Defence Research and Development Canada | Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Public Safety Broadband Network Architecture Description

Prepared By:
Jack Pagotto, DRDC Centre for Security Science
Gino Scribano, Motorola Solutions Inc.
Richard Cayouette, Martello Defense Security Consultants Inc.
Dr. Stephen Braham, Ph.D, Simon Fraser University
Jacob Gurnick, Communications Research Centre Canada, Government of Canada
Charles Auger, Communications Research Centre Canada, Government of Canada
Eric Lafond, Communications Research Centre Canada, Government of Canada
Joe Fournier, Communications Research Centre Canada, Government of Canada
Tewfik Doumi, Alcatel-Lucent
Claudio Lucente, Fiorel Systems
Mike Dixon, Web4Wirleless

Edited by: Luc Samson, Briskwave Consulting.

Defence R&D Canada –Centre for Security Science

Technical Report
DRDC CSS TR 2013-009
August 2013

Canada

Public Safety Broadband Network Architecture Description

Prepared By:
Jack Pagotto, DRDC Centre for Security Science
Gino Scribano, Motorola Solutions Inc.
Richard Cayouette, Martello Defense Security Consultants Inc.
Dr. Stephen Braham, Ph.D, Simon Fraser University
Jacob Gurnick, Communications Research Centre Canada, Government of Canada
Charles Auger, Communications Research Centre Canada, Government of Canada
Eric Lafond, Communications Research Centre Canada, Government of Canada
Joe Fournier, Communications Research Centre Canada, Government of Canada
Tewfik Doumi, Alcatel-Lucent
Claudio Lucente, Fiorel Systems
Mike Dixon, Web4Wirleless

Edited by: Luc Samson, Briskwave Consulting.

Defence R&D Canada –Centre for Security Science
Technical Report
DRDC CSS TR 2013-009
August 2013

Principal Author

Jack Pagotto

Section Head, Multi-Agency Crisis Management S&T
DRDC Centre for Security Science

Approved by

Dr. Andrew Vallerand

Director Public Safety and Security S&T
DRDC Centre for Security Science

Approved for release by

Dr. Mark Williamson

Document Review Panel Chair
DRDC Centre for Security Science

Abstract

WHAT PUBLIC SAFETY NEEDS IN AN EMERGENCY IS…
A public safety-controlled network with the ability to efficiently access and share accurate and timely voice and information during all stages of an event in any geographic location with the appropriate resources, interoperability, robust and reliable capacity, based upon the needs of the responders, and with the ability to dynamically scale to changes in the situation. [1]

This document describes the network architecture for a Canadian public safety broadband communications network expected to operate in the 700 MHz band. It aligns with the governance model as currently endorsed by the senior officials responsible for emergency management in Canada (SOREM), which contains two layers of operational responsibility – a national entity and multiple regional service delivery entities (RSDE). The network architecture is also aligned with the service delivery model whereby the users of the public safety broadband network (PSBN) are clients of the RSDE, while also being owners of the information networks.

The PSBN interfaces with several external networks. The network architecture describes, at a high level, how the PSBN could interface with selected external networks. Furthermore, it is expected that Canada's public safety community will rely on deployable systems to deliver broadband services to isolated areas of the country where no broadband communications infrastructure exists and to areas where the infrastructure has been damaged. There is a section dedicated to the topic of deployable communications.

[1] U.S. Department of Justice - Community Oriented Policing Services (COPS), "National Forum on Public Safety Broadband Needs" August 23, 2010. http://www.cops.usdoj.gov/files/RIC/Publications/e021111338-broadband-forum.pdf

Résume

EN SITUATION D'URGENCE, SÉCURITÉ PUBLIQUE A BESOIN …

d'un réseau contrôlé par la sécurité publique, permettant d'accéder efficacement à de l'information, y compris des données vocales, de partager celles-ci exactement et opportunément durant toutes les étapes d'un événement, peu importe l'emplacement géographique, de disposer d'une capacité robuste et fiable, de l'interopérabilité et des ressources appropriées, selon les besoins des intervenants, et de s'adapter de manière dynamique aux changements de situation.[2]

Le présent document décrit l'architecture d'un réseau de communication canadien à large bande pour la sécurité publique qui devrait être exploité sur la bande de 700 mégahertz. Cette architecture cadre avec le modèle de gouvernance prôné par les cadres supérieurs responsables de la gestion des urgences au Canada (CSRGU) et correspond aux deux ordres de responsabilité opérationnelle – une entité nationale et plusieurs entités régionales de prestation de services (ERPS). L'architecture de réseau cadre aussi avec le modèle de prestation de services où les utilisateurs du réseau à large bande de sécurité publique (RLBSP) sont à la fois clients des ERPS et propriétaires des réseaux d'information.

Le RLBSP est lié à plusieurs réseaux externes. L'architecture du réseau décrit, à un niveau élevé, comment le RLBSP pourrait interagir avec des réseaux extérieurs sélectionnés. En outre, il est prévu que la communauté de la sécurité publique du Canada s'appuiera sur les systèmes déployables pour fournir des services à large bande dans les régions isolées du pays où aucune infrastructure de communication à haut débit existe et dans des régions où les infrastructures ont été endommagées. Une section entière a été consacrée au sujet des communications déployables.

Note : Seulement l'avant –propos et le sommaire exécutif furent traduits

[2] U.S. Department of Justice - Community Oriented Policing Services (COPS), "National Forum on Public Safety Broadband Needs" August 23, 2010. http://www.cops.usdoj.gov/files/RIC/Publications/e021111338-broadband-forum.pdf

Executive summary

Public Safety Broadband Network Architecture Description

Jack Pagotto, Gino Scribano, Richard Cayouette, Dr. Stephen Braham, Jacob Gurnick, Charles Auger, Eric Lafond, Joe Fournier, Tewfik Doumi, Claudio Lucente, Mike Dixon; DRDC CSS TR 2013-009; Defence R&D Canada –Centre for Security Science August 2013

The development of the network architecture for the 700 MHz PSBN was undertaken to illustrate the technical underpinning of the governance model as endorsed by Canada's public safety community. The network architecture is based on Long Term Evolution (LTE) and is supplemented by various other technologies that, in its ensemble, forms the PSBN. Governance, the service delivery model, and technology are important factors that were considered in the preparation of the network architecture for the PSBN.

The concept of governance for the PSBN is based on a federation of regional sub-networks that, together, comprise the nationwide PSBN. It is a 2-tiered structure for governance consisting of a national operator, i.e. primary licensee and operator of the PSBN, and regional service delivery entities (RSDE), i.e. subordinate licensees and regional operators of the PSBN. This approach allows each region to implement its portion of the PSBN with its selected vendors/partners and to implement it according to its budgets and timelines. However, it is expected that each regional sub-network will comply with a set of requirements in order to achieve nationwide interoperability such that end-users from any region in Canada can be served over the PSBN regardless of which region they are in. A national network layer serves as the host for nationwide applications and interconnects the regional sub-networks. The national network layer should be implemented prior to, or at the same time as the first regional sub-network

The service delivery model (SDM) is based on the premise that users are subscribers of the regional operators of the PSBN. The PSBN is used to link users with their information networks and ensures they can access their information from any regional sub-network in Canada. Facilitated by roaming agreements, users would also be able to access their information when they are on partner networks.

The SDM lays out the roles of the principal actors in bringing broadband services to end-users. The network architecture assumes an SDM whereby the end-users are subscribers to a wireless service offered by the RSDE. The RSDE also serves as the gateway to connect the end-users' information networks (including applications). The information networks are assumed to be owned and managed by the various agencies to which the end-users pertain. As such, it would be within the purview of the end-user agencies to grant appropriate access to their information networks as required during day-to-day operations and for the specific interoperability needs during incidents. The end-user agencies would control the profiles of the end-users within their jurisdictional authority.

Federal Departments and Agencies such as RCMP, Canada Border Services Agency, Canada Coast Guard, etc, in the exercise of their federal/national mandate, will use the Federal Access Network as their gateway to the PSBN. The Federal Access Network consists of the interface to federal information networks as well as the interface to external networks whose access is managed by federal agencies. Federal agencies under contract to P/Ts or municipalities, such as the RCMP, will be tied to the RSDE. Federal agencies not tied to specific regions may also need to support any region or multiple regions during times of emergency. It is expected that users from federal agencies will access their information networks through RSDEs.

The RSDEs would be responsible to provide radio coverage of the PSBN over the geographic area that forms their region. The RSDEs also interface with external networks such as the Internet and other access networks. This allows the end-users to communicate with publicly addressable users outside the PSBN anywhere in the world, and to access their information networks when they are outside the coverage footprint of the PSBN.

The National Entity would be responsible to interconnect the regional sub-networks into one nationwide network and for managing the roaming agreements with other wireless carriers, including FirstNet, the U.S. PSBN operator. The National Entity could host applications that are standardized for nationwide use. For example, messaging and Voice-over-LTE (VoLTE) applications could be hosted nationally.

Another important consideration for the network architecture is to deliver broadband services in isolated areas. Given the vastness of Canada's unpopulated areas it is not feasible to provide permanent radio coverage over the PSBN in these regions. Thus, when incidents occur in these regions the SDM assumes that first responders will carry in deployable communications infrastructure to establish broadband communications over the incident area. The network architecture is designed to connect remote deployments to the PSBN through satellite or other backhaul technologies. Where backhaul is not available, the incident response teams can deploy stand-alone broadband systems that can synchronize with the PSBN if/when backhaul is established. In a similar manner end-user agencies can augment existing PSBN coverage and/or capacity within an incident area by deploying their own 'cells-on-wheels' type systems. Particular attention to technical aspects and heightened coordination is required in the case of augmenting fixed PSBN installations with deployable systems so as to not cause interference.

A topic of current interest for commercial wireless carriers and within international standards development organizations is "traffic offloading". Offloading is intended to relieve the main radio access network of some of the traffic demands for high speed data by using other access technologies within the network or actual separate networks. For example, the 3GPP and Wireless Broadband Alliance are developing standards to use WiFi to offload traffic from LTE networks, with the ability to authenticate user credentials across both networks and to hand-off traffic from one to the other. The network architecture of the PSBN allows for the possibility that in-fill strategies will leverage low-cost technologies such as WiFi access points as either trusted or untrusted networks.

Mission critical voice services are expected to continue to be offered over narrowband land mobile networks (LMR) for the foreseeable future. The network architecture of the PSBN will be able to originate and terminate voice sessions between PSBN users and LMR users. In addition, the PSBN will be able to connect voice sessions over different LMR domains such as P25 and

TETRA. Standards for these use-cases have not yet been completed by their respective standards development organizations. The network architecture assumes that the LMR domains will include gateways that interface with the PSBN at the IP level and which will also serve as the border security terminating points. It is expected that the PSBN will not transcode the voice payload between all the different possible voice encoding protocols. However, this will be addressed again as the standards evolve.

The PSBN network architecture considers the possibility of sharing spectrum with commercial users, if permitted by Industry Canada and if it is agreed upon between the RSDEs and commercial operators. Priority and QoS mechanisms would be asserted according to policies that would be established between the partners.

The PSBN is expected to be available to serve first responders during disasters and must therefore be highly resilient. The NAD describes a number of approaches to increase the resiliency of the PSBN. The National Entity and RSDEs would need to determine the optimum balance between acceptable risk and cost of resiliency.

The primary interface for information networks and external networks to the PSBN is through packet data gateways (P-GW). The P-GWs use the profile information stored in the home subscriber server (HSS) for access control privileges, including priority. Although it is not covered in depth in the NAD, it is assumed that suitable security measures will be in place to protect the network and the information (user, control, and management) carried over it or stored on it.

The network architecture assumes that the National Entity will host value added services for common use by all subscribers. The most important one that was identified by the work group is a class of services for unified multimedia messaging, which includes voice services. Messaging and voice services are unique in that they require user-specific addresses to be resolved for both incoming and out-going traffic. Many commercial services are available as over-the-top applications such as Skype™ and other proprietary messaging applications such as BBM Messenger™. However, these services are accessible only to subscribed users. The NAD assumes that users will originate and terminate voice and messaging sessions with anyone within and outside the PSBN. As such, an IP Multimedia Subsystem (IMS) has been included as an enhanced service option on the basic architecture.

Sommaire

Public Safety Broadband Network Architecture Description

Jack Pagotto, Gino Scribano, Richard Cayouette, Dr. Stephen Braham, Jacob Gurnick, Charles Auger, Eric Lafond, Joe Fournier, Tewfik Doumi, Claudio Lucente, Mike Dixon; DRDC CSS TR 2013-009; Recherche et développement pour la défense Canada –Centre des sciences pour la sécurité Aout 2013

L'on a développé l'architecture de réseau pour le RLBSP de 700 MHz afin d'illustrer les fondements techniques du modèle de gouvernance prôné par les intervenants de la sécurité publique du Canada. L'architecture du réseau se fonde sur une technologie d'évolution à long terme (LTE), complétée par diverses autres technologies qui, conjuguées, formeront le RLBSP. La gouvernance, le modèle de prestation de services et la technologie sont autant de facteurs pris en compte dans la préparation de l'architecture de réseau du RLBSP.

Le concept de la gouvernance du RLBSP se fonde sur l'idée d'une fédération de sous-réseaux régionaux qui, ensemble, composent le RLBSP national. Il s'agit d'une structure de gouvernance à deux niveaux : un opérateur national, soit le principal titulaire de permis et exploitant du RLBSP, et plusieurs entités régionales de prestation de services, soit les titulaires secondaires et exploitants régionaux du RLBSP. Cette approche permet à chaque région de mettre en oeuvre sa partie du RLBSP en collaboration avec ses fournisseurs et partenaires, dans le respect de ses budgets et calendriers. Ceci dit, l'on s'attend à ce que chaque sous-réseau régional réponde à une série d'exigences en vue d'assurer l'interopérabilité nationale, pour que les utilisateurs de n'importe quelle région du Canada puissent être servis par le RLBSP. Le réseau national héberge les applications pancanadiennes et assure la communication entre les sous-réseaux régionaux. Ce réseau national devrait être mis en œuvre avant ou en même temps que le premier sous-réseau régional.

Le modèle de prestation de services se fonde sur le principe que les utilisateurs sont des abonnés des exploitants régionaux du RLBSP. Le RLBSP relie les utilisateurs à leur réseau d'information et leur assure l'accès à partir de n'importe quel sous-réseau régional au Canada. Grâce à des ententes d'itinérance, les utilisateurs pourront accéder à leur information à partir de réseaux partenaires.

Le modèle de prestation de services définit les rôles des principaux acteurs fournissant des services à large bande aux utilisateurs finaux. L'architecture de réseau suppose un modèle de prestation de services où les utilisateurs finaux sont abonnés à un service sans fil offert par l'ERPS. L'ERPS sert aussi de passerelle pour relier les réseaux d'information de l'utilisateur final (y compris les applications). Les réseaux d'information sont supposés être détenus et gérés par les différents organismes auxquels les utilisateurs finaux se rapportent. Ainsi, il serait de la compétence des agences de l'utilisateur final d'accorder un accès approprié à leurs réseaux d'information selon les besoins pendant les opérations quotidiennes et pour les besoins

spécifiques d'interopérabilité pendant les incidents. Les agences de l'utilisateur final contrôleraient les profils des utilisateurs finaux au sein de leur autorité juridictionnelle.

Les agences fédérales comme la GRC, l'Agence des services frontaliers du Canada, la Garde côtière canadienne, etc, dans l'exercice de leur mandat fédéral / national, vont utiliser le réseau d'accès fédéral comme passerelle à la RLBSP. Le réseau d'accès fédéral se compose de l'interface aux réseaux d'information fédéraux ainsi que l'interface avec les réseaux externes dont l'accès est géré par des organismes fédéraux. Les organismes fédéraux ayant des accords avec des provinces, territoires ou municipalités, comme la GRC, seront liés aux ERPS. Les organismes fédéraux qui ne sont pas liés à des régions spécifiques peuvent également avoir besoin d'appuyer n'importe quelle région ou de plusieurs régions en situation d'urgence. On s'attend à ce que les utilisateurs des organismes fédéraux auront accès à leurs réseaux d'information à travers les ERPS.

Les ERPS seraient chargées de fournir une couverture radio du RLBSP sur la zone géographique qui constitue leur région. Les ERPS seront également en liaison avec les réseaux externes, tels que l'Internet et autres réseaux d'accès. Cela permet aux utilisateurs finaux de communiquer avec les utilisateurs adressables publiquement en dehors du RLBSP partout dans le monde, et d'accéder à leurs réseaux d'information quand ils sont en dehors de la zone de couverture du RLBSP.

L’entité nationale interconnecterait les divers sous-réseaux régionaux pour créer un grand réseau pancanadien et gérerait les ententes d’itinérance conclues avec d’autres fournisseurs de service sans fil, y compris FirstNet. L’entité nationale hébergerait aussi les applications normalisées pancanadiennes, comme les celles de messagerie et de voix sur LTE (VoLTE).

Autre importante considération de l’architecture de réseau : la prestation de services à large bande en région éloignée. Étant donné l’étendue du territoire non peuplé du Canada, il est irréaliste de vouloir offrir une couverture RLBSP radio permanente dans ces régions. Aussi, le modèle de prestation de services prévoit que lorsque des incidents se produisent dans ces régions, les premiers intervenants apportent leur propre infrastructure de communications déployable afin d’assurer les communications à large bande dans la région touchée. L’architecture du réseau prévoit la connexion des déploiements ponctuels au RLBSP permanent grâce à un lien satellitaire ou autre technologie de raccordement. Lorsqu’une telle technologie n’est pas disponible, l’équipe d’intervention peut déployer un système indépendant à large bande qui pourra être synchronisé au RLBSP lorsqu’un raccordement devient accessible. De la même façon, les entités d’utilisateurs finaux peuvent augmenter leur couverture ou capacité de RLBSP existante en cas d’incident en déployant leur propre réseau cellulaire d’appoint. Il faudra toutefois faire particulièrement attention aux aspects techniques et de coordination afin d’éviter les interférences entre les installations de RLBSP permanentes et les systèmes déployables ponctuels.

Un enjeu d’actualité pour les fournisseurs de services sans fil commerciaux ainsi que pour les organisations internationales de normalisation est le délestage de trafic (« traffic offloading »). Le délestage consiste à détourner une partie des demandes d’accès au service de données haut débit du principal réseau radio vers d’autres technologies d’accès au sein du même réseau ou carrément

vers d'autres réseaux. Par exemple, le partenariat 3GPP et le Wireless Broadband Alliance sont en cours d'élaboration de normes pour détourner une partie du trafic des réseaux LTE vers un réseau WiFi, tout en conservant la possibilité d'authentifier les utilisateurs sur les deux réseaux et de transférer le trafic d'un réseau à l'autre. L'architecture de réseau du RLBSP prévoit la mise en œuvre de stratégies d'appoint afin d'exploiter des technologies à faible coût comme les points d'accès WiFi à titre de réseaux sécurisés ou non.

Les services critiques de radios mobiles terrestres (RMT) devraient continuer d'être offerts sur des réseaux mobiles terrestres à bande étroite pour l'avenir prévisible. L'architecture du réseau du RLBSP permettra l'ouverture et la cession de sessions voix entre les utilisateurs RMT et les utilisateurs du RLBSP. En outre, le RLBSP sera capable de connecter les sessions voix sur les différents domaines de RMT comme le P25 et le TETRA. Les normes pour ces cas d'usage n'ont pas encore été déterminées par leurs organismes d'élaboration de normes respectives. L'architecture de réseau suppose que les domaines RMT comprendront des passerelles qui interagiront avec le RLBSP en protocole internet et qui seront également les points de terminaison sécurisés. L'on ne s'attend pas à ce que le RLBSP convertisse tous les différents protocoles de données voix imaginables. Ceci dit, cette hypothèse pourra être révisée au fil de l'évolution des normes.

L'architecture de réseau du RLBSP considère la possibilité de partager du spectre avec les utilisateurs commerciaux, si cela est autorisé par Industrie Canada et, s'il est convenu entre les ERPS et les opérateurs commerciaux. Les mécanismes prioritaires et de qualité de service (QoS) seraient affirmés en fonction des politiques qui seraient établies entre les partenaires.

Le RLBSP, qui aura pour vocation d'être au service des premiers intervenants en cas de catastrophe, devra être extrêmement robuste. La description de l'architecture de réseau décrit plusieurs façons de renforcer la robustesse du RLBSP. L'entité nationale et les ERPS devront trouver un juste milieu entre le risque et le coût de résilience.

L'interface principale pour les réseaux d'information et les réseaux externes au RLBSP est à travers les passerelles de données par paquets (P-GW). Les P-GW utilisent les informations de profil stockées dans le serveur d'abonnés (HSS) pour les privilèges de contrôle d'accès, y compris la priorité. Même si ce n'est pas abordé en profondeur dans la description de l'architecture du réseau, il est supposé que des mesures de sécurité adéquates seront mises en place pour protéger le réseau et les informations (utilisateur, contrôle et gestion) circulant sur celui-ci ou qui y sont stockées.

L'architecture de réseau suppose que l'entité nationale hébergera les services à valeur ajoutée pour l'usage commun par tous les abonnés. Le plus important qui a été identifié par le groupe de travail est une classe de services pour la messagerie multimédia unifiée, qui comprend les services vocaux. Les services de messagerie et de voix sont particuliers étant donné qu'ils imposent la résolution des adresses spécifiques des utilisateurs afin de résoudre le trafic entrant et sortant. De nombreux services commerciaux sont disponibles en tant qu'applications sur poste de travail

telles que Skype™ et d'autres applications de messagerie propriétaires comme BBM Messenger™. Toutefois, ces services ne sont accessibles qu'aux utilisateurs abonnés à ces services. La description de l'architecture du réseau suppose que les utilisateurs amorceront et termineront les sessions de voix et de messagerie avec quelqu'un à l'intérieur et à l'extérieur du RLBSP. Ainsi, un sous-système multimédia IP (IMS) a été inclus comme une option de service complémentaire à l'architecture de base.

Note : Seulement l'avant –propos et le sommaire exécutif furent traduits.

Table of Contents

List of figures

List of tables

Acknowledgements

The network architecture was developed through a collaborative effort in consultation with industry, commercial carriers, first responders, Canadian and Provincial/Territorial government emergency management officials, academia, consultants, and other public safety stakeholders.

There is no single "right" network architecture to the exclusion of other designs and therefore it was not unexpected that participants held different views and opinions on the advantages and disadvantages of several options of network architecture that were considered. Although the work group did not achieve unanimous consensus for recommended network architecture, the discussions revealed that all options carry their own set of technical challenges. It is the Technical Advisory Group's (TAG)[3] position that the network architecture described in the NAD adequately reflects the governance model, service delivery model, and technical constraints.

The 700 MHz TAG acknowledges the invaluable contributions and dedication of the participants listed below in the many work sessions that resulted in this document. Any omissions are not intentional.

Simon Arcand, Communications Security Establishment Canada, Government of Canada
Andy McGregor, Ericsson
Mark Marriott, Cisco
Azhar Sayeed, Cisco
Andrew Robinson, Information Systems Architects
Brian Smith, Bell Canada
Rob Peaker, Alcatel-Lucent
Jean Lajoie, Centre des Services Partagés du Québec, Gouvernement du Québec
Gaetan Trepanier, Centre des Services Partagés du Québec, Gouvernement du Québec
Simon Perras, Communications Research Centre Canada, Government of Canada

[3] The TAG is composed of a collaborative group of vendor-neutral technical experts led by Centre for Security Science and includes scientific authorities from the Communications Research Center of Canada, Simon Fraser University, and technical experts from Federal/Provincial/Territorial/Municipal agencies

1. Operational Requirements Summary

The Operational Requirements (ORs) are statements describing what users expect of the PSBN and the way that the PSBN is intended to serve them. Operational requirements are linked to use-cases, which express how the users intend to make use of the PSBN and what information they intend to transmit or access through the PSBN. The OR document[4] serves as a reference for the Network Architecture Description (NAD).

1.1 Operational Conditions

The PSBN is intended to provide service to users over a broad range of conditions.

1.1.1 Geography

For the purpose of this document, a total of four geographic areas are identified, categorized primarily by their respective physical requirements. Geography definitions are presented in the 'Definitions' section of the document and summarized below.

- Urban: Urban areas are associated with population centres.
- Suburban: Typically existing as part of an urban area or as a separate community within commuting distance.
- Rural: Consisting of scattered small towns, villages or settlements typically located away from large population centres.
- Remote: Consisting of small settlements, mining camps and other industrial campuses which may be located several hundreds of kilometers away from any population centre.

1.1.2 Environment

- Benign: Office setting, especially for back-office users.
- Moderate: Portable, outdoor, vehicular, exposed to wide range of climactic conditions.
- Harsh: Hazardous conditions such as inside burning structures and explosive atmosphere requiring intrinsically safe devices.

Furthermore the PSBN is intended to serve emergency response teams during disasters and restoration of damaged communications infrastructure, during search and rescue operations, and during recovery operations.

1.2 Interoperability

One of the most important considerations for the PSBN is interoperability between agencies, across jurisdictions, and with FirstNet (U.S.) users. Interoperability means that users can

[4] Currently in Draft - version 1 to be published by fall 2013.

seamlessly fit into an incident command structure within their jurisdiction or while on mutual-aid missions. In addition, a core interoperability infrastructure is required to interface to the wide range of existing emergency responder communication tools. The PSBN is an enabler of interoperability by providing all the users with a common communications tool.

1.3 Applications

The PSBN is, in essence, an intelligent access network that provides a means for users to exchange information among them and with information repositories. Applications make the exchange possible and meaningful. The PSBN will enable a wide range of applications to be used on the network through "network services". Network services is the current of data that runs "under the hood" of the network. Data, such as location, key performance indicators, real-time and statistical usage, can be used by upper level applications to deliver meaningful information to users and network administrators.

The PSBN can also deliver hosted services such as SMS/MMS messaging, VoIP (eg. VoLTE), VPN, and other nationally and regionally-hosted applications.

1.4 Network Management

Network administrators comprise an important category of users. They provision services to users and can also disable service when necessary. They monitor how the network is used and how it performs in real-time and non-real-time. They initiate action to upgrade or repair the network. The PSBN provides network administrators with the ability to access the information they need to accomplish their tasks, and the means by which they can control the network. Network administrators must also perform these functions in times of emergency and/or disaster, when other networks may not be available. The level of authorization required for network administrators to control the network varies according to the degree of control that is intended for the specific network administrator. It is expected that there will be a hierarchy of network administration functions with each subsequent level having authority to access more sensitive levels of control.

1.5 Congestion Management

It is expected that the capacity of the PSBN will not be sufficient to support the demands for data communications for incidents that involve a large number of responders in a small geographic area. It is, therefore, necessary to apply congestion management techniques and policies to prioritize traffic and allocate Quality of Service (QoS) to applications in accordance with pre-established polices. The techniques need to allow dynamic adaptation of priorities and QoS in response to the communications needs of the incident response team as the nature of the incident evolves.

1.6 Resiliency

The ability for users to access their services and applications under all possible environmental conditions, no matter where they are located is of prime importance. Meeting this need is a strong cost driver and, as such, a judicious cost-sensitive approach is necessary to balance the degree of resilience and the cost to achieve it.

Networks can be hardened to withstand adverse conditions to various degrees, such as providing back up power for all sites and extended back up power for critical sites. Multiple levels of redundancy can be built into the network, such as redundant backhaul for critical sites. In addition, an approach based on "assured fall-back" can ensure that if the primary communications network fails, that an available back-up network is present to pick up the load. The fall-back may present a lower grade of service, but would not be less than the minimum required to support the most critical needs of the mission. Another approach to increase resiliency is to provide overlapping cellular coverage, but this requires more infrastructure and thus is achieved at a substantial cost premium.

A layered protection scheme could provide elements of all the above approaches but applied selectively so that escalating degrees of protection are applied in proportion to the severity of damage to the infrastructure and the urgency to restore or upgrade the communications network.

Layered resiliency is based on waveform diversity and access diversity. Waveform diversity means that there are multiple radio technologies that are used for the communications network. For example, emergency vehicles could create a mesh network among themselves which could allow communications to be carried through the vehicle that is covered by the PSBN or a roaming partner's network. There could also be vehicles that are specially equipped to connect via satellites. Access diversity means that users can connect to any of a number of networks that are present. The users could also be connected in a mesh network. The technologies that render a communications network resilient should form networks that are self-healing, dynamic, adaptive, and autonomously re-configurable to maximize availability and throughput, at the lowest cost.

Graceful degradation is another instance of resiliency, whereby the network has the ability to maintain limited functionality and/or performance even following a catastrophic failure.

1.7 Security

The PSBN leverages open standards and is based on Internet Protocol (IP). Furthermore, the PSBN is connected to external networks such as the Internet in order to share information and messages globally. The PSBN is accessed by a wide range of users accessing a wide range of types of data. The users are assumed to be first responders, emergency management officials, defence forces, intelligence agencies, and even consumers, if allowed. Data can have varying degrees of sensitivity. Due to the purpose of the PSBN, it will attract internal and external threats. Thus, the PSBN is exposed, accessible, and attractive to potential hackers. Security risks must be mitigated by suitable policies and by applying robust security mechanisms to address the threats.

The Security Requirements[5] are intended to support a three-axes security architecture according to ITU-T recommendation X.805. See Figure 1-1 for an illustration of the security architecture. The three axes that form the basis of X.805 are: (i) security dimensions, (ii) security layers, and (ii) security planes.

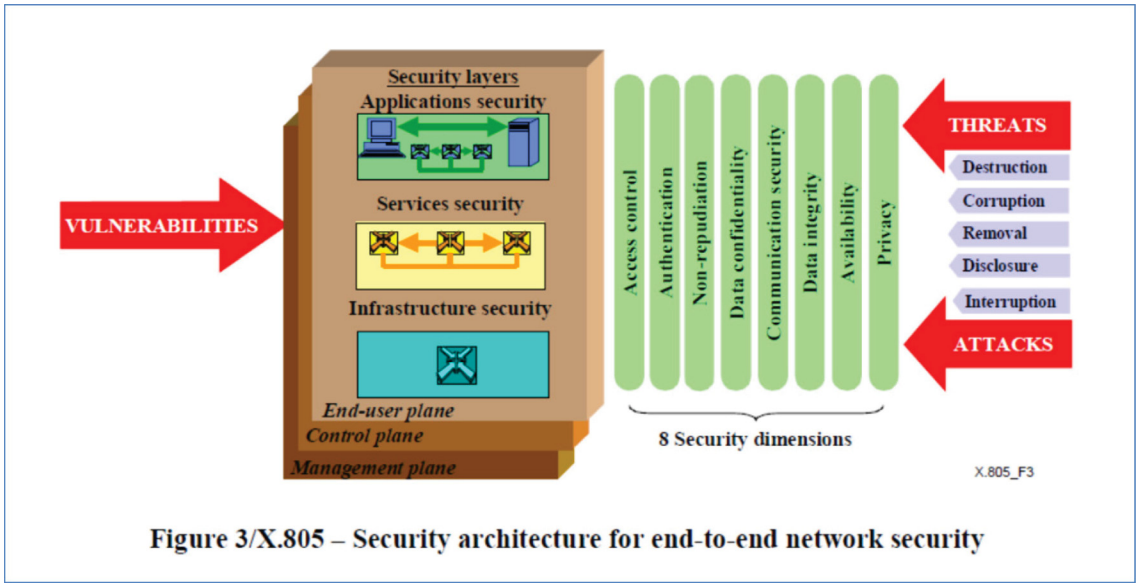

Figure 1-1: Security Architecture

In addition to network and information security, the Security Requirements also address the physical security of the infrastructure.

2. Network Architecture Considerations

The network architecture of the Public Safety Broadband Network (PSBN) is influenced by governance, service delivery, emergency response use-cases, economic, and technical considerations. They are outlined in this chapter along with the manner in which they influence the network architecture.

The statements in this section served as inputs to the development of the network architecture. Some of the assumptions will need to be validated, and some requirements may change. If the inputs change, the NAD will be updated to reflect the changes.

2.1 Governance considerations

The governance model consists of the following actors:

[5] Public Safety Broadband Communications Network - Security Requirements Document – CSS/DRDC V.P01 – DRAFT (Forecast publish date: Fall 2013).

- National Entity as the primary spectrum licensee. The National Entity is assumed to be responsible for the following:
    - As the licensed operator, be the named entity for the national Public Land Mobile Network Identifier (PLMN ID)
    - Define operational and performance requirements for the PSBN
    - Define the national interoperability requirements
    - Establish the cost and fee structure
    - Implement connectivity between regions
    - Host national applications
    - Administer roaming agreements with other carriers
    - Implement and operate the national portion of the PSBN
    - Define security polices and oversee their implementation

It is expected that the National Entity will be an independent not-for-profit corporation whose board members will represent the interests of the public safety community.

- Regional Service Delivery Entities (RSDE) as the subordinate licensees. The RSDE is assumed to be responsible for the following:
    - Implement and operate the regional portions of the PSBN
    - Interface directly with the public safety agencies and the users
    - Provide service coverage in their geographic jurisdictions
    - Collect fees for services delivered from the End User Agencies
    - Pay the allocated fees to the National Entity
    - Adhere to the licensing conditions, which include the national interoperability requirements in addition to whatever Industry Canada may impose as licensing conditions on the National Entity

Additional actors are:

- End User Agencies (EUAs) as the user community. The EUA is assumed to be responsible for the following:
    - Pay for services received from the RSDE
    - Administer the service and access privileges for the users under their jurisdiction
    - Procure devices and network equipment in accordance with approved specifications,
    - Adhere to security requirements
    - Host approved applications on their data networks

It is expected that EUAs will own strategic caches of RAN equipment that EUAs will deploy in an emergency to add capacity or increase coverage. Such equipment would conform to national and regional specifications for deployable/tactical nodes.

2.2 Service Delivery Model

Figure 2-1 illustrates the Service Delivery Model (SDM). The SDM shows how each of the three principal actors - the National Entity, the RSDEs, and the End User Agencies fit into the overall chain of connecting users to their information networks.

The National Entity and the RSDEs are depicted as being distinct from the users and the end user agencies (EUA) they pertain to. The EUAs own the information networks, whereas the National Entity and RSDE own the PSBN infrastructure. Applications can be hosted by the National Entity, RSDEs, and by End-User Agencies.

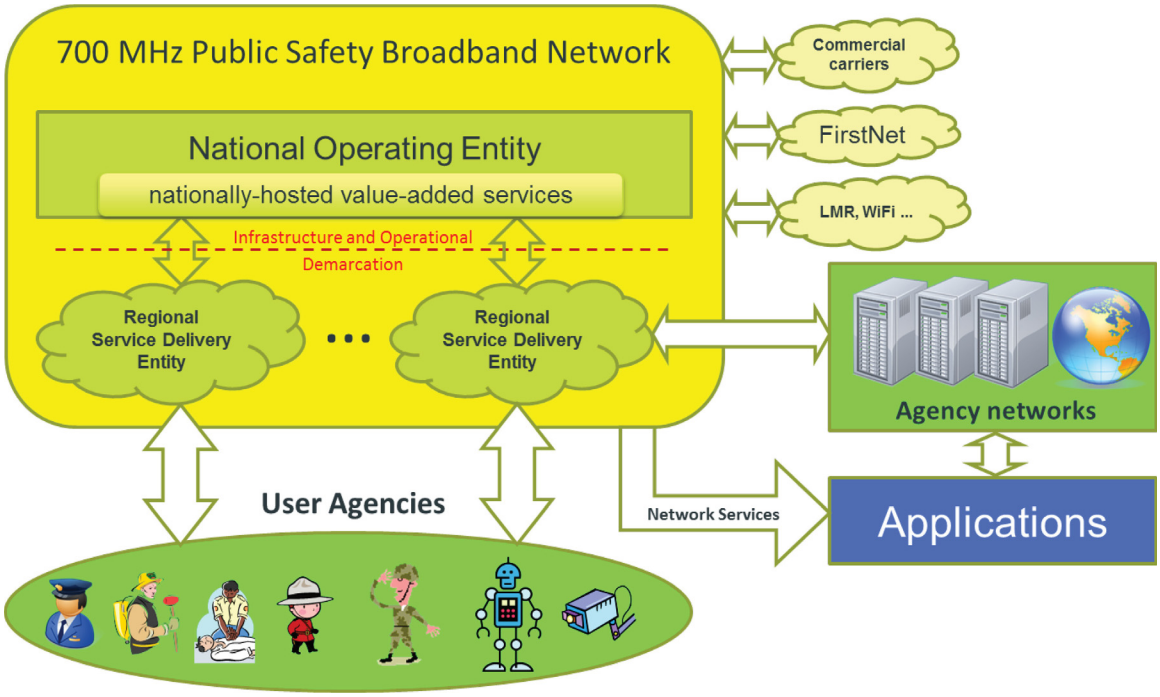

Figure 2-1: Service Delivery Model

The PSBN operators will interconnect the PSBN with external networks. Examples are shown in Figure 2-1 and will be covered in greater detail in Section 4.2.

2.3 Roles and Responsibilities – National Entity, RSDE, and EUA

Table 2-1 lists the roles and responsibilities of the principal actors in the service delivery model. This is not an exhaustive list. Table 2-1 is simply an input to this document, and it is not within the scope of this document to modify its contents. The purpose is to allocate some of the key

operational responsibilities to the principal actors which may have an impact on the network architecture.

	Operational dimensions	National Entity	Regional Service Delivery Entity	End User Agency	Notes
1	UE devices				
1.1	UE device certification	X			
1.2	UE procurement			X	From a list of approved devices
1.3	USIM procurement and distribution	X	X		National Entity distributes to RSDE; RSDE distributes to EUA
1.4	IMSI block/range allocations	X			National Entity manages Network Identifiers.
1.5	UE configuration and registration			X	
1.6	UE troubleshooting			X	
1.7	UE repairs/replacement			X	
1.8	UE performance monitoring		X	X	
1.9	UE updates push, track		X	X	
1.10	UE inventory management			X	
1.11	UE security policies - define	X			
1.12	UE security management - adherence to policies			X	
2	End-Users				
2.1	User registration, service provisioning			X	
2.2	User profile management			X	
2.3	User training on devices, applications, and procedures			X	
2.4	User service provisioning			X	
2.5	User-centric helpdesk			X	
2.6	User-centric web-based self-help tools			X	
2.7	User information network hosting (primary)			X	
2.8	User information network hosting (back-up)			X	
2.9	User authentication - credentialing			X	EUAs own the process to verify users' credentials.
2.10	User authentication - access control			X	EUAs own the policies for which users can access their information networks.
2.11	Development and maintenance of SOPs		X	X	may require coordination at national level
2.12	Define the guidelines for priority and QoS	X			National Entity defines profile template.
2.13	Priorty and QoS dynamic override during emergencies			X	
3	Applications				
3.1	Vetting applications according to standards	X			National Entity owns the approved applications list.
3.2	Procurement of applications software	X	X	X	
3.3	Hosting and management of applications, incl. installation.	X	X	X	
3.4	Security policies regarding applications	X			
3.5	Assigning Quality of Service (QCI) parameters per application	X			Harmonized across all regions
3.6	Troubleshooting applications	X	X	X	depends which entity has the contractual relationship with the vendor
4	Radio Access Network				
4.1	RF coverage objectives, implementation plan		X		
4.2	RF coverage implementation		X		
4.3	RAN performance monitoring and management	X	X	X	
4.4	Fixed radio infrastructure - ownership		X		
4.5	Deployable radio infrastructure - ownership		X	X	
4.6	Configuration standards for re-deployable radio infrastructure	X	X		able to inter-operate with fixed infrastructure in any region.
4.7	Configure radio infrastructure according to standards and maintain config images		X	X	
4.8	Spectrum audit		X		check if spectrum is clear at start and periodic check over time.
4.9	Congestion management policies	X			
4.10	Verification of interoperability of RAN		X		with other elements in the regional network and the core network
5	Core Network				
5.1	Ownership of the Core Network elements	X	X		according to the network architecture and demarcation points.
5.2	Procurement	X	X		
5.3	Configure core network elements according to stds and maintain config images	X	X		
5.4	Interconnection to external networks		X	X	PGW is owned by the RSDE, in general. However some EUAs may own PGW.
5.5	Security of interconnection to external networks		X	X	
6	Network Administration				
6.1	Security audit	X	X	X	If the PSBN is subject to external security audit.
6.2	Business process standards, (ISO-20000 ?)	X	X		every entity would be certified and audited against applicable standards
6.3	Network performance monitoring - service delivery portion		X	X	
6.4	Network performance monitoring - national layer and end-to-end	X			
6.5	Roaming agreements with other carriers	X			negotiating and owning the agreements
6.6	Ownership of assests used for interconnection to other carrier networks		X		
6.7	Settlement of roaming charges	X			assumes Clearinghouse can resolve call detail records to IMSI range.
6.8	Collection of payment from users		X		
6.9	Collection of payment from regional operators	X			
6.10	Network Identifiers management	X			
6.11	Management of Operational and Interoperability Requirements	X			change management under National entity
6.12	Training network administrators	X	X		
6.13	Management of SLA between regional service delivery entitiy and its partners		X		
6.14	Management of SLA between national operator and regional entities	X	X		
7	Maintenance				
7.1	Upgrades: establish the case or need for an upgrade	X	X		need can originate at either level.
7.2	Upgrades: assess impact on interoperability	X	X		onus on originator
7.3	Upgrades: verify impact on interoperability	X			National Entity would coordinate Change Control Board (reps from all RSDEs)
7.4	Upgrades: coordinate implementation of upgrades	X	X	X	
7.5	Vet credentials of staff that perform on-site maintenance	X	X	X	each level resp for the sites under its area of responsibility

Table 2-1: Roles and Responsibilities of the National Entity, the RSDE, and the EUA

2.4 Assumptions & Capabilities

2.4.1 Base

1) The National Entity would be the primary spectrum license-holder (granted by Industry Canada) for operating or overseeing the operation of a nation-wide public safety broadband network (PSBN) in the 700 MHz band.

2) The Regional Service Delivery Entities (RSDEs) would each hold a subordinate license. In order to qualify as a licensee, the RSDEs would need to adhere to interoperability requirements and other terms that would flow down from the National Entity, and include the license conditions that Industry Canada would impose on the primary licensee. There may be licensing fees and other cost recovery conditions. RSDE will hold the sublicense and will ensure adherence to the national interoperability requirements

3) A Regional Service Delivery Entity (RSDE) is defined as a province or territory or a collection of provinces and territories.

4) The Public Safety Broadband Network would be based on the Long Term Evolution (LTE) Rel.10 standards.

5) There is one Public Land Mobile Network Identifier (PLMN ID) for the nationwide Public Safety Broadband Network.

2.4.2 Mandatory

1) Network IDs are managed by the National Entity.

2) The National entity would not assume the duties of a Regional Service Delivery Entity in terms of delivering services to a specific region if the RSDE is unable to fulfill its obligations.

3) All authorized users served by the Public Safety Broadband Network may attach to any region of the Public Safety Broadband Network regardless of which agency they pertain to. There is no roaming by such users anywhere on the Public Safety Broadband Network. Access privileges and Quality of Service would be asserted locally to visiting users.

4) The National Entity is responsible for establishing and managing roaming agreements.

5) The Public Safety Broadband Network will provide messaging services to the users. This includes SMS, MMS, paging, status messages, and incoming alerts.

6) Roadmap of future services supported by the Public Safety Broadband Network shall include, as a minimum:

    a. Voice services comprising Push-To-Talk, Group Call, Conferencing, and Talk Around (when supported by LTE).

b. Connection to the Public Switched Telephone Network.
c. Connection to NG-911 systems.
d. Connection to emergency alert broadcast system.

7) The network operator shall not be required to store user data that is carried over the Public Safety Broadband Network, except if required by regulations.

8) Billing (due to roaming) will be reconciled at the national level. The National Entity will settle the inter-carrier charges. It will collect or credit the amount attributed to the specific Regional Service Delivery Entity.

9) Sensitive data shall remain under Canadian jurisdictional control while in transit or at rest, and must not leave Canada. That means that sensitive data must not traverse through network devices such as routers or servers outside Canada. There may be special dispensation granted that would allow sensitive data to exit Canada.

10) Multi-vendor interoperability is required through the use of open standards.

2.4.3 Desired

1) The user can roam onto commercial carriers when he/she is outside the coverage footprint of the Public Safety Broadband Network. This implies that roaming agreements are in force between the National Entity and the commercial carriers. It also requires that the user devices are compatible between the roaming partners in terms of frequency bands and Radio Access Technologies. Roaming can only occur between partners that have roaming agreements in force.

2) Active sessions should remain active when roaming (either direction) between the Public Safety Broadband Network and the commercial network.

3) User profiles contain default priority settings. This may be temporarily overridden by Incident Command.

4) No single points of failure. Layered assured fail-over, redundancy, and hardening are used according to cost vs. benefit. Fail-over to an assured operating back-up can be an option. It is also possible to consider that the performance achieved through the back-up could be reduced temporarily.

5) Users' profile and access privileges are assigned and managed by the end-user agency. This includes access privileges for visiting and roaming users. An automatic default template should provide minimum access privileges. Privileges are assigned by the appropriate administrator. A default "time out" shall remove access privileges from visitors. User access and profile management would be performed by the local End User Agency. Ex. Ottawa police user profiles would be administered by an employee of the Ottawa police (administrator) - not by the Ontario Regional Service Delivery Entity, nor by the National Entity. User profiles and access privileges for US responders roaming

onto the Canadian Public Safety Broadband Network would be managed by the End User Agency requesting the cross-border aid.

6) It is envisaged that the administrators of the user profiles would use a common template to enter the information. The GUI could be provided by the National Entity to have a common look-and-feel. On the policy side, a process is needed whereby users are granted access to certain information. The local agency administrator may be able to grant access to information belonging to his/her agency, but would likely not be able to grant access to info that does not belong to it. It is important that the administrator of one group of users not be able to access the user profiles of users under the administration of another agency.

7) The Public Safety Broadband Network may be required to support legal interception of traffic, including encrypted traffic. This is subject to regulations from Industry Canada or other authorized government agency.

8) Evolved Multimedia Broadcast and Multicast Systems (eMBMS) should be used to make efficient use of the downstream resource allocations for data which must be simultaneously broadcasted to a large number of users.

9) Sharing of public safety spectrum with commercial carriers is possible, with suitable agreements for security, service level, and priority access. The public safety spectrum could also be shared with utilities and providers of critical infrastructure. This assumes that Industry Canada permits such sharing.

10) Sharing of infrastructure is possible, as long as security and interoperability requirements are met.

11) End-user devices will be regulated. Only approved devices will be allowed to access the Public Safety Broadband Network.

12) End-user agencies own the information and data repositories. The PSBN may offer value-added services in a hosted manner to subscribing agencies. The user agencies would not necessarily own the infrastructure. They would own the data, including the data of user profiles. The physical Home Subscriber Server (HSS) would be owned and managed by the National Entity. The National Entity would make available to the user agencies a means by which they can enter user profile information.

13) End-user agencies may own fill-in or drop-in nodes and deploy them to suit the needs of the response to the incident. These nodes could be small cells or relay nodes, and can use current radio access technologies such as LTE, WiFi, WiMAX, mobile ad hoc networking systems, or other future technologies. In some cases these fill-in systems need to integrate with the PSBN.

14) Traffic off-loading to trusted and untrusted WiFi networks will be supported. Support for priority and QoS will depend on the version of WiFi used (Ex: 802.11e). Examples of trusted WiFi networks are those which are owned by End User Agencies. These can be

portable hot spots or fixed hot spots. Examples of un-trusted WiFi networks are hot spots used to enhance indoor coverage such as in stadiums and convention centres.

15) Traffic off-loading to other Radio Access Technologies (RATs), such as WiMAX and satellite-based mobile services may be considered. This implies that that the user devices include those RATs. A potential off-load configuration is to use the emergency vehicle as the gateway to these networks. The user could connect to the vehicle using WiFi and vehicle could connect to a WiMAX or satellite network.

2.5 Standards

The PSBN will be based on the 3GPP's LTE series of specifications and standards. The 3GPP standards and specifications will not be enumerated here because the list is extensive and also to avoid omitting applicable references. It is expected that as standards evolve and new ones are created, they will serve as references for the design of the network architecture.

The PSBN will comprise non-3GPP technology too and will also interface with networks that are non-3GPP. Adherence to inter-networking standards will be critical in order to ensure on-going interoperability between networks which are under different ownership.

An important consideration in the PSBN network architecture is the inter-networking between the mobile infrastructure and the fixed infrastructure. 3GPP is currently evaluating standards for fixed and mobile convergence (FMC)[6]. For example, one of the issues currently under study by the 3GPP is how policy and charging control and QoS can be used in the same way between the mobile network and a fixed network. This is of interest to at least 2 use cases for public safety: (i) off-loading the 700 MHz mobile network when fixed access networks are available, and (ii) using the first responder's vehicle as a WiFi hot spot for officers and, at the same time, serving as the gateway to the 700 MHz mobile network. Priority and QoS must be asserted according to pre-established policies in a similar manner regardless of which network is serving the first responder. Other considerations for Fixed Mobile Convergence (FMC) are:

- Seamless off-loading
- Security
- User authentication

The telecommunications industry has long recognized the importance of automating the processes that communications carriers use in the day-to-operations of their network. Automation has been largely achieved by applying software systems to manage the flow of information between network elements in response to human triggers or machine-originated triggers. Over the past several years, important strides have been made by the TeleManagement Forum (TM Forum) and other standards development organizations to standardize the interfaces of the network elements and the adaptors that allow the network elements to participate in the automation processes. The TM Forum created a model that allows disparate applications to collaborate in workflow processes without the need to customize each application to the adjacent ones in the workflow.

[6] http://www.3gpp.org/3GPP-and-the-Broadband-Forum

The model facilitates the interconnection of diverse Operations Administration Provisioning and Management (OAP&M) applications with the intent of simplifying their integration into a single network operations support system (OSS). The model is known as Frameworx™.[3]

In the area of applications development, the GSMA has proposed a standard for APIs, called OneAPI, which is being adopted by operators internationally. "OneAPI is a global GSMA initiative to provide application programming interfaces (APIs) that enable applications to exploit mobile network capabilities, such as messaging, authentication, payments and location-finding with a cross-operator reach. For example, a messaging network API could be used to enable an app to send an SMS message to another device, while a payment network API could be used to add an in-app purchase to the user's mobile phone bill. Major operators, such as AT&T, Deutsche Telekom, Orange, Telefonica and Vodafone, Rogers, Bell Canada, TELUS, are working with the OneAPI initiative to expose network APIs through their developer programmes."[7]

2.6 Regulations

The operators of the PSBN will need to adhere to government regulations, such as those from Industry Canada. The license conditions are not currently known but are expected to address, as a minimum:

- Population coverage targets
- Categories of users that are authorized to be served by the PSBN
- License fees
- Radio Frequency (RF) emissions masks
- Lawful intercept

The design considerations in the NAD assume that consumers will be permitted to share the public safety spectrum.

2.7 Serving rural and remote areas

Rural and remote areas (as defined in the Definitions section) may or may not be served by commercial carriers, depending on the business case for return on investment. In the case were there are no terrestrial broadband telecommunication services available in these areas, they become in fact isolated. For those isolated areas where the physical geography makes the establishment of such services impractical, these areas could instead be reached via satellite links. During a disaster situation in a remote region (e.g. plane crash, pipeline breech, wildfires etc), deployable 'cell-on-wheels' type systems with appropriate backhaul links may be used.

2.8 Roaming with commercial carriers

In early deployments of the PSBN, it is expected that the geographic coverage of the public safety spectrum will be less than the more mature and better funded deployments of the commercial carriers. As such, the ability for first responders to be served over commercial spectrum should be considered. It is envisaged that roaming agreements will be established between the PSBN National Entity and commercial carriers.

[7] Source: http://www.gsma.com/oneapi

While roaming on commercial networks, first responders will want to reach their data networks and application servers with the same level of security as they have on the PSBN. First responders will desire to have priority service[8] on commercial networks during emergencies.

[8] Mapping of QCI and ARP by both PSBN and commercial networks according to roaming agreements.

2.9 Interworking with FirstNet

It is expected that the National Entity will enter into a roaming agreement with FirstNet such that first responders from either side of the US-Canadian border may access their services over a public safety broadband network when they are operating across the border. Authorization may be required and is expected to flow from agreed-upon protocols for how to provision services to first responders from across the border.

Since it is likely that FirstNet and the PSBN will operate on the same frequency band, care needs to be taken to avoid coverage gaps along the border due to interference. The spectrum should be managed between FirstNet and the PSBN in a way that makes the maximum amount of bandwidth available to first responders regardless of which side of the border they are on. This is predicated on an agreement for the conditions and circumstances under which the spectrum will be shared. Cross-border coordination of congestion management protocols may become critical in some highly populated regions such as Windsor/Detroit.

2.10 Cost effective network implementation and operation

Cost is an important consideration in the design of the network architecture. As such, any means by which cost can be reduced or ways in which the spectrum can be more effectively utilized and monetized should be pursued.

2.10.1 Infrastructure sharing

Figure 2-2 presents the potential savings that could be achieved through various sharing options. It is highly desirable to share facilities, network elements, and operations with other organizations to some degree. This includes other End User Agencies, public institutions, utilities, commercial carriers, private network operators, etc.

The degree of sharing depends on the point where organizational objectives are common and where they diverge. For example, utilities may have a greater motivation to harden radio sites to the same degree as public safety than do commercial carriers. On the other hand, commercial carriers have a greater motivation to densify their networks in urban areas than utilities.

2.10.2 Spectrum sharing

One way to increase the revenue stream for the RSDE is to share spectrum with other user groups. This is predicated on Industry Canada granting permission to share the public safety spectrum. Assuming such permission is granted, priority to access the radio resources during periods of congestion should be with first responders.

Some considerations when sharing spectrum with consumers:

- Lawful intercept orders for consumers should be served by the commercial network operator and should not impact the operations of the RSDE nor of the National Entity.
- There should be precautions taken to prevent malicious applications on consumer devices to attempt to interfere with the availability of the spectrum for other users. For example, a

consumer device, or a number of them may be turned into radio jammers on Band-14, thus denying service to all users.

- Policy on priority and QoS needs to consider how to prioritize emergency calls made by consumers.

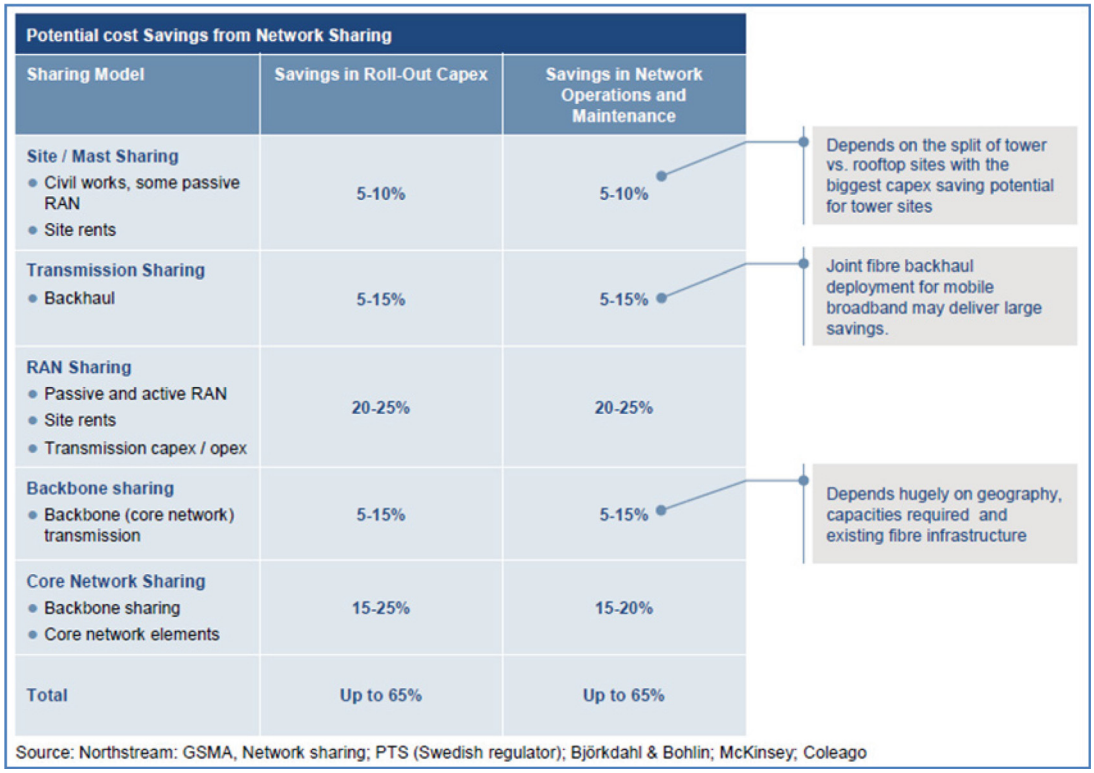

Figure 2-2: Potential savings in capex and opex from various sharing options.

2.11 Interworking with public and private networks

The PSBN is expected to interface with other networks or systems. These networks or systems, as currently identified, are:

- Public Internet
- End User Agency (EUA) data networks – federal, provincial, territorial, municipal
- Public alerting networks
- Commercial carrier partner network with whom Band-14 spectrum is shared, assuming this is allowed by Industry Canada
- Commercial carriers through roaming agreements
- FirstNet through roaming agreements
- Clearinghouse IP eXchange
- Satellite hub station
- VSAT terminals
- Transport network (backhaul)
- Lawful intercept

- NG 911 network
- E911 network
- Untrusted wireless networks
- Trusted wireless networks

The PSBN is composed of sub-networks and elements which need to interoperate. These are:

- National Entity
- RSDE
- Federal Network Access
- End-user devices
- IP Multimedia Subsystem (IMS)
- Application Service Delivery networks

We shall not consider Operations Support Systems (OSS) and Business Support Systems (BSS) at the present time. It is assumed that these are application networks that interface with element management layers of the various network elements and that they do not impact the network architecture.

2.12 Integrating other wireless networks

It is highly desirable to leverage the presence of small cells to off-load traffic from the macro wireless network and to capitalize on the enhanced coverage from an anticipated dense deployment of small cells. The 3GPP and the Wireless Broadband Alliance are intent on developing standards to allow LTE and non-UMTS networks to interoperate whereby priority and QoS policies can be applied in the same manner on both networks. In addition, the standards will also address seamless authentication, authorization, and accounting (AAA) as users migrate from one coverage domain to the other.

2.13 Priority & QoS management

It is essential to be able to manage the data traffic congestion on the PSBN during periods when demand exceeds capacity. First Responders will expect that the information they need to conduct their missions will be available to them in a reliable and timely manner. Priority and QoS policies will be required which govern how the bandwidth will be shared during periods of congestion. In turn, it is expected that the policies will affect Standard Operating Procedures (SOP). This means that it is likely that SOPs will assume a certain availability of the data service. It would not be practical for first responders to have to check their devices to know what network they are registered on in order to infer what kind of priority and QoS to expect from the network serving them at any point in time. As such, it is required for all networks on which first responders are authorized to access, to have the same priority and QoS capabilities, and that all their owners and operators adopt the same priority and QoS policies.

2.14 Resiliency

In the context of the PSBN, resiliency is synonymous with survivability. It is an attribute of the network to continue to operate during disasters. Thus, it directly affects service availability.

Resiliency can be achieved through several infrastructure strategies.

- Protect all active network elements with redundant network elements
- Provide alternative paths for communications traffic
- Harden sites to withstand severe environmental conditions and long duration disaster events
- Apply stringent controls on sourcing network elements, applications, and devices; control device operating systems

All the above measures could be considered in imparting a high degree of resiliency on the network. Whichever strategy or combination of strategies is applied will depend greatly on the cost versus risk. The strategies can be applied locally independently of each other.

In the layered resiliency strategy of alternative access, we assume that some first responders are outside the footprint of the terrestrial LTE network. One part of the strategy is to extend the reach of the terrestrial network (LTE eNB) using the vehicles which are within the coverage zone as repeaters for those other vehicles and first responders that are outside the coverage area. In addition, the devices of the first responders could also be able to communicate with each other in a mesh-type arrangement and to the vehicles. The vehicles themselves could use long-range non line-of-sight (NLOS) waveforms to connect each other in a high capacity Vehicular Ad hoc mesh NETwork (VANET).

In cases where some towers are damaged or non-existent, satellite could be considered as an alternative backhaul. The long transit delay should be taken into consideration when determining what signals are carried over the satellite path. In this case one or more specialized vehicles could contain the satellite terminals and the other vehicles are served through the VANET. LTE service could be temporarily restored through mobile LTE nodes using satellite backhaul for non-latency sensitive traffic.

3. Base Network Architecture

This section presents a network architecture that conforms to the governance model and meets the operational requirements summarized in Section 1.

The architecture is presented by first illustrating the base network block diagram of the PSBN and explaining the demarcation points for the entities involved. The core network, radio access networks, network services, and internetworking gateways are then described.

3.1 PSBN Network Block Diagram

The PSBN is a tiered network which consists of a National Entity, multiple Regional Service Delivery Entities, and a number of Federal Network Access sub-networks as shown in Figure 3-1 below. Based on the requirements, this figure demonstrates the concept using 3GPP's System Architecture Evolution (SAE) and Long-Term Evolution (LTE), though other core network or Radio Access Network (RAN) technologies may also be used to provide additional capabilities or services. Logical boxes with an underlying box represent a network component which is duplicated or redundant and items highlighted in green are optional based on the requirements of the serving entity i.e. National Entity or RSDE.

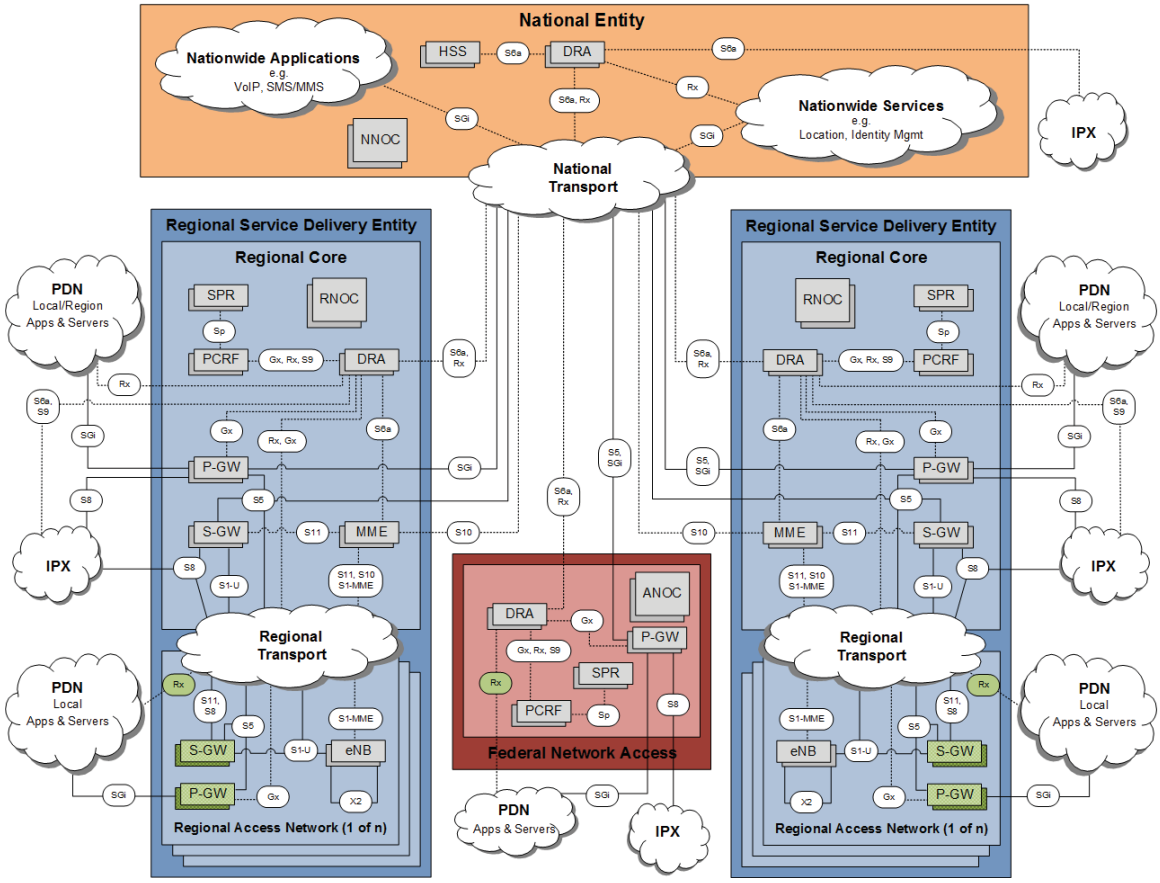

Figure 3-1: PSBN Network Block Diagram

Table 3-1 and Table 3-2 respectively list and describe the components and interfaces shown in Figure 3-1 above, while the following sub-sections expound on the previous definitions and roles of the PSBN entities.

Table 3-1: PSBN Network Block Diagram Components

Component	Name	Description
S-GW	Serving Gateway	The S-GW is the point of interconnect between the radio-side and the EPC; all user IP packets are transferred through the S-GW. The S-GW routes and forwards user data packets and serves as the local mobility anchor for the data bearers when the user equipment (UE) moves between eNodeBs. It also retains the information about the bearers when the UE is in the idle state and temporarily buffers downlink data while the MME initiates paging of the UE to re-establish the bearers. In addition, the S-GW performs some administrative functions in the visited network such as collecting information for charging (for example, the volume of data sent to or received from the user) and lawful interception. It also serves as the mobility anchor for interworking with other 3GPP technologies such as general packet radio service (GPRS) and UMTS.
P-GW	Packet Data Network Gateway	The P-GW is the point of interconnect between the EPC and the external IP networks. It provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. It is responsible for IP address allocation for the UE, as well as QoS enforcement and flow-based charging based on rules from the PCRF. It also serves as the mobility anchor for interworking with non-3GPP technologies such as CDMA2000 and WiMAX networks.
MME	Mobility Management Entity	The MME is the key control-node for the LTE access-network. It is responsible for idle mode UE tracking and paging procedure including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW for a UE at the initial attach and at time of intra-LTE handover involving core network node relocation. It is responsible for authenticating the user by interacting with the HSS.
PCRF	Policy and Charging Rules Function	The PCRF is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities which resides in the P-GW. It provides the QoS authorization that decides how a certain data flow will be treated by the P-GW and ensures that this is in accordance with the user's subscription profile.
HSS	Home Subscriber Server	The HSS is a data base that stores the information of each and every user in the network and performs the authentication and authorization of the users and services provided to them. It contains users' subscription data such as the subscribed QoS profile and any access restrictions for roaming. It also holds information about the PDNs to which the user can connect. In addition, the HSS holds dynamic information such as the identity of the MME to which the user is currently attached or registered.
SPR	Subscriber Profile Repository	The SPR contains information about the users' subscription to specific services. The PCRF uses the SPR to determine the rules to apply to data flows based on profiles stored in the SPR.
DRA	Diameter Routing Agent	The DRA provides routing capabilities for the Diameter control protocol used by many LTE core network components to exchange information about end-user device tracking, session tracking, session management, data usage, entitlements and other details. The DRA allows for the centralization of the Diameter routing functionality, therefore avoiding a Diameter mesh between core network components. While not required in

Component	Name	Description
		the EPC, DRAs simplify network deployment and facilitate future expansions.
(N/R/A) NOC	Network Operation Center	The Network Operations Centre is the site from where the PSBN is administered and monitored. There are 3 instances: National NOC (NNOC), Regional NOC (RNOC) and Agency NOC (ANOC).

Table 3-2: PSBN Network Diagram Interfaces

Interface	Description
Gx	Interface between the PCRF and the Policy and Charging Enforcement Function (PCEF) in the P-GW for the dynamic control of policy rules. Uses the Diameter protocol.
Rx	Interface between the PCRF and the Application Function (AF) in a given application network for the transfer of IP filtering and QoS information. Uses the Diameter protocol.
S1-MME	Interface for the S1-AP control plane protocol between the eNB and the MME. S1-AP uses the Stream Control Transmission Protocol (STCP)/IP protocol, which guarantees delivery of signaling messages between the MME and eNodeB.
S1-U	Interface between the eNB and S-GW for the per bearer user plane tunneling and inter-eNB path switching during handover. S1-U communicates via GPRS Tunnelling Protocol for the user plane (GTP-U).
S5	Interface between the S-GW and P-GW providing user plane tunneling and tunnel management. Two variants of this interface are being standardized, namely, the GPRS Tunneling Protocol (GTP) and the Proxy Mobile IP (PMIP).
S6a	Interface between the MME and HSS providing subscriber authentication and location services. Uses the Diameter protocol.
S8	Inter-PLMN variant of S5 used in roaming scenarios.
S9	Interface between PCRFs in roaming scenarios. Uses the Diameter protocol.
S10	Interface between MMEs for MME relocation (i.e. handover) and MME to MME information transfer. Uses the GPRS Tunneling Protocol for the Control Plane (GTP-C).
S11	Interface between the MME and S-GW providing functions for paging coordination and mobility. Uses the GPRS Tunneling Protocol for the Control Plane (GTP-C).
SGi	Interface between the P-GW and the Packet Data Network (PDN). The PDN may be an operator-external public or private network or an intra-operator network (e.g. for provision of IMS services).
Sp	Interface between the SPR and the PCRF for the transfer of subscriber related information.
X2	Interface between eNBs for handover scenarios and for the transfer of Self-Organizing Network (SON) messages.

3.1.1 National Entity

The National Entity is the primary license holder for the public safety spectrum and deals directly with Industry Canada. The National Entity sub-licenses the spectrum to Regional Service Delivery Entities (RSDE) as long as they agree to and abide by a common set of policies and regulations. It also provides a means for the RSDEs to connect to each other and to national services and applications. The responsibilities of the National Entity are described in Sections 2.1 and 2.3.

Within the PSBN, the National Entity will deploy, manage, and maintain the following elements:

Table 3-3: National Entity Components

Component	Description
National Transport	The national transport interconnects the RSDEs and allows these entities to connect to the subscriber database and to national services and applications. In particular, it supports the S5, S6a, S10, SGi, and Rx interfaces. The QoS-aware national transport can consist of multiple transport, network, and data link technologies. These can include satellite backhaul links.
Subscriber Database	The subscriber database (HSS) contains subscriber information for every user in the network. In addition to managing and maintaining the database, the National Entity also administers the Network IDs and assigns IMSI blocks to RSDEs. Authorized EUA administrators must have access to the subscriber database in order to enter, modify, or delete user profiles. Alternatively, the PSBN can use the User Data Convergence (UDC) model. In such case, the National Entity would host a user data repository (UDR) instead of an HSS as per the 3GPP TS 23.335.
Nationwide Services	Nationwide services are services such as user location displays or identity management databases that can be used by Canadian End User Agencies, regardless of where they operate in Canada.
Nationwide Applications	Nationwide applications are applications such as user VoIP and SMS that can be used by Canadian End User Agencies, regardless of where they operate in Canada. They are expected to be tested and certified for use by the National Entity.

3.1.2 Regional Service Delivery Entity

Regions are defined as Provinces or Territories. It is envisioned that each province and territory will create one RSDE. RSDEs would work directly with the National Entity and become sub-licence holders. They would govern all users within their respective geographic regions to ensure adherence to national standards. The responsibilities of the RSDEs are described in Sections 2.1 and 2.3.

Within the PSBN, the Regional Service Delivery Entity will deploy, manage, maintain, and operate the core network and access network as described in the following table.

Table 3-4: Regional Service Delivery Entity Components

Component	Description
Core Network	With the exception of the subscriber database which is hosted at the national level, the RSDE is responsible for the deployment and operation of the Evolved Packet Core (EPC) components.
Radio Access Network	The radio access network is composed of eNodeBs and possibly other RAN technologies, which are distributed across the region. These tie into the regional transport in order to connect to the regional core.
Regional Access Network	Large municipal areas or remote locations may opt to include P-GWs and S-GWs near the radio access network to reduce loading on backhaul and/or reduce latency. For the purpose of this document, this mixture of radio access network and core components is referred as the regional access network.
Regional Transport	The regional transport interconnects the region's multiple radio access networks and regional access networks with the main core components. It allows clients in the access networks to connect to regional and national data networks and services. It carries data from the S1-U, S1-MME, S5, S8, S11, Gx, and Rx interfaces. The QoS-aware regional transport can consist of multiple transport, network, and data link technologies. These can include satellite backhaul links. The regional transport shall abide by the same QoS requirements as the national transport.
Connection to End User Agency Networks	End User Agencies can attach their network or part of their network to the PSBN. The RSDE would provide an Access Point Name and configure a P-GW and a Firewall to connect to this particular packet data network. The end-user administrator would then be able to select that APN for their users. It is expected that the network would only be available to the users of that particular agency, though this does not preclude the agency from allowing access to other users.

3.1.3 Federal Network Access

Federal agencies are not tied to specific regions and may need to support any region or multiple regions during times of emergency. It is expected that users from federal agencies will access their information networks through RSDEs.

In the block diagram of the network architecture, the Federal Network Access consists of the interface to federal information networks as well as the interface to external networks whose access is managed by federal agencies. Federal agencies (e.g. RCMP, DND) may own deployable systems just as other EUAs may also own deployable systems.

3.2 Core Network

The PSBN network architecture is based on existing wireless communication standards. More specifically, the architecture is designed according to 3GPP's System Architecture Evolution (SAE) to provide Internet Protocol (IP) based voice and data services to the first responder community. The core components of the architecture are referred to as the Evolved Packet Core (EPC), a high-capacity, all-IP core network capable of providing real-time and media-rich

sessions for mobile users. The EPC is responsible for the overall control of the User Equipment (UE), the establishment of the bearers, and configuring the communication channels with QoS or flow-based data transmission characteristics.

As shown in the PSBN Network Block Diagram, the core network components are located within the RSDE level in the area identified as the Regional Core. One exception is made for the Home Subscriber Server (HSS) component which is located at the National Entity level. This allows for the centralisation of subscriber information for every user in the network, therefore providing a single point of entry for authentication and authorization regardless of the location of the user.

Instead of using the regional serving or packet data network, some municipalities may opt to deploy local gateways in order to reduce latencies or provide better service if needed. This is illustrated in the PSBN Network Block Diagram (Figure 3-1), where the S-GW and the P-GW in the regional network access box are highlighted in green. These gateways use the regional transport network to connect with other core network components. As such, they must be interoperable with other regional core components.

Each RSDE is expected to deploy, maintain and operate a Regional Core to meet the communication requirements of public safety entities in the region, while maintaining interoperability with networks of other RSDEs. This model provides flexibility for the regions to develop and deploy their respective Regional Core based on their timelines and according to their operational requirements and financial status. It also allows for regions to control the equipment provider selection process and to enter into agreements with commercial operators for purposes of building, operating, and/or entering into various sharing arrangements. Other advantages of the Regional Core model include:

- Minimized cross-region interoperability issues since internal/non-roaming EPC interfaces are not exposed;
- Follows proven approach and current commercial practices;
- Allows for regional control over the maintenance and upgrade of the network

All core network components should be duplicated and monitored regularly. These should be duplicated in a geographically separate location such that the RSDE can remain operational if the main components become damaged or disconnected. The duplicate components should be located in a region that is not subject to the same environmental hazards as the main network components, and should be powered from a separate power grid. This level of redundancy can tolerate the simultaneous failures of two serial network elements and the catastrophic failure of the main components. All components should be interconnected by a redundant backbone network where each fibre (assuming fibre optic backbone) should be carried on a different physical bundle and each bundle should be routed on a different geographic path. This is to avoid the possibility that a disruptive event cuts one fibre bundle thereby taking out the entire backbone network. Regional networks should also have redundant connections to the backbone network.

Two or more regions may also decide to share redundancy efforts to ensure that their secondary network is in a region that is not subject to the same environmental hazards as the main network

components. For instance, the core network components of one region can be configured to act as the back-up component of one or more regions should their networks fail.

3.3 Radio Access Network

The PSBN's radio access network (RAN) is based on E-UTRAN's LTE standard. The main component of this standard is the evolved Node B or eNodeB. This device communicates directly with the handset and to the EPC.

The RSDEs are responsible for deploying and maintaining the RAN within their region. It is expected that they will deploy sufficient RAN components to serve a large portion of the region or population, though exact coverage goals and strategies will depend on timelines, funds and national or regional policies.

The RAN components use the regional transport network to connect back to the regional core. In some cases, these components will be deployed in remote rural areas which may not have a fixed backhaul link. These areas may have to rely on a satellite link or some other remote communications technology to connect back to the core. This scenario is further described in Section 4.3 and Section 4.4.

RSDEs may also opt to use other RAN technologies such as Wi-Fi or WiMAX in order to offload data or to allow users to use locally available hot-spots. Although this option is not shown in Figure 3-1, it is discussed in more detail in Section 4.2.3.

3.4 Network Elements

Since the National Entity and the RSDEs will deploy and maintain their respective network, networking elements such as routers, switches, and firewalls are thus required in order to interconnect these networks into a single PSBN system. To avoid service interruption, these devices should be redundant and secure.

Table 3-5 describes the main network elements used within the PSBN.

Table 3-5: Network Elements

Element	Description
Router	Routers interconnect different subnets together and allow one segment of a network to connect to another. Routers and firewalls can be combined in a single unit. The National Entity is responsible for managing the network IDs. It is expected that the National Entity will assign an IP address block to each RSDE. Each RSDE will then be able to set-up and configure their respective network. In this scenario, each region would use one or more routers within or at the borders of their network in order to connect to remote areas within their territory, to other entities via the national transport, or to other external networks.
Switch	Switches are used to distribute traffic within a respective network. Some switches include routing capabilities. For the purpose of this example, such switches are treated as routers as per the description above.

Element	Description
	It is expected that multiple switches will be deployed within each entity network in order to distribute traffic across the network. It is also expected that some if not all will use VLANs to separate and differentiate certain traffic flows.
Firewall	Firewalls protect the internal PSBN networks and are located at every ingress point within the network and in front of devices or networks which require more limited access. Firewalls rely on various access control lists (ACLs) to block incoming or outgoing traffic with specific ports or addresses. These ACLs may be different depending on the location and purpose of the firewall, though they should be tailored based on the policies and regulations of the National Entity and the RSDEs.

3.5 Network Services & Application Networks

The PSBN will provide access to essential network services and application networks. Figure 3-2 illustrates an example of how the National Entity and the RSDEs interconnect and connect to services and application networks. This example is for illustration purposes only. The PBSN may require more network elements or provide more services than what is shown here.

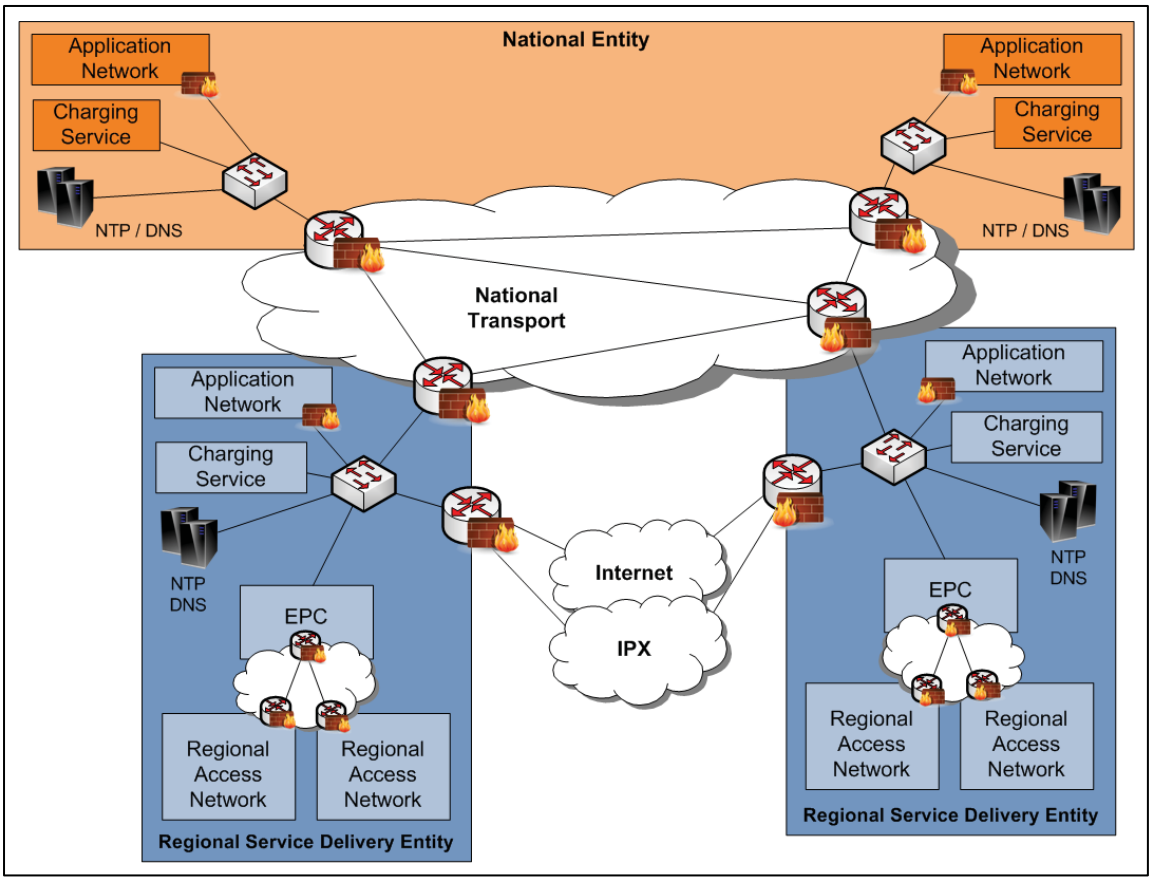

Figure 3-2: Example of PSBN Inter-Connection

In this example, RSDEs connect to each other and to the National Entity by means of routers. Each router uses a firewall to limit particular IP addresses or ports based on the policies and regulations in place. Once inside the network, one or more switches distribute the traffic to the proper device, service, or application network; each of which may have their own firewall to limit access as required. The following sub-sections briefly describe the essential network services provided by the PSBN. Section 3.5.4 gives a few examples of application networks and describes how the PSBN will use access point names to connect to these networks.

3.5.1 Network Time Service

The network time service provides and synchronizes accurate time to devices, operations, and users. It is required for the proper functioning and operation of the EPC and RAN as well as other network elements and services.

Although many solutions exist, Figure 3-2 illustrates one possible implementation of a network time service. In this example, Network Time Protocol (NTP) servers within the National Entity provide the main network time source for the PSBN using either GPS time or a very accurate clock. Regional NTP servers then synchronize to one or both of these to obtain the precise time. Local users and devices subsequently obtain the time from the regional NTP servers.

3.5.2 Domain Name Service

Domain name services allow users and devices to connect to particular services, equipments, or users by name instead of by an IP address.

Figure 3-2 shows a basic example where the National Entity and the RSDEs each have their own Domain Name Service (DNS). Each entity is thus able to customize and tailor their respective DNS according to their needs. While simple, this example may be vulnerable to certain forms of attacks. Separating the DNS into different planes can add more robustness and security.

3.5.3 Charging Service

The PSBN will require a charging system if the National Entity or the RSDEs plan to charge users for services or time used on the network and/or allow commercial users on the network. Such systems provide functions that implement offline and online charging mechanisms on the bearer (e.g. EPC), subsystem (e.g. IMS) and service (e.g. MMS) levels. In order to support these charging mechanisms, the network performs real-time monitoring of resource usage on the above three levels in order to detect the relevant chargeable events. Typical examples of network resource usage are a voice call of certain duration, the transport of a certain volume of data, or the submission of a multimedia message of a certain size.

3.5.3.1 Offline and Online Charging

The 3GPP charging architecture identifies two types of charging mechanisms which may be used simultaneously and independently for the same chargeable event; offline and online charging.

Offline charging is a process where charging information for network resource usage is collected concurrently with that resource usage, but which does not affect, in real-time, the service

rendered. The charging information is then passed through a chain of logical charging functions which results in the creation of Charging Data Record (CDR) files which are then transferred to the network operator's Billing Domain for the purpose of subscriber billing or inter-operator accounting.

Online charging is a process where charging information for network resource usage is collected concurrently with that resource usage in the same fashion as in offline charging. However, authorization for the network resource usage must be obtained by the network prior to the actual resource usage to occur. This authorization is granted by the Online Charging System (OCS) upon request from the network. When receiving a network resource usage request, the network assembles the relevant charging information and generates a charging event towards the OCS in real-time. The OCS then returns an appropriate resource usage authorization. This authorization may be limited in its scope (e.g. volume of data or duration) therefore it may have to be renewed from time to time as long as the user's network resource usage persists.

3.5.3.2 Event and Session Based Charging

Both online and offline charging can be categorized into two distinct classes, namely event based charging and session based charging.

Event based charging implies that a chargeable event is defined as a single end-user-to-network transaction (e.g. the sending of a multimedia message). This chargeable event is then mapped to an appropriate charging event, resulting in a single CDR (for offline charging) or in a single credit control and resource usage authorization procedure (for online charging).

Session based charging is characterized by the existence of a user session, such as a circuit call, an IP connectivity access network bearer, or an IMS session. This user session is then matched by a charging session, resulting in the generation of multiple chargeable/charging events and the creation of one or more CDRs (for offline charging) or the performance of a credit control session (for online charging).

3.5.3.3 Support for Roaming

The standard also provides information on inter-PLMN accounting for roaming traffic, which would be required for scenarios where users (first responders or commercial network users) roam between the PSBN and commercial cellular networks. The CDRs collected from the network also include details of the services employed by visiting and inbound roaming subscribers. The charges for Mobile Originated Calls (MOCs) and for supplementary services used are calculated as for home subscribers, converted to an agreed accounting currency and included in the CDRs which are exchanged with the commercial operator.

3.5.4 Access Point Names

Application networks can be used to host data, services, or servers for use by local, provincial, territorial, and national public safety users. Examples include:

- First-responder apps

- Regional or national news
- User equipment updates
- Shared databases
- Mobile VPN gateways

To support various use cases and interoperability between End User Agencies and users, it is expected that one or more application networks will be deployed within the National Entity network and the RSDE network. These application networks will be reachable through unique Access Point Names (APNs), which must be managed and coordinated nationally. In the context of the PSBN, two levels of APN scopes are expected:

- Nationwide APNs providing universal access to common applications and services
- Regional APNs providing access to applications and services specific to end-user groups

As shown in Figure 3-3, the EPC uses the APN to determine what network connection should be established for each service data flow, including the P-GW that can be used to establish that network connection. Within the P-GW, an APN can be viewed as a virtual routing domain, which provides route isolation across packet data networks and, in this case, application networks. A UE client must be bound to an APN to establish service data flows with its associated servers. Each of those service data flows can be allocated a particular EPS bearer and each EPS bearer is assigned one of the network-defined QoS Class Identifier (QCI). This QCI value defines parameters like bit rate, packet loss and delay. Simultaneous service data flows to multiple PDNs are also supported in the EPS (based on network policies and user subscription) through a single PGW or even separate P-GWs.

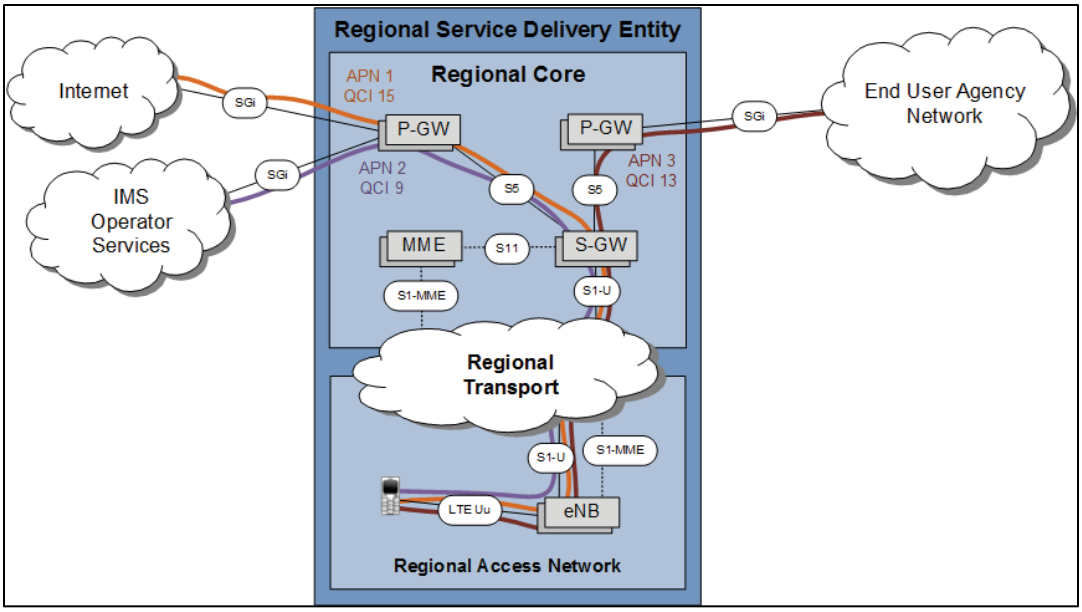

Figure 3-3: Example of Multiple APN Connections

A particular APN can be configured as the default APN, whereby the APN is configured in the HSS subscription data and used when the UE does not provide a desired APN during initial setup. The subscription data also contains a list of accessible APNs. If a particular APN is not on this list for a user, the user is not able to establish a service flow to that APN.

3.6 Gateways

The PSBN is expected to interface with other networks and systems. The following sub-sections describe and illustrate the gateway requirements to support these interfaces.

3.6.1 Intra-PSBN Entities

As shown in Figure 3-1, the PSBN consists of multiple RSDE networks, which can act independently for regional users and applications but must also provide support for visiting users and therefore allow for inter-entity connections. In essence, PSBN users can be transparently served anywhere on the PSBN network.

For any user (home or visiting), parenting of eNBs, MMEs, and S-GWs is done within a single RSDE. The P-GW is assigned dynamically based on the end-user APN request, and can require inter-entity bearer establishment. The following table lists some of the RAN and EPC interfaces and states whether they need to be open (i.e. accessible) between RSDEs to support visiting users.

Table 3-6: Intra-PSBN Entity Gateway Interfaces

Interface	Components	State	Description
LTE Uu	UE to eNB	Open	LTE Uu is the air interface between the eNB and the user equipment.
X2	eNB to eNB	Open	Required to support inter-entity ICIC and X2-based handovers
S1-MME	eNB to MME	Closed	eNBs and related pools of MMEs are managed by a single RSDE
S1-U	eNB to S-GW	Closed	eNBs and related pools of S-GWs are managed by a single RSDE
S10	MME to MME	Open	Required to support inter-MME tracking area updates
S11	S-GW to MME	Closed	Closed: Parented MMEs and S-GWs are managed by a single RSDE
S5	S-GW to P-GW	Open	Required to let users access their APNs (and related P-GW) from anywhere
SGi	P-GW to PDN	Open	Required to let users access particular packet data networks
S6a	MME to HSS	Open	Required to let users access the PSBN from anywhere (i.e. interface between regional and national entities)
Gx	P-GW to PCRF	Closed	Closed: parented PCRFs and P-GWs are managed by a single entity
Rx	PCRF to AS	Open	For national entity-based app servers (e.g. IMS) to control QoS anywhere in the PSBN

3.6.2 Agency Networks

It is expected that Public Safety users will use the PSBN to access their agency's network or services. This link will most likely be encrypted and protected by means of a VPN-type connection. The respective agencies may require dynamic control of the QoS policies for PDN data transfers. As shown in Figure 3-4, connections to Agency Network PDNs will be realized through the SGi of the P-GW for data transfer and the Rx interface of the PCRF for session control and QoS information.

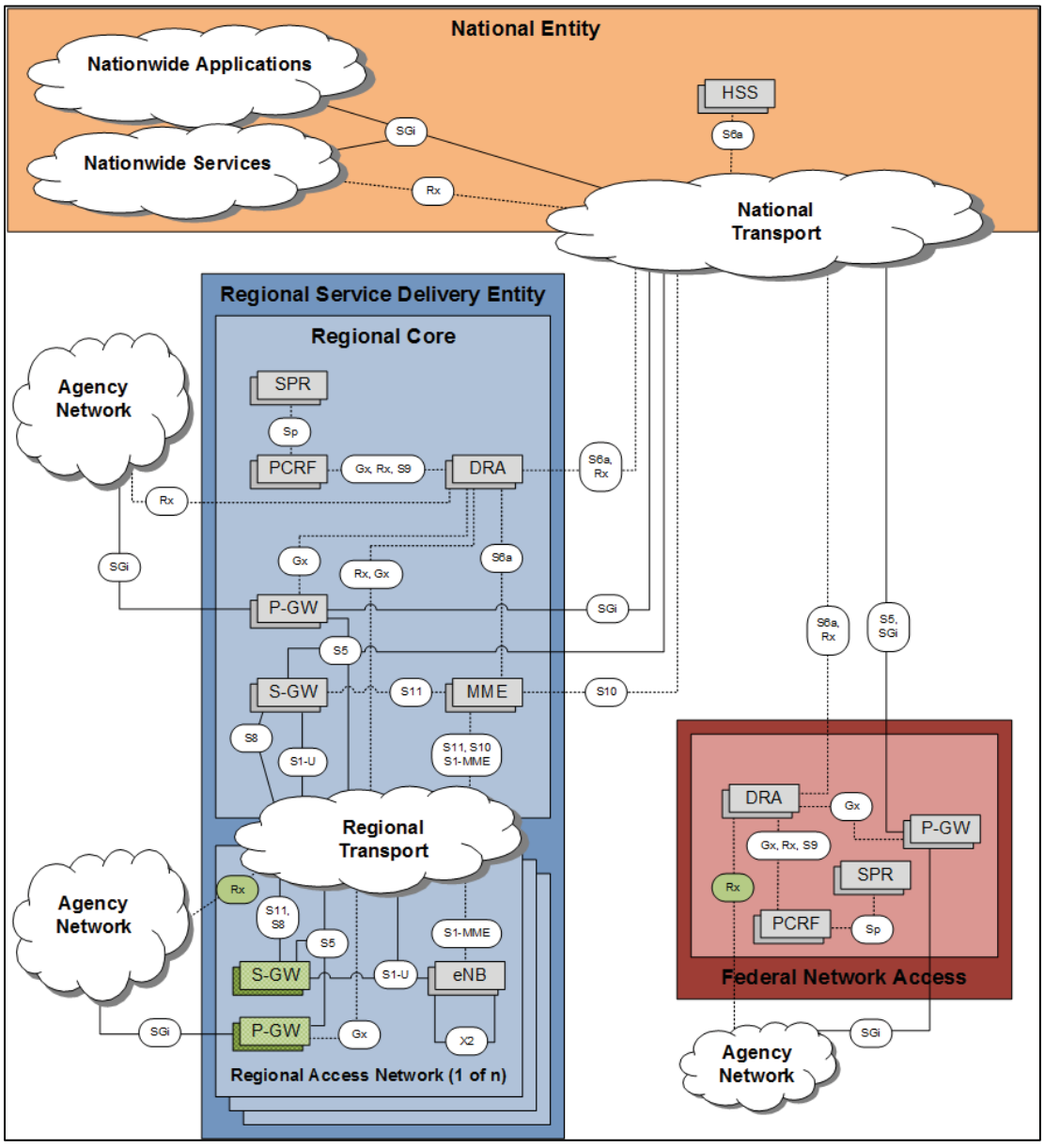

Figure 3-4: Connection to End User Agency Network

3.6.3 Private Networks

Access to private data networks is likely performed via VPN connections through the P-GW's SGi interface. In this instance, control over QoS policies is out of reach of the PSBN and the PCRF/Rx interface is not used.

3.6.4 Internet

PSBN users should have access to the Internet, based on the policies and regulations in place by the serving entity i.e. National Entity or RSDE. The internet connection passes through a P-GW, via the SGi interface.

4. Enhanced Network Capabilities

This section describes features that can be added unto the base network architecture to enhance the network's capabilities. Although they are not part of the base network architecture shown in the previous section, some of these features may be mandatory depending on the policies and regulations of the National Entity and the RSDEs. Other features can be added into the PSBN during or after the initial deployment.

4.1 Services

The following services can be included in the PSBN to provide voice and multimedia broadcast capabilities.

4.1.1 IP Multimedia Sub-system

IP Multimedia Sub-system (IMS) is an architectural framework for offering multimedia and voice over IP services. Since the SAE and LTE is completely IP based, analog voice is no longer supported. Instead, SAE uses Voice over LTE (VoLTE), a special type of Voice over IP (VoIP) technology which relies on IMS to manage and control signaling and media transcoding messages between the network and the PSTN.

IMS consists of session control, connection control and an applications services framework layered over an existing network infrastructure (e.g. LTE). It enables new converged voice and data services, while allowing for the interoperability of these converged services between internet and cellular subscribers using open standard IP protocols. IMS is access independent as it supports multiple access technologies such as GSM, WCDMA, CDMA2000, WLAN, and LTE.

In the context of the PSBM, IMS can be used to support IP based voice services (VoLTE), Multimedia Message Service (MMS) and also act as a bridging technology to external services and application such as Next Generation 911 (NG911) and Land Mobile Radio (LMR).

As the name implies, the IP Multimedia Sub-system consists of various components. These are listed and described in Table 4-1 below. The IMS interfaces are subsequently described in Table 4-2.

Table 4-1: IMS Components

Component	Name	Description
P-CSCF	Proxy Call Session Control Function	The P-CSCF is responsible for security of the messages between the network and the user and allocation of resources for the media flows.

Component	Name	Description
I-CSCF	Interrogating Call Session Control Function	The I-CSCF is a session control entity for endpoint devices that maintains session state. It is responsible for querying the HSS to determine the S-CSCF for a user.
S-CSCF	Serving Call Session Control Function	The S-CSCF is responsible for processing registrations to record the location of each user, user authentication, and call processing (including routing of calls to applications). The operation of the S-CSCF is controlled by policy stored in the HSS.
MRFC	Media Resource Function Controller	The MRFC is a signaling plane node that interprets information coming from an application server and S-CSCF to control the MRFP.
MRFP	Media Resource Function Processor	The MRFP is a media plane node used to mix, source or process media streams. It can also manage access right to shared resources.
BGCF	Breakout Gateway Control Function	The BGCF is a SIP proxy which processes requests for routing from an S-CSCF when the S-CSCF has determined that the session cannot be routed using DNS or ENUM/DNS. It includes routing functionality based on telephone numbers.
MGW	Media Gateway	The MGW interfaces with the media plane of the circuit switched network, by converting between RTP and PCM. It can also transcode when the codecs are not equivalent (e.g., IMS might use AMR, PSTN might use G.711).
MGCF	Media Gateway Controller Function	The MGCF controls the resources in a MGW and manages the distribution of sessions across MGWs.

Table 4-2: IMS Interfaces

Interface	Description
Cr	Used by MRFC to fetch documents (e.g. scripts, announcement files, and other resources) from an application server. Also used for media control related commands. Uses the SCTP protocol.
Cx	Used to send subscriber data to the S-CSCF, including authorization, authentication, filter criteria and their priority. Uses the Diameter protocol.
Iq	Conveys the necessary information needed to allocate and release transport addresses. Uses the H.248 protocol.
ISC	Reference point between S-CSCF and application servers. Main functions are to notify the application server of the registered IMPU and UE capabilities and supply the application server with information to allow it to execute multiple services. Uses the SIP protocol.
Mb	Interface to exchange RTP packets between the MGW and the IMS-AGW.
Mg	ISUP signaling to SIP signaling and forwards SIP signaling to I-CSCF. Uses the SIP protocol.
Mi	Used to exchange messages between S-CSCF and BGCF. Uses the SIP protocol.

Interface	Description
Mj	Used for the interworking with the PSTN/circuit switched domain, when the BGCF has determined that a breakout should occur in the same IMS network to send SIP message from BGCF to MGCF. Uses the SIP protocol.
Mn	Allows control of user-plane resources. Used the H.248 protocol.
Mr	Used to exchange information between S-CSCF and MRFC. Uses the SIP protocol.
Mw	Used to exchange messages between CSCFs. Uses the SIP protocol.
Rx	Used to exchange policy and charging related information between P-CSCF and PCRF. Uses the Diameter protocol.
SGi	Reference point between the P-GW and a packet data network. It 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.
Sh	Used to exchange User Profile information (e.g., user related data, group lists, user service related information or user location information or charging function addresses (used when the AS has not received the third party REGISTER for a user)) between an AS (SIP AS or OSA SCS) and HSS. Also allow AS to activate/deactivate filter criteria stored in the HSS on a per subscriber basis. Uses the Diameter protocol.

In the PSBN, these components are expected to be deployed within the National Entity and the RSDEs networks as shown in Figure 4-1 below. The Federal Network Accesses are not expected to require IMS components. This does not preclude them from installing their own IMS system if required.

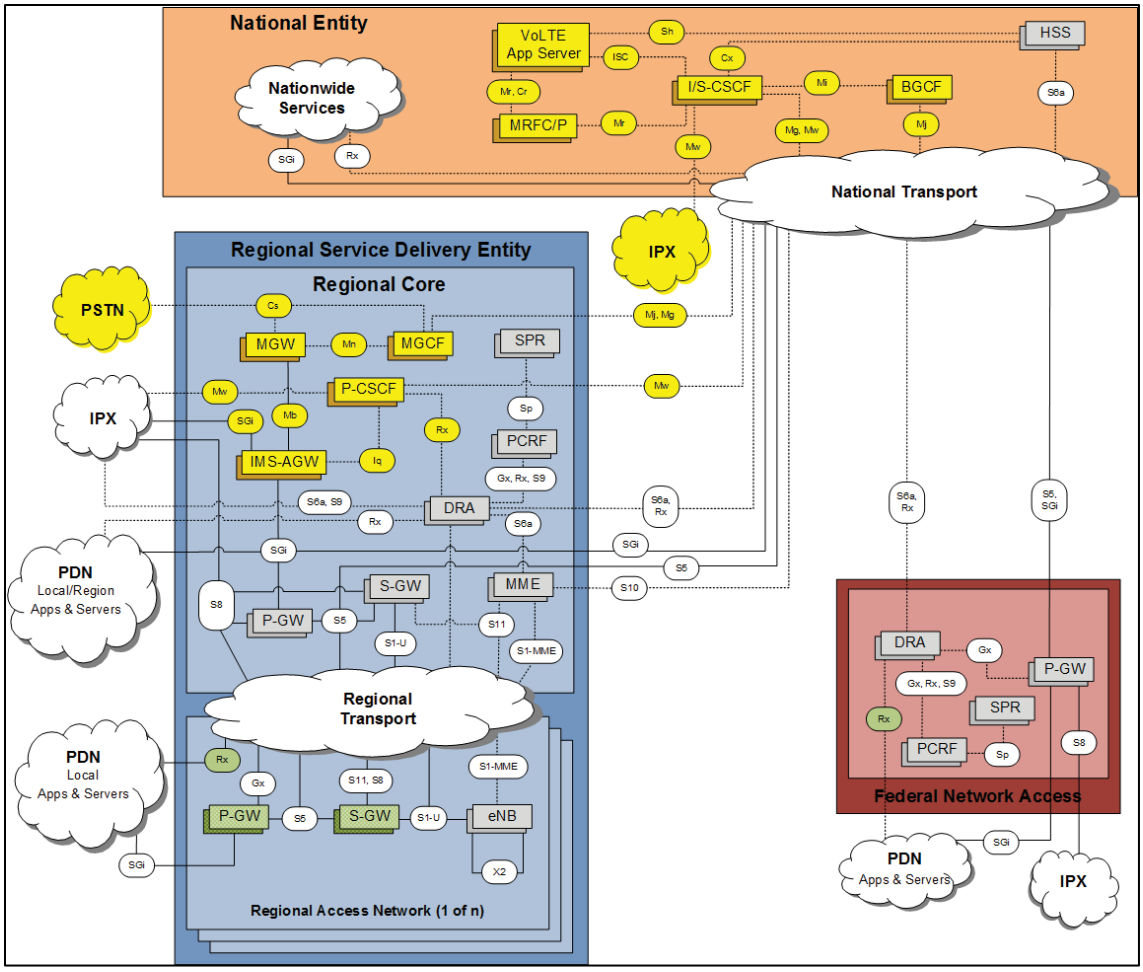

Figure 4-1: IMS Block Diagram

4.1.2 Evolved Multimedia Broadcast Multicast Service

The PSBN will require a multimedia broadcast multicast service (MBMS) if it plans to offer point-to-multipoint services to users over LTE. MBMS on LTE is also called evolved MBMS (eMBMS). In contrast to MBMS, eMBMS only provides broadcast services within the network. The same carrier frequencies are used to transmit both unicast and broadcast messages in LTE. As such, a portion of the total available bandwidth must be allocated for broadcast use in order to provide eMBMS services.

With respect to content provision, the same entities are involved whether services are provided in a unicast or broadcast fashion. As such, a content provider can be a third party organization or even a multimedia server within the RSDE network. In the context eMBMS however, user equipment do not connect directly to content servers. The Broadcast/Multicast Service Center (BM-SC) controls the broadcast sessions and maps content provider data onto broadcast bearers as configured by the network administrator.

A few key components are required in order to enable eMBMS functionality in the LTE network. They are listed and briefly described in Table 4-3 below. The eMBMS interfaces are subsequently listed and described in Table 4-4.

Table 4-3: eMBMS Components

Component	Name	Description
BM-SC	Broadcast Multicast Service Center	Provides functions for MBMS user service provisioning and delivery, including; membership, session and transmission, proxy and transport, service announcement, security, content synchronization and header compression.
MBMS GW	MBMS Gateway	Forwards MBMS user plane data to eNBs using IP Multicast. Performs MBMS Session Control Signaling towards the E-UTRAN via the MME.
MCE	Multi-cell/multicast Coordination Entity	The MCE is involved in MBMS Session Control Signaling. It provides functions such as admission control and the allocation of radio resource for MBMS transmissions, including additional radio configuration details such as Modulation and Coding Scheme (MCS). Additional functions include suspension and resumption of MBMS sessions as well as counting and acquisition of results for MBMS services.

Table 4-4: eMBMS Interfaces

Interface	Description
M1	User plane interface for the delivery of MBMS data (via IP) from MBMS GW to eNBs.
M2	Interface for the provision of radio configuration data and Session Control Signaling between MCE and eNB.
M3	Interface to support MBMS Session Control Signaling (e.g. MBMS session initiation and termination) between MME and MCE
SGmb	Interface for the control plane between BM-SC and MBMS GW (e.g. MBMS session start, update and stop, and session attributes like service area, QoS, etc.).
SGi-mb	Interface providing MBMS data delivery function between BM-SC and MBMS GW.
Sm	Interface for the control plane between MBMS GW and MME.

Figure 4-2 illustrates an example where an RSDE uses eMBMS components. These are highlighted in yellow.

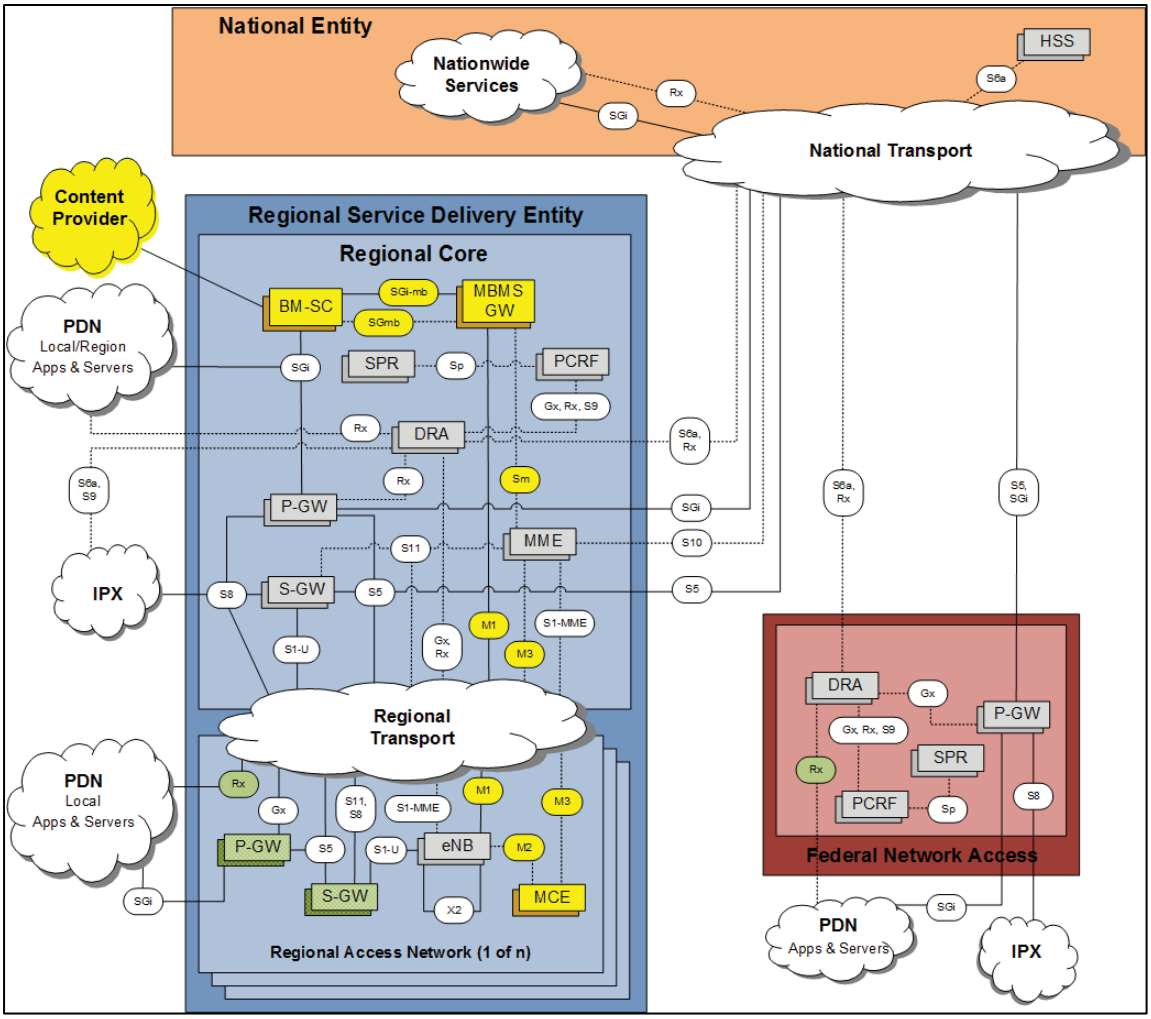

Figure 4-2: eMBMS Block Diagram

4.2 Gateways

In addition to the list in Section 3.6, the PSBN can also interface with the following networks and systems. It may be mandatory for the PSBN to connect with some of these depending on the policies and regulations of the National Entity and RSDEs.

- FirstNet
- Commercial Network
- Public Alerting System
- Trusted & un-trusted wireless networks
- Lawful Intercept System
- Next Generation 911 (NG911)
- Land Mobile Radio (LMR)

The following sub-sections describe and illustrate the gateway requirements to support these interfaces.

4.2.1 FirstNet

FirstNet users should be able to roam onto the PSBN when providing assistance during an event in Canada. Similarly, it is expected that PSBN users will be able to roam onto FirstNet when providing assistance during an event in the U.S. In either scenario, roaming users should be able to use local break-out mechanism, which consists in the local provisioning of data services by the visited network, with no intervention of the home provider in data services supply except for authentication. Local break-out allows the most efficient access to services available in the visited network, including access to the Internet and local incident information. When mission critical voice is involved, it enables visiting responders to easily and securely be added to talk groups that are supporting the response effort. Assuming cross-border traffic is permitted, PSBN users should also have the ability to securely connect to their home networks while roaming on FirstNet. This approach, called home routed, may be critical for access to public-safety databases and facilitates the proper security and logging of transactions in the home network.

If FirstNet and PSBN support voice via IMS, both home routed and local breakout approaches should be supported for voice communication roaming.

An alternative approach to inter-PLMN handovers would consist in session continuity via a mobile VPN approach. But technical and governance issues may render this approach difficult to implement. Furthermore, some mobile VPN solutions may not support having different QoS and Priority values per stream

The following table lists the inter-PLMN interfaces required to support different types of roaming approaches.

Table 4-5: Interfaces to Support Roaming unto FirstNet

Interface	Components	Description

Interface	Components	Description
S6a	Visited MME to home HSS	Required to authenticate users when using either home or local routing mechanisms. Uses Diameter protocol.
S8	Visited S-GW to home P-GW	Required to provide services to users when using home routing mechanisms.
S9	Visited PCRF to home PCRF	Required to retrieve appropriate QoS settings when using either home or local routing mechanisms. Uses Diameter protocol.
Mw	Visited P-CSCF to home S-CSCF	Required for voice sessions when using local routing mechanisms. Uses SIP protocol.
Mm (*)	S-CSCF (a) to S-CSCF (b)	Required for voice session when using either home or local routing mechanisms. Uses SIP protocol.
Mb (*)	IMS AGW (a) to IMS AGW (b)	Required for voice session when using either home or local routing mechanisms. Uses RTCP/RTP protocol.

(*) Not per se roaming interfaces, but rather interconnection interfaces

4.2.2 Commercial Network

Public Safety users should be able to roam onto commercial 4G networks if an area of interest is not served by the PSBN or if the local PSBN does not meet the minimum connectivity requirements for the user. Similarly, commercial users may be allowed to roam into the PSBN depending on the national or regional policies and regulations. Roaming to or from 3G networks should also be supported as long as the 3G network appears as a 4G network to the PSBN such that the 3G-LTE internetwork function is implemented in the visited PLMN. In this scenario, an IPX service is used as the framework for mobile data roaming.

For both voice and data, roaming PSBN users should use a home routing mechanism where a P-GW within the PSBN is used to connect to a segment of the PSBN network or to any other network. This ensures that users abide by PSBN policies and regulations even when roaming onto other networks.

The following table lists the EPC interfaces that must be opened or shared to support inter-PLMN roaming.

Table 4-6: Interfaces to Support Roaming unto Commercial Networks

Interface	Components	Description
S6a	Visited MME to home HSS	Required to authenticate users when roaming on commercial networks. Uses Diameter protocol.
S8	Visited S-GW to home P-GW	Required to allow users to connect back to PSBN networks and application networks when roaming.
S9	Visited PCRF to home PCRF	Required for local breakout scenarios and where dynamic charging & QoS policies are implemented between the HPLMN and VPLMN

4.2.3 Trusted and Un-Trusted Wireless Networks

The PSBN should support the use of trusted and un-trusted wireless networks. These can be used to quickly extend the coverage or improve the capacity of the PSBN when needed. This interworking requires that the end-user devices support a USIM card.

Some approaches currently under development may be considered for the bridging of cellular networks to WLANs technologies. The following list is not meant to be an exhaustive list. Other solutions may also exist.

- Hotspot 2.0 is a WiFiAlliance program (i.e. not 3GPP) that provides network discovery, authentication, and roaming. It is not yet fully integrated into 3GPP.
- IWLAN (Integrated/Interworked WLAN) is a 3GPP standard for Cellular-WiFi Integration on UMTS network (i.e. not LTE/EPC) which addresses:
    - Scenario 1: Common Billing and Customer Care (TS 23.234)
    - Scenario 2: 3GPP system based Access Control and Charging (TS 23.234)
    - Scenario 3: Access to 3GPP system PS based services
    - Scenario 4: Service Continuity (TS 23.327 & TS 23.261)
    - Scenario 5: Seamless services (TS 23.327 & TS 23.261)
    - Scenario 6: Access to 3GPP CS Services (work in progress)

- The more recent EPC 3GPP standards adds the following capabilities (TS 23.401 and TS 23.402)
    - Policy and QoS management entities in the core network.
    - Dynamic management & switching of individual IP-Flows from one radio interface to another based on QoS requirements, user subscription, and equipment type (TS 23.261 via DSMIP).
    - Support for trusted and un-trusted networks.
    - Introduction of the Access Network Discovery and Selection Function (ANDSF) server that provides operator policies regarding discovery and selection of Wi-Fi access (TS 24.302 and TS 24.312).

The following two 3GPP off-loading standards are not considered here since they entail potential mobility limitations, legal intercept constraints, and charging issues

- Selected IP Traffic Offload (SIPTO) : bypasses the mobile core network for traffic destined to the internet
- Local IP Access (LIPA) : bypasses the mobile core network for traffic destined to a local IP Network

The following tables list the components and interfaces involved in the connection to trusted and un-trusted non-3GPP networks:

Table 4-7: Components to Support Trusted and Un-Trusted Wireless Networks

Component	Name	Description
ePDG	Evolved Packet Data Gateway	The main function of the ePDG is to secure the data transmission with a UE connected to the EPC over an un-trusted non-3GPP access. For this purpose, the ePDG acts as a termination node of IPsec tunnels established with the UE.
3GPP AAA Server	3GPP Authentication, Authorization, and Accounting Server	An AAA server is a server program that handles user requests for access to computer resources and provides authentication, authorization, and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information.
ANDSF	Access Network Discovery and Selection Function	Contains data management and control functionality necessary to provide network discovery and selection assistance data as per operators' policy. The ANDSF responds to UE requests for access network discovery information (pull mode operation) and may be able to initiate data transfer to the UE (push mode operation), based on network triggers or as a result of previous communication with the UE.

Table 4-8: Interfaces to Support Trusted and Un-Trusted Wireless Networks

Interface	Description
S2a	Provides the user plane with related control and mobility support between trusted non 3GPP IP access and the Gateway.
S2b	Provides the user plane with related control and mobility support between ePDG and the Gateway.
S2c	Provides the user plane with related control and mobility support between UE and the Gateway. This reference point is implemented over 3GPP access and trusted and un-trusted non-3GPP access. The S2c interface is based on the Dual-Stack Mobile IP Version 6 (DSMIPv6) protocol and requires user equipment to support it.
S6b	Reference point between PDN Gateway and 3GPP AAA server/proxy for mobility related authentication if needed. This reference point may also be used to retrieve and request storage of mobility parameters and to retrieve static UE QoS profiles for non-3GPP access in case dynamic Policy and Charging Control is not supported.
Gx	Provides transfer of QoS policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the P-GW.
Gxa	Provides transfer of QoS policy information from PCRF to trusted non-3GPP accesses.
Gxc	Provides transfer of QoS policy information from PCRF to the S-GW.
SWa	Connects the un-trusted non-3GPP IP access with the 3GPP AAA Server/Proxy and transports access authentication, authorization and charging-related information in a secure manner.

Interface	Description
STa	Connects the trusted non-3GPP IP access with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters and charging-related information in a secure manner.
SWm	Reference point located between 3GPP AAA Server/Proxy and ePDG used for AAA signalling such as transport of mobility parameters, tunnel authentication and authorization data. This reference point also includes the MAG-AAA interface functionality and Mobile IPv6 NAS-AAA interface functionality.
SWn	Reference point between the un-trusted Non-3GPP IP access and the ePDG. Traffic on this interface for a UE-initiated tunnel has to be forced towards ePDG. This reference point has the same functionality as Wn which is defined in TS 23.234.
SWu	Reference point between the UE and the ePDG and supports handling of IPSec tunnels. The functionality of SWu includes UE-initiated tunnel establishment, user data packet transmission within the IPSec tunnel, tear down of the tunnel and support for fast update of IPSec tunnels during handover between two un-trusted non-3GPP IP accesses.
SWx	Reference point located between 3GPP AAA Server and HSS and used for transport of authentication, subscription and PDN connection related data.
S14	Reference point between UE and Home ANDSF or Visited ANDSF for direct queries via pull. It enables dynamic provision of information to the UE for access discovery and selection procedures related to 3GPP and non-3GPP accesses. This dynamic provision is supported with Pull (UE-initiated session) and with Push (ANDSF-initiated session), if feasible. Communication over S14 is secured as specified in TS 33.402.

4.2.4 Public Warning System

An Emergency Population Warning Systems (EPWS) is the vehicle by which local, regional or national authorities can warn the public of an impending emergency and they usually differ between countries. Furthermore, the dissemination of emergency warning notifications over wireless fabrics requires a Wireless Public Alerting System (WPAS) which bridges the EPWS and wireless telecommunication networks. The PSBN will need to interface with a Canadian WPAS to enable Public Safety users to receive emergency warning notifications on their user devices. In the context of LTE, the Public Warning System (PWS) is the mechanism by which warning notifications are distributed to end-user. As a result, the PSBN will also require PWS functionality.

The United States, for example, have integrated several systems under a single multi-agency EPWS termed the Integrated Public Alert and Warning System (IPAWS) which is overseen by FEMA. They have also implemented the WPAS that interfaces with IPAWS to deliver warning messages to the public over various wireless mobile fabrics. This system is referred to as the Commercial Mobile Alert System (CMAS). In Canada, the closest equivalent to a national EPWS solution is the National Alert Aggregation & Dissemination (NAAD) system owned and operated by Pelmorex Communication Inc. While Canada does not currently have a WPAS solution that interfaces with Pelmorex's NAAD, it is expected that such a system will become available in the future and indeed studies (Wireless Public Alerting and Dissemination project) are currently in progress through the Canadian Safety and Security Program (CSSP).

Since wireless public alerting systems differ between countries, PWS supports several WPAS which utilize a common architecture and signaling procedures. The supported WPAS in LTE are presented in the table below.

Table 4-9: Supported WPAS in LTE

WPAS	Region	PWS Support
ETWS	Japan	Rel. 8
CMAS	USA	Rel. 9
KPAS	South Korea	Rel. 10
EU-ALERT	European Countries	Rel. 11

PWS distributes warning messages using one of the logical control channels, the Broadcast Control Channel (BCCH). While utilizing the BCCH ensures both a timely and efficient delivery mechanism, it also imposes a restriction as to warning messages content and size. In CMAS for example, emergency warning notifications are restricted to 90 character text messages.

It is important to remember that while PWS functionality is achieved by using subcomponents of the Cell Broadcast Service (CBS), this does not enable cell broadcast functionality in the LTE network. PWS can only be used to broadcast emergency warning notifications. Furthermore, PWS-enabled UEs are required in order to receive and properly display emergency warning notifications. A few key components are required to enable PWS functionality in LTE and thus in the PSBN. They are listed and briefly described in the Table 4-10 below. The PWS interfaces are subsequently listed and described in Table 4-11.

Table 4-10: Public Warning System Components

Component	Name	Description
CBC	Cell Broadcast Centre	Responsible for the management of warning messages and initiates the broadcast by sending the warning message to the MME.
CBE	Cell Broadcast Entity	The functionality of the CBE is outside of the scope of 3GPP specifications; however it is assumed that the CBE is responsible for all aspects of formatting PWS warning messages.

Table 4-11: Interfaces to Support Public Warning System

Interface	Description
SBc	Interface between MME and CBC. SBc is used for the delivery of warning messages and control information signaling.
Unnamed #1	Interface between CBE and CBC. Like the CBE, its definition is out of the scope of 3GPP specifications.

Figure 4-3 illustrates an example where an RSDE uses PWS components (highlighted in yellow).

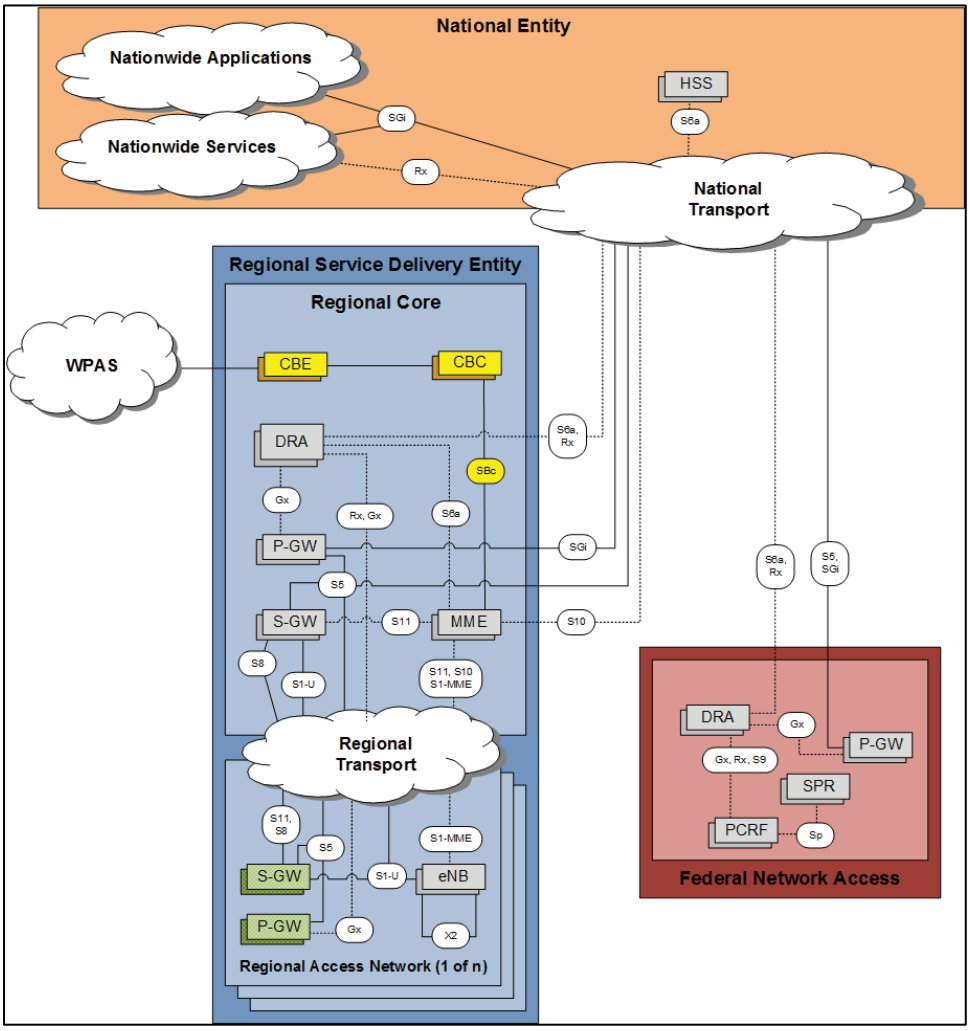

Figure 4-3: PWS Block Diagram

4.2.5 Lawful Intercept System

The PSBN may have to provide lawful intercept capabilities depending on national or regional policies and regulations. In such cases, it will need to interface with various law enforcement agency networks in order to securely receive intercept commands and to relay intercept records and data as per 3GPP TS 33.107.

In essence, lawful interception consists of intercepting IP layer data from the user plane and control plane. User data is referred to as the Content of Communication (CC), while the control plane information is referred to as the Intercept Related Information (IRI).

Figure 4-4 illustrates how lawful interception can be implemented in the PSBN. This example shows the Administration Function (ADMF) within the National Entity. This provides a single administration point for law enforcement agencies to submit their lawful intercept requirements.

The ADMF then coordinates with national and regional delivery functions in order to deliver the proper intercept records to the appropriate agency.

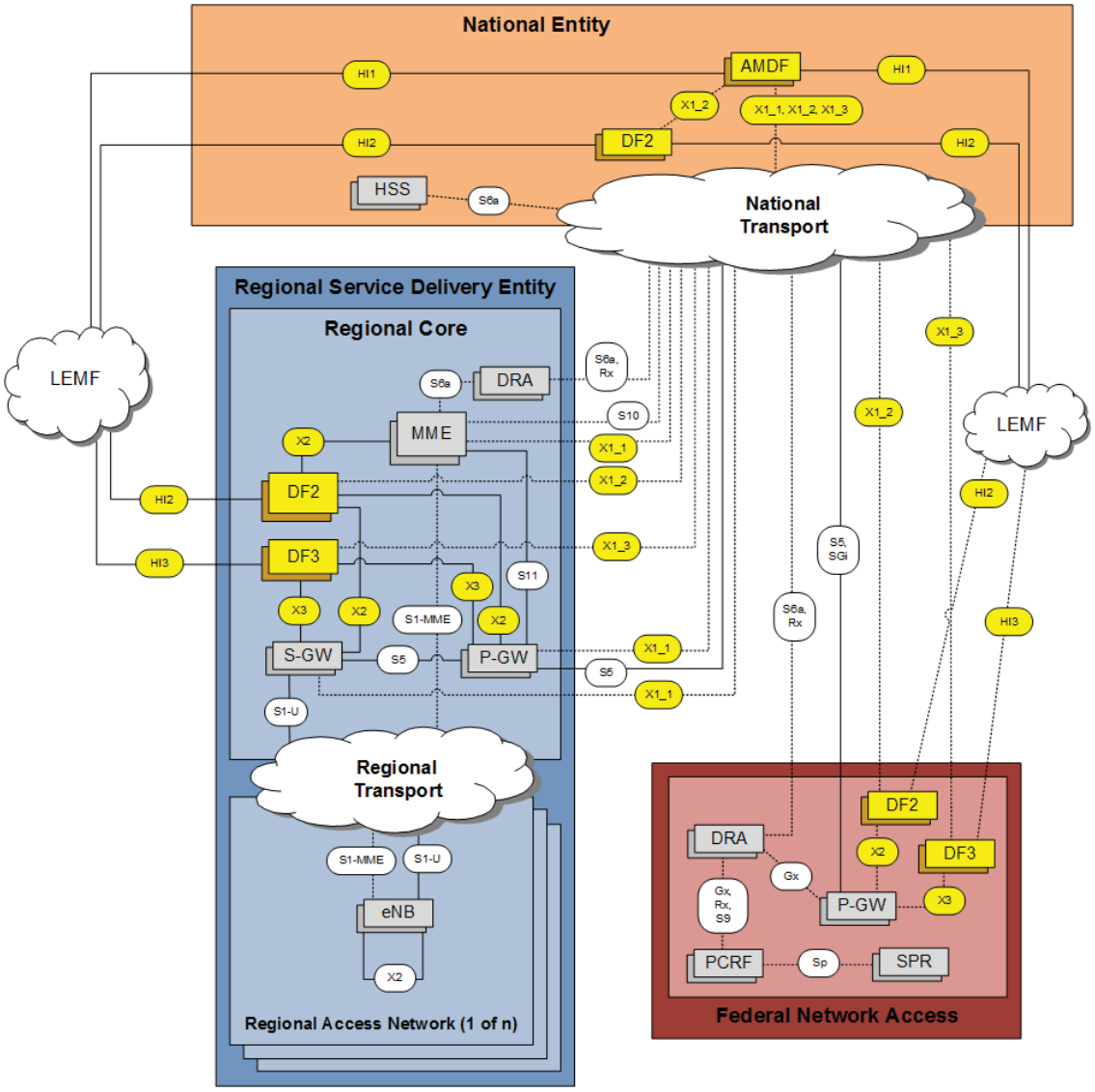

Figure 4-4: Lawful Intercept Block Diagram

Alternatively, it may also be possible for RSDEs to each have their own ADMF. However, law enforcement agencies would then have to send their lawful intercept requirements to multiple ADMFs in order to capture data from the HSS and from core components from potentially different regions.

Table 4-12 and Table 4-13 list and describe the lawful intercept components and interfaces respectively.

Table 4-12: Lawful Intercept System Components

Component	Name	Description
LEMF	Law Enforcement Monitoring Facility	Monitoring facility of law enforcement agency that needs to intercept data from the network. The PSBN could interface with multiple LEMFs.
ADMF	Administrative Function	Interfaces with law enforcement agencies and keeps intercept activities of individual agencies separate. Hides that there may be multiple activations by different agencies on the same target.
DF2	Delivery Function 2	Delivers Intercept Related Information (IRI) to law enforcement agency.
DF3	Delivery Function 3	Delivers Content of Communication to law enforcement agency. Also responsible for call control (signaling) and bearer transport for the Content of Communication.

Table 4-13: Interfaces to Support Lawful Intercept

Interface	Description
HI1	Interface between LEMF and ADMF. Used by LEMF to initiate a lawful intercept for a particular target in an area of interest.
HI2	Interface between LEMF and DF2. Used to distribute Intercept Related Information to the relevant law enforcement agency.
HI3	Interface between LEMF and DF3. Used to deliver Content of Communication to the relevant law enforcement agency. Also handles the signaling and bearer transport for the Content of Communication.
X1_1	Interface between the ADMF and the intercept control element (i.e. HSS, MME, S-GW, P-GW). Delivers target identities (i.e. IMSI), information on whether Content of Communication needs to be provided, address of DF2, address of DF3, and interface areas in case of location dependent interception.
X1_2	Interface between the ADMF and DF2. Delivers target identity, address for delivery of Intercept Related Information (e.g. LEMF address), subset of information to send, warrant reference number, intercept areas in case of location dependent interception.
X1_3	Interface between the ADMF and DF3. Delivers target identity, address for delivery of Content of Communication (e.g. LEMF address), warrant reference number, intercept areas in case of location dependent interception.
X2	Interface between intercept control element and DF2. Delivers Intercept Related Information.
X3	Interface between intercept control element and DF3. Delivers Content of Communication.

4.2.6 Next Generation 9-1-1

Next Generation 911 (NG9-1-1) is intended to replace the existing narrowband, circuit switched 9-1-1 networks with a system supporting seamless, end-to-end IP-based communication of emergency-related voice, text, data, photos, and video between the public and Public Safety Answering Points (PSAP). NG9-1-1 requires the implementation of Emergency Services IP networks (ESInets), which provide interconnectivity and interworking between originating wireless networks and PSAPs. The ESInet is intended to be a nationwide network-of-networks that interconnects local and regional PSAP networks.

The National Emergency Number Association (NENA) created the i3 set of requirement and architecture documents which define Session Initiation Protocol (SIP) based interfaces to interact with the NG9-1-1 system. The scope includes gateways for legacy wireline and wireless networks that are used to initiate emergency calls and which do not create call signaling matching the interfaces defined for the ESInet.

The 3GPP standards body also published a specification on IMS emergency sessions (TS 23.167) which introduces an additional role in the IMS architecture called Emergency Call Session Control Function (E-CSCF), along with reference points to connect to PSAPs via IP or traditional PSTN links. This concept is illustrated generically in Figure 4-5 where the PSBN's data (P-GW) and voice (IMS) domains are connected to the NG9-1-1 network via a gateway.

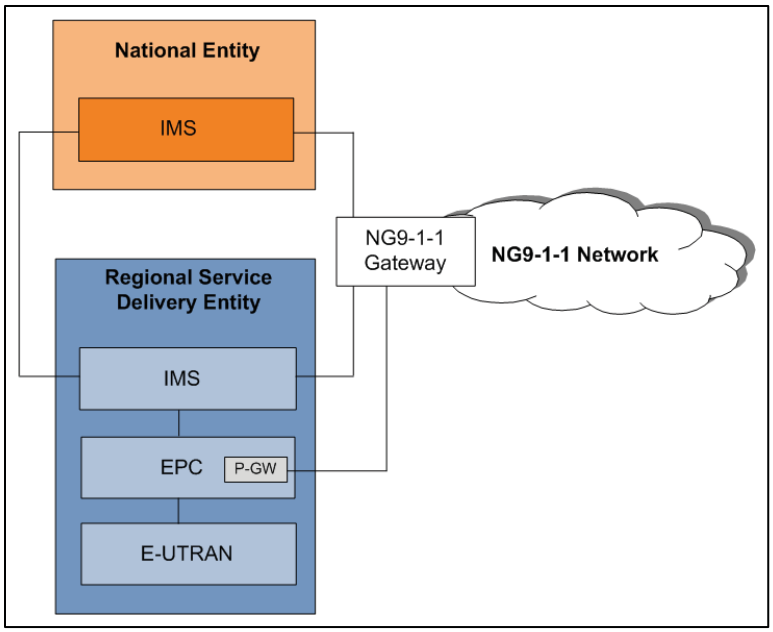

Figure 4-5: PSBN and NG9-1-1 Interconnection

4.2.7 LMR

Many End User Agencies currently rely on Land Mobile Radio or other narrow band technologies to provide mission critical voice and data communications to their users. Many of these systems are still being deployed and expanded and will remain operational for at least 10-15 years, while

others are due for replacement in 3-8 years.[9] Moreover, the PSBN is not expected to provide mission critical voice services until the capabilities become implemented in a manner which is endorsed by public safety operational authorities.

In light of the above, it is expected that End User Agencies will use a mixture of both LMR and PSBN for the foreseeable future. LMR will provide mission critical voice while the PSBN will provide non-mission critical data and voice. Since both systems will be in use, RSDEs may be able to bridge both systems together such that a PSBN user can connect to an LMR user and vice versa for non-mission critical voice and data.

Figure 4-6 illustrates a high level illustration of this concept. The premise is to use an LMR gateway that connects LMR data to a particular P-GW and also connects LMR voice services to the PSBN IMS system.

Interconnecting both systems may be challenging however, since the various narrow band technologies in use today are not all interoperable.

As there are currently no 3GPP standards that cover the interface between P25 and LTE, and TETRA and LTE, no standard interfaces can be presented in this section, at this point in time. However, 3GPP has recently accepted a proposal from PSRC (via ATIS) and European Critical Communications (TETRA) organization to add direct-mode communications to LTE (will appear in Release #12).

[9] General Architecture Considerations for GCSE LTE Work, TCCA CCBG SA

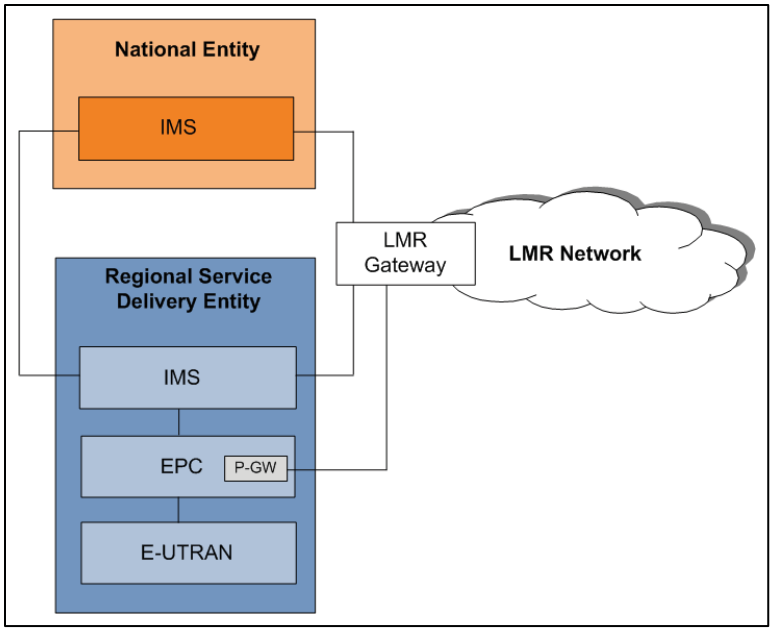

Figure 4-6: PSBN and LMR Interconnection

4.3 Fixed Remote Deployments

The PSBN may be deployed in remote or rural areas to provide a fixed long-term coverage to an otherwise isolated area. These areas may not have a fixed backhaul link and may instead have to rely on a satellite link or some other remote communications technology to connect back to National Entity, RSDE, or Agency components. It is assumed that this connection is relatively compromised, and has increased latency and lower data rate than urban-deployed backhaul infrastructure. It may also have a higher Packet Loss Rate (PLR).

More specifically, satellite connections generally have extra security encryption and access control layer provided, due to the open nature of satellite downlink transmissions. The effect of latency on interfaces and protocols must also be considered. In particular, the solution of using link accelerators to mitigate bandwidth-delay product protocol performance problems over satellite may not be fully functional over a satellite unless outer link acceleration architecture is used.

In situations where the PSBN is deployed in an isolated community, the following interfaces may be required to travel over satellite connections or other remote communications technology.

Table 4-14: Fixed Remote Deployments: Interfaces over Satellite and other Remote Access Technologies

Interface	Description
S2a	Proxy Mobile IP interface to and from remote trusted non-3GPP systems via remote field P-GW.

Interface	Description
S2b	Interface to and from the RSDE ePDG and remote field P-GW for un-trusted access to remote field network from PSBN.
S2c	Dual-Stack Mobile IPv6 (DS-MIPv6) interface to and from remote trusted non-3GPP systems via remote field P-GW.
S5	Data interface for S-GW to RSDE, National Entity, or End User Agency interface. Uses GTP or DS-MIPv6 protocol.
S6a	Signalling interface between HSS and remote field MME.
S8	Data interface for roaming. Equivalent to S5 for remote network as H-PLMN or V-PLMN.
S9	Signalling interface for roaming communication between remote network PCRF and PLMNs external to PSBN.
S10	Signalling interface to support handoffs between MMEs in multiple remote deploy or remote-fill situations.
SWu	Data interface for IPSec-secured communications between remote field un-trusted networks (to ePDG within the RSDE or from RSDE, National Entity, or End User Agency un-trusted networks to remote field network (via remote field ePDG).
Gx	Signalling interface for QoS configuration from remote field PCRF to RSDE, National Entity, or End User Agency P-GWs, and from RSDE PCRFs to remote field P-GW.
Rx	Signalling interface for QoS requests from PSBN applications to remote field PCRF, and from remote field applications to RSDE PCRFs.

Figure 4-7 illustrates a network architecture for a fixed remote implementation of the PSBN. The network architecture assumes a high-performance satellite connection is available, which could be substituted by fibre-optic or high-performance microwave backhaul. All authentication services (HSS/PCRF) are supplied by the National Entity with corresponding interfaces and protocols traversing the satellite/remote link.

As depicted in the figure, network operators may opt to deploy certain core elements (highlighted in green) in the remote area to minimize backhaul traffic. In this example, a local MME is used to avoid the use of S1-MME over the remote satellite link, due to expected performance problems with high-latency and potentially high packet-loss links. The X2 interface and multiple eNBs are presented as a solution, to allow for larger coverage areas in complex terrains when required.

Also shown are two potentially independent components that provide access to trusted and un-trusted data or services. The ePDG allows for an IPSec-based (SWu) interface between authenticated clients and services on the un-trusted network and the PSBN. This allows non-LTE wireless clients to be connected at the trusted and un-trusted levels.

In some very small community cases, the number of users in the area may not be significant. In these cases, small, localized, "EPC in a Box" solutions, consisting of a single hardware platform providing all core network functions, may be appropriate. However, the majority of small Canadian communities have complex topographies and will require LTE deployments that are

capable of providing for multiple eNBs, with corresponding RAN functionalities. Furthermore, even an "EPC in a Box" must provide for all the required 3GPP external interfaces to allow it to fully communicate with the PSBN Core and thus provide full inter-agency interoperability. These solutions are typically offered as low-footprint/transportable form factors suitable for rapid deployment.

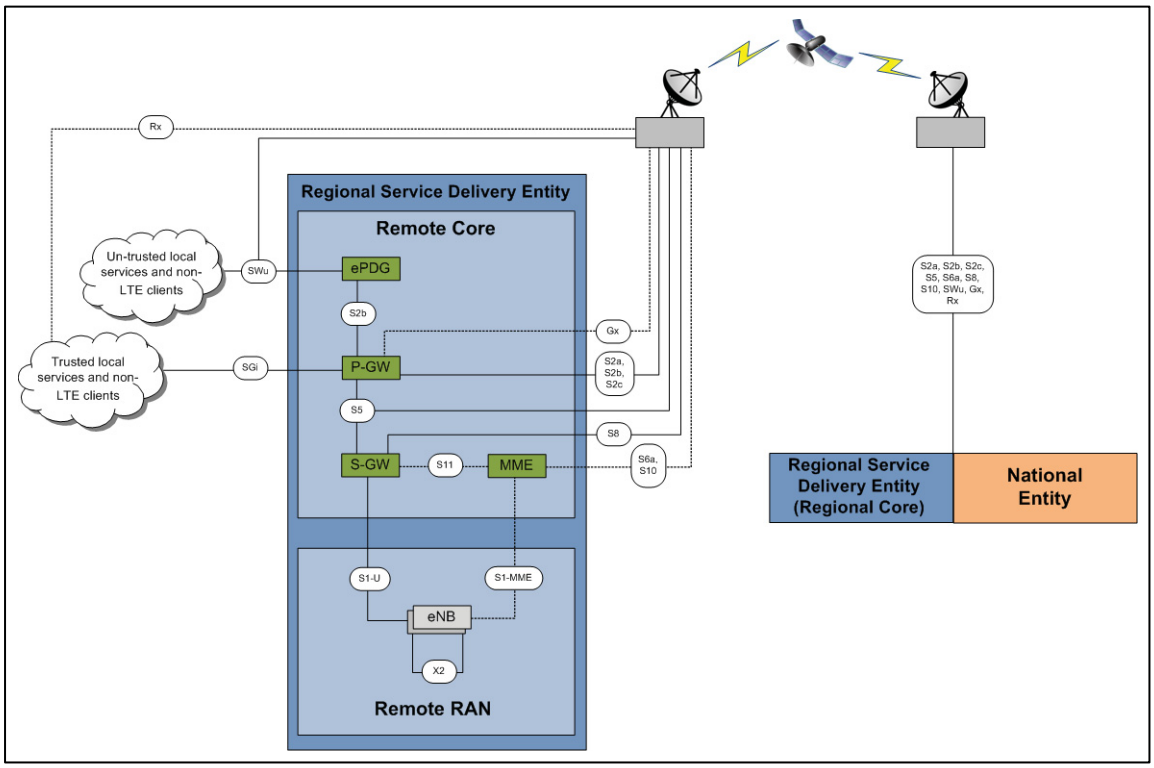

Figure 4-7: Fixed Remote Deployment Block Diagram

In this example, it is expected that encryption will be performed immediately before and after satellite communication, after which traffic passes through link acceleration hardware, allowing the encryption to be transparent to the link accelerators. This will generally not provide acceleration for the SWu interface, which is already IPSec encrypted, thus impacting performance of this interface in the field for communication over the satellite / remote field link. Communication via SWu within the remote field is not impacted, as this flows via the ePDG to and from the P-GW. In the case of SWu over satellite, it is possible, in some cases, to tune the network stack performance of clients and servers to reduce impact and/or to consider using special network protocols designed for space-segment communications (such as SCPS-TP[10] or the DTN Bundle Protocol[11]) when possible.

[10] Space Communications Protocol Specification – Transport Protocol, http://public.ccsds.org/publications/archive/714x0b2.pdf
[11] Bundle Protocol Specification, http://tools.ietf.org/html/rfc5050

4.4 Rapidly Deployable Networks

During an emergency, initial response teams may need to establish a quick means of communication in areas where the PSBN is either not available or does not provide the minimum communication requirements. In such cases, rapidly deployable network solutions such as "Cells on Wheels" or "Backpack Cells" may be deployed by any Public Safety Agency, acting under the authorization and according to the rules and regulations of the Regional Service Delivery Entity. Again, it is important that these solutions expose all required 3GPP external interfaces to allow full interoperable operations via the PSBN Core.

Although deploying these solutions may improve local communications, special care should be taken to ensure that the rapidly deployed network does not impact or disrupt other nearby PSBN cells.

Figure 4-8 illustrates a rapidly deployable network that can be deployed to provide a quick communication platform for first responders. Core components highlighted in green are optional and would normally be self-contained in a portable, rugged frame. They can be included depending on the nature of the emergency and the communication requirements to provide better services to local first responders. In this example, the deployed network provides full, localized data services, alternate localized communication technologies, and 700 MHz UE access. It is assumed that there is a high-capacity backhaul link to the regional core and the National Entity such that users can still be authorized by the National Entity HSS.

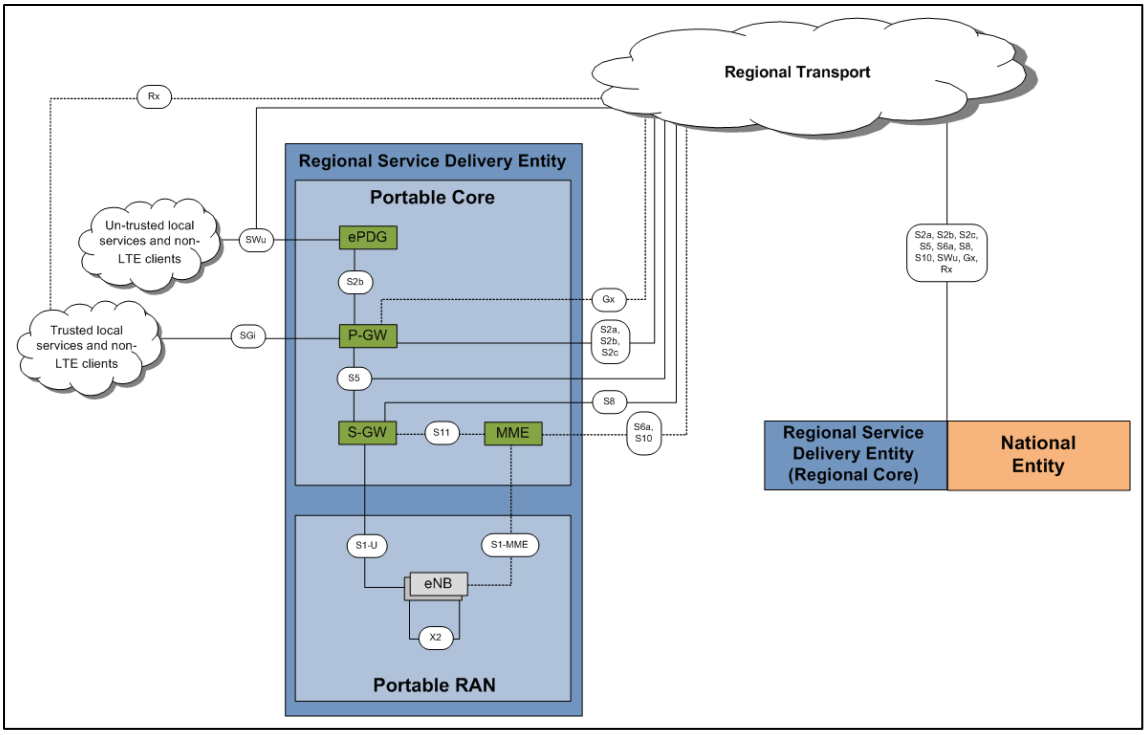

Figure 4-8: Rapidly Deployable Network

In situations where a backhaul link is not available and where it is not possible to authorize users with the National Entity HSS, it may be necessary to use a local HSS and PCRF as shown in Figure 4-9. The deployed network can thus operate in a fully self-contained fashion. The HSS and PCRF components allow other deployed components to operate without an external remote connection. This HSS may contain a replica or subset of the National Entity's user credential database or may be temporarily left blank to allow for immediate communication requirements (e.g. while a remote connection to the National Entity's HSS is being setup). The un-trusted network may be located on un-secured local communication links away from other deployed components, with protection provided via the ePDG.

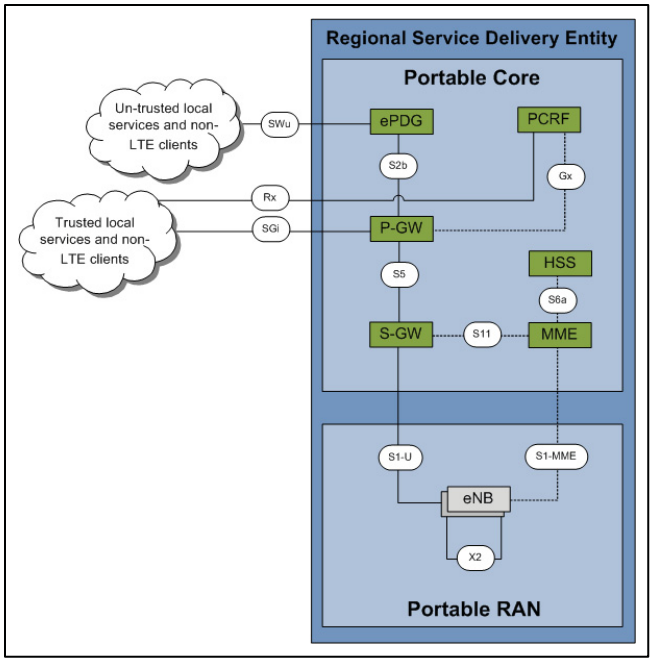

Figure 4-9: Rapidly Deployable Network without Backhaul Link

If a communication link back to the regional core and National Entity becomes available at a later point (through satellite or other remote communication systems), the local HSS and PCRF may be disabled if necessary and if this does not impact local communication.

4.5 Spectrum Sharing

If permissible by Industry Canada, the National Entity and the RSDEs may form partnerships with commercial carriers to deploy, maintain, and operate parts of the PSBN. In such agreements, public safety entities may allow the commercial partner to use some, or all, of their 20 MHz public safety band when the band is not in use or in low use. In return, the commercial partner allows the public safety entity to leverage some of the carrier's equipment, network or services. Different types of partnerships are possible and will depend entirely on the needs of the public safety entity and the level of service that the commercial partner can provide.

Regardless of the agreements put in place, these public private partnerships are required to abide by the policies and regulations of the PSBN. For example, public safety users from other regions must still be able to connect to a region served by a commercial partnership. QoS and latency requirements must also be met.

Figure 4-10 illustrates one example where an RSDE partners with a commercial carrier to provide coverage in their region.

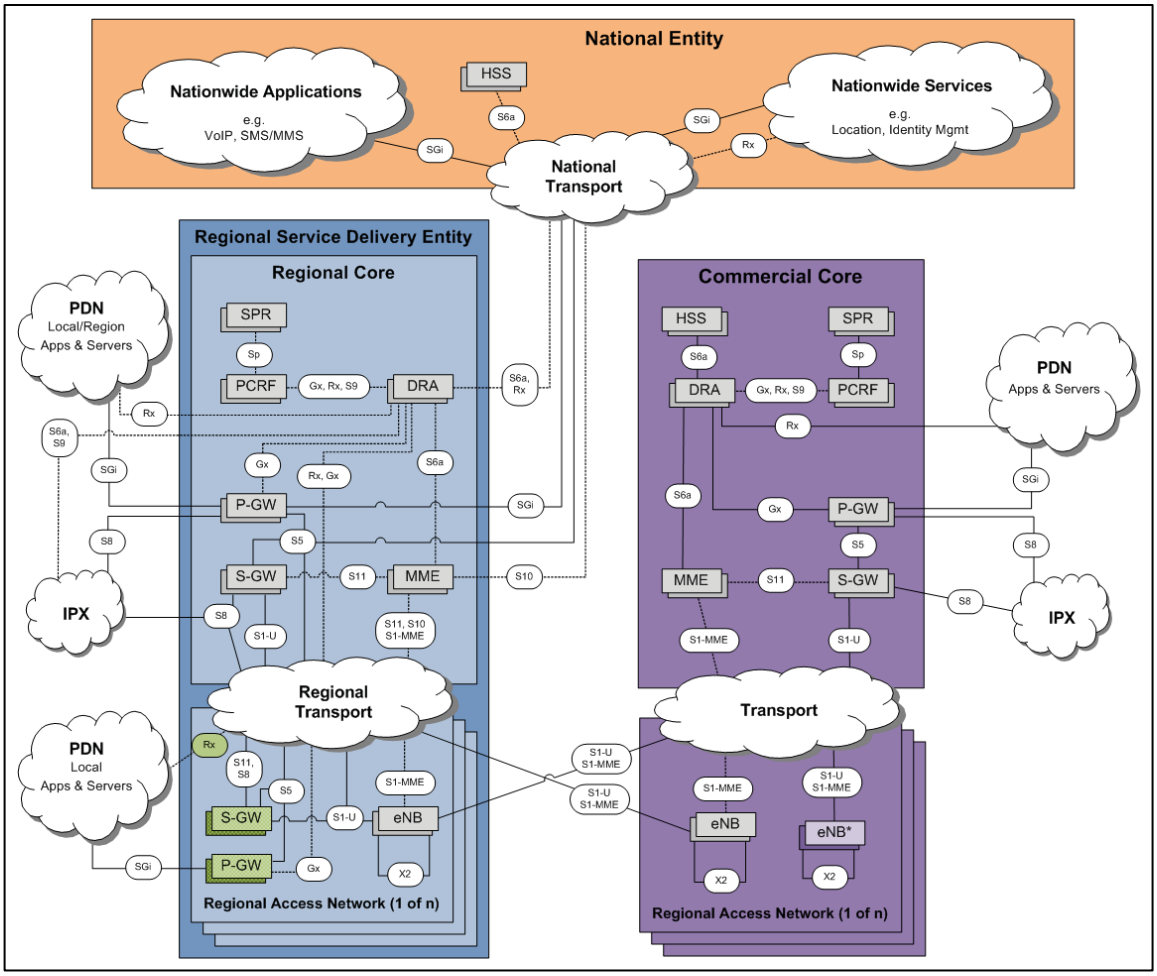

Figure 4-10: Example of Spectrum Sharing

5. Conclusion

The network architecture of the PSBN has been derived from the efforts of the Infrastructure Work Group – one of three technical work groups that were launched by the Centre for Security Science between July and August 2012 under the Technology Track which supports the 700 MHz Project Management Team.

The network architecture is driven by a number of fundamental considerations. The topmost considerations are (i) the governance model – a network of federated regional networks, and (ii) the service delivery model involving a national operating entity, regional service delivery entities, and end-user agencies and (iii) technology.

Operational considerations also influenced the network architecture. The principal ones are:

- Local administrative oversight of user access privileges,
- Local ownership of information networks and applications servers,
- Priority and QoS management during periods of peak demand,
- Avoiding proprietary or non-standardized technologies,
- Serving rural and remote areas,
- Roaming with commercial carriers and FirstNet,
- Access to any information network, as authorized, from any location on the nationwide footprint of the PSBN and from that of roaming partner networks,
- Ability to originate and terminate interactive voice sessions and send/receive multimedia messages with any other PSBN user and with anyone outside the PSBN network that is publicly addressable.

The PSBN network architecture has the following attributes and features:

- Based on 3GPP LTE Rel.10 or later. Other technologies are used as required to complement LTE.
- Minimum number of interfaces between the National Entity and the RSDE simplifies technical interoperability.
- Flexible configuration of deployable systems allows independent operation or operating with high-latency, high error-rate, low bandwidth connections to the PSBN.
- Incident-level data traffic is kept as localized as possible to minimize loading on national and regional backhaul networks.

The network architecture is designed to interface with the following external networks.

- Commercial carrier networks through roaming agreements,
- FirstNet through a roaming agreement,

- Next Generation 9-1-1 systems,
- The public Internet,
- Private data networks,
- Land Mobile Radio systems,
- Alternative access networks such as WiFi – both trusted and un-trusted hotspots,
- Public Warning System,
- Lawful Intercept system,
- Public Switched Telephone Network.

The network architecture for the PSBN will likely evolve as the roles and responsibilities of the principal stakeholders are further defined and as action dictates from operational effectiveness reviews. The Pilot network, being the first instance of the implementation of the PSBN, is expected to reveal issues that impinge on the network architecture, which will also engender changes to the NAD. These changes will be captured in future updates to this document as new versions are appended.

The Canadian model for the PSBN is unique. All wireless broadband networks, as far as it is known, have a monolithic governance structure. Hence, there is no known equivalent network architecture that has been implemented as the one that is described in the NAD. The work group has benefitted from the expertise and experience of its members to achieve a singular accomplishment in providing the public safety community a network architecture that meets the challenges posed by the Canadian governance construct for the PSBN.

Bibliography

1. NPSTC, “Public Safety Broadband High Level Launch Statement of Requirements”, December 7, 2012
   http://www.npstc.org/download.jsp?tableId=37&column=217&id=2609&file=BBWG_SoR_Launch_12112012.pdf

2. US Department of Homeland Security – Office for Interoperability and Compatibility, “Public Safety Statement of Requirements for Communications and Interoperability”, Volume 1, version 1.2, October 2006
   http://www.safecomprogram.gov/library/Lists/Library/Attachments/302/Statement_of_Requirements_Volume_I%20-%20Version%201_2.pdf

3. U.S. Department of Justice - Community Oriented Policing Services (COPS), “National Forum on Public Safety Broadband Needs” August 23, 2010.
   http://www.cops.usdoj.gov/files/RIC/Publications/e021111338-broadband-forum.pdf

4. International Telecommunications Union, “Security architecture for systems providing end-to-end communications”, Recommendation X.805, 2004
   Summary: www.ietf.org/proceedings/63/slides/saag-3/saag-3.ppt

5. Federal Communications Commission, “Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band”, 3rd Order & Report and 4th Notice of Proposed Rulemaking FCC 11-6A1, January 26, 2011.
   http://www.fcc.gov/Daily_Releases/Daily_Business/2011/db0204/FCC-11-6A1.pdf

6. “Desirable Properties of a National Public Safety Network”, Draft Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology, Nov.21, 2011.
   http://www.nist.gov/director/vcat/upload/vcat-public-safety-subcommitte.pdf

7. “Canadian Public Safety Broadband Communications Network - Security Requirements”, v.P-01 DRAFT, Centre for Security Science – Defence Research and Development Canada, Government of Canada, 2013

8. “Canadian Public Safety Broadband Communications Network - Operational Requirements”, v.P-03 DRAFT, Centre for Security Science – Defence Research and Development Canada, Government of Canada, 2013.

9. Responses to NTIA’s “Notice of Inquiry on FirstNet Conceptual Network Architecture” Nov.2012.
   http://www.ntia.doc.gov/federal-register-notice/2012/comments-nationwide-interoperable-public-safety-broadband-network-noi

Definitions

Catastrophic failure: The inability of the PSBN to deliver the required communications services at or above a minimum level of acceptable quality due to failure of connectivity, equipment, software, or capability for which there is no working stand-by or automatic recovery. This may result from simultaneous failures of the main and redundant systems. Recovery from a catastrophic failure requires a manual intervention to repair the fault to a sufficient level that the capability is restored, even if initially it is without back-up.

First Responder: Those individuals who are responsible for the protection and preservation of life, property, evidence, and the environment, 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. Also includes federal, provincial, territorial, and local emergency public safety, law enforcement, emergency response, emergency medical, including hospital emergency, and related personnel, agencies, and authorities.

Geographic Areas: There are many ways to classify geographic areas. Geographic units can range from administrative units (municipality, counties, etc.) to detailed census subdivisions. One key unit often used in defining geographic areas is demographic data in terms of population total and/or density. Statistics Canada replaced the term 'urban' in 2011 by 'population centre' to define a geographic area with a total population of at least 1000 and a density no fewer than 400 people per square km . Population centres are further divided into three groups based on the total size of the population to reflect the existence of an urban-rural continuum:

- small population centres, with a total population between 1,000 and 29,999;
- medium population centres, with a total population between 30,000 and 99,999;
- large urban population centres, with a total population of 100,000 and over.

The term 'rural' is used to define all other geographic areas in Canada where the population total is less than 1000 and where the density is below 400 people / km2.

For the purpose of this document the above definitions are further augmented and defined by their respective physical environments (i.e. manmade structures, vegetation and physical geography, etc.). This categorization is created to better assess the feasibility of establishing terrestrial telecommunication services for each area. A total of four geographic areas are identified below. While a wide variety of physical environments may exist within each area, the intent is not to define every possible scenario but rather describe the physical environments considered to be the most typical.

- Urban: Urban areas are associated with population centres; Primarily characterized by high- to mid-rise developments i.e. tall and large buildings of several floors with

concrete, steel, and reflective glass construction; Deep underground parking garages; Possible road and subway tunnels; Heavy motor traffic; High density of users.

- Suburban: Typically existing as part of an urban area or as a separate community within commuting distance; Primarily characterized by mid- to low-rise developments interspersed with residential developments (single or double storey dwellings) of varying construction; Heavy to light foliage possible; Medium to light motor traffic; Medium to low density of users.
- Rural: Consisting of scattered small towns, villages or settlements typically located away from large population centres. Primarily characterized by dispersed developments (low-rise and residential) of varying construction; Physical geography features interact to make the establishment of terrestrial telecommunication services challenging such as medium to small expanse of territory which can be flat, hilly, or mountainous; Heavy to light foliage possible; Light motor traffic; Low density of users.
- Remote: Consisting of small settlements, mining camps and other industrial campuses which may be located several hundreds of kilometers away from any population centre; Characterized by dispersed developments of varying construction; Physical geography features interact to make access difficult by land and the establishment of terrestrial telecommunication services difficult such as large expanse of territory, large bodies of water, etc.; All types of foliage possible; Severe climatic conditions possible (e.g. desert or arctic conditions); motor traffic may be inexistent; Low density of users to un-populated areas.

Finally, the term 'isolated' will be used herein to describe a geographic area characterized by the absence of any terrestrial broadband telecommunication service. While any of the four areas described above could potentially qualify as isolated, in Canada rural and remote areas will most typically fall in the isolated category.

Incident Area Network: An Incident Area Network is a subset of the Regional network. Its boundaries are defined by the coverage area served by the PSBN base stations at an incident location.

Internet Packet Exchange (IPX): Developed by GSMA to foster open standardized IP connectivity for multiple types of service providers, it provides for end-to-end QoS in support of both roaming and interworking for LTE and IMS

Interoperability: Wireless communications interoperability refers to the ability of users to share information via voice and data applications – on demand, in real time, when needed, and as authorized[12]. The operational requirements address only the Technology lane of the Communications interoperability Continuum, as shown in Figure D1. Other measures are required to mature the capabilities in the other lanes.

[12] From Safecom definition of Interoperability. http://www.safecomprogram.gov/interoperability/Default.aspx

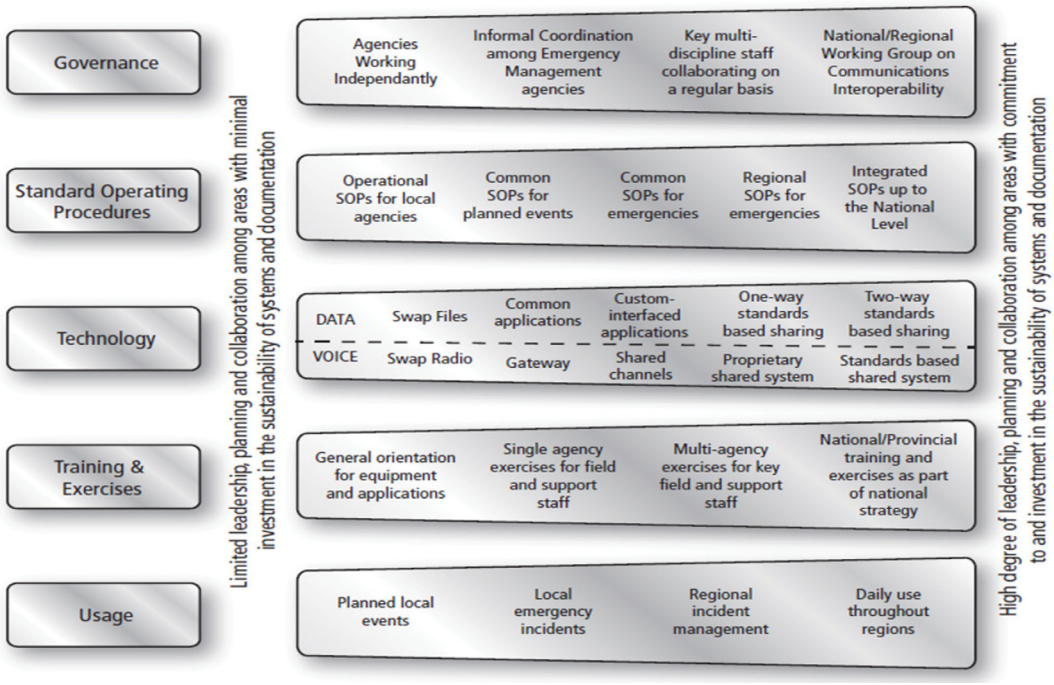

Figure D1: Communications Interoperability Continuum[13]

Mission-critical: Refers to a system, device, service, or activity whose failure or disruption will result in the immediate inability of a person or entity to fulfill its mission.

Network Administrator: The person(s) responsible for overseeing the set-up, operation, and maintenance of the PSBN. The network administrator interacts directly with the PSBN as an administrative user and has higher levels of authorized access to the PSBN. There may be a hierarchy of authorization levels within the network administration function. Network Administrators are members of the Network Operator's organization.

Network Operator, Regional Network Operator, National Network Operator: The Network Operator is the entity that is authorized to operate and administer the PSBN. If the architecture of the PSBN is one of regional federated networks, then there would be two tiers of network operators – a national-level operator and a number of regional network operators. This document does not attempt to define the demarcation of responsibilities between the two levels. If the architecture of the PSBN is a single national network then there is only the National Network Operator. If the PSBN is implemented as a public-private-partnership, then the Network Operator referred to in this document is the entity responsible for administering public safety's use of the PSBN, regardless of the network architecture.

Operational Requirements: Operational requirements represent the problem space of the requirements hierarchy as illustrated in the Transportation Safety Administration (TSA)

[13] Communications Interoperability Strategy for Canada http://www.publicsafety.gc.ca/prg/em/cisc-eng.aspx

example of Figure 12. The Technical requirements represent the solution space Typically, Operational Requirements are qualitative statements that describe a needed capability.

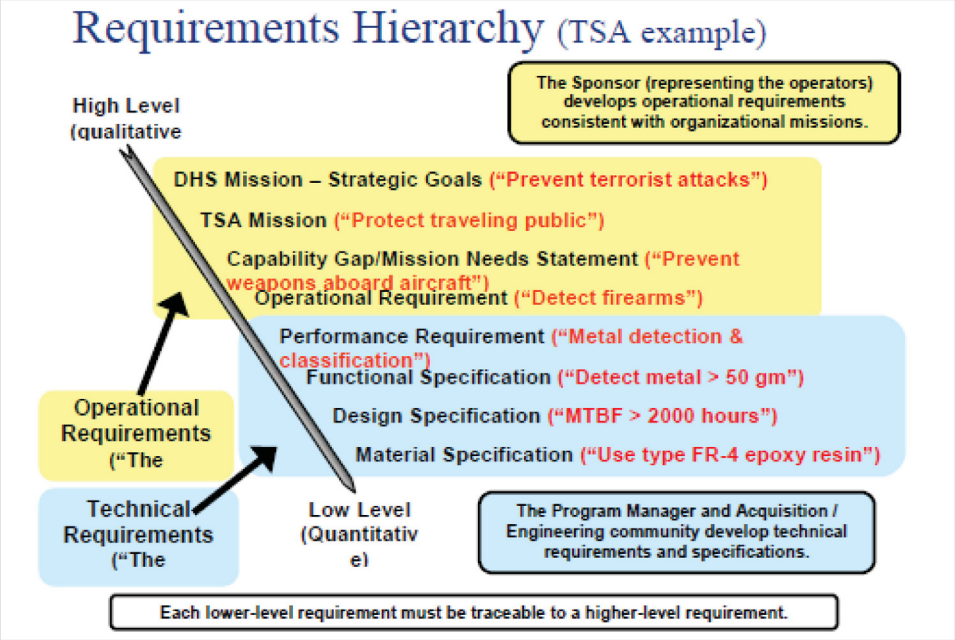

Figure 2:: The requirements hierarchy – TSA example [14]

Private Network: a communication network owned by one or more entities for their exclusive use.

Public Safety Broadband Network (PSBN): The physical and logical infrastructure that makes up the public safety broadband communications network. It is the collection of the regional and national components, physical facilities, applications, user equipment, and other devices.

Regional jurisdiction, Region, Jurisdiction: The three terms are used synonymously in this document. It can be a town, city, territory, province, or an agglomeration of these. In a Federated Regional Networks architecture, a Region is an administrative entity and operator of the regional broadband communications network. Administrative boundaries of the PSBN may or may not coincide with political or municipal boundaries.

Untrusted Network: any type of access network that neither is under control of the operator (public open hotspot, subscriber's home WLAN, etc.) nor does it provide sufficient security (authentication, encryption, etc.). Figure D3 provides a view of the ITU-T Security Trust Model showing Network Border Elements (NBE) and Terminal Equipment (TE) a of NGN provider across different security zones.

[14] US Department of Homeland Security, "Developing Operational Requirements – A Guide to the Cost-Effective and Efficient Communications of Needs", version 2.0, Nov. 2008. http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf

Trusted Network: any type of access network that either is under control of the operator (operator-managed small cells, etc.) or provides sufficient security (authentication, encryption, etc.). See Figure D3.

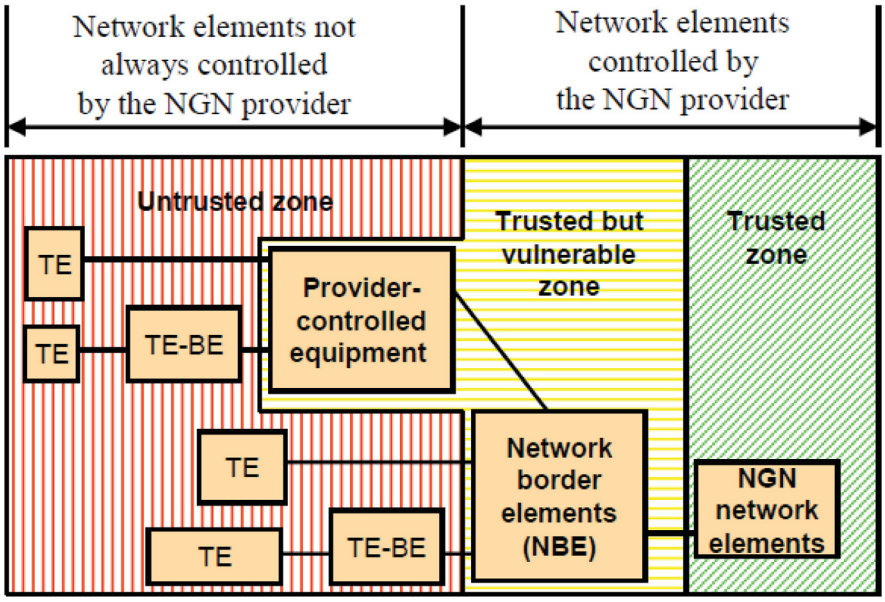

Figure D3: ITU-T Security Trust Model[15]

User: A user is a person or machine authorized to access the resources available on the PSBN and to communicate with other users on the network, or subscribers of other services globally. For the purposes of defining operational requirements, the broadest possible definition is used in this document. As of the time of this writing, Industry Canada has not declared who are the user categories that can be served by the PSBN. User definition will be updated when Industry Canada will announce who are eligible users. Hence, provisionally, the users are deemed to belong to the following user groups:

1. Front-line users

   a) Category 1 public safety agencies according to Industry Canada classification: Police, Fire, Emergency Medical Services; from municipal, provincial/territorial, and federal agencies.

   b) Industry Canada category 2: forestry, public works, public transit, dangerous chemical clean-up, customs, and other agencies contributing to public safety.

[15] ITU-T Y.2701 - Security requirements for NGN release 1

c) Industry Canada category 3: other government and certain NGO agencies or entities,

d) FirstNet subscribers when roaming into Canada.

e) Consumers: if permitted by Industry Canada and Regional Service Delivery Entities.

2. Back-office users

a) Network administrators: interface with the network; able to configure service-affecting and non-service-affecting parameters according to hierarchical levels of authorization.

b) Security officer: monitor usage; policies and procedures.

3. Operations support users

a) Field technicians with access to physical facilities: may or may not be authorized to perform service-impacting maintenance actions.

b) Network engineers: conduct performance evaluations and tests; take action related to expansion or optimization of the network; likely to impact service.

c) Value-Added Services (VAS) staff: bring new applications on-line.

4. Machines

a) Mobile access routers: gateway to dismounted officers' handheld devices, vehicle telemetry, dashboard cameras, license plate readers, vehicle-mounted computer.

b) Portable sensors: tactical optical and IR cameras, chemical sniffers, sound recording devices, Unattended Ground Sensors (UGS).

User Agency, End User Agency: An organization that represents users or employs users. Examples of User Agencies are (i) a municipal police service, (ii) a provincial ambulance service, or (iii) a federal entity such as Canadian Border Services Agency.

User Agency Administrator (UAA): A person responsible for administering the user profiles of the users within the jurisdiction of his/her user agency. The UAA can monitor the Key Performance Indicators (KPI) of the PSBN within prescribed limits. The UAA can also control some configurable parameters of the PSBN, such as Priority and Quality of Service, within prescribed limits. This will be discussed in the relevant sections of this document.

Visiting and Roaming users: When a user moves from one public safety jurisdiction of the PSBN into another public safety jurisdiction he/she is “visiting”. A user whose service is provided by a network other than the PSBN is deemed to be roaming. “Roaming” specifically refers to movement between networks with different PLMN IDs.

List of acronyms

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AC	Admission Control
ACL	Access Control List
ADMF	Administrative Function
AES	Advanced Encryption Standard
AMBR	Aggregate Maximum Bit Rate
AN	Access Network
ANDSF	Access Network Discovery and Selection Function
ANOC	Agency Network Operation Center
API	Application Programming Interface
APN	Access Point Name
ARP	Allocation and Retention Priority
AS	Access Stratum
ATP	Acceptance Test Procedure
ATIS	Alliance for Telecommunications Industry Solutions
BCCH	Broadcast Control Channel
BGCF	Breakout Gateway Control Function
BGP	Border Gateway Protocol
BM-SC	Broadcast/Multicast Service Center
BS	Base Station
BSS	Business Support System
CAD	Computer Aided Dispatch
CALEA	Communications Assistance for Law Enforcement Act
CBC	Cell Broadcast Centre
CBE	Cell Broadcast Entity
CC	Content of Communication
CDF	Charging Data Function
CDMA	Code Division Multiple Access
CDR	Call Detail Record
CGF	Charging Gateway Function
CGW	Charging Gateway
CIRTEC	Communication Interoperability Research Test and Evaluation Center
CM	Congestion Management
CMAS	Commercial Mobile Alert System
COLT	Cell On Light Truck
COPS	Community Oriented Policing Services
COW	Cell On Wheels
CPE	Customer Premise Equipment

CRC	Communications Research Centre
CSS	Centre for Security Science
CSSP	Canadian Safety and Security Program
CTIA	Cellular Telecommunications Industry Association
DA	Delegated Authority
DCH	Data Clearing House
DDoS	Distributed Denial of Service
DF2	Delivery Function 2
DF3	Delivery Function 3
DHS	Department of Homeland Security
DHS OEC	Department of Homeland and Security Office of Emergency Communications
DL	Downlink
DM	Device Management
DMZ	De-Militarized Zone
DNS	Domain Name Service
DNSSec	Domain Name Server Security
DOJ	Department Of Justice
DoS	Denial of Service
DRA	Diameter Routing Agent
DSMIP	Dual Stack MIP
DUT	Device Under Test
E911	Enhanced 9-1-1
EAP	Extensible Authentication Protocol
ECPC	Emergency Communications Preparedness Center
eHRPD	Enhanced High Rate Packet Data
eMBMS	Evolved Multimedia Broadcast Multicast Service
EMS	Emergency Medical Services
eNB	Evolved Node B
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
EPWS	Emergency Population Warning Systems
ERIC	Emergency Response Interoperability Center
ESF	Emergency Support Function
ESINet	Emergency Services IP NETwork
eTOM	enhanced Telecommunications Operations Map
ETS	Enabler Test Specifications
ETSI	European Telecommunications Standards Institute
EUA	End User Agency
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
E-UTRAN	Evolved Universal Terrestrial Radio Access
EvDO	Evolution Data Optimized

FCC	Federal Communications Commission
FCH	Financial Clearing House
FEMA	Federal Emergency Management Authority
FICAM	Federal, Credential, Identity and Access Management
FirstNet	First Responder Network Authority
FISMA	Federal Information Security Management Act
FMC	Fixed-Mobile Convergence
FOA	First Office Application
FTP	File Transfer Protocol
GBR	Guaranteed Bit Rate
GCF	Global Certification Forum
GCS	Ground Control Station
Gm	Gm interface provides support for SIP-related signaling with the UE
GoS	GoS Grade of Service
GPS	GPS Global Positioning System
GSA	General Services Administration
GSM	Groupe Service Mobile
GSMA	GSMA GSM Association
GW	Gateway
HE	Home Environment
HLR	Home Location Register
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
ICIC	ICIC Inter-Cell Interference Coordination
ICS	Incident Command System
I-CSCF	Interrogating Call Session Control Function
ID	Identifier
IDS	Intrusion Detection System
IMS	Incident Management System
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IOT	Interoperability Testing
IP	Internet Protocol
IPAWS	Intergraded Public Alert and Warning System
IPsec	Internet Protocol security
IPX	Internet Packet Exchange
IRI	Intercept Related Information
ISO	International Organisation for Standardisation
ITEF	Internet Engineering Task Force
ITEF	IT Information Technology
ITU	International Telecommunication Union
KPI	Key Performance Indicator

LBS	Location Based Services
LEMF	Law Enforcement Monitoring Facility
LIPA	Local IP Access
LMR	Land Mobile Radio
LOC	Location services
LTE	Long Term Evolution
MANET	Mobile Ad-hoc mesh NETwork
MBMS	Multimedia Broadcast Multicast Services
MBMS GW	MBMS Gateway
MBR	Maximum Bit Rate
MCE	Multi-cell/multicast Coordination Entity
MCS	Modulation and Coding Scheme
MCV	Mission Critical Voice
ME	Mobile Equipment
MGCF	Media Gateway Controller Function
MGW	Media Gateway
MIMO	Multiple Input Multiple Output
MIP	Mobile IP Protocol
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MOC	Mobile Originated Call
MOCN	Multi-Operator Core Network
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MSF	Multi Service Forum
MVPN	Mobile Virtual Private Network
NAAD	National Alert Aggregation & Dissemination
NAD	Network Architecture Description
NAS	Non Access Stratum
NAT	Network Address Translation
NB	Narrow Band
NCIC	National Crime Information Center
NDA	Non Disclosure Agreement
NENA	National Emergency Number Association
NFIRS	National Fire Incident Reporting System
NFPA	National Fire Protection Association
NG	Next Generation
NG 9-1-1	Next Generation 9-1-1
NGN-PS	Next Generation Network - Priority Services
NGO	Non-Government Organization
NGOSS	Next Generation Operating and Support System
NIEM	National Information Exchange Model

NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NLETS	National Law Enforcement Telecommunications System
NNOC	National Network Operation Center
NOC	Network Operations Center
NPSBN-U	Nationwide Public Safety Broadband Network User
NPSTC	National Public Safety Telecommunications Council
NRF	National Response Framework
NSPAN	Nationwide Public Safety Application Network
NSPBN	Nationwide Public Safety Broadband Network
NSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
NTP	Network Time Protocol
NVIOT	Network Vendors Interoperability Test Forum
O&M	Operations and Maintenance
OAM	Operations, Administration, and Maintenance
OAM&P	Operations, Administration, Maintenance, and Provisioning
OCS	Online Charging System
OEM	Original Equipment Manufacturer
OLA	Operational Level Agreement
OMA	Open Mobile Alliance
OMA-DM	Open Mobile Alliance - Device Management
OR	Operational Requirement
OS	Operating System
OSS	Operations Support System
OTA	Over The Air
PCRF	Policy Charging and Rules Function
PCS	Personal Communications System
P-CSCF	Proxy Call Session Control Function
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
P-GW	Packet Data Gateway
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PLR	Packet Loss Rate
PPP	Public Private Partnership
PS	Public Safety
PSA	Public Safety Agency
PSAC	Public Safety Advisory Committee
PSAN	Public Safety Application Network
PSAP	Public Safety Answering Point

PSBN	Public Safety Broadband Network
PSE	Public Safety Entity
PSEN	Public Safety Enterprise Network
PSG	Public Safety Grade
PSS OAC	Public Safety Spectrum Trust Operator's Advisory Council
PSST	Public Safety Spectrum Trust (USA)
PSTN	Public Switched Telephone Network
PTCRB	PCS Type Certification Review Board
PTT	Push To Talk
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RF	Radio Frequency
RFP	Request for Proposal
RNOC	Regional Network Operation Center
RRC	Radio Resource Control
RRM	Radio Resource Management
RSDE	Regional Service Delivery Entity
SAE	System Architecture Evolution
S-CSCF	Serving Call Session Control Function
SDF	Service Delivery Framework
SDM	Service Delivery Model
SDO	Standards Development Organization
SDP	Service Delivery Platform
SEG	Security Gateway
S-GW	Serving Gateway
SIEC	Statewide Interoperable Executive Committee
SIGB	Statewide Interoperability Governing Board
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIPTO	Selected IP Traffic Offload
SLA	Service Level Agreement
SMS	Short Message Service
SN	Serving Network
SOA	Service Oriented Architecture
SOP	Standard Operating Procedure
SOR	Statement Of Requirement
SPR	Subscriber Profile Repository
SRVCC	Single Radio Voice Call Continuity
SUPL	Secure User Plane Location
SWAT	Special Weapons and Training

TAG	Technology Advisory Group
TAP	Transfer Accounting Procedure
TAN	Technical Advisory Note (CSS product)
TBD	To Be Determined
TETRA	Terrestrial Trunked Radio (an ETSI standard)
TIA	Telecommunications Industry Association
TIR	Technical Interoperability Requirement
UASI	Urban Area Security Initiative
UC	Unified Command
UDC	User Data Convergence
UDR	User Data Repository
UE	User Equipment
UGS	Unattended Ground Sensors
UICC	Universal Integrated Chip Card
UL	Uplink
UMTS	Universal Mobile Telecommunications System
USAT	Universal Subscriber identity module Application Toolkit
USB	Universal Serial Bus
USB-IF	Universal Serial Bus – Implementers Forum
USIM	Universal Subscriber Identity Module
V-CDF	Visited Charging Data Function
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VoLTE	Voice over LTE
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network
VQiPS	Video Quality in Public Safety
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAS	Wireless Public Alerting System
WPS	Wireless Priority Service

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – CSS
222 Nepean St
Ottawa, Ontario K1A 0K2

2. 2a. SECURITY MARKING
(Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC JUNE 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Public Safety Broadband Network Architecture Description

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Pagotto, J.;Scribano, G.; Cayouette R.; Braham S.; Gurnick J.; Auger C.; Lafond E.; Fournier J.; Doumi T.; Lucente C.; Dixon M.,

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
August 2013	88	16

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – CSS
222 Nepean St
Ottawa, Ontario K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
PSTP 3782-2011-33br00-03	
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS TR 2013-009	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unclassified/Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable
that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification
of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include
here abstracts in both official languages unless the text is bilingual.)

WHAT PUBLIC SAFETY NEEDS IN AN EMERGENCY IS…
A public safety-controlled network with the ability to efficiently access and share accurate and timely voice and information during all stages of an event in any geographic location with the appropriate resources, interoperability, robust and reliable capacity, based upon the needs of the responders, and with the ability to dynamically scale to changes in the situation. [16]

This document describes the network architecture for a Canadian public safety broadband communications network expected to operate in the 700 MHz band. It aligns with the governance model as currently endorsed by the senior officials responsible for emergency management in Canada (SOREM), which contains two layers of operational responsibility – a national entity and multiple regional service delivery entities (RSDE). The network architecture is also aligned with the service delivery model whereby the users of the public safety broadband network (PSBN) are clients of the RSDE, while also being owners of the information networks. The PSBN interfaces with several external networks. The network architecture describes, at a high level, how the PSBN could interface with selected external networks. Furthermore, it is expected that Canada's public safety community will rely on deployable systems to deliver broadband services to isolated areas of the country where no broadband communications infrastructure exists and to areas where the infrastructure has been damaged. There is a section dedicated to the topic of deployable communications.

EN SITUATION D'URGENCE, SÉCURITÉ PUBLIQUE A BESOIN …

d'un réseau contrôlé par la sécurité publique, permettant d'accéder efficacement à de l'information, y compris des données vocales, de partager celles-ci exactement et opportunément durant toutes les étapes d'un événement, peu importe l'emplacement géographique, de disposer d'une capacité robuste et fiable, de l'interopérabilité et des ressources appropriées, selon les besoins des intervenants, et de s'adapter de manière dynamique aux changements de situation.[16]

Le présent document décrit l'architecture d'un réseau de communication canadien à large bande pour la sécurité publique qui devrait être exploité sur la bande de 700 mégahertz. Cette architecture cadre avec le modèle de gouvernance prôné par les cadres supérieurs responsables de la gestion des urgences au Canada (CSRGU) et correspond aux deux ordres de responsabilité opérationnelle – une entité nationale et plusieurs entités régionales de prestation de services (ERPS). L'architecture de réseau cadre aussi avec le modèle de prestation de services où les utilisateurs du réseau à large bande de sécurité publique (RLBSP) sont à la fois clients des ERPS et propriétaires des réseaux d'information.

Le RLBSP est lié à plusieurs réseaux externes. L'architecture du réseau décrit, à un niveau élevé, comment le RLBSP pourrait interagir avec des réseaux extérieurs sélectionnés. En outre, il est prévu que la communauté de la sécurité publique du Canada s'appuiera sur les systèmes déployables pour fournir des services à large bande dans les régions isolées du pays où aucune infrastructure de communication à haut débit existe et dans des régions où les infrastructures ont été endommagées. Une section entière a été consacrée au sujet des communications déployables.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be
helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a
published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Emergency Planning; Public Alerting; Broadband Communications; 700MHz

[16] U.S. Department of Justice - Community Oriented Policing Services (COPS), "National Forum on Public Safety Broadband Needs" August 23, 2010. http://www.cops.usdoj.gov/files/RIC/Publications/e021111338-broadband-forum.pdf