an external location server (ELS) that is connected to the NEAD Platform.
2. The WLAN environment is represented by a polygon (e.g., pixel map, or rectangular shape) that represents the area in which the Wi-Fi APs or BLE beacons have coverage. This is commonly thought of as a building floor map.
3. There should be one polygon per floor of a multi-level structure.
4. Each polygon has a description of a civic location assigned to it in the ELC system. The civic address information should contain enough information to make it dispatchable to public safety, including street address and sub-address information as applicable; including building number, unit, floor, and placetype.
5. The ELC sends the polygon with associated civic address to the ELS.
6. The ELS validates the civic address to determine if it is dispatchable. If so, the ELS geocodes the dispatchable address, storing the information. If not dispatchable, the ELS returns an error message to the ELC, and does not store any information.
7. Wi-Fi APs, and optionally, BLE beacons are deployed within the building coverage area (i.e., polygon).
8. The ELC should be “tuned” for the environment, including antenna direction, signal strength, etc.
9. The ELC discovers each Wi-Fi AP or BLE beacon that it is responsible for and that it intends to use for indoor location.
10. The ELC updates the ELS, in real time, each new or changed AP or BLE beacon.

Methods to “figure out” location:

Common approaches to determine and/or acquire location:

a. Associate – acquire the location of something else that is in close proximity to the thing being located.
b. Provision – enter location data into a database before it’s needed, then access the data when its needed at call time.
c. Determine -- calculate by way of one or more techniques based on measurement data, e.g., utilize some known reference points with timing offsets in order to perform trilateration. “Known points” implies that some kind of surveying, whether manual or estimated, must take place for the Wi-Fi APs in this case.
d. Derive – take one form in and produce another form out (e.g., geocode from civic address to a lat/lon).
e. Pattern match, (fingerprint), where the device “sees” a radio signal environment at a known point and attempts to match a similar stored RF signature that is associated to a position.

ELCs have their own proprietary methods to determine the position of the UE within their managed domain as represented by the floor map, or polygon. A common approach used is that of relative Received Signal Strength Indication (RSSI), but some systems perform Angle of Arrival (AoA) and/or Fine Timing Measurements (FTM), which offer greater accuracy but require more sophisticated hardware. In the same way that GPS or AGPS works for outdoor positioning, determination techniques are not explained in detail here and are documented elsewhere.

With the RSSI approach, the network of Wi-Fi APs managed by the ELC can be described as a network-based passive location technique. The UE is not actively involved in collecting and passing any information to the ELC for this technique. The ELC “listens” for any UE (the UE must be powered on and have the Wi-Fi interface turned on) then the APs collect RSSI and potentially other measurement data. The ELC then reduces the measurements to both a position (e.g., pixel offset) and an associated candidate civic location (embedded into the polygon).

If the ELS receives the BT-PDA along with the UE WLAN MAC address over the Na, then it can attribute the appropriate zone information (assuming zones are provisioned with the floor map). If, for example, the UE reported only one Bluetooth identifier (BT-PDA), the ELS would get only one Na query and the ELS should still be able to find the UE within the appropriate floor map, zone, etc.

The ELC calculates the pixel offset according to the calibrated floor map. The ELC provides the pixel offset to the ELS, along with the map that the position references, the zone that is referenced on the map and the civic address embedded into the floor map. The Dispatchable Location (including zone information) and geocoded location get sent back to the NEAD/LS. Other information is not currently used.

Many of these indoor location systems utilize Wi-Fi for bi-directional communication during and after the location determination process. Some systems incorporate Bluetooth Low Energy (BLE) to achieve a finer grained location than what may be produced using Wi-Fi alone. Making BLE location work, can happen in a few different ways. The current, most common use of BLE beacons incorporates physical BLE devices that are placed around a room or hallway using fairly short spacing (e.g., every five meters) to deliver a broadcast message that an end device can pick up and utilize or look up the BLE information in a database. The NEAD is an example of this database approach.

There is at least one other type of Real Time Location System (RTLS) that makes use of virtual BLE beacons to provide fine grained position information. This kind of system doesn't have the same power and scaling challenges that physical beacons are faced with yet claims good indoor accuracy (3 meter resolution).

The use of floor maps:

Floor map files, or polygons that represent the "indoor" extent of the area that the end device is being located within are used with most Wi-Fi based indoor systems that perform measurements and associations. An association can be done successfully if the target device is found inside the polygon and not outside of it.

The floor map, which might be as simple as a rectangle that encompasses the floor area, must be created ahead of data provisioning and would be part of an indoor space deployment process. Deployment can be straightforward or complex, depending on the level of detail desired. Once created, the floor map is tagged with civic address information and optionally further divided into zones (for example, directional quadrants, conference room areas, etc.). It is then sent to the ELS as part of the existing deployment protocols (proprietary among vendors). The floor map is represented as a graphics file with embedded metadata describing the associated address and zone information. Once the ELS receives the file with metadata, it can:

1. Validate the civic address.
2. Geocode the civic address.
3. Provision the URI and CMA information into the NEAM.

The ELC actively manages all Wi-Fi APs under its control, knowing their relative positions within the floor map and aggregating measurement and performance information from each managed AP. Each Wi-Fi AP that supports Bluetooth also monitors for any BLE broadcasts and reports them to the ELC.

During an emergency call, the managed WLAN itself provides two primary functions for determining location. First, it provides Wi-Fi and BLE broadcast information to the handset enabling the handset to collect the Wi-Fi and BLE identifier information which is then passed to the LS (over LPP). These are the Reference IDs that must be provisioned into the NEAD (via the NEAM) for the system to work. Second, the WLAN provides the ELC measurement information that the ELC uses in determining position of any target UE that the WLAN "sees".

Once an emergency call is initiated, and as part of the carrier-based location processes, the UE captures Wi-Fi AP and BLE beacon Reference ID's, sending them to the LS. After the ELS receives a query for location determination from the NEAD, (initiated from the LS), the ELS communicates with the ELC to provide back to the ELS location information that includes: a relative position (e.g., pixel offset), associated civic address and zone information. The ELC uses RSSI measurement data and other techniques (based on implementation) to determine that the UE is within a specific polygon and zone and is then able to extract the associated civic address and zone description from the selected polygon, forwarding the results to the ELS along with other data contained within the ELS such as a geocoded position and CMA value. The ELS returns this candidateDispatchable Location and geocoded location to the NEAD in the response to the original query after which it gets forwarded to the LS where it can be compared with the typical position information obtained from the carrier location infrastructure.

Comparison between WLAN location systems supported by ELS and proximate WLAN systems

Proximate Wi-Fi location:

a. A Wi-Fi AP Reference Point identifier and associated civic address is entered into the NEAM, validated, geocoded, and stored in the NEAD database.
b. The UE has its Wi-Fi interface enabled.
c. At emergency 9-1-1 call time, the UE "scans the air" to see any Wi-Fi AP(s) in proximity.
d. The UE collects one or more Wi-Fi AP Reference IDs that is in range of the UE's Wi-Fi interface and sends to the LS.
e. Based on an internal algorithm, the LS determines which Wi-Fi AP Reference IDs to send to the NEAD.

f. The NEAD returns provisioned candidate Dispatchable Location (civic address) for each queried Reference ID, if found, along with geocoded lat/lon.

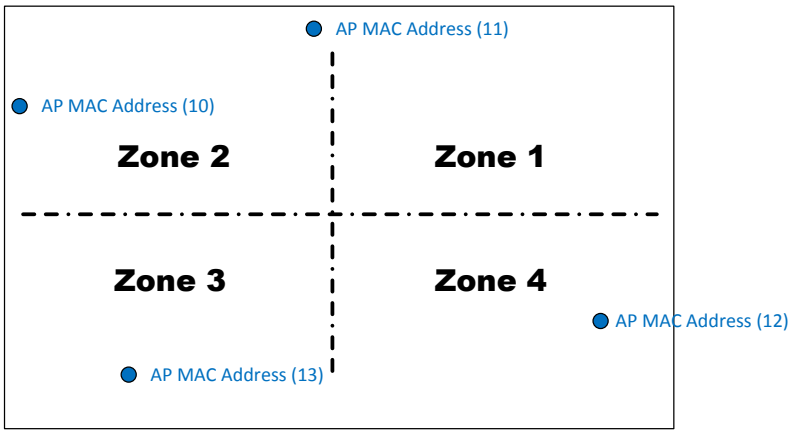
WLAN Managed Wi-Fi and Bluetooth location:

a. A Wi-Fi AP and BLE beacon Reference ID and URI is entered into the NEAM and stored in the NEAD database.
b. The UE has its Wi-Fi interface enabled.
c. At emergency 9-1-1 call time, the UE "scans the air" to see any Wi-Fi AP(s) in proximity.
d. The UE collects one or more Wi-Fi AP or BLE beacon Reference IDs that is in range of the UE's Wi-Fi and Bluetooth radio interfaces and sends to the LS along with the UE WLAN MAC address.
e. Based on an internal algorithm, the LS determines which Wi-Fi AP or BLE beacon Reference ID to send to the NEAD, along with UE WLAN MAC address if available.
f. The NEAD, based on a URI associated with the Reference ID, initiates a query to the ELS to find and return the candidate Dispatchable Location for the building footprint where the Wi-Fi AP or BLE beacon is deployed, along with geocoded lat/lon.

Graphic example of WLAN Location determination:

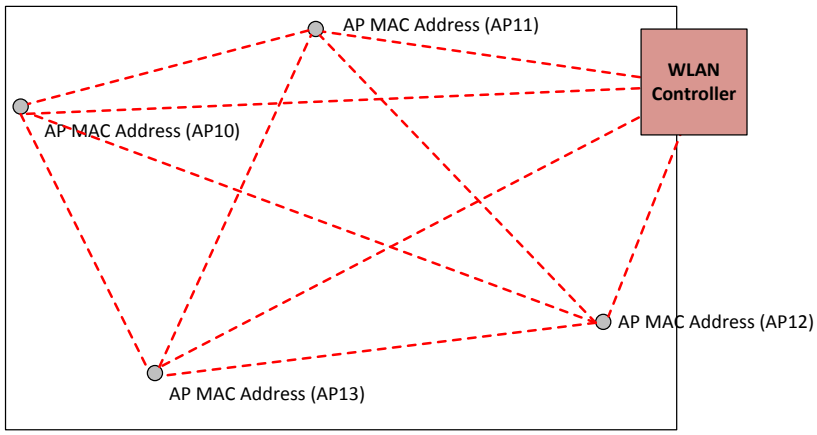
A. A polygon, (or pixel extent), is created for each floor or space, representing an indoor area that is a managed domain of Wi-Fi or BLE devices. A civic address, a candidate Dispatchable Location, is embedded into a rectangular graphics file representing the polygon within the ELC system. This file is sized in proportion to the area of coverage, e.g., 80 x 50 pixels represents an area with length and width equal to this same 8/5 ratio. A civic address that represents the area is embedded into the file as metadata, here shown as, "123 Main Street, Building A, Floor 4, Sometown, SomeState, SomeZIP".

B. Zones are defined within the polygon area, then both Wi-Fi APs and BLE beacons that are deployed across the polygon are added within the polygon. The details of creating the polygon, embedding civic address and zone metadata within it, establishing the Wi-Fi AP and BLE beacon positions are out of scope for this document, but are accomplished by using existing vendor tools.



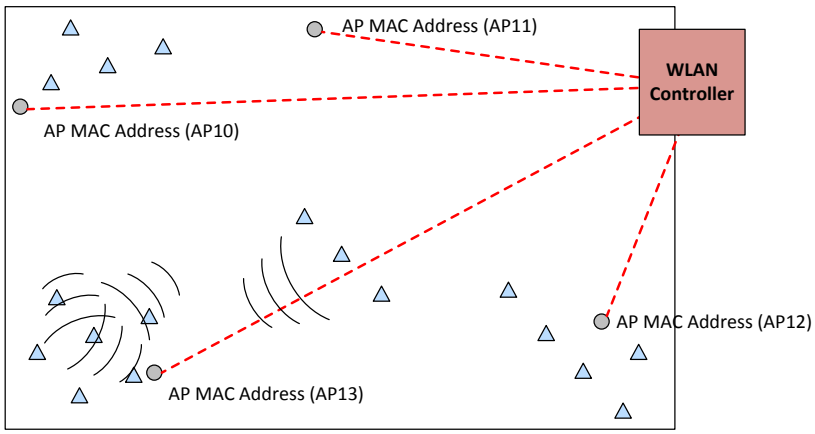
123 Main Street, Building A, Floor 4, Sometown, SomeState, SomeZIP

C. The ELC (labeled WLAN controller in these diagrams) discovers each Wi-Fi AP and its relative location within the polygon.



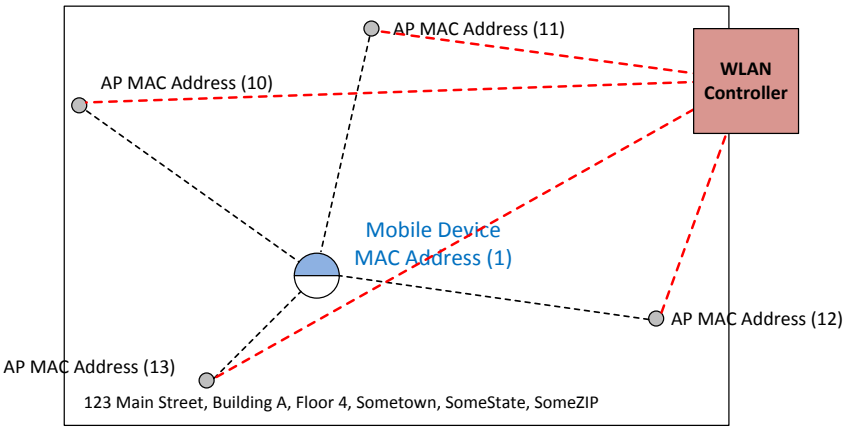
123 Main Street, Building A, Floor 4, Sometown, SomeState, SomeZIP

D. The ELC communicates with its network of Wi-Fi APs, including the monitoring of any BLE beacons (shown as triangles in the diagram) that may have been reported by the UE at emergency call time.

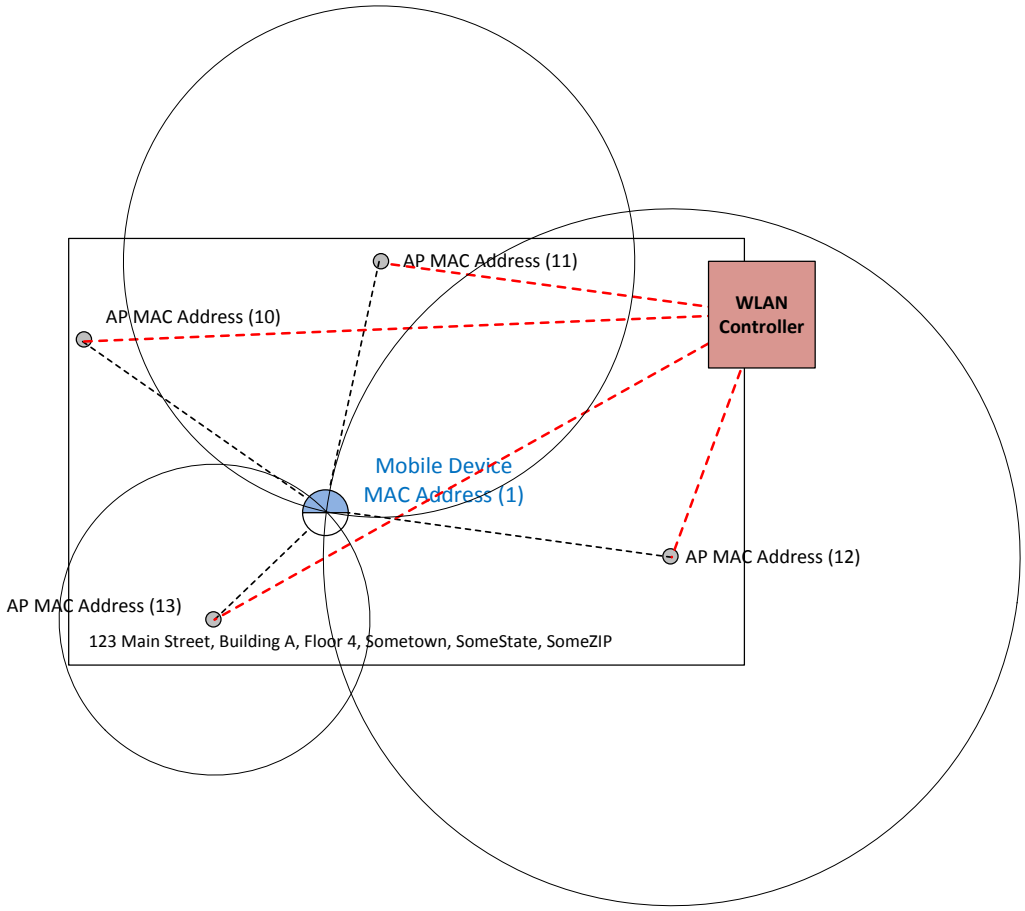


123 Main Street, Building A, Floor 4, Sometown, SomeState, SomeZIP

E. The ELC calculates the position of the UE within the polygon and returns the associated Dispatchable Location information to the ELS.



F. The techniques to calculate position vary by implementation. Shown here is a 2D intersecting circle technique using three circles, each at some distance "r" away from the UE. This position within the polygon is a certain number of pixels from the left and top boundaries, represented as a set of coordinates that provides a graphical representation of where the UE is, relative to the floor map.



G. Based on calibration of pixels to some distance (e.g., in meters), the relative position within the floor map can be output, for example, as 30 meters from the left wall, 35 meters from the back wall. Other coordinate outputs, such as latitude/longitude are possible, but require anchoring the floor map to an identified datum – an additional deployment step not covered here.

80 x 50 pixels, scale: 1 pixel = 1 meter