Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network

Prepared by:

Technical Advisory Board for First Responder Interoperability

Final Report

May 22, 2012

Contents

List of Tables

List of Figures

1 Executive Summary

1.1 Introduction

This report fulfills the statutory reporting requirements of the Technical Advisory Board for First Responder Interoperability pursuant to Title VI – "Public Safety Communications and Electromagnetic Spectrum Auctions" of the Middle Class Tax Relief and Job Creation Act of 2012 (Spectrum Act).[1] Pursuant to the Spectrum Act, the Federal Communications Commission (FCC) established the Technical Advisory Board for First Responder Interoperability (Interoperability Board). The duties of the Interoperability Board, in consultation with the NTIA, NIST, and the Office of Emergency Communications of the Department of Homeland Security, are twofold:

(A) Develop recommended minimum technical requirements to ensure a nationwide level of interoperability for the Nationwide Public Safety Broadband Network (NPSBN); and
(B) Submit to the Commission [FCC] for review

In fulfillment of these duties, this report presents recommendations in the following areas:

- 3GPP LTE Standards, Interfaces and Guidelines
- User Equipment and Device Management
- Testing
- Evolution
- Handover and Mobility
- Grade of Service
- Prioritization and Quality of Service
- Security

1.2 Purpose

Across the United States, the public safety community responds to routine and emergency situations at a moment's notice regardless of the severity. These types of situations occur daily in every city and town in the country. The response of the public safety community relies on a communications network. Coordinated response, across agency lines, including multiple disciplines, is necessary to protect the communities and citizens the public safety community is charged to serve. In times of emergency, people look to their public safety officials to act swiftly and correctly, in order to do the things necessary to save lives, help the injured, and restore order. Most disasters will occur without warning. All require a rapid and flawless response. There is no room for error. Whether the event is a fire, natural disaster, vehicular collision, act of terrorism or the apprehension of a suspect, the key piece of that response is the ability to communicate. The communications network spans cities, counties and in some cases state borders. Without reliable and interoperable communications, the safety of our nation's first responders becomes jeopardized and the ability to perform their critical mission is compromised.

Two-Way Voice radio has been the predominant form of communication employed by public safety to date. With the advent of wireless broadband, we are at the beginning of the next major epoch in mission critical communication for first responders. The future wireless broadband network will offer additional data, video and voice services to further improve the effectiveness and safety of first responders. The report of the Interoperability Board specifies the "Minimum Technical Requirements" necessary to achieve a national interoperable broadband network for our nation's first responders. As specified in the Spectrum Act, FirstNet will use these recommendations to help develop and maintain the NPSBN, a goal which can only be met with through extensive and on-going cooperation among States and communities.

This work is critically important to all first responders, and the future FirstNet organization that will develop, implement and manage the network. However, we must also remember that technologies are used by people. That component is the human factor. Whatever the technology, it will have to fit in the hands of those who will use it to protect and serve. It will have to be as simple to use as today's smart phones. It will have to be ruggedized and able

[1] Middle Class Tax Relief and Job Creation Act of 2012, Title VI – Public Safety Communications and Electromagnetic Spectrum Auctions.

to withstand the rigors of public safety use. The applications will need to be reliable and easy to use, whether a first responder is in pursuit of a subject, responding to a medical emergency, directing traffic or reporting to the scene of a disaster. The NPSBN will serve first responders who are part of the “internet generation”. This generation of users grew up with mobile broadband technology; they adapt to it quickly and they understand the enormous capability that it affords. They aren’t as concerned with who builds it as they are with what applications are available. Does it just work? Does it work everywhere? Is it automatic? What is the latest application that will assist me in my job? Will it be as reliable, resilient and predictable in times of emergency as the land mobile radio systems are today? Can I bet my life on it?

The underlying technology is one aspect of achieving interoperability; however, interoperability can only truly be established and preserved over time through vigilant policies, governance, and practices associated with creation, evolution and operation of the network by FirstNet.

1.3 Recommended Requirements Summary

In all cases where these recommendations reference specific 3GPP standards (e.g. 3GPP TS 36.101), the intended meaning is that the standard to be applied is contained in Release 9 of the 3GPP standards, or the future evolved equivalent of that standard that applies to future releases.

1.3.1 3GPP LTE Standards, Interfaces and Guidelines

[1] Hardware and software systems comprising the NPSBN SHALL implement interfaces consistent with Table 2: Standards Implementation Methodology.

[2] Hardware and software systems comprising the NPSBN SHALL support the interfaces enumerated in Table 1: Minimum Interoperable Interfaces.

[3] Hardware and software systems comprising the NPSBN SHALL support management functions.

[4] Hardware and software systems comprising the NPSBN SHALL support APNs defined for PSAN usage.

[5] Hardware and software systems comprising the NPSBN SHALL support nationwide APNs for interoperability.

[6] Hardware and software systems comprising the NPSBN SHALL enable QoS control for PSAN-hosted applications via the 3GPP ‘Rx’ interface.

[7] The NPSBN SHALL support IPv4, IPv6, and IPv4/v6 PDN types defined in 3GPP TS 23.401.

[8] The NPSBN SHALL support IPv4 and/or IPv6 transport for the EPS interfaces enumerated in Table 1: Minimum Interoperable Interfaces, consistent with the FirstNet design.

[9] Any sharing agreement that FirstNet enters into SHALL implement network sharing according to 3GPP TS 23.251 and SHALL NOT impact public safety operations.

[10] The NPSBN SHALL include the capability to collect and convey UE location data to applications using a standardized interface in near real time.

[11] The NPSBN SHALL be capable of providing public safety subscribers with access to the global Internet.

1.3.2 User Equipment and Device Management

[12] All User Devices (UEs) deployed on the NPSBN SHALL conform to the 3GPP Release 9 Uu interface enumerated in Table 1: Minimum Interoperable Interfaces.

[13] All User Devices (UEs) deployed on the NPSBN SHALL conform to the 3GPP TS 36.306 UE Radio Access Capabilities, Release 9.

[14] All User Devices (UEs) SHALL support interworking of the device with the USIM/USAT applications on the UICC in accordance with the relevant 3GPP 31.101, 31.102, and 31.111 standards.

[15] All User Devices (UEs) deployed on the NPSBN that support roaming onto commercial LTE networks SHALL operate on any FirstNet roaming partner network using bands supported by the device.

[16] All UEs SHALL support dual IPv4/IPv6 stacks.

1.3.3 Testing

[17] Prior to IOT and System-Level testing UEs SHALL have already met 3GPP conformance and certification requirements per an independent conformance testing organization (e.g. PTCRB).

[18] Prior to operational deployment on the NPSBN, UEs SHALL have passed FirstNet-required Interoperability Testing (e.g. using a subset of applicable test cases from CTIA IOT and UICC functional test cases, vendor IOT or similar commercial LTE industry practice).

[19] Prior to operational deployment on the NPSBN, UEs SHALL have passed FirstNet-required UICC functional testing.

[20] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet-required Interface Conformance Testing (e.g. testing S1-MME conformance to 3GPP) on the interfaces specified by FirstNet.

[21] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet-required Interoperability Testing at a system level as per the specific IOT requirements for the NPSBN.

[22] Infrastructure deployed on the NPSBN SHALL be included in the FirstNet-required FOA process as part of the NPSBN deployment.

1.3.4 Evolution

[23] The equipment comprising the NPSBN SHALL provide backwards compatibility of interfaces, from time of deprecation, for a minimum of two full major release/upgrades of the network. This requirement may be waived (i.e., interface obsolescence accelerated) if FirstNet can ascertain from the user community that there are no dependencies on a given interface.

1.3.5 Handover and Mobility

[24] The NPSBN SHALL support user mobility across the entire NPSBN (including Opt-out states).

[25] The NPSBN SHALL support S1 and SHALL preferentially support X2 handover between adjacent NPSBN cells (including cells owned by opt-out states) whose proximity supports a handover opportunity.

[26] If roaming between the NPSBN and commercial LTE networks is implemented, the NPSBN SHALL follow GSMA PRD IR.88.

[27] If roaming between the NPSBN and commercial 3GPP 2G/3G networks is implemented, the NPSBN SHALL follow 3GPP TS 23.002 to support roaming into 3GPP 2G/3G networks.

[28] If roaming between the NPSBN and commercial 3GPP2 (eHRPD) networks is implemented, the NPSBN SHALL follow 3GPP 23.402 to support roaming into 3GPP2 (eHRPD) networks.

[29] The NPSBN SHALL support the use of mobile VPN technology to support mobility between the NPSBN and other networks.

1.3.6 Prioritization and Quality of Service

[30] The NPSBN SHALL provide the ability for national, regional, and local applications to dynamically change a UE's prioritization and QoS using the 3GPP 'Rx' interface.

[31] The NPSBN SHALL support all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.

[32] QoS mechanisms in the NPSBN SHALL comply with 3GPP TS 23.203.

[33] The NPSBN SHALL support the usage of all 15 ARP values defined in 3GPP 23.203.

[34] The NPSBN SHALL support the ARP pre-emption capability and vulnerability functions as defined in 3GPP 23.203.

[35] The NPSBN SHALL implement a nationwide scheme for assigning Access Classes to public safety users and secondary users following the 3GPP recommendations in TS 22.011, Section 4.2.

[36] The NPSBN SHALL implement a nationwide scheme for assigning QoS Class Identifier priority to IP network and backhaul priority across the entire NPSBN.

[37] The NPSBN SHALL support the use of industry standard VPN and MVPN technology, while providing priority and Quality of Service for encapsulated applications.

1.3.7 Security

[38] The NPSBN SHALL use a nationwide common security profile for user plane and control plane traffic between UEs, eNBs and MMEs, in accordance with 3GPP LTE Network Access Domain protocols. The profile SHALL be based on 3GPP TS 33.401, and will be determined by FirstNet based on a system design and other considerations as it deals with evolving cyber threats. As a minimum, the profile SHALL include specification of ciphering algorithms (for example, use of AES-128 vs. SNOW 3G).

[39] The nationwide common security profile SHALL include ciphering of control plane traffic in order to provide for interoperable cyber protection of the network. Ciphering of user plane traffic is optional and is based on policy decisions that involve FirstNet and user agencies.

[40] To enable interoperable authentication, the USIM and HSS SHALL be capable of supporting the same key derivation functions, such as Milenage per 3GPP TS 35.205, 35.206.

[41] Network Domain Security SHALL be implemented in accordance with 3GPP TS 33.210, which stipulates the use of IPSec to protect IP communication between administrative domains (including all network connections used to interconnect the domains).

[42] The NPSBN SHALL comply with TS 33.310 as the authentication framework for Public Key Infrastructure to authenticate these network interfaces.

[43] In order to ensure secure and interoperable interfaces between the NPSBN and external elements (e.g. all SGi, Rx and Srvs services as shown in Figure 2), these interfaces SHALL be protected with a FirstNet-approved security mechanism.

[44] User Domain Security SHALL be implemented in accordance with 3GPP TS 33.102, TS 31.101, and TS 22.022.

[45] USIM-based applications that require messaging between the USIM and network components SHALL implement Application Domain Security in accordance with 3GPP TS 33.102 and TS 31.111.

[46] In such cases where visibility is required for devices on the NPSBN, the implementations SHALL comply with 3GPP TS 33.102 and TS 22.101.

1.4 Recommended Considerations Summary

This section contains recommendations for consideration by the FCC and FirstNet as they develop finalized requirements to be included in RFPs. These recommendations for consideration are distinct from the recommended requirements in the previous sections, in that they are not considered by the Interoperability Board to be in scope as described in Section 3.2.

1.4.1 3GPP LTE Standards, Interfaces and Guidelines

(1) Hardware and software systems comprising the NPSBN SHOULD support integration of existing network elements via the necessary commercial standards-defined LTE interfaces enumerated in Table 1: Minimum Interoperable Interfaces.

(2) Billing information from the NPSBN SHOULD be provided to each local and/or regional entity for the NPSBN services.

(3) The NPSBN SHOULD support existing Public Safety applications, deployed regionally or within agencies.

(4) The NPSBN SHOULD provide a method to connect a device to a packet data network where a "home page" application is hosted with location specific content.

(5) The NPSBN SHOULD provide a method where a "home page" application is available via an alternate access network, other than the NPSBN. This is a recommendation that the home page be made available and location-aware while roaming or over Wi-Fi.

(6) The NPSBN SHOULD provide a specification for locating a "home page" based on current or manual location.

(7) The NPSBN SHOULD support use of field-deployed server applications.

(8) The NPSBN SHOULD support devices that are reachable via the global internet and can be used to host field based server applications (i.e. deployable servers).

(9) The NPSBN SHOULD allow the devices outside of their normal jurisdiction to connect to a local packet data network and to the device's home packet data network to carry out incident objectives.

(10) The NPSBN SHOULD provide the ability for users to send and receive Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages.

(11) Voice Sessions SHOULD be handed off within the NPSBN with limited delay and loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature is a future evolution capability.

(12) The NPSBN SHOULD support Voice over LTE (cellular voice) capabilities using GSMA PRD IR.92.

1.4.2 User Equipment and Device Management

(13) The NPSBN SHOULD allow the integration of high power LTE UEs as they become available, based on the methodology contained in Table 2: Standards Implementation Methodology.

(14) User Devices and Device Management solutions SHOULD support remote management capabilities over-the-air, including software update, discovery, device platform configuration, lock, unlock, wipe, and security configuration.

(15) The software systems that comprise the NPSBN SHOULD support the ability to enable local entities to install, update and manage their own applications. This may include security, transport and local APN provisioning.

(16) The software systems that comprise the NPSBN SHOULD provide published and version-controlled subscriber provisioning interfaces to enable end-to-end subscriber provisioning by the local entities. These interfaces SHOULD be verified during interoperability testing.

1.4.3 Testing

(17) Prior to operational deployment on the NPSBN, infrastructure equipment SHOULD have passed FirstNet-required Performance Testing of individual interfaces, nodes and overall system as per the specific performance requirements of the NPSBN.

(18) Nationwide applications on the NPSBN SHOULD have passed FirstNet-required security testing to proper security levels (e.g. Criminal Justice Information Services [CJIS]) to ensure protection of FirstNet and public safety information.

1.4.4 Evolution

(19) The NPSBN SHOULD allow for connection and operation of IP-based LMR voice interoperability gateways using open interfaces as they are developed.

(20) The NPSBN SHOULD be constructed and evolved in adherence to a multi-year roadmap.

(21) Infrastructure equipment procured for the NPSBN SHOULD support backwards compatibility with deployed LTE devices.

(22) Infrastructure equipment in the NPSBN SHOULD be upgradeable to minimally two major 3GPP releases (i.e. n+2, where n is the release available at deployment provided that the equipment does not need to implement a new air interface specification).

(23) Hardware and software systems comprising the NPSBN SHOULD support industry practices for management of standard network interfaces from each supplier. These industry practices include formal publication of interface compliance, deprecation of interfaces, support for backwards compatibility and graceful obsolescence of interfaces.

(24) The NPSBN SHOULD support industry practices for life cycle management of interfaces that it exposes to applications or users of the network to ensure backward compatibility for a reasonable interval, using industry-practice interface deprecation and obsolescence methods. The interfaces include, but may not be limited to: Network messaging Protocols, Application Programming Interfaces, Web-based Interfaces, Protocol/Messaging Interfaces, and User Interfaces such as Command Line Interfaces.

(25) The EPC equipment in the NPSBN SHOULD support optional local and geographic redundancy.

(26) The equipment in the NPSBN SHOULD support transport redundancy wherever economically feasible (i.e. connections to local switching equipment or WAN connectivity between sites or core locations).

1.4.5 Handover and Mobility

(27) If roaming between the NPSBN and commercial LTE networks is implemented, and IMS is implemented in the NPSBN, the NPSBN SHOULD implement support for IMS while roaming into other LTE PLMNs.

1.4.6 Grade of Service

(28) Coverage maps SHOULD be maintained that show pictorially which GoS Tiers are supported over a geographic area. Detailed maps SHOULD be made available to authorized public safety agencies.

(29) NPSBN coverage maps showing planned future coverage SHOULD be maintained. The maps SHOULD show planned coverage at regular intervals (e.g. quarterly) into the future. These maps SHOULD be made available to authorized public safety agencies.

(30) The NPSBN SHOULD use a set of pre-defined GoS Tiers to provide clear and uniform description of the services of network performance provided within a Coverage Area.

(31) The GoS Tiers SHOULD include the minimum set of GoS Attributes defined in Section 4.6.3.

(32) The expected or actual GoS Tier SHOULD be disclosed to authorized public safety agencies in a geographic region.

(33) Each Coverage Area SHOULD be designed to operate with a defined GoS tier.

(34) Service probability SHOULD be specified for each GoS Tier, in order to specify the quality of the user experience provided by the network.

(35) The expected minimum uplink (mobile to network) and downlink (network to mobile) rates of data transmission SHOULD be specified for each GoS Tier. The specifications must also include the protocol layer at which the data rates are to be measured.

(36) The NPSBN SHOULD implement a scheme for engineering RAN boundaries according to a national cell coordination plan.

1.4.7 Prioritization and Quality of Service

(37) A set of default QoS profile templates SHOULD be defined for each responder function (e.g. police, fire, EMS) supported by the NPSBN.

(38) Each QoS profile template SHOULD contain a descriptive definition of the responder function and default values for ARP, Access Class, UE-AMBR, and APN-AMBR.

(39) Since the NPSBN could also support secondary users, default QoS profile templates SHOULD be defined for public safety and secondary users.

(40) Every user of the NPSBN (public safety and secondary users) SHOULD be assigned a default prioritization and QoS profile using the set of pre-defined QoS profile templates.

(41) A process SHOULD be established and followed to manage the assignment of templates to users to ensure template assignment rules are uniformly applied for all users using the NPSBN.

(42) FirstNet SHOULD make an API available to national, regional, and local applications to expose Priority and QoS control.

1.4.8 Security

(43) The NPSBN security implementation SHOULD include pre-planned bypass mechanisms that have defined security and interoperability implications.

(44) Equipment used in the NPSBN SHOULD support AES and SNOW 3G algorithms.

(45) FirstNet SHOULD establish the security controls and policy for inter-domain security and require that all parties (e.g. public safety agencies) who connect to the NPSBN utilize FirstNet-approved cipher suites.

(46) FirstNet SHOULD consider using IPSec interfaces that utilize IKEv2 and utilize PKI to authenticate the peers of the IPSec Security Associations.

(47) When EPS elements are located in trusted locations without wide area communication links between them, the use of network domain security SHOULD be optional.

(48) Network interfaces between domains SHOULD be monitored and intrusion detection/prevention tools

SHOULD be deployed.

(49) The developed security mechanisms SHOULD permit local entities to hide the topologies and address spaces of their networks.

(50) Security mechanisms layered by a jurisdiction on top of the NPSBN SHOULD NOT inhibit interoperability for users visiting from outside of the security domain in which it is implemented.

(51) As FirstNet enters into roaming agreements with commercial partners, security policies SHOULD be implemented that ensure integrity of the NPSBN and that NPSBN security practices are not compromised.

(52) FirstNet SHOULD consider supporting implementation of a national framework for user identity management.

(53) FirstNet SHOULD consider supporting implementation of a national framework for user identity federation to enable user interoperability across administrative domains within the NPSBN, where authorized.

(54) Implementation of the national framework for user identity management and federation SHOULD include a set of guidelines and rules for applications to participate in the national identity management framework.

(55) The agency, organization or entity that utilizes the NPSBN Identity Management framework SHOULD be responsible for enforcing authorization constraints on access to information as per their own security policy.

2 Introduction

2.1 Statutory Framework for Deployment of a Nationwide Interoperable Public Safety Broadband Network

The Spectrum Act established the First Responder Network Authority ("FirstNet") as "an independent authority within [the National Telecommunications and Information Administration (NTIA)]"[2] to "ensure the establishment of a nationwide, interoperable public safety broadband network."[3] FirstNet is also the spectrum licensee for the re-allocated D Block for public safety services and the existing public safety broadband spectrum, collectively referred to as Band 14.[4]

Under the Spectrum Act, the FCC was responsible for selecting the membership of the Technical Advisory Board for First Responder Interoperability (Interoperability Board),[5] which was tasked to develop recommended "minimum technical requirements for interoperability"[6] for the FCC to submit to the FirstNet (with possible revisions). The Interoperability Board will "terminate 15 days after the date on which the Commission transmits the recommendations to the First Responder Network Authority".[7]

FirstNet will then use the minimum technical requirements for interoperability to develop and issue RFPs for the construction and operation of the NPSBN, "without materially changing them." FirstNet has been funded up to $7 Billion from incentive auctions to be deposited in a Network Construction Fund. To pay for operating expenses, FirstNet is authorized to assess user fees and fees associated with leasing network capacity and infrastructure.

The Spectrum Act also provides a process by which a State may choose to "Opt Out" of the planned FirstNet deployment in its jurisdiction and operate its own radio access network. As a component of this process the FCC will evaluate the State's alternative plan using the minimum technical requirements for interoperability as a component of its evaluation. The FCC will determine whether the State's plan or the FirstNet plan will be used for the construction and operation of the radio access network (RAN) network within the State. States that successfully opt out must be interoperable with the NPSBN.

2.2 Technical Advisory Board for First Responder Interoperability

The Spectrum Act required that the FCC Chairman establish the Interoperability Board within 30 days of enactment. The Interoperability Board is required to consist of 15 members, with 14 voting members appointed by the FCC and one non-voting member appointed by the National Telecommunications and Information Agency (NTIA). The Spectrum Act requires the Interoperability Board membership to be made up of 4 representatives of wireless providers; 3 representatives of equipment vendors; 4 representatives of public safety entities; 3 representatives of State and local governments; and one non-voting member appointed by NTIA.

[2] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6204 (a).

[3] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6202 (a).

[4] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6201(a).

[5] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (a).

[6] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c)(1).

[7] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (f).

The FCC issued a Public Notice on February 28, 2012 seeking nominations to the Technical Advisory Board.[8] FCC Chairman Julius Genachowski appointed the fourteen voting members of the Technical Advisory Board for First Responder Interoperability (Interoperability Board) on March 22, 2012.[9] Those selected for membership on the Interoperability Board are identified in Section 2.2.1 below.

The Interoperability Board held its initial meeting on March 23, 2012 to begin developing its structure and processes for accomplishing its legislative mandate.[10] In this meeting the Chairman (Charles L. K. Robinson) and Vice Chairman (Kenneth C. Budka) were elected by the board members and the board established the agenda for its second meeting, which was a face-to-face meeting held on March 26 and 27, 2012.

This second meeting of the Interoperability Board focused on developing a mutual understanding of the general definition of interoperability, the scope of topics necessary to "ensure a nationwide level of interoperability"[11], how the Interoperability Board should structure itself to accomplish this work, and a schedule to meet the statutory deadline for completing the work.[12] After developing consensus around the general elements of the definition of interoperability, the Interoperability Board developed a scope for its work, organized itself into four subcommittees, and selected Chairpersons for each subcommittee.

- Subcommittee 1 focused on Standards, Interfaces, and Guidelines; User Equipment and Device Management; and Network Evolution; (Chair: Paul Steinberg)
- Subcommittee 2 focused on Mobility and Handover; Grade of Service; Prioritization and Quality of Service; (Chair: Kenneth C. Budka)
- Subcommittee 3 focused on Security; (Chair: Brian Shepherd) and
- Subcommittee 4 served as the Drafting Subcommittee (Chair: Dennis Martinez) and was responsible for organizing the content of the Interoperability Board's report.

The Interoperability Board adopted the principle of transparency as a key component of its work and success. This principle guided the board's discussion on how best to engage the public and meet its statutory requirement to consult with the National Telecommunications and Information Agency (NTIA), the National Institute of Standards and Technology (NIST), and the Office of Emergency Communications (OEC) of the Department of Homeland Security[13] - hereafter referred to as "Consulting Agencies". During its March 26th session, the Interoperability Board decided that beginning with its session on March 27th the Consulting Agencies would be allowed to listen in or be present at all open Board meetings. Although the Consulting Agencies could not participate in the board's deliberations, they were able to respond to questions and provide documentation if requested by the board. The board did have several closed sessions for deliberations at which no one except board members were present.

The Interoperability Board was also keenly aware of the interest in, investment in, and commitment to the success of the NPSBN by organizations and individuals outside of the board's membership and the Consulting Agencies. The Interoperability Board took action at its March 26th session to ensure that these organizations and individuals could participate in the development of its recommendations in two ways: the Interoperability Board requested that the FCC open a docket[14] to receive input from interested parties and established a date to conduct a Public

[8] Federal Communications Commission Public Notice DA 12-303.

[9] Federal Communications Commission Public Notice DA 12-455.

[10] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c).

[11] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c)(1)(A).

[12] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c)(1).

[13] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c)(1).

[14] Federal Communications Commission Public Notice DA 12-474

Workshop[15] to seek information from the public on the components of interoperability the board considered within its scope.

While the members of the Interoperability Board were leaders in their organizations and individual areas of expertise, the board quickly realized that they would need the help of subject matter experts (SMEs) - both inside and outside their organizations in order to complete work within the statutory time limit. At its March 27th session, the board developed rules for the engagement of SMEs in its work processes. This engagement proved to be critical to the quality of the board's work and to the overall success of the board.

The Interoperability Board developed a timeline for completing its work, completed the organization of the subcommittees and held the initial meetings of its subcommittees on March 27th. The board closed this second meeting by establishing the preliminary schedule for subcommittee meetings. Over the next three weeks, subcommittees conducted individual conference calls up to three times per week with a goal of having an initial draft of their recommended requirements by April 19, 2012. Many board members participated in subcommittee conference calls outside of their assigned subcommittee, devoting much of their available time to this important work. The Chairman of the Drafting Subcommittee developed a document framework for the board's final report and each subcommittee began developing their recommended requirements according to this framework.

The Interoperability Board conducted its Public Workshop on April 23, 2012. The workshop consisted of four panels with four speakers on each panel. Speakers were selected to provide the board with the broadest perspectives possible on the issue of interoperability within the NPSBN[16]. After the Public Workshop, the board held work sessions on April 23rd and 24th. On April 23rd, subcommittees met to consider the information they had received in the Public Workshop. On April 24th, subcommittees briefed the board on their initial recommended requirements and how the information received at the Public Workshop would impact their work.

On April 23rd, the board decided how to proceed with its statutory consultation requirement with the Consulting Agencies. The board decided to provide the Consulting Agencies with its draft recommendations document on April 27, 2012 and request that the Consulting Agencies provide any suggested changes, comments, and recommendations by May 2, 2012. The board also elected to provide the FCC with the same opportunity. In addition to having the opportunity to provide specific suggested changes, comments and recommendations on the draft document, each of the Consulting Agencies and the FCC were invited to participate in the board's May 2nd conference call to provide a summary and context for their recommendations.

In closing its work session on April 24, 2012, the Interoperability Board decided to no longer meet as subcommittees after April 27th. Subcommittees would work to incorporate the germane information they received during the Public Workshop and provide it to the Drafting Subcommittee Chairman by April 27, 2012. Beginning on April 30th, the Interoperability Board met three days a week to continue refining its recommended requirements through May 14, 2012. The board also set the date for its final work session at the FCC offices on May 16th and 17th.

The May 2nd meeting between the Interoperability Board, the Consulting Agencies and the FCC proved to be invaluable in developing the recommended requirements. The suggested changes, comments and recommendations to the draft document were thoughtful, forward thinking, and focused on the board's statutory responsibilities. The summary and contextual comments provided during the meeting effectively framed their suggestions for the document and provided the board a better understanding of the context of their recommendations.

The Interoperability Board continued to refine its recommended requirements leading up to its work session on May 16 and 17, 2012. As the work continued the defined scope became more precise and the number of requirements began to drop. For example, from Version 1.1 of the board's recommended requirements to Version 1.2, there was a 30% reduction in the number of recommended requirements.

As the Interoperability Board met for its final scheduled work session on May 16th and 17th, its members were confident in the board's ability to meet the target completion date. Though much had been accomplished over the previous 7 weeks, the open issues proved to be the most difficult for the board to resolve. Over these two days the

[15] Federal Communications Commission Public Notice DA 12-538 and 12-617

[16] Federal Communications Commission Public Notice DA 12-617

board continued the process of open collaboration between its members, their SMEs and the Consulting Agencies that had brought it successfully to this final session. In the end these difficult issues were resolved with the same focus and commitment the board had demonstrated throughout its work.

As demonstrated here, the Interoperability Board organized itself quickly, developed an effective execution plan, and diligently worked this plan to meet the statutory mandate. In the process, the board not only included the Consulting Agencies as required by statute, but provided ways for other organizations and individuals to participate. The board's commitment to transparency and seeking the broadest possible input within its constrained schedule has resulted in a set of recommended minimum technical requirements, within the scope of the Spectrum Act, that will "ensure a nationwide level of interoperability".

2.2.1 Interoperability Board Membership

The Interoperability Board was comprised of the following members:

- Bob Azzi, Senior Vice President, Network, Sprint Nextel Corporation
- Todd Bianchi, Firefighter Paramedic, Washington, District of Columbia Fire and EMS Department
- Kenneth C. Budka, Senior Director, Advanced Mission-Critical Communications, Bell Labs Chief Technology Office, Alcatel-Lucent
- Ed Chao, Senior Vice President, Corporate Engineering and Network Operations, MetroPCS Communications, Inc.
- Brenda L. Decker, Chief Information Officer, State of Nebraska
- Colonel Kenneth C. Hughes, Jr., (Ret), Regional Communications Coordinator, New Orleans Urban Area Security Initiative
- Dennis Martinez, Chief Technology Officer, RF Communications Division, Harris Corporation
- Dereck Orr, Program Manager, Public Safety Communications Standards, Office of Law Enforcement Standards, NIST (non-voting member representing NTIA).
- Bill Price, Director Broadband Programs, Department of Management Services Division of Telecommunications, State of Florida
- Steve Proctor, Executive Director, Utah Communications Agency Network
- Charles L. K. Robinson, Director, Business Support Services, City of Charlotte, North Carolina
- Brian Shepherd, Deputy Director, Adams County (Colorado) Communication Center
- Paul Steinberg, Senior Vice President and Chief Technology Officer, Motorola Solutions, Inc.
- Ron Strecker, Chief Executive Officer, Panhandle Telephone Cooperative, Inc., and Panhandle Telecommunications Systems, Inc.
- Diane C. Wesche, Executive Director, Government Network & Technology, Verizon

3 Objective, Scope, and Methodology

3.1 Objective

The adoption of LTE technology will fundamentally change the way first responders communicate. Additionally, the establishment of FirstNet will fundamentally change the ways public safety networks are built, operated and maintained.

Adoption of LTE technology, a technology embraced by commercial service providers worldwide will bring significant benefits to first responders. Adoption of LTE makes the NPSBN part of a multi-billion dollar commercial technology ecosystem, allowing first responders to take advantage of current and future advances in wireless communications technology, wireless devices, applications, networking, security and network infrastructure. Further, adoption of LTE allows public safety to benefit from the exceptionally high level of interoperability achieved on commercial service provider networks.

The high level of interoperability achieved on commercial service provider networks did not happen by accident. One critical factor responsible for the high level of interoperability achieved on commercial service provider networks is the process used by the commercial market to develop and maintain technology standards. The open, consensus-based process adopted by 3GPP, for example, creates a forum which encourages both technological innovation and the maintenance of backward compatibility. This approach has allowed service providers to offer new services while protecting the significant investments they have made in the construction and operations of their networks.

The use of rigorously defined architectures and interfaces in LTE promotes interoperability by giving service providers stable interfaces around which to design their networks. Furthermore, this practice promotes competition, drives innovation and lowers costs among vendors of equipment, user devices, software and services.

One of the most significant factors responsible for the high level of interoperability achieved on commercial service provider networks is the *extensive* testing that is performed to ensure adherence to standards and inter-vendor interoperability.

While public safety communication requirements share a tremendous amount of commonality with the communications requirements of the consumer market, there are notable differences. We expect that many of these requirements can be satisfied with standard interfaces and features supported (or planned to be supported) by LTE. In some cases, FirstNet may opt to implement functionality either not supported by LTE standards or LTE features not in use by commercial service providers. The rewards of such functionality must be carefully weighed against the risks of maintaining interoperability as LTE evolves and the potential high costs incurred through such customization.

Under the Spectrum Act, the Interoperability Board is required to “develop recommended minimum technical requirements to ensure a nationwide level of interoperability for the nationwide public safety broadband network.” The Spectrum Act further requires the Interoperability Board to “base the recommended minimum technical requirements on the commercial standards for Long Term Evolution (LTE) service.”

In developing the minimum technical requirements contained in this document, the Interoperability Board’s objective has been (1) to create in the NPSBN levels of interoperability that mirror the levels of interoperability achieved in commercial service provider networks and (2) to reflect how LTE technology would be used to meet public safety’s unique mission requirements. In doing so, we have been guided by a foundational philosophy: in order for the NPSBN to take advantage of the interoperability achieved by LTE, FirstNet must *fully* embrace the technologies, standards and best practices used by commercial service providers to ensure interoperability on day 1 of network deployment and beyond.

3.2 Scope

The U.S. Department of Homeland Security's SAFECOM program's Interoperability Continuum[17] establishes the critical elements that must be addressed to ensure communications interoperability. These elements include governance, standard operating procedures, technology, training and exercises, and usage of interoperable communications. It is important to note that technology - the focus of the Interoperability Board as mandated by the Spectrum Act - is but one aspect of the work needed to ensure a nationwide level of interoperability for the NPSBN. Furthermore, since LTE is but one of the many technologies that will be deployed in the NPSBN, development of technical requirements for LTE is but part of the work needed to address the technology elements of interoperability.

The U.S. Department of Homeland Security's SAFECOM program defines interoperability as "the ability of emergency response agencies to talk to one another via radio communications systems – to exchange voice and/or data with one another on demand, in real time, when needed and when authorized."[18] SAFECOM's definition of interoperability covers the full spectrum of public safety communications. Because of the Interoperability Board's focus on minimum technical interoperability requirements based on commercial standards for Long Term Evolution (LTE) technology, the Interoperability Board felt it prudent to adopt a definition of interoperability that more appropriately reflected this limited scope.

The success of meeting the goal of a nationwide level of interoperability for the NPSBN will be grounded in the actions taken by the Interoperability Board in setting technical requirements that will allow for the deployment of a network comprised of equipment, services, and applications from a diverse set of companies.

For the purpose of facilitating the Interoperability Board's work under the limitations placed upon it by the Spectrum Act of 2012, we define ***interoperability*** as the ability of all authorized local, state and federal public safety entities and users to operate on the NPSBN and commercial partner networks, to access rapid, reliable and secure communication services, in order to communicate and share information via voice and data. These communications services must support existing and future applications and operate across functional, geographic and jurisdictional boundaries.

We note that the NPSBN will be implemented in phases using equipment from multiple vendors. It is therefore important to ensure interoperability is maintained throughout all deployment phases. As discussed in Section 4.6.4, for example, we note that careful planning is required to ensure seamless service across potential implementation boundaries that may be introduced during the build out of the NPSBN's RAN. Such implementation boundaries, for example, can exist between eNBs provided by different vendors or between RAN segments deployed and managed by states which have decided to exercise the Spectrum Act's opt out provision.

The scope of the Interoperability Board's requirements is limited to minimum requirements necessary to facilitate ***technical interoperability*** in the NPSBN. Technical interoperability is defined as follows:

> ***Technical interoperability is the ability of two or more systems or components, from the same or different manufacturers or service providers, to successfully exchange data and use information based on underlying interface standards.***

It is important to note that this derived scope eliminates governance, operational, policy and procedural practices from our consideration in developing recommended minimum technical requirements. However, in cases where deemed important, the Interoperability Board did include ***Recommended Considerations*** covering subject matter outside of this derived scope.

In finalizing its set of recommended requirements, the Interoperability Board carefully assessed the sometimes competing factors. There were many discussions around the following topics:

- Whether draft requirements could be considered "minimum technical requirements" as mandated by the

[17] See http://www.safecomprogram.gov/SiteCollectionDocuments/Interoperability_Continuum_Brochure_2.pdf

[18] http://www.safecomprogram.gov/about/default.aspx.

Spectrum Act
- Whether draft requirements addressed operability or interoperability
- Whether draft requirements were technical or operational
- Striking a proper balance between granting FirstNet the flexibility it will need to build and maintain the NPSBN while providing the specificity needed to both set a proper course for FirstNet and give the FCC useful tools to determine whether to approve State opt-out plans
- The proper of level of detail to specify requirements in the absence of a nationwide network architecture
- How best to ensure interoperability is maintained as FirstNet and LTE technology evolves

3.3 Methodology

3.3.1 Assumptions

The Interoperability Board made two key assumptions in developing its recommendations:

- The Interoperability Board could not assume any particular network architecture.
- The requirements would use 3GPP LTE Release 9 as the baseline reference point.

The first assumption was made to ensure that the final architecture of the NPSBN was reflective of FirstNet's deployment plans. Accordingly, the board's recommendations reflect the possibility that the NPSBN could consist of either a homogenous or heterogeneous network architecture. The board's assumption of the possibility for a heterogeneous network architecture was based on the Spectrum Act's requirement for FirstNet to leverage interim existing federal, state, tribal, and local infrastructure "to the maximum extent economically desirable".[19]

3.3.2 Public Safety Requirements and LTE Standards

Public safety imposes unique requirements that cannot all be satisfied with LTE standards that are available today. This is represented in Figure 1 below.   An example of such a requirement is Mission Critical Voice, which includes Push to Talk (PTT), off-network operation, and a variety of related functions.

Therefore, as LTE standards continue to evolve, and organizations such as FirstNet participate in the 3GPP standards processes to drive desired capabilities, more of the public safety requirements can be satisfied with products based on these standards.

[19] Middle Class Tax Relief and Job Creation Act of 2012, Title VI, Section 6206, (c)(3).

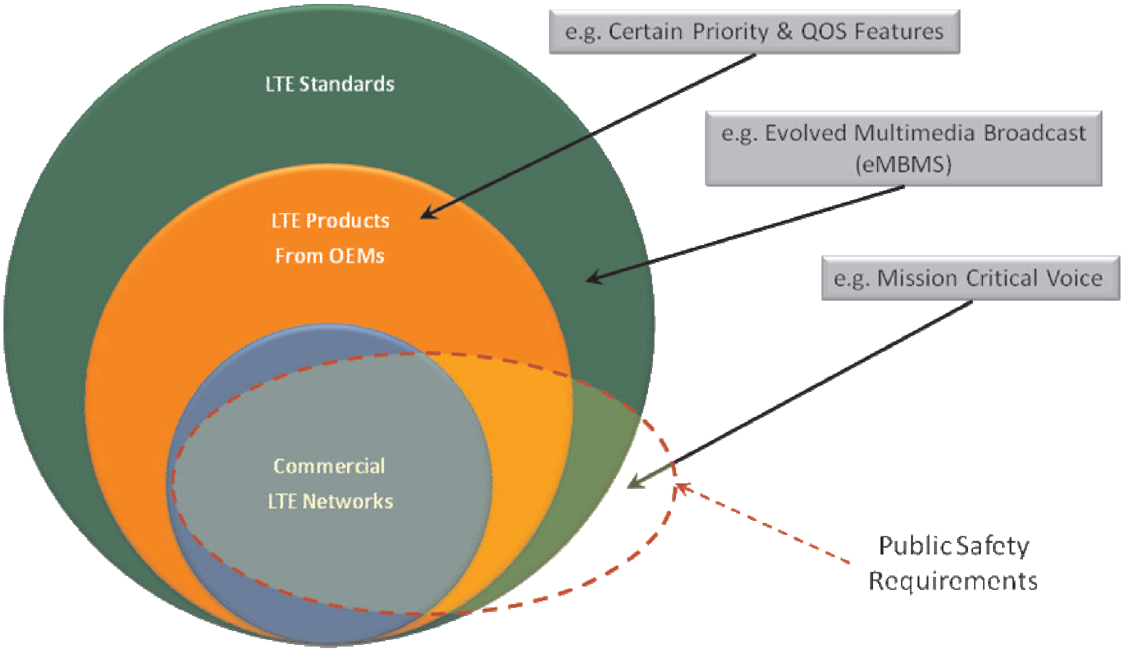

LTE Standards
LTE Products From OEMs
Commercial LTE Networks
e.g. Certain Priority & QOS Features
e.g. Evolved Multimedia Broadcast (eMBMS)
e.g. Mission Critical Voice
Public Safety Requirements

Figure 1: Public Safety Requirements and Standards

3.3.3 Document Structure

Section 4 of this report contains the Interoperability Board's recommendations for minimum technical requirements to ensure a nationwide level of interoperability for the NPSBN. The structure of the recommendations is consistent with common practice for development of technical requirements that are part of an RFP process, with some noteworthy explanations.

Recommended requirements are explicitly noted in the document and use the exclusive verb forms SHALL and SHALL NOT. These are referred to as *Normative* clauses. Recommended requirements are very short, usually single sentences per requirement. Many recommended requirements require a contextual framework to ensure that the requirement is interpreted in an unambiguous way. Therefore the document contains *Informative* language that frames the recommended requirements in their proper context, and therefore *Informative* clauses should accompany the requirements in RFPs.

The document also contains recommendations for consideration that are not phrased as *Normative* clauses. These recommendations for consideration are generally noted explicitly and/or use verb forms such as SHOULD and SHOULD NOT. The Interoperability Board included these types of recommendations to indicate that the subject matter should be addressed by FirstNet as it carries out its duties under the Spectrum Act, but these recommendations fall outside the Interoperability Board's scope, as described in Section 3.2.

4 Recommendations

In this section, the Interoperability Board details its recommended minimum technical requirements to ensure a nationwide level of interoperability. In addition it details recommended considerations that lie outside the scope of these recommended minimum technical requirements. The latter are provided as recommendations that FirstNet should consider as it develops more complete requirements as part of its RFP processes.

In all cases where these recommendations reference specific 3GPP standards (e.g. 3GPP TS 36.101), the intended meaning is that the standard to be applied is contained in Release 9 of the 3GPP standards, or the future evolved equivalent of that standard that applies to future releases.

4.1 3GPP LTE Standards, Interfaces and Guidelines

The Spectrum Act requires the Interoperability Board to develop recommended minimum technical requirements to ensure a nationwide level of interoperability for the NPSBN. The Spectrum Act provides that these recommendations shall be based on the commercial standards for LTE technology. LTE is a common term used to describe a family of global standards that are specified by the Third Generation Partnership Project (3GPP). LTE is an all-Internet Protocol technology platform that is composed of a set of network elements within the 3GPP network architecture. These network elements constitute the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and associated Evolved Packet Core (EPC) and support other network elements. The E-UTRAN and EPC are collectively referred to as the Evolved Packet System (EPS).

3GPP specifications, the LTE specifications in particular, are broad in the scope of functionalities that they address. Only a minimum subset of these specifications are required for the NPSBN to be interoperable nationwide. Specification of a 3GPP standards release does not necessarily guarantee that implementers will build products supporting all the features appearing in the release. Implementing a feature typically requires support across the LTE ecosystem: service providers, chipset manufacturers, user device manufacturers, network infrastructure manufacturers, software developers, etc. Market needs that were anticipated when planning for a release may have changed by the time implementation negotiations begin. As a result, only a subset of the features in each release will typically initially be implemented. Additional features may be phased in at a later stage or may never be developed. This dynamic has important implications for planning the evolution of the NPSBN. Each LTE release provides additional functionality that may be beneficial to public safety. Evolution plans must take into account the features planned for each LTE release as well as what actually gets implemented commercially (and also specific vendor availability). In addition, specific features required by public safety may not be supported by the commercial requirements driving LTE standards. In these cases, either alternative ways must be found to realize the desired functionality or new functionality must be introduced into the 3GPP standards.

Furthermore, there are specifications and guidelines developed by other bodies such as the GSM Association (GSMA) and the Open Mobile Alliance (OMA) that warranted consideration as minimum technical requirements in order to enable the interoperability of the NPSBN. These factors were examined in the process of identifying the minimum technical interoperability requirements for the network, recognizing that interoperability problems can occur if network requirements are ambiguous or not defined with sufficient specificity.

The minimum technical requirements recommended to FirstNet are an input to the RFPs to be issued by FirstNet for vendor bids and contracts. The RFPs issued by nationwide wireless service providers and the resulting contracts typically make extensive use of references to the technical specifications that are developed by bodies such as 3GPP. The Interoperability Board anticipates the same will hold true for FirstNet. Because the minimum technical requirements developed by the Interoperability Board will be used by FirstNet in developing RFPs, the minimum requirements that the Interoperability Board developed include specific reference to 3GPP technical specifications, interfaces, and options within the standard. These specifications, accompanied by a rigorous testing regimen, can ensure that the products from multiple vendors, and the interworking of network elements across multiple jurisdictions by a diverse community of users, are interoperable. Considering a minimum subset of LTE specifications in the RFP process is important to ensure the nationwide interoperability of the NPSBN.

4.1.1 Interoperability Assumptions

The following assumptions are reflected throughout Section 4.1:

1. The NPSBN EPC elements will use a single common PLMN ID for supporting public safety users. If the NPSBN RAN is shared with other EPCs, on a secondary basis, those EPC elements will use one or more PLMN IDs which are different from the NPSBN PLMN ID used for public safety users.
2. The interoperable EPC functions and interfaces are expected to be based on 3GPP Release 9 or later.

Given that technology evolves rapidly, the network components and associated interfaces identified in the present document are also expected to evolve over time. As such, these aspects of the present document are intended to represent a state-of-the-art snapshot at the time of writing. In this context, the standards, functions, and interfaces referenced in the present document are intended to prescribe statements of intent. Variations or substitutions are expected to accommodate technological evolution consistent with the evolution of 3GPP and other applicable standards.

4.1.2 NPSBN Landscape Diagram

The following diagram is a top-level 'landscape' view of the networks associated with the NPSBN. The specific networks which are in-scope of the present document are encapsulated in the dashed box.

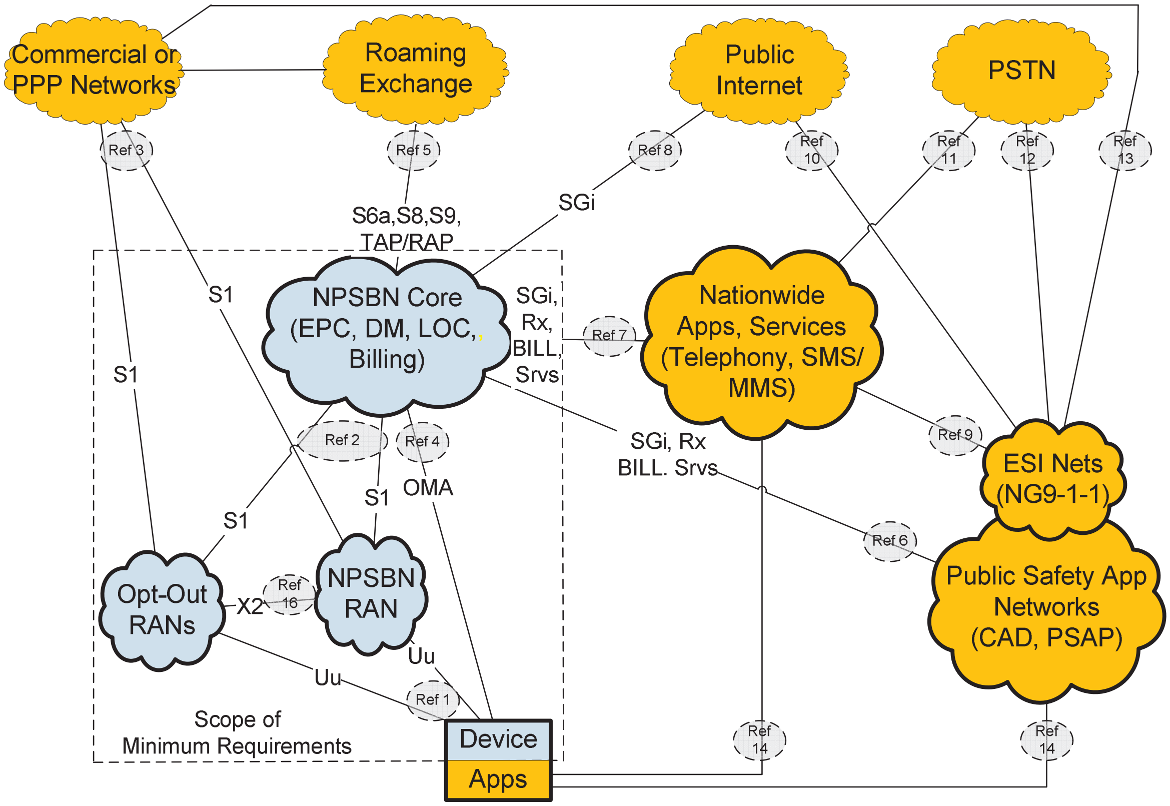


Figure 2: NPSBN Landscape Model

4.1.3 Mapping to 3GPP LTE Reference Architecture

A more detailed view of the LTE interfaces that are contained within the "in-scope" clouds can be represented by stage-2 level standards reference architecture. A detailed view of the EPC and RAN components are shown in the figure below. This figure was adapted from 3GPP 23.401, Section 4.2.

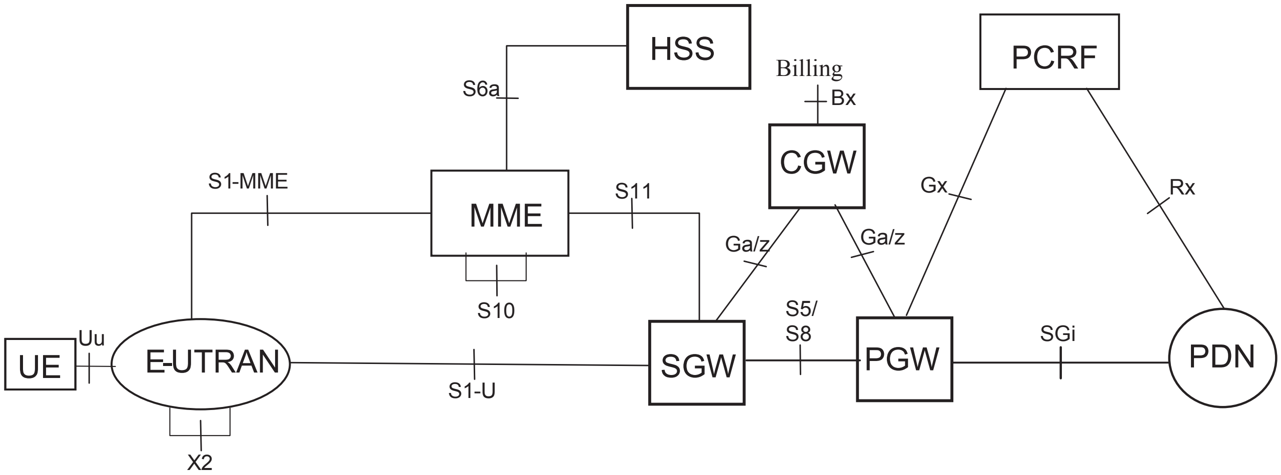


Figure 3: 3GPP LTE Reference Architecture

4.1.4 Existing Infrastructure Integration Scenarios

Spectrum Act section 6206(c)(3) stipulates "Leveraging Existing Infrastructure … the First Responder Network Authority shall enter into agreements to utilize, to the maximum extent economically desirable, existing – (A) commercial or other communications infrastructure; and (B) Federal, State, tribal, or local infrastructure." The Interoperability Board concluded that this stipulation may require the First Responder Network Authority under section 6206(b) Duty and Responsibility to Deploy and Operate a Nationwide Public Safety Broadband Network, to consider leveraging existing infrastructure. In accordance with this conclusion, reference configurations in which existing infrastructure elements (such as the Waiver systems deployed under FCC Order 10-79) deployed prior to the instantiation of the FirstNet Authority can be leveraged into the NPSBN, while meeting the requirements for interoperability, are described herein.[20]

4.1.4.1 Interim Existing Infrastructure Assumptions

1. Existing RAN infrastructure deployed prior to operation of the NPSBN RAN may be integrated with the NPSBN RAN and Core.
2. Existing EPC infrastructure deployed prior to operation of the NPSBN EPC may be integrated into the NPSBN Core.
3. If existing EPC infrastructure elements are integrated into the NPSBN EPC, the existing and NPSBN EPC elements will use a common PLMN ID.

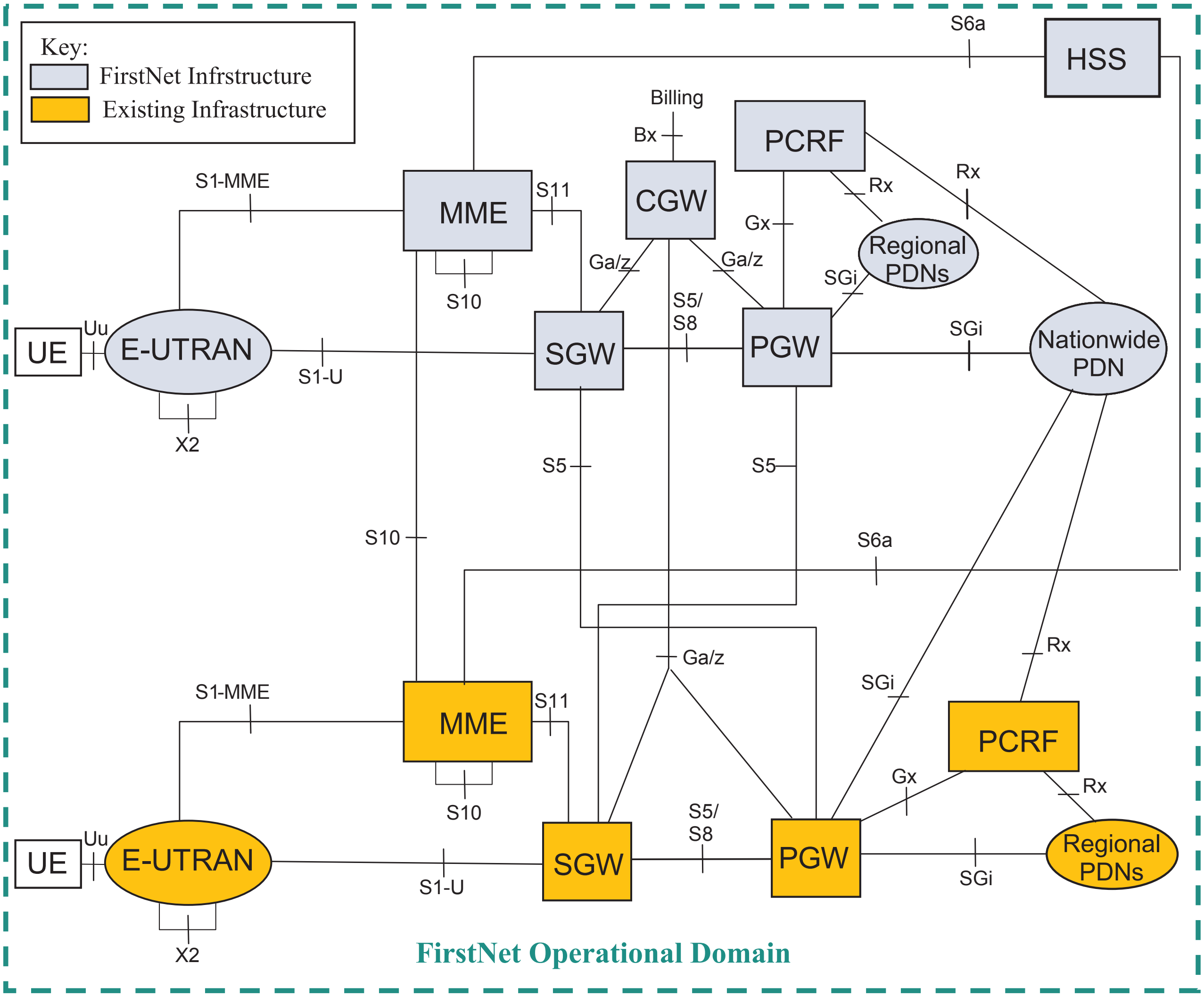
The following diagram is identical to that shown in Figure 2 except for the addition of existing Core and RAN elements. These elements and their associated interfaces are included to provide a broader NPSBN landscape context. Existing Core and RAN infrastructure elements are anticipated to be either assimilated into the NPSBN or deprecated over time. For this reason, the existing Core and RAN infrastructure components are identified separately in this interim context.

Figure 4: NPSBN – Interim Infrastructure Landscape Model

[20] May 2010 FCC Order 10-79.

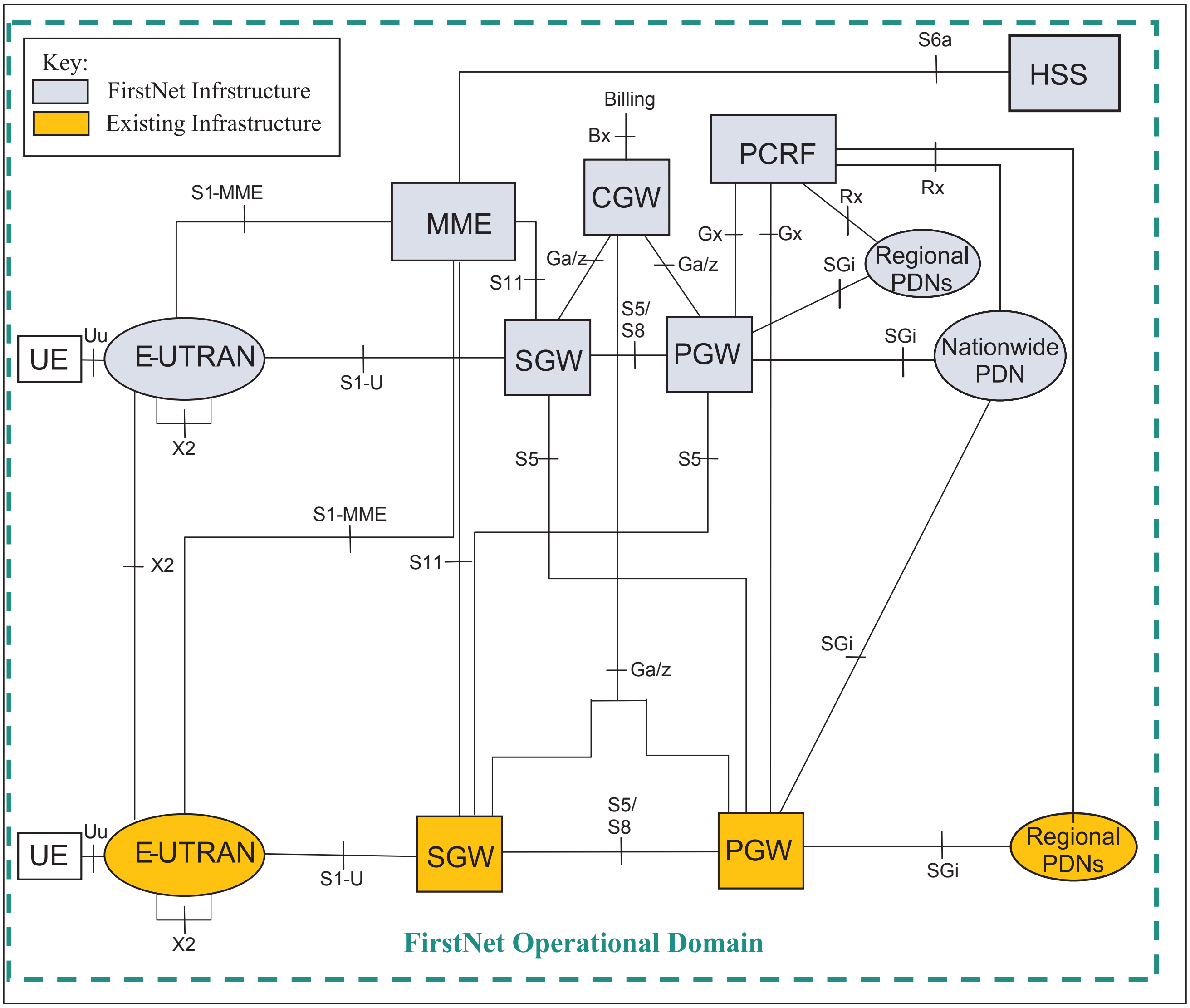
4.1.4.2 Configuration 1 – Leverage User Plane and Signaling Plane Elements of the Existing Infrastructure Networks

In this example, the existing UEs, E-UTRAN (a.k.a, RAN), MME, S-GW, P-GW, PCRF, and Regional Packet Data Networks (PDNs) are integrated into the NPSBN. One logical HSS would exist so the existing HSS's would not be integrated into the NPSBN. The interfaces which extend between the NPSBN elements and the existing infrastructure elements are S5, S6a, S10, SGi, and Rx.



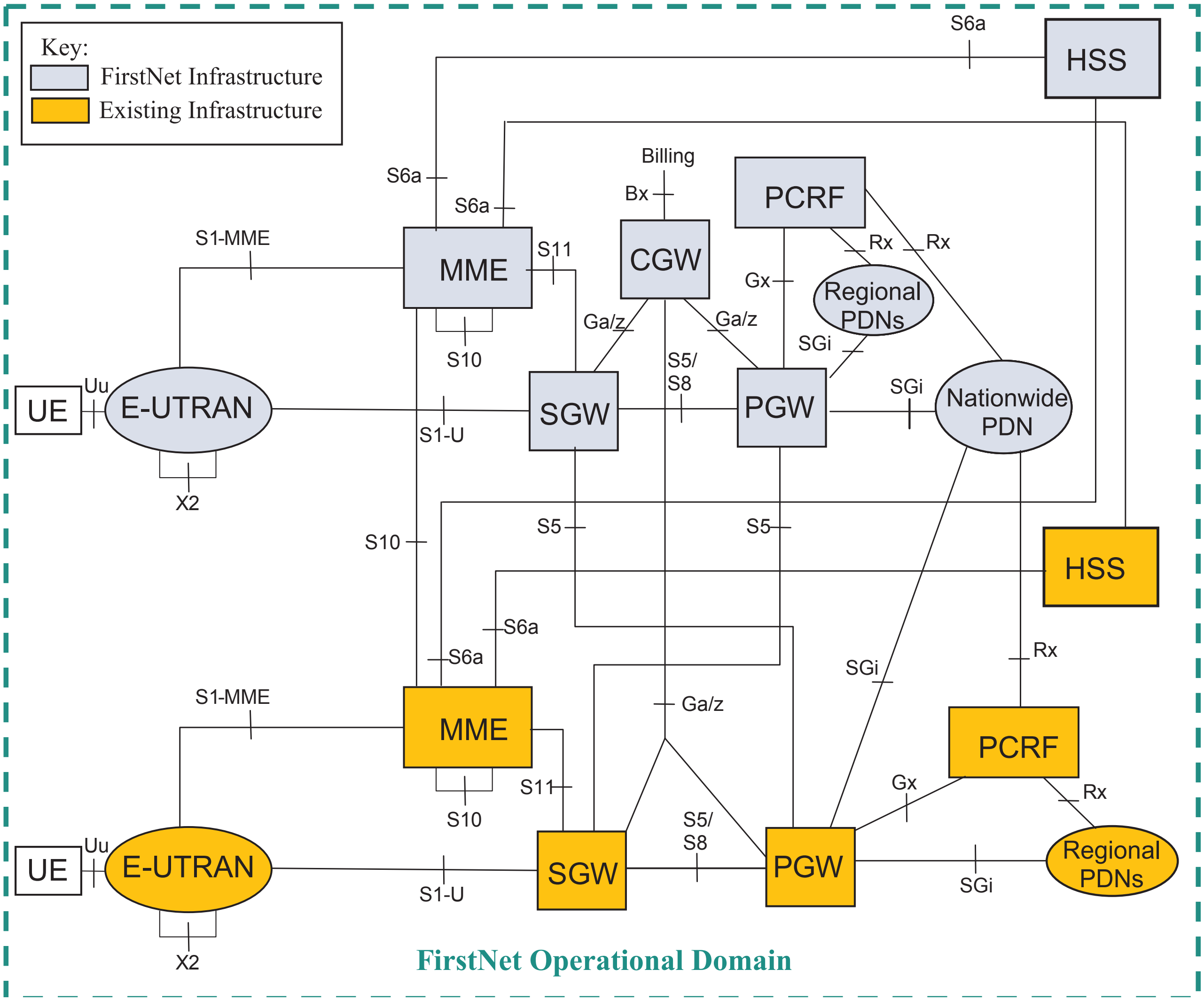
4.1.4.3 Configuration 2 – Leverage User Plane Elements of the Existing Networks

In this example, the existing UEs, E-UTRAN (a.k.a, RAN), S-GW, P-GW, and Regional Packet Data Networks (PDNs) are integrated into the FirstNet-procured NPSBN. Only one logical HSS and one logical PCRF would exist in the NPSBN, however, so these network elements of the existing networks would not be integrated into the NPSBN. The interfaces which extend between the FirstNet elements and the existing infrastructure elements are S1-MME, S5, S11, SGi, and Rx.



4.1.4.4 Configuration 3 – Leverage User Plane, Signaling Plane, and HSS Elements of the Existing Networks

In this example, the existing UEs, E-UTRAN (a.k.a, RAN), MME, S-GW, P-GW, PCRF, HSS, and Regional Packet Data Networks (PDNs) are integrated into the FirstNet NPSBN. Multiple logical HSSs and PCRFs would need to be integrated into the NPSBN. Integrating multiple HSSs into the NPSBN will require support of Diameter Routing Agent functions. Note that these functions would be components of a transport infrastructure and are not illustrated in the diagram. The interfaces which extend between the FirstNet elements and the existing infrastructure elements are S5, S6a, S10, SGi, and Rx.



4.1.4.5 Existing Infrastructure Integration Considerations

Recommended Considerations

(1) Hardware and software systems comprising the NPSBN SHOULD support integration of existing network elements via the necessary commercial standards-defined LTE interfaces enumerated in Table 1: Minimum Interoperable Interfaces.

4.1.5 Interoperable Network Elements

Components depicted in the previous figures are described in the following sections.

4.1.5.1 Device or UE

Spectrum Act section 6206(b)(2)(B) specifies that "… First Responder Network Authority shall … promote competition in the equipment market, including devices for public safety communications, by requiring that equipment for use on the network be - (i) built to open, non-proprietary, commercially available standards; (ii) capable of being used by any public safety entity and by multiple vendors across all public safety broadband networks operating in the 700 MHz band; and (iii) backward-compatible with existing commercial networks to the extent that such capabilities are necessary and technically and economically reasonable;…" Devices are also referred as User Equipment (UE) in 3GPP parlance.

4.1.5.2 NPSBN RAN

Spectrum Act section 6202(b)(2) indicates that the NPSBN RAN comprises "cell site equipment, antennas, and backhaul…that are required to enable wireless communications with devices…". The RAN utilizes Band 14 radio spectrum.

4.1.5.3 Opt-out RAN

Spectrum Act section 6302(e)(2)(B) allows a state to "conduct its own deployment of a radio access network…".

4.1.5.4 Existing RAN

Identified in the present document as RAN equipment which has been deployed under provisions of the FCC Waiver Orders (e.g. May 2010 FCC Order 10-79). The statute is silent on existing RAN infrastructure; however such assets have been deployed and may be considered for integration into the NPSBN.

4.1.5.5 Public Safety Application Network (PSAN)

PSAN's are defined in the present document as State, Regional, Local, Tribal, or Agency application networks which provide public safety services with local scope. Examples of such services are Next Generation Public Safety Answering Points (PSAPs) and Computer Aided Dispatch (CAD). Spectrum Act section 6206(b)(2)(C) directs FirstNet to promote integration of the network with PSAPs.

4.1.5.6 Emergency Services IP Network (ESI Net)

Identified in the NENA i3 architecture as transit networks supporting integration with Public Safety Answering Point (PSAP), ESI Nets are defined in the National Emergency Number Association Interface Standards for Next Generation 9-1-1 (NENA i3). NENA i3 defines an ESI Net as an IP-based inter-network shared by all agencies which may be involved in any emergency.[21] The i3 Public Safety Answering Point (PSAP) is capable of receiving IP-based signaling and media for delivery of emergency calls conformant to the i3 standard.

4.1.5.7 NPSBN Core Network

Spectrum Act section 6202(b)(1) indicates that the NPSBN Core Network comprises the "national and regional data centers, and other equipment … and (B) provides the connectivity between – (i) the radio access network ….

4.1.5.8 Nationwide Public Safety Applications Network (NPSAN)

Spectrum Act section 6202(b)(1) indicates that the NPSBN Core Network (B) provides the connectivity between – (b) the public internet or switched network…". In order to support connectivity to these networks, the FirstNet Applications Network includes Nationwide Applications and Services.

[21] National Emergency Number Association Technical Committee. NENA Functional and Interface Standards for Next Generation 9-1-1. December 2007. Version 1.0 (i3) at http://www.nena.org/?TechnicalStandards.

4.1.5.9 Public Internet

Spectrum Act section 6202(b)(1)(B)(ii) indicates that the NPSBN Core Network may provide connectivity to the public Internet.

4.1.5.10 Public Switched Telephone Network

Spectrum Act section 6202(b)(1)(B)(ii) indicates that the NPSBN Core Network may provide connectivity to the public switched network. The Public Switched Telephone Network (PSTN) is an example of a public switched network.

4.1.5.11 Commercial Networks

Spectrum Act section 6206(c)(5) indicates a FirstNet duty to negotiate and enter into roaming agreements with commercial network providers as appropriate. Spectrum Act section 6211 allows the Commission, if necessary, to adopt rules to improve the ability of public safety networks to roam onto commercial networks.

4.1.5.12 Roaming Exchange Networks

Roaming Exchange Networks are identified in the present document as third party service networks required under provisions of the January 2012 FCC Waiver Order DA 12-25. These networks include Internet Packet Exchange (IPX), Data Clearing House (DCH) and Financial Clearing House (FCH) functions, and are commonly used in the commercial industry to support service provider roaming and therefore relevant to the NPSBN Core Network.

4.1.5.13 NPSBN IMS Network

The NPSBN IMS Network is defined herein to support IMS session layer and telephony applications. The NPSBN IMS Network may be considered to support connectivity to the PSTN, although other alternatives are possible. IMS is a 3GPP standardized technology that is being adopted by service providers and, coupled with VoLTE, would be a reasonable foundation for FirstNet to consider should it decide to introduce voice telephony services and applications into the NPSBN.

4.1.6 Reference Point Descriptions

4.1.6.1 Ref 1 - Reference point between Device and RANs

Ref 1 supports radio connections between Devices and the NPSBN RANs via the 3GPP Uu air interface operating in Band 14. This reference point supports all types of Devices and RANs permissible in the NPSBN.

4.1.6.2 Ref 2 – Reference point between NPSBN Core and RANs

Ref 2 supports the backhaul connections between the NPSBN Core and RANs via the 3GPP S1-U and S1-MME interfaces. The S1-U interface carries User Plane traffic between the eNB and S-GW. The S1-MME interface carries Signaling Plane traffic between eNB and MME.

4.1.6.3 Ref 3 – Reference point between RANs and Commercial/PPP Networks

Ref 3 is similar to Ref 2 in that it supports the backhaul connections and it relies on the same 3GPP interfaces as Ref 2. However Ref 3 supports backhaul for RAN sharing scenarios implied by statute sections 6302(g)(1), which states that "… A State that chooses to build its own radio access network shall not provide commercial service to consumers or offer wholesale leasing capacity of the network within the State except directly through public-private partnerships for construction, maintenance, operation, and improvement of the network within the State." and 6208(a)2(B)(i) which provides for "… access to network capacity on a secondary basis for non-public safety services …"

4.1.6.4 Ref 4 – Reference point between NPSBN Core and Device

Ref 4 supports the Device Management and Device Location services of the NPSBN Core. Device Management functions should minimally include inventory information retrieval, configuration, lock and wipe, and firmware updates. Device configuration should minimally include connection management aspects of LTE (e.g. APNs), application services, and additional access networks (e.g. WLAN). Device Location functions should minimally include secure user plane positioning methods, multiple radio access technologies (e.g. LTE, 3G, WLAN), and roaming support.

4.1.6.5 Ref 5 – Reference point between NPSBN core and IPX, DCH, and FCH service providers

Ref 5 supports roaming with commercial service provider networks and potential Public-Private Partnership (PPP) networks. Typical commercial network practice is to utilize third party service providers to support the roaming functions; however "direct" network-to-network interfaces can be implemented without the use of third party service providers. Roaming functions include User Plane routing, Signaling Plane routing, and Transfer/Return Accounting Procedures. User Plane routing is required for the S8 interface. Signaling Plane routing is required for the S6a and S9 interfaces. The Transfer Accounting Procedure (TAP) and Returned Accounting Procedure (RAP) are required for the GSMA data clearing and financial clearing functions.

4.1.6.6 Ref 6 - Reference point between Public Safety Application Networks (PSANs) and NPSBN Core or Existing Cores

Ref 6 supports public safety applications such as Computer Aided Dispatch (CAD) and Public Safety Answering Point (PSAP) applications using the NPSBN. Reference point 6 is supported by the 3GPP 'Rx' interface, the 3GPP SGi interface, the BILL reference point, and a collection of Service (Srvs) oriented interfaces. The SGi carries User Plane application data traffic between the public safety application servers and the NPSBN/existing Core. Within the User Plane of SGi, users authenticate to applications. In order to ensure interoperable access to applications a common framework to identify users is enabled by using standards-based identity protocols such as Security Assertion Markup Language (SAML). The BILL interface carries formatted charging detail records to enable billing functions to be implemented as part of the application networks. The Srvs is defined in the present document as a collection of miscellaneous interfaces to support NPSBN subscription provisioning and Application Programming Interfaces for applications to request QoS policy and charging control from the NPSBN/existing Core. The Srvs interfaces may be specified by Standards Development Organizations other than 3GPP. The Rx interface enables applications to request QoS policy and charging control from the NPSBN/existing Core.

4.1.6.7 Ref 7 - Reference point between Nationwide Public Safety Application Network (NPSAN) and NPSBN Core or Existing Cores

Ref 7 is similar to Ref 6, except that Ref 7 supports nationwide public safety applications such as Telephony and SMS/MMS applications using the NPSBN. Reference point 7 is supported by the same interfaces as Ref 6.

4.1.6.8 Ref 8 - Reference point between NPSBN Core and Public Internet

Ref 8 supports Public Internet access to/from the NPSBN Core for User Plane connectivity with the NPSBN Devices. This reference point is supported by the 3GPP SGi interface.

4.1.6.9 Ref 9 - Reference point between Nationwide Public Safety Application Network and ESI Net

Ref 9 supports 9-1-1 calls originated by secondary users on the NPSBN to be routed to the ESI Net. The ESI Net completes the call routing to a regional PSAP. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.10 Ref 10 - Reference point between ESI Net and Public Internet

Ref 10 supports incident reports originated from Internet-based applications to be routed to the ESI Net. The ESI Net completes the call routing to a regional PSAP. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.11 Ref 11 - Reference point between NPSBN IMS Network and Public Switched Telephone Network

Ref 11 supports Public Switched Telephone Network (PSTN) access for NPSBN UEs via a nationwide telephony application and an interface between the telephony application and the PSTN. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate potential relationships among networks which are peripheral to the NPSBN.

4.1.6.12 Ref 12 - Reference point between ESI Net and PSTN

Ref 12 supports routing 9-1-1 calls originated from the PSTN to regional PSAPs. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.13 Ref 13 - Reference point between ESI Net and Commercial or PPP networks

Ref 12 supports routing 9-1-1 calls originated from the Commercial or PPP Networks to a regional PSAP via ESI Nets in accordance with the NENA i3 architecture. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.14 Ref 14 – Reference point between Device Applications and Application Managers

Ref 14 supports download, upgrade, configuration, and deprecation of application software residing on Devices via application managers in the Nationwide Public Safety Application network and in the Public Safety Application Networks. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.15 Ref 15 - Reference point between NPSBN Core and Existing Core

Ref 15 supports Device access, mobility, and handover between the NPSBN Core and existing Cores.

4.1.6.16 Ref 16 - Reference point between E-UTRANs

Ref 16 supports inter-eNB handovers. As such, X2 is beneficial only between eNBs that provide adjacent RF coverage. As of 3GPP release 10, the X2 handover procedures are limited to cases where the MME is unchanged during the handover; that is, handover between eNBs which are connected to a common MME. The S1-based handover procedure is used when the X2-based handover cannot be used.

4.1.6.17 Ref 17 - Reference point between NPSBN IMS Network and NPSBN Core or Existing Cores

Ref 17 supports IMS session and telephony services for the NPSBN Core and Existing Cores. Ref point 17 is supported by the Cx, Gm, Mb, Rx, and Sh, interfaces. The Cx interface provides support for storage/retrieval of IMS-related subscription and routing information stored in the HSS. The Gm interface provides support for SIP-related signaling with the UE. The Mb interface provides support for bearer traffic between the UE and IMS applications. The Rx interface enables IMS applications to request QoS policy and charging control from the NPSBN or Existing Core. The Sh interface provides for storage/retrieval of IMS application-specific information stored in the HSS.

4.1.7 Minimum Required Interoperable Interfaces and Standards

The table below enumerates minimum interoperable interfaces and standards associated with the NPSBN. Note that the standards referenced herein are relevant at the time of this writing. These standards are required to be supported as long as they are relevant to the NPSBN. However, it is recognized that standards evolve over time and hence it is expected that the standards enumerated in this table may be deprecated and/or replaced in the future.

Table 1: Minimum Interoperable Interfaces

Interface Name	Description	Required Standards
Uu	Air Interface between Device (aka, UE) and eNB.	3GPP TS 36.101, 36.104, 36.133, 36.141, 36.201, 36.211, 36.212, 36.213, 36.214, 36.314, 36.321, 36.322, 36.323, 36.331
S1	Comprised of two interfaces: S1-U user plane between eNB and S-GW; S1-MME signaling plane between eNB and MME, UE and MME.	3GPP TS 23.122, 24.301, 36.410, 36.411, 36.412, 36.413, 36.414, 33.210, 33.310
S6a	Signaling plane interface between MME and HSS.	3GPP TS 29.272
S5/S8	User plane interface between S-GW and P-GW.	3GPP TS 29.274, 29.281
S9	Signaling plane interface between PCRF in home network and PCRF in visited network.	3GPP TS 29.215
S10	Signaling plane interface between MMEs.	3GPP TS 29.274
S11	Signaling plane interface between MME and S-GW.	3GPP TS 29.274
SGi	User plane interface between P-GW and external IP networks.	3GPP TS 29.061
Gx	Signaling plane interface between PCRF and P-GW.	3GPP TS 29.212, 29.213
Rx	Signaling plane interface between PCRF and external Application Functions.	3GPP TS 29.214
X2	User plane and Signaling plane interface between eNBs.	3GPP TS 36.420, 36.421, 36.422, 36.423, 36.424

4.1.8 Recommended Requirements for Interface Interoperability

LTE interfaces evolve over time. Therefore in developing recommendations based on these evolving interfaces, it is important to give precedence to standardized LTE interfaces that are deployed in commercial practice over those that are earlier in the evolution process. Furthermore, as FirstNet designs and deploys the NPSBN, the Interoperability Board recognizes the possibility that required functions and interfaces that don’t exist within available LTE standards will arise. To that end, in developing its recommendations, the Interoperability Board includes the following methodology that prescribes precedence ordering for selection of standards and interface specifications for use in the NPSBN. The intent of this precedence ordering is that succeeding steps are only executed when reasonable options do not exist with preceding steps.

Table 2: Standards Implementation Methodology

Step 1.	Implementation based on open, consensus-based, non-proprietary, commercially available standards, commonly used by commercial service providers
Step 2.	Implementation based on open, consensus-based, non-proprietary, commercially available standards established for use by commercial service providers
Step 3.	Implementation based on the development and adoption of open, consensus-based, non-proprietary, commercially available standards within recognized standards setting organizations, through direct participation in these standards-setting activities by FirstNet
Step 4.	FirstNet may implement a solution based on open specifications available to all authorized parties

[1] Hardware and software systems comprising the NPSBN SHALL implement interfaces consistent with Table 2: Standards Implementation Methodology.
[2] Hardware and software systems comprising the NPSBN SHALL support the interfaces enumerated in Table 1: Minimum Interoperable Interfaces.
[3] Hardware and software systems comprising the NPSBN SHALL support management functions.
[4] Hardware and software systems comprising the NPSBN SHALL support APNs defined for PSAN usage.
[5] Hardware and software systems comprising the NPSBN SHALL support nationwide APNs for interoperability.
[6] Hardware and software systems comprising the NPSBN SHALL enable QoS control for PSAN-hosted applications via the 3GPP ‘Rx’ interface.
[7] The NPSBN SHALL support IPv4, IPv6, and IPv4/v6 PDN types defined in 3GPP TS 23.401.
[8] The NPSBN SHALL support IPv4 and/or IPv6 transport for the EPS interfaces enumerated in Table 1: Minimum Interoperable Interfaces, consistent with the FirstNet design.
[9] Any sharing agreement that FirstNet enters into SHALL implement network sharing according to 3GPP TS 23.251 and SHALL NOT impact public safety operations.

4.1.9 NPSBN Services Offered to Applications

The NPSBN would benefit from implementing a set of common nationwide network services which can be accessed by applications and used in a standard and interoperable manner. Examples of such services are Billing, Short Message Service (SMS) messaging, Location, Presence, and Device Management. These services are typically not directly visible to end-users, but rather made available to end-user applications or administrative-user applications.

In the commercial service provider environment, these services are typically based on standards; however, each network service provider tends to select unique standard options that best fits its needs. As a result, there are multiple standards-based options to realize such services. For this reason, there are multiple ‘state-of-the-art’ practices that could be leveraged by the NPSBN. This situation will require FirstNet to select specific standards-based options to implement these services. After specific options are selected, these services can be deployed while maintaining interoperability within the NPSBN context. While not universal among service providers at this writing, IMS offers a useful standards framework for FirstNet to consider for implementation of these services.

4.1.9.1 Billing Capability

The ability to receive billing information from the NPSBN will be essential to the success of the network. Public Safety has unique charging scenarios (jurisdictional charging, investment credits, mutual aid, regional users, etc.), and each local entity and/or regional entity typically sets its own policies for these charging scenarios.

Consolidated public safety systems (referred to in this section as regional entities) will need the ability to efficiently and accurately identify charges to the appropriate “cost causer” and receive the appropriate data that will enable the “rebilling” of charges. It is important that FirstNet agree to publish billing records directly to local entities (format TBD, but potentially TAP3 or CDRs) for all charges that will be passed on to these local/regional entities. It is important that this function be performed in the most economical way possible, without additional “per transaction” costs.

Billing becomes a technical requirement because of the way most consolidated/regional systems are funded. For example, in the majority of state governments across the country, the IT organizations are established under a charge-back-for-services model. The agencies receive little or no funding from their respective Legislature, and sustainability of the services offered is accomplished through a fee for service. IT organizations purchase or create services at discounted pricing and “re-sell” these services to their customer base at a price that covers their cost of providing the service. Rates for services must comply not only with individual state laws, but with Federal OMB Circular A-87 rules and regulations. These regulations assure that neither the state nor the federal government customers pay more than their “fair share” of the charges. Therefore it is extremely important that these types of organizations can identify the appropriate entity/person to re-bill. Currently, all state government IT organizations are billing clients for network services that include data (broadband), voice and video. Additionally, several of these same entities currently re-bill services for their state land mobile radio services.

The unique charging scenarios for public safety are mostly ignored by service-provider-focused billing vendors. In fact, the current emphasis by commercial service-provider-focused billing vendors on real-time billing, used today primarily to enforce usage limits, is mostly unhelpful to public safety.

The ability of local/regional entities to work with FirstNet to ensure billing is provided to meet their unique environment will ensure that they can produce one integrated invoice per-user or per-agency for their public safety LTE and other local Entity services.

Recommended Considerations

(2) Billing information from the NPSBN SHOULD be provided to each local and/or regional entity for the NPSBN services.

4.1.9.2 Location Based Data Capability

Location data should be accessible to appropriate applications and only the appropriate end users, as may be authorized by management level policy. Location data applications may be on both UE’s and associated agency level command/control applications. UEs of future public safety networks should meet the same minimum location data information requirements (format and accuracy) as is applicable on commercial services networks in order to retain a broad level of compatibility with incumbent systems.

The LTE standards support several methods of locating devices using GPS or network assisted calculation methods. Use of a network assisted location service does not need to be limited to just working over LTE and can additionally report location using 3G or Wi-Fi access. If additional location coverage is desired beyond GPS, network assisted location will need to be part of an evolution plan for the network services layer.

There are several methods to implement the signaling of location information between the UE and the network. The two methods generally implemented are control plane solutions based on 3GPP TS 23.271 or a user plane solution based on OMA (Open Mobile Alliance) Secure User Plane Location (SUPL). The user plane solution is referenced from 23.271 but the details are covered in OMA specifications. A service provider typically chooses a single method to deploy in their network.

Recommended Requirements

[10] The NPSBN SHALL include the capability to collect and convey UE location data to applications using a standardized interface in near real time.

4.1.10 Network Applications

4.1.10.1 Recommended Minimum Requirements

A number of the applications specified by the National Public Safety Telecommunications Council (NPSTC) Broadband Task Force indicated below can be supported with best-effort IP data access – a service that will be available on all initial and subsequent LTE network deployments. In the commercial world, such applications are known as “Over the Top Applications”, referring to their ability to run on top of a best-effort IP data service without requiring additional integration effort at the network transport layers. Data applications currently used by public safety agencies that run over commercial service provider networks, for example, operate as “Over the Top Applications.” These applications can be readily migrated to the public safety wireless broadband network, leveraging existing applications, procedures, processes and expertise. All Over the Top Applications can be further enhanced through the use of priority services, services that require the exchange of signaling messages between the LTE network and application to allow the application to request a specific priority treatment. The use of Over the Top applications will have an impact on network capacity requirements and perhaps other aspects of the LTE network as it evolves. LTE is further anticipated to greatly increase mobile video usage within the public safety workflow. Enhanced support for this and other applications through the introduction of QoS, priority services or other supplemental security services that are required by public safety must be considered as part of the network evolution plan.

Recommended Considerations

(3) The NPSBN SHOULD support existing Public Safety applications, deployed regionally or within agencies.

4.1.10.1.1 Internet Access

The NPSTC Broadband Task Force report recommends that support of internet access be required on all LTE networks deployed. This access can come directly or via access to a home network with internet connectivity. Many of the home network services are only available on the agency private network and would better be served with private connectivity to the agency. Private connectivity allows for priority/QoS to be applied. Connectivity through the internet normally implies best effort only.

Recommended Requirements

[11] The NPSBN SHALL be capable of providing public safety subscribers with access to the global Internet.

4.1.10.1.2 Information “Home page”

The NPSBN may be required to provide public safety a universal method to obtain a "home page" for visitors to the system. This "home page" will facilitate access to and distribution of available applications, alerts, incident specific information, system status information, and information that the service provider deems important to share with visitors to the system.

Recommended Considerations

(4) The NPSBN SHOULD provide a method to connect a device to a packet data network where a “home page” application is hosted with location specific content.
(5) The NPSBN SHOULD provide a method where a “home page” application is available via an alternate access network, other than the NPSBN. This is a recommendation that the home page be made available and location-aware while roaming or over Wi-Fi.
(6) The NPSBN SHOULD provide a specification for locating a “home page” based on current or manual location.

4.1.10.1.3 Field-Based Server Applications

Recommended Considerations

Public safety users have the need for client devices to consistently and continuously reach server-based applications that may be hosted in jurisdictional networks or accessible via the global internet. Field-based server applications include, for example, Computer-aided Dispatch (CAD) and Records Management Systems (RMS).

(7) The NPSBN SHOULD support use of field-deployed server applications.
(8) The NPSBN SHOULD support devices that are reachable via the global internet and can be used to host field based server applications (i.e. deployable servers).

4.1.10.1.4 Access to Responders under Incident Command System (ICS)

Recommended Considerations

(9) The NPSBN SHOULD allow the devices outside of their normal jurisdiction to connect to a local packet data network and to the device's home packet data network to carry out incident objectives.

4.1.10.1.5 Status/Information "SMS-MMS Messaging"

Recommended Considerations

(10) The NPSBN SHOULD provide the ability for users to send and receive Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages.

4.1.10.1.6 PSTN Voice

PSTN Voice refers to the ability of the NPSBN to support telephony services; both mobile-to-mobile and mobile-to-land. Because LTE is a packet-only technology, some form of additional voice-over-IP technology is necessary to support telephony services. While not required by the Spectrum Act, it is envisioned that the NPSBN will support telephony services at some point in the future. Commercial service provider support for telephony services over LTE is anticipated in the near future. However, as of this writing, commercial service providers in the U.S. have not commercially deployed an LTE telephony solution, and thus it is not prudent to require FirstNet to advance ahead of commercial service provider deployments with this technology.

In addition, there may be several public safety specific issues which need to be resolved in order to provide PSTN voice service via the NPSBN. Examples of these issues are:

- Precedence of a 911 call vs. a first responder PTT emergency call
- End-to-end signaling confidentiality to avoid exposing responder-specific information
- Session continuity when roaming to avoid dropped calls
- Pre-emption of secondary users during congestion (including 911 and CALEA calls)
- Selective logging of calls for evidentiary purposes
- NAT traversal across various network segments (including Opt-Out) in the NPSBN

One application that warrants special attention when roaming is Voice over LTE (VoLTE). VoLTE can be used in the NPSBN to provide cellular type telephony services similar to voice services provided today in commercial mobile networks. Support of telephony voice services on the NPSBN has been called out in a number of practioner-driven requirements efforts, including NPSTC's Broadband Statement of Requirements.[22] Note VoLTE is distinct from the PTT/MCV application additionally required by public safety. VoLTE is an IMS application as defined by 3GPP TS 22.173 and follows the "IMS profile for voice and SMS" as defined in GSMA IR.92. When roaming from the NPSBN to commercial LTE networks, a roaming user should be able to establish calls as long as the roaming LTE network provides support for VoLTE. Note, if a user leaves the NPSBN while on a VoLTE call, the call will drop, requiring the user to re-establish the call on the roaming network. The initial application of VoLTE on the NPSBN will therefore be less functional than the application of VoLTE in a commercial network

[22] NPSTC, Public Safety 700MHz Broadband Statement of Requirements – Version 0.6, November 8th, 2007.

where a service provider can leverage techniques such as Single Radio Voice Call Continuity (SRVCC) to hand over to other radio technologies. Consequently deployment of VoLTE may need to wait for a region to have significant NPSBN coverage. Also, the new network may not have the bandwidth available to continue previous services such as video sessions with the same QoS. Additionally the NPSBN may need to support E911 calling for secondary users of the NPSBN, including support for location, and possibly CALEA.

If roaming to non-LTE commercial networks the user device will require the support of the appropriate voice solution used in the specific network it is roaming onto in order to make cellular type telephony calls.

Recommended Considerations

(11) Voice Sessions SHOULD be handed off within the NPSBN with limited delay and loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature is a future evolution capability.

(12) The NPSBN SHOULD support Voice over LTE (cellular voice) capabilities using GSMA PRD IR.92.

4.1.11 Additional Recommended Reference Points and Standards

The table below enumerates additional interoperable reference points and standards which are recommended to be implemented within the NPSBN. These reference points are not part of the recommended minimal technical requirements because they are either emerging at the time of this writing or have not been widely adopted in the industry. When available, these interfaces should be implemented with open, consensus-based, non-proprietary, and commercially available standards.

Table 3: Reference Points and Standards

Ref Name	Description	Recommended Standards
OMA	Collection of Device related service interfaces supporting Location (LOC) services, and Device Management (DM) services.	Device Management services should comply with the following OMA-DM requirements and Enabler Test Specifications (ETS): • Basic protocol v1.2, Acc, DevInfo, DevDetail as specified in OMA-RD-DM-V1_2-20070209-A (requirements) OMA-ETS-DM-V1_2-20110128-C (enabler test spec). • Firmware Update Management Object (FUMO) as specified in OMA-RD-DM-V1_2-20070209-A (requirements) OMA-ETS-FUMO-V1_0-20101125-C (enabler test spec). • Lock and Wipe Management Object (LAWMO) as specified in OMA-RD-LAWMO-V1_0-20080610-C (requirements) It should be noted that LAWMO is an emerging specification and does not yet have an associated Enabler Test specification which has been approved for release. However, this should be adopted if/when such specification becomes available in the future. • Connection Management Object (ConnMO) as specified in OMA-RD-ConnMO-V1_0-20081024-A (requirements). It should be noted that although ConnMO has been approved for release, it is comprised of a large number of optional sub-components and it does not have an associated Enabler Test specification defined. FirstNet should develop certification spec that details the required ConnMO object instances. Location Services should comply with the following 3GPP and OMA location specifications: • 3GPP TS 36.355 (LTE positioning protocol) • Secure User Plane Location protocol as specified in OMA-RD-SUPL-V3_0 (requirements) OMA-AD-SUPL-V3 (architecture)

		OMA-ERELD-SUPL-V3_0 (enablers) OMA-TS-ULP-V3_0 (user plane protocol) • Mobile Location Protocol services as specified in OMA-RD-MLS-V1_3 (requirements) OMA-AD-MLS-V1_3 (architecture) OMA-ERELD-MLP-V3_1 (enablers) OMA-LIF-MLP-V3_3 (mobile location protocol) OMA-TS-LPPe-V1_1 (LPP extensions)
Srvs	Server Side QoS Interfaces for LTE Aware Applications	Applications that require/desire specific bearer QoS or priority should use the Rx interface. API services for Web-based applications should comply with the emerging open, consensus-based, non-proprietary, commercially available standards.
	Server Side QoS Interfaces for Over the Top Applications	These applications are outside the scope of this document, and can continue to use the interfaces used today.
	Subscriber Provisioning services	Subscriber Provisioning enables subscriptions to be added, modified, or deleted from subscription databases within the NPSBN/existing Cores. Subscriber Provisioning includes provisioning portals which enable agencies to manage subscriptions for their users. These capabilities are not supported by commercial standards. Therefore, NPSBN-specific interfaces will be required to support this functionality.
	Identity Management and Identity Federation	Public Safety applications should utilize a standardized framework for user identity management based on the Security Assertion Markup Language (SAML). SAML identity federation profiles enable users to strongly authenticate to applications and then based on application policies users can be authorized to appropriate levels of access within the application. The SAML v2.0 is recommended and associated specifications are located at http://docs.oasis-open.org/security/saml/v2.0. The core SAML specification is Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005, located at http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
TAP/ RAP	Transferred Accounting Procedure / Returned Accounting Procedure	GSMA BA.12 – Transferred Account Procedure and Billing Information GSMA BA.13 - Returned Account Procedure GSMA TD.57 - Transferred Account Procedure Data Record Format Specification Version Number 3
BILL	Accounting and Charging Data Records	The accounting and charging data record interface is specified in 3GPP TS 32.297 and 32.298.
IMS	Collection of interfaces supporting the IMS Session and Telephony services.	The IMS interfaces Cx, Gm, Mb, and Sh are specified in 3GPP TS 23.228

4.2 User Equipment and Device Management

Interoperability in the areas of user equipment and device management is important to the success of the NPSBN. The ability to use devices across the different types of broadband networks (e.g. NPSBN and Commercial Roaming Partner networks) is critical for ubiquitous first responder broadband capabilities. The ability to procure mobile broadband devices from a variety of sources will yield significant cost, functional, and performance benefits. The ability to remotely manage devices over-the-air will simplify operations related to devices.

4.2.1 User Equipment

4.2.1.1 Standards

3GPP provides extensive standards relevant for LTE devices and necessary for interoperability over reference point 1 (see Section 4.1.6.1).

Recommended Requirements

[12] All User Devices (UEs) deployed on the NPSBN SHALL conform to the 3GPP Release 9 Uu interface enumerated in Table 1: Minimum Interoperable Interfaces.

[13] All User Devices (UEs) deployed on the NPSBN SHALL conform to the 3GPP TS 36.306 UE Radio Access Capabilities, Release 9.

4.2.1.2 USIM/UICC

In the network architecture of 3GPP, user equipment devices, or user equipment (UE), consist of at least two physically separate elements. The first element is a physically secure element—an Integrated Circuit card, or smart card, called the Universal Integrated Circuit Card (UICC)—that hosts authentication applications, such as the Universal Subscriber Identity Module (USIM), used for accessing services provided by the mobile network. The second element is Mobile Equipment (ME), which includes the radio interface and other mobile network access functions.

FirstNet should leverage existing UICC IOT standards as described by 3GPP PCS Type Certification Review Board (PTCRB) and add specific test cases to enable any specific baseline standardization for the USIM/USAT applications that run on any UICC that will be installed in a public safety device. This will enable public safety entities to source their own UICC (SIM cards) independently and thus will avoid the creation of single source (monopoly) and any perceived bottlenecks for UICC availability. Such a process will also allow the market forces to drive the cost of UICC while making sure that UICC elements have been completely tested to work in commercial service provider networks and the NPSBN.

Recommended Requirements

[14] All User Devices (UEs) SHALL support interworking of the device with the USIM/USAT applications on the UICC in accordance with the relevant 3GPP 31.101, 31.102, and 31.111 standards.

4.2.1.3 Roaming

FirstNet subscribers should be able to obtain service on commercial LTE and 2G/3G networks. FirstNet should establish interoperability requirements related to band class support and network selection for selected classes of UEs. For example, FirstNet might specify handheld User Devices should support Public Safety LTE, one or more Commercial LTE band, and either 3GPP or 3GPP2 bands. These requirements should be verified during Device Certification as defined in Section 4.3.2.

FirstNet should ensure that its devices enable FirstNet to enter roaming agreements and public-private partnership arrangements with any commercial service provider and allow FirstNet users to obtain service in those commercial networks. A device that is capable of obtaining such service in certain bands shall operate on all FirstNet roaming partner networks operating in those bands and not be locked to a subset of FirstNet roaming partner networks operating in those bands.

Recommended Requirements

[15] All User Devices (UEs) deployed on the NPSBN that support roaming onto commercial LTE networks SHALL operate on any FirstNet roaming partner network using bands supported by the device.

4.2.1.4 Public Safety Specific Device Performance

Section 4.6 outlines the Grade of Service required for public safety, including coverage areas for the NPSBN. In order to meet the necessary grade of service, public safety entities may require devices with higher than typical transmit power (e.g. vehicular modems) to expand coverage and minimize the required number of eNBs. This can also have an impact on Grade of Service for low power UEs.

The need to support a mixture of high and low power mobile broadband devices creates unique coverage, capacity, and interference scenarios for the NPSBN. These issues are unique to public safety broadband and not typically experienced in a commercial service provider LTE deployment, thus requiring special consideration by the FirstNet.

Recommended Considerations

(13) The NPSBN SHOULD allow the integration of high power LTE UEs as they become available, based on the methodology contained in Table 2: Standards Implementation Methodology.

4.2.1.5 Future Readiness

It is widely accepted that migration to IPv6 is inevitable for the NPSBN.

Recommended Requirements

[16] All UEs SHALL support dual IPv4/IPv6 stacks.

4.2.2 Device Management

4.2.2.1 Overview

The ability to remotely manage devices over-the-air will simplify operations related to devices. Commercial LTE service providers use a variety of commercially available, standards-based solutions for device management. FirstNet should follow this service provider model.

It has not been determined how device platform management and device application management responsibilities will be divided between FirstNet and the public safety entities. The possible divisions of responsibility include:

- All DM capability is performed by FirstNet, including device platform management and device application management.
- All DM capability is performed by the public safety entities, including device platform management and device application management.
- DM capabilities are divided between FirstNet and the public safety entity. For example, the NPSBN might be responsible for managing a device platform and set of national applications, while the public safety entity is responsible for managing a set of local applications.

The division of responsibility between the public safety entity and FirstNet as well as the specificity of standards prescribed is still to be determined. The DM solution should provide the necessary interoperability to support the three device management models outlined above.

4.2.2.2 Standards

Recommended Considerations

(14) User Devices and Device Management solutions SHOULD support remote management capabilities over-the-air, including software update, discovery, device platform configuration, lock, unlock, wipe, and security configuration.

4.2.2.3 Application Management

As stated in the overview, no determination has been made regarding the divisions of responsibilities between the FirstNet and the local entities for managing applications in devices served by the NPSBN. In order to ensure an interoperable application management capability between the NPSBN and the local entities, FirstNet should define and verify the mechanisms that enable application management by the local entity. Issues that require definition include security requirements, transport requirements, and the method for binding applications to local APNs.

Recommended Considerations

(15) The software systems that comprise the NPSBN SHOULD support the ability to enable local entities to install, update and manage their own applications. This may include security, transport and local APN provisioning.

4.2.3 Subscriber Provisioning

Subscriber management is a critical function of any service provider and is especially important in the NPSBN, where rapid and reliable provisioning of the network and first responder devices is a fundamental capability. While subscriber management is generally considered an operations issue, the subscriber provisioning task must function across the NPSBN and local entity domains and hence impacts interoperability.

It has not been determined how subscriber provisioning will be performed in the NPSBN. FirstNet must provide a mechanism for local entities to independently add and manage subscribers. Independent subscriber management by local entities requires a point of interoperability between the NPSBN and the local entities. It is imperative that the NPSBN includes an interoperable subscriber provisioning function in order to guarantee timely and reliable addition, modification and deletion of subscribers to the NPSBN by the local entities.

To facilitate external provisioning capabilities, a subscriber provisioning interface should be published and version controlled by FirstNet. This enables end to end provisioning regardless of the divisions of responsibilities between FirstNet and the local entity when provisioning subscribers. These interfaces must be verified during interoperability testing.

Recommended Considerations

(16) The software systems that comprise the NPSBN SHOULD provide published and version-controlled subscriber provisioning interfaces to enable end-to-end subscriber provisioning by the local entities. These interfaces SHOULD be verified during interoperability testing.

4.3 Testing

4.3.1 Testing Overview

FirstNet will be deploying a new technology (LTE) with multiple vendors supplying equipment into the "network". Within the network, it is necessary that many elements connect with one another, and each one of these connections must meet a minimum set of specifications to ensure it can interwork with all others. Within the high level 3GPP diagram illustrated in Figure 3 there may be multiple vendors supplying the user equipment (UE), the operating system (OS) on the UE, applications that run on the OS on the UE, eNB antenna electrical down-tilt controllers, EPCs, etc., all the way to the application servers and everything in between. The ability to provide quantitative data for FirstNet for each of these interconnections among network interfaces should be determined by a specific and thorough test regimen that ensures not only interoperability but also operability of the network.

This of course doesn't assume that every piece of equipment deployed in the network itself has been tested. Instead, it is expected that a representative model of equipment has been tested and passed in a controlled environment under predetermined test conditions, before other models of the same type can be deployed in the network.

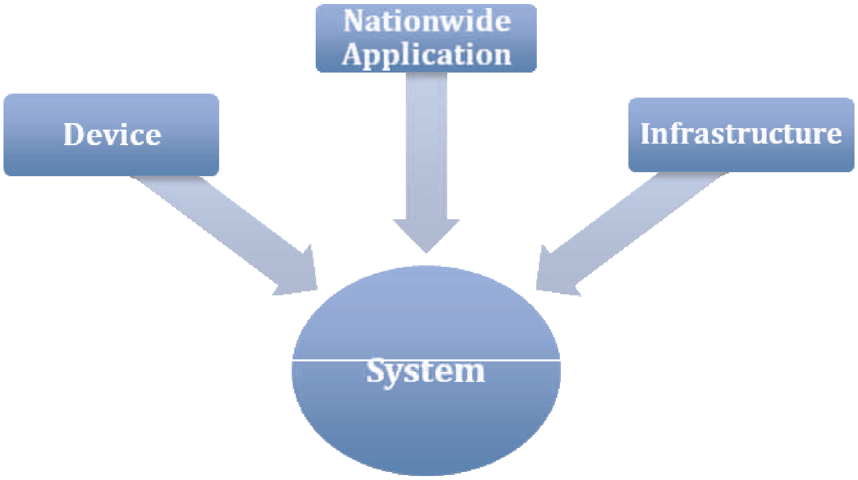


Figure 5: Testing Regimen

Testing can be partitioned into different categories. The entire LTE network or system level tests comprise three main sub-categories of testing: 1) Infrastructure; 2) Devices; and 3) Nationwide Applications. To be able to perform end-to-end system-level tests, each one of the primary subsystems within the network needs to be tested at multiple stages. In order to maximize cost savings, the NPSBN should leverage testing conducted by vendors and existing commercial certification processes.

It should also be recognized that testing is an ongoing activity and not a "once and done" event. Software updates, bug fixes, new feature releases and introductions, standards updates, new vendors, and many other factors require continual testing to ensure network operability and interoperability. Figure 6 below depicts this testing lifecycle.

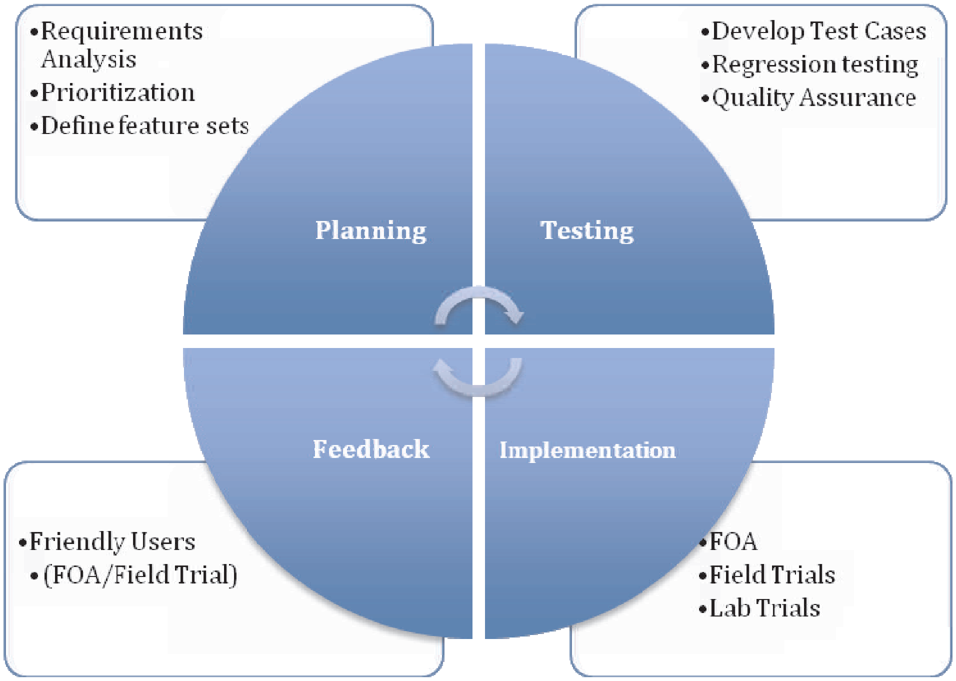


Figure 6: Testing Life Cycle

4.3.2 Device Testing

Commercial network service providers perform several different types of tests on devices they are deploying to ensure that they provide operability within their network and interoperate with their roaming partners, which potentially are operating on different frequencies and/or radio access technologies (RAT). To avoid unnecessary overhead and adversely impacting device availability and/or device interoperability with commercial networks, FirstNet should align with the existing certification processes used by the commercial LTE community. FirstNet should avoid creating a parallel process duplicating already existing test activities and should seek to complement these activities only where and if required.

There are several steps involved in device interoperability and testing in the commercial LTE device eco-system: GCF/PTCRB, Device IOT, regulatory certifications (e.g. FCC part 90), infrastructure vendor IOT and service provider field verification. The service provider does not typically handle the first three steps, but the service provider is presented with the results of the testing. The field verification is service provider specific. A subset of test cases, based on the NPSBN device profile, is used to validate the service provider specific situations. FirstNet should define the NPSBN-specific test scenarios and consider the following testing areas for all devices allowed on the network.

4.3.2.1 Device Conformance Tests

Conformance testing that utilizes independent test organizations such as GCF or the PTCRB should be the first level of testing required. The conformance testing currently evaluates the Device Under Test (DUT) against a validated test platform. These tests evaluate RF, Radio Resource Management, and Protocol Signaling conformance to the 3GPP standard. Additionally, other tests can be added at the request of FirstNet, however, these additions should be minimal as not to require extra cost and time. These types of tests could be additional RF interference testing, or any physical layer test FirstNet may require.

The partners FirstNet utilizes may require optional testing for other networks such as EVDO or HSPA. These tests should be at the discretion of FirstNet.

4.3.2.2 Device Interoperability Tests

Interoperability between a specific device and multiple infrastructure vendors also must be tested before devices are deployed in a mixed-vendor network. FirstNet should adopt a similar process leveraging interoperability tests performed by vendors and industry associations such as the CTIA LTE IOT Program (CPWG110615-1). Being developed by the CTIA Certification Program Working Group, the LTE IOT Program would be appropriate to consider. This would assure FirstNet that a newly introduced device from a device vendor will interoperate on all of its chosen infrastructure vendors and its commercial roaming partners' networks. Additional tests for multiple users, inter-LTE (other bands) and inter-RAT could also be part of this testing.

4.3.2.3 Device System Tests

Once conformance and interoperability testing is completed, another set of testing is performed before approving a device on the network for operation. The following is an example of the testing that commercial service providers perform on their devices as part of their certification process. Before launching a new device or allowing it to access the network, FirstNet could adopt a similar certification process based on NPBSN defined device testing requirements. It is recommended these testing requirements be included in addition to full lab conformance testing:

- Safe-For-Network Test Plan
- Field Test Plan
- Common Services Test Plan (e.g. SMS, VoLTE, PTT)
- Data Retry Test Plan

4.3.2.4 Device Ancillary Function Tests

Additional device tests could be performed to test the ancillary functions within the device. Other radio access technologies may be implemented within a FirstNet device. If the device utilizes these technologies it is suggested that they are tested. Below is an example list of device ancillary features and their respective testing or test organization:

- Bluetooth - Bluetooth Qualification Requirements[23], established by the Bluetooth Special Interest Group (Bluetooth SIG)
- Wi-Fi – Use Wi-Fi Alliance® test plans[24] to have certified Wi-Fi connectivity
- Universal Integrated Circuit Card (UICC) - USIM/ ISIM applications on the UICC according to 3GPP TS 31.121 and TS 31.124
- Location Based Services – Test to selected LBS specifications, e.g. A-GPS using 3GPP TS 34.171 and 3GPP TS 51.010-1.

4.3.2.5 Requirements for Device and Device Management Testing

[17] Prior to IOT and System-Level testing UEs SHALL have already met 3GPP conformance and certification requirements per an independent conformance testing organization (e.g. PTCRB).

[18] Prior to operational deployment on the NPSBN, UEs SHALL have passed FirstNet-required Interoperability Testing (e.g. using a subset of applicable test cases from CTIA IOT and UICC functional test cases, vendor IOT or similar commercial LTE industry practice).

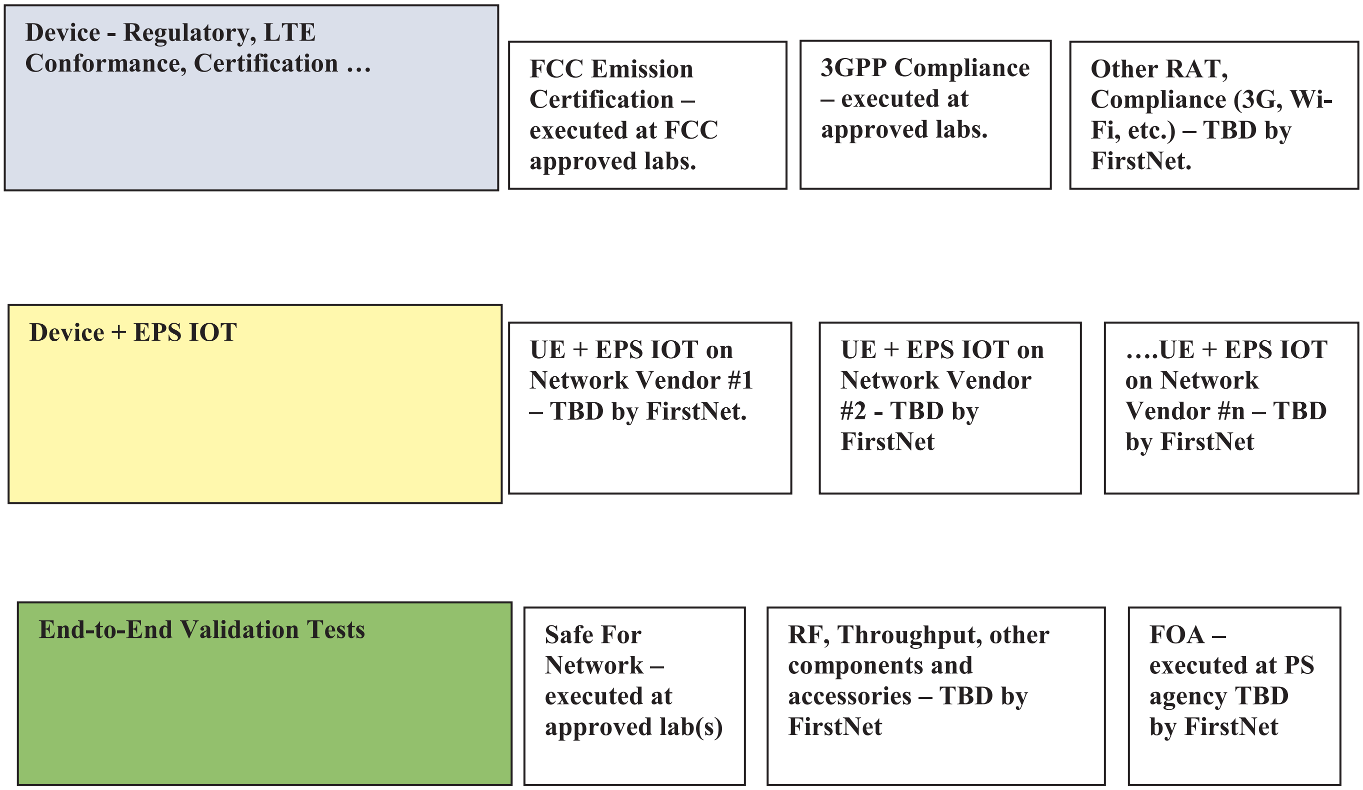
[19] Prior to operational deployment on the NPSBN, UEs SHALL have passed FirstNet-required UICC functional testing.

[23] https://www.bluetooth.org/login/default.aspx?ReturnUrl=/technical/qualification/requirements.htm

[24] http://www.wi-fi.org/certification/programs

4.3.2.6 Device Test Life Cycle

This section is an example of the potential device testing life cycle that could be implemented by FirstNet.



Device - Regulatory, LTE Conformance, Certification …	**FCC Emission Certification – executed at FCC approved labs.**	**3GPP Compliance – executed at approved labs.**	**Other RAT, Compliance (3G, Wi-Fi, etc.) – TBD by FirstNet.**
Device + EPS IOT	**UE + EPS IOT on Network Vendor #1 – TBD by FirstNet.**	**UE + EPS IOT on Network Vendor #2 - TBD by FirstNet**	**….UE + EPS IOT on Network Vendor #n – TBD by FirstNet**
End-to-End Validation Tests	**Safe For Network – executed at approved lab(s)**	**RF, Throughput, other components and accessories – TBD by FirstNet**	**FOA – executed at PS agency TBD by FirstNet**

4.3.3 Infrastructure Testing

Within the LTE network, the system is often split into the Radio Access Network (RAN) and Evolved Packet Core (EPC). Entities outside of the EPC are often considered part of the Packet Data Network (PDN) and can consist of the IP Multimedia Subsystem (IMS), APN servers, Device Management (e.g. OMA DM), IP eXchange (IPX) or essentially any other ancillary systems that are outside of the typical 3GPP LTE diagram [ref 23.401][25]. Each of these systems have specifications or reference implementations within their appropriate Standards Development Organizations (SDOs) such as 3GPP, IETF, and OMA. Due to the vast number of available interfaces and the complexity required to address all of them, the context for this section will be to determine what types of tests FirstNet should require of their vendors.

It is suggested that a set of end-to-end call flows for different scenarios be developed in conjunction with the infrastructure vendors to facilitate better interoperability between the different network elements and the UE. This should be only distributed to infrastructure and trusted UE / chipset vendors under Non Disclosure Agreement (NDA). This will help to drive additional test cases for interoperability.

4.3.3.1 Infrastructure Interface Conformance Tests

These tests will assure that the subsystem under test conforms to the specifications for that equipment. An example of this would be tests developed for the EPC S5 interface to verify conformance to 3GPP specifications. The interfaces are usually divided into the user plane (payload) and control plane (signaling). Both portions of the interface should be tested but typically the primary focus is on the signaling portion within the interface. Some interfaces such as the Uu (air interface) have unique physical layer traits that should be tested in a manner similar to the aforementioned device testing.

4.3.3.2 Infrastructure Interoperability Tests

These tests focus on the evaluation of how different vendor network elements interact with each other. In theory, if the specifications are written perfectly and implemented perfectly, the entire network would be “plug and play” and interoperability testing (IOT) would not be required. In practice, vendors often interpret specifications differently, are at different versions of the specification, or have implemented proprietary methodologies that may not allow interoperability among vendors. An example of IOT is testing the S6a interface between the MME and HSS from two different vendors.

Interoperability testing allows the network to support multiple vendors between specific interfaces. This would allow FirstNet to leverage competition within the elements of the network and provide more choices for a cost-benefit of features and price among different companies. Several different organizations such as the Multi Service Forum (www.msforum.org) and the Network Vendors Interoperability Test Forum (www.nviot-forum.org) provide a framework for system level IOT on LTE systems and can be leveraged for use by FirstNet to engage in this type of testing.

4.3.3.3 Infrastructure Performance Tests

In order to determine how well a subsystem performs, where the limits are for scaling, and to ensure reliability, it becomes necessary to test to evaluate the peak and loaded performance of the subsystem. This data can be then used to check system reliability, gauge service level agreement (SLA) requirements and load balance the network. An example of testing for this would be simulating several thousand cells on an MME and increasing the calls per second until failure. The Interface Conformance Testing referred to below includes testing of each type of interface deployed per vendor. Subsequent quantities of this same equipment are not tested prior to deployment.

[25] www.3gpp.org/ftp/Specs/html-info/23401.htm

4.3.3.4 Recommendations for Infrastructure Testing

Recommended Requirements

[20] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet-required Interface Conformance Testing (e.g. testing S1-MME conformance to 3GPP) on the interfaces specified by FirstNet.

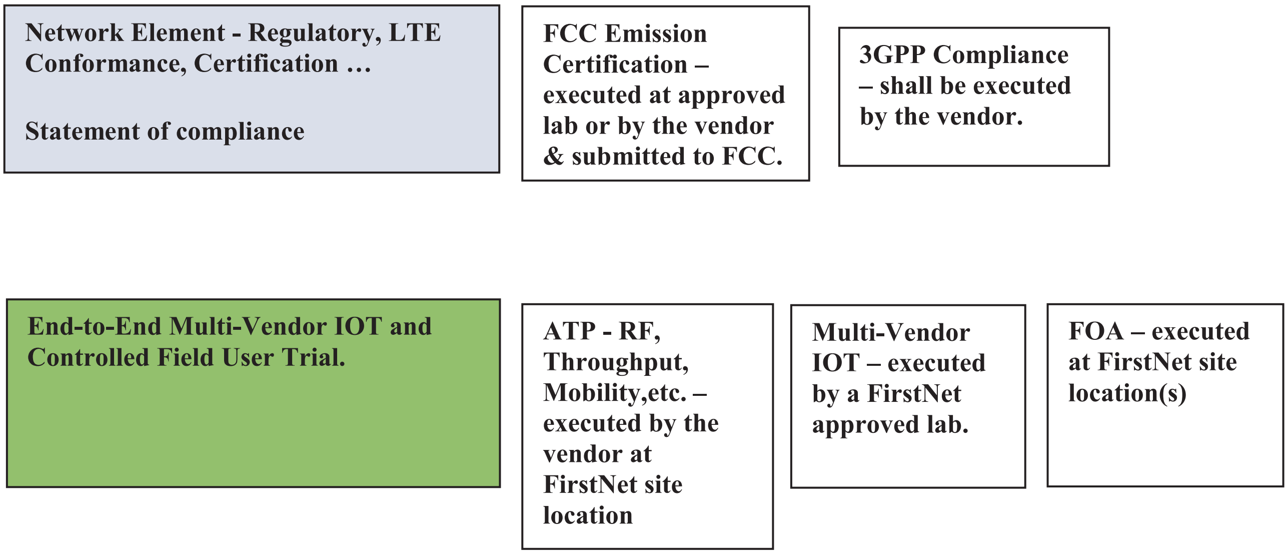
[21] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet-required Interoperability Testing at a system level as per the specific IOT requirements for the NPSBN.

Recommended Considerations

(17) Prior to operational deployment on the NPSBN, infrastructure equipment SHOULD have passed FirstNet-required Performance Testing of individual interfaces, nodes and overall system as per the specific performance requirements of the NPSBN.

4.3.3.5 Network & Network Elements Test Life Cycle

This section is an example of the potential infrastructure testing life cycle that could be implemented by FirstNet.



Network Element - Regulatory, LTE Conformance, Certification …

Statement of compliance

FCC Emission Certification – executed at approved lab or by the vendor & submitted to FCC.

3GPP Compliance – shall be executed by the vendor.

End-to-End Multi-Vendor IOT and Controlled Field User Trial.

ATP - RF, Throughput, Mobility,etc. – executed by the vendor at FirstNet site location

Multi-Vendor IOT – executed by a FirstNet approved lab.

FOA – executed at FirstNet site location(s)

4.3.4 Nationwide Application Testing

Application testing for mobile devices is a complicated task since LTE devices will be in multiple forms such as USB dongles, vehicle modems, and Smartphones. These devices typically run on different operating systems, including Android, Windows 7, Symbian, and iOS. Typically commercial service providers utilize a common connection manager to provide a common user interface across multiple hardware platforms and Operating Systems. For example, a video client on an Android Smartphone and on a Windows 7 embedded modem laptop may operate similarly to the end user but the way they operate to access the QoS to the network is typically operating system and connection manager dependent.

FirstNet may establish specific Application Programming Interface (API) specifications for applications on the network such as Push-To-Talk (PTT). The reason for developing the API specifications is that the PTT application may have specific parameters assigned to it for quality of service (QoS), APN usage, encryption and other application specifications. Application treatment is necessary for FirstNet users; therefore, each FirstNet software application for nationwide use (e.g. PTT, VoLTE, SMS) utilized on the network should pass through a set of tests to ensure it works properly on the device and does not cause unnecessary harm to the network. Most commercial service providers require application certification. FirstNet should employ similar requirements. Testing to the API for security issues may help prevent security issues that could be introduced into the network. Other local jurisdictional software applications are not mandated to pass this testing but it is highly recommended that this type of testing be performed to prevent network issues. FirstNet should consider developing a software applications development guideline, to be used by all software applications deployed on the network, to prevent unintentional network degradation."

4.3.4.1 Recommendations for Nationwide Application Testing

(18) Nationwide applications on the NPSBN SHOULD have passed FirstNet-required security testing to proper security levels (e.g. Criminal Justice Information Services [CJIS]) to ensure protection of FirstNet and public safety information.

4.3.5 System Level Testing

System testing is often called end-to-end testing and typically involves all the components of the network. After all subsystem testing is completed, FirstNet may require that the entire network or major subsystems be run through a series of tests to determine if the functional or systems level requirements for the system have been achieved.

Typically this type of system testing takes place in the form of a First Office Application (FOA) test process. The FOA test case development is a collaboration between the vendor(s) and FirstNet. The FOA performs the following functions:

- Validates that products (equipment & software) meet the test and functional requirements
- Evaluates new features and functionality in customer environment
- Provides essential design feedback between vendor, FirstNet and end customers that will provide quality assurance

4.3.5.1 Recommended Requirements for First Office Application Testing

[22] Infrastructure deployed on the NPSBN SHALL be included in the FirstNet-required FOA process as part of the NPSBN deployment.

4.4 Evolution

4.4.1 Overview

Section 6206 of the Spectrum Act defines FirstNet's duties to include building, deployment, operation and maintenance of the NPSBN. These duties include the need to update and revise established policies established to take into account new and evolving technologies. It is essential that interoperability is maintained as evolution of the NPSBN occurs throughout its lifetime. Wireless service providers typically maintain an organization responsible for establishing network evolution plans and corresponding development and execution strategies. FirstNet will own that responsibility for the NPSBN.

An important element of the policies surrounding development of the NPSBN is establishment of a network evolution framework that will enable public safety officials to leverage the technological advancements that regularly occur in the wireless industry. This provides assurance that first responders will have access to the most advanced communications capabilities possible and that the nationwide public safety wireless broadband network will keep pace with innovations occurring in the private sector. Successful network evolution necessitates striking a suitable balance between the risks, benefits and costs of adopting or not adopting new technologies as technologies and mission requirements evolve. Toward this end, the recommendations provided in this section are intended to help ensure the United States' Emergency Response Providers are able to effectively, and in a cost efficient manner, take advantage of new technologies in a way that best supports public safety mission requirements and sustains nationwide interoperability.

4.4.2 Evolution Scope

The NPSBN evolution plan can be tracked across the layers that comprise the network. Products will clearly fall in a single layer of the network. System features will require coordinated work across multiple layers. The following graphic shows the network layers and the scope of planning for network evolution:

Figure 7: Network Evolution Planning

Planning for coverage, capacity, security and network resilience are additional aspects of the overall plan. Coverage typically impacts only the RAN. Capacity, security and network resilience impact the infrastructure used to provide the network, network services and applications.

4.4.3 Future Applications and Network Services

4.4.3.1 Interoperability with Land Mobile Radio Systems

Networks that provide voice service as an application should provide voice interoperability interfaces to existing agency LMR systems in the area served by the broadband network. Public Safety users on such home or visited networks should be able to call or hail an authoritative dispatch agency or control point using the broadband network subscriber device with microphone and speaker for two-way audio, and talk or be connected to other serving agency voice communications resources. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement.

Recommended Considerations

(19) The NPSBN SHOULD allow for connection and operation of IP-based LMR voice interoperability gateways using open interfaces as they are developed.

4.4.3.2 One-to-Many Communications across All Media – Future Requirement

To ensure nationwide interoperability, the NPSBN should include one-to-many communications capabilities to users within and outside of their jurisdiction (e.g. responding in mutual aid). These communications capabilities should extend from voice, as commonly used in traditional land mobile radio systems, to text messaging, to video, and other forms of data communications. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement.

One-to-many communications could be built utilizing evolved Multimedia Broadcast Multicast Services (eMBMS). eMBMS is standardized in 3GPP and designed to provide efficient downlink (aka, download) delivery of broadcast and multicast services. However, eMBMS is unique in that it requires additional EPS functions and interfaces to support the service and also has impacts to the UE equipment as well. The basic eMBMS service was first introduced in 3GPP Release 9 and has been enhanced in release 10 and 11. As such, eMBMS is a relatively new technology and has not yet been widely deployed in commercial networks. Current target commercial applications include mobile TV and radio broadcasting, as well as file delivery and emergency alerts. Future target public safety applications may include group-oriented multi-media and PTT communications, which could be useful for incident scenarios involving large numbers of NPSBN users who are concentrated in a relatively small geographic area. Obviously a service like eMBMS poses the potential to introduce interoperability issues given its cross-network / UE implications and relative immaturity. We stop short of requiring that eMBMS be implemented in the network, because the delays in availability of final standards and subsequent implementation could unnecessarily delay the construction of the NPSBN.

When eMBMS becomes available and sufficiently capable to support public safety applications, its deployment in the NPSBN should be based on 3GPP standards (R9 or its future successors). Additionally, eMBMS will need to be deployed ubiquitously across the NPSBN in order to provide interoperable services to all NPSBN users. eMBMS would constitute a significant technology enhancement, and as such should be carefully planned and coordinated across the NPSBN. To ease in the transition, infrastructure equipment which is initially deployed into the NPSBN should be upgradable to support eMBMS in the future.

The NPSBN equipment should support eMBMS, when useful and practical, based upon 3GPP standards (current and future evolutions thereof). To the extent that 3GPP standards do not fully specify all interoperable aspects of the eMBMS service (e.g. application APIs and / or interfaces to access the capability), then those aspects should be based on open, consensus-based, non-proprietary, and commercially available standard interfaces.

4.4.4 Evolution of LTE

Driven by needs of the commercial wireless market, evolution of LTE standards proceeds incrementally over a series of releases. Each release of the LTE standard provides a new set of features as required by the market, and a consistent set of specifications from which implementers can build products. New releases of the standards are developed to maintain backward compatibility: LTE user devices built to earlier releases will continue to operate on networks supporting later releases of the standard but may not have the ability to leverage any of the new release’s functionality. Development of each release specification occurs incrementally over three distinct stages, allowing different releases to be developed in parallel:

- Stage 1 specifications define the service requirements from the user point of view.
- Stage 2 specifications define an architecture to support the service requirements.
- Stage 3 specifications define an implementation of the architecture by specifying protocols in detail. In addition, specifications related to the testing of each feature are developed in stage 3.

The standardization process ensures development of a consistent set of specifications from which implementers can build products.

4.4.5 Roadmap

To track the evolution of the network, a roadmap for introducing functions into the network is required. The roadmap should track feature availability from vendors, integration testing across vendors, planned market deployment and general availability across the network. The roadmap is used to show services available to end-users in the near term and is used to show need to vendors for longer term items. An open roadmapping process allows both network users and vendors to understand the current high level plan for the network. A key continuing output of the governance of the network is maintenance of a roadmap.

Recommended Considerations

(20) The NPSBN SHOULD be constructed and evolved in adherence to a multi-year roadmap.

This practice is typical of service provider networks and is important to interoperability in that it presents users with foresight of new services and network capabilities as well as plans for elimination of capabilities. This practice is important to the RFP process to allow equipment proposed to be sized for anticipated new features where possible.

4.4.6 Evolution Framework

This section outlines the major considerations that FirstNet should take into account in planning the evolution of the network.

4.4.6.1 Commercial Technology

There is an intrinsic tradeoff between capability/currency and stability/predictability in the adoption of new technology (a risk vs. reward tradeoff). On the one hand, staying current with commercial technology provides public safety with economies of scale, interoperability and best-in-class technology. On the other hand, the standard of reliability and predictability for technology that is used in mission critical situations must be absolutely predictable and reliable. Since the public safety wireless broadband network will employ a commercial technology (LTE), it is important for the network to keep pace with industry advances but in a measured manner. To maximize the stability of the technology, the timing of rollout of each increment (e.g. 3GPP Releases) of technology should lag that of the commercial marketplace, allowing public safety to take advantage of the vast amount of testing performed by commercial service providers. While this may be prudent in order to ensure adequate technology maturity, it may also be dictated by sheer logistics. The challenge here could be to ensure that funding sources are sufficient to keep up with the pace of commercial technology adoption (albeit somewhat phase shifted to allow for maturation).

The 3GPP specification process for LTE ensures backward compatibility from one LTE release to the next. 3GPP specifications do not require instantaneous synchronization of LTE releases across different networks. Not all portions of the standard are being implemented by vendors and the commercial service providers; furthermore, not all service providers are implementing the standards in exactly the same ways (e.g. some optional features maybe selected by one service provider and not another) or in the same timeframes. Introduction of many capabilities require complex coordination across networks and devices. For example, eMBMS requires changes to the infrastructure (E-UTRAN and Evolved Packet Core) as well as to device chipsets and software. Taking advantage of this new network functionality may require extensive network software upgrades, deployment of new network equipment, and replacement or reprogramming of user devices. FirstNet and public safety should review the specifications in conjunction with vendors and network service providers to determine a feature/function set that best suits public safety.

FirstNet will be responsible for mandating any of the LTE standards as network requirements. FirstNet should, in complementing network evolution, consider existing infrastructure deployments and assimilate them into the evolution of the nationwide network.

Recommended Considerations

(21) Infrastructure equipment procured for the NPSBN SHOULD support backwards compatibility with deployed LTE devices.

(22) Infrastructure equipment in the NPSBN SHOULD be upgradeable to minimally two major 3GPP releases (i.e. n+2, where n is the release available at deployment provided that the equipment does not need to implement a new air interface specification).

4.4.6.2 Compatibility

As commercial technology evolves, new capabilities are introduced. Public safety jurisdictions will need to determine what new capabilities they would leverage for its applications, plan an introduction roadmap, and also ensure that uses of earlier technology is not compromised. This primarily affects four aspects:

Application to Application: This involves ensuring that devices/clients are compatible with other corresponding devices/clients (peer to peer) as well as between the device/client and the network components of the application (e.g. device client to application server such as a database).

Device to Network: This is the area of most scale and individual impact. The evolution plans must consider the useful life / support window for devices on the network and plan the introduction of new technology to accommodate this compatibility window.

Network Element to Network Element: This comes into play as new capabilities are introduced into the network and the updates involve more than one entity in the network and thereby implicitly impact the interfaces between network elements. Introduction of new capabilities (software or hardware) may need to be coordinated to ensure that all impacted elements are properly orchestrated and supported.

Network to Network: There are three main areas of consideration for this.

- Regional operational domain to regional operational domain (IOT and mobility considerations)
- NPSBN to service provider network (primarily roaming considerations)
- NPSBN to Public safety P25/LMR Network

In order for the NPSBN to provide a long-term viable capability, it must evolve along with technology and the commercial industry. In general, standards bodies, such as 3GPP, recognize this as well as the importance of managing this evolution for users of the network. Interfaces that are extended to users of the network (end-users, application developers, state/agency IT, etc.) must be carefully managed in order to allow users to migrate their dependencies gracefully as the network services evolve over time.

It will be necessary for the equipment comprising the NPSBN to be upgradable to support future features and releases of the applicable standards (e.g. 3GPP). This is common industry-practice in order to ensure cost effective and non-disruptive network evolution. Management of inter-network element (potentially inter-vendor) interfaces is crucial to ensure that the equipment interoperates through successive releases and the evolution of the network.

Recommended Requirements

[23] The equipment comprising the NPSBN SHALL provide backwards compatibility of interfaces, from time of deprecation, for a minimum of two full major release/upgrades of the network. This requirement may be waived (i.e., interface obsolescence accelerated) if FirstNet can ascertain from the user community that there are no dependencies on a given interface.

Recommended Considerations

(23) Hardware and software systems comprising the NPSBN SHOULD support industry practices for management of standard network interfaces from each supplier. These industry practices include formal publication of interface compliance, deprecation of interfaces, support for backwards compatibility and graceful obsolescence of interfaces.

(24) The NPSBN SHOULD support industry practices for life cycle management of interfaces that it exposes to applications or users of the network to ensure backward compatibility for a reasonable interval, using industry-practice interface deprecation and obsolescence methods. The interfaces include, but may not be limited to: Network messaging Protocols, Application Programming Interfaces, Web-based Interfaces, Protocol/Messaging Interfaces, and User Interfaces such as Command Line Interfaces.

4.4.6.3 NG 911 Services

While not completely defined, NG (Next Generation) 9-1-1 services will have an effect on the NPSBN. The following statistics indicate the possible potential to increase network traffic as these devices report public safety events, accidents, injuries or whatever the call might be. Today in the United States, there are approximately 330 million wireless connections, while the U.S. population is slightly more than 312 million. Smartphones are in the hands of about 43% of mobile phone users (62% if you are 25-34) and this number is growing rapidly. Voice communications account for only 1/3 of mobile usage, with the remaining 2/3 of mobile traffic arises from text messaging, applications, video calling, and so forth. Likewise, 32% of adults and 36% of children now live in wireless-only households. In the 9-1-1 arena, 70-80 percent of 9-1-1 calls originate from mobile devices.

Consumers rightly and reasonably expect to be able to send data (pictures, video, and text messages) to 9-1-1 call centers. As FirstNet develops the public safety wireless broadband network, it must ensure seamless and secure communications paths exist from the individuals who originate 9-1-1 traffic, through the call/dispatch center, and onto FirstNet's customers in the field. FirstNet must ensure that its network interoperates and interconnects with Next Generation 9-1-1systems to meet the expectations of consumers who request service through 9-1-1. Finally, FirstNet must ensure that its network includes location determination capabilities commensurate with those available to consumers so that its own subscribers can be located when necessary.[26]

4.4.6.4 Coverage

As the network is initially built out, it is expected that it will incrementally expand to increase geographic coverage. As regional networks "grow" together, it will be important for the evolution to take into account a cohesive RF plan and interconnect strategy (e.g. as rural areas add RF coverage, they could be hosted by urban or state-wide networks).

Coverage is complex to engineer in LTE broadband networks since it has many variable components. In general, uplink and downlink user throughputs diminish as one moves from cell center to cell edge (by potentially an order of magnitude or more). User data rates (and, hence, overall capacity) are also affected by adjacent cell activity (interference). This is much different than today's LMR systems, for example. As application types (and priorities) vie for this dynamically varying bandwidth, the network will have to adapt in real time to ensure that the highest priority applications and users are served in the best way possible.

4.4.6.5 Capacity

As usage of the network increases, capacity may need to be enhanced. Capacity enhancements may affect RF planning as well as increase the signaling and bearer traffic loads on core network elements.

Addition of capacity is typically accomplished through the addition of cells (the initial network may be built on a relatively sparse grid). As traffic loading in the network increases, the core network elements and/or links may need additional capacity. Capacity engineering guidelines may be defined and published relative to support for classes of public safety applications and the number of concurrent instances of an application class that can be supported by a given data rate. These would be input to network engineering activities and would help align expectations of network performance overall. However, it is unrealistic to mandate minimum supported rates/performance unilaterally across all networks and locations within the networks. Capacity planning must be coordinated between regional portions of the network and shared national components to ensure that the entire network scales end-to-end.

NOTE: These decisions may be left to regional/local network operation or made in consultation with regional/local authorities.

4.4.6.6 Resiliency

As the NPSBN topologically evolves (sites are added, EPC nodes are added, etc.), overall consideration of network resiliency has to be continually evaluated. This is necessary to ensure that application data centers, EPC nodes, interconnect/backhaul, and RF (where applicable) redundancy is properly engineered and maintained to the necessary standards. Resiliency has to be applied at the regional level to ensure that each such deployment is robust but also must be applied on a national scale for network assets that are truly operated nationwide (e.g. an IP backbone used to interconnect regional deployments). This involves ensuring adequate equipment redundancy to serve expected capacity, geographic redundancy to protect against localized disasters, diversely routed connections, etc. To maximize resiliency, the availability and use of multiple communications technologies and RF bands should be considered.

[26] The source of the statistics cited above is the 2011 Annual Report of CTIA – The Wireless Association.

Recommended Considerations

(25) The EPC equipment in the NPSBN SHOULD support optional local and geographic redundancy.

(26) The equipment in the NPSBN SHOULD support transport redundancy wherever economically feasible (i.e. connections to local switching equipment or WAN connectivity between sites or core locations).

4.5 Handover and Mobility

Handover is a key element of ensuring interoperable communications across the NPSBN. Per 3GPP Standards, handover allows a UE's sessions to be maintained as it traverses parts of the network's coverage area that are served by different cells. Such cells can belong to the same or different PLMNs. In addition, depending on device capabilities, cells may use different radio access technologies (RATs) deployed in different spectrum bands. Seamless service continuity is achieved when the potential interruptions experienced during handover are minimal. Further, for a better user experience, packet loss can be minimized when packets are forwarded from the original cell to the new cell while the handover is being completed.

Roaming refers to the ability of a user device to connect to a network that is not its home network. Such networks may operate in different bands using different technologies. Hence, the user device must also support these technologies to successfully support roaming to the new network. Support for roaming is an essential element of interoperability between disparate systems. It is addressed herein only in the context of roaming between the NPSBN and other networks, such as commercial cellular networks.

4.5.1 Definitions

We define the following terms:

Handover: The process of transferring active voice or data session(s) associated with a wireless device from one cell site to another cell site in the same or a different wireless network while maintaining the device's session(s). To provide a seamless handover experience, the length of time that it takes for the device to switch between the two cell sites (called the interruption time) must be minimized. 3GPP standards do not currently specify the interruption time for intra-LTE handovers.

Roaming: The ability of a wireless user to receive services in a network provided by a different service provider, using a PLMN identity differing from that in the user's home network. This can include mobile as well as Wi-Fi networks. The roaming user is typically charged roaming fees while making use of the roaming network.

4.5.2 Handover

The following schematic will be used to illustrate the handover mechanisms supported by LTE.

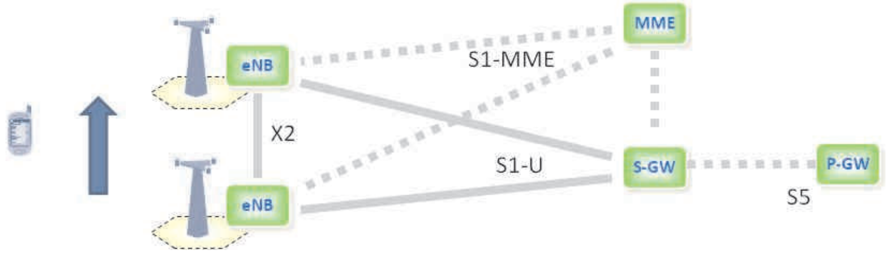


Figure 8: LTE Handover Mechanisms

The following handover scenarios are identified:

- Handover between cells in the NPSBN served by the same MME.
- Handover between cells in the NPSBN served by different MMEs.
- Handover between Band 14 networks with different PLMNs. Such a scenario is representative of a handover between the NPSBN and a commercial provider with whom FirstNet or an opt-out state has a public/private partnership arrangement. Such business arrangements are envisaged by the Spectrum Act, and supported by RAN sharing features supported by LTE.

Recommended Requirements

[24] The NPSBN SHALL support user mobility across the entire NPSBN (including Opt-out states).
[25] The NPSBN SHALL support S1 and SHALL preferentially support X2 handover between adjacent NPSBN cells (including cells owned by opt-out states) whose proximity supports a handover opportunity.

4.5.2.1 Handover between cells in the NPSBN served by the same MME

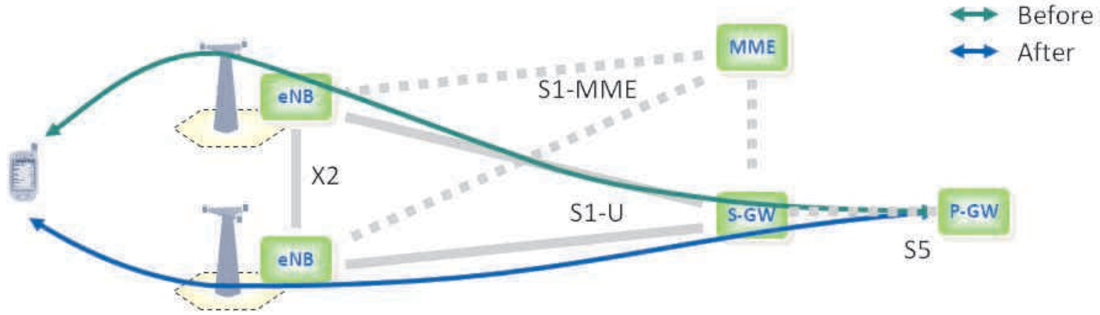


Figure 9: Intra-MME Handover

As shown above, both cells are under the control of a common MME. (As of 3GPP R10, X2-based handovers are only supported between eNBs served by a common MME.) In this scenario, the handover process leverages the X2 interface, supported by supplementary signaling carried over the S1-MME interface. Data forwarding for X2-based handovers is supported via the X2 interface.

During the handover process, Information Elements and signaling messages defined by the 3GPP standards are exchanged between source and target cells over the X2 interface. While X2 handovers use 3GPP's open standard interface, X2 handovers between different vendors' eNBs require inter-vendor testing to ensure interoperability. To reduce the amount of testing required during the early stages of introduction of a new wireless technology, commercial service providers use a practice known as "grouping" – grouping network elements from vendors in their network deployments. The current best practice used by commercial service providers is grouping eNBs from a common vendor into clusters of adjacent cells. These clusters, in turn, are served by a common MME for the purpose of executing X2 handovers and supporting other air interface functions provided over the X2 interface (e.g. scheduling, Inter-Cell Interference Coordination (ICIC), etc.). At the boundaries of these clusters, S1-based handovers are used between eNBs provided by different vendors.

There is on-going work to perform the additional testing required to ensure the interoperability of inter-vendor X2 handovers. As and when commercial service providers start deploying inter-vendor X2 handovers, the NPSBN will also be in a position to support inter-vendor X2 handovers as governed by the NPSBN's network evolution planning. Such an approach will allow the NPSBN to leverage the testing performed by the commercial market. An alternate and potentially resource-intensive approach is for the NPSBN to perform such testing on its own initiative. Until this testing is completed, X2 handovers across vendors cannot be considered interoperable, and hence should not be exclusively required in the NPSBN.

4.5.2.2 Handover between Cells in the NPSBN Served by Different MMEs

When a user/device moves into an adjacent region served by a different MME, the standardized S1 handover mechanism, as shown below, provides seamless mobility.

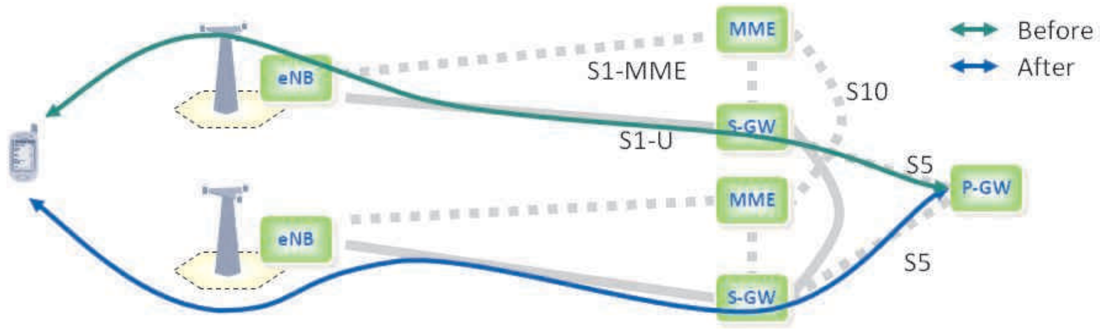


Figure 10: Inter-MME Handover

As illustrated, the handover uses the S1 interface between the source eNB and MME, with the MME coordinating the handover. The MME, in turn, uses the S10 interface to communicate with the MME serving the target eNB to which the user is handed off to. As part of the handover, a new S-GW may be selected as well. In this case packets will be forwarded from the original S-GW to the new S-GW during the handover to minimize packet loss.

4.5.2.3 Handover between Band 14 Networks with Different PLMNs

There may be scenarios in which handover between multiple Band 14 networks, each with a different PLMN ID, is required, e.g. in a public/private partnership with utilities, transportation, or a commercial wireless service provider. The S1 method of handover described in the previous section can also be used to provide handover between Band 14 networks with different PLMN IDs, using the S10 interface between the MMEs in each of the networks. As clarified in 3GPP 23.401, Section 4.2.3, the S10 interface can cross PLMN boundaries. It is expected that the coordination overhead between these networks will be minimal since the number of neighboring cells will be minimal, and primary use may be to handoff to a provider who shares the RAN already.

4.5.3 Roaming from NPSBN onto Commercial Mobile Networks

Sections 6206 and 6211 of the Spectrum Act clearly identify roaming to commercial networks as a key capability required in the NPSBN. It will be especially important during the initial phases of deployment when Band 14 coverage is not yet ubiquitous. Although 3GPP standards support inter-RAT, inter-network handovers between different networks, its implementation would require a significant effort by both the NPSBN and commercial network service providers. For instance, both networks have to open up additional interfaces and provision neighboring cells in each cell of both networks. Currently, this approach is cumbersome and subject to constant churn. One of two alternative approaches should be used:

- Roaming without service continuity, i.e. no seamless service
- Roaming using mobile VPN technology to support session persistence.

FirstNet should also consider Access Network Discovery and Selection Function (ANDSF) as defined in 3GPP 23.402 for roaming to trusted WLAN as alternative to VPNs. ANDSF leverages the LTE credentials for authenticating users, allows seamless handover between LTE and trusted Wi-Fi, and provides similar security as used in LTE. This may allow public safety users to securely and seamlessly roam between NPSBN and their own Wi-Fi networks, e.g. in police and fire stations, without the need for a mobile VPN. The associated cost/benefit should be carefully analyzed on a case by case basis.

4.5.3.1 Roaming Without Service Continuity

To support roaming onto 3GPP and/or 3GPP2 networks, a Band 14 LTE device must accommodate at least one additional 3GPP or 3GPP2 frequency band. If roaming is enabled, the device stays on the NPSBN until the LTE signal becomes insufficient for service, causing the device to go idle and scan for other networks stored in its roaming/white list. If an alternate accessible network is found, the UE will attempt to attach to that network. When this happens, all active connections are released (dropped), and must be re-established on the new serving network. Note that while roaming onto the commercial network, the user may not have the same capabilities/QoS as experienced on the NPSBN, subject to roaming agreements. While in roaming mode, the device periodically checks for availability of the (home) NPSBN when it is idle as described in 3GPP TS 23.122. Once available, the device moves back to the NPSBN when idle. It is expected that FirstNet will enter in to roaming agreements and associated fees with various commercial service providers. Furthermore, under the terms of the Spectrum Act, FirstNet would make the decision to implement roaming with commercial networks.

The figure below illustrates roaming to a commercial LTE network when home-routed APNs are employed. For this particular case the S6a and S8 interfaces are required between the two networks. An Internetwork Packet Exchange (IPX) provider is expected to be leveraged for the connectivity between the NPSBN and the commercial LTE network for both home-routed and local breakout options as recommended by GSMA PRD IR.88 – LTE Roaming Guidelines.

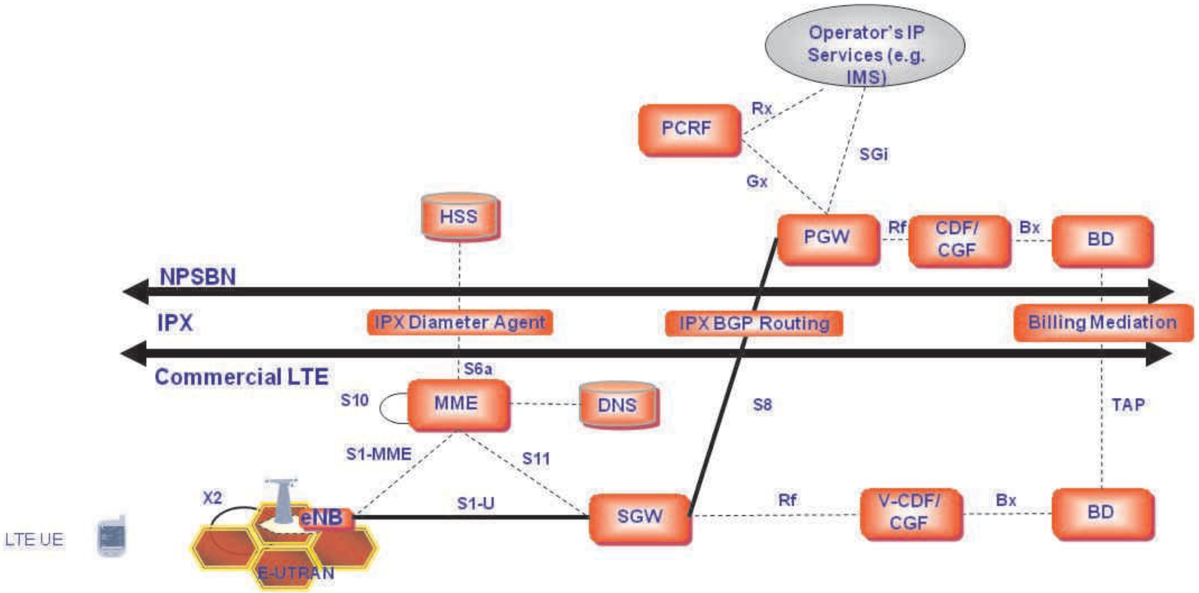


Figure 11: Roaming Using Home-Routed APN

To support local breakout APNs, the S6a and S9 interfaces are required between the two networks as shown in Figure 12.

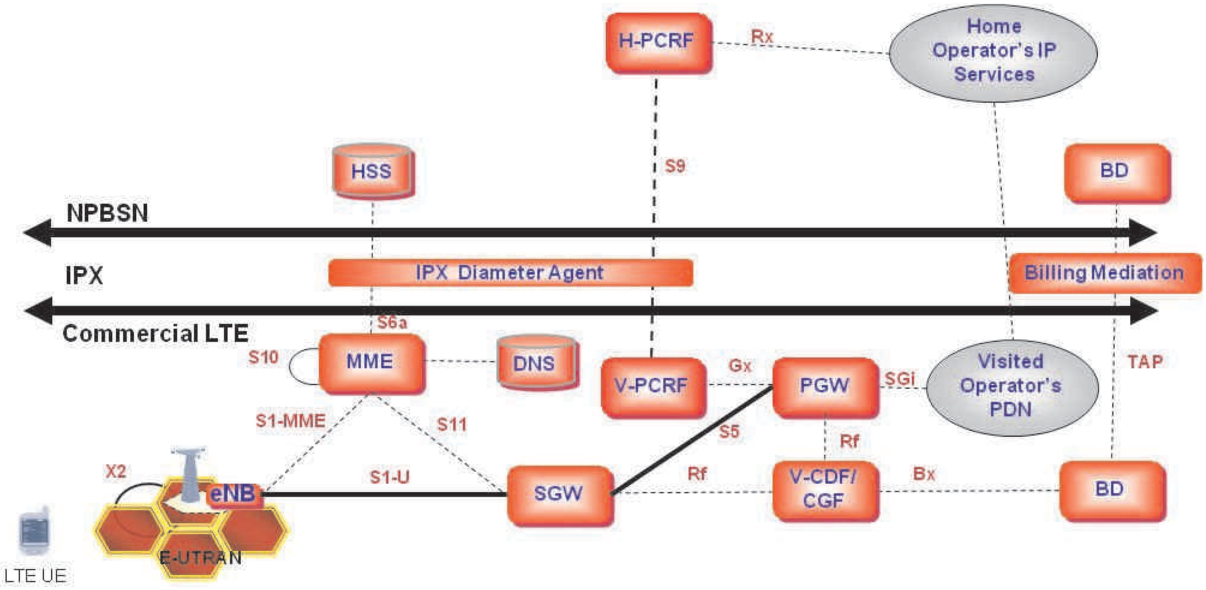


Figure 12: Roaming Using Local Breakout APN

If roaming to 3GPP 2G/3G networks is supported, these networks require the HSS to act as an HLR to the 2G/3G networks to provide an HLR view of subscriber's HSS data as defined in 3GPP TS 23.002. If roaming to 3GPP2 (eHRPD) networks is supported, the HSS needs to support the SWx interface as defined in 3GPP 23.402 to enable an Authentication, Authorization and Accounting (AAA) view of the subscriber's HSS data, e.g. for authentication of the user.

Recommended Requirements

[26] If roaming between the NPSBN and commercial LTE networks is implemented, the NPSBN SHALL follow GSMA PRD IR.88.
[27] If roaming between the NPSBN and commercial 3GPP 2G/3G networks is implemented, the NPSBN SHALL follow 3GPP TS 23.002 to support roaming into 3GPP 2G/3G networks.
[28] If roaming between the NPSBN and commercial 3GPP2 (eHRPD) networks is implemented, the NPSBN SHALL follow 3GPP 23.402 to support roaming into 3GPP2 (eHRPD) networks.

Recommended Considerations

(27) If roaming between the NPSBN and commercial LTE networks is implemented, and IMS is implemented in the NPSBN, the NPSBN SHOULD implement support for IMS while roaming into other LTE PLMNs.

4.5.3.2 Use of Mobile VPN Technology to Provide Session Persistence when Users Roam

Support of session persistence when users roam to other RATs/networks can be provided using mobile VPN solutions. However, the user may experience a short interruption depending on the specific mobile VPN selected. Mobile VPN solutions are currently in use by public safety to, for example, support service continuity between commercial wireless networks and Wi-Fi. In the NPSBN, the choice of whether to use mobile VPNs, and which vendor equipment to use can continue to be made by the individual agencies. Typically this functionality resides in a vehicle laptop or a trunk-mounted vehicle router. To support multiple wireless networks, the mobile VPN device supports a wireless modem for each of the networks it needs to connect to. Each modem has its own wireless subscription with associated monthly fees.

Today, mobile VPN is used with 2G/3G technologies to support best effort services only. When used for guaranteed bit rate services with dedicated LTE bearers, a mobile VPN will be able to maintain service availability, but the alternate access technology may not be able to provide the same quality of experience. For example, if a user is sending real-time video on LTE and loses LTE connectivity, the new network may not have the bandwidth available to continue this video service with the same quality of experience.

Recommended Requirements

[29] The NPSBN SHALL support the use of mobile VPN technology to support mobility between the NPSBN and other networks.

4.6 Grade of Service

An interoperable nationwide broadband network dedicated to public safety must be capable of supporting essential mission critical public safety broadband applications and services on a nationwide basis. A uniform minimum grade of service requirement provides service transparency across various regions and jurisdictions within the NPSBN. Minimum performance requirements also contribute to interoperability by ensuring that mobile users receive consistent service as they move from one area of the network to another, especially in times of emergency.

We acknowledge that budgetary constraints, lack of base station sites (e.g. in remote areas) and other factors may make it difficult to provide a uniform grade of service, especially in the early years of the NPSBN. Because of this constraint, we foresee additional value in providing the NPSBN the ability to offer different Grades of Service in different parts of the country. In such an operating environment, we foresee value in developing a "common language" to be used across the NPSBN to describe the grade of service provided in different geographic regions. Use of a common language to describe GoS promotes interoperability in the following ways:

- Emergency response planners can take into account the grade of service provided in different geographic regions when developing incident response plans and operating procedures.
- Predictability of service - helping responders know which applications can be supported where. (We note that RF coverage design is not the only factor that influences the data rates users experience. Data rates may be further constrained by policy controls, for example.)

There are additional benefits to providing a common language for grade of service beyond supporting interoperability:

- Common design criteria that can be used for RFPs, helping determining inter-site distances for high-level designs and coverage predictions for RF designs
- Common criteria for measuring grade of service once networks are brought on line

A set of measurable GoS attributes must be established in order to design networks (for purposes of RFPs, for example) and measure performance (for purposes of performance validation, for example). This section discusses GoS attributes used for RAN design. Performance measures used to evaluate a network during acceptance testing or post-launch are also critical. It is recommended that measures and processes be established for both acceptance testing and on-going monitoring of GoS in the NPSBN.

Minimum design requirements adopted for the network must strike a balance between network deployment cost, user quality of experience and network spectral efficiency. In considering these factors, adoption of minimum requirements does not preclude the NPSBN from providing service that exceeds this baseline in different regions.

4.6.1 Coverage Area

A methodology based on the percentage of geographic area covered should be used to determine the degree of coverage within a geographic area. The geographic area is defined as the location (e.g. county, state, city boundary, etc.) within the United States that the NPSBN has targeted for operation. Geographic areas include interior U.S. waterways contained within an area's boundaries. The coverage area is the portion of the Geographic Area where NPSBN service is supported. Different parts of a geographic area may provide different Tiers of Service, as described in Section 4.6.2. As much as possible, coverage areas within a geographic area should be contiguous, thereby maximizing handover opportunities and minimizing service interruptions for mobile users.

In-building coverage, or portability, may be required in densely populated areas or specific venues such as police, fire and EMS stations, hospitals, and other critical infrastructure. On-street coverage, or mobility, may be required in sparsely populated areas. Sparsely populated areas, for example, could be determined on a county by county basis using county-level population densities. It will be important to determine over which portions of a coverage area on-street or in-building coverage is required.

Coverage maps, maps which show pictorially which GoS Tiers (see Section 4.6.2) are supported over a geographic area, are useful tools for operational planning, and hence aid in supporting interoperability. Coverage maps are also useful tools for measuring the progress of network deployment over time and informing the First Responder community of deployment plans.

Recommended Considerations

(28) Coverage maps SHOULD be maintained that show pictorially which GoS Tiers are supported over a geographic area. Detailed maps SHOULD be made available to authorized public safety agencies.

(29) NPSBN coverage maps showing planned future coverage SHOULD be maintained. The maps SHOULD show planned coverage at regular intervals (e.g. quarterly) into the future. These maps SHOULD be made available to authorized public safety agencies.

4.6.2 GoS Tiers

GoS is a multi-dimensional measure of network performance achieved within a Coverage Area. Grade of Service, for example, can be used to describe the minimum expected uplink and downlink data rates and reliability of service throughout a coverage area. The use of different GoS tiers provides the ability for different GoS levels to be supported in different parts of a geographic area based on mission needs, availability of infrastructure and other factors.

To assist public safety practitioners, each GoS Tier should also describe the types of applications that can be supported with clear, common and consistent definitions.

The table below is illustrative of how GoS tiers could be defined.

Tier	Percent Covered	On-Street/ In-Building	Service Probability	Data Rates (kbps)	Applications Supported
1	X%	X	X%	X DL / X UL	X
2					
3					
4					

Recommended Considerations

(30) The NPSBN SHOULD use a set of pre-defined GoS Tiers to provide clear and uniform description of the services of network performance provided within a Coverage Area.

(31) The GoS Tiers SHOULD include the minimum set of GoS Attributes defined in Section 4.6.3.

(32) The expected or actual GoS Tier SHOULD be disclosed to authorized public safety agencies in a geographic region.

(33) Each Coverage Area SHOULD be designed to operate with a defined GoS tier.

4.6.3 GoS Attributes

4.6.3.1 Service Probability

This metric, which can also be called coverage reliability, defines the probability a minimum level of service (e.g. data rate) is met within the coverage area. It quantifies the level of confidence associated with in accessing services within a coverage area. If a service probability is defined as high, then the users will be able to gain and maintain access to the network more frequently and be refused or have difficulty maintaining service less often.[27]

[27] RFPs issued by FCC Waiver Recipients have largely specified a 95% probability of service for the Public Safety network. [See LA RICS RFP Addendum 1 Sec. 8.20.5; also City of Mesa, AZ RFP #2010209 Sec. 1.9.1]

RF engineering will have a significant impact on the performance of the network and therefore affect service probability. Once a coverage area is specified, cell tower placement, system tuning and ongoing performance maintenance among other factors are critical to achieving high service probability specifications.

Recommended Considerations

(34) Service probability SHOULD be specified for each GoS Tier, in order to specify the quality of the user experience provided by the network.

4.6.3.2 Data Rates

Cell edge data rates, the minimum data rates achieved across a site coverage area with a certain confidence level, are critical design metrics. Cell edge data rates determine the minimum required signal levels that must be supported over a coverage area. The signal levels needed to achieve a target data rate vary across infrastructure and device vendors because of their respective systems' specifications and resource allocation strategy.

Cell edge data rates should be utilized for engineering purposes as they provide a consistent measure of worst-case performance over a coverage area. Minimum data rate is readily measurable, and therefore is a useful statistical tool for quantifying system performance.[28] Due to protocol overhead bits inserted at different layers of the protocol stack, data rates at different reference points in the protocol stack vary. Hence, when minimum data rates are specified, they must also include the protocol layer at which the data rates are to be measured.

Recommended Considerations

(35) The expected minimum uplink (mobile to network) and downlink (network to mobile) rates of data transmission SHOULD be specified for each GoS Tier. The specifications must also include the protocol layer at which the data rates are to be measured.

4.6.3.3 Usage Models

The amount of traffic generated in a coverage area affects interference level, and hence, network performance. Therefore, the NPSBN should be engineered to meet defined Usage Models for each Coverage Area, for example Light, Medium, Heavy or Emergency.

Expected utilization of the network plays a key role in determining the design and effectiveness of the network. A usage model should take into account different customer usage patterns and the data volumes of the applications they will utilize (web browsing, FTP, VoIP, Streaming Video, etc.).

4.6.4 RAN Boundaries & Coordination

The handling of RAN boundaries plays a critical role in the design and performance of the NPSBN. As discussed in Section 4.5.2, X2 and S1 handovers provide seamless service. Other handovers, however, can temporarily disrupt service, or, at worst, cause a mobile session to terminate, disrupting service. As a result, handover boundaries must be carefully designed.

Special attention must be paid to boundaries between State Opt-Out RANs and RANs deployed by FirstNet. In addition, interference at such RAN boundaries must be managed. LTE supports multiple capabilities for cell coordination and definition/management of handovers. Whichever approach is selected by FirstNet, it is imperative that it be done in a coordinated manner across the NPSBN. Without coordination, network performance can suffer.

[28] RFPs issued by FCC Waiver Recipients have largely specified 768k downlink [system-to-mobile] and 256k uplink [mobile-to-system] for the Public Safety network. [See LA RICS Addendum 8 Section 8.3.3

Recommended Considerations

(36) The NPSBN SHOULD implement a scheme for engineering RAN boundaries according to a national cell coordination plan.

4.7 Prioritization and Quality of Service

Prioritization and Quality of Service (QoS) are essential functions in the NPSBN. Prioritization is the network's ability to determine which connections have priority over others. Quality of service is the network's ability to ensure that IP packet flows associated with different applications satisfy performance objectives (e.g. packet loss, delay and throughput) needed for different applications to operate. Thus, prioritization addresses the network connection while QoS addresses the treatment of traffic after the connection is established.

Support of prioritization in the NPSBN must ensure that high priority users can establish connections with higher level of certainty relative to low priority users. In general, priority levels for connections can be defined and assigned based on various criteria (and combinations thereof), including the user's role (or user priority), user application types, or incident type.

Priority access and QoS contribute to interoperability by ensuring that users receive consistent service as they move from one jurisdiction to another, most crucially during times of emergency. Further, priority and QoS help ensure that consistent service is maintained during periods of network congestion. The establishment of a uniform approach to supporting priority access and QoS across the NPSBN that provides service transparency across various regions and jurisdictions within the NPSBN is essential.

In addition, public safety applications[29] such as Computer Aided Dispatch, Incident Command Systems and other applications which exchange information streams over the NPSBN that require QoS support for their proper operation (e.g. real-time video and voice) will require standardized mechanisms to inform the network of the prioritization and QoS attributes of these IP packet streams. Further, these applications will need the ability to modify prioritization and QoS attributes in real-time. In response to an incident, there may be a need to change the priorities of different users, and hence their IP packet flows, to ensure that specific users, devices and applications have appropriate access to network resources. For example, dispatchers might dynamically change specific users' prioritization to ensure that devices and applications have access to network resources during times of congestion.

Hence, applications used by public safety must be able to change priorities and specify QoS treatment of different IP flows using a set of network services that are interoperable across the NPSBN. There are several methods available to public safety applications in order to perform these priority and QoS changes:

- Current standards support use of the 3GPP 'Rx' interface to allow an application to convey the responder's priority and provide this information to the NPSBN. A common FirstNet profile detailing usage of the 3GPP 'Rx' interface can provide consistent configuration and prioritization across the NPSBN. Given the mature nature of the 'Rx' interface standard, it is envisioned as suitable for initial usage by the NPSBN.
- Use of open Application Programming Interface (API) technology and Service Oriented Architecture (SOA) frameworks are accepted industry practices leveraging commercial, open standards for exposing such network features to new and existing applications. Use of open standard APIs such as GSMA's OneAPI with potential extensions for public safety promotes interoperability by providing a stable interface between applications and the underlying LTE network, shielding applications from low-level changes and enhancement of the LTE network as the NPSBN evolves. Leveraging (and, if needed, extending) existing open standard APIs such as GSMA's OneAPI can provide interoperable access to LTE network services.

LTE's prioritization mechanisms provide useful mechanisms for prioritization of public safety traffic. In addressing the topics of prioritization and Quality of Service for the NPSBN, the Interoperability Board reviewed draft work by the National Public Safety Telecommunications Council (NPSTC) Broadband Working Group's Priority and QoS Task Group.[30] Prior to passage of the Spectrum Act, NPSTC's Priority and QoS Task Group began studying how

[29] Legacy IP-based applications will not support this functionality without additional support functions or enhancement. Standardized mechanisms to inform the network of the prioritization and QoS attributes of these IP packet streams are necessary to ensure that future applications are able to take advantage of these essential prioritization and QoS mechanisms in a common way to ensure interoperability.

[30] "Priority and QoS in the Nationwide Public Safety Broadband Network," Rev. 1.0, April 17, 2012. (See http://www.npstc.org/download.jsp?tableId=37&column=217&id=2304&file=PriorityAndQoSDefinition_v1_0_clean.pdf)

LTE's standard prioritization and QoS mechanisms could be used to meet public safety's unique mission needs. The Task Group's work continues. We note that some of the mechanisms currently envisioned by the Task Group are currently supported by the LTE standards. Some of the mechanisms, however, will require development of supplemental standards to provide desired functionality (e.g. the creation of Priority and QoS APIs). A description of some of the functional requirements developed by NPSTC is included in Appendix 1.

4.7.1 Profiles: Default Values

3GPP standards define a number of standardized mechanisms to control prioritization and QoS in LTE networks. These mechanisms, tied to the identity of LTE user equipment, utilize a number of parameters which control the way priority and QoS are enforced on a user or class of users, an EPS bearer basis, or multiple EPS bearers per user. These parameters include:

> **Access Class:** Every UE belongs to one or more access classes. A UE's assigned access class is used to determine how often it may attempt to access the network in case of network congestion. Such a form of access control is not generally intended for use under day-to-day network operations: it is expected to be enforced during network congestion or large-scale emergencies (e.g. hurricanes, earthquakes, etc.). A UE's Access Class is stored in its USIM. (See additional background on Access Class in Section 4.7.5.)
>
> **Allocation and Retention Priority (ARP):** The ARP value, assigned per EPS bearer, is used in admission control and is characterized by a priority level, a pre-emption capability and a pre-emption vulnerability. Essentially, this parameter governs if a responder's resource request is granted by the NPSBN. This parameter is also used to determine if a responder's existing application(s) can be pre-empted.
>
> **UE-AMBR:** Defined per UE, the Aggregate Maximum Bit Rate (AMBR) represents the upper limit of aggregate bit rate consumed by a UE for all non-GBR bearers which can be set separately for the uplink and downlink traffic.
>
> **APN-AMBR:** Defined per UE and APN, APN-AMBR represents the upper limit on the aggregate bit rate consumed by a UE for all non-GBR bearers associated with an APN which can be set separately for the uplink and downlink traffic.

Default priority values for these parameters define the day-to-day treatment of user equipment in the NPSBN. Some of these default values (e.g. Access Class) are stored in the user device's USIM. Others are stored in the LTE network's Home Subscriber Server, or Subscriber Profile Repository, and retrieved when a user attaches to the NPSBN.

There are many potential combinations of default values that can be defined for the priority and QoS parameters shown above. To help facilitate operational interoperability, a common set of user profile templates could be used to specify the default values assigned to a user based on the user's day-to-day role. Defining a set of common templates to be used across the NPSBN helps promote operational interoperability by reducing complexity and allowing creation and enforcement of common operating procedures across the NPSBN.

Recommended Considerations

(37) A set of default QoS profile templates SHOULD be defined for each responder function (e.g. police, fire, EMS) supported by the NPSBN.
(38) Each QoS profile template SHOULD contain a descriptive definition of the responder function and default values for ARP, Access Class, UE-AMBR, and APN-AMBR.
(39) Since the NPSBN could also support secondary users, default QoS profile templates SHOULD be defined for public safety and secondary users.
(40) Every user of the NPSBN (public safety and secondary users) SHOULD be assigned a default prioritization and QoS profile using the set of pre-defined QoS profile templates.
(41) A process SHOULD be established and followed to manage the assignment of templates to users to ensure template assignment rules are uniformly applied for all users using the NPSBN.

4.7.2 Profiles: Dynamic modification

Supporting public safety incident response, planned events, and other situations may require temporary changes to a user's default prioritization and QoS treatment. Hence, the NPSBN must allow temporary override of the default profiles.

Recommended Requirements

[30] The NPSBN SHALL provide the ability for national, regional, and local applications to dynamically change a UE's prioritization and QoS using the 3GPP 'Rx' interface.

Recommended Considerations

(42) FirstNet SHOULD make an API available to national, regional, and local applications to expose Priority and QoS control.

4.7.3 QoS Class Identifiers (QCIs)

LTE has developed standardized mechanisms for defining the QoS requirements of different IP packet flows. These mechanisms are used by the LTE network, for example, to determine how packets should be scheduled for transmission and how other network resources should be assigned to users to ensure the delay, loss and throughput requirements of the IP flows are met.

3GPP TS 23.203 defines a standardized set of QoS Class Identifiers (QCIs) (shown in the table below). This set of QCIs describes the QoS characteristics of all applications that are currently envisioned to be carried over an LTE network. Use of a common set of QCI definitions across the NPSBN facilitates interoperability by ensuring there is a common way to describe the QoS requirements of all applications which use the NPSBN. Use of the standardized set of QCIs defined in the table below also facilitates roaming onto commercial networks – as these networks also use the same standard definitions of QCI defined in TS 23.203.

Table 4: QoS Class Identifiers (Excerpted from table 6.1.7 of 3GPP 23.203 V9.11)

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services
1	GBR	2	100 ms	10^{-2}	Conversational Voice
2		4	150 ms	10^{-3}	Conversational Video (Live Streaming)
3		3	50 ms	10^{-3}	Real Time Gaming
4		5	300 ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
5	Non-GBR	1	100 ms	10^{-6}	IMS Signalling
6		6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8		8	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		9			

Recommended Requirements

[31] The NPSBN SHALL support all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.
[32] QoS mechanisms in the NPSBN SHALL comply with 3GPP TS 23.203.

4.7.4 Preemption

Pre-emption is an essential function in the NPSBN to allow appropriate management of the system resources, especially during emergencies. Usage of all 15 ARP values by the NPSBN is essential to provide sufficient priority differentiation for the default and dynamic priority requirements outlined in this section.

Recommended Requirements

[33] The NPSBN SHALL support the usage of all 15 ARP values defined in 3GPP 23.203.
[34] The NPSBN SHALL support the ARP pre-emption capability and vulnerability functions as defined in 3GPP 23.203.

4.7.5 Access Class

Per the 3GPP standards, every UE is assigned to one or more access classes. A UE's assigned access class is used to determine how often it may attempt to establish communications with the LTE network. Per 3GPP standards, Access Class Barring was designed to give certain classes of UE preferential access to the system (e.g. police get preferential access over consumer users on a commercial system). The ultimate goal of the capability is to protect against random access channel congestion at a site resulting from an "access storm" by many UEs at one time.

Under heavy congestion, it is possible to engage Access Class Barring at a given site. Once engaged, certain classes of UE may be substantially delayed from any communication with the NPSBN. This capability is required in the NPSBN primarily in a public/private partnership arrangement where first responders/secondary users as well as commercial users share the Band 14 spectrum and eNBs. Consequently, UEs homed to the NPSBN must be provisioned with an appropriate access class.

Recommended Requirements

[35] The NPSBN SHALL implement a nationwide scheme for assigning Access Classes to public safety users and secondary users following the 3GPP recommendations in TS 22.011, Section 4.2.

4.7.6 IP Network Priority

In order to provide consistent end-to-end treatment of Public Safety traffic, prioritization of NPSBN resources must be provided both over the air as well as within the IP network infrastructure. A traditional practice is to align the priority used by the NPSBN IP network and backhaul technology with the scheduling priority (QoS Class Identifier priority, Section 4.7.3). Failure to align these priorities, for example, may result in low over-the-air packet loss rate, but a high IP transport network packet loss rate. This would create a poor user experience, especially for voice and video applications.

Recommended Requirements

[36] The NPSBN SHALL implement a nationwide scheme for assigning QoS Class Identifier priority to IP network and backhaul priority across the entire NPSBN.

4.7.7 (M)VPN Priority and QoS

Public safety relies on VPN and Mobile VPN technology today to securely transport responder traffic from mobile devices to application servers. For example, secure CJIS queries are encapsulated to provide confidentiality and integrity of the transported citizen information. With (M)VPN technology, a variety of applications (CAD, tactical video, surveillance video, etc.) are typically encapsulated into a single 'tunnel'. Because LTE technology is expected to greatly expand the number and types of multimedia applications available, either multiple (M)VPN tunnels or multiple application flows encapsulated within a tunnel are needed per user to account for the different types of traffic.

The use of a VPN obscures the source of traffic flowing towards a UE. This creates a problem for an application supporting an Rx interface that is unaware of the VPN. This requires an arbitrating function that is Rx and VPN aware is introduced between the application and the EPC.

Recommended Requirements

[37] The NPSBN SHALL support the use of industry standard VPN and MVPN technology, while providing priority and Quality of Service for encapsulated applications.

4.8 Security

The Spectrum Act §6206(b)(2)(A) provides that one duty of FirstNet is to ensure the safety, security, and resiliency of the NPSBN, including protecting and monitoring the network against cyber attack. It is important to note that providing for cyber security requires addressing two distinct types of threats. First, there is the need to protect the network itself from malicious attacks that aim to hamper or interfere with proper operation of the network. Second there is the need to protect identities and information from compromise. In general, specific cyber security mechanisms are designed to address one or both of these threats.

A complete Information Assurance (IA) framework that addresses cyber security involves not only the technical aspects of the security implementation, but also the policies and procedures that form and direct the operational component of the IA implementation. In the same manner that DHS developed a comprehensive view of interoperability, covering Governance, Standard Operating Procedures, Technology, Training and Exercises and Usage, NIST has developed a holistic approach to IA that provides a comprehensive framework for implementing cyber security systems.[31] Cyber security is a multi-dimensional problem and inherently cyber security mechanisms intersect with interoperability considerations on multiple levels. Full treatment of an IA implementation is beyond the scope of the Interoperability Board. Therefore the requirements and recommendations contained in this section are limited to those that are technical in nature and constitute a minimum interoperable security baseline for the NPSBN.

The NPSBN, the collection of state, local and tribal jurisdictional networks and other networks as depicted in Figure 2, will constitute a multitude of security/information domains. SP 800-27 provides a context for discussing information domains:

> *The term information domain arises from the practice of partitioning information resources according to access control, need, and levels of protection required. Organizations implement specific measures to enforce this partitioning and to provide for the deliberate flow of authorized information between information domains. The boundary of an information domain represents the security perimeter for that domain.*
>
> *An external domain is one that is not under your control. In general, external systems should be considered insecure. Until an external domain has been deemed "trusted," system engineers, architects, and IT specialists should presume the security measures of an external system are different than those of a trusted internal system and design the system security features accordingly.*

Figure 13 illustrates a simplified representation of the of the security domains that the NPSBN will interface to.

[31] NIST Special Publication 800-27 Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.

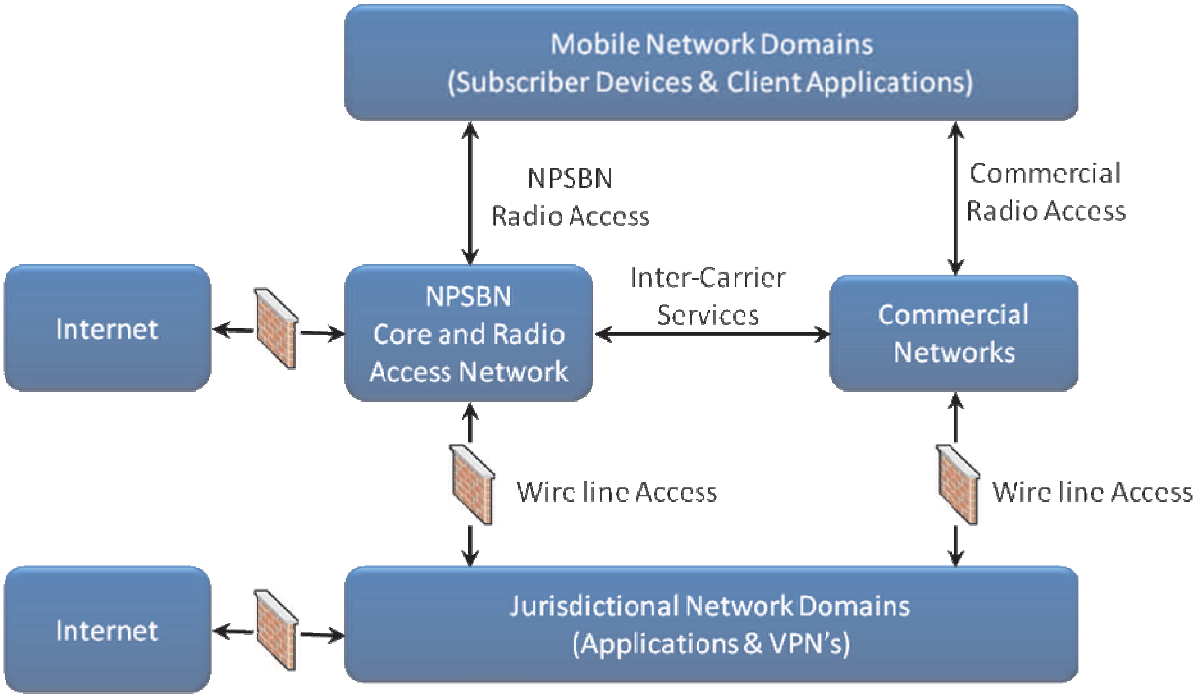


Figure 13: Security Domains

One of the prevailing strategies for dealing with the full spectrum of cyber threats is the implementation of a layered architecture. In SP 800-27 this is described as:

> *Securing information and systems against the full spectrum of threats requires the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. This is due to the highly interactive nature of the various systems and networks, and the fact that any single system cannot be adequately secured unless all interconnecting systems are also secured.*
>
> *By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected. Through user training and awareness, well-crafted policies and procedures, and redundancy of protection mechanisms, layered protections enable effective protection of information technology for the purpose of achieving mission objectives.*

A layered architecture also serves the purpose of enabling overlay of security implementations that are required by jurisdictional entities in accordance with their individual security policies. For example, as described below, LTE provides a variety of security mechanisms that protect the transport network, including the Radio Access Services and the Internetworking of LTE EPC components. Individual jurisdictions may have a need to augment these security mechanisms in order to provide end-to-end protection of sensitive information, or to provide controlled access to network resources, such as through a secure VPN connection that runs on top of the IP transport services provided by the NPSBN.

As noted earlier, full treatment of cyber security for the NPSBN and associated networks is beyond the scope of the Interoperability Board's charter. Therefore, consistent with the focus on minimum technical requirements for interoperability, and the board's working definition of interoperability, specific requirements and recommendations are limited to the transport network, specifically whose boundaries are defined by 3GPP standards. This focus ensures that two distinct interoperability boundaries are treated, consistent with a multi-vendor environment.

- UE to NPSBN (Core and RAN)
- Connectivity between Core and RAN building blocks

The first case ensures uniform and secure access by UEs to NPSBN transport services, where UEs are provided by multiple vendors that are capable of full mobility across the national footprint of the NPSBN. The second case permits implementation of the NPSBN (Core and RAN) with equipment procured from multiple vendors that possibly exists in one or more security domains. A special case that is provided for are State opt out RANs.

4.8.1 Definitions

When discussing security domains in the broad context, involving both LTE and non-LTE components, the following definitions of domain security are used:

- **Intra-domain security** refers to the system connections and components that exist within a unique combination of network components that constitute a security domain.
- **Inter-domain security** refers to the system connections and components that exist within unique collections of network components, each of which constitute a security domain.

The LTE Evolved Packet System (EPS) composed of the Evolved Packet Core (EPC) and E-UTRAN (RAN) is a flat all-IP architecture with separation of control plane and user plane traffic. Distinct security protection mechanisms are applied to each type of traffic, consistent with the security threats being addressed by each LTE security component. At the discretion of FirstNet, the NPSBN may be implemented with one or more security domains. For example, the NPSBN Core and RAN might exist in a single security domain, and State opt out RANs might exist in their own distinct security domains. The 3GPP Security Architecture in TS 33.210 provides the following definitions for this Inter and Intra domain security. These definitions are applicable to components that are covered by the 3GPP standards and not to the broader security context that involves system elements outside the NPSBN

- **LTE Intra-domain security** refers to the RAN and EPC connections and components that exist under the administrative control of a single administrative authority that can apply a level of security controls and policies across network elements and interfaces within that network.
- **LTE Inter-domain security** refers to the connections that inherently exist between separate network administrative domains. To communicate securely between different administrative domains requires coordination and specification of common security controls and policies to ensure interoperable secure interfaces.

4.8.2 Cyber Security Evolution and Mitigation Strategies

Evolution of the cyber security architecture warrants special attention. Given the prolific deployment of LTE on a worldwide basis, this technology standard will experience unprecedented levels of cyber threats. Cyber threats that are successful against commercial LTE networks may pose a direct threat on the cyber security of the NPSBN, particularly if the NPSBN is implemented with the same vulnerabilities that enabled successful attacks on commercial networks. Given the NPSBN's mission, it is prudent to expect that this network will be the subject of direct attacks on a frequent and evolving basis. It is also prudent to expect that evolution of cyber threats will occur at a faster pace than evolution of 3GPP and other standards used in the NPSBN. This is evidenced in commercial markets by the rapid pace at which software vendors distribute security patches compared to the much slower pace at which standards are published and put into practice. For example, LTE releases occur approximately on annual cycles and software security patches to commercial software platforms commonly occur multiple times within a year.

Hence, the Interoperability Board believes it is necessary to afford FirstNet flexibility in addressing rapidly evolving cyber threats, while carefully balancing the somewhat opposing forces of interoperability and security. Therefore, the Interoperability Board recognizes that in response to eminent or present cyber attacks, security policies, implemented by FirstNet, may dictate the need to depart from security requirements contained in the following sections. The goal is to maintain the highest level of security using commercially available standardized security technologies, consistent with a full Cost/Risk/Vulnerability analysis.

The Interoperability Board also recommends that consistent with layered security architecture, mitigation strategies be employed in the event of major breaches in security. For example, the impact of breach at a lower layer in the security architecture can be mitigated through upper layers, and vice versa. One best practice used in security implementations is the use of bypass mechanisms that permit a compromised security feature to be disabled or bypassed.

Recommended Considerations

(43) The NPSBN security implementation SHOULD include pre-planned bypass mechanisms that have defined security and interoperability implications.

4.8.3 3GPP Security Baseline

As a baseline for its recommendations, the Interoperability Board used the existing report titled “Considerations and Recommendations for Security and Authentication” (“PSAC Report”) issued by the Public Safety Advisory Committee (PSAC) commissioned through the Emergency Response Interoperability Center (ERIC) released in May of 2011.[32] While this report was focused on overall network security from a broader perspective, the Interoperability Board felt its work and recommendations were relevant to Interoperability Security.

The Interoperability Board (as well as the PSAC Report) determined that the existing LTE Security Architecture, as outlined in the 3GPP offered the most concise framework around which to develop recommendations. Figure 14 illustrates the LTE Security Architecture.[33] It consists of five security groups. Each security group addresses certain threats and accomplishes certain security objectives:

- (I) Network Access Security – The set of security features that provide users with secure access to services, and which in particular protect against attacks on the (radio) access link.[34]
- (II) Network Domain Security – The set of security features that enable nodes to securely exchange signaling data, user data (between AN and SN and within AN), and protect against attacks on the wire line network.[35]
- (III) User Domain Security – The set of security features that secure access to mobile stations[36]
- (IV) Application Domain Security – The set of security features that enable applications in the user and in the provider domain to securely exchange messages.[37]
- (V) Visibility and Configurability of Security – The set of features that enables the user to determine whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.[38]

[32] Emergency Response Interoperability Center, Public Safety Advisory Committee (PSAC), Considerations and Recommendations for Security and Authentication, Security and Authentication Subcommittee Report, May 2011.

[33] 3GPP TS 33.401 V8.7.0 (20-10-04)

[34] 3GPP TS 33.401

[35] 3GPP TS 33.210

[36] 3GPP TS 33.102

[37] 3GPP TS 33.102 and TS 31.111 is an optional feature

[38] 3GPP TS 33.102 and TS 22.101 is an optional feature

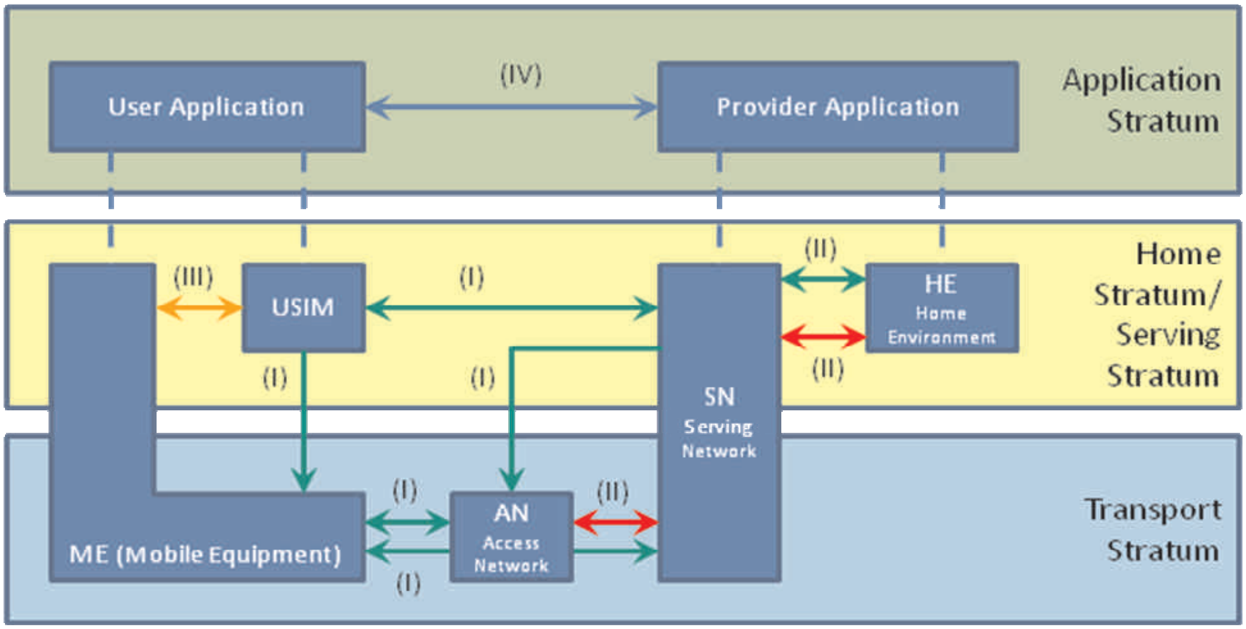
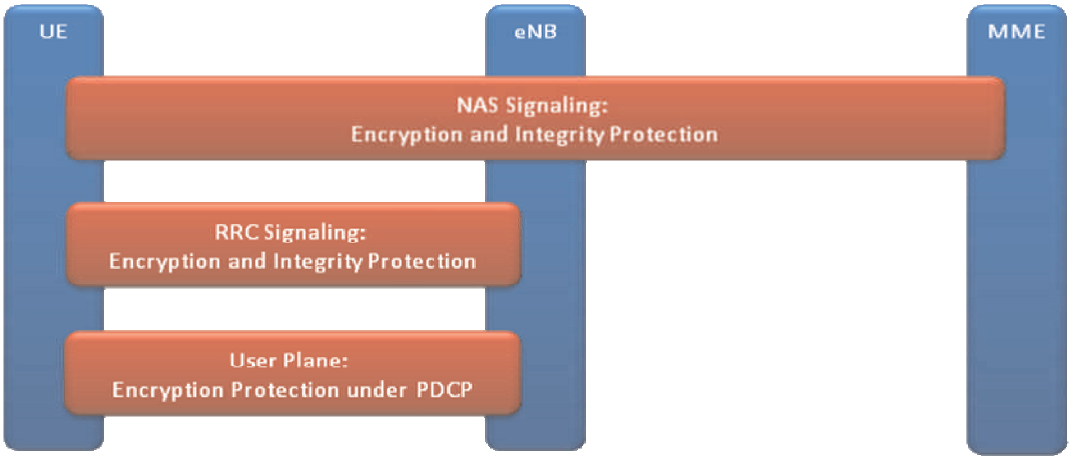


Figure 14: LTE Security Architecture

From this foundation, the Interoperability Board identified the key elements that apply to interoperability.

4.8.3.1 Network Access Security

The UE to EPS interface (radio link) is the most exposed interface and therefore represents heightened security vulnerability. At the same time, a uniform approach to Network Access is required to ensure nationwide mobility, a key component of achieving nationwide interoperability. The 3GPP TS 33.401 Security Architecture shown in Figure 14 defines network access security protocols for UE to RAN and EPC communication, as summarized in Figure 15. In order to ensure interoperable communication between multiple vendors of infrastructure and device equipment, compliance and certification testing to 3GPP security specifications is necessary.



UE
eNB
MME
NAS Signaling:
Encryption and Integrity Protection
RRC Signaling:
Encryption and Integrity Protection
User Plane:
Encryption Protection under PDCP

Figure 15: Network Access Security Protocols

Key functions that implement Network Access Security are:

- Access Control – the eNB ensures that only authenticated UEs are permitted to transmit user data to the eNB. UEs that do not successfully authenticate will be prevented from requesting resources from the network to transmit user data.
- Authentication – the UE/USIM and the NPSBN mutually authenticate each other through the use of a cryptographic authentication algorithm that relies on shared key material in both the UE and the HSS. To perform this authentication, both the USIM and the HSS must agree on the same authentication algorithm

and share a common set of keys.

- Non-Repudiation – Successful authentication by a UE proves to the LTE network that the device has possession of the physical USIM. USIMs are manufactured utilizing strong physical security techniques to protect the keys used for authentication.
- Data Confidentiality and Privacy – To ensure that information is not disclosed to any unauthorized users via the LTE air interface, both control and user traffic is encrypted utilizing 128-bit AES.
- Data Integrity – 3GPP does not define the use of an integrity algorithm for user data. There are however, integrity algorithms used for all UE-eNB and UE-MME signaling messages.

Interoperable network access security therefore relies on:

- Coordination of the generation of the USIMs with the provisioning and activation of UE devices within the NPSBN HSS is required.
- Enabling HSS to MME signaling so that authentication can be performed. This is required when the UE is attaching to the NPSBN from any eNB in the NPSBN and must also be possible when the UE is roaming to a commercial LTE service provider.
- Enabling the 3GPP defined (but optional per the standard) over the air encryption and integrity features.

Recommended Requirements

[38] The NPSBN SHALL use a nationwide common security profile for user plane and control plane traffic between UEs, eNBs and MMEs, in accordance with 3GPP LTE Network Access Domain protocols. The profile SHALL be based on 3GPP TS 33.401, and will be determined by FirstNet based on a system design and other considerations as it deals with evolving cyber threats. As a minimum, the profile SHALL include specification of ciphering algorithms (for example, use of AES-128 vs. SNOW 3G).

[39] The nationwide common security profile SHALL include ciphering of control plane traffic in order to provide for interoperable cyber protection of the network. Ciphering of user plane traffic is optional and is based on policy decisions that involve FirstNet and user agencies.

[40] To enable interoperable authentication, the USIM and HSS SHALL be capable of supporting the same key derivation functions, such as Milenage per 3GPP TS 35.205, 35.206.

Recommended Considerations

As of the writing of this report, TS 33.401 specifies two different algorithms for 128-bit encryption and message authentication, SNOW 3G and AES.

(44) Equipment used in the NPSBN SHOULD support AES and SNOW 3G algorithms.

The intention is to ensure cryptographically agile deployments that can be reconfigured to utilize an alternative encryption standard (SNOW 3G) if exploits to the 128-bit AES algorithm are discovered.

4.8.3.2 Network Domain Security

The Interoperability Board recommends that FirstNet define the networks, identify the domains of the system, and then apply consistent security policies for interfaces both internal to domains under the control of the NPSBN and also between domains. In the following figure the administrative Domain A controls NE1, NE2 and NE3 and determines the security controls and policies for communication between these network elements. The same is true with the equipment in administrative Domain B for NE4, NE5 and NE6. The interface between these two distinct administrative domains is governed by interoperable security controls and policies. 3GPP TS 33.210 specifies the use of IPSec as the Inter-Domain security control.

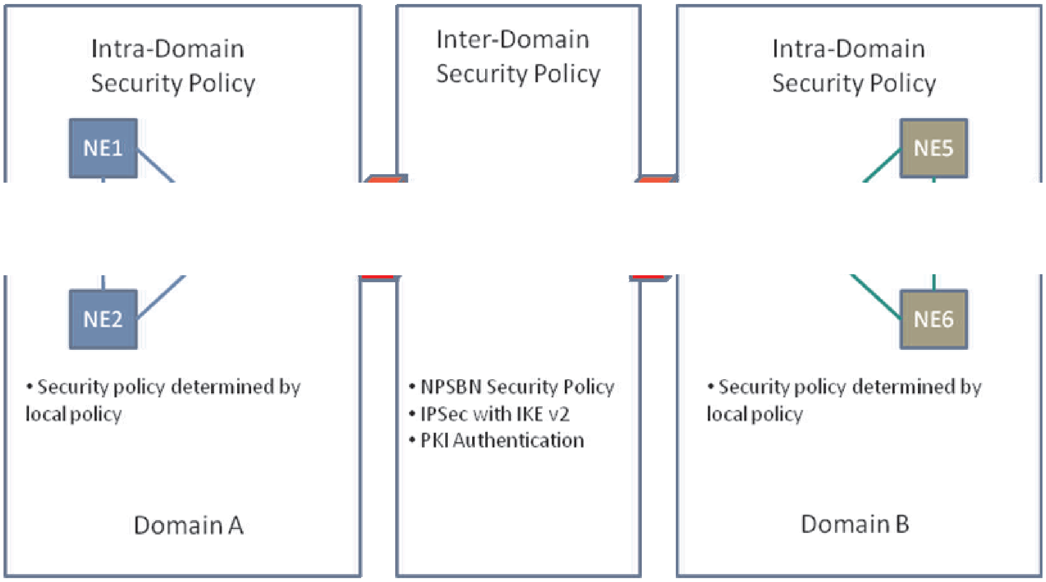

Intra-Domain Security Policy
Inter-Domain Security Policy
Intra-Domain Security Policy
NE1
NE5
NE2
NE6
• Security policy determined by local policy
• NPSBN Security Policy
• IPSec with IKE v2
• PKI Authentication
• Security policy determined by local policy
Domain A
Domain B

Figure 16: Intra-Domain and Inter-Domain Illustration

Due to the expected threat profile that the NPSBN will be faced with, as noted below, the Interoperability Board recommends that Intra-Domain security controls that are considered optional by 3GPP be required for the NPSBN network deployment. In particular, RANs that rely on long-haul transport networks potentially utilizing commercial and private/government IP wide area network interfaces should secure communication with the EPC utilizing IPSec.

A public key infrastructure is important to provide a scalable key management for the inter-domain interfaces of the NPSBN. To create a PKI, FirstNet would need to establish the policies, procedures, hardware, software and personnel responsible for creation, management, distribution, use, storage, and verification practices of the digital certificates that provide the key material for the network.

Although the Interoperability Board is chartered with identifying Interoperability requirements for the NPSBN, the Interoperability Board recommends that FirstNet undertakes a security risk assessment on the internal interfaces of administrative domains. In particular the Interoperability Board recommends that the NPSBN utilize IPSec to secure network interfaces that cross wide-area network interface such as between the eNB and the EPC.

Figure 2 illustrates the control and user data network interfaces that could potentially fall within the NPSBN. Many of the interfaces that extend from the NPSBN externally will require inter-domain security controls. The Interoperability Board recommends that inter-domain security controls and policies be applied to:

- Ref 3: All S1 interfaces to commercial or PPP networks that transport S1.
- Ref 5: All IP Exchange DCH/FCH, S6a, S8, and S9.
- Ref 6: All IP traffic between the NPSBN and Public Safety Application networks (e.g. public safety agencies).
- Ref 7: Note: IMS specifies the use of IPSec between the UE and the P-CSCF which would occur on top of the Sgi interface within the diagram's Ref 14 interface; however the user data plane is not similarly protected by IMS.
- Ref 8: This interface represents an open interface to the Internet. As such, it is assumed that UE's who utilize an APN from the Public Internet will be sufficiently hardened.
- Ref 15: LTE mobility interfaces to a Waiver Core.

Recommended Requirements

[41] Network Domain Security SHALL be implemented in accordance with 3GPP TS 33.210, which stipulates the use of IPSec to protect IP communication between administrative domains (including all network connections used to interconnect the domains).
[42] The NPSBN SHALL comply with TS 33.310 as the authentication framework for Public Key Infrastructure to authenticate these network interfaces.
[43] In order to ensure secure and interoperable interfaces between the NPSBN and external elements (e.g. all SGi, Rx and Srvs services as shown in Figure 2), these interfaces SHALL be protected with a FirstNet-approved security mechanism.

Recommended Considerations

(45) FirstNet SHOULD establish the security controls and policy for inter-domain security and require that all parties (e.g. public safety agencies) who connect to the NPSBN utilize FirstNet-approved cipher suites.
(46) FirstNet SHOULD consider using IPSec interfaces that utilize IKEv2 and utilize PKI to authenticate the peers of the IPSec Security Associations.
(47) When EPS elements are located in trusted locations without wide area communication links between them, the use of network domain security SHOULD be optional.
(48) Network interfaces between domains SHOULD be monitored and intrusion detection/prevention tools SHOULD be deployed.
(49) The developed security mechanisms SHOULD permit local entities to hide the topologies and address spaces of their networks.

4.8.3.3 User Domain Security

Per 3GPP Standards, User Domain Security involves two features:

User-to-USIM authentication:

> *This feature provides the property that access to the USIM is restricted until the USIM has authenticated the user. Thereby, it is ensured that access to the USIM can be restricted to an authorised user or to a number of authorised users. To accomplish this feature, user and USIM must share a secret (e.g. a PIN) that is stored securely in the USIM. The user gets access to the USIM only if he/she proves knowledge of the secret. This security feature is implemented by means of the mechanism described in TS 31.101.*

USIM-Terminal Link

> *This feature ensures that access to a terminal or other user equipment can be restricted to an authorised USIM. To this end, the USIM and the terminal must share a secret that is stored securely in the USIM and the terminal. If a USIM fails to prove its knowledge of the secret, it will be denied access to the terminal. This security feature is implemented by means of the mechanism described in TS 22.022.*

Recommended Requirements

[44] User Domain Security SHALL be implemented in accordance with 3GPP TS 33.102, TS 31.101, and TS 22.022.

4.8.3.4 Application Domain Security

Application Domain Security enables for secure messaging between the USIM and the network (TS 33.102).

> *USIM Application Toolkit, as specified in TS 31.111 [15], provides the capability for operators or third party providers to create applications which are resident on the USIM (similar to SIM Application Toolkit in GSM). There exists a need to secure messages which are transferred over the network to applications on the USIM, with the level of security chosen by the network operator or the application provider.*

> *Security features for USIM Application Toolkit are implemented by means of the mechanisms described in TS 23.048 [7]. These mechanisms address the security requirements identified in TS 22.048 [16].*

Recommended Requirements

[45] USIM-based applications that require messaging between the USIM and network components SHALL implement Application Domain Security in accordance with 3GPP TS 33.102 and TS 31.111.

4.8.3.5 Visibility and Configurability of Security

In some public safety use cases, it is desirable or even necessary to provide user feedback concerning the security level that a user device is operating (such as Secure or Not Secure). 3GPP LTE standards provide mechanisms for:

- indication of access network encryption: The property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up.
- indication of the level of security: The property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with a lower security level.

The ciphering indicator feature is specified in 3GPP TS 22.101.

3GPP TS133.102 describes configurability as:

> *Configurability is the property that the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user, are in operation. The following configurability features are suggested:*
>
> - Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication, e.g. for some events, services or use;
> - Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;
> - Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;
> - Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.

As noted in the ERIC PSAC report, user control of security parameters or their usage is not a generally accepted practice in public safety.

Recommended Requirements

[46] In such cases where visibility is required for devices on the NPSBN, the implementations SHALL comply with 3GPP TS 33.102 and TS 22.101.

4.8.4 Support for Jurisdictional Security Policies

It is essential that the NPSBN support layered security policies that permit jurisdictions to implement their unique security policies, provided that doing so does not compromise the overall security of the NPSBN. Inherently, a jurisdictional security implementation, layered on top of the NPSBN will only be interoperable to users authorized by the jurisdictional security authority. While these layered security mechanisms must be supported, doing so must not be to the detriment of interoperability for users that are not part of that security domain. For example, a jurisdiction may require a particular 2-factor authentication scheme in connection with a secure VPN, based on a commercially available technology. The secure VPN will limit access to a network domain to only authorized users. It is important that this VPN does not have a negative impact to users that are not part of that network domain.

Recommended Considerations

(50) Security mechanisms layered by a jurisdiction on top of the NPSBN SHOULD NOT inhibit interoperability for users visiting from outside of the security domain in which it is implemented.

4.8.5 Roaming

Section 6206(c)(5) of the Spectrum Act permits FirstNet to enter into roaming agreements with commercial network providers. There are many security implications for these roaming agreements that will require robust risk/threat/vulnerability analysis. Of particular concern is the possibility that implementation of these agreements could undermine the security requirements contained in this document. As an example, with 3GPP technologies, a user device is authenticated in the Home Network, and not in the visited network. Therefore, a user device homed to a commercial network would be authenticated by the commercial network and not the NPSBN. If the commercial network operates with an authentication implementation that is less stringent than the NPSBN, a form of "bidding-down" of security requirements will occur for users that are homed on a commercial network but operating on the NPSBN RAN and Serving network. FirstNet will need to balance the security requirements with meeting an interoperability goal of this board: to utilize commercially adopted standards.

Recommended Considerations

(51) As FirstNet enters into roaming agreements with commercial partners, security policies SHOULD be implemented that ensure integrity of the NPSBN and that NPSBN security practices are not compromised.

4.8.6 Identity Management and Identity Federation

3GPP standards implement security mechanisms such as authentication from a device perspective, specifically the UE. While these mechanisms are built on sound security principles, they do not support many of the use cases that are important in public safety. There is growing consensus at all levels of government that there is the need to provide authentication not only for user devices, but also for individuals that have access to the NPSBN and for data objects that are accessible by authorized users.

With the proliferation and mobility of devices it will be imperative that the NPSBN ensure that not only are devices authenticated, but that those attempting to use those devices are also authenticated. Because first responders are often asked to support other agencies in mutual aid scenarios, an open, standards based, federated identity management framework is essential to enable users to have interoperable access to applications and data when authorized to do so. Without an Identity Management framework, application authentication would require unique credentials for each application or applications within an administrative domain and between administrative domains. Such proliferation of access credentials will quickly become a barrier to usability and therefore interoperability if first responders are expected to manage credentials for many different such networks and applications. In such situations it is common for users to replicate the same passwords or write down passwords thereby weakening the security of the system as a whole. We recommend that a framework that retains control of a user's identity by their home agency yet permits these identities to be trusted by applications hosted by other agencies and applications be established. One potential solution has been identified by the Interoperability Board from the DHS/DOJ/HSS National Informational Exchange Model.

Although the NPSBN framework for user identity management provides strong verification of the identity of the user, the information that the user is authorized to access must be determined by the entity that controls the information.

Recommended Considerations

(52) FirstNet SHOULD consider supporting implementation of a national framework for user identity management.

(53) FirstNet SHOULD consider supporting implementation of a national framework for user identity federation to enable user interoperability across administrative domains within the NPSBN, where authorized.

(54) Implementation of the national framework for user identity management and federation SHOULD include a set of guidelines and rules for applications to participate in the national identity management framework.

(55) The agency, organization or entity that utilizes the NPSBN Identity Management framework SHOULD be responsible for enforcing authorization constraints on access to information as per their own security policy.

5 Conclusions

The establishment of minimum technical requirements to ensure a nationwide level of interoperability may seem like a relatively straightforward task. Long Term Evolution (LTE), after all, is based on a set of international standards (3GPP) which are being widely deployed in functioning commercial networks around the world. When one realizes the long term implication of these minimum requirements to the most critical function of government - ensuring the safety of its citizens - the task takes on an added level of gravity and complexity.

This gravity and complexity was noted by Deputy Assistant Secretary Anna Gomez in her remarks before the Interoperability Board on April 23, 2012. In describing the requirements the Interoperability Board was charged with developing, Deputy Assistant Secretary Gomez said "we [NTIA] view [them] as a constitution." This analogy was recalled at numerous times during the Interoperability Board's deliberations as it considered aspects of its work that protected the constituency of the NPSBN (public safety) and the role of those that would govern the NPSBN (FirstNet).

One of the most difficult issues the Interoperability Board dealt with throughout its deliberations was the very thin line that often exists between operability and interoperability. Establishing minimum requirements without a clear understanding of why they are important and how they should be used (operability) is analogous to the United States Constitution without the Federalist Papers. Just as the Federalist Papers are key to the understanding of our Constitution, the informative comments and recommendations made in this document are critical to understanding and implementing the minimum technical requirements for interoperability in a way that ensures operability. While these informative comments and recommendations do not rise to the level of an "incomparable exposition of the Constitution" as historian Richard B. Morris said of the Federalist Papers, the Interoperability Board believes them to be critical to the development of the NPSBN and to its overall success.

In finalizing its set of recommended requirements, the Interoperability Board carefully assessed the sometimes competing components of its relevance tests. There were many discussions around the following topics:

- Whether draft requirements could be considered "minimum technical requirements" as mandated by the Spectrum Act
- Whether draft requirements addressed operability or interoperability
- Whether draft requirements were technical or operational
- Striking a proper balance between granting FirstNet the flexibility it will need to build and maintain the NPSBN while providing the specificity needed to both set a proper course for FirstNet and give the FCC useful tools to determine whether to approve State opt-out plans
- The proper of level of detail to specify requirements in the absence of a nationwide network architecture
- How best to ensure interoperability is maintained as FirstNet and LTE technology evolves

In all its discussions, the Interoperability Board members considered the valuable input it received through the filings in the Docket and its Public Workshop, and the important contributions made by the Consulting Agencies.[39]

The Interoperability Board expresses its gratitude to the Consulting Agencies and subject matter experts that gave many hours of their time to this effort. The Interoperability Board extends a special thanks to the staff of the Public Safety and Homeland Security Bureau of the FCC, without whose support the Interoperability Board could not have accomplished its task. Through this unique collaboration between 15 Interoperability Board members, many SMEs, the Consulting Agencies and the public, the Interoperability Board was able to achieve its legislative mandate in the allotted 60 days. The Interoperability Board is confident that its recommended minimum technical requirements will provide a solid foundation for the successful development of the NPSBN.

[39] Federal Communications Commission Public Notice DA 12-474.

Appendix 1: Public Safety Emergency Services

NPSTC's Priority and QoS Task Group has developed an initial set of functional requirements for a collection of public safety functions, broadly classified in this report as Public Safety Emergency Services.[40] NPSTC continues to develop these key functional requirements for public safety use of the NPSBN to support its mission critical needs. The Interoperability Board recognizes the importance of these functions and the importance of ensuring that these functions eventually are implemented in a fully interoperable manner. Consequently, this informative appendix is included to foster continued dialog by FirstNet, the public safety community and the eco-system that will eventually supply these capabilities to our nation's first responders.

Responder Emergency

Similar to an emergency button on today's LMR radios, activation of this capability provides priority to the first responder's voice service, but also notifies dispatchers and other appropriate personnel of the life-threatening condition. If implemented in the NPSBN at some time in the future, this critical feature must be interoperable across the NPSBN. It is also essential that open standards be developed for this feature and adherence to these standards be validated through testing. For informational purposes, we include the functional requirements developed by NPSTC's Priority and QoS Task Group:

- Provision of standard mechanisms to activate and clear a Responder Emergency by the responder's UE, by a 3rd party via UE (such as a field command tablet), and by 3rd party via a back-end application (such as a dispatch terminal).
- Ability for a responder's agency to define the applications used when one of the agency's responders activates the Responder Emergency capability.
- Activation of the Responder Emergency function provides the highest ARP priority level for emergency applications.
- When activated, Responder Emergency preempts other lower-priority applications on the NPSBN if necessary, in order to obtain resources. Applications used when the Responder Emergency function is activated are prohibited from being preempted.

Immediate Peril

Because all application types (voice, video, data) share a single set of LTE resources, this presents public safety with a new problem not present in LMR systems. A static (default) ordering of application types typically de-prioritizes video and other high-bandwidth applications. This creates a strong lack of flexibility in the framework and likely would prevent video from becoming mission critical. To address these needs, NPSTC's Priority and QoS Task Group defined functional requirements for a prioritization feature which allows a normally de-prioritized application to be "re-prioritized" by the NPSBN for a specific first responder, in the event of an *imminent threat to human life*. (We note that this is one example of how such functionality could be implemented. The discussion in this section is not intended to constrain the NPSBN from using other ways of providing this functionality, if needed.)

If such a feature is supported on the NPSBN, it must be interoperable across the NPSBN. Furthermore, open standards must be developed for this feature and adherence to these standards be validated through testing before it is supported on the NPSBN. For informational purposes, we include the functional requirements developed by NPSTC's Priority and QoS Task Group:

- Provision of a standard mechanisms to activate and clear Immediate Peril by the responder's UE, by a third party via UE (such as a field command tablet), and by a third party via a back-end application (such as a dispatch terminal).
- Ability for the entity initiating the Immediate Peril condition to be able to select the application(s) to receive heightened ARP priority level.
- The ability to utilize both the Responder Emergency and Immediate Peril capabilities from the same entity.

[40] NPSTC Broadband Working Group – Priority and QoS Task Group – Priority and QoS in the Nationwide Public Safety Broadband Network, Rev 1.0, April 17, 2012.

Responder Emergency and Immediate Peril are fundamentally different capabilities and are differentiated by: (1) who chooses the applications to be prioritized, and (2) pre-emption capabilities.

Incident Command System Incident Priority

In an effort to improve mutual aid and the overall ability for responders to work together, the National Incident Management System (NIMS) was developed by DHS and issued in 2004. A best practice that was incorporated into NIMS was the Incident Command System (ICS). ICS is a nationally standardized incident organizational structure for on-scene management of all-hazards incidents. It incorporates a Unified Command (UC) approach, whereby individuals designated by their jurisdictional authorities jointly determine objectives, plans and priorities and work together to execute them. ICS is commonly used today for incident command and control. Key elements of ICS are (1) standardized incident classification and (2) standardized roles within a given incident organizational chart.

NPSTC's Priority and QoS Task Group determined a linkage between standard ICS management practices and standard LTE priority and QoS was needed. In effect, this linkage provides public safety with needed per-incident prioritization capabilities. Without this capability, the NPSBN will be unable to distinguish resources for a four-alarm fire from a minor traffic accident.

Traditionally, incident classification is performed by the Computer Aided Dispatch (CAD) terminal or the ICS COML (communications unit leader) command application. Once this classification is made, an association with NPSBN priority can be made.

Jurisdictional Priority

A first responder's jurisdiction is their day-to-day operating area to which they are normally accountable for their function. For example, federal agents may have a jurisdiction which is the entire U.S. territory and local responders may have a jurisdiction the size of a portion of one city. The definition of jurisdiction is relative to the responder's agency.

There are a variety of reasons for a responder to exit their jurisdictional area. Examples:

1. Driving to court
2. Training
3. Vehicle maintenance
4. Going home or on vacation

Given these example scenarios, it is possible for a responder's UE to unintentionally consume critical resources needed by another jurisdiction. For example, a responder driving to court may stream video from their vehicle in the same cell as a four-alarm fire. Jurisdictional priority is intended to modify (typically lower) a UE's ARP priority level when the UE is operating outside its normal jurisdictional area. This prevents accidental use of critical resources in a cell.

However, there are reasons for a responder to operate outside their normal jurisdictional area and still have priority, such as when they provide assistance in a mutual aid incident.

If such a feature is supported on the NPSBN, it must be interoperable across the NPSBN. Further, open standards must be developed for this feature and adherence to these standards be validated through testing before it is supported on the NPSBN. For informational purposes, we include the functional requirements developed by NPSTC's Priority and QoS Task Group:

- Ability to define and store a jurisdictional area.
- Ability to assign a UE to a home jurisdictional area.
- Ability to allow the local jurisdiction full control of priorities of home and visiting users within the nationwide framework.

Appendix 2: Trusted Delivery Process

The NPSBN is expected to be a highly secure network that will invite cyber attacks because of its highly critical role. A process, defined here as the Trusted Delivery Model, would provide an additional level of scrutiny to help prevent intrusive attacks on the infrastructure elements that would impair or compromise the operation of the NPSBN.

The Trusted Delivery model provides a guideline for applying security assurances to the delivery of network infrastructure hardware, software and firmware. There is not a prescribed standard, but this approach has been adopted by at least one service provider in the United States and one in Canada. The model has four key attributes.

1. An independent assessor is selected by the equipment provider and approved by FirstNet. The assessor does not have to be the same for all equipment.
2. The hardware, software and firmware of the equipment provider are evaluated by the independent assessor. The evaluation identifies security vulnerabilities, malware, Trojans, back door access, and other potentially illicit code. Problematic code is identified to the equipment supplier for corrective action.
3. The hardware, software and firmware delivery method must also be reviewed by the assessor to insure the independently certified equipment is the equipment delivered for installation. This process is also followed for upgrades, maintenance releases and patches.
4. The software and firmware source code should be held in escrow in an independent U. S. based facility to insure a certified copy is always available.

In order to implement this model, these requirements should be included in the Request for Proposal and language inserted in the procurement contract. The Interoperability Board recognizes that this is an emerging area but recommends this as a best practice for the high level of security required for the NPSBN.

Appendix 3: Supporting Agencies and Individuals

The Interoperability Board would like to thank these organizations and individuals for their contributions to the development of the minimum technical requirements recommendations for interoperability. This work could not have been completed without their dedication to the development of the NPSBN.

- **State of Nebraska**
  - Jayne Scofield, IT Administrator
  - Mike Jeffres, Public Safety Systems Manager
  - Matt Schnell, Nebraska Public Power District

- **City of Charlotte**
  - Steve Koman, Public Safety LTE Program Manager
  - Randy Moulton, Chief Security Officer

- **Federal Communications Commission**
  - The staff of the Public Safety and Homeland Security Bureau
  - The staff of the Office of the Managing Director

- **Department of Commerce, National Telecommunications and Information Agency**
  - Regina Harrison
  - Jeffrey Bratcher
  - Dan Phythyon
  - Andrew Thiessen
  - D.J. Atkinson

- **Department of Homeland Security, Office of Emergency Communications**
  - Robert Rhoads

- **National Institute of Standards and Technology**
  - Emil Olbrich

- **Alcatel-Lucent**
  - Wim L. Brouwer
  - Tewfik L. Doumi

- **Harris**
  - Dan Ericson
  - Tom Hengeveld
  - Reid Johnson
  - Patrick Sullivan

- **MetroPCS**
  - Bejoy Pankajakshan

- **Motorola Solutions**
  - Craig Ibbotson
  - Frank Korinek
  - Trent Miller
  - Craig Reilly
  - Gino Scribano
  - Steve Upp

- **Panhandle Wireless**
  - Patrik Ringqvist (Ericsson)
  - G.S. Sickand (Ericsson)

- **Sprint Nextel**
  - Seth Jones
  - Jill Rabach
  - Mark Vangerpen

- **Verizon**
  - David Andersen
  - Bruce Ciotta
  - Renato Delatorre
  - Renitta Burt Geiger

- **Public Workshop Participants**
  - Brian Fontes, CEO, National Emergency Number Association
  - Anna Gomez, Deputy Assistant Secretary for Communications and Information, National Telecommunications and Information Administration
  - Robert LeGrande, Advisor to the City of Baton Rouge, LA
  - Jeff Cohen, Chief Counsel – Law and Policy Director of Government Relations, Association of Public-Safety Communications Officials (APCO)
  - Tom Sorley, Chair, National Public Safety Telecommunications Council (NPSTC) Technology Committee
  - Ajit Kahaduwe, Head of Industry Environment – North America, Nokia Siemens Networks
  - Patrik Ringqvist, Vice President, Wireless Network Solutions, Ericsson
  - Martin Dolly, Lead Member of the Technical Staff, Core Network and Government Regulatory Standards, AT&T
  - Pat Amodio, Chief Engineer, DHS Joint Wireless Program Management Office, U.S. Customs and Border Protection
  - Roger Quayle, Chief Technology Officer and Co-Founder, IPWireless
  - Robert Wilson, Telecommunications Manager, Wyoming Department of Transportation, State of Wyoming
  - Scott C. Somers, Vice Mayor, Mesa City Council, City of Mesa, AZ
  - Mark Adams, Director, Principal Architect, Networks and Communications, Northrop Grumman
  - Thomas Farley, Senior Systems Engineer, Network Centric Systems, Raytheon
  - Matt Schnell, Supervisor of Telecommunications, Nebraska Public Power
  - Mark Althouse, Technical Director – Mobility Mission Management, National Security Administration

Appendix 4: List of Acronyms

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AMBR	Aggregate Maximum Bit Rate
AN	Access Network
ANDSF	Access Network Discovery and Selection Function
API	Application Programming Interface
APN	Access Point Name
APN-AMBR	APN Aggregate Maximum Bit Rate
ARP	Allocation and Retention Priority
AS	Access Stratum
ATP	Acceptance Test Procedure
BD	Billing Device
BGP	Border Gateway Protocol
CAD	Computer Aided Dispatch
CALEA	Communications Assistance for Law Enforcement Act
CDF	Charging Data Function
CDMA	Code Division Multiple Access
CGF	Charging Gateway Function
CGW	Charging Gateway
CJIS	Criminal Justice Information Services
COML	Communications Unit Leader
ConnMO	Connection Management Object
CTIA	Cellular Telecommunications Industry Association
DA	Delegated Authority
DHS	Department of Homeland Security
DHS OEC	Department of Homeland and Security Office of Emergency Communications
DCH	Data Clearing House
DL	Downlink
DM	Device Management
DOJ	Department of Justice
DNS	Domain Name System
DoS	Denial of Service
DUT	Device Under Test
EAP	Extensible Authentication Protocol
eHRPD	Enhanced High Rate Packet Data
eMBMS	Evolved Multimedia Broadcast Multicast Service
EMS	Emergency Medical Services
eNB	Evolved Node B
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EPC	Evolved Packet Core
EPS	Evolved Packet System
ERIC	Emergency Response Interoperability Center
ESI Net	Emergency Services IP NETwork
ETS	Enabler Test Specifications
E-UTRAN	Evolved Universal Terrestrial Radio Access
EvDO	Evolution Data Optimized
FCC	Federal Communications Commission
FCH	Financial Clearing House
FOA	First Office Application
FTP	File Transfer Protocol
FUMO	Firmware Update Management Object
GBR	Guaranteed Bit Rate
GCF	Global Certification Forum
GoS	Grade of Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSMA	GSM Association

HE	Home Environment
HLR	Home Location Register
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
IA	Information Assurance
ICIC	Inter-Cell Interference Coordination
ICS	Incident Command System
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IOT	Interoperability Testing
IPX	Internet Packet Exchange
IT	Information Technology
ITU	International Telecommunication Union
LAWMO	Lock and Wipe Management Object
LBS	Location Based Services
LMR	Land Mobile Radio
LTE	Long Term Evolution
MCV	Mission Critical Voice
ME	Mobile Equipment
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MVPN	Mobile Virtual Private Network
NAS	Non Access Stratum
NAT	Network Address Translation
NDA	Non Disclosure Agreement
NENA	National Emergency Number Association
NG	Next Generation
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NPSAN	Nationwide Public Safety Application Network
NPSBN	Nationwide Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OMB	Office of Management and Budget
OS	Operating System
OSINT	Open Source Intelligence
PCRF	Policy Charging and Rules Function
PCS	Personal Communications System
PDN	Packet Data Network
P-GW	Packet Data Gateway
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PPP	Public Private Partnership
PRD	Permanent Reference Document
PSAC	Public Safety Advisory Committee
PSAN	Public Safety Application Network
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTCRB	PCS Type Certification Review Board
PTT	Push To Talk
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAP	Returned Accounting Procedure
RAT	Radio Access Technology
RFP	Request for Proposal
RMS	Records Management System
RRC	Radio Resource Control
RRM	Radio Resource Management

SAML	Security Assertion Markup Language
SDO	Standards Development Organization
SEG	Security Gateway
S-GW	Serving Gateway
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SN	Serving Network
SOA	Service Oriented Architecture
SRVCC	Single Radio Voice Call Continuity
SUPL	Secure User Plane Location
TAP	Transfer Accounting Procedure
TBD	To Be Determined
UC	Unified Command
UE	User Equipment
UICC	Universal Integrated Chip Card
UL	Uplink
UMTS	Universal Mobile Telecommunications System
USAT	Universal Subscriber identity module Application Toolkit
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
V-CDF	Visited Charging Data Function
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VoLTE	Voice over LTE
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPS	Wireless Priority Service