



Indoor Location Accuracy ATIS Emergency Location (ELOC) Standards

Christian Militeau

ATIS ELOC Task Force Co-Chair

Director, Technical Standards

West Safety Services (formerly Intrado)

christian.militeau@intrado.com

720-864-5245

Agenda

- Background
- ATIS ELOC Architecture
- NEAD Platform Overview
- Architecture & Call Flows
- Future Standards Development



- The four (Tier 1) wireless carriers – AT&T, Verizon, Sprint and T-Mobile
- Smaller carriers (Tier 2&3) represented by CCA
- CTIA is taking an overseeing role with the following Working Groups
 - Oversight/Advisory Working Group
 - Test Bed Working Group
 - NEAD Development Working Group
 - PSAP Implementation Working Group
 - Dispatchable Location Outreach Working Group
 - Z-Axis Working Group
 - Standards Working Group
 - Demonstration Working Group

- ATIS Emergency Location (ELOC) Task Force
 - Formed by ATIS to identify standards gaps and/or develop new standards
 - Made up of the Emergency Services Interconnection Forum (ESIF) and Wireless Technology and Systems Committee (WTSC)
- ESIF Emergency Services and Methodologies (ESM)
 - Defining Criteria for the location accuracy test bed and associated testing methodologies

- Defining the standard for which the NEAD RFP is based
- Hosted by ATIS Wireless Technology and Systems (WTSC) Committee and Emergency Services Interconnection Forum (ESIF)
- Co-Chairs
 - Peter Musgrove – AT&T Mobility
 - Christian Militeau – West Safety Services
- Participation by all major wireless carriers (AT&T, Sprint, Verizon and AT&T)
- Participation by many wireless location product vendors (Ericsson, Nokia, TCS, NextNav, TruePosition, Polaris Wireless, etc.)

- Voluntary Agreement
 - Agreed upon by the four major wireless carriers, NENA and APCO
 - Signed November 2014
 - Adopted by CCA for smaller carriers
 - FCC Fourth Report and Order
 - Issued March 2015
 - Adopted the Voluntary Agreement
 - Generally gave smaller carriers an extra year
 - Put specific dates for roll out of improved location accuracy
 - Defined Dispatchable Location (civic) as preference
 - Z-axis – Uncompensated Barometric Pressure (UBP)
 - NEAD – a new location database

- January 29, 2015 FCC Votes to accept 4th Report and Order on indoor location accuracy. March 4, 2015 Final Rules published in Federal Register
- Adds to but does not replace existing Wireless Phase II requirements
- Adopts “dispatchable location” and improved horizontal location requirements
- Requires near term delivery of uncompensated barometric pressure data and long term deployment of Z-axis solution
- Assesses performance using live 9-1-1 call data in representative cities
- Dispatchable location is Public Safety’s “gold standard”
- Leverages WiFi/BLE beacons, Small Cells and other technologies to provide dispatchable location
- Established National Emergency Address Database (NEAD)
- Set confidence level to fixed value of 90%
- Establish a 30-second maximum period for E9-1-1 location (TTFF)

- Wireless Providers Must provide “Dispatchable location” or “Latitude/Longitude coordinates within 50m” for the caller for:
 - 40% of all wireless 9-1-1 calls within 2 years
 - 50% of all wireless 9-1-1 calls within 3 years
 - 70% of all wireless 9-1-1 calls within 5 years
 - 80% of all wireless 9-1-1 calls within 6 years
- Non-nationwide carriers can extend the 5 and 6 years deadlines by six months and 1 year respectively based upon timing of VoLTE deployment in their networks
- Within 3 years
 - Provide uncompensated barometric pressure data to PSAPs from any capable device
 - Develop z-axis metric proposal to be submitted for commission approval
- Z-axis Metric
 - Populate NEAD with reference points equal to 25% if population of CMA or
 - Deploy Z-axis technology to cover 80% of population of CMA
- Non-nationwide carriers have an additional year to achieve these benchmarks

The value of a Civic Address over X/Y to Public Safety

Public Safety does not dispatch to a X/Y:

39° 41' 11.93" N Latitude

104° 58' 54.72" W Longitude

50 Meter Point Radius Uncertainty

Public Safety dispatch to a Civic Address



***Reverse Geocoding
Nearest Intersection***

***Reverse Geocoding
Address Range***

***Reverse Geocoding
Point Match***

S Pennsylvania St & E Iowa Ave
Denver, CO

1600-1650 S Pennsylvania St
Denver, CO

1615 S Pennsylvania St
Denver, CO



NEAM Assumptions

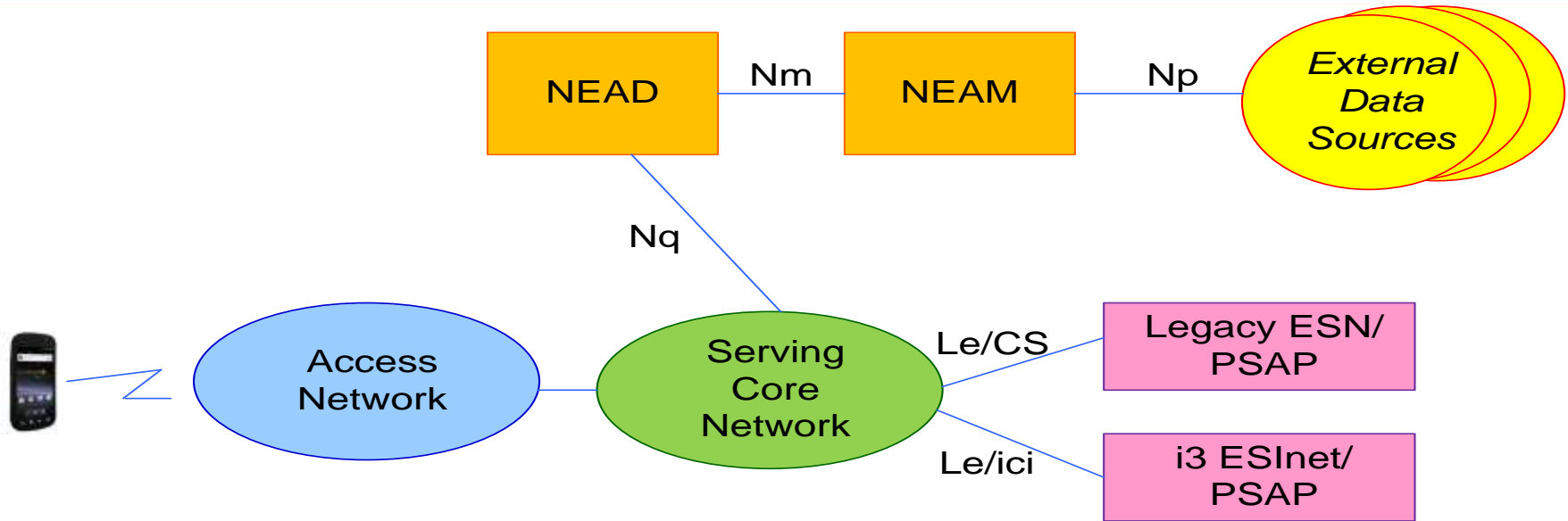
- External Data Sources will have a secure method to provision reference points into the NEAM (e.g., via web services).
- External Data Sources will be uniquely identified to enable the NEAM to include unique source IDs in its database (e.g., to allow all reference points provisioned by a particular External Data Source to be identified at a later date).
- Reference Points provisioned into the NEAM will include a single correlation between the reference point and a civic address.
- 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.
- All civic addresses will be validated against appropriate 9-1-1 addressing databases and geocoded prior to the NEAM pushing them to the NEAD.
- If validation or geocoding fails, the NEAM will provide that indication to the External Data Source.
- When pushing reference point information to the NEAD, the NEAM will indicate whether the information is new and to be added, existing information that is to be modified or whether an association is to be deleted.
- The NEAM will have full OA&M capabilities to include logging, reporting, alarming, etc.
- There may be multiple NEAM elements connected to a single NEAD.
- 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.
- It is assumed that an input over the Np may be in a variety of address forms.



NEAD Assumptions

- Following assumptions are for the NEAD:
- The NEAD is queried by or on behalf of the serving CMRS Network.
- NEAD hosting is carrier-independent.
- 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).
- The NEAD returns a civic address and an associated geocoded location determined by the NEAM 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.
- If the query cannot resolve to a civic address, the NEAD will return an error.
- All civic addresses will be validated and geocoded by the NEAM prior to being provisioned into the NEAD.
- The NEAD could be a single national database or a distributed database. The latter implies the need for a discovery or routing mechanism.
- If the NEAD is a distributed database, there will be a mechanism to synchronize any duplicate data among the elements.
- The NEAD will perform the addition, deletion, and modification of entries as directed by the NEAM.
- The NEAD will have full OA&M capabilities to include logging, reporting, alarming, etc.
- Crowdsourced geodetic location is not expected to be available as part of the NEAD.
- The NEAD will be able to accept multiple reference points for any call and return multiple civic addresses and geocoded locations in the response(s).
- The response may include either a location or an error code.
- The civic addresses returned by the NEAD may or may not include the actual dispatchable location of the UE as determined by the CMRS network.
- The NEAD will deliver over the Nq whatever form of candidate dispatchable location it has been provisioned with.
- In the context of this standard, the term MAC address is equivalent to a Wireless MAC/Basic Service Set Identifier (BSSID). Other common usages of MAC address may exist, but such usages are not applicable within this standard.

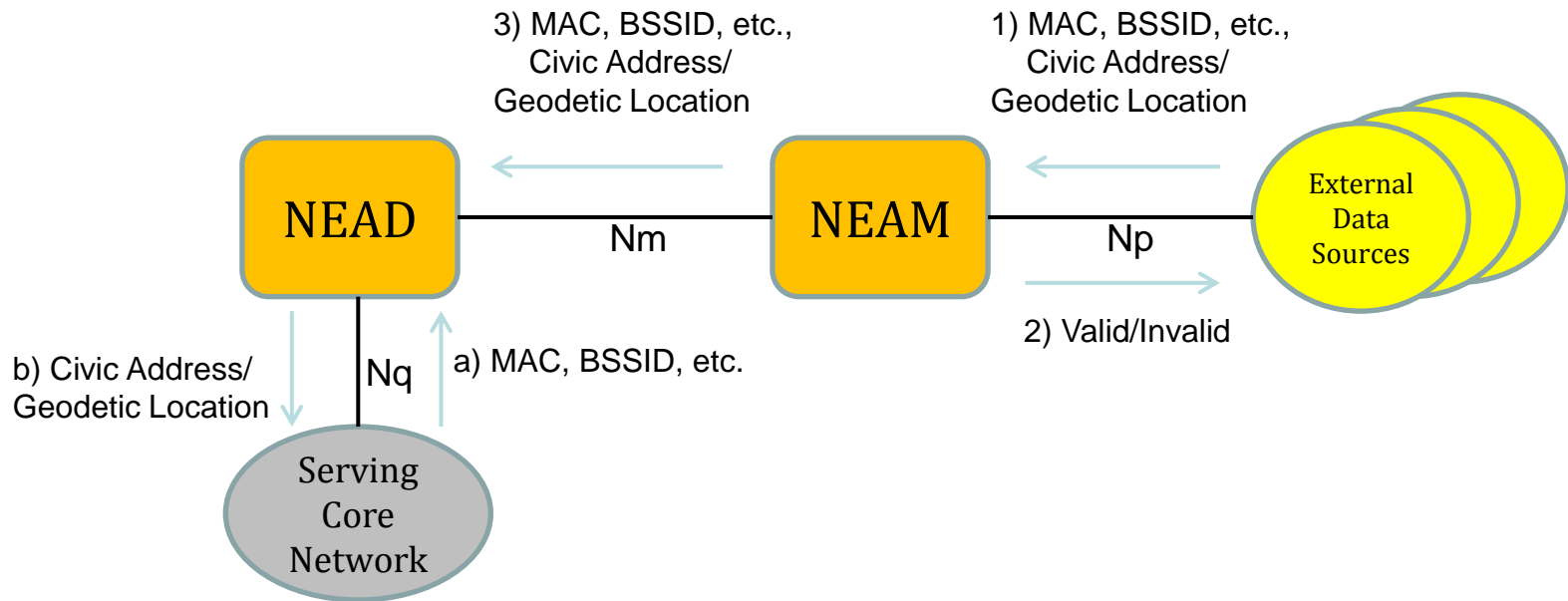
ATIS ELOC Architecture



- National Emergency Address Manager (NEAM)
- National Emergency Address Database (NEAD)
- Serving Core Network – includes e-SMLC and e-SLP

- External Data Sources
 - Enterprises, retail companies, hotels and the like that are responsible for WiFi Access Points and Bluetooth beacons
 - Enter their AP (or Bluetooth) location into the NEAD/NEAM
- NEAM
 - OA&M function that allows users to enter their data, validates the location, geocodes the location and pushes it to the NEAD
- NEAD
 - Real time server that hosts WiFi AP (and Bluetooth) location information
 - Queried by Serving Core Network for WiFi AP (and Bluetooth) location information
- Serving Core Networks
 - Queries the NEAD for WiFi AP (and Bluetooth) location
 - Determines “best” location to be sent to the PSAP
 - Includes IMS components – e-SMLC, e-SLP, LRF
 - Includes some legacy components – GMLC/MPC

Logic Flow



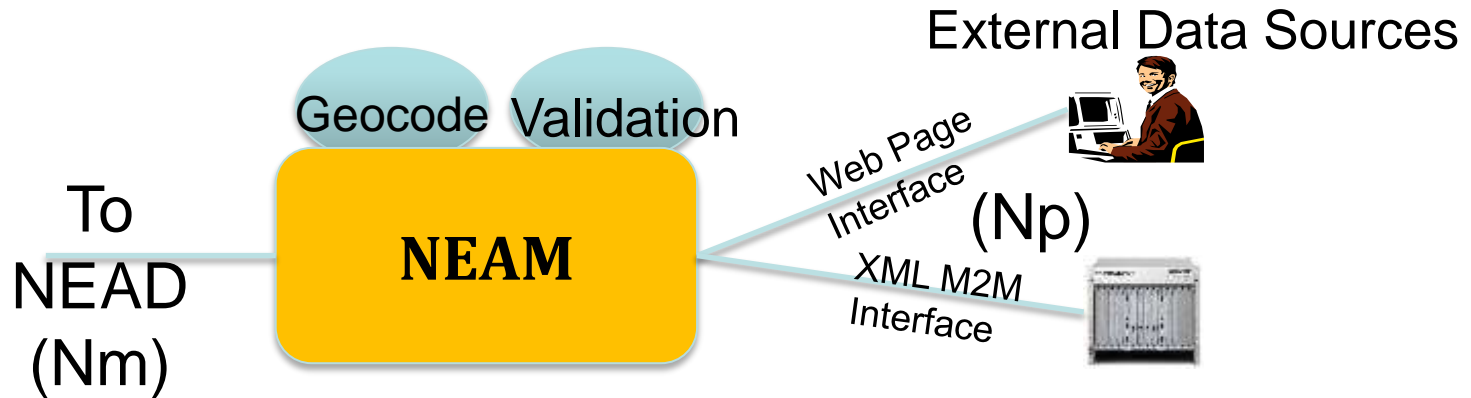


- Np
 - Provisioning interface that allow users to input their WiFi AP (or Bluetooth) location information into the NEAM
 - Protocols defined by ATIS ELOC:
 - A web page interface (HTML)
 - A web services XML M2M interface
- Nm
 - Interface that “pushes” location information from the NEAM to the NEAD after validation
 - Not currently defined by ATIS ELOC: Left to vendor implementation (must be published)
- Nq
 - Real time interface that allows the Serving Core Network to query the NEAD with WiFi AP (or Bluetooth) identifiers and returns location information
 - Serving Core Network will query the NEAD for all WiFi APs that the mobile device sees
 - Protocol defined by ATIS ELOC:
 - HELD with Identities (with multiple IDs in a single query)

- Must receive location information from authorized External Data Sources based upon ATIS ELOC defined protocols (Np)
 - Users may query for, add, modify or delete information related to their WiFi (or Bluetooth) access points
- Must validate location received from External Data Sources and geocode location
 - Details have not been discussed for validation type: MSAG or LVF (NG9-1-1)
 - Must notify user of validation success/failure (error)
 - Most likely requires some Data Integrity functionality
- Must “push” validated location and geocoded location to the NEAD
 - Protocol not defined for the Nm interface since it is likely that NEAM and NEAD will be closely tied and from the same provider
 - Concepts such as reliability, redundancy, maintainability, etc. have not been fully addressed an will be part of an Implementation Guidelines

- Will receive dispatchable locations and geocoded locations for WiFi APs (and Bluetooth) from the NEAM
- Must have the capability to add, modify or delete WiFi APs (and Bluetooth) location information sent from the NEAM
- Must be accessible in real time by all “authorized” wireless carriers
- Will be queried using WiFi AP ID (or Bluetooth Beacon Public Device Address) and must return location (civic and geocoded)
- Query protocol is HELD with Identities
- Concepts such as reliability, redundancy, maintainability, etc. will be addressed in an Implementation Guidelines

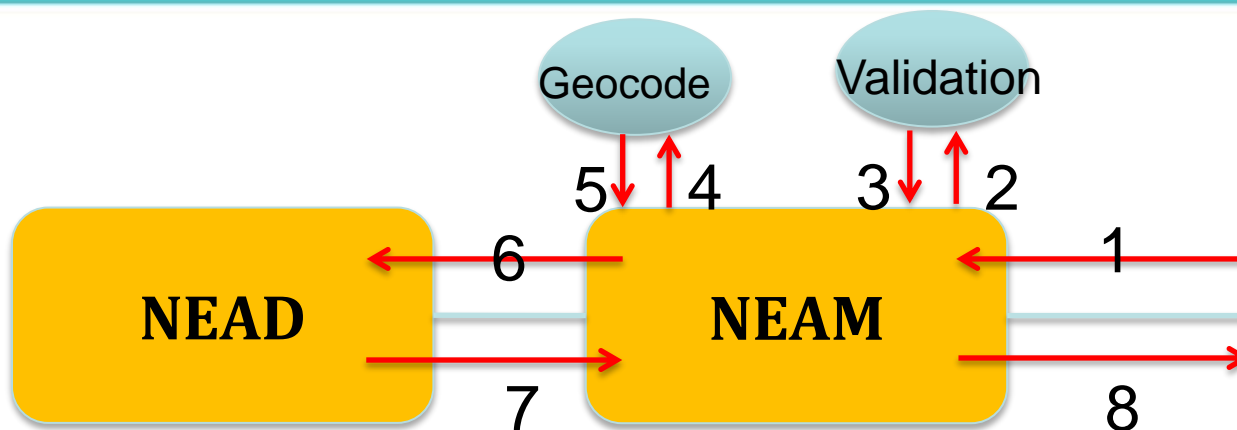
NEAM Characteristics



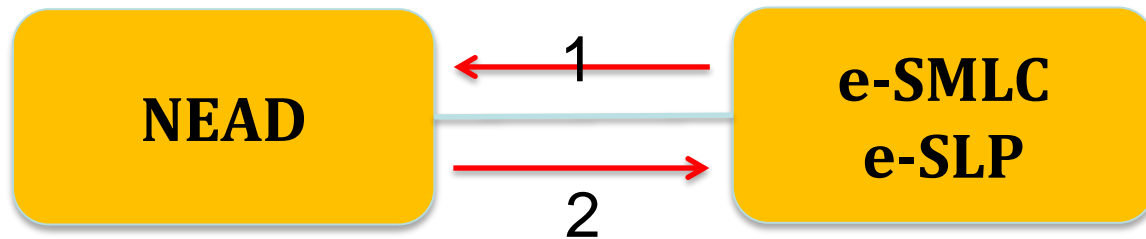
- Users access NEAM via Np interface to manage location information
- Np may be a web page (HTML) or XML M2M interface
- Users may query, add, modify or delete WiFi Access Point or Beacon information
- Information validated and geocoded before being pushed to NEAD via Nm
- XML M2M supports bulk adds

- External Data Sources expected to be “owners” of WiFi Access Points or Beacons from smaller entities
 - e.g. small businesses. Not expected to be residential users.
- May be also used by NEAD provider employees with expanded scope to manage all information
- External Data Sources can only manage WiFi Access Point or Beacon information that the “own”
 - Requires development of privileges in the NEAM
- Allows for 3rd parties to manage WiFi Access Point or Beacon information on behalf of a “owner”
 - Requires development of privileges in the NEAM to correlate users to one or more owners
- May query for information by MAC or address information (e.g. county and state)
- May add WiFi Access Point or Beacon information
- May modify WiFi Access Point or Beacon information that currently exists in the system
- May delete WiFi Access Point or Beacon information that they “own”

- External Data Sources expected to be “owners” of Access Points or Beacons from larger entities
 - E.g. enterprises.
- XML schema allows for bulk queries, adds, modifies, and deletes
- External Data Sources can only manage Access Point or Beacon information that the “own”.
 - Requires development of privileges in the NEAM.
- Allows for 3rd parties to manage Access Point or Beacon information on behalf of a “owner”
 - Requires development of privileges in the NEAM to correlate users to one or more owners
- May query for information by MAC or address information (e.g. county and state)
- May add Access Point or Beacon information
- May modify Access Point or Beacon information that currently exists in the system
- May delete Access Point or Beacon information that they “own”

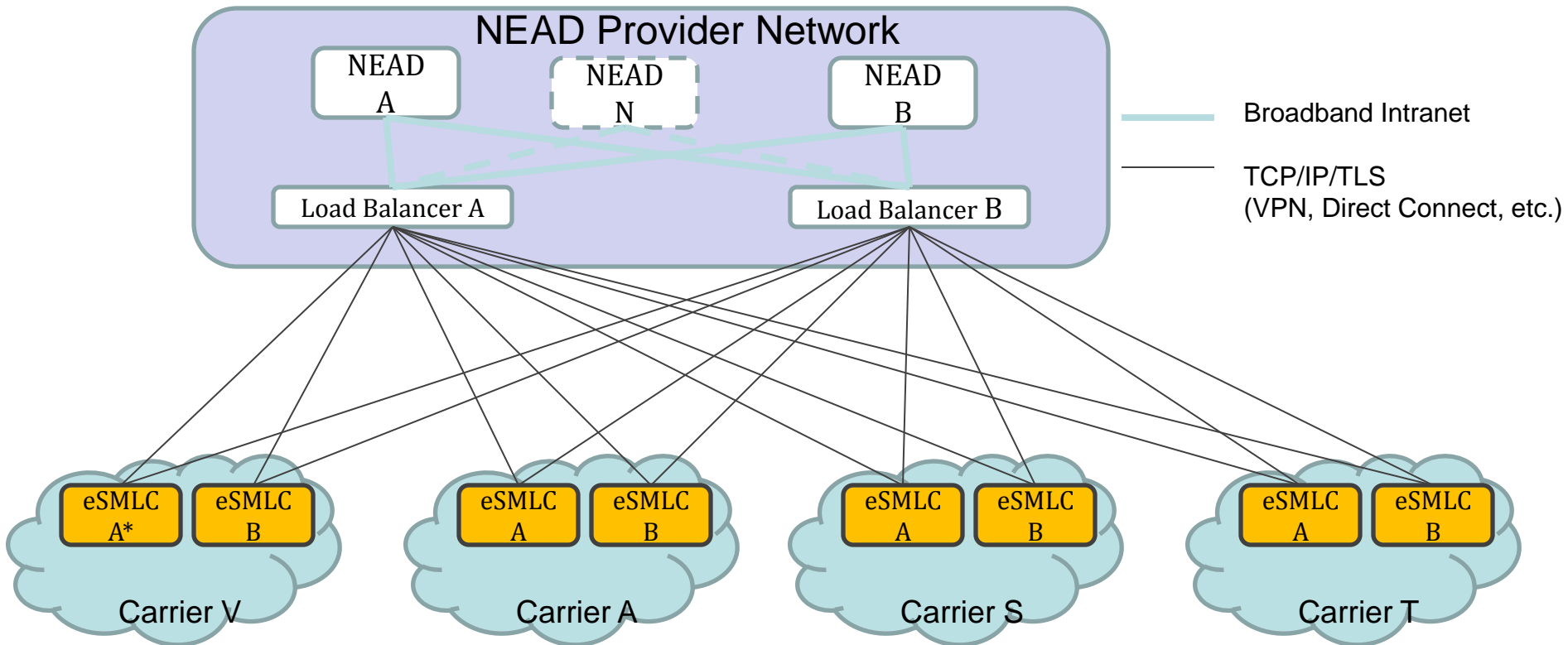


1. User submits address
2. NEAM requests validation
3. Validation successful (if error, return notification to user)
4. NEAM requests geocode
5. Geocode successful (if error, return notification to user)
6. NEAM pushes MAC and Address (civic and geocoded)
7. Push successful (if error, return notification to NEAM)
8. NEAM notifies user of success (or error)

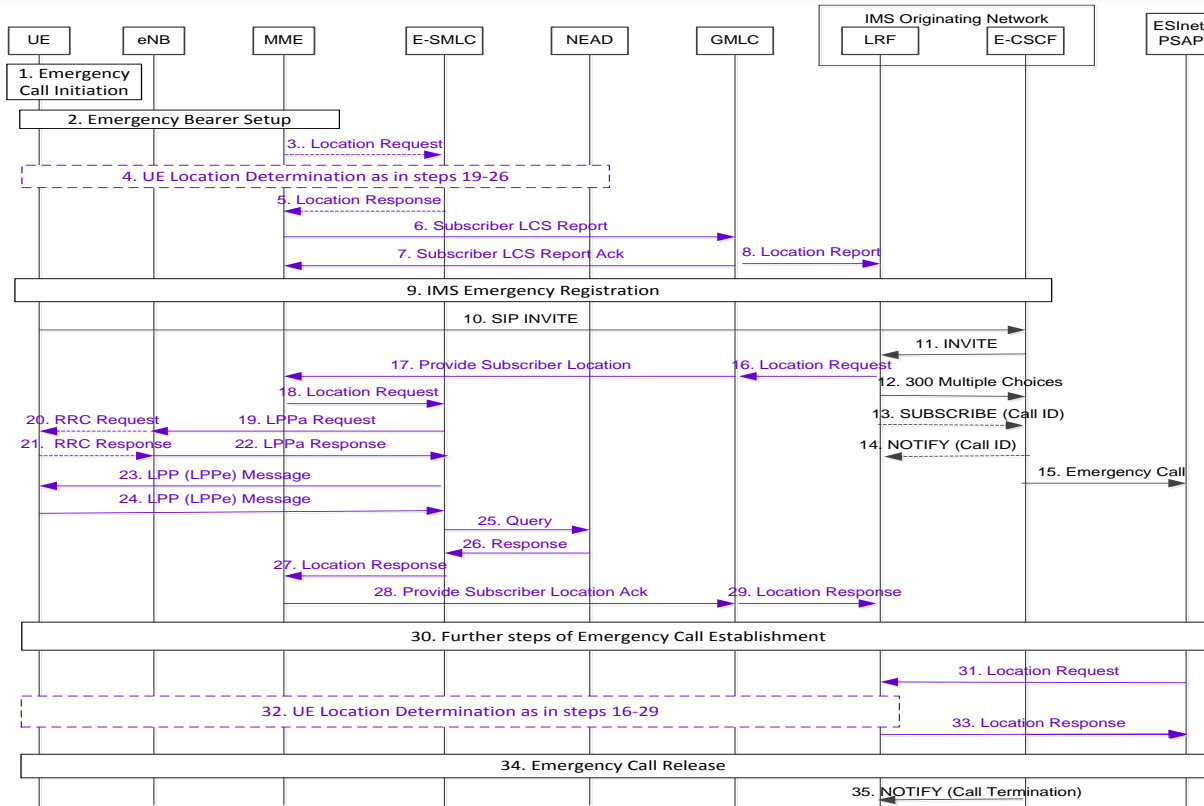


1. e-SMLC/e-SLP queries with the MAC address of the WiFi Access Point or Bluetooth Beacon
 2. NEAD returns:
 1. Validated address and geocoded location OR
 2. Error if MAC address is not provisioned
- (Note: may be as many as 64 queries per call)*

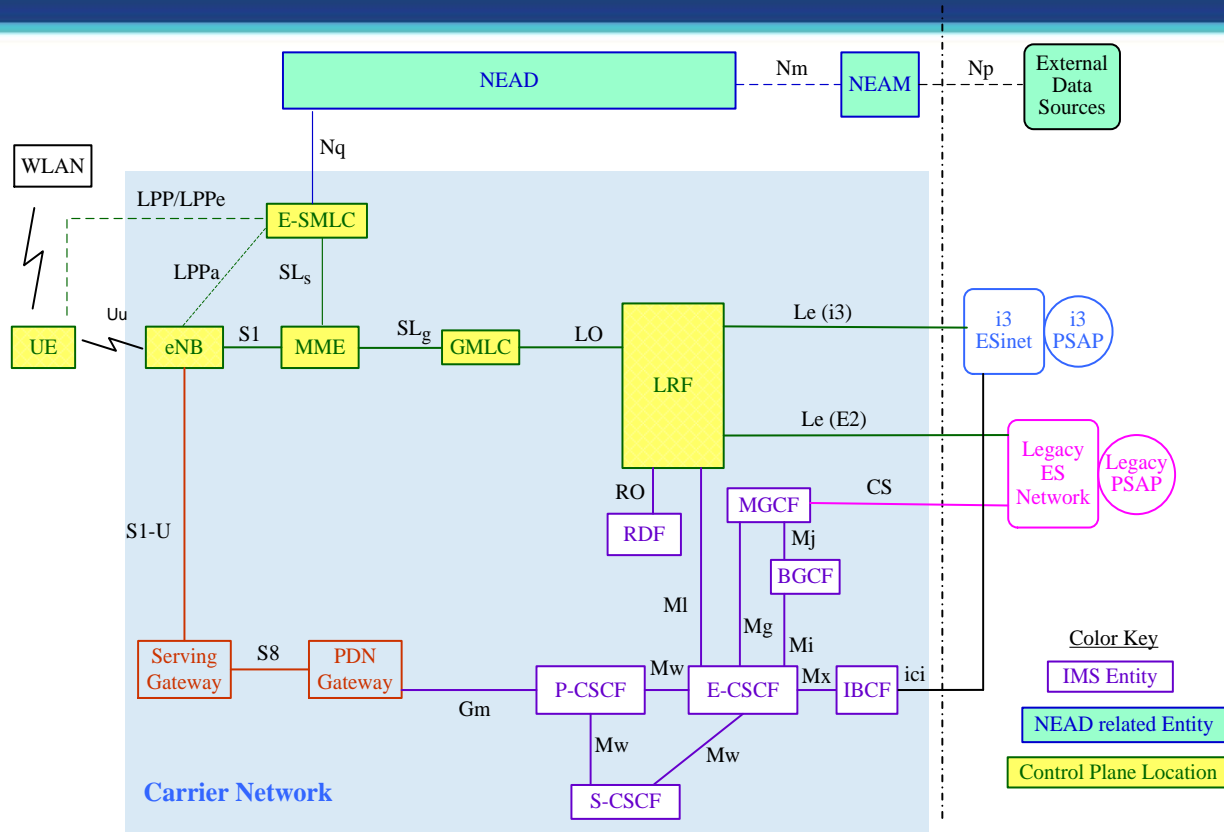
NEAD Architecture for Capacity Analysis



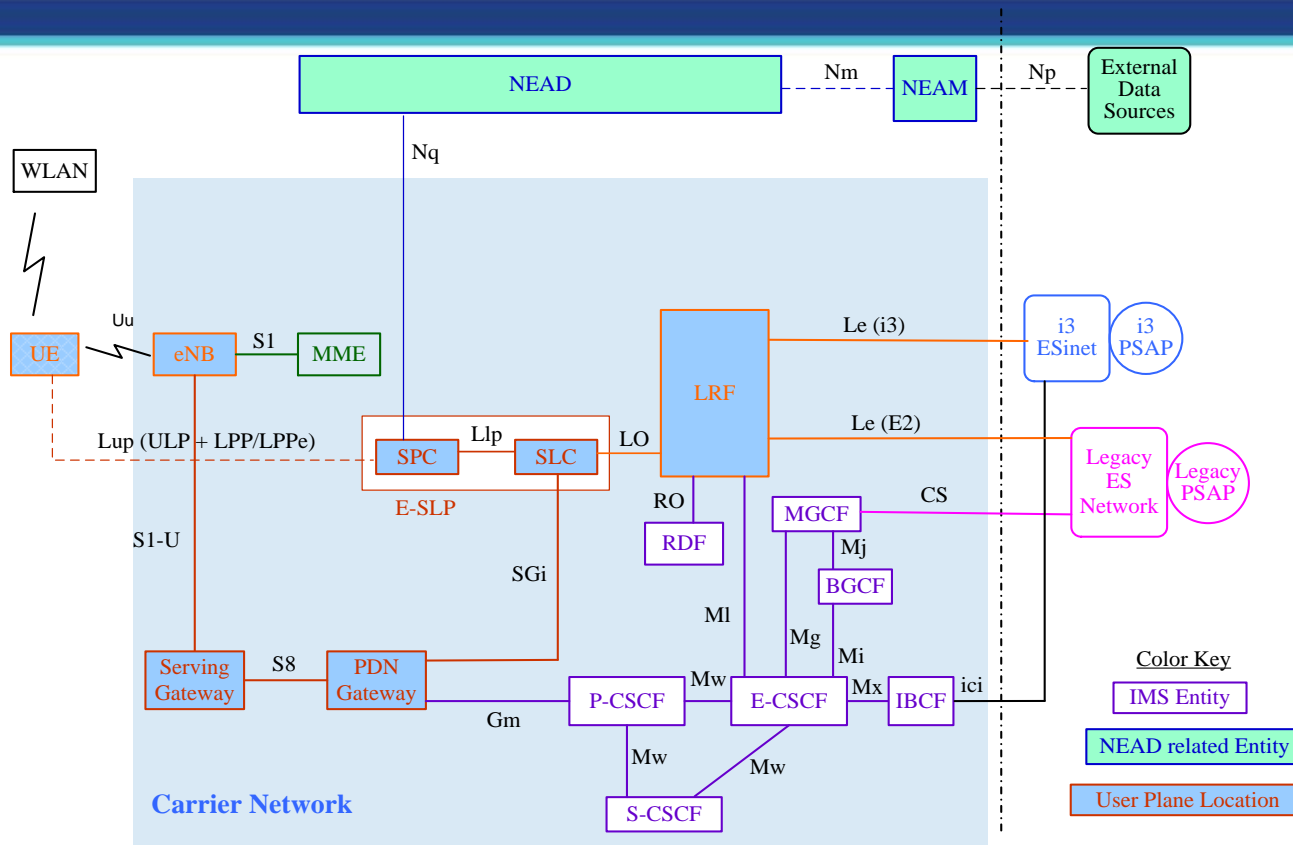
Example end-to-end Call Flow



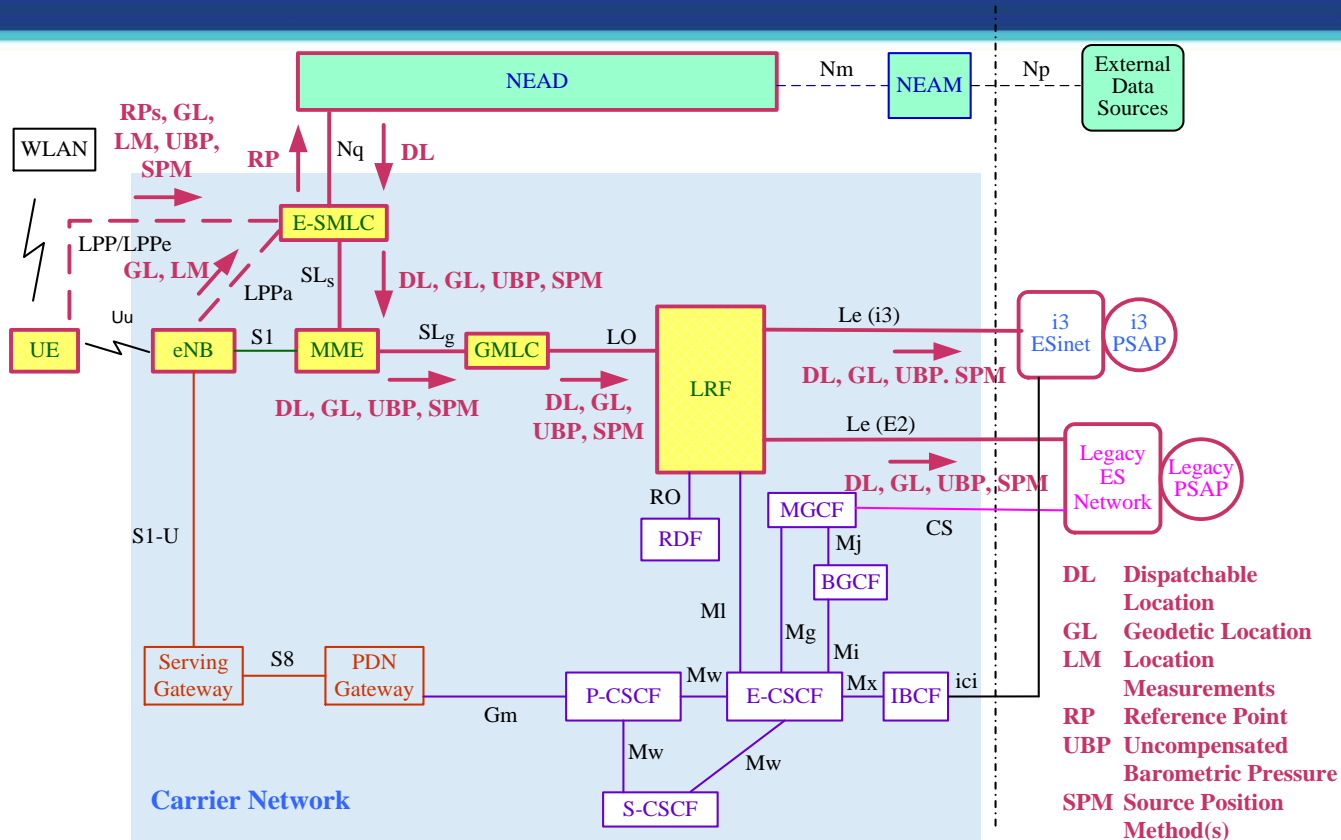
Architecture with LTE Access and Control Plane Location



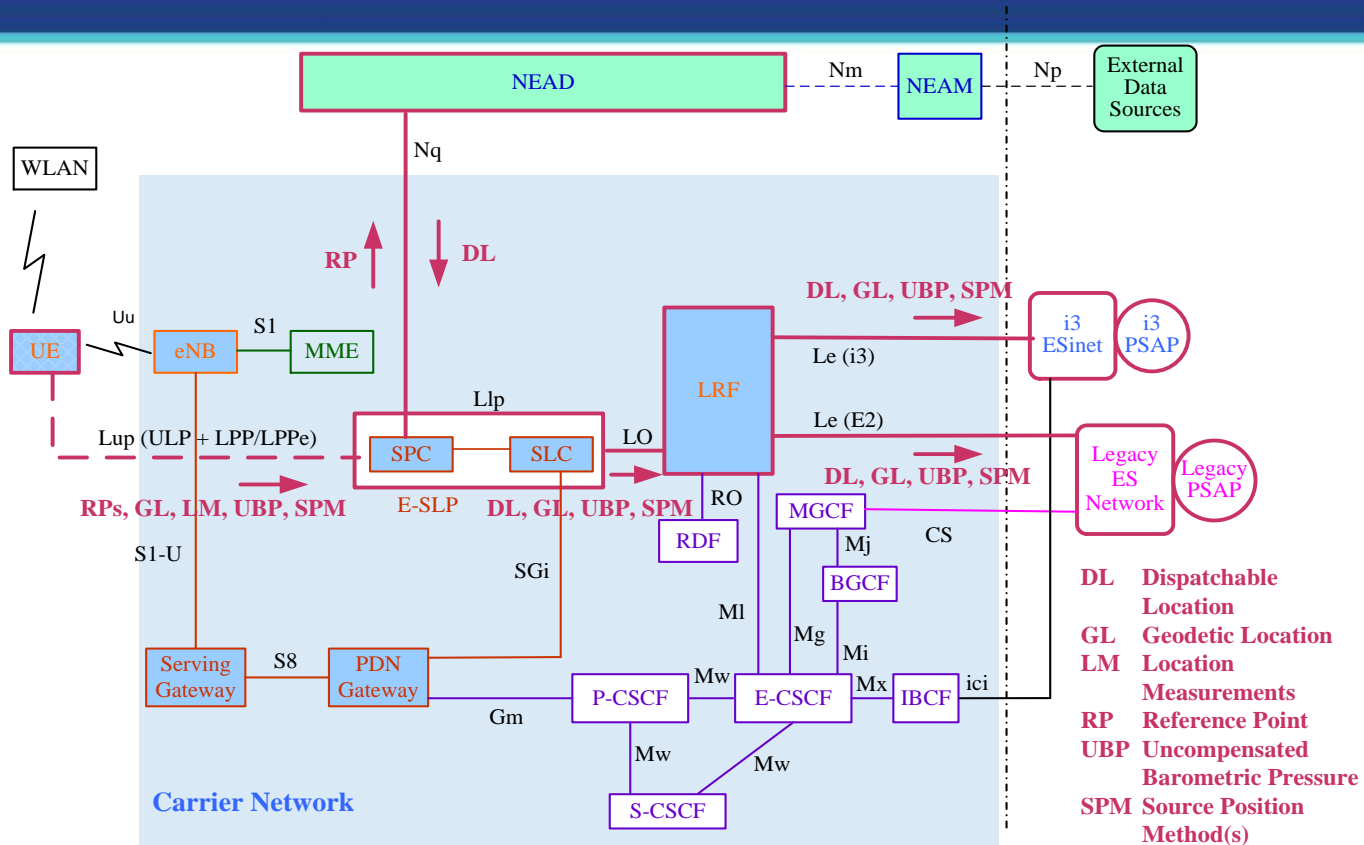
Architecture with LTE Access and User Plane Location



Overview of Acquisition/Conveyance and Control Plane Location



Overview of Acquisition/Conveyance and User Plane Location



Future Standards Development

- Algorithms to determine the best possible location associated with the mobile device
- Enterprise solution
- Additional functionality for the support other technologies

Questions?

Thank You...

christian.militeau@intrado.com