NATIONAL PUBLIC SAFETY TELECOMMUNICATIONS COUNCIL

NPSTC

700 MHz Public Safety Broadband Task Force Report and Recommendations

Chair David Buchanan
Operations Work Group Co-Chairs Dan Hawkins and David Troup
Technical Work Group Co-Chairs Andrew Thiessen and Emil Olbrich
Governance Work Group Co-Chairs Laura Phillips and Bill Schrier

September 4, 2009

Table of Contents

1 Executive Summary 5

2 Introduction, Objectives, Process, and Organization 6

2.1 Introduction and Objectives 6

2.2 Process 7

2.3 Organization 8

3 Operations Work Group 9

4 Technical Work Group 9

5 Governance Work Group 9

6 Recommendations 10

6.1 General 11

6.1.1 Regional Operator Advisory Group 11
6.1.2 D Block Spectrum 11
6.1.3 Public/Private Partnerships 12
6.1.4 Common Clearinghouse 12
6.1.5 Equipment and Features Test Facility 12

6.2 Operations 13

6.2.1 Internet Access -Required 13
6.2.2 VPN Access to any Authorized Site and to Home Networks - Required 13
6.2.3 Status/Information "Homepage" - Required 13
6.2.4 Status/Information "SMS-MMS Messaging" - Required 13
6.2.5 Access to Responders under Incident Command System (ICS) – Required 13
6.2.6 LMR Gateway Devices - Required 14
6.2.7 Field-Based Server Applications - Required 14
6.2.8 Location Based Data Capability - Desired 14
6.2.9 One-To-Many Communications across All Media - Desired 14
6.2.10 LMR Voice - Desired 14
6.2.11 PSTN Voice – Desired 15

6.3 Technical 15

6.3.1 System Identifiers 15
6.3.2 Minimum Applications 20
6.3.3 Security 21

6.4 Governance 21

6.4.1 FCC Rule Changes 21
6.4.2 PSBL Spectrum Lease to Regional Operators 21
6.4.3 Use of Spectrum 22

7 Conclusions 22

8 Appendix A: BBTF Assumptions 23

8.1 Spectrum 23

8.2 Waivers 23

8.3 Use of Recommendations 23
8.4 Additional Spectrum 23
8.5 No Duplication of Effort 23
8.6 Regional Network Cooperation 23
8.7 Cooperating Agencies and Agreements 23
8.8 Operating Protocols 23
8.9 National Network 24
8.10 Broadband Access 24
8.11 Build Out of Networks 24
8.11.1 Public Safety (PS) Entity 24
8.11.2 Service Operator 24
8.11.3 Shared Equipment 24
8.11.4 Service Operator with Commercial Access 24
8.12 Nationwide Network Compatibility 25
9 Appendix B: BBTF Definitions 25
9.1 National Broadband Data System 26
9.2 Regional System (Regional Network) 26
9.3 Spectrum Lease 26
9.4 Intra-system Roaming 26
9.5 Inter-system Roaming 26
9.6 Interoperability 26
9.7 First Responder 27
9.8 Emergency Response Support 27
10 Appendix C: Term Sheet 27
11 Appendix D: Roaming White Paper 31
Roaming and the Shared Wireless Broadband Network 31
12 Appendix E: Operations WG Working Documents 36
12.1 Concept of Operations 36
12.2 Task Definition 37
12.3 Terms and Definitions 37
12.4 Assumptions 37
12.5 Operational Requirements 38
13 Appendix F: Technical WG Working Documents 48

Technical Working Group 48

700 MHz LTE Network Interoperability 48

13.1 Scope 48

13.2 48

13.3 Table of Contents 48

13.3.1 LTE Network and Device Specifications 50
13.3.2 System Identifiers 51
13.3.3 Frequency Spectrum 55
13.3.4 Network Interfaces 56
13.3.5 Mobility and Handover Implications 60
13.3.6 Inter-network Authentication and Connectivity 61
13.3.7 Devices 62
13.3.8 Standards Testing 62
13.3.9 Applications and Quality of Service 63
13.3.10 LTE Security 65
13.3.11 Appendix 1 - Definitions 67
13.3.12 Appendix 2 – Commercial and non-3GPP roaming 72
13.3.13 Appendix 3 – PLMN ID Info 77
13.3.14 Appendix 4 – 3GPP Standards 81

14 Appendix G: Governance WG Working Documents 82

700 MHz Public Safety Broadband Task Force Report and Recommendations

1 Executive Summary

At its June 2009 meeting, the National Public-Safety Telecommunications Council (NPSTC) voted to endorse Long Term Evolution (LTE) as the technology of choice for the Nationwide Broadband Data System (NBDS). At the request of the Public Safety Spectrum Trust (PSST), NPSTC's Governing Board also voted to form a 700 MHz Broadband Task Force (BBTF). Within 60 days, the BBTF was given the mission to develop the minimum recommendations necessary to ensure roaming and interoperability among localities and regions that have submitted waivers to the Federal Communications Commission (FCC) to build out 700 MHz broadband networks ahead of a nationwide network. The instructions to the BBTF were to assume the use of LTE technology and to make recommendations only on the minimum requirements for roaming and interoperability, leaving the regional systems free to design and specify the technical parameters of their systems to meet local needs and giving the freedom to the regional systems to employ any additional requirements and applications needed locally beyond those recommendations in this report. The Task Force also recognized that the regional systems would be part of the NBDS.

The BBTF created three Work Groups (WGs): Operations, Technical, and Governance. The BBTF membership was open to all persons wishing to participate. The work product was openly posted on various websites and the press was invited to monitor and report on the progress of the Work Groups. Each Work Group, after much input and discussion, made recommendations to support the mission and objectives of the BBTF. The specific recommendations are reported in Section Six of this report. Key recommendations include the following.

- The Governance WG recommended the establishment of an Advisory Group made up of representatives of the regional system operators and PSST to continue follow-on work and to provide advice to the PSST Board.
- The key applications recommended by the Operations WG are that the NBDS support roaming and interoperability through Internet and Virtual Private Network (VPN) access, both available in the current release of the LTE standard. These two applications enable the implementation of several other Operations WG recommended applications. The BBTF members strongly support quick approval for the regional operators to start building

systems. The BBTF recognizes that some recommendations and applications may need follow-on work or may not be supported by the current release level of the LTE standard and this should not hold up the approval and quick build out of the regional systems. The Advisory Group should develop timelines for regional systems to fully implement the recommendations in this report, and the Advisory Group should monitor the LTE standards process and recommend features to add to the LTE standard that support the recommendations of this report. The PSST Board should attempt to influence the LTE standards process to adopt those features.

One very important recommendation is that NPSTC and the member organizations of NPSTC, with the PSST and other public safety organizations, should begin a coordinated effort to have the D Block 5+5 MHz of spectrum allocated for public safety use, and licensed to the Public Safety Broadband Licensee (PSBL), currently the PSST. During the work of the BBTF, it was apparent to members that the current 5+5 MHz of spectrum available for public safety use for broadband data systems will not be sufficient to support disaster operations. Also some or many of the regional systems will need to enter into public/private partnerships as described in this report in order to fund implementation and operation of the regional systems. Without the D Block spectrum, there will be insufficient spectrum for these partnerships to most effectively operate.

2 Introduction, Objectives, Process, and Organization

2.1 Introduction and Objectives

Introduction

Following the auction that produced no winning bidder of the D Block license in early 2008, a number of major cities in the United States filed waivers for building and operating in the 700 MHz band. The National Public Safety Telecommunications Council (NPSTC) formed this Task Force to develop a set of minimum requirements for those entities that file a waiver to ensure that those networks are compatible with the Nationwide Broadband Data System (NBDS)[1] and to guide the PSST[2] and FCC in crafting rules for and agreements with the regional systems to operate via a spectrum lease under the PSBL license[3].

At the June 2009 NPSTC meeting, the Governing Board voted to endorse use of the Long Term Evolution (LTE) technology for use in the NBDS, and formed the 700 MHz Broadband Task

[1] See Appendix B for the Definition of the NBDS
[2] The PSST is the Public Safety Spectrum Trust - this entity holds the national license for the 700 MHz Public Safety Broadband Spectrum that will be leased to the regional operators to build out regional public safety systems.
[3] The PSBL is the Public Safety Broadband Licensee and is held by the PSST

Force (BBTF). The NPSTC Governing Board also directed the BBTF to assume use of LTE by the regional systems in the development of the BBTF recommendations. Therefore, all recommendations assume the national and regional systems will be built out using LTE technology and the technical recommendations are focused on those parts of the LTE standards required to meet the BBTF objectives.

Objectives

1. Define the minimum requirements for public safety built 700 MHz broadband networks that enable national interoperability for users of the 700 MHz band.
2. Provide a governing framework for the relationship among public safety regionally built systems, and the PSST, and include the option for public/private partnerships as defined in this report.
3. Accommodate the potential scenarios for the 700 MHz D Block and PSBL as they may be defined by Congress and the FCC, including reallocation of the D Block to public safety as recommended in this report.
4. Defer defining requirements necessary to provide operability to the public safety entities authorized to deploy regional systems in their respective areas, and recognize the right of the regional operators to select and deploy applications beyond those defined as necessary for roaming and interoperability.
5. Offer recommended technical requirements that public safety entities use in procurements to satisfy the 700 MHz minimum roaming and interoperability requirements.
6. Provide a base set of recommended requirements by August 2009 to allow entities that have filed for 700 MHz waivers to fulfill their 700 MHz broadband objectives as rapidly as possible.
7. Provide a set of best practices for network architectures and configurations for items that are not required, yet are suggested as quickly as possible.

2.2 Process

The BBTF used a transparent and open process to reach consensus on the recommendations in this report. The membership of the BBTF was open to all persons wishing to participate. The trade press was invited to monitor and report on the progress. The BBTF included members representing public safety, federal government representatives, vendors, and consultants. All decisions were made by the consensus of the members that represented public safety entities.

The Task Force met as a group mainly by weekly conference calls and at two face-to-face meetings, one in Boulder, Colorado, and the other at the Association of Public-Safety Officials – International (APCO) 2009 conference. The Work Groups also met by weekly conference calls. Between meetings much discussion and information exchange was done via email.

The BBTF would like to thank the Department of Homeland Security (DHS) Office for Interoperability and Compatibility (OIC) and the Department of Commerce Public Safety Communications Research (PSCR) program for support and participation in this work, in particular for the work and technical expertise of Andrew Thiessen and Emil Olbrich, PSCR. The BBTF also thanks APCO for its support of the Operations Work Group and for hosting the in-person meeting at the 2009 APCO Conference.

2.3 Organization

The BBTF organized three Work Groups: Operations, Technical, and Governance. The Operations WG developed the operational requirements for roaming and interoperability that the other two WGs used to formulate their recommendations. The Technical WG specified the technical recommendations necessary to support the operational needs for roaming and interoperability. The Technical WG also coordinated with the Governance WG to support governance recommendations. The Governance WG developed a term sheet of recommended terms for agreements between the regional operators and the PSST, and developed recommendations necessary for roaming and Interoperability both intra- and inter- system. The BBTF organization chart is pictured below:

3 Operations Work Group

The Operations WG performed an extensive review of prior work from the 700 MHz Broadband Statement of Requirements (SoR) and from the Project MESA Technical Specifications Group – System Functional Requirements definitions. These two documents detail a wide range of operational requirements. The WG also took suggestions from the members for operational requirements. The WG sorted through these requirements and narrowed them down to seven required applications and four desired applications. These applications were selected as those most critical to be supported by roaming and interoperable requirements. These are not intended to be an all inclusive list of applications that the regional operators may deploy on their networks. Public safety entities should have open access rights to deploy additional applications as they so choose to support their operational requirements. The recommended applications are intended to ensure that the roaming and interoperability needs of the NBDS are met as required for proper public safety roaming and interoperability. The desired applications are recommended but not required and may not be technically supported for early build out of regional networks.

4 Technical Work Group

The Technical WG received input from the Operations and Governance WGs and used that input to determine the LTE architecture required to implement the Operations and Governance recommendations. The Technical WG extensively reviewed the LTE standard and received input from LTE equipment vendors and commercial providers of broadband services. From this a set of required recommendations and best practices, recommendations were developed. Best practices are suggested to the regional operators but are not a requirement for roaming and interoperability. The Technical WG working paper contains considerable background and reference material and should be consulted to implement the technical recommendations. In general, the Technical WG found that LTE encompasses sufficient attributes to support many of the data and video applications envisioned.

5 Governance Work Group

The Governance WG had representatives of many, but not all, of the agencies requesting waivers to build out regional networks. This WG focused on the minimum requirements necessary to define the agreements and recommendations for the relationship with the PSST and the regional system operators. This WG also focused on those matters requiring changes to existing laws or FCC rules needed to implement regional systems. The Governance WG formulated recommendations that are consistent with the concept of regional systems operating as part of the NBDS and ensuring roaming and interoperability is maintained on a national basis.

6 Recommendations

The recommendations below are the final consensus recommendations of the BBTF and each of the Work Groups. In the Appendix the work product of each WG is provided for reference and to give perspective to the recommendations. In the event of a conflict between the recommendations below and the Appendix WG work product, the recommendations in this section below should prevail.

During the process of developing recommendations, it was pointed out by the equipment vendors and commercial operators that for public safety to field devices on the 700 MHz public safety spectrum, chip manufacturers would need to develop the RF chips that include the public safety spectrum. There are indications there is interest to do this, but NPSTC and the PSST will need to actively monitor and push for the appropriate chip sets to be developed and marketed for public safety devices.

During the course of developing these recommendations, the Task Force members expressed a strong concern that the regional networks need the ability to start to build out quickly. Some recommendations in this report cannot be implemented on day one, in particular a few of the required Operations recommendations. The LTE standards are evolving over time and are expected to support all recommendations in this report in the future. The BBTF strongly recommends that the regional operators be allowed to build out as soon as possible. Further the BBTF recommends the Advisory Group determine those recommendations that cannot be implemented on day one and determine a timeline for regional networks to implement. Because the LTE standard is evolving, it is possible that it will not be possible to meet one or more of the recommendations or that they must be implemented differently than envisioned in this report. The Advisory Group should monitor the standards work and though recommendations to the PSST Board influence the inclusion of features necessary for public safety operations.

6.1 General

6.1.1 Regional Operator Advisory Group

The PSST and the regional system operators should form an Advisory Group consisting of a representative of each regional operator and of the PSST for follow-on work and to resolve any issues that arise as systems are being deployed and experience is gained in their operation. As a condition of receiving a spectrum lease[4], each regional system operator must participate in and fund a representative to the Advisory Group. Each of the BBTF Work Groups identified follow-on issues that need to be resolved to allow the best operations by the regional systems. These are not issues that will hold up the procurement of system equipment or the granting of a spectrum lease; the recommendations in this report resolve issues that would further delay the build out of the regional systems.

Many current public safety voice systems that are regional in nature employ a user's group concept to work out policy and operational issues. Over time this has proved to be an effective way for multiple agencies to work together to resolve issues.

This Advisory Group would:

- Continue the work of the BBTF to extend and codify the operations, governance, and technical requirements for the network;
- Advise the PSST Board; and
- Work with the PSST Board on other standards and agreements which improve the operability and interoperability of the national public safety broadband wireless network.

6.1.2 D Block Spectrum

NPSTC and the member organizations of NPSTC, along with the PSST and other public safety organizations should begin a coordinated effort have the D Block 5+5 MHz of spectrum allocated for public safety use and licensed to the PSBL. During the work of the BBTF it was apparent that the current 5+5 MHz of spectrum available for public

[4] See Appendix B Definitions for the definition of spectrum lease

safety use for broadband data systems will not be sufficient to support disaster operations. Also some or many of the regional systems will need to enter into public/private partnerships as described in this report in order to fund implementation and operation of the regional systems. Without the D block spectrum, there will be insufficient spectrum for these partnerships to most effectively operate.

6.1.3 Public/Private Partnerships

The FCC should allow the option for commercial roaming onto the national network and the regional systems to facilitate private/public partnerships, with prioritization of communications set by the host agencies deploying regional systems for their respective areas. The assumptions listed in Appendix A describe the different methods regional systems can use to build out. Section 8.11.4 assumes a private/public partnership with commercial roaming onto the public safety spectrum. In addition and while outside the scope of the BBTF, it appears the PSST may need to use some form of public/private partnership to build out the national system in areas not served by the regional systems.

6.1.4 Common Clearinghouse

A common/single third party clearinghouse should be utilized by the national and regional network to allow roaming. The Advisory Group should recommend to the PSST Board specifications based upon bi-lateral roaming agreements.

The Advisory group should make recommendations to the PSST Board on selection of the common clearinghouse provider and the PSST should enter into an agreement for interconnection services for Inter-system and Intra-system "roaming" rather than negotiating individual agreements or memoranda of understanding (MOUs) between regional system operators.[5]

6.1.5 Equipment and Features Test Facility

NPSTC and the PSST should ask the PSCR if they could set up a LTE equipment and features test facility to test the implementations recommended in this report. This test facility would also be used to test the features in LTE that support the roaming and interoperability requirements recommended in this report. This recommendation is not

[5] See section 13.3.6 for more details.

intended to duplicate any commercial test beds or the compatibility testing that is part of the LTE standards process. The results would guide regional operators in configuring their systems.

6.2 Operations

6.2.1 Internet Access -Required

Public safety subscribers shall have access to the global Internet. Users will use the Internet both as a way to access home network systems and to access other systems and services available over the public Internet, including but not limited to messaging systems and web servers.

6.2.2 VPN Access to any Authorized Site and to Home Networks - Required

The regional operator and commercial networks operating in conjunction with the PSBL shall be required to allow establishment and use of VPN connections by roaming users on their networks to other networks.

6.2.3 Status/Information "Homepage" - Required

Public safety or public/private partnership network operators shall provide 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 operator deems important to share with visitors to the system.

6.2.4 Status/Information "SMS-MMS Messaging" - Required

Public safety, public/private partnership, and commercial network operators shall provide the ability for users to send and receive Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages.

6.2.5 Access to Responders under Incident Command System (ICS) – Required

First responders, emergency response support, and all other mutual aid responders managed under the ICS structure of a requesting agency served by a public safety broadband network shall be provided access to that network to carry out incident objectives and communicate with their home networks.

6.2.6 LMR Gateway Devices - Required

Networks shall allow for connection and operation of IP-based voice interoperability gateways.

6.2.7 Field-Based Server Applications - Required

The ***regional systems*** shall support the use of field-deployed server applications. This requirement includes the need for client devices to consistently and continuously reach these server-based systems from any other location on the Internet. The capability is not required for every subscriber device on the broadband network but is limited to a subset of the users that actually require such a feature.

6.2.8 Location Based Data Capability - Desired

Regional networks should include the capability to collect and convey subscriber unit location data in real time. The technical ability to covey location information should be inherent on any public safety network and associated commercial networks. Location data should be accessible to appropriate applications, as may be authorized by management level policy. Location data applications may be located on both subscriber units and associated agency level command/control applications. Subscriber units of future public safety networks should meet the same minimum location data information requirements (format and accuracy) as is currently applicable on current commercial services networks in order to retain a broad level of compatibility with incumbent systems.

6.2.9 One-To-Many Communications across All Media - Desired

Regional networks should provide one-to-many communications capabilities to outside network users responding in mutual aid to the that Regional Network. 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.

6.2.10 LMR Voice - Desired

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.

6.2.11 PSTN Voice – Desired

Public safety 700 MHz voice capable devices such as cell phones, PDAs, or their equivalent shall be capable of placing and receiving full-duplex telephone calls to any telephonic device on the Public Switched Telephone Network (PSTN) in the visited network with the same functionality that cellular telephones operate nationally today. This includes location based PSAP call routing, E911 Phase II location transmission, and, if necessary CALEA. In the case where the user transitions in to or out of one regional system, the voice session shall be handed off between the two networks with limited loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement.

6.3 Technical

6.3.1 System Identifiers

Public safety LTE systems must comply with 3GPP standards and therefore they must be assigned a PLMN ID. Since PLMN IDs are a limited resource shared by all 3GPP wireless networks worldwide, the use of PLMN IDs should be effectively managed. The Technology Working group has considered two alternatives for assignment of PLMN IDs:

1. Single PLMN id shared by all public safety networks
2. Individual PLMN id for each public safety network

The following are the recommendations for System Identifiers:

1. A common schema should be used to identify public safety users and regional networks (intra-system – category 1 roaming).
2. Per the definition, a PLMN must be operated by an administration or by a recognized operating agency (ROA).
    a. For either single PLMN or individual PLMNs, the PSBL and/or the NPSTC Governance Working Group must determine the structure of the ROA.

3. The PSST board with advice from the advisory group must determine the long term strategy for the organization of Public Safety PLMNs and have it apply to the initial waiver requesters.
4. The PSST board with advice from the advisory group will determine with the IOC, the recommended number of PLMN IDs
    a. If the PSST becomes the overall operator for regional public safety 700 MHz LTE networks, then a single PLMN ID should be adopted
    b. If individual PLMN IDs are chosen to be assigned to regional networks
        i. PLMN ID regions should be based upon some form of geographic, population and demographic determination.
        ii. Logically each network will be organized and operated as an independent PLMN.
        iii. The number of PLMN IDs allocated will be the determination of the IOC but the actual amount recommended should be less than 100 IDs
5. PSBL will apply for dedicated PLMN ID(s) (MCC/MNC/HNI) from the IOC
    a. Use an existing MCC as determined by ATIS and IOC.
    b. Recommend that the PSST investigate and potentially ask for a dedicated MCC for public safety networks.
6. USIM is provisioned by the home network administrator with
    a. Home IMSI (HPLMN)
    b. Prioritized list of permitted VPLMNs
    c. Forbidden PLMNs list

6.3.1.1 Phone Numbers

In order to support and facilitate future voice and SMS text messaging the use of phone numbers will be required. This will also be necessary subscriber identification, billing and any connections to the PSTN.

The following are the recommendations for Phone Numbers:

1. Every user will be assigned a MSISDN number that is coordinated with the MSIN e.g. MSISDN and IMSI/MSIN will both be stored in the HSS

    a. Specific implementation of E.164 and E.169 will be investigated further

2. PSBL will assume responsibility for coordinating, assigning and managing allocations of phone numbers

    a. PSBL will work with regional networks and NANPA on approved NPA and phone number allocations

b. PSBL will work with regional networks and NANPA on approved CIC allocations

c. PSBL will work with regional networks and commercial service providers as necessary if a public/private model is adopted

6.3.1.2 Required Interfaces

To support initial network build outs that support roaming the following interfaces are required:

1. Uu – LTE Air Interface

2. S6a – Visited MME to Home HSS - Diameter signaling

6.3.1.2.1 Recommended Optional Interfaces

The following interfaces are highly recommended to fully support inter- and intra-system roaming:

1. S8 – Visited SGW to Home PGW
2. S9 – Visited PCRF to Home PCRF for dynamic policy arbitration. The S9 is primarily used for QoS functionality from the PCRF but its inclusion will allow easier migration to a QoS enabled network.
    a. Gx – PGW to PCRF interconnection required if S9 is implemented
3. S10 Interface – MME to MME support for intra-system (category 1) handover support
4. GTP Tunnel between home SGW and visited SGW

6.3.1.2.2 Interface Interoperability Testing

The technical working group recommends the PSBL require the following interfaces perform IOT:

1. Multi-vendor interoperability (IOT) supported on the S1-MME and S1-U interface between the eNb and the EPC
2. X2 – Intra-network eNodeB connection shall be required within a homogeneous public safety 700 MHz regional network – this does not include geographically adjacent systems e.g. intra-system roaming
    a. IOT required for multi-vendor support

6.3.1.3 Handover Recommendations

1. Handover of active sessions on geographically adjacent public safety 700 MHz LTE networks. Intra-system handover for data session between home and visited networks is required. This is defined as intra-RAT handover and may be phased in over time.

    a. Typically not implemented in commercial networks for intra-system, category 1 type roaming (Different PLMN) – this may require the implementation of additional interfaces.

    b. These types of handovers will be subject to pre-arranged roaming agreement(s).

2. Handover of active sessions between home and visited networks is not required when a visited network is using another RAT such as 3GPP2 or another release of 3GPP (e.g. Release 7). This is defined as inter-RAT handover.

3. After handover from the 700 MHz public safety LTE network to a commercial carrier (inter-RAT), the user may come back (idle and active) into the coverage area of their home network. The cell search mechanisms should support the ability to identify and re-attach to public safety LTE neighbor cells.

4. Public safety networks should be the primary networks for cell reselection. As such the white-list maintained on the Ue, PLMN ids or the equivalent of the neighbor cell list (NCL) should be programmed to facilitate public safety LTE networks as the primary choice.

6.3.1.4 Interwork Connectivity Recommendations

1. A common/single 3rd party clearing house should be utilized by public safety

    a. PSBL and/or public safety representative will determine specifications based upon bi-lateral roaming agreements

2. All 700 MHz public safety LTE networks will minimally utilize 3GPP TS 23.401 defined attach and authorization schemes

    a. For systems that use a 3rd party interworking provider the implementation of Near Real Time Roaming Data Exchange (NRTRDE)

may be required between public safety networks and between public safety and commercial networks to combat fraud and facilitate the exchange of roaming data.

i. NRTRDE and similar mechanisms will be investigated by the technical working group – especially for systems that are directly connected to each other and do not utilize a 3rd party interworking provider

3. Provisions should be allowed to directly interconnect geographically close 700 MHz public safety LTE networks to each other.

   a. Directly connected networks will need to ensure to PSBL and/or public safety representatives that all proper authentication credentials are processed accordingly

4. Redundant, geographically separate 3rd party clearing house centers will need to be supported to address disaster scenario's

   a. Backup solution will need to be available to authenticate roaming users when 3rd party network isn't available and mutual aide is required from roamers

6.3.1.5 Devices

The minimum requirements and specifications, but not limited to, for a public safety device are the following:

1. Band class 14 should be supported for 5 and 10 MHz channel sizes in Frequency Division Duplex (FDD) mode as per 3GPP TS 36.101 v8.6.0

2. USIM should be unlocked to allow public safety users to switch out UICC cards between multiple devices

3. Every system shall be able to utilize any PSBL approved UEs while roaming on the national 700 MHz Public Safety network.

6.3.1.5.1 Optional device requirements and specifications

1. IMS authentication and services via support of the ISIM as per 3GPP TS 31.103: Characteristics of the IP Multimedia Services Identity Module (ISIM)

2. Multi-mode support of 3GPP Rel. 7 HSPA and/or 3GPP2 EVDO Rev. A

3. Multi-band support for 3GPP & 3GPP2 commercial 700, 850 and 1900 MHz bands

6.3.1.6 Standards Testing

The minimum requirements and specifications, but not limited to, for a public safety 700 MHz LTE Standards testing are the following:

1. Minimally, public safety 700 MHz LTE infrastructure and subscriber equipment will need to have been tested and certified by the aforementioned 3GPP test suites that the Global Conformance Forum (GCF) is overseeing.

2. If GCF testing is not available within the timeframe of network deployment the vendors and public safety network operators should have the option to perform specific testing as determined by the PSBL and/or public safety network representative.

6.3.2 Minimum Applications

See the Appendix F for the full list of specific application support information.

6.3.2.1 Internet access

Internet access is required to support operational requirements.

6.3.2.2 VPN access

VPN access is required to any authorized site and back to home networks.

6.3.2.3 Visited network home page

Intra-network roaming users will have a common webpage, text message, or delivered information on applications and services offered by the visited network and relevant alerts.

6.3.2.4 Text messaging

Application level SMS over IP will be allowed but recommend the use of a common SMS delivery system as described in 3GPP TS 23.204 V8.4.0 and 3GPP TS 24.341 V8.1.0[6]

Current SMS capability is supported via media gateways that are designed for control plane/circuit-switched networks. Legacy SMS support is tentatively scheduled for 3GPP Release 9 (or 10 depending on the delivery platform).

6.3.3 Security

- For public safety LTE networks, these optional security layer features specified in 3GPP shall be implemented.
  - 3GPP TS 33.401.
- The use of network layer VPN will be allowed on public safety LTE networks.
  - VPNs provide secure communication tunnels to home servers/applications and can support (e.g. NCIC/CJIS, AES, and HIPPA) public safety security requirements.
  - Coordination of ports and Quality of Service (QoS) will need to be determined as necessary between home and visited networks.

6.4 Governance

6.4.1 FCC Rule Changes

NPSTC and/or the PSST should petition the FCC to to allow individual city or county governments, or groups of governments, to construct regional networks using the 700 MHz broadband spectrum assigned to public safety, using this report as a framework for requirements. The FCC should grant waivers to allow qualified regional requestors who agree to build subject to the terms and conditions specified in this report.

6.4.2 PSBL Spectrum Lease to Regional Operators

The FCC should allow the PSBL to lease spectrum to (or the appropriate legal equivalent) regional system constructors and operators authorized by waiver or under the changed rules. The terms of the lease are contained in the lease

[6] Inclusion of this specification may require the use of the IP Multimedia Subsystem (IMS)

agreement term sheet. The regional network operator will have all rights to use the spectrum and operate the regional network as if they were the licensee, except as provided in the lease agreement term sheet.

6.4.3 Use of Spectrum

NPSTC and/or the PSST should seek changes to laws or FCC rules to explicitly allow use of the national interoperable broadband wireless network in spectrum allocated to public safety by not only first responders, but also by emergency response support agencies as defined in Appendix B. Such emergency response support agencies are critical to the safety of the public during daily incidents and emergencies, but especially during local, regional, and national disasters. Prioritization of network use between all such users would be controlled by the regional network operator.

7 Conclusions

This report represents the best recommendations of the work groups and the members to meet the objectives assigned to the BBTF. The BBTF tried to reach a balance with recommendations being as complete as possible to support roaming and interoperability required by the NBDS without imposing recommendations that are beyond the minimum needed. The LTE is still an evolving standard and implementation of some recommendations may not be possible day one of regional system build outs. The BBTF does not see a need to delay regional system build outs until all recommendations can be met but it is important for the PSST and the regional operators to commit a goal of implementing these recommendations when possible to ensure true nationwide interoperability.

The need for additional spectrum is clear from the requirement of public/private partnerships and from the capacity needs during disasters. The BBTF found the D Block Spectrum is the only practical spectrum available to meet these needs. The BBTF strongly recommends that the PSST and NPSTC along with its member organizations work together to have the D Block allocated for public safety use.

8 Appendix A: BBTF Assumptions

8.1 Spectrum

The FCC will continue to allocate 10 MHz in the 700 MHz spectrum for use by public safety to create a wireless broadband network. A single PSBL will continue to hold the nationwide license to use this spectrum.

8.2 Waivers

The FCC will grant specific waivers to regional groups/agencies (and/or change the FCC rules) allowing those agencies to build wireless networks with this spectrum. The PSBL will then lease the use of the spectrum to each such regional group/agency subject to the protocols and standards established in the BBTF recommendations document.

8.3 Use of Recommendations

The PSBL and regional operators will use the BBTF recommendations and the materials developed by the BBTF to manage the spectrum nationally, and to govern the way regional operators interact with the PSBL and each other.

8.4 Additional Spectrum

Congress may re-allocate the 10 MHz of 700 MHz spectrum known as the D block for the use of public safety, which would be added to the national PSBL. If so, the Task Force recommendations would also apply to use of that spectrum.

8.5 No Duplication of Effort

The BBTF will rely on and will not duplicate previous efforts to develop detailed technical requirements for public safety networks, e.g. reliability, availability, etc.

8.6 Regional Network Cooperation

Within individual regional operators, there will usually be multiple agencies, jurisdictions, and/or city/county departments, which cooperate to build the regional network.

8.7 Cooperating Agencies and Agreements

The agreements and protocols established by the BBTF Recommendations would apply to all such individual agencies.

8.8 Operating Protocols

The BBTF assumes the regional operators and cooperating agencies explicitly may establish their own operating protocols governing internal interoperability and internal use of their network(s).

8.9 National Network

The BBTF assumes a national interoperable public safety network in this spectrum.

8.10 Broadband Access

As many public safety users as possible, urban and rural, in cities and towns and rural areas, must have access to an interoperable broadband wireless data network.

8.11 Build Out of Networks

If there is no D Block licensee to build the regional networks, there are several potential ways in which regional operators could fund, build, and operate the regional networks. Since their requirements and resources vary, regional operators need to have considerable freedom to negotiate public/private partnerships for network construction in their regions. However, it is assumed that one of the following approaches would be used.

8.11.1 Public Safety (PS) Entity

A public safety (PS) entity funds, builds, and operates the regional network for PS users of all types (i.e., no commercial users on the network).

8.11.2 Service Operator

PS entity funds the network but contracts with a service operator to build (and possibly operate) the regional network for PS users of all types. The regional network equipment is separate from the equipment used by commercial customers of the service operator.

8.11.3 Shared Equipment

PS entity funds the network but contracts with a service operator to build and operate the regional network for PS users of all types. In order to reduce costs, the network operator shares some equipment across commercial and the PS users. However, only PS user devices have access to the PS spectrum.

8.11.4 Service Operator with Commercial Access

PS entity contracts with a service operator to build and operate the regional network. In order to fund the construction and operation of the network, commercial users will be allowed on the network (i.e. use the PS spectrum). In this case, some arrangement for a commercial user roaming into the regional networks dedicated to PS users (i.e., approaches 8.11.1 – 8.11.3) may be required.

8.12 Nationwide Network Compatibility

The governance protocols and operational requirements the BBTF develops should accommodate at least a "mixture" of these approaches. All approaches must be compatible with a nationwide broadband network.

9 Appendix B: BBTF Definitions

These definitions are specific to the BBTF report and recommendations and are not intended as general definitions for public safety communications.

9.1 National Broadband Data System

A National Broadband Data System (NBDS) is the overall framework under which the regional systems operate. Build out of the regional systems will begin the process of building the NBDS.

9.2 Regional System (Regional Network)

Public safety agencies in several areas of the country have filed waiver or rule change requests with the FCC to build out a broadband public safety data network in a specific geographical area on spectrum allocated to public safety in the 700 MHz band and operating under the PSBL held by the PSST. When the term "regional operator" is used in this report, it refers to the operator of the regional system.

9.3 Spectrum Lease

The regional system operator will get operating authority from the FCC grant of their waiver request and it assumed the FCC will direct the PSBL to allow the regional systems to operate under the PSBL license. For this report, the regional system operator is defined as holding a spectrum lease from the PSBL.

9.4 Intra-system Roaming

The regional networks will be stand alone systems, part of a single national system, so public safety users roaming from their home regional systems to another regional system are considered to be roaming within (intra) the system.

9.5 Inter-system Roaming

Public safety users that are part of a regional system may roam off of the national system and commercial users may roam onto the national system. This roaming is defined as inter-system roaming.

9.6 Interoperability

Interoperability is the ability of first responders and emergency response support personnel to talk to one another via radio communication systems -- to exchange voice and/or data with one another on demand, in real time, when needed, and **as authorized.** For this report only, data interoperability (voice and video are considered a data application) is considered. This interoperability may involve access to applications by first responders and emergency response support personnel (**as authorized**) from their home regional system or access from the regional system to which they are responding.

9.7 First Responder

Those individuals in the early stages of an incident who are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in Section 2 of the Homeland Security Act of 2002 (6 U.S.C. § 101), as well as emergency management, public health, clinical care, public works, and other skilled support personnel, such as equipment operators, who provide immediate support services during prevention, response, and recovery operations." The federal Homeland Security Act of 2002 provides that the term "emergency response providers" includes "federal, state, and local emergency public safety, law enforcement, emergency response, emergency medical, including hospital emergency, and related personnel, agencies, and authorities.[7]

9.8 Emergency Response Support

Emergency response support is defined as those who are involved in the critical mission areas surrounding the incident response, such as protecting against the incident, preventing the incident, or recovering from the incident.

10 Appendix C: Term Sheet

PROPOSED TERM SHEET
FOR AGREEMENT BETWEEN REGIONAL OPERATOR
AND PUBLIC SAFETY BROADBAND LICENSEE

NOTE: This is a Term Sheet describing the proposed key points of a future Agreement between Regional Operator and the Public Safety Broadband Licensee (PSBL); it is not an effort to establish contractual language, but rather to describe the intent of parties on key issues. Though it refers to "this Agreement," it is not an Agreement in and of itself, but rather a description of terms that may be included in the future, contemplated Agreement. This Term Sheet refers throughout to the requirements developed by the NPSTC 700 MHz Broadband Task Force (BBTF). It should be understood that when an Agreement is ultimately developed and agreed to by the Regional Operator and the PSBL, some version of those requirements will have been presented by NPSTC to the PSBL, and the PSBL will have endorsed some version of those requirements. Accordingly, the Agreement will refer to such requirements by a different name, such as

[7] From Homeland Security Presidential Directive #8 (HSPD-8)

"Interoperability Requirements," "Technical Requirements," or other agreed-upon terminology.

1. **Agreement.**

    a. This Agreement is contingent upon the FCC granting waivers for Early Build-Out and providing any authority needed by the PSBL to enter into such an Agreement for the Regional Operator use of the PSBL spectrum. It is also contingent upon requirements imposed by the FCC. The term "Local Builder" refers to any eligible public safety agency or group thereof, whether local, regional, or statewide in nature, that obtains authority by rule or waiver to deploy their own 700 MHz broadband public safety system. Such local system would be constructed as a local portion of the national 700 MHz public safety broadband network.

    b. PSBL permits Regional Operator to use within Local Builder's geographic area the 700 MHz public safety broadband allocation for which the PSBL holds the FCC license. The Regional Operator may use up to but no more than the full amount of spectrum covered by the PSBL license. Broadband may not be deployed in the guard band segment of the PSBL's licensed spectrum.

    c. PSBL allows Regional Operator to exercise PSBL's rights and obligations under the FCC license to the extent permitted under the legal framework adopted for this Agreement (*e.g.,* Secondary Market *de facto* transfer of control or Spectrum Manager framework—TBD). This allowance would be subject to any rights or authority the PSBL would be required to maintain as the licensee. The guiding principle for this allowance is that the Regional Operator would, as much as possible under FCC rules and subject to the Task Force Recommendations, take on the rights and obligations of the PSBL license in the Local Builder's geographic area.

    d. To ensure a nationally interoperable network, the PSBL also agrees that any portion(s) of the national network that it causes to be built will also be built in compliance with the Task Force Recommendations, to the extent those Recommendations are endorsed and/or allowed by the FCC.

    e. Regional Operator agrees to use the spectrum to build and operate a local portion of the national public safety broadband network within its geographic area consistent with FCC rules and the minimum technical, operational, and governance requirements developed by the NPSTC BBTF ("Task Force Recommendations"), to be attached to this Agreement.

        i. Regional Operator and PSBL agree that local portions of the national network in PSBL spectrum under this Agreement may be used by any eligible users as defined by the FCC, pursuant to prioritization determined by the Local Builder.

ii. There is no security instrument (such as a letter of credit) associated with this Agreement for the use of the spectrum; Local Builder's consideration for use of the spectrum is agreeing that it will comply with the Task Force Recommendations.

iii. Regional Operator agrees to meet reasonable Build-Out schedule as defined by the FCC in waiver grants. In exchange, Regional Operator receives under this Agreement (see "Term") the use of the spectrum for as long as the PSBL holds the national license.

iv. Regional Operator and PSBL recognize the need to establish a mechanism for considering and adopting future requirements to ensure and improve national interoperability. Such a mechanism will not allow PSBL unilaterally to impose such requirements upon Local Builder; likewise, adoption of future requirements may not require consensus among the PSBL and all Local Builders. Regional Operator and PSBL agree to work in good faith to establish and participate in such a mechanism.

v. Regional Operator is responsible for the costs of building and operating the local portion of the network; unless otherwise specified in this Agreement or via subsequent agreement, the Regional Operator has no financial obligation to the PSBL.

2. Scope of Spectrum Usage Rights.

a. Regional Operator receives maximum usage rights permitted under FCC rules and this Agreement, including the attached Task Force Recommendations.

3. Term.

a. Starting from the effective date of this Agreement and continuing as long as the PSBL holds the national license, including any renewals or extensions of the PSBL's current license term

4. Termination.

a. Either party may terminate upon written notice if the other party breaches by following this process:

i. Written notice of noncompliance
ii. Up to 60 days to cure unless it is an issue that requires immediate attention
iii. Written notice of failure to cure and termination.

5. Durability of Regional Operator Use of Spectrum.

a. While Regional Operator remains in compliance with FCC rules and Task Force Recommendations, PSBL may not terminate this Agreement or otherwise curtail Local Builder's use of the spectrum in order to effectuate a different network using the spectrum; if the PSBL begins to deploy a network in the 700 MHz public safety broadband allocation, either with a commercial partner or otherwise, it must not infringe upon the Local Builder's use of the spectrum in the Local Builder's geographic area during the term of this Agreement.

b. Should the D Block be successfully auctioned, the network sharing agreement between the PSBL and the D Block winner(s) must respect the Local Builder's rights to the spectrum for the duration of this Agreement as long as the Regional Operator meets FCC rules as well as the Task Force Recommendations of this Agreement. Regional Operator agrees to negotiate in good faith with applicable D Block winner, with input from the PSBL, to develop any mutually agreeable potential partnership between the D Block winner and the Local Builder, as operational needs dictate.

c. In the event that the D Block is allocated to public safety and is included within the PSBL's license, the PSBL spectrum addressed in this Agreement includes the D Block as well as the current public safety allocation.

6. Compliance with FCC Rules and Requirements of This Agreement.

a. PSBL may terminate this Agreement if Regional Operator violates an FCC rule that, if the PSBL had committed such violation, would have been grounds for the FCC terminating the PSBL's license. Same notice and cure period applies as to Termination under item 4.

b. PSBL also may terminate this Agreement if Regional Operator does not comply with the Task Force Recommendations set forth in the Appendix. Same termination notice and cure period apply as in item 4.

c. PSBL shall have the right to make scheduled inspections to ensure compliance with this Agreement, including the Task Force Recommendations.

7. Representations and Warrantees.

a. Regional Operator is duly authorized to enter into this Agreement and meet its requirements.

b. PSBL will keep the license from becoming encumbered, ensure timely filing for license renewal, and maintain license in good standing.

8. Regulatory Compliance.

a. Both parties will remain compliant with FCC rules and will notify each other if they become or expect to become non-compliant.

b. The requirements for regulatory compliance will be dependent on the legal structure defined in the FCC's rules and/or waiver conditions, whether the structure be a secondary markets (*de facto* transfer of control) approach or a spectrum manager approach. To the extent the FCC requires any filings or information to be submitted by the Local Builder, Regional Operator agrees to provide such filings or information to FCC on a timely basis after coordinating with the PSBL.

c. The PSBL can rely upon Local Builders' operations in demonstrating compliance with any construction or substantial service requirements.

9. Indemnification.

a. To the extent relevant, both parties indemnify each other from third-party liability, except where loss arises from negligent or intentional acts or omissions.

b. Boilerplate on Defense of Third Party Claims, No Consequential Damages, and Survival of Indemnification provisions.

10. Miscellaneous—basic boilerplate, including:

a. Severability—yes.

b. Successors and Assigns—yes, Agreement may be assigned with consent of the Parties.

c. Governing Law—leave it to the individual Local Builder, or make the default the home jurisdiction of the PSBL (DC).

d. Specific Performance—yes, absolutely.

11 Appendix D: Roaming White Paper

Roaming and the Shared Wireless Broadband Network

11 August 2009 - V4

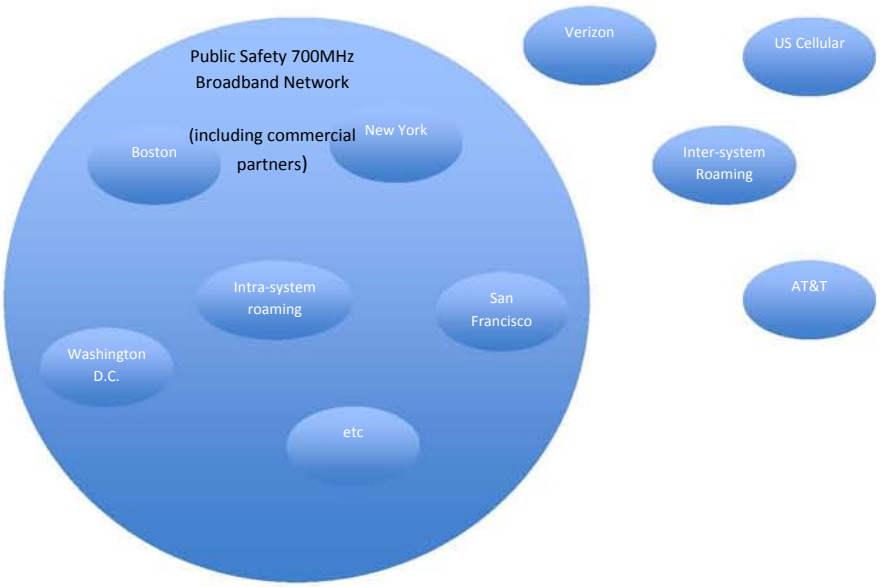
Introduction

In exclusively commercial mobile networks, roaming is an essential capability for providing users with the experience of national connectivity. Even after 25 years of development and tens of billions of dollars of investment, no single terrestrial mobile service provider in the United States can provide a truly national footprint to its customers without relying on roaming services from other operators. A nationwide, interoperable wireless broadband network, referred to here as the National Broadband Data System (NBDS) for public safety will not be built overnight and it will take many years to even approximate ubiquitous coverage. During that period, the ability of public safety users to roam on commercial networks will be essential. Likewise, while not a first order priority for public safety, the ability of commercial users to roam onto the NBDS, utilizing otherwise idle capacity may be essential to rendering the NBDS financially viable in much of the country.

Roaming between the NBDS and commercial networks will be referred to in this paper as "inter-system" roaming. Inter-system roaming requires interworking at the business and operational levels including not only network authentication, but also bilateral roaming agreements between the Public Safety Broadband Licensee (PSBL) and commercial networks in addition to some type of clearinghouse mechanism to settle accounts between parties.

This paper will also address "intra-system" roaming. The vision is that the NBDS will function, to the extent possible, as a single network. Significant elements of that network may be shared. It is also possible that elements of the network may be owned and operated locally, either by "local builder" public safety agencies or by D Block licensees or other private commercial partners. Depending on which elements are deployed and managed locally and which are shared across the NBDS, "roaming" arrangements may be required between participants in the NBDS. In the world of circuit-switched mobile voice services, for example, this type of roaming occurs *within* the networks of every multi-regional service provider since platforms for user authentication such as Home Location Registers (HLRs) and Visiting Location Registers (VLRs) are associated with each Mobile Switching Center (MSC) in an operator's network. The architecture of mobile data networks is not as geographically-constrained, so the deployment strategy for analogous elements, such as Packet Data Serving Nodes (PDSNs), Gateway/Serving GPRS Packet Support Nodes (GGSN/SGSNs) is more a matter of network reliability, economic efficiency and governance considerations than a fixed technical requirement.

The following diagram illustrates possible relationships between parties in the inter- and intra-system roaming contexts:



Roaming Categories

The Broadband Task Force Technical Working Group has identified the following requirements for roaming:

- In the absence of coverage from the home network, the ability for the User Equipment (UE) to scan supported bands, perform cell selection and authentication on a visited network.
- After authentication on a visited network, the assignment of an IP address, and the ability to communicate with the public Internet.
- Handoff of active sessions / calls between home and visited networks is required when both networks are using LTE technology.
- Handoff of active sessions / calls between home and visited networks is not required when a visited network is using earlier generation wireless technologies.

Authentication: The primary function required to support roaming at the network level is authentication. In order to operate a device on a mobile network, user equipment must be authorized for use on that network. This is a function performed in every mobile network regardless of whether a customer is roaming or operating within the home network. As noted above, in circuit-switched (non-IP) voice networks, the distinction of "home" and "visited" network is an important one. Networks are defined around an individual Mobile Switching Center (MSC) and, even when using their own service provider's network, users are roaming whenever they attempt to operate a mobile device outside their home area. For data services, these boundaries are not as important from a technical architecture standpoint. Assuming that

the NBDS is functionally a single network, local components of that network would likely share national platforms for authentication and that sharing would likely be governed by Network Sharing Agreements (NSAs) between those local participants (local builder public safety agencies and/or commercial D Block licensees) and the PSBL. If necessary, authentication could be provisioned on a local or regional basis, in which case local areas would function, from an operational standpoint, more as individual networks. This decision is driven to a greater degree by governance and operational control considerations than by the technology.

Delivering this operational capability, however, requires more than performing the required functions in the network. Roaming, particularly "inter-system roaming" as we have defined it here, requires business arrangements between network operators. This aspect of roaming, which encompasses the commercial and legal frameworks between network operators, consists of two primary elements:

Roaming Agreements: Intra-system roaming can be governed by NSAs and is primarily a function of validating and authorizing users. Roaming between systems, on the other hand, usually involves additional, more formal, arrangements. Commercial carriers exchanging roaming traffic typically execute bi-lateral roaming agreements. These agreements identify geographic areas, define rates and other commercial terms, and specify certain technical requirements. Agreements to facilitate roaming between the NBDS and commercial networks could follow either of the following models, depending on a variety of factors, including whether the D Block is included, and, if it is included, how it is ultimately licensed:

1. Agreements between the PSBL and commercial roaming partners – the preferred model if the entire NBDS is operated by public safety rather than under NSAs with D Block licensees.
2. Agreements between the local/regional operators of "sub-networks" (either public safety "local builders" or D-block licensees).

Roaming Settlements: Roaming traffic is not always symmetrical between networks and, in the commercial context, it is generally necessary for roaming partners to settle net differences through some clearing mechanism. This is one role that companies like Syniverse and TNS play in the roaming process. If, within the NBDS, owners and operators of parts of the network are willing to allow roaming without this type of settlement, the process can be simplified. However, to the extent that significant asymmetries produce a financial burden on some operators or parts of the network, this mechanism may be important even in the "intra-system" context. If a financial settlement is required between entities that are part of the NBDS, it could be managed by the PSBL (perhaps outsourced to a clearinghouse) rather than by individual arrangements between local entities. It is worth noting, however, when considering

these asymmetries, that one important roaming scenario involves mutual aid situations. In these contexts, the beneficiary of the roaming activity is really the region receiving the roaming traffic and it may be inappropriate for a region experiencing a major incident to charge roaming fees to agencies coming to its aid.

The following table lays out the difference between inter- and intra-system roaming as it relates to the three functions discussed above.

	Inter-Network Authentication	**Roaming Agreement**	**Clearinghouse/Settlements**
Intra-System Roaming PS user roaming onto another part of the NBDS outside the home area.	Depends on the architecture. Yes, if each local area operating its own PDSN. No if that function is shared.	Perhaps not, provided that agreements with the PSBL allow the PSBL to facilitate any required flow of funds between owners/operators of local components of the NBDS.	Yes, if a flow of funds is required between owners/operators of local NBDS components.
Inter-System Roaming without commercial D Block licensees PS user roaming onto a commercial network or commercial user roaming onto the NBDS.	Yes	Yes. Likely bi-lateral agreements between the PSBL and commercial roaming partners.	Yes.
Inter-System Roaming with commercial D Block licensees PS user roaming	Possibly. Inter-network authentication may not be required if roaming onto the commercial	Yes. Likely bi-lateral agreements between the PSBL or the D Block licensee in that area and other	Yes.

	Inter-Network Authentication	Roaming Agreement	Clearinghouse/Settlements
onto a commercial network or commercial user roaming onto the NBDS.	network of the D Block licensee serving that PS user's area.	commercial roaming partners.	

Conclusion

Roaming capabilities are essential to providing users of the NBDS with seamless or near-seamless nationwide services. Delivering those capabilities requires functionality in the network to support authentication. It may also require legal and financial arrangements between network operators and between operators and a clearinghouse provider. As with many other issues related to the NBDS, the specific arrangements depend on both technical and governance considerations, including roles played by the PSBL, local builders, and D Block licensees/private commercial partners in building, owning, and operating the network.

12 Appendix E: Operations WG Working Documents

NPSTC Broadband Task Force
Operations Working Group

12.1 Concept of Operations

29 August 2009 – V4

The Operations Working Group of the NPSTC Broadband Task Force (BBTF) submits the following concept of operations with overall recommendations to NPSTC, the Public Safety Broadband Licensee (PSBL), and the Federal Communications Commission (FCC). Terms and definitions relevant to this document are introduced below, followed by enumerated consensus recommendations of the Working Group, and further described through usage scenarios. Time has not allowed development of planned outcome measures.

Change log:

- Version 1 (V1) – Initial draft

- Version 2 (V2) – Draft with changes following first Working Group call to consider the document.
- Version 3 (V3) – Final draft with format changed to move 'Usage Scenarios & Analysis' segments to immediately follow each requirement. Minor additions were made to the 'homepage' and 'location services' items. Minor editorial changes were also made throughout for consistency.
- Version 4 (V4) – Final report with mark up removed and pagination added. No content changes from Version 3.

12.2 Task Definition

The Operations Working Group sought to describe operational requirements between systems, or ***interoperability***, for use of the ***national system*** and ***regional networks*** by regular users of other, compatible public safety and commercially operated networks. It did not address operational capabilities of individual systems or their own users. These requirements describe services required from an operational perspective across systems.

12.3 Terms and Definitions

For internal developmental purposes, the Operations Working Group adapted several terms from the SAFECOM Statement of Requirements (SoR). In the present document, all terms formalized by the Task in "700 MHz BBTF Definitions Document", Version 3 (8-11-2009) are incorporated. They are indicated here in text by the use of ***bold italics***. The following terms and definitions are specialized in this document. They are *italicized* in subsequent use.

- **Operational Scenarios** – Situational end-use circumstances that shape operational requirements.
- **Routine Use** – Use of a visited network for routine or incidental purpose, whether through ***intra- or intersystem roaming***.
- **Mutual Aid Use** – Use of a visited network during an emergency in providing aid to agencies in the jurisdiction maintaining the visited network.
- **Operational Service Scenarios** – Network circumstances that shape fulfillment of operational requirements.

Use of the terms "shall", "must", and "may" in this document are consistent with the intent of the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2119, "Key words for use in RFCs to Indicate Requirement Level".

12.4 Assumptions

The Operations Working Group adopted and has attempted to consistently use the "700 MHz BBTF Assumptions Document", Version 5 (8-11-2009). These supersede assumptions included in

the Working Group's own "Proposed Scope and Deliverables" document, all versions, including the final, Version 1 (7-15-2009).

In addition, the Working Group carried out its work with the following subordinate assumptions established in its "Proposed Scope and Deliverables" document.

- The Operations Working Group will use and will not duplicate previous efforts to develop detailed technical requirements for public safety networks, e.g. reliability, availability.
- Two *operational scenarios* are assumed:
    - *Routine use*, and
    - *Mutual aid use*.
- Two sets of *operational service scenarios* are assumed.
    - ***Intrasystem roaming*** in areas of continuous or discontinuous coverage. Users of similar, jurisdiction-owned broadband wireless networks will roam into or respond in aid to others with networks maintained for similar purposes.
    - ***Intersystem roaming*** in areas of continuous or discontinuous coverage. Users of commercial wireless network will roam into or respond in aid to a jurisdiction that maintains a network itself for similar purposes.

  Geographically, the jurisdictions referenced may be sufficiently adjacent that networks overlap to some degree or they may be sufficiently separated that there would be a gap in service between the two. Technologically, no attempt is made here to define the extent of overlap or service boundaries.

12.5 Operational Requirements

In the following, an initial paragraph following the application or service title states the requirement. Each is followed by a "Usage Scenario" to describe one possible use of the capability and an "Analysis" statement providing further background on Working Group intent.

Two classes of requirements are distinguished in the following by the use of key words in the initial paragraph indicating requirement level. Imperative (e.g. shall, must) or permissive (e.g. may, should) language in the "Usage Scenario" or "Analysis" statements *is not* a restatement of the requirement level established in the initial paragraph. The initial paragraph is the requirement statement.

The Working Group chose to use permissive wording for desired applications and services considered unlikely to be practically implemented initially with public safety broadband networks. It chose imperative wording for those considered to be essential for interoperability.

1. **Internet Access** - Public safety and ***emergency response support*** users shall have access to the global Internet. The Internet will be used to access both home network systems and other systems and services available over the public Internet, including but not limited to messaging systems and web servers.

   - Usage Scenario

   A Public Safety user arrives for mutual aid during a disaster recovery and uses the visited network to access the visited state's web-based EOC management site, a publicly available traffic camera web site, home network e-mail system to correspond, and sets up an IP voice and video conference with a distant incident command post to coordinate activities. Various types and volumes of IP traffic are transported to and from the public Internet by the subscriber device.

   - Analysis

   While network operators (Public Safety, commercial or Public/Private Partnership) may engage in some traffic shaping and traffic or content filtering for network protection purposes, the subscriber should expect broadly open access to the global Internet on home or visited broadband networks. Network operators shall make every effort not to filter traffic unless necessary for security of systems. For example, Public Safety or Public/Private Partnership network operators should not restrict VoIP traffic. Network operators shall publish in a secure manner their particular network restrictions to the PSST so that public safety users understand network or application limitations and appropriate configurations. (These notifications apply to public Internet traffic and do not require agencies to publish internal firewalling information.)

2. **VPN Access to Home Networks** - Regional operators operating in conjunction with the Public Safety Broadband Licensee (PSBL) shall allow establishment and use of virtual private network (VPN) connections by roaming users on their networks to other networks.

   - Usage Scenario

   A police officer from an agency served by a public safety broadband network travels to another jurisdiction to extradite an individual held as a suspect in a crime in the officer's home jurisdiction. The officer uses a broadband network device connected by VPN across the visited regional network to the home network to communicate securely with the home police agency, access criminal records systems that the home agency is responsible to secure, and access office productivity applications hosted by the home agency to submit reports.

- Analysis

Public safety and other public sector users of wireless broadband networks require access to home networks and applications while roaming on other public and commercial networks. Virtual private networks are commonly used to logically extend home networks and provide security for information traversing untrusted networks. U.S. criminal justice agencies accessing Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) Division systems, such as the National Crime Information Center (NCIC) and criminal records systems are subject to the particular security requirements that commonly lead to the use of VPNs.

3. **Visited Area Status/Information Homepage** – ***National*** and ***regional system*** operators shall provide 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 operator deems important to share with visitors to the system. No additional login shall be required, though specific applications accessible through it may have further access, authentication, and authorization requirements.

- Usage Scenario

A Public Safety user arrives on a visited network while responding for mutual aid operations. She opens her browser and automatically accesses an informational welcome page which provides general information and the ability to input credentials for authentication. The page may also warn of specific safety hazards on main roads in the area. Information provided after authentication may include such items as interoperable radio frequency, Incident Command System (ICS) facility locations, command assignment and may also allow input of NIMS-compliant resource typing. A web page provides operational information and allows further access or input based on credentials.

- Analysis

Users visiting a network will need a simple and universal way to obtain basic information. The method for reaching this home page should be straightforward and the same across networks. In addition to displaying basic information about the network itself, this page can and should be used to list available applications, incident information and updates, AMBER alerts and so on. Some information may be on a need-to-know basis and should be protected by credentials issued to the visitor. As new incidents develop, network operators may re-capture users for updates.

4. **Status/Information "SMS-MMS Messaging"** - Public Safety, Public/Private Partnership, and Commercial network operators shall provide the ability for users to send and receive SMS and MMS messages.

   - Usage Scenario

   A Public Safety user arrives on a visited network while responding for mutual aid for disaster recovery. She is able to receive text messages providing status updates on staging locations and voice radio assignments. Once on the scene, she is able to take photographs of damaged infrastructure and send them to the local EOC. She also exchanges multimedia messages with support staff who utilize commercial cellular phones on commercial networks run by various carriers.

   - Analysis

   The ability to send and receive SMS and MMS messages on commercial networks is presently accepted as standard service of commercial data networks. This capability should also be provided on the nationwide network by all network providers.

5. **Land Mobile Radio (LMR) Gateway Devices** - Networks shall allow for connection and operation of Internet Protocol (IP)-based voice ***interoperability*** gateways.

   - Usage Scenario

   A large portion of a region's voice radio system is knocked out by a hurricane, though the broadband network is still operational. Multiple incident commands and an emergency operations center (EOC) are brought up around the area and are staffed by local responders and large numbers of out-of-area mutual aid responders. Each Incident Command Post (ICP) has established local communications but the ICPs and EOC cannot talk to each other. IP-based LMR gateways are brought to each ICP and the EOC and are connected to each other over the broadband network to provide overall command and control communications. The LMR gateway is brought to a command post and connected by Ethernet to a broadband network subscriber. VoIP traffic carries audio from the disparate radio systems back and forth over the IP network.

   - Analysis

   A mutual aid responder should be able to field-deploy an IP-based voice gateway (Examples: Raytheon ACU-2000, Sytech RIOS) to bridge disparate voice systems (Example: LMR systems on different frequency bands or trunking architectures) using the broadband network as some portion of the IP connectivity between gateways. The gateway should be capable of being contacted in any visiting location, i.e. use a static IP.

The gateway will require a broadband network subscriber device to provide an Ethernet port. The setup shall be simple and the authentication and flow of information shall be transparent to the user.

6. **Access to Responders Under ICS** – ***First Responders, Emergency Response Support***, and all other mutual aid responders managed under the ICS structure of a requesting agency served by a public safety broadband networks shall be provided access to that network to carry out incident objectives and communicate with their home networks.

   - Usage Scenario

   A train derailment in a metropolitan area results in a large release of hazardous materials and a fire. Emergency responders from both the immediately affected jurisdictions and mutual aid partners convene on the scene of the derailment. They are managed under the National Incident Command System (NIMS) Incident Command System (ICS) according to national standards. All personnel are provided access to the broadband network serving the scene to carry out their respective tasks in addressing the derailment, as well as to communicate status and other information to their home agencies. An ICS Communications Unit Leader works on-scene during the emergency according to NIMS principles, objectives established in a formal Incident Action Plan, and further guidance from the Incident Management Team to effect the communications requirements of all responders.

   - Analysis

   Responders in mutual aid to agencies served by public safety broadband networks need access to the network to carry out their responsibilities and communicate with the agencies served. The National Incident Management System (NIMS) Incident Command System (ICS) provides a logical framework for command, control, and communications that can be used to determine information nodes and flows. All responders falling within the ICS structure defined for the mutual aid incident may need access.

7. **Field-Based Server Applications** - The ***regional systems*** shall support the use of field-deployed server applications. This requirement includes the need for client devices to consistently and continuously reach these server based systems from any other location on the Internet. The capability is not required for every subscriber device on the broadband network but is limited to a subset of the users that actually require such a feature.

   - Usage Scenario

A public safety user may need to deploy an application for which other client devices will need to find the application server for that service where the server is deployed anywhere on the broadband network and the clients (or other servers) are located anywhere on the Internet. In other words, the visiting network must be capable of the equivalent of a static IP address that is reachable from any public IP address (while this is not the proscribed solution, it is merely included as an example of an acceptable solution). A variety of scenarios exist where this feature could become required. For example, a mutual aid agency could field-deploy its command bus that is equipped with email, VoIP, video, and web servers to facilitate communication at a major incident. These applications would need to be reachable by their respective clients.

- Analysis

The broadband public safety systems must support the field-deployment of application servers. The servers will likely be deployed as part of a mutual aid operation whereby applications are delivered as part of the overall emergency operations (e.g., a command vehicle serving email). In order for incident client devices to be able to communicate with these servers, the system must support a method for them to communicate with the server anywhere on the national broadband network and while the devices are anywhere on the Internet. It is anticipated that servers will consist of the majority of cases where this capability is needed, however, it is possible that other scenarios may necessitate consistently reachable client devices. Therefore, the system should provide such capability to any subscriber device requiring such capabilities be it a subscriber that provides connectivity for a server or client. It is not required that all devices shall have this capability.

8. **Location Based Data Capability -** National ***system*** and ***regional networks*** should include the capability to collect and convey subscriber unit location data in real time. The technical ability to covey location information should be inherent on any public safety network and associated commercial networks. Location data should be accessible to appropriate applications, as may be authorized by management level policy. Location data applications may be located on both subscriber units and associated agency level command/control applications. Subscriber units of future public safety networks should meet the same minimum location data information requirements (format and accuracy) as is currently applicable on current commercial services networks in order to retain a broad level of compatibility with incumbent systems. Any device on the national broadband network, independent of its home network location, would be able to be located using the network assisted location technology on any portion of the national

network, with administrative controls for the capability to be disabled as required by using agencies.

- Usage Scenario

A police officer from an agency served by a public safety broadband network travels to another jurisdiction to extradite an individual held as a suspect in a crime in the officer's home jurisdiction. The officer uses the location based data capabilities of the of broadband user device to navigate with software applications on the device provided by the home agency. Another application provided on the device by the home agency periodically transmits the officer's location to a home computer-aided dispatch (CAD) system to track the officer for safety purposes.

- Analysis

Location based data information is the fundamental geo-spatial data information indicating the physical location of a subscriber unit in real time. The network administrator may use any technical means to provide location based data as may be appropriate for their specific network as long as the method meets the appropriate functionality of this capability.

Location identification technology is proving to be an invaluable tool for managing mobile fleets. In the public safety LMR role, it is referred to as AVL used to track and manage a mobile work force. In commercial services, it is referred to as Location Based Services to generate Wireless Enhanced 9-1-1 location status and additionally has many other commercial applications. Location is typically developed by subscriber device initiated GPS reception and/or infrastructure based location support. Location identification capability will have a large base of application possibilities ranging from subscriber unit navigation to personnel/equipment tracking and management. Location services have a significant safety-of-user component as well as utilitarian management applications. Location data access needs to be managed by either the subscriber unit or agency application in order to address security concerns.

9. **One-To-Many Communications Across All Media -** Regional operators should provide one-to-many communications capabilities to outside network users responding in mutual aid to the operators. 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.

   - Usage Scenario

   A large propane tanker catches fire in a metropolitan area, putting many citizens at risk should the tanker bleve. Emergency responders from both the immediately affected jurisdictions and nearby mutual aid partners work rapidly in concert to evacuate threatened businesses and homes. The Incident Management Team relies on the use of the broadband network to convey regular status updates concurrently by text messaging to all Operations Section supervisory personnel.

   - Analysis

   First responders and other emergency response support personnel rely on the one-to-many communications provided by traditional land mobile radios. As responders increasingly rely on other media of communications, the need for one-to-many exchanges continues. Jurisdictions have an obligation to provide communications services to responders providing them mutual aid. For purposes of scope, a video broadcast to up to 10 simultaneous receiving users at the scene of an incident is estimated as the practical maximum one-to-many usage expectation. Simultaneous receipt of video means that all recipients are able to see the same image at the same time.

10. **LMR Voice** - 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.

    - Usage Scenario

    A responder arrives in an area served by a broadband network for mutual aid and connects to the Public Safety network with a handset. He calls the universal "hailing"

number/channel and requests assignment and asks to be patched to the incident command assignment channel/talkgroup for further instruction. The broadband network subscriber with microphone and speaker for two-way audio places a cellular voice call to a universal “hailing” number or destination to reach a dispatch center and is later patched to the agency LMR system for voice interoperability.

- Analysis

Different than the "LMR Gateway" interface, this should provide a fixed interface to agency LMR systems such that broadband network subscribers with voice service can be connected or "patched" to existing agency voice radio networks for communications interoperability. As with the existing 800 MHz national calling channel, an authoritative dispatch agency should monitor any calling channel/number provided by the broadband network. Operators may restrict visiting users to only specific hailing/calling channels until further authorization by the control point. Operators may further restrict certain groups or classes of users to a listen-only mode if appropriate. While this interface is not obligatory, it is imperative we come up with a national, interoperable solution such that this functionality works the same in every network.

11. **PSTN Voice** - Public safety 700 MHz voice capable devices such as cell phones, personal digital assistants (PDAs), and their equivalent should be capable of placing and receiving full-duplex telephone calls to any telephonic device on the Public Switched Telephone Network (PSTN) in the visited network with the same functionality that cellular telephones operate nationally today. This includes location based PSAP call routing, E911 Phase II location transmission, and, if necessary CALEA. In the case where the user transitions in to or out of one regional system, the voice session shall be handed off between the two networks with limited loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement.

- Usage Scenario

Public Safety subscribers shall have access to the global Public Switched Telephone Network and it's full-duplex voice capabilities. When a public safety user roams in to a visited network, the public safety user shall have access to voice telecommunications services using commercially available cell phone like devices. This includes the ability to place and receive phone calls while in the visited network. The network operator shall make reasonable efforts to provide good audio quality on the network and it is recommended to block or queue calls in the event that network resources can not

sustain a good call. The visited network is not required to provide these voice services; only provide the conduit for them to be successfully delivered in visited region.

- Analysis

This capability may not be available on the outset of broadband service due to the business plans of the public safety and commercial carriers. In advance of this, it is expected that public safety voice needs will be met using a variety of proprietary or open source non-mobile based VoIP solutions. When the commercial market does mature to allow for such devices using 700 MHz LTE, the public safety devices should accommodate nationwide voice roaming and do so in an interoperable manner. It is acceptable to implement this capability in the same manner that the cellular carriers implement the feature, including, if necessary, using 2G/3G voice networks. In that case, however, the regional network shall be required to redirect the LTE user to a 2G/3G network capable of supporting local voice capabilities.

13 Appendix F: Technical WG Working Documents

NPSTC 700 MHz Broadband Network Requirements Task Force (Task Force)

Technical Working Group

700 MHz LTE Network Interoperability

13.1 Scope

This paper documents the minimum requirements necessary to enable roaming between LTE networks built by multiple, independent public safety organizations and commercial service providers, where roaming users will have initial access to the Internet, <additional applications/services as defined by operations WG>.

This does not prevent organizations from deploying additional applications/services that are available to roaming users, but provides a minimum expectation.

13.2

13.3 Table of Contents

LTE Network and Device Specifications *50*
System Identifiers *51*
Frequency Spectrum *55*
Network Interfaces *56*
Mobility and Handover Implications *60*
Inter-network Authentication and Connectivity *61*
Devices *62*
Standards Testing *62*
Applications and Quality of Service *63*
LTE Security *65*
Appendix A - Definitions *67*
Appendix B – Commercial and non-3GPP roaming *72*
Appendix C – PLMN ID Info *77*
Appendix D – 3GPP Standards *81*

13.3.1 LTE Network and Device Specifications

Roaming is defined as:

- Roaming minimally requires a device capable of 700 MHz radio network interoperability based on the commercial 3GPP LTE standards.
- In the absence of RF coverage from the home network, the ability for the UE to scan supported bands, perform cell selection and authentication on a visited network
- After authentication on a visited network, the assignment of an IP address, and the ability to communicate with the public Internet, obtain local services as applicable, or access the home network to obtain services supported by the home provider.

Interoperability is defined as:

- The capability to automatically (roam) onto a visited network and have access and share appropriate information/services as authorized.

Based upon discussions with the Work Group leads, service providers, and industry, we recommend four categories of roaming for the Technical Work Group (in order of importance) to focus work on.

1. Roaming between 700 MHz public safety LTE networks – e.g., UE from Newark, New Jersey works in New York City. Assumption is that both networks involved in this roaming scenario (visited and home networks) are Evolved Packet Core/System Architecture Evolved (EPC/SAE) networks. This will be defined as intra-network roaming.
2. Roaming between private 700 MHz public safety LTE and D Block Shared LTE Network – could also be another 3GPP or non-3GPP technology. As defined per current FCC D Block plans for regional licensing.
3. Roaming between 700 MHz public safety LTE networks to commercial 700 MHz LTE networks – e.g., UE from San Francisco (home) roams to local Verizon/AT&T (visited) network and roams back.
4. Roaming between 700 MHz public safety LTE networks to commercial and private broadband networks (3GPP and non-3GPP) in other bands. – e.g., UE from San Francisco (home) roams to local AT&T HPSA (visited) network and roams back.

NOTE: Category 1 and 2 may be combined if the D Block is reallocated to public safety as recommended by the BBTF, this would include operation over both the D and PSBL blocks .

Categories 2, 3, and 4 can generically be called inter-network roaming and even further defined as inter-RAT (Radio Access Technology) and inter-frequency networks.[8] The initial scope of the group will be to define the minimum set of interfaces required to support intra-network (category 1) roaming. The work for this (similar/common interfaces) can then be applied to the remaining roaming categories. Since the LTE specification was chosen and it is based on the 3GPP standards, the required interfaces have already or are in process of being defined. This document will merely reference those interfaces that we deem necessary to fulfill our interoperability needs.

It should be well understood that the LTE standard (3GPP Release 8) is a relatively new standard in which a first draft was just accepted in March 2009. Features and performance will grow with each release and iteration of LTE. NOTE: Previous standards work and deployment of existing W-CDMA, WiMAX, and EVDO networks often happened 2 to 5 years after the standards were adopted.

13.3.2 System Identifiers

Several waiver requests from states and cities have been submitted to the FCC to approve the deployment of broadband networks on the PSBL spectrum. The likelihood of having regional networks is very probable – public safety will become a mobile broadband operator. Unanimous consensus was reached in the Technical Work Group based on the fact that a common methodology of identifying public safety networks is required.

In 3GPP networks, the term Public Land Mobile Network (PLMN) is used to describe the Home (HPLMN) or visited (VPLMN) networks for roaming use cases. Standards describe the International Mobile Subscriber Identity (IMSI) that is used by both 3GPP (GSM) and 3GPP2 (CDMA) to uniquely identify every user. In 3GPP networks, every terminal contains a USIM (Universal Subscriber Identity Module) smartcard that permanently stores a unique IMSI and a secret key that is used for authentication. It consists of a 3 digit Mobile Country Code (MCC) and a 2 or 3 digit Mobile Network Code (MNC), which creates the Home Network Identifier (HNI). The addition of a unique 9 digit Mobile Station Identification Number (MSIN) creates the IMSI. Users are identified typically by their PLMN ID and more specifically their IMSI.

[8] See NPSTC Broadband Task Force Governance Group Roaming Whitepaper

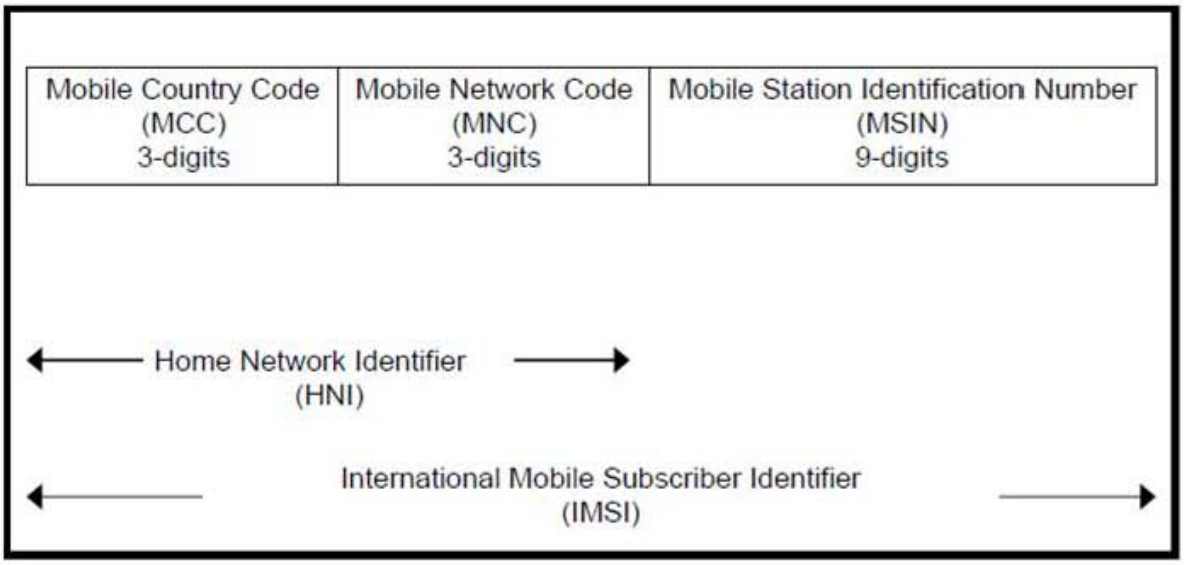


Figure 1: IMSI

In order to differentiate the public safety networks from each other, commercial networks and yet enable them for roaming, a PLMN and IMSI assignment process will be developed for public safety LTE networks. Currently the United States has MCCs 310 – 316, and code 310 has been used to avoid international roaming ambiguities. The MNC is a three digit number (999 possible combinations) that network operators use to differentiate themselves and so that limits the amount available to public safety networks. The Home Network Identifier (HNI), which is a combination of the MCC and MNC is used to identify the PLMN. HNIs are administered by Telcordia according to procedures established by the IMSI Oversight Committee (IOC) which is a committee of the Alliance for Telecommunication Industry Solutions (ATIS). Unique HNI's are required to distinguish between eNodeBs from home and visited networks. The PLMN part of the IMSI (which is stored in the UICC card of the device) is used to determine the proper HSS to query for subscriber information.

Alliance for Telecommunication Industry Solutions (ATIS) and the IMSI Oversight Committee (IOC) have expressed their willingness to work with public safety representatives in assigning PLMN IDs. This will be necessary as IOC rules state that to qualify for a HNI, the following must be criteria must be met and the PSBL does not currently meet these.

- Applicants must offer public telecommunications service. Public telecommunications service is defined as a public service, the subscribers to which must be capable of being reached over the PSTN.1.
- In the event an applicant is providing network services but is not a public mobile operator, the applicant must be at least an associate member with the Global System

for Mobile Communication (GSM) association or other recognized/approved industry governing body, and submit evidence of same.

- Applicants must offer non-discriminatory access of this resource to users. That is, the applicant must offer the availability of services to any end-user customer requesting the service.

These rules are designed for circuit-switched services (voice) and not the data networks being proposed. The PSBL or whomever the governance group determines is a public safety representative will need to address this issue.

It is unlikely that multiple hundreds of PLMN IDs will be assigned for individual public safety networks due to limitations within the IMSI specification. This is an issue that will need to be addressed for early system deployments so that public safety networks can be differentiated from each other and commercial networks.

In order to use LTE systems and devices complying with 3GPP standards, provide for support of the four roaming categories, and for early public safety network deployments – they must assigned a PLMN ID. Since PLMN IDs are a limited resource shared by all 3GPP wireless networks worldwide, the use of PLMN IDs should be effectively managed. The Technical Work Group has considered two alternatives for assignment of PLMN IDs:

3. Single PLMN id shared by all public safety networks.
4. Individual PLMN id for each public safety network.

Both implementations have specific considerations and implementation issues as shown in the table below and more detailed information is available in Appendix C.

Consideration	**Single PLMN id shared by all PS networks**	**Individual PLMN id for each network**
Coordination for Non-overlapping IMSI	PS agencies must coordinate usage of MSIN to avoid overlapping IMSI.	Unique PLMN ID for each PS agency assures non-overlapping IMSI.
Identifying the HSS containing HSS subscriber data	If multiple HSS are used (one for each regional PS network or a few regions pool their resources to buy and maintain an HSS but it is still not national) a Diameter Redirect or Proxy Agent as described in TS 29.272 is required. The Diameter Agent must be operated as a shared entity for all regional PS	Unique PLMN ID can be used to identify the correct HSS in both the roaming and non-roaming cases.

	networks. The Diameter Agent must use info from MSIN to identify the correct HSS. An alternative is to share a single HSS among all regional PS networks.	
Determining the home network for usage records for roaming	May require an additional centralized process to accept usage records from roamed networks and forward to correct regional PS network based on additional information beyond just the PLMN ID. However in some cases the roaming user may be accessing local services, in which case the visited network needs to generate records to send to the user's home network for purposes of charging. This should not be any different in public safety networks and may not be difficult to implement.	Follows industry practice of sorting by PLMN ID
Cell ID transmitted by LTE cells contains the PLMN id. Cell ID is used by mobile device to determine on which network to register and is a factor in eNodeB handover decisions	Cell reselection, which will trigger PLMN selection, is controlled via specific parameters. A potential problem is when a UE with home network coverage may attempt to roam on a visited network if the signal strength is stronger than the home network cell. Ideally a user moving out of coverage will have its device look for other networks based on a specific threshold and hence move to that network. When coming back to its own network, the device still searches for cells and when it finds its "home" PLMN it jumps back to that cell. There is also the possibility of manual PLMN selection when a user can request the device to scan for available PLMNs and order the device to select one.	Having each regional PS network have its own PLMN ID follows standard industry practice.
Users roaming on a visited network will have the same PLMN ids as home users. PS	MME must make decisions to lower priority based on something other than PLMN ID – APN for example. In this case the priority is not determined by the PLMN of the user but rather the subscription	MME can make decisions to lower the priority of visiting users based on PLMN ID. This is a relatively simple

assumptions state that visiting users should be assigned lower priority than home users	of the user. Can potentially be done statically where roaming users always get lower priority after restrictions apply. May be more difficult provisioning task since APNs change more frequently than PLMN IDs.	extension of data already present in the MME to control which customers are allowed to roam using PLMN IDs. Follows industry practice.

Table 1 - PLMN ID

The following are recommendations for public safety PLMN ID allocation and implementation:

7. A common schema should be used to identify public safety users and public safety regional LTE networks (intra-network – category 1 roaming).
    a. Which PLMN ID scheme should be implemented?
    b. Schema for intra-network (category 2, 3, 4) will not be explicitly defined with the exception of specific network interfaces.
8. PSBL will apply for dedicated PLMN ID (MCC/MNC/HNI) from the IOC
9. Use an existing MCC as determined by ATIS and IOC.
10. USIM is provisioned by the home network administrator with
    a. Home IMSI (HPLMN).
    b. Prioritized list of permitted VPLMNs.
    c. Forbidden PLMNs list.
11. For voice, MMS, SMS and PSTN support, the PSBL and/or public safety representatives should coordinate and manage MSIN - ITU-T E.169 PSTN number allocations.

13.3.3 *Frequency Spectrum*

The waiver requests and the likely intent of the FCC are to grant spectrum in the public safety band only and not the adjacent D Block (this is all subject to change – as with New York City latest filing).

This creates a possible issue with how 3GPP defines band classes. 3GPP TS 36.101 v8.6.0 defines band class 14 is for 10 MHz wide channels using Frequency Division Duplex (FDD). This band class includes both the D-Block and public safety band as one contiguous band class.

The public safety specific band is defined for operations in 763-768 MHz and 793-798 MHz range. 3GPP/LTE supports multiple and scalable bandwidths. Within band class 14, 5 MHz channels sizes are supported and can therefore accommodate public safety 5 MHz allocations.

Recommendation is that networks and devices deployed for public safety have the minimum capability to support 3GPP TS 36.101 v8.6.0 band class 14 and make band classes 12, 13, and 17 optional. Pending the waiver grants, operationally the network and devices may initially only use the upper 5 MHz, public safety band only – again this is subject to change pending.

E-UTRA Operating Band	Downlink (DL) operating band BS transmit UE receive	Uplink (UL) operating band BS receive UE transmit	**Duplex Mode**	**Channel bandwidth $BW_{Channel}$ [MHz]**	**Transmission bandwidth configuration N_{RB}**
14	758 – 768 MHz	788 – 798 MHz	FDD	10	50
14 - PS	763 – 768 MHz	793 – 798 MHz	FDD	5	25
14 – D	758 – 763 MHz	788 – 793 MHz	FDD	5	25

Table 2 - Band Class– Note that 3GPP only defines band 14, the –PS and –D suffixes are for a more detailed Public Safety definition of the sub band characteristics.

The use of full duplex, FDD will be the primary access method used in public safety LTE networks. The use of half-duplex FDD will not be supported by public safety due to issues with time to market, data throughput loss, lack of supporting UE and eNodeB equipment.

13.3.4 Network Interfaces

The LTE/SAE/EPC architecture has several defined interfaces for interoperating with the network. These interfaces will allow users to roam into networks via these interfaces. In discussions with the Work Group leads, vendors, service providers, and public safety the ***initial*** goal for network roaming and interoperability is defined as allowing users who leave their home network to authenticate automatically (roam) onto a visited network and have access to:

1. Public Internet access.
2. Best effort data.
3. VPN access to their home network.

LTE, EPC, and IMS are maturing technologies and as new features and capabilities are added, public safety will be able to utilize these. Optional features within an LTE network are Quality of Service (QoS), Priority, and Pre-emption. These are essential features to many future public safety applications and may be implemented in future regional networks. Having those features follow a user when they roam into another network is not within the scope of this initial document. The amount of complexity, application service delivery, availability of

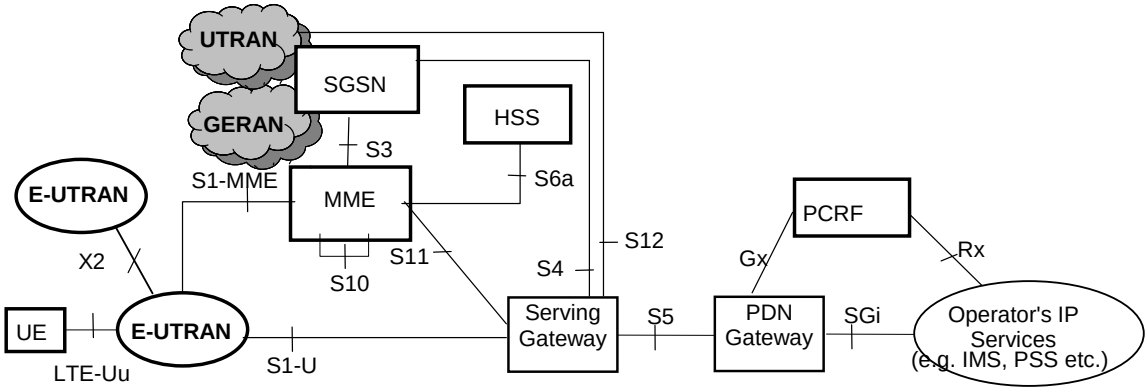
equipment, and overall timeline for this work group do not allow us to address this fully. However, it is fully understood that these features are key to a public safety network and we will continue to research the best possible implementations.

As network and application functionality increases, public safety enhancing features such as QoS, multicast/broadcast (MBMS – Release 9 target) and priority can be added to the roaming capabilities. This may require that supplementary roaming agreements be allowed between agencies and commercial service providers.

It is assumed that each network built out be a 3GPP Evolved Packet Core (EPC) network. We will define the system interfaces and the roaming cases necessary to support intra-network roaming (Category 1).

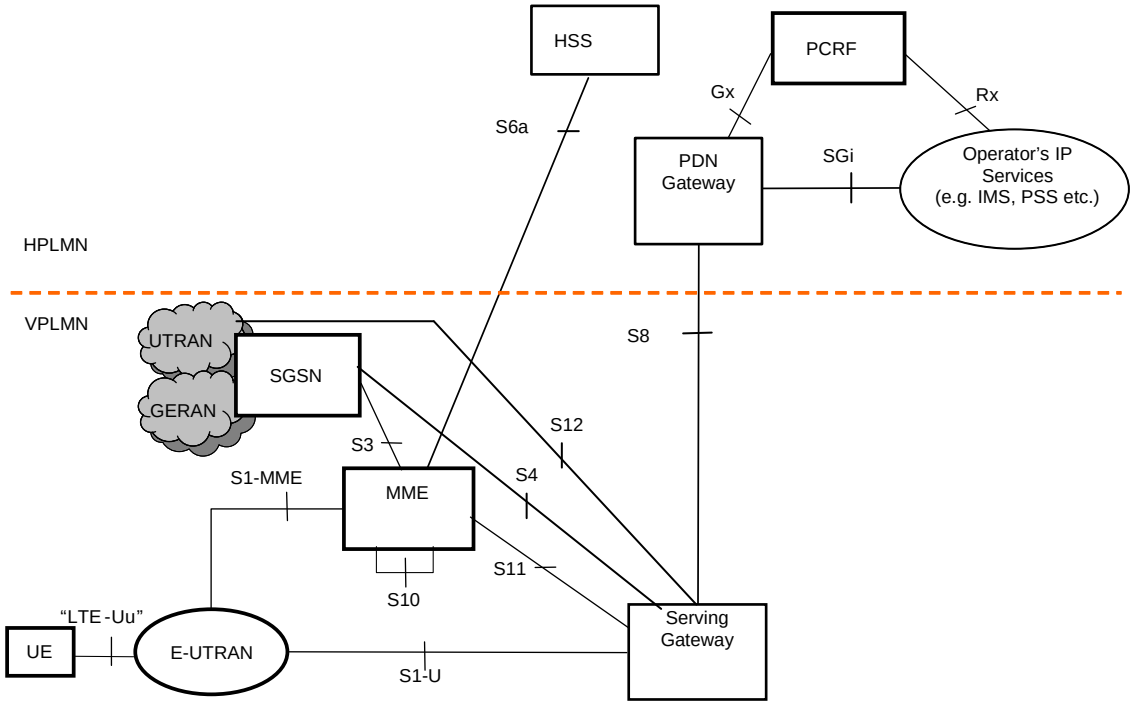
In general the network should support initially support LTE to LTE handovers (Category 1 and 2) as per 3GPP Release 8 Specifications (March 2009). See Appendix D for more detailed information regarding the specific 3GPP documents.

The following section uses multiple diagrams and network information from 3GPP TR 23.882, 23.401 and 23.402.

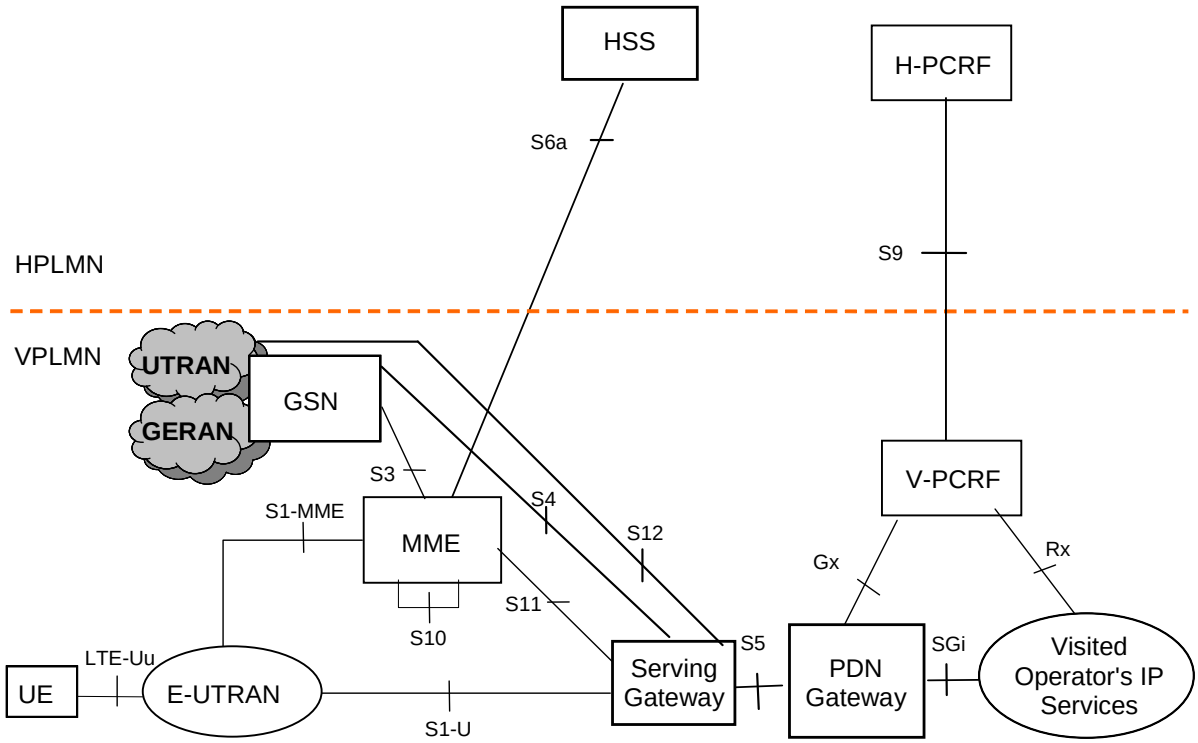


The general system diagram (PLMN) shows several new interfaces. What we need to determine is what interfaces are required to support our roaming scenarios and when they will be available from the vendors.

To support the four categories of roaming, it may be necessary to support roaming traffic that is homed to both the Home PLMN (HPLMN) and the Visited PLMN (HPLMN). An example would be web access while roaming; the UE would not be required to route traffic through the VPLMN to the HPLMN but instead utilize the Internet access via the VPLMN. In the instance that you use a VPN to get email or database access, then payload traffic would flow from VLPMN to Internet to Home Internet portal (VPN), then to local applications.



EPC Roaming architecture – Home routed traffic



EPC Roaming architecture – Local Breakout

To support initial network build outs that support roaming for category 1 networks the following interfaces are required:

5. Uu – LTE Air Interface
6. S6a – Visited MME to Home HSS - Diameter signalling

<u>The following interfaces are highly recommended to fully support category 1, 2, and 3 networks:</u>

7. S8 – Visited SGW to Home PGW
8. S9 – Visited PCRF to Home PCRF for dynamic policy arbitration. The S9 is primarily used for QoS functionality from the PCRF but its inclusion will allow easier migration to a QoS enabled network.
    a. Gx – PGW to PCRF interconnection required if S9 is implemented
9. Multi-vendor interoperability (IOT) supported on the S1-MME and S1-U interface between the eNb and the EPC
10. X2 – Intra-network eNodeB connection shall be required within a homogeneous public safety 700 MHz regional network – this does not include geographically adjacent systems
    a. IOT required for multi-vendor support

Category 4 roaming and network diagrams are covered in Appendix B.

13.3.5 Mobility and Handover Implications

Handover is the process that happens when a UE moves from coverage of one cell to the coverage area of another cell. (The assumption is that the UE is in the RCC connected state, else if the UE is in the idle state, it is a cell reselection per the RRC state machine.) LTE supports the use of two types of handover delivery mechanisms called seamless and lossless handover. How each of these handover delivery mechanisms are applied is dependent on the QoS assigned to the radio bearer. UE active session handover is accomplished via the S1 or X2 interface.

Handover requirements will be as follows:

- Handover of active sessions on geographically adjacent public safety 700 MHz LTE networks. Intra-network handover for data session between home and visited networks is required. This is defined as intra-RAT handover.
    - These types of handovers will be subject to pre-arranged roaming agreement(s).
- Handover of active sessions between home and visited networks is not required when a visited network is using another RAT such as 3GPP2 or another release of 3GPP (e.g., Release 7). This is defined as inter-RAT handover.
- After handover from the 700 MHz public safety LTE network to a commercial carrier (inter-RAT), the user may come back (idle and active) into the coverage area of their home network. The cell search mechanisms should support the ability to identify the public safety LTE neighbor cells.
- Public safety networks should be the primary networks for cell reselection. As such the white-list maintained on the UE, PLMN IDs, or the equivalent of the neighbor cell list (NCL) should be programmed to facilitate public safety LTE networks as the primary choice.

Pending the outcome of the waiver requests and the potential addition of voice capability or if the FCC requires this by rule, the implementation of lawful intercept (CALEA) may be required on the public safety LTE network. The MME, PGW, and SGW have the necessary interfaces to support this functionality and public safety LTE networks should use 3GPP TS 33.107 v8.8 (or later) as a reference on how to support this functionality.

13.3.6 Inter-network Authentication and Connectivity

In order for roaming and more specifically authentication to be enabled, there must be several interfaces that are connected between each home and visited network. To support this, multiple leased lines would be required, thus putting a large technical and financial burden on the public safety network. Commercial service providers traditionally use third party clearinghouses to provide their roaming authentication and interworking functionality. This allows inter-RAT roaming such as CDMA and GSM to interwork with each other (e.g., GPRS Roaming Exchange (GRX) and CDMA Roaming Exchange (CRX)), number portability, SMS/MMS/IM, and many other functionalities that follow users as they roam. In addition, roaming fraud has been a serious problem for operators. To combat this growing problem, the GSMA has implemented Near Real Time Roaming Data Exchange (NRTRDE).

Public safety should utilize similar methodologies for roaming to enable them the most flexibility and cost savings. A third party commercial interworking provider can support a common authentication scheme for all public safety networks, thus supporting both inter- and intra-network roaming.

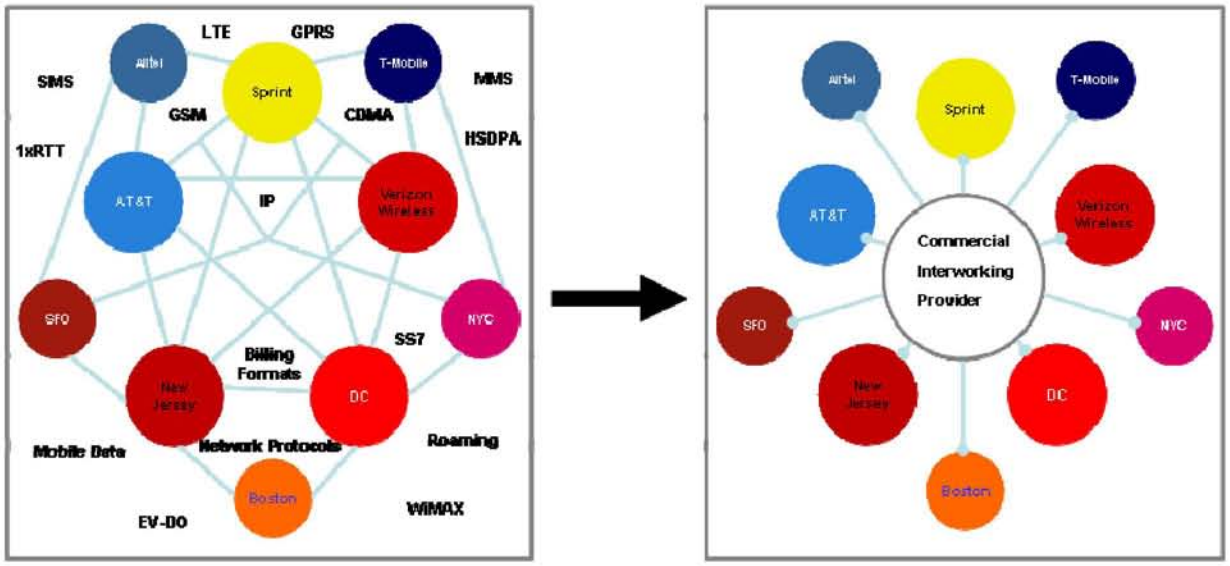


Figure 2: 3rd Party Interworking

Interwork Connectivity Recommendations

1. A common/single third party clearinghouse should be utilized by public safety
    a. PSBL and/or public safety representative will determine specifications based upon bi-lateral roaming agreements.
2. All 700 MHz public safety LTE networks will utilize a similar authentication scheme.
    a. Implementation of NRTRDE between public safety networks and between public safety and commercial networks to combat fraud and facilitate the exchange of roaming data.
3. Provisions should be allowed to directly interconnect geographically close 700 MHz public safety LTE networks to each other.
    a. Directly connected networks will need to ensure to PSBL and/or public safety representatives that all proper authentication credentials are processed accordingly.
4. Redundant, geographically separate third party clearing house centers will need to be supported to address disaster scenarios.
    a. Back-up solution will need to be available to authenticate roaming users when third party network isn't available and mutual aid is required from roamers.

13.3.7 Devices

Public safety LTE devices will initially share or be the same as commercially available devices. Initial devices for the LTE market in the U.S. will consist of PCI Express and USB dongle configurations. Smart phone and phone-type devices will likely follow on in the 2011 timeframe. The minimum requirements and specifications, but not limited to, for a public safety device are the following:

1. Band class 14 should be supported for 5 and 10 MHz channel sizes in Frequency Division Duplex (FDD) mode as per 3GPP TS 36.101 v8.6.0.
2. USIM should be unlocked to allow public safety users to switch out UICC cards between multiple devices.

Optional requirements and specifications

1. IMS authentication and services via support of the ISIM as per 3GPP TS 31.103: *Characteristics of the IP Multimedia Services Identity Module (ISIM).*
2. Multi-mode support of 3GPP Rel. 7 HSPA and/or 3GPP2 EVDO Rev. A.
3. Multi-band support for 3GPP & 3GPP2 commercial 700, 850, and 1900 MHz bands.

13.3.8 Standards Testing

LTE has been selected as the wireless broadband standard for public safety. There is already a very robust test methodology in place due to the fact that LTE is being adopted by commercial service providers worldwide. The conformance-test standards (TS) are split into two document— the three-part TS 36.521 deals with all the transmitter and receiver tests and RRM) while 36.523 deals with the signaling (protocol) tests. Within 3GPP RAN WG1 – WG4, they are working on system level tests and RAN WG5 are working on UE-related tests. (ETSI/3GPP have over 400 mandated tests already.)

3GPP Special Task Force 160 (STF 160) is working on using TTCN3 as the test language for LTE and have all leading manufacturers working in that group. ETSI and 3GPP are working closely with the Global Certification Forum (GCF) Ltd and the PCS Type Certification Board (PTCRB) to select a certain number of test cases and define how many test cases must be passed to certify the device under test. These test cases are then executed by accredited test labs such as Cetecom and 7 Layers.

The minimum requirements and specifications, but not limited to, for a public safety 700 MHz LTE standards testing are the following:

1. Minimally, public safety 700 MHz LTE infrastructure and subscriber equipment will need to have been tested and certified by the aforementioned 3GPP test suites that the GCF is overseeing.
2. If GCF testing is not available within the timeframe of network deployment, the vendors and public safety network operators should have the option to perform specific testing as determined by the PSBL and/or public safety network representative.

13.3.9 Applications and Quality of Service

Within the Evolved Packet System (EPS), IP connectivity is provided between the UE and the PLMN external packet network; e.g., Public Internet Access, this is called PDN Connectivity Service. As defined by the scope of this Work Group, the primary application for users who are roaming will be Internet access. Specific applications as defined by the Operations Working Group include but are not limited to the following:

1. Internet access
2. VPN access to home networks
3. Visited network home page
    a. Intra-network roaming users will have a common webpage, text message or delivered information on applications and services offered by the visited network and relevant alerts.
4. Text messaging

    a. Application level SMS over IP will be allowed but recommend the use of a common SMS delivery system as described in 3GPP TS 23.204 V8.4.0 and 3GPP TS 24.341 V8.1.0
        i. *NOTE: Inclusion of this specification may require the use of the IP Multimedia Subsystem (IMS).
    b. Current SMS capability is supported via media gateways that are designed for control plane/circuit0switched networks. Legacy SMS support is tentatively scheduled for 3GPP Release 9 (or 10 depending on the delivery platform).
        i. Will follow 3GPP development and industry trends for supporting legacy SMS.
5. Location identification
    a. Location Based Services will require user plane interfaces as opposed to current circuit switched PDE type implementations.
        i. Under investigation by technical working group for solutions and will track industry trends.
        ii. Will require unified support from chipset, subscriber, and infrastructure vendors.
    b. User and control plane support for LBS targeted for 3GPP Release 9.
6. LMR gateway interconnection
    a. Use of the latest Bridging Systems Interface Specification (BSI) is the recommended LMR gateway interconnect

Desired Applications – These requirements are under continuing investigation by the Technical Work Group.

1. LAN bridging to broadband networks
    a. This will likely require the use of wireless router and need to utilize QoS to prevent overloading the cell.
2. One-to-many communications across all media.
    a. Multimedia Broadcast Multicast Service (MBMS & E-MBMS) for LTE is scheduled for 3GPP Release 9.
        i. Further investigation on requirements is necessary to determine system impacts and implementations.
3. Commercial Mobile Alert System (CMAS-Public Warning System)
    a. Defined by the FCC under Part 10 rules, to handle broadcast of geo-targeted imminent threat to life or property emergency alerts distributed by the federal government though a CMAS aggregation function under the FEMA iPAWS program.
        i. This includes deployment of a CMSP Gateway in the public safety network to receive the alerts from the FEMA Federal Alert Gateway, and distribution of those alerts in the LTE network via a Cell Broadcast Center.

        ii. ATIS and TIA, in conjunction with FEMA, have defined the interface between the Federal Alert Gateway and the CMSP Gateway, and ATIS is developing specifications for supporting CMAS on LTE.
        iii. PWS, which includes CMAS support, is scheduled for 3GPP Release 9.
    b. Support for CMAS functionality in the mobile devices consistent with the Joint ATIS/TIA CMAS Mobile Device Behavior Specification (J-STD-100, January 30, 2009).
        i. Public safety mobile devices should give consideration for support of the Required Monthly Test (which do not go to consumer devices).
4. E-911 support for Part 90 systems
    a. Investigate the necessity to support E-911 for initial data only public safety LTE network.
    b. Also address FCC requirement based upon PSTN voice capability added to public safety LTE network.
    c. Investigate control plan implementation impact for IMS based emergency calls.

Quality of Service (QoS), priority, and pre-emptive access are all important features to public safety networks. Within 3GPP Release 8, QoS is defined in TS 23.401 and in TS 23.203. Public safety networks should utilize QoS as defined in these documents.

The EPS uses logical channel bearers (bearer), pre-defined QoS values, Uplink Traffic Flow Templates (TFT), and Downlink TFT to enable QoS. Many other parameters such as the APN-AMBR, UE-AMBR, QCI, ARP, GBR, MBR, and several others need to be defined. These parameters must then be mapped across the network, mapped to the roaming networks (commercial and public safety), and even to 3G networks. The goal of standardizing these interfaces and parameters is to ensure that the services and applications mapped to a QoS class receive the same minimum level of QoS when roaming or within a multi-vendor deployment. Needless to say this is a complicated and important aspect to designing networks that enable QoS. Continuing work will be required to create templates for public safety applications and services. It should be noted that the use of dynamic policy control (PCRF) used within LTE will minimally require the Rx and Gx interfaces.

13.3.10 LTE Security

For network and subscriber security, it is recommended that common 3GPP authentication and security is used for public safety networks.

3GPP LTE supports the Authentication and Key Agreement (AKA) scheme as defined in TS 33.401. The credentials that are exchanged are the IMSI, and the permitted network service

capabilities are fetched from the Home Subscriber Server (HSS). The Packet Data Convergence Protocol (PDCP) layer processes the security functions for the radio bearer. These security functions include:

- User Plane - integrity protection and verification of data.
- Control/User Plane – ciphering/deciphering of data.

These security features are never deactivated in a LTE network and will be used in public safety LTE networks. Possible exceptions would be an emergency call without a USIM.

The Radio Resource Control (RRC – TS 36.311) protocol layer may optionally implement LTE signalling layer security features. The Network Access Stratum (NAS – TS 24.301) protocol layer may optionally implement EPC signalling layer security features. The Packet Data Convergence Sublayer (PDCP – TS 36.323) protocol layer may optionally implement user data plane security features. For public safety LTE networks, these optional security layer features specified in 3GPP TS 33.401 should be implemented.

The use of network layer VPN will be allowed on public safety LTE networks. VPNs provide secure communication tunnels to home servers/applications and can support (e.g., NCIC/CJIS, AES, and HIPPA) public safety security requirements. Coordination of ports and QoS will need to be determined as necessary between home and visited networks.

Continued research and requirements can be fed into 3GPP Release 10 where a study on new Encryption and Integrity EPS security algorithms, which could include public safety-specific requirements, is being done.

13.3.11 Appendix 1 - Definitions

The following are LTE Interfaces: (Ref: TS 23.401 v 841)

- **S1-MME** :- Reference point for the control plane protocol between E-UTRAN and MME.
- **S1-U**:- Reference point between E-UTRAN and Serving GW for the per bearer user plane tunneling and inter eNodeB path switching during handover.
- **S3**:- It enables user and bearer information exchange for inter 3GPP access network mobility in idle and/or active state.
- **S4**:- It provides related control and mobility support between GPRS Core and the 3GPP Anchor function of Serving GW. In addition, if Direct Tunnel is not established, it provides the user plane tunneling.
- **S5**:- It provides user plane tunneling and tunnel management between Serving GW and PDN GW. It is used for Serving GW relocation due to UE mobility and if the Serving GW needs to connect to a non-collocated PDN GW for the required PDN connectivity.
- **S6a**:- It enables transfer of subscription and authentication data for authenticating/authorizing user access to the evolved system (AAA interface) between MME and HSS.
- **Gx**:- It provides transfer of (QoS) policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PDN GW.
    - **Gxa:-** Allows PCRF to subscribe to appropriate event triggers in the Bearer Binding and Event Reporting Function (BBERF) located in a trusted non-3GPP access gateway, as defined in 29.212
    - **Gxc**:- Allows PCRF to subscribe to appropriate event triggers in the Bearer Binding and Event Reporting Function (BBERF) located in the S-GW, as defined in 29.212.
- **S8**:- Inter-PLMN reference point providing user and control plane between the Serving GW in the VPLMN and the PDN GW in the HPLMN. S8 is the inter PLMN variant of S5.
- **S9**:- It provides transfer of (QoS) policy and charging control information between the Home PCRF and the Visited PCRF in order to support local breakout function.
- **S10**:- Reference point between MMEs for MME relocation and MME to MME information transfer.
- **S11**:- Reference point between MME and Serving GW.
- **S12**:- Reference point between UTRAN and Serving GW for user plane tunnelling when Direct Tunnel is established. It is based on the Iu-u/Gn-u reference point using the GTP-U protocol as defined between SGSN and UTRAN or respectively between SGSN and GGSN. Usage of S12 is an operator configuration option.
- **S13**:- It enables UE identity check procedure between MME and EIR.
- **SGi**:- It is the reference point between the PDN GW and the packet data network. Packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provision of IMS services. This reference point corresponds to Gi for 3GPP accesses.
- **Rf/Gz** - PCEF to Offline Charging System (OFCS) Interface as specified in 3GPP TS 32.240.

- **Ro/Gy** - PCEF to Online Charging System (OCS) Interface as specified in 3GPP TS 32.240.
- **Rx**:- The Rx reference point resides between the AF and the PCRF in the TS 23.203 [6].
- **SBc**:- Reference point between CBC and MME for warning message delivery and control functions.

Protocol assumption:
- The S1-U is based on GTP-U protocol;
- The S3 is based on GTP protocol;
- The S4 is based on GTP protocol;
- The S5 is based on GTP protocol. PMIP variant of S5 is described in TS 23.402 [2];
- The S8 is based on GTP protocol. PMIP variant of S8 is described in TS 23.402 [2].
- S3, S4, S5, S8, S10 and S11 interfaces are designed to manage EPS bearers

LTE Network elements

E-UTRAN

E-UTRAN is described in more detail in TS 36.300 [5].

In addition to the E-UTRAN functions described in TS 36.300 [5], E-UTRAN functions include:
- Header compression and user plane ciphering;
- MME selection when no routing to an MME can be determined from the information provided by the UE;
- UL bearer level rate enforcement based on UE-AMBR and MBR via means of uplink scheduling(e.g. by limiting the amount of UL resources granted per UE over time);
- DL bearer level rate enforcement based on UE-AMBR;
- UL and DL bearer level admission control;
- Transport level packet marking in the uplink, e.g. setting the DiffServ Code Point, based on the QCI of the associated EPS bearer.

MME

MME functions include:
- NAS signaling;
- NAS signaling security;
- Inter CN node signaling for mobility between 3GPP access networks (terminating S3);
- UE Reachability in ECM-IDLE state (including control and execution of paging retransmission); - Tracking Area list management;
- PDN GW and Serving GW selection;
- MME selection for handovers with MME change;
- SGSN selection for handovers to 2G or 3G 3GPP access networks;
- Roaming (S6a towards home HSS);
- Authentication;
- Bearer management functions including dedicated bearer establishment.

- Lawful Interception of signaling traffic.
- Warning message transfer function (including selection of appropriate eNB).
- UE Reachability procedures.

NOTE: The Serving GW and the MME may be implemented in one physical node or separated physical nodes.

Gateway General

Two logical Gateways exist:
- Serving GW (S-GW);
- PDN GW (P-GW).

NOTE: The PDN GW and the Serving GW may be implemented in one physical node or separated physical nodes.

Serving GW

The Serving GW is the gateway which terminates the interface towards E-UTRAN.
For each UE associated with the EPS, at a given point of time, there is a single Serving GW.
The functions of the Serving GW, for both the GTP-based and the PMIP-based S5/S8, include:
- the local Mobility Anchor point for inter-eNodeB handover;
- sending of one or more “end marker” to the source eNodeB, source SGSN or source RNC immediately after switching the path during inter-eNodeB and inter-RAT handover, especially to assist the reordering function in eNodeB.
- Mobility anchoring for inter-3GPP mobility (terminating S4 and relaying the traffic between 2G/3G system and PDN GW);
- ECM-IDLE mode downlink packet buffering and initiation of network triggered service request procedure;
- Lawful Interception;
- Packet routing and forwarding;
- Transport level packet marking in the uplink and the downlink, e.g. setting the DiffServ Code Point, based on the QCI of the associated EPS bearer;
- Accounting on user and QCI granularity for inter-operator charging;
- UL and DL charging per UE, PDN, and QCI(e.g. for roaming with home routed traffic).
- Interfacing OFCS according to charging principles and through reference points specified in TS 32.240 [51].

Additional Serving GW functions for the PMIP-based S5/S8 are captured in TS 23.402 [2].
Connectivity to a GGSN is not supported.

PDN GW

The PDN GW is the gateway which terminates the SGi interface towards the PDN.
If a UE is accessing multiple PDNs, there may be more than one PDN GW for that UE, however a mix of S5/S8 connectivity and Gn/Gp connectivity is not supported for that UE simultaneously.
PDN GW functions include for both the GTP-based and the PMIP-based S5/S8:

- Per-user based packet filtering (by e.g. deep packet inspection);
- Lawful Interception;
- UE IP address allocation;
- Transport level packet marking in the uplink and downlink, e.g. setting the DiffServ Code Point, based on the QCI of the associated EPS bearer;
- UL and DL service level charging as defined in TS 23.203 6;
- Interfacing OFCS through according to charging principles and through reference points specified in TS 32.240 [51].
- UL and DL service level gating control as defined in TS 23.203 [6];
- UL and DL service level rate enforcement as defined in TS 23.203 6;
- UL and DL rate enforcement based on APN-AMBR(e.g. by rate policing/shaping per aggregate of traffic of all SDFs of the same APN that are associated with Non-GBR QCIs);
- DL rate enforcement based on the accumulated MBRs of the aggregate of SDFs with the same GBR QCI(e.g. by rate policing/shaping);
- DHCPv4 (server and client) and DHCPv6 (client and server) functions;
- The network does not support PPP bearer type in this version of the specification. Pre-Release 8 PPP functionality of a GGSN may be implemented in the PDN GW;
- packet screening.

Additionally the PDN GW includes the following functions for the GTP-based S5/S8:
- UL and DL bearer binding as defined in TS 23.203 [6];
- UL bearer binding verification as defined in TS 23.203 [6];
- Functionality as defined in RFC 4861 [32].

The P-GW provides PDN connectivity to both GERAN/UTRAN only UEs and E-UTRAN capable UEs using any of E-UTRAN, GERAN or UTRAN. The P-GW provides PDN connectivity to E-UTRAN capable UEs using E-UTRAN only over the S5/S8 interface.

SGSN

In addition to the functions described in TS 23.060 [7], SGSN functions include:
- Inter EPC node signaling for mobility between 2G/3G and E-UTRAN 3GPP access networks;
- PDN and Serving GW selection: the selection of S-GW/P-GW by the SGSN is as specified for the MME;
- MME selection for handovers to E-UTRAN 3GPP access network.

GERAN

GERAN is described in more detail in TS 43.051 [15].

UTRAN

UTRAN is described in more detail in TS 25.401 [16].

PCRF

General

PCRF is the policy and charging control element. PCRF functions are described in more detail in

TS 23.203 [6].
In non-roaming scenario, there is only a single PCRF in the HPLMN associated with one UE's IP-CAN session. The PCRF terminates the Rx interface and the Gx interface.
In a roaming scenario with local breakout of traffic there may be two PCRFs associated with one UE's IP-CAN session:
- H-PCRF that resides within the H-PLMN;
- V-PCRF that resides within the V-PLMN.

Home PCRF (H-PCRF)

The functions of the H-PCRF include:
- terminates the Rx reference point for home network services;
- terminates the S9 reference point for roaming with local breakout;
- associates the sessions established over the multiple reference points (S9, Rx), for the same UE's IP-CAN session (PCC session binding).

The functionality of H-PCRF is described in TS 23.203 [6].

Visited PCRF (V-PCRF)

The functions of the V-PCRF include:
- terminates the Gx and S9 reference points for roaming with local breakout;
- terminates Rx for roaming with local breakout and visited operator's Application Function.

The functionality of V-PCRF is described in TS 23.203 [6].

PDN GW's associated AAA Server

The PDN Gateway may interact with a AAA server over the SGi interface. This AAA Server may maintain information associated with UE access to the EPC and provide authorization and other network services. This AAA Server could be a RADIUS or Diameter Server in an external PDN network, as defined in TS 29.061 [38]. This AAA Server is logically separate from the HSS and the 3GPP AAA Server.

PSTN - is composed of all transmission and switching facilities and signal processors supplied and operated by all telecommunications common carriers for use by the public. Every station on the PSTN is capable of being accessed from every other station on the PSTN via the use of NANP E.164 numbers.

UE - user equipment (UE) a.k.a cell phone, subscriber unit, air card is any device used directly by an end-user to communicate to the LTE network. The UE connects to the eNb via the UU.

USIM - Universal Subscriber Identity Module is the logical entity on a UICC smart card running on a 3G mobile phone. It can store subscriber, authentication, phone contact and SMS information

UICC - Universal Integrated Circuit Card is the smart card used in the UE on a LTE network

13.3.12 Appendix 2 – Commercial and non-3GPP roaming

As stated within 3GPP TS 23.401 and TS 23.402, the EPS supports the use of both 3GPP based and non-3GPP IP access networks to access the EPC. The EPS enables the concept of trusted and non-trusted non-3GPP networks. Interworking between WiMAX IEEE 802.16e and CDMA 2000 EVDO networks are considered trusted non-3GPP networks and these will be the likely targets for roaming. An example of a non-trusted network would be a 802.11 Wi-Fi network.

- The EPS supports IETF-based network-based mobility management mechanism (e.g., PMIP) and host-based mobility management mechanism (e.g., MIP) over S2 reference points.
- The EPS supports IETF-based network-based mobility management mechanism (e.g., PMIP) over S5, and S8 reference points.

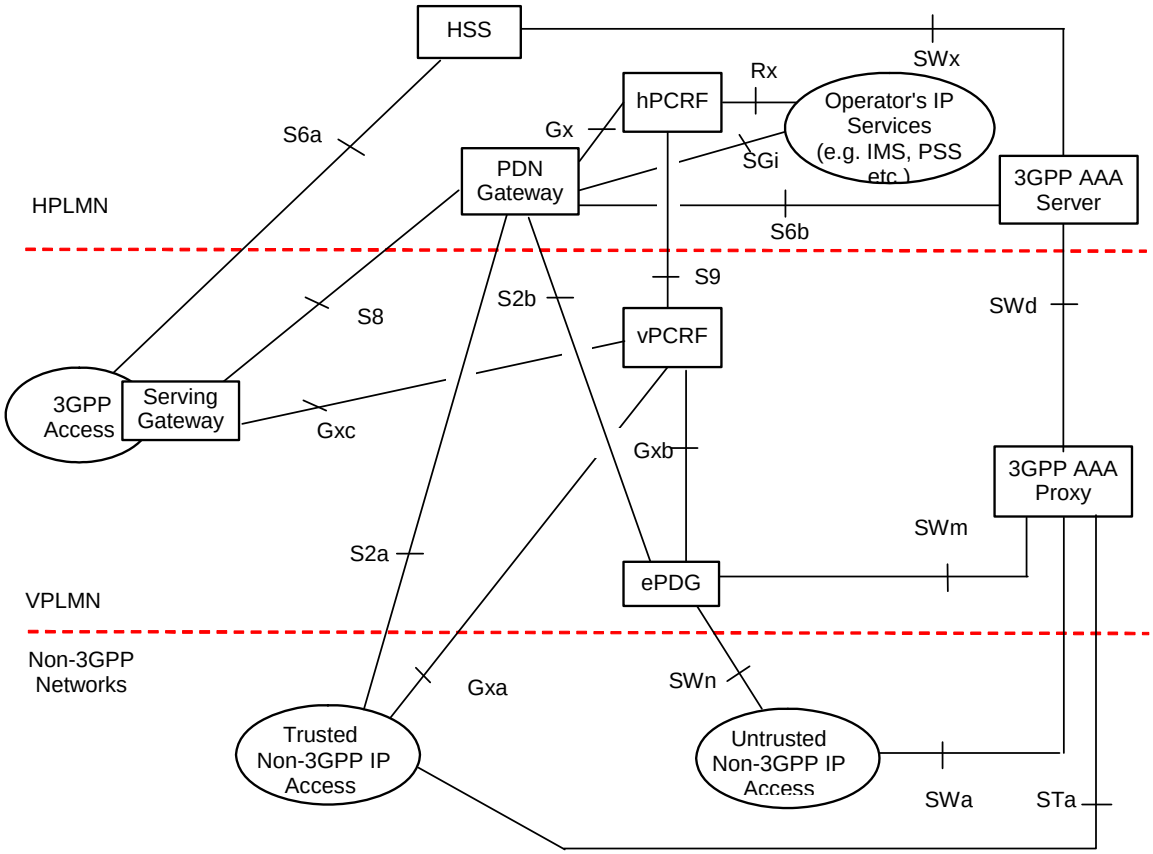
Several new interfaces can be utilized as roaming interfaces and within 3GPP there are several supported variations.

UTRAN – EPS Networks

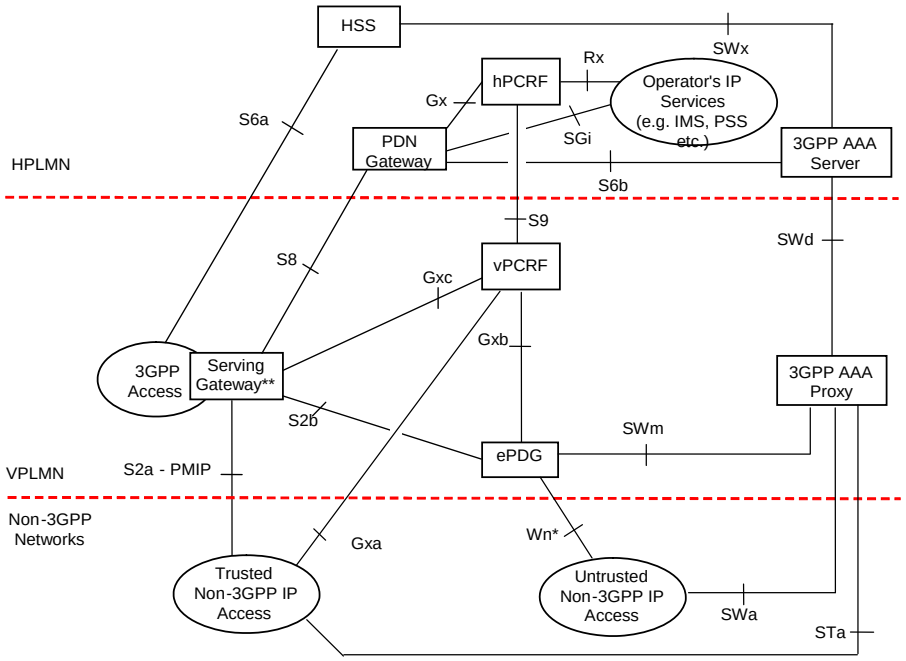
- S12 – UTRAN to SGW
- S4 – SGSN to SGW
- S3 – SGSN to MME
- SWx and SWz – HSS and AAA

Trusted Non-3GPP – EPS Networks (Interfaces from the non-3GPP IP Access Network to EPS nodes)

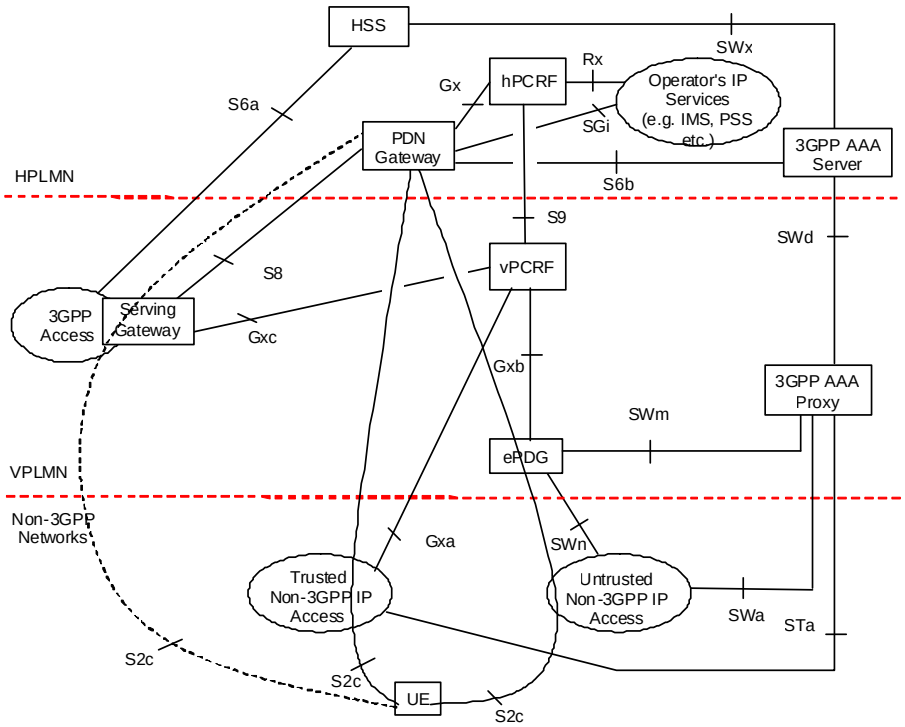
- S2a – PGW
- Gxa – vPCRF
- STa – AAA
- S2aPMIP – SGW
- S2c – UE to PGW
- S101 – MME to HRPD
- S103 – SGW to HSGW



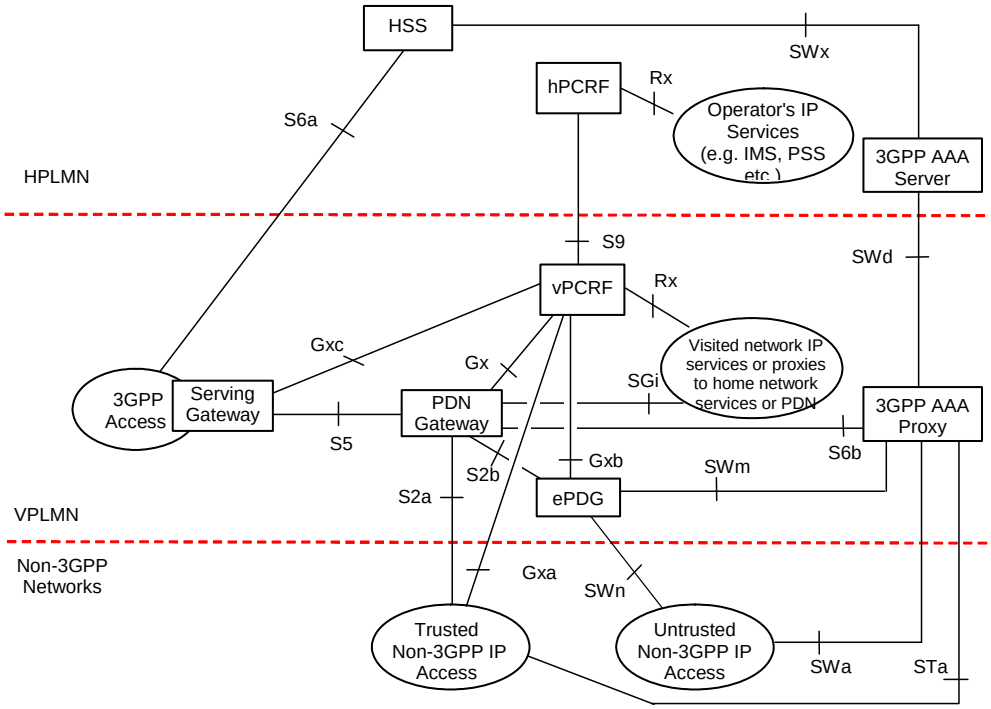
Roaming Architecture for EPS using S8, S2a– S2b - Home Routed



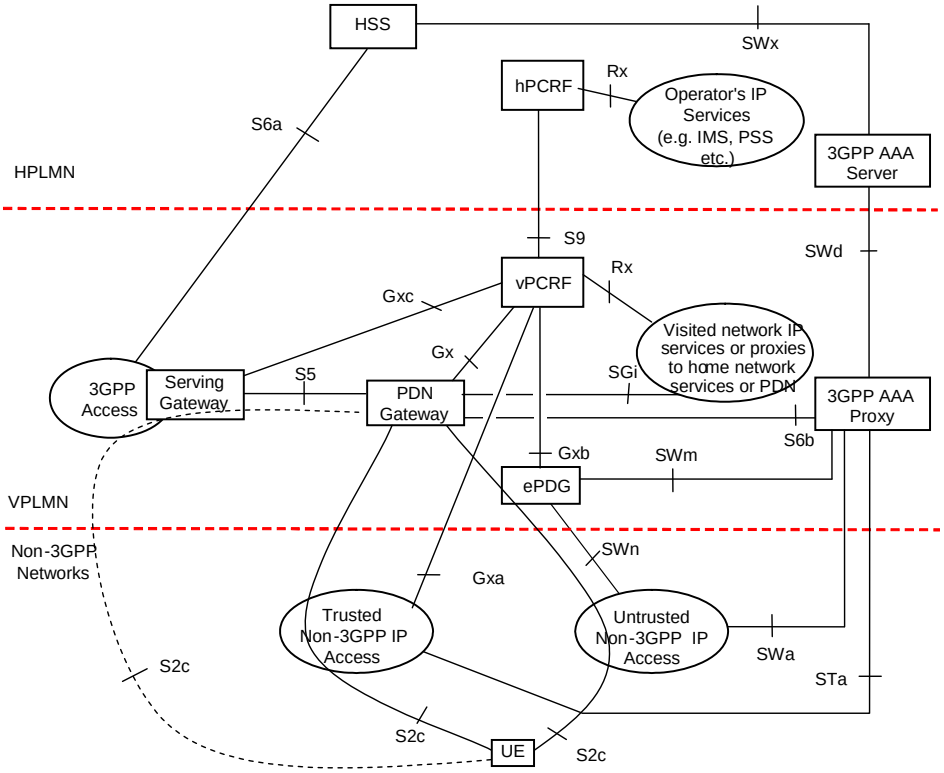
Roaming Architecture for EPS using PMIP-based S8, S2a, S2b (Chained PMIP-based S8-S2a/b) - Home Routed



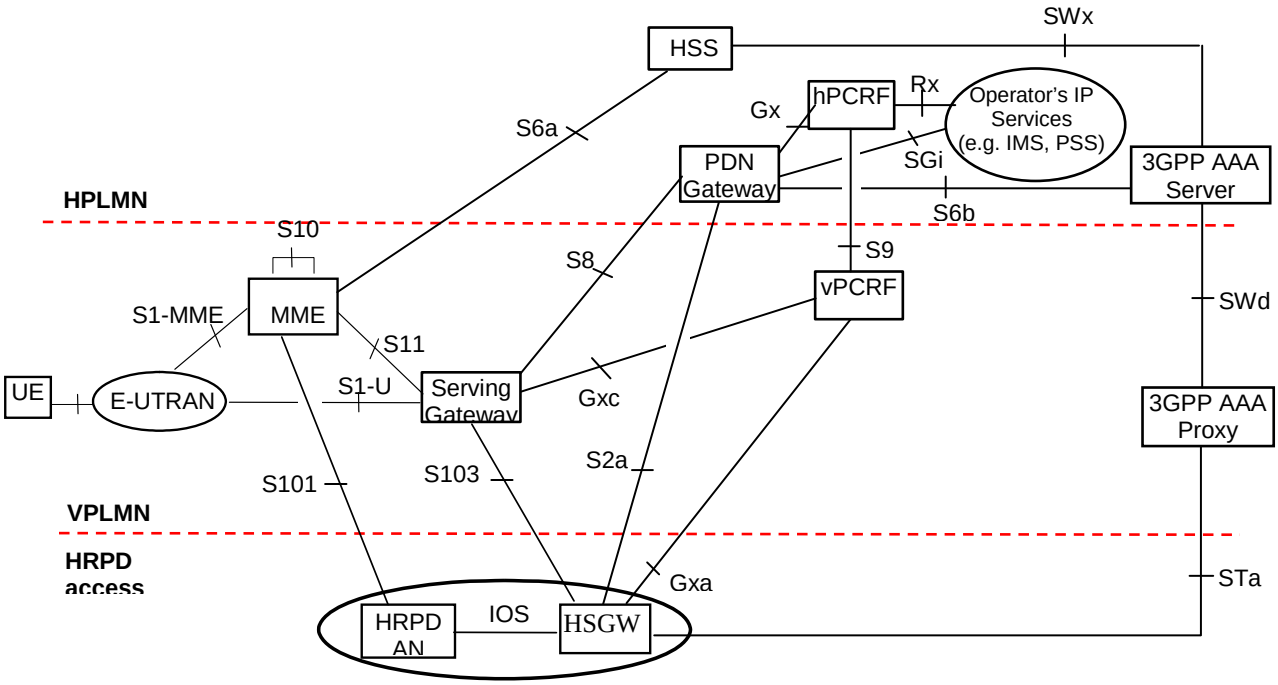
Roaming Architecture for EPS using S8 – S2c - Home Routed



Roaming Architecture for EPS using S5, S2a, S2b – Local Breakout



Roaming Architecture for EPS using S5, S2c – Local Breakout



Architecture for optimised handovers between E-UTRAN access and cdma2000 HRPD access (roaming case; Home routed)

13.3.13 Appendix 3 – PLMN ID Info

PLMN ID Information and diagrams

PLMN IDs are used in several ways in 3GPP networks:

1. The first digits in the IMSI are the PLMN ID. This assures that IMSIs assigned by different network operators are unique.
2. The PLMN ID in the IMSI is used to identify the Home Subscriber Server (HSS) containing the user's service subscription information. In case of roaming, this allows the visited network to query the HSS in the correct home network.
3. The PLMN ID is part of the Cell ID that is broadcast by each LTE cell. This allows the mobile device to first attempt to camp on a cell from the home network and camp on a visited network cell only if no home network cell is detected. The device is programmed with a list of the PLMN ID of networks with which the home network operator has roaming agreements.
4. The PLMN ID in the IMSI is used by the MME to determine whether a visiting user is allowed to connect as a roaming user. It can also be used to identify visiting users and override the requested QOS and insure that home users receive higher priority and QOS treatment
5. PLMN ID may be used to identify the home network of visiting users for the purpose of aggregating roaming usage for accounting purposes.
6.

APN Attach Info

One very workable solution within LTE and specified in 3GPP 23.401-860 is the use of an attach (address assignment) to the default PDN, that is associated with a fully qualified domain name as the identifier. This could potentially be used as an alternative for LTE-to-LTE network roaming cases even if the PLMN identifier is the same. This would utilize existing methodologies within the Access Point Name (APN), the Fully Qualified Domain Name (FQDN) stored in the USIM, and the Packet Data Network Gateway (PDN-GW). Once a UE (subscriber device) in LTE attaches to any network it tries to attach to its default APN. The APN is identified by its FQDN and will result in the selection of a specific PDN GW for the default bearer.

An example would be that all networks use MCC 310 and a MNC is assigned (xxx) to the PSBL to identify public safety networks. Each network would then have their own APN, so New York City users might get an APN of nyc.ny.emergency-networks.net and the users in San Francisco would be designated sfo.ca.emergency-networks.net. To support category 1 roaming, when a New York user powers on their device in San Francisco, the PLMN will be accepted (Public Safety User) and when setting up the default bearer the network in San Francisco would know

to take it back to New York and vice-versa. This is one potential solution that circumvents the limitation of MNC numbering and allows for proper billing/roaming charges.

SLF Info

Another solution would be to use the Home Network Identifier (HNI), which is a combination of the MCC and MNC, to identify the PLMN. Each network would be assigned a HNI by the IMSI Oversight Committee (IOC,), a committee of the Alliance for Telecommunication Industry Solutions (ATIS). Unique HNIs are required to distinguish between eNodebs from home and visited networks. The PLMN part of the IMSI (which is stored in the UICC card of the device) is used to determine the proper HSS to query for subscriber information.

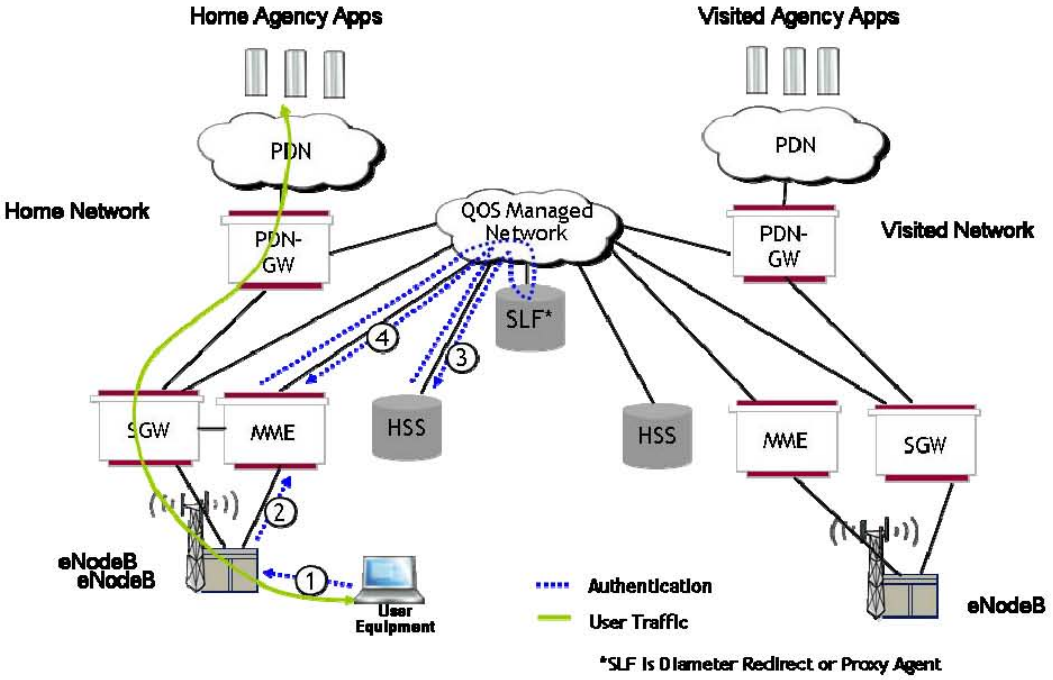
When a user roams into another network, the device is programmed to first try to select Home PLMN. If the HPLMN is not available, then the device is given a list of Visitor PLMNs that can be used with for roaming. A common or central HSS would be a logical solution but it may not be very practical with multiple, geographically separate systems. This means that in order for the networks of different public safety agencies to have separate HSSs, they must also have different HNIs. However, a common HSS is not necessarily needed even if each LTE network has the same MCC/MNC. Another possibility is where there is a SLF (Subscriber Location Function) that points to the correct HSS. This SLF could be owned by the PSST and it does not need to contain the entire user information but only the pointer to the HSS. This would work well as there is also a need for a DNS server to translate the domain name to a particular IP address. Instead of having one DNS server per market with duplicate databases there can be a few geographically distributed but logically centralized networks.

Dual USIM

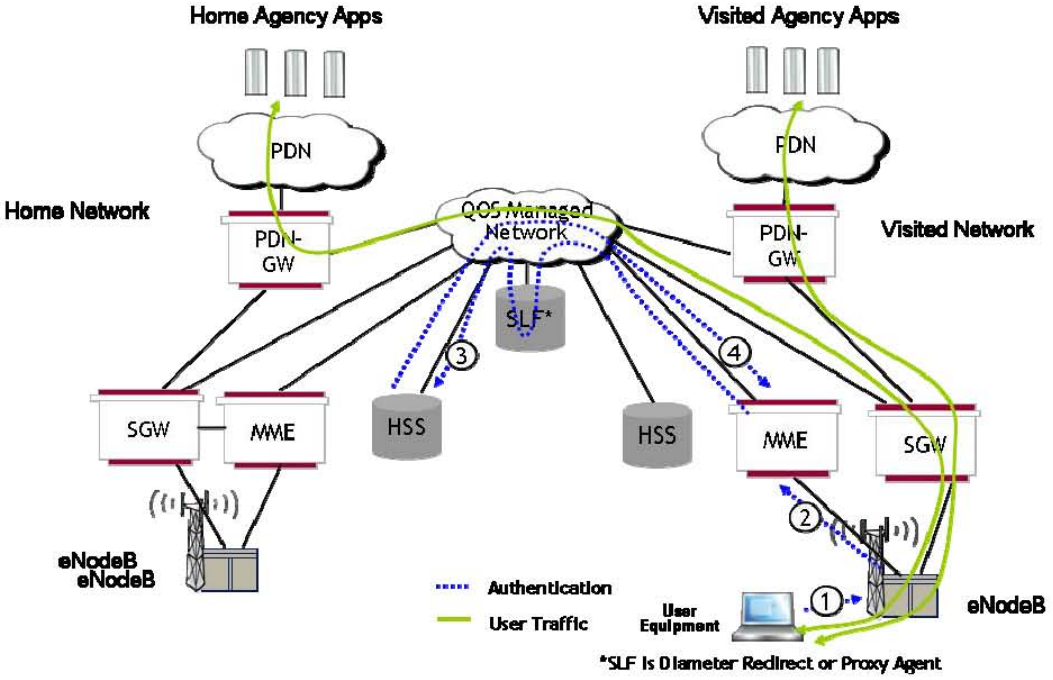
Another alternative in the short/medium term solution for public safety networks operating under waivers is dual-uSIM support in UEs, together with multi-mode, multi-band support for roaming to commercial 3GPP networks (release 8 and earlier releases). This may make reduce the network integration for public safety networks working under waivers.

This would allow use of the device on commercial 3GPP networks without requiring a roaming agreement or interconnection between the public safety LTE and commercial networks.

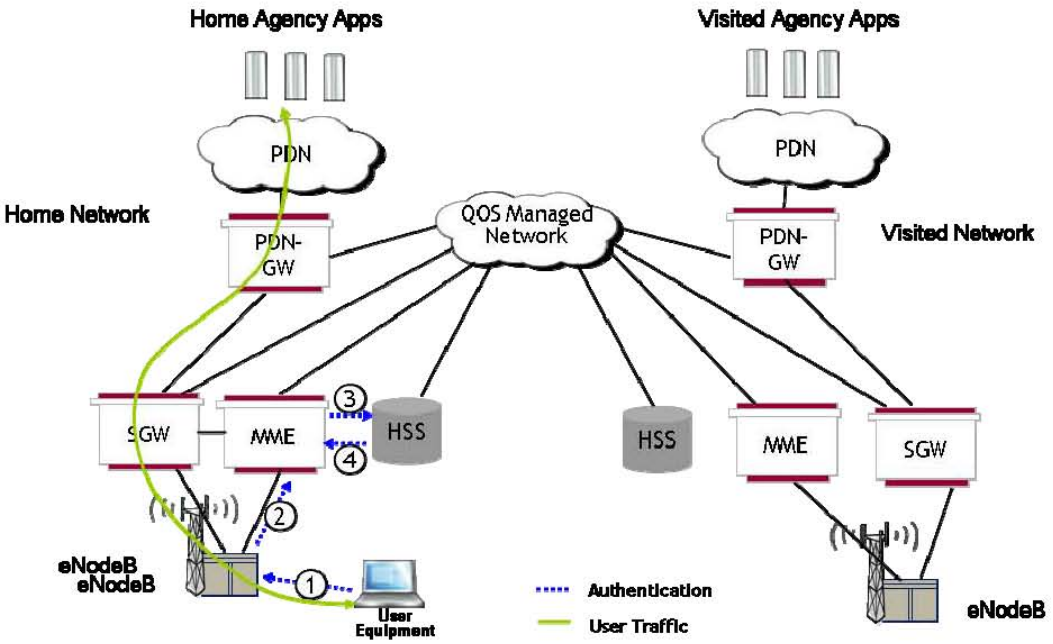
Network Interconnection with one PLMN id
Home Network



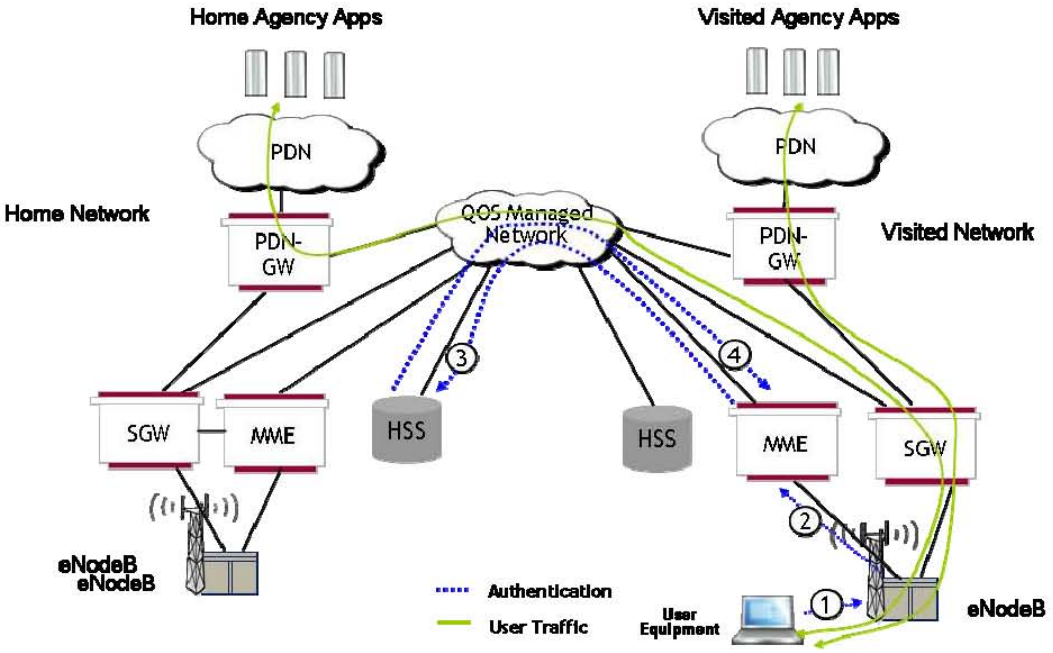
Network Interconnection with one PLMN id
Visited Network



Network Interconnection with separate PLMN id for each network
Home Network



Network Interconnection with separate PLMN id for each network
Visited Network



13.3.14 Appendix 4 – 3GPP Standards

3GPP Release 8 Specifications (March 2009)

3GPP TS 23.401: *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*

3GPP TS 29.274: *3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3*

3GPP TS 29.275: *Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols*

3GPP Standards Required for LTE (E-UTRA) Physical Layer Interoperability

3GPP TS 36.211 Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation

3GPP TS 36.212 Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding

3GPP TS 36.213 Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures

3GPP TS 36.214 Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer – Measurements

3GPP TS 36.104 Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception

3GPP TS 36.101 Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception

3GPP Standards Required for LTE (E-UTRA) Data Link Layer Interoperability

3GPP TS 36.321 Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification

3GPP TS 36.322 Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification

3GPP Standards Required for LTE (E-UTRA) Network Layer (Access Stratum) Interoperability

3GPP TS 36.323 Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification

3GPP TS 36.331 Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification

3GPP TS 36.304 Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode

3GPP TS 25.304 User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode

3GPP Standards Required for LTE (E-UTRA) Network Layer (Non-Access Stratum) Interoperability

3GPP TS 24.301 Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3

3GPP TS 24.122 Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode

3GPP Standards Required for EPC S6a Interface Interoperability

3GPP TS 29.272: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (Release 8)

14 Appendix G: Governance WG Working Documents

NPSTC Broadband Task Force
Governance Group

Recommendations

2 September 2009 - V4

The Governance Workgroup of the NPSTC Broadband Task Force (BBTF) makes these overall recommendations to NPSTC, the Public Safety Broadband Licensee (PSBL), and the Federal Communications Commission (FCC):

1. NPSTC and/or the PSST should petition the Federal Communications Commission to allow individual city or county governments, or groups of governments, to construct regional networks using the 700 MHz spectrum assigned to public safety. The FCC should grant

waivers to qualified regional requestors who agree to build subject to the terms and conditions specified in the NPSTC report.

2. The FCC should allow the PSBL to lease PSBL spectrum to regional system constructors and operators authorized by waiver or under changed rules. The terms of the lease are contained in the lease agreement term sheet . The regional network operator will have all rights to use the spectrum and operate the regional network as if they were the licensee, except as provided in the lease agreement term sheet.

3. Congress and the FCC should re-allocate the D block to public safety, thereby giving the PSBL and regional network waiver holders 20 MHz of spectrum for operation of public safety wireless broadband networks. With this allocation of the D Block to Public Safety, the total spectrum should be governed by the same governance structure as the current public safety spectrum managed by the PSBL.

4. Congress and the FCC should explicitly allow regional builders, subject to the term agreement, to use public-private partnerships for construction and operation of their networks.

5. The PSBL and regional network operators who build without a private telecommunications partner should use interconnection services for intersystem and intrasystem "roaming" rather than negotiating individual agreements or memoranda of understanding with other regional system operators. (Also is a technical recommendation)

6. Congress and the FCC should explicitly allow use of the national interoperable broadband wireless network in spectrum allocated to public safety by not only first responders, but also by emergency response support agencies (such as utilities, transportation, certain Federal government agencies, and general government). Such emergency response support agencies are critical to the safety of the public during daily incidents and emergencies, but especially during local, regional and national disasters. Prioritization of network use between all such users would be controlled by the regional network operator. (This recommendation should also be formulated into the definitions section to define public safety and the support agencies)

7. The PSBL should convene a group of regional entities who are authorized to construct regional networks using the 700 MHz spectrum. This group of entities would:

a. continue the work of the Broadband Task Force (BBTF), as directed by the appropriate authority to extend and codify the operations, governance and technical requirements for the network;

b. advise the PSBL, FCC or other appropriate authority;

c. work with the PSBL on other standards and agreements which improve the operability and interoperability of the national public safety broadband wireless network.

d. Note: Participation in this group would be a requirement of the regional builders or holders of term agreements. Regional builders must insure they have the commitment and financial ability to participate.