Implications of Service Delivery Model Options on Interoperability and Operational Efficiency in a Public Safety Mobile Broadband Network

Joe Fournier
Claudio Lucente
DRDC – Centre for Security Science

Prepared For:
Mark Williamson

Defence Research and Development Canada

Scientific Report
DRDC-RDDC-2017-R038
March 2017

Abstract

Delivering broadband services to the subscribers of the Public Safety Broadband Network (PSBN) can be achieved by several different approaches. Each approach entails different sets of actors in the service delivery fabric and different distributions of functions between the actors. Four approaches (options) are examined and compared for how they could satisfy fundamental requirements for (i) nationwide and agency-wide interoperability and (ii) operational efficiencies in delivering broadband service. The evaluation was based to a large degree on previous work by DRDC CSS that examined the technical underpinnings to achieve inter-working at the network level and interoperability at the service and user levels. In general, nation-wide interoperability can be more easily achieved by centralizing the functions that are implicated in delivering the services than by replicating those functions among independent regional actors. Furthermore, centralizing those key functions also leads to service delivery efficiencies because of reduced capital costs for the infrastructure and reduced costs to operate and maintain those functions. A hybrid option, between a fully centralized model and one consisting solely of independent regional actors, can be an efficient way to operate the PSBN and facilitate interoperability. The hybrid option consists of a national proxy of the regional actors to whom they would have delegated their authority to perform some of their functions. In all the options, a centralized coordination function is required that acts as the custodian of the interoperability standards for the PSBN.

Significance to Defence and Security

The wireless PSBN will be a nationwide cellular network primarily for public safety, security and defence communities. It will be a transformational capability that will revolutionize the way first responders and defence personnel communicate and share information with one another for decades to come. Putting broadband mobile in their hands will greatly increase their ability to anticipate, respond to and recover from emergencies, disasters and acts of terrorism by increasing their situational awareness, which will ultimately help protect and save lives, limit property damage and loss, and make communities safer. Indeed, while commercial cellular service is able to deliver broadband to public safety users for day-to-day use, it quickly becomes unavailable when major incidents occur and networks become severely congested. The PSBN will address this by ensuring that public safety users have access to their broadband applications and services when they need them most during disasters, emergencies and large planned events.

This report will inform the public safety and defence communities on different possible approaches for how the PSBN could deliver mobile broadband services. The report examines four different service delivery model options and the implications on interoperability, technical operations, administration and management (OAM) of delivering mobile broadband service for public safety and defence. The report explores the factors that impact interoperability and how a service delivery model can either facilitate or hinder interoperability. In addition, the operating efficiency of delivering mobile broadband services for different service delivery options is compared. Consideration of these factors as described in this document will significantly contribute to the successful implementation of the PSBN in Canada.

The Director Generals of Defence Research and Development Canada – Centre for Security Science (DRDC CSS), Public Safety Canada (PS) and Innovation, Science and Economic Development (ISED) all have a high level of interest in the contents and findings of this scientific report, as does the PSBN Federal/Province/Territorial Interoperability Working Group (F/P/T IWG) which has been expanded to include municipalities and the tri-services.

Résumé

On peut assurer de diverses façons la prestation de services à large bande aux utilisateurs du Réseau à large bande de sécurité publique (RLBSP); chacune présente des groupes d'intervenants différents dans la structure de prestation des services et une répartition différente des fonctions entre ces mêmes intervenants. Quatre démarches (options) sont analysées et comparées en fonction de leur capacité à répondre aux exigences de base visant (i) l'interopérabilité à l'échelle de l'Agence et du pays, ainsi que (ii) l'efficacité opérationnelle de la prestation des services à large bande. Cette analyse se fonde dans une large mesure sur des travaux précédents du CSS de RDDC, dans lesquels on a étudié les fondements techniques pour assurer l'interopérabilité à l'échelle du réseau, sur le plan des services et au niveau de l'utilisateur. En règle générale, centraliser les fonctions qui entrent en jeu dans la prestation des services permet d'assurer l'interopérabilité à l'échelle nationale plus aisément que répartir ces mêmes fonctions entre des intervenants régionaux indépendants. La centralisation des fonctions essentielles permet également d'assurer l'efficacité de la prestation des services, autant grâce à une capitalisation moindre pour l'infrastructure qu'à une réduction des coûts d'exploitation et de maintenance des fonctions. Une option hybride à mi-chemin entre le modèle entièrement centralisé et un groupe formé d'intervenants indépendants peut être aussi un moyen efficace d'exploiter le RLBSP et d'assurer l'interopérabilité. Dans ce modèle, les intervenants régionaux délèguent leur autorité d'exécuter certaines fonctions à un mandataire national. Toutes les options analysées, cependant, exigent une fonction de coordination centralisée qui assure l'application des normes d'interopérabilité du RLBSP.

Importance pour la défense et la sécurité

Le RLBSP sans fil sera un réseau cellulaire national destiné surtout à la sécurité publique, ainsi qu'aux communautés de la sécurité et de la défense. Cet instrument de transformation révolutionnera les communications et l'échange de renseignements entre les premiers intervenants et le personnel de la défense durant des décennies. Les services mobiles à large bande à portée de la main augmenteront considérablement la capacité de prévoir les urgences, les sinistres et les actes terroristes, d'intervenir et de rétablir les choses. Le fait d'améliorer ainsi leur conscience de la situation permettra au bout du compte de protéger et sauver des vies, de limiter les dommages et les pertes matérielles, et rendra les collectivités plus sûres. Les services cellulaires commerciaux sont certes suffisants pour l'utilisation quotidienne par les agents de la sécurité publique, mais en cas d'incident grave, ils deviennent vite incapables de répondre à la demande car ils s'engorgent sérieusement. Le RLBSP permettra de pallier ces lacunes, car il assurera que les agents de sécurité publique ont accès aux applications et services à large bande quand ils en le plus besoin, c'est-à-dire en cas de sinistre, d'urgence et d'événement public d'envergure.

Le rapport expose à l'intention des communautés de la défense et de la sécurité publique les diverses démarches possibles qui permettraient au RLBSP d'assurer les services mobiles à large bande. On analyse quatre modèles possibles et leurs répercussions sur l'interopérabilité, les opérations techniques, l'administration et la gestion des services mobiles à large bande pour la

sécurité publique et la défense. Puis, on explore les divers facteurs qui ont une incidence sur l'interopérabilité et la façon dont un modèle de service précis peut la simplifier ou l'entraver. En outre, on compare pour chaque option l'efficacité opérationnelle de la prestation des services mobiles à large bande. En tenant compte des facteurs exposés dans le rapport, on facilitera considérablement la mise en place réussie du RLBSP au Canada.

Les propos et conclusions du rapport intéresseront au plus haut point les directeurs généraux du Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (CSS RDDC), de Sécurité publique Canada (SPC) et d'Innovation, Sciences et Développement économique Canada (ISDE), ainsi que le Groupe de travail fédéral, provincial et territorial sur l'interopérabilité du RLBSP, élargi ici pour englober aussi les municipalités et les trois services.

Table of Contents

List of figures

List of tables

This page intentionally left blank.

1 Purpose

The purpose of this technical report is to inform the public safety community on different possible service delivery model (SDM) options and their implications on delivering mobile broadband services to emergency responders using Long Term Evolution (LTE). The report examines four different service delivery model options and the implications on interoperability, technical operations, administration and management (OAM) of delivering mobile broadband service for public safety. The report explores the factors that impact interoperability and how a service delivery model can either facilitate or hinder interoperability. In addition, the operating efficiency of delivering mobile broadband services for different service delivery options is compared.

At the time of this writing it is not known what the Conditions of License (CoL) for the public safety broadband network (PSBN) will be, nor the spectrum licensing framework. Because of this, all references to either in this report are purely notional and are not intended to indicate what the actual CoL and spectrum licensing framework would be. Furthermore, the options do not infer any governance structure for the PSBN or for any of the actors in the service delivery fabric.

2 Introduction

There are many ways to deliver wireless services to a user community. In the case of a mobile public safety broadband network (PSBN) providing vital services to first responders, two key considerations in determining the most effective service delivery model are interoperability and service delivery efficiency.

Communications interoperability amongst emergency responders is a fundamental driver for establishing a mobile broadband network serving their communications needs, while also providing them with the means to access and share, in real time, information that is rich in content such as voice, images and video. Such a communications network must be secure, reliable and affordable. It must allow emergency responders from any jurisdiction or agency to operate seamlessly across Canada, as authorized, and to be able to interoperate with their U.S. counterparts during incidents that require mutual aid [1]. If permitted, the PSBN may also accommodate commercial traffic during times when, and at locations where the public safety spectrum is not fully utilized.

The Communications Interoperability Strategy for Canada (CISC) [1] illustrates by way of the Interoperability Continuum, that the state of interoperability is not binary, i.e., having achieved interoperability or not. But rather, the CISC allows for interoperability to be evaluated over a continuum between low interoperability and having achieved a high level of interoperability. Interoperability is not solely dependent on technology. The other 4 factors that affect it, according to the CISC, are: (i) governance, (ii) training and exercises, (iii) standard operating procedures, and (iv) usage. This technical report examines 4 different service delivery model options that consider network architecture, roaming aspects, the ability to support interoperability and service delivery efficiency. While it is beyond the scope of this report to conduct a detailed costing analysis of the different service delivery models, a relative cost impact analysis and the operational efficiencies of one model relative to another are examined. Operational (in)efficiencies have a direct impact on the costs incurred by an organization, which in turn impact the price that is charged for the wireless service and the long term sustainability of the operation.

Section 3 presents four different hypothetical service delivery model options. Section 4 examines different roaming scenarios and the obligations of wireless mobile network operators (MNOs) that are contained in roaming agreements. The emphasis of this report is in Sections 5, 6 and 7, which examine the implications of the different service delivery models on interoperability, a comparison of the service delivery efficiencies of the 4 options and the national functions that are required to support nationwide interoperability. The conclusion in Section 8 contains a summary of the factors that are used in comparing the different service delivery options in this report.

Annex A contains an overview of the Public Land Mobile Network Identifier (PLMN ID) composition and how it is used in wireless networks.

3 Service Delivery Options

The broadband mobile communication needs of public safety users can be delivered in three different manners (implementation models):

- a dedicated public safety network used exclusively by public safety;
- a public safety network that is shared with commercial subscribers, with priority access privileges for public safety users; and
- a commercial network that supports public safety users.

The hypothetical service delivery model options for a public safety broadband network (PSBN) that are examined in this report are based on the shared implementation model listed above and are illustrated in Figures 1 to 4. As public safety broadband is a relatively new notion with very few operational deployments globally, there is little reference material to base models on, in particular for shared service delivery models. As such, the four options captured in this report have been created by the authors. Some options are less feasible than others for technical, administrative, or other reasons, many of which will be examined herein. These options are considered nonetheless so as to dispel any potential pre-conceptions by the reader regarding their viability. The model where there is more than one licensed operator of the PSBN in any given region is not considered in this report.

The four models in this report were chosen based on the significant distinctions among them, and as such are felt to fully cover a comprehensive, wide breadth of possible service delivery models for a PSBN. While more models could have potentially been considered in this report, they would simply be relatively close variants of the four described herein.

Ultimately, the choice of a SDM will consider, as a minimum, nationwide interoperability and with the U.S., access and sharing of information, service delivery efficiency, roaming arrangements, advanced services, a common user experience, and efficient use of spectrum. All of the models described herein can accommodate sharing of the network with commercial users. The following options are notional and not intended to affirm what the actual CoL and spectrum licensing framework would be, nor a governance framework.

a) **Option-A:** One national mobile network operator (MNO) licensed to operate a PSBN throughout Canada (one PLMN ID).

b) **Option-B:** Multiple independent regional MNOs (different PLMN IDs) licensed to operate in specific non-overlapping geographic regions of Canada.

c) **Option-C:** Similar to b) in that each regional MNO would be a licensed operator of the PSBN on a primary basis. But, unlike b), all the regional MNOs would share the same PLMN ID.

d) **Option-D:** Multiple regional MNOs each holding a secondary or subsidiary license to operate the PSBN and a national functions body being the primary license holder (one PLMN ID).

The following assumptions for service delivery are made for each option.

A PSBN national coordination body is present in all four options. It may assume different functions, depending on how it could complement the other actors in the service delivery fabric of each option. A list of the minimum network functions that support interoperability is presented in §7. It is evident that the breadth and depth of expertise and corresponding funding for the national coordination body would vary significantly depending on the scope of functions that it would assume. Some of the functions pertain to coordination whereas others are operational in nature. The dotted line depiction between the national coordination body and the MNO(s) of the PSBN, shown in Figures 1 to 4, is intended to illustrate that the national coordination body would not have a direct role in the day-to-day operation of the PSBN. Furthermore, in all cases it is assumed that it would not host any communications infrastructure of the PSBN. Such operational functions would need to be undertaken by other actors of the PSBN. Option-D introduces an actor not found in the other three options that could undertake day-to-day operational functions. This is intended to provide an avenue for the regional MNOs to centralize some of their functions and as much of the core infrastructure as feasible to minimize duplication of common elements.

Option-A (One National MNO): The MNO would hold a nationwide license to serve all the users that subscribe to its service across Canada. The wireless service can be delivered through regional operating entities that would essentially be regionalized operations of the national organization. The national MNO would also interface with all external networks and roaming partner networks via a roaming exchange service, and be responsible to comply with the obligations imposed on it by the conditions of license (CoL), Service Level Agreements (SLA) or other obligations. It would define and adhere to interoperability standards[1] and satisfy the stipulations of the CoL. In this option the national MNO could incorporate most, and possibly all of the functions listed in §7.

Option-B (Multiple Independent Regional Licensed MNOs; Multiple PLMN IDs): The regional MNOs would each hold an operating license with specific geographic boundaries demarcating their respective service regions. Current guidelines of the Canadian Radio-television and Telecommunications Commission (CRTC) allow for only one Mobile Network Code (MNC) to be assigned for public safety broadband [2, Appendix 2]. No assumption is made in this report as to whether or not the guidelines would or could be changed to allow multiple MNCs.

Each MNO would individually contract with a roaming exchange service to provide interconnection to international and national roaming partners. National partners would include other regional MNOs and could include commercial carriers that can fill-in possible coverage gaps of regional MNOs. In this model, all regional MNOs would enter into roaming agreements with each other and with national and international partners. Each regional MNO would be responsible to deliver wireless service to the users in its geographic license area. No assumption is made in this report that each province and territory (P/T) would contract with its own MNO. But financial considerations would suggest that certain P/Ts with small user bases would not be able to contract with an MNO on their own, and would, therefore, need to join with other P/Ts to contract with a regional MNO serving multiple P/Ts.

[1] Section 7 contains a list of points that should be the subjects of interoperability standards. It is not the intent of this Report to present actual Interoperability Standards.

As independent licensees, each regional MNO would be required to comply with its regulatory and other contractual obligations. The interoperability standards would need to be in place at the outset and then updated as warranted.[2] Given that in this option there is no central operating function, it would befall the national coordination body and the regional MNOs to undertake all of the functions listed in Section 7. The interoperability standards that apply to all the regional MNOs would need to be managed over their lifetime. There is no actor in this option that would allow centralizing operational functions and network infrastructure to any extent.

Option-C (Regional MNOs as Primary Licensees; Shared PLMN ID): Each regional MNO would hold a primary spectrum license for the PSBN with one PLMN ID shared between them. No assumption is made in this report as to the feasibility of having multiple MNOs apply for the same MNC vis-à-vis the Canadian Numbering Administration (CNA). However, the interpretation of the CRTC Guidelines [2, §7] by the CNA suggests that only one MNO, or a proxy representing multiple MNOs, can be assigned an MNC. As such, the national coordinating entity could be the applicant for the MNC and manage the allocation of mobile subscription identification numbers (MSIN) to the MNOs.

Each regional MNO would serve the users in the geographic territory permitted by their license. The service delivery model for this option is similar to that of Option-B with the exception of sharing the same PLMN ID. In both options though, the interoperability standards may be coordinated through a national coordination body, but ensuring compliance could be through inter-MNO contractual agreements and through the CoL. In Option-C, the regional MNOs would be accountable to the spectrum regulatory body for the authority to operate the PSBN. The role of the national coordination body for this option would be essentially the same as in Option-B.

Option-D (PSBN Operated Jointly by Multiple Regional MNOs with Centralized National Functions): This option contains an actor in the service delivery fabric that is not found in the other options—a national proxy. Conceptually, this actor could be established as a joint-venture of the regional MNOs and hold the primary spectrum license. It should be able to assume the prerogatives that may be contractually delegated to it by the regional MNOs. The national proxy would administer the national interoperability standards as endorsed by the regional MNOs and the national coordination body. It would undertake a large number of the functions listed in Section 7. The national proxy would undertake operational functions such that it can enter into roaming agreements with other national and international MNOs and serves as the interface for national level information networks such as those of Federal agencies. Furthermore, this option would allow for many of the value added services described in Section 6 to be offered at a national level.

As in Option-B, the regional MNOs would serve the users in their respective geographic regions. But unlike Option-B, subscribers of each regional MNO could be considered subscribers of a

[2] It is reasonable to expect that interoperability standards will evolve over time as new technologies are introduced (ex. 3GPP releases) and as experience matures. It is highly likely that some interoperability standards may be missing at the outset or may need to be re-stated shortly after the launch of the PSBN service, and as new use-cases arise over the lifetime of the PSBN. It will be necessary to react quickly to adjust the interoperability standards as errors, omissions and new developments that impact interoperability are discovered. No assumption is made in this report on the timeliness and feasibility of updating CoL and interoperability standards in reaction to the discovery of interoperability issues as they arise.

national network operating under one PLMN ID. The single PLMN ID would be shared[3] by all the regional MNOs.

Alternatively in this option, the regional MNOs could be the primary license holders without significantly impacting the functions of the national proxy. Therein lies a key distinction with Option-C with regards to exercising leverage to enforce compliance to interoperability standards, the resolution of disagreements, and the degree of involvement of the regulatory authority in these matters.

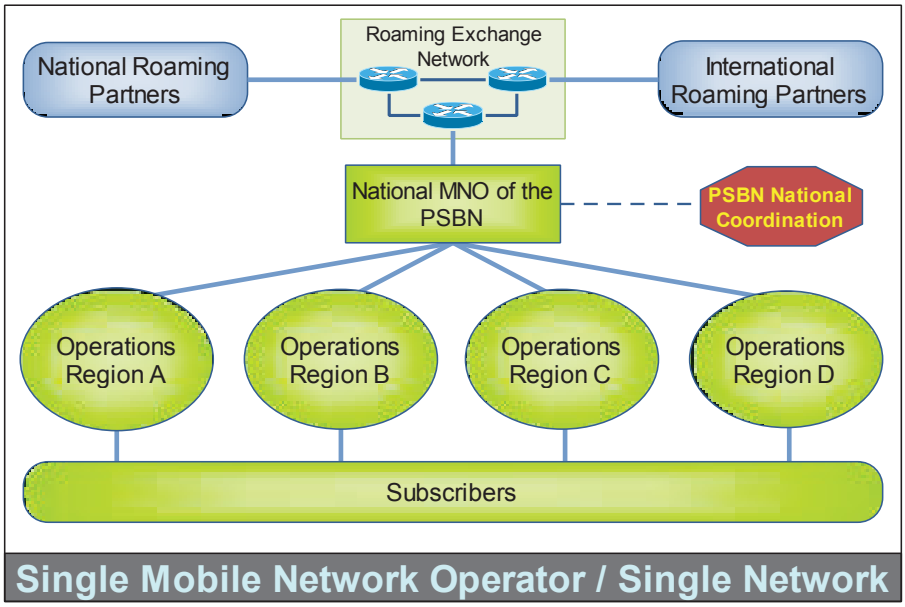

Figure 1: *Service Delivery Model Option-A: One national licensed MNO; one PLMN ID.*

[3] The notion of "shared Mobile Network Codes (MNC)" has been proposed by the CEPT Electronic Communications Committee [3] as way to utilize MNCs more efficiently and to enable new business models for MNOs.

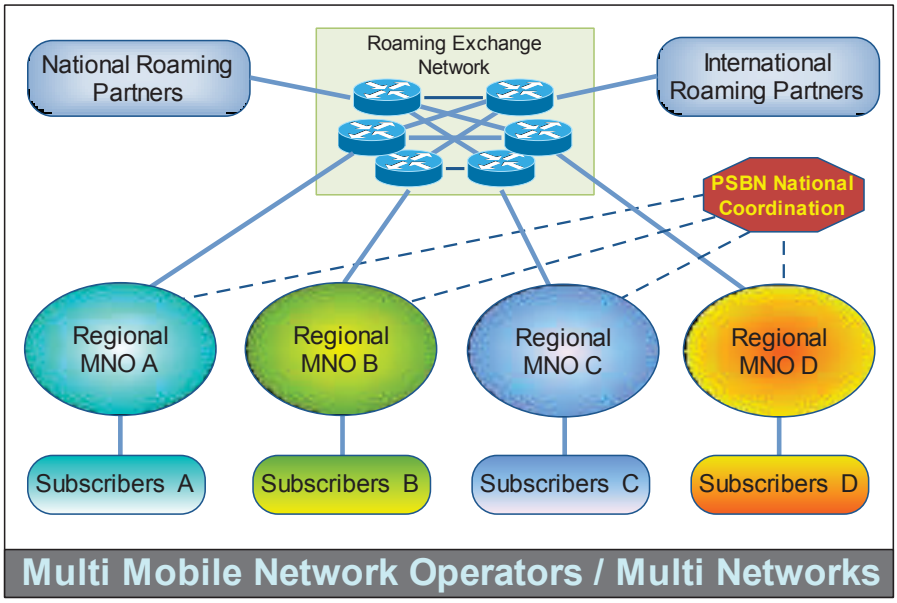

Figure 2: *Service Delivery Model Option-B: Multiple licensed regional MNOs; multiple PLMN IDs.*

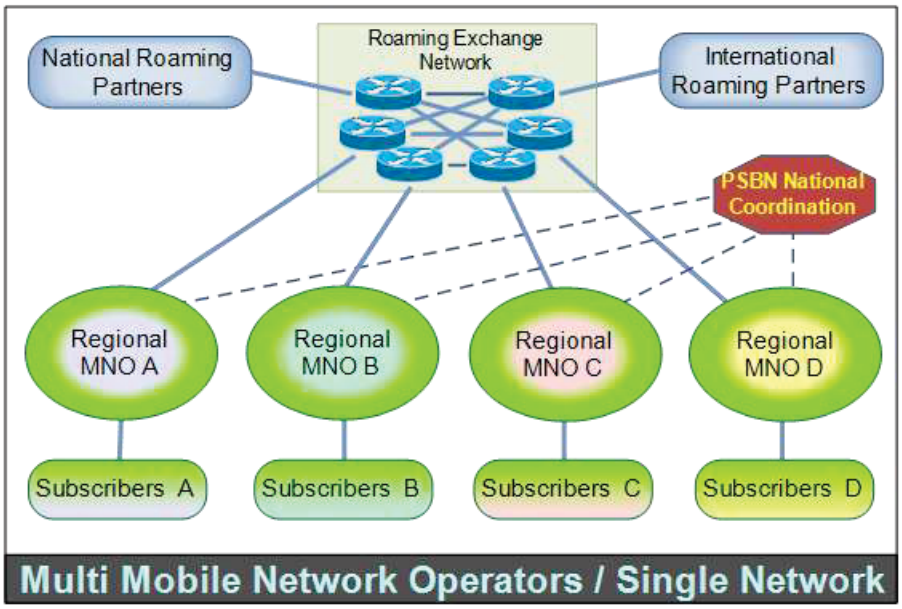

Figure 3: *Service Delivery Model Option-C: Multiple licensed regional MNOs; one shared PLMN ID.*

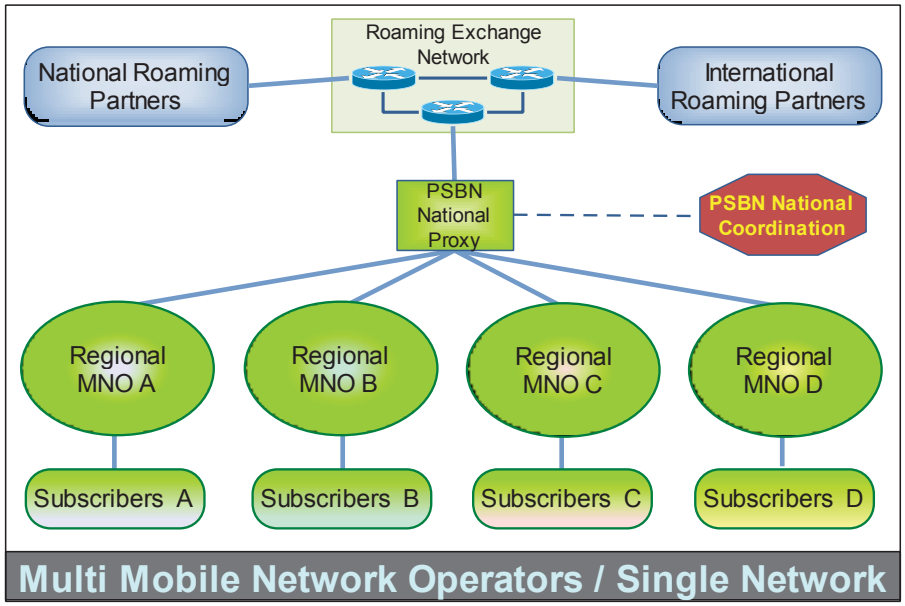

Figure 4: *Service Delivery Model Option-D: National primary licensed entity (proxy); sub-licensed regional MNOs; one shared PLMN ID.*

It is assumed that the PSBN, while dedicated to public safety, will not be used exclusively by public safety but will allow commercial users to access the network. Several MNOs can share the wireless communications infrastructure. Mobile Virtual Network Operators (MVNO) are resellers of mobile services and do not own any physical wireless network infrastructure except for some elements of the core network (CN), the least being the Home Subscriber Server (HSS). In addition to this, an MVNO operator would typically host the provisioning and billing functions of an Operations Support System. Each MVNO would be assigned its own PLMN ID. LTE base stations known as evolved Node B (eNB) are able to support up to a maximum of six PLMN IDs. That means up to 6 MVNOs can share the same physical LTE network in the same geographic area. The network architecture where public safety owns and operates its own CN but shares the Radio Access Networks (RAN) with commercial MNOs is known as the Multi-Operator Core Network (MOCN) [4], and is illustrated in Figure 5. Therefore, if the MOCN architecture were to be applied to the PSBN it would require an entity with an operational role in the PSBN to host the public safety CN. All service delivery options can support the MOCN architecture. Option-A and Option-D could have one MVNO public safety operator, whereas Option-B and Option-C could have as many public safety MVNOs as there are regional MNOs.

According to the network architecture for the PSBN as recommended by Defence Research and Development Canada – Centre for Security Science (DRDC CSS), the Evolved Packet Core (EPC) portion of the CN can be distributed at the regional level and the HSS would be hosted nationally [5].

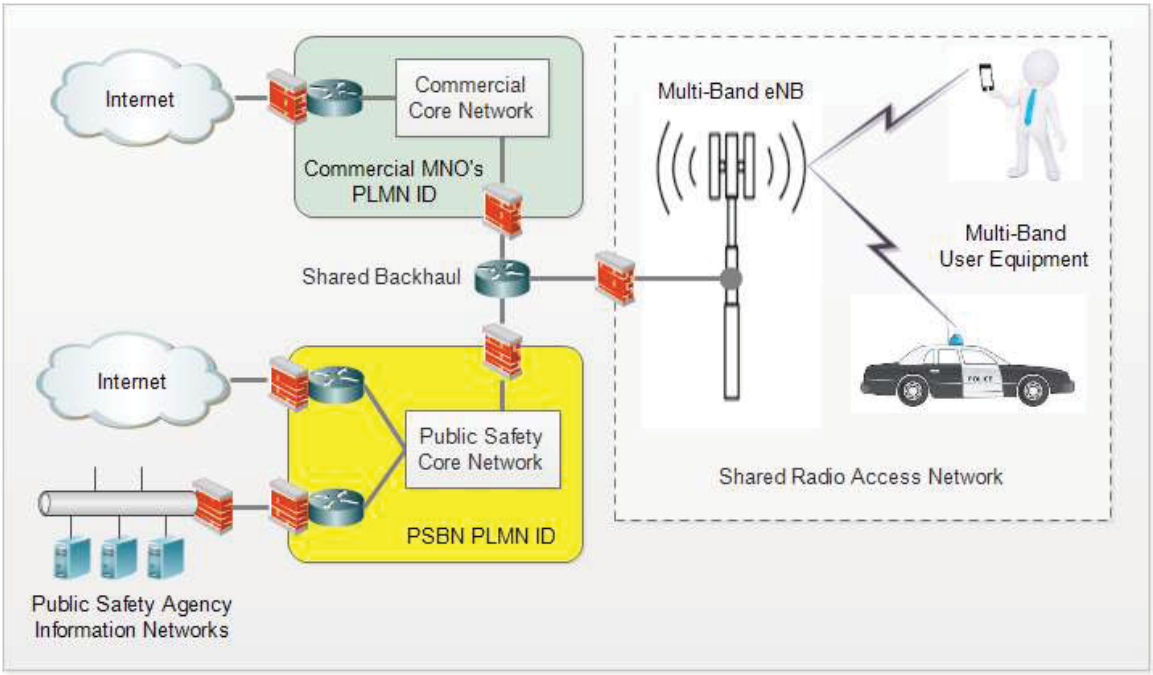

Figure 5: *Multi-Operator Core Network (MOCN): separate Core Networks; shared Radio Access Network.*

4 Inter-carrier Roaming

An important consideration in selecting an appropriate service delivery model is inter-MNO roaming. Typically, roaming is characterized by the ability of users to access mobile wireless services while they are outside the coverage footprint of their Home PLMN (HPLMN). Roaming is enabled by agreements between MNOs. Additionally, user devices must also be able to operate in the frequency bands of the visited public land mobile networks (VPLMN) and support the air-interface protocols of those networks. Visitors to the HPLMN are referred to as *inbound roaming* relative to the HPLMN. Users from the HPLMN that are visiting the VPLMN are referred to *outbound roaming* relative to the HPLMN. This is illustrated in Figure 6, where User-B is an inbound roamer relative to Network-A and User-A is an outbound roamer relative to Network-A.

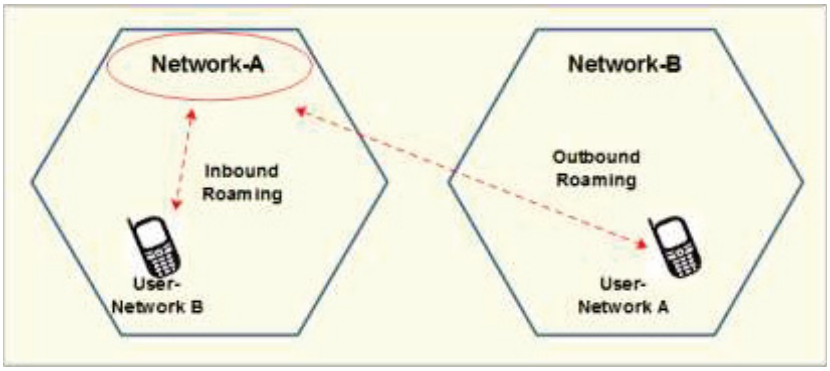

Figure 6: *Illustration of inbound and outbound roaming relative to Network-A.*

4.1 Roaming Scenarios

The following inter-MNO roaming scenarios are considered in this report:

a) Roaming in different geographic licensed areas. Example: Videotron and Rogers Wireless agreement to allow Videotron customers to roam on the Rogers Wireless network outside of Québec and eastern Ontario.[4] From a public safety broadband perspective, another example is between a Canadian PSBN and FirstNet, the U.S. national PSBN, where users on each network would, presumably, be permitted to roam onto the visited network.

b) Roaming in the same geographic licensed area. Example: Telus Mobility and Bell Mobility agreement to leverage each other's networks where one MNO has a dominant coverage footprint relative to the other in areas where both MNOs are licensed to operate their own wireless network.[5] Public Safety Broadband examples

[4] July 22, 2009 CBC news item: http://www.cbc.ca/news/technology/videotron-strikes-roaming-deal-with-rogers-1.821753.
[5] October 17, 2001 news release: http://www.bce.ca/news-and-media/releases/show/bell-signs-wireless-agreement-with-telus-which-will-significantly-expand-access-to-digital-voice-and-data-services-across-canada.

include: a) users on a Canadian PSBN being permitted to roam onto a visited commercial network when (i) additional bandwidth is required or (ii) when PSBN coverage is inadequate; and b) users on a commercial network being permitted to roam onto a Canadian PSBN when PSBN network bandwidth is available.

In all scenarios, the roaming interfaces between networks are the same. Figure 7 illustrates the roaming interfaces between two LTE networks. The green data path pertains to the case where the visiting user is routed to the home packet data network (PDN). The purple path pertains to the case where the visiting user is routed to the visited PDN. The latter case, where the user data does not traverse the boundary of the visiting network, is known as local breakout. The interfaces that must be connected between carriers for roaming are: S6a, S9, S8. The latter, S8, is not used for local breakout. The home network's access control priority and quality of service (QoS) policies, contained within the home policy charging rules function (hPCRF), would apply to local breakout. S9 carries information related to the user's profile for Quality of Service, Priority and Pre-emption (QPP). If the VPLMN does not support QPP, then those settings don't apply to the roaming user. The VPLMN can override the HPLMN settings. Interface S10 could also be interconnected in order for the bearer sessions to remain persistent during the hand-over of the UE between MNOs. This allows a user's session to remain active when his/her connection is handed over between networks.

The significance of home routed service versus local breakout is in the use of core network resources and in terms of performance. Local breakout uses fewer core network resources and does not traverse the roaming exchange network. With a shorter path to the PDN, the user should experience better performance. Local breakout enables lower roaming charges due to a more limited use of the roaming exchange (IPX) and by allowing the VPLMN operator to offer roaming services, effectively competing with the HPLMN operator for roaming services.[6] Local breakout is the subject of agreements between MNOs. However, using a virtual private network (VPN) service to protect sensitive data may preclude local breakout. This is examined in more detail in §5.1.

[6] The European Union capped roaming rates in July 2014. Local Breakout is the enabling technology. http://synergy.syniverse.com/2013/08/countdown-to-july-2014-a-primer-on-the-new-eu-roaming-regulations/.

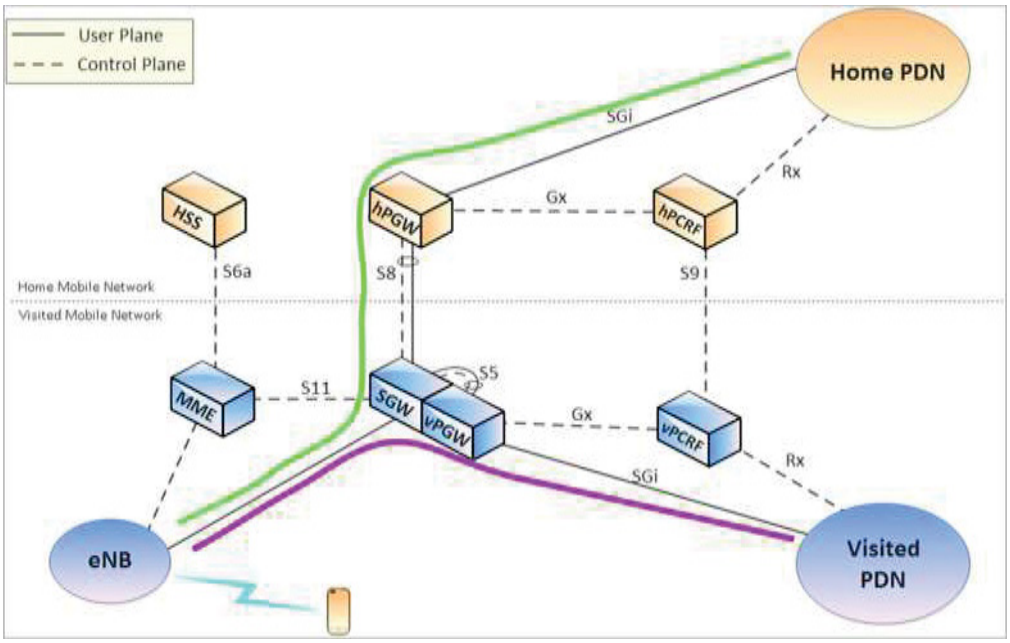

Figure 7: *LTE interfaces for roaming. The green path pertains to home-routed data. The purple path pertains to local breakout. (Source: [6]).*

With Option-A, Option-C and Option-D it is assumed that only one PLMN ID is assigned to the PSBN. The key inbound roaming scenario that applies to these models is when users from other MNOs operating networks on different PLMN IDs roam onto the PSBN. An outbound roaming scenario that applies to these models within Canadian territorial boundaries is where the local coverage with public safety spectrum is insufficient but the area is served by another MNO operating a network with a different PLMN ID (roaming scenario -b). Another outbound scenario where roaming would be required is when the public safety spectrum becomes congested and public safety users can be served by an alternative mobile network [7]. In the cases of Option-A and -D, roaming between regions of the PSBN is not required.

With Option-B it is assumed that each regional MNO would be assigned its own PLMN ID. Therefore, both roaming scenarios described at the beginning of this section apply to this option. An IP eXchange (IPX) Diameter Signalling Service (DSS) is priced on a per ‘roaming partner’ basis and billed monthly to each MNO. National roaming among all the PSBN’s regional MNOs, Canadian commercial carriers, and US network(s) would increase the aggregated cost for roaming.

In Option-A, -B and -D, the PLMN ID is sufficient to locate the HPLMN HSS in order to authorize the visited network to grant access to the roaming subscriber. In Option-C, by having the same PLMN ID shared between all the regional MNOs, additional technical and administrative complexity is introduced with regards to roaming. Option-C requires customized configuration of the routing function in order to parse the Mobile Subscriber Identity Number (MSIN) [Annex A]. Locating the correct HPMN HSS would be determined by the range of MSINs assigned to each regional MNO, as illustrated in Figure 8. This method has not been defined by the GSMA, which sets the inter-operator roaming standards. The IP eXchange (IPX), which provides the interconnection services to enable roaming, would need to implement a

customized solution using a Diameter Proxy Agent [8] that all the regional MNOs would need to agree on. Together, the regional MNOs would need to specify unique IMSI ranges that pertain to each of them, and require the IPX to parse the query string to inspect the IMSI, compare it against the ranges supplied by the MNOs, and route the query to the correct HSS. Since this is a non-standard solution, every roaming partner of the regional MNOs would need to be assured that the customized solution could handle billing data correctly and that their users can roam onto each regional PSBN network and vice-versa. For the IPX to implement a non-standard solution would entail non-recurring engineering cost, additional testing cost and recurring cost. Successful testing is a pre-requisite for roaming agreements. Tests cover the ability to meter traffic for billing, the business-to-business exchange of billing records, the ability to access the home subscriber server to get acknowledgment on the permissions granted to the users, etc. The additional DSS costs would be incurred in Option-B if the inter-regional roaming is enabled using an IPX. Inter-regional roaming could be accomplished using a private transport and managed by a national proxy, thereby reducing the costs that would otherwise be incurred by the use of an IPX. Regardless of which approach is taken to allow users subscribed to one regional MNO to be served on all the other regional MNOs, Option-C would be more costly than Option-A and -D, and similar to Option-B.

An important capability for public safety users is service continuity, which is the ability for a user to maintain a continuous communication session during the hand-over from one network to another or from one MNO of the PSBN to another [7]. Essentially, it is seamless roaming without impacting service connectivity and the communications sessions. To ensure service continuity for users as their connections are handed over from the eNB of one regional MNO to the eNB of another regional MNO, the regional MNOs having overlapping cellular coverage must interconnect the S10 interfaces between the Mobile Management Entities (MME) of their LTE CNs. Furthermore, to minimize the reduction in data throughput due to interference within the areas of overlapping coverage between the eNBs of adjoining regional networks, the regional MNOs would need to interconnect the highly delay-sensitive X2 interface of their eNBs. The S10 and X2 interfaces are not standard inter-operator connections. The regional MNOs would need to enter into SLAs that, as a minimum, would address responsibilities for implementing and managing the interconnections between them as well as the performance targets for the connections.

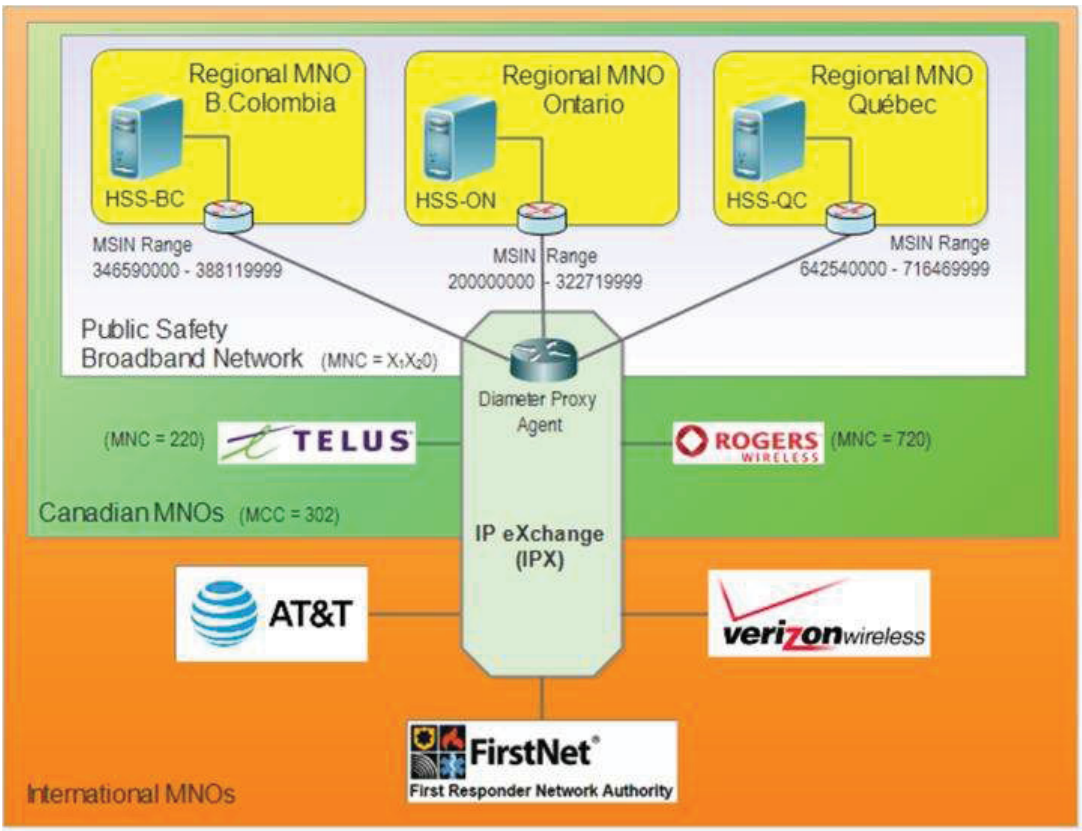

Figure 8: *Selecting the correct Regional HSS based on hypothetical MSIN ranges allocated to each regional MNO comprising the PSBN; for the purpose of international roaming (example).*

4.2 Roaming Agreements

Roaming agreements (RA) involve multiple parties in order to allow subscribers of one MNO to be served by another MNO in a different geographic area or within the same geographic area, as in the case where the local coverage of the "home" MNO is absent but is served by another MNO.

Licensed network operators are required to enter into RA if they wish to allow their subscribers to use other MNOs' networks when they are outside the coverage footprint of the home network (outbound) and to be able to serve subscribers of other MNOs on their network (inbound).

Roaming agreements must conform to international standards that are overseen by the Groupe Spéciale Mobile Association (GSMA) and can only be entered into by operators that are licensed by Innovation Science and Economic Development (ISED) and registered as telecommunications carriers with CRTC.[7] The GSMA has published a template for RA, although MNOs are not obligated to use it. The RA are intended to cover, as a minimum, the information that the GSMA

[7] For the purposes of this report a spectrum license holder and a licensed MNO may be different and distinct entities.

maintains in its Roaming Agreement Exchange (RAEX) database [9] for each MNO as listed in Annex B.

The number of RA increases geometrically as the number of partners according to the equation below. Table 1 illustrates by way of example the number of RA that would be established assuming one PSBN operator for Option-A and -D and thirteen PSBN operators for Option-B and Option-C. In this example, Option-D is effectively the same as Option-A. The number of roaming partners used in the example is hypothetical.

$$RA = \sum_{i=2}^{N} (i - 1)$$

Where: RA ≡ number of roaming agreements, and

N ≡ number of roaming partners

Table 1: *Example of number of roaming agreements as a function of the number of roaming partners.*

Mobile Network Operators	Option-A	Option-B	Option-C	Option-D
Public safety broadband licensees	1	13	13	1
Canadian commercial MNOs	3	3	3	3
FirstNet (US public safety licensee)	1	1	1	1
US commercial MNOs	4	4	4	4
Total number of roaming partners	9	21	21	9
Number of roaming agreements	36	210	210	36

Clearinghouse service providers broker the RA between partners thus reducing the burden that each MNO would otherwise incur to manage all the RA. Clearinghouse service providers typically offer the following services:

- Roaming agreement broker and management: Negotiate, prepare, and document the RA. Act as a single point of contact for the client MNO vis-à-vis all of its roaming partners.
- Facilitate roaming between partners that adhere to incompatible standards for billing formats, signalling, interfaces, protocols, etc.
- Billing settlement: monthly reconciliation of debits and credits, foreign exchange, taxes, etc.
- Business intelligence: usage reports.
- Fraud detection.

Annex B contains a list of the subjects that are typically covered in RAs.

Each MNO incurs the cost of the Clearinghouse services and maintains internal administrative staff and procedures to manage the Clearinghouse vendor.[8] Each MNO would also maintain a revenue assurance function. Consolidating these functions into a central service is more cost-effective than replicating the functions among multiple independent MNOs. Hence, Option-B and Option-C would have the highest cost associated with managing roaming agreements when aggregated across all the regional MNOs. In Option-D, a national proxy could manage the roaming agreements as a centralized service on behalf of the regional MNOs. Furthermore, it potentially could reduce the number of connections to an external IP exchange since roaming amongst regional MNOs is not required. But, because it would reconcile the billing settlement among all the regional operators, its revenue assurance and billing operations would be more expensive than those of Option-A.

[8] The procedures referred to here are those that form part of an MNO's operational procedures to manage the roaming agreements and the sub-contractors that it uses to enable the roaming function. The procedures would be maintained in compliance to International Standards Organization (ISO) requirements.

5 Service Delivery Models Impact on Interoperability

This section examines how the four service delivery models that are defined in §3 impact interoperability. A definition of interoperability that is commonly used in the context of public safety wireless broadband is as follows:

> *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 [1].*

Interoperability means that users, when and as authorized, are able to access and share the information they need to accomplish their missions, and are able to obtain a consistent user experience from any location across Canada that will be served by the PSBN. The manner by which mobile broadband services are delivered to public safety users has a major impact on how interoperability is achieved and the ease with which it can be sustained. LTE represents several generational leaps over LMR in terms of capabilities that users can benefit from. LTE enables MNOs to converge their communications platforms to an IP-based packet-switched network, in much the same way as IP allowed wireline carriers to converge their voice and data networks—driven by opportunities for cost savings and organizational efficiencies. But the flexibility of IP and LTE is accompanied by a great number of configuration options and choices for the operators of such networks. Inter-working at the level of the infrastructure is a pre-requisite for interoperability at the user level.

The topics that are covered in this section have been selected because they are strongly impacted by the choice of a particular service delivery model. Each subject is treated at a high level in order to cover as many as possible in keeping with the purpose of this report. A greater level of examination of the degree of impact on interoperability can be undertaken in the future.

5.1 Virtual Private Networks

A virtual private network (VPN) imparts confidentiality and privacy protection on IP data packets traversing between two end points. An oft-used metaphor for VPN is that of traffic flowing inside a private tunnel within a shared pipe. In essence, VPN creates a secure connection-less link between two end-points and affords similar protection to selected traffic as a dedicated physical connection. VPN protects the data packets by encrypting the payload and the IP address headers. The encrypted packet is then encapsulated within a VPN packet and a new IP-routable address is appended. Figure 9 illustrates a conceptual diagram of the information flow between the two end points using VPN. The encryption/decryption process is negotiated between the two end-points. A commonly used industry standard for instantiating VPN tunnels is IPsec[9] [10] [11] [12]. Although it is governed by industry standards, IPsec implementations are highly configurable and connection issues can and do arise due to misconfigurations.

[9] The latest version is IPsec-v3.

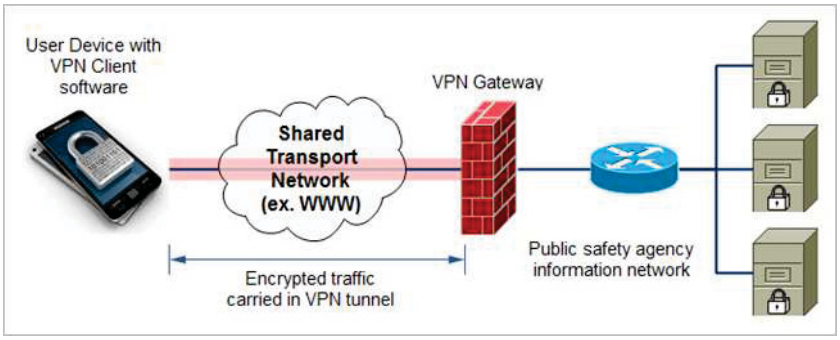

Figure 9: *Illustration of point-to-point VPN tunnel to protect user information.*

A VPN client establishes a security association with the VPN gateway that is protecting an information network. A VPN client that is associated with a VPN gateway of another network is only admitted to the information network behind that VPN gateway. This has implications for interoperability when it is necessary to share protected information among team members if their devices' VPN clients are not all associated with the same VPN gateway. It then follows that the more independent VPN implementations there are among a group of emergency responders, the higher the likelihood that interoperability among them will be hindered when it is required.

There are two common implementations for VPN—enterprise-hosted and carrier-hosted. Enterprise-hosted VPN is analogous to each public safety agency implementing its own VPN server and gateways. Carrier-hosted VPN is offered as a managed service to client organizations. Carrier-hosted VPN implementations could all be referenced to a common VPN server within that carrier's network. By coupling the VPN service with a device management service, the carrier can ensure that the VPN client software is configured to be associated with the central VPN server. In effect, this allows the entire pool of users to access enterprise networks that reside behind each VPN gateway. While this would facilitate interoperability, it introduces a different problem. It is necessary that not every emergency responder be able to access any information network within the larger space of public safety databases and servers at any time. This problem can be addressed by identity, credentials and access control management (ICAM), which is examined in §5.2.2.

In service delivery Option-B and Option-C, the regional MNOs would each have their own security domain. Technically, it is possible to provide access to information networks within one security domain to users of another security domain. But, it requires a work-around consisting of back-end connections behind the VPN gateways. This is illustrated in Figure 10. For the purposes of this report, the separate domains are assumed to pertain to two different carrier-hosted VPN services. The access control policy node represents the rules for who, or what machine, can access which information network and under what circumstances. Although one node is shown, there could be at least one access control policy server per agency information network. The green path illustrates the data flow for VPN-protected traffic between user-A and its associated VPN gateway and agency information network, all within its HPLMN or home mobile network operator (HMNO). User-B is roaming. Its VPN client is associated with the VPN gateway of its home network, which in this example, is the VPLMN or visited mobile network operator (VMNO). If it is required for user-B to access the information network of Agency-A, then the VPN-protected data flow would be routed to his/her home network via the roaming exchange network, IPX (yellow path). Once the data packet is stripped of the VPN wrapper at the VPN

gateway-B, it is revealed that the destination IP address is a server in Agency-A's network and the routing would occur through the back-end connection. The access control function would ultimately determine if the user is permitted to access the particular information/application server.

In the case of Option-A, if the national PSBN carrier were to offer a managed VPN service, then all the user's devices could be associated with a central VPN server that would act as a reference for de-centralized VPN gateways. This does not preclude the possibility for specific agencies to establish their own VPN-protected information enclaves. In Option-A, data packets would not traverse the roaming exchange network. The agency information networks are accessible by virtue of being connected to the various Packet Data Network Gateways (PGW) that would be distributed throughout the PSBN.

In the case of Option-B and Option-C, if each regional MNO offered a managed VPN service to its subscribers, then the situation is as shown in Figure 10. The number of back-end connections would be a function of the number of regional MNOs that wish to interconnect their subscribing agencies' information networks. As these connections cross network security domains, the issue of who owns and manages the interconnections would need to be addressed within the inter-MNO SLAs. Technically, the IPX provider can also provide the interconnection service for this interface. But, as it is not part of the standard set of roaming interfaces, the back-end interface would be subject to a customized agreement between all the regional MNOs and contracted to the IPX to deliver. IPX revenue is a function of how many interconnections they support. Option-B and Option-C would result in higher costs than Option-A.

Option-B and Option-C are less amenable to supporting Federal users that operate across Canada because the agencies to which Federal users pertain would need to implement their own MVPN solutions in order to be able to reach their secure information networks from any location served by the PSBN. This means that their VPN-protected traffic must flow across the Internet rather than connecting directly to a dedicated PGW. It would not be possible to assert end-to-end quality of service performance if sessions are carried across the Internet. In addition, this approach hinders interoperability if users outside the security domain of a specific agency would need to have access to that agency's information.

An alternative approach to reduce the amount of traffic flowing over the IPX network is to temporarily re-configure the visiting VPN client to associate with the VPN server of the network he/she is visiting. This requires inter-MNO coordination of device management and mutual trust with sensitive security settings. The authors contend that, if the regional MNOs are also competitors for commercial clients nationwide, trusting that they will agree to exchange sensitive information regarding their core business would be a difficult issue to resolve.

A managed VPN service can be offered at either the national level or at a regional level. In the case of Option-D, it is assumed that the roaming interconnection would be at the national level rather than at the regional level. In this case, a national VPN server, which is the anchor for security associations for the PSBN mobile devices, would be hosted as a national function and the regional MNOs would host the regional VPN gateways that are associated to the national VPN server. This is similar to Option-A. If each regional MNO would offer its own independently managed VPN service, then this is similar to Option-B and Option-C where no national level VPN service is possible.

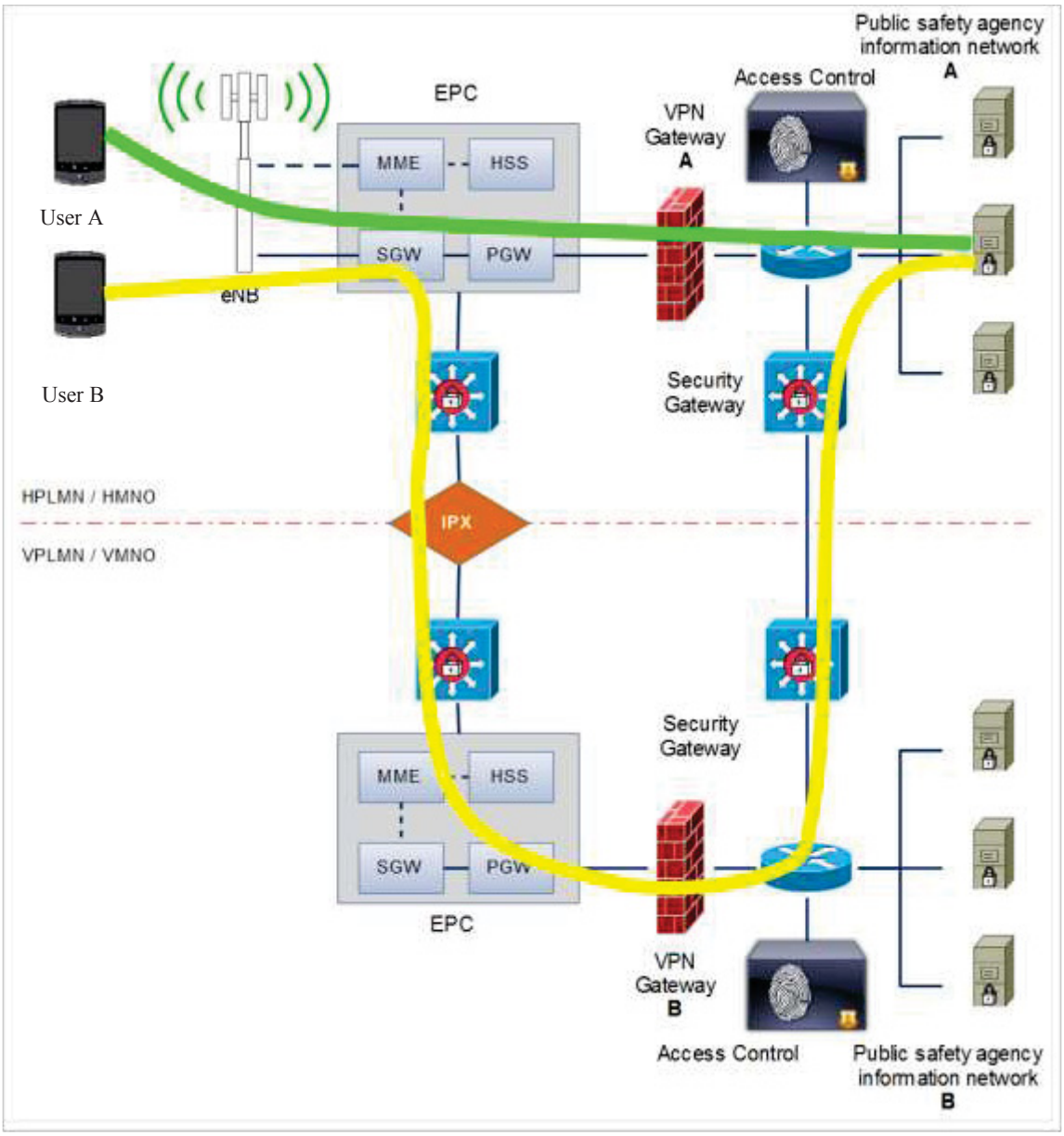

Figure 10: *Illustration of data flows for VPN-protected traffic for home-based security association (green path) and for roaming users with a different VPN security association (yellow path).*

5.2 Access Control, Priority and Quality of Service

This section examines the impact of the four service delivery options on the process for authenticating and authorizing devices and users to access mobile broadband services and agency information networks. They are two distinct processes and are assumed to be under the auspices of two different entities. Access to mobile broadband services is owned by the MNO, while access to agency information networks is owned by the public safety agencies. The MNO has no

involvement in determining who or what machine has access to what information. The mobile network merely determines if access to mobile broadband services are granted to a device, and with knowledge of the user's subscription, the mobile network determines what priority and QoS settings to apply to each session bearer.

5.2.1 Mobile Network Access

Within an LTE mobile network, the elements that are implicated in the access control process are:

- Home Subscriber Server (HSS): database of device identities derived from the international mobile subscriber identity (IMSI). When a device requests radio resources, the HSS is queried for the subscription status of the device pertaining to a particular IMSI. The structure of the IMSI is shown in Figure A.1.
- Subscriber Profile Repository (SPR): database of the subscription profiles of the users. The SPR is queried during the process of establishing session bearers. It contains information on subscriber's allowed services, subscriber's allowed maximum bit rate and guaranteed bit rate, and the subscriber's charging related information.
- Policy Rules Charging Function (PCRF): provides network control regarding service data flow detection, blocking or allowing packets, QoS control and flow-based charging. It can also apply security procedures before accepting information from the application function such as an IP Multimedia Subsystem (IMS), if it is present.
- Packet Data Network Gateway (PGW): provides connectivity from the user equipment (UE) to an external PDN by being the point of entry or exit of traffic for the UE. The PGW manages policy enforcement, packet filtering for users, charging support and lawful intercept.

When users are roaming on partner networks, the VPLMN queries the home network's HSS to determine if the IMSI is valid and the subscription is current. If so, radio resources are assigned to the visiting user's UE. Interface S9 conveys the QoS parameters to be used for bearer binding, particularly for local breakout.

The three interoperability lanes, (i) training and exercises, (ii) standard operating procedures, and (iii) usage strongly impact the user-experience. The expectation of user-experience is shaped as the users train with the PSBN and use the PSBN during their day-to-day missions and when responding to emergencies. The user-experience is also likely to be affected by standard operating procedures. That user-experience is defined by the quality of the service that the user receives, in particular when the PSBN is subjected to demands and stresses that exceed its ability to fully serve the sum of the instantaneous demands. During these instances, congestion management policies will determine who is served with higher priority, which applications can be served with less throughput, which ones can pre-empt others, and which ones can be pre-empted. These policies are maintained in the PCRF, of which there is at least one per mobile network. In order to support interoperability, the MNO(s) should configure their PCRFs the same way.

In the case of Option-A, the configuration parameters would flow from a common priority and QoS policy that applies throughout its network. The users could then be expected to have a similar user-experience throughout the entire footprint of the national PSBN.

In the case of Option-B and Option-C, the user-experience could vary from one network to the other since the MNOs are independent of each other. The degree to which the MNOs would harmonize their priority and QoS policies would be the subject of agreements between them. For an MNO that is also sharing the public safety spectrum with commercial users, the priority and QoS policy has an impact on its revenue—depending on the level of usage that is set to trigger congestion management mechanisms in the shared network. If it is a matter that is negotiated between an MNO and the public safety stakeholders at the regional level, it is conceivable that the commercial agreements would treat priority and QoS differently from one regional MNO to the other. Hence, it would fall upon a regulatory authority to require that a common QPP policy be adopted by all the regional MNOs.

In the case of Option-D, a national proxy could be empowered to establish operational policies that ensure a common user experience for the subscribers of all the regional MNOs that it represents, regardless of which regional network the subscribers would be served by.

5.2.2 Access to Agency Information Networks

Most commercial mobile broadband services today connect the users to the Internet. As long as a user's account is in good standing there is no additional authorization step required to access the Internet. If a user wishes to access other servers via the Internet then an additional log-in step is presented by the server that hosts the requested information or application. Emergency responders will want to access information networks that contain operationally relevant and incident-level data. For example, emergency responders will need to access records management systems, computer-aided dispatch, criminal databases, health records, etc. All these information assets could be accessed via the Internet using VPN services if they are connected to the Internet. Or, they can be connected directly to the MNO's PGW without connecting to the Internet. In either case, there will need to be an additional level of authorization to determine if a user is allowed to access the information he/she requests. That level of permission is assumed to be the purview of the responder agency or the owner of the information asset—not the MNO.

The on-boarding process for a new emergency responder normally includes establishing the credentials of the individual. As a minimum, the person must deposit two secrets (username and password) that will be used to validate the log-in to the databases and servers. Depending on the sensitivity of the information asset, there may be other credentialing factors that the individual must present in order for permission to be granted. For example, the person may be required to enter a randomly generated series of digits displayed on a token that changes periodically. Or the person may need to present a unique physical attribute such as a fingerprint or images of his/her irises. Each additional factor is intended to increase the level of confidence that the person presenting the credentials during a log-in step is actually who he/she says they are [13].

A public safety agency knows who they have accredited. They will have established, for each individual, a profile of privileges for access to the information assets they control. For the purpose of interoperability, some information would need to be shared among users, some of whom, under normal circumstances, may not be allowed to access it [7]. If all the users are known to the agency that controls the information assets, then the gatekeeper of the assets may modify the access privileges of the users requiring provisional access rights. However, if an event requires assistance from emergency responders from another public safety agency then there is an issue of how to grant permission to those external resources that need to share the hosting agency's

information—only with those users and only for the duration of the event. It is unlikely that the hosting agency would modify the access privileges of the visiting users to conform to the criteria that the hosting agency has defined for access to its information assets. A more likely approach is to use a service, referred to as Identity Credentials and Access Management (ICAM) that agencies would subscribe to [14].

ICAM is based on using a trusted party to assert the identities of the users that request access to information networks, whether they are part of the same agency that owns the information assets or another agency. It can also apply to non-human users, i.e., machines and sensors that read or write sensitive information, such as location of public safety assets. An ICAM solution could reference the user profile information from the SPR, but it is otherwise independent of the MNO or the service delivery model. The onus is on the public safety agencies to subscribe to an ICAM service. By doing so, they could potentially expose the profiles of their users, but it is possible that they can be represented anonymously to the ICAM service provider, thereby protecting the actual identities of the users.

5.3 Advanced Services

This section examines the impact of service delivery options on the delivery and interoperability of advanced services over LTE. The specific services that are examined are:

- Voice over LTE (VoLTE)
- Proximity Services (ProSe)
- Mission-Critical Push-to-Talk (MCPTT)
- Location Services (LCS)

5.3.1 Voice and Multimedia Services over LTE

Voice-over-LTE (VoLTE) is a term that refers to IP-converged voice and data on LTE. In the same way that enterprises unified their voice and data services onto an IP platform several years ago, VoLTE does the same for wireless broadband services. The IP Multimedia Sub-system (IMS) is one of the technologies that MNOs can leverage in order to deliver interoperable voice/multimedia services over LTE with controlled QoS. There are over-the-top (OTT) applications for voice-over-IP (VoIP) such as Skype™ and WhatsApp™, but these are closed group services. That is, only users that have opted to download those applications can participate in voice sessions with each other. To illustrate the point, a Skype user cannot engage in a voice call with a WhatsApp user directly over IP.

Some OTT applications can call phone numbers. In the case of a Skype user calling a mobile subscriber, the voice session would be handed off to the public switched telephone network at the OTT host's softswitch and directed to the mobile gateway of the MNO that serves the called party. If the LTE network does not support VoLTE, then the voice session would be carried using circuit-switched fallback on the mobile device's 2G or 3G radio.

Other real-time IP communications technologies are available such as WebRTC, espoused by Google, Mozilla and others.[10] WebRTC is intended to enable browser-based voice and multimedia sessions. But, in the telco-dominated world of voice communications IMS is the dominant technology for unified communications.

The 3rd Generation Partnership Project (3GPP), which is responsible for the LTE specifications, has defined an architecture for VoLTE that leverages the IMS [15]. According to the Global mobile Suppliers Association data released in August 2016, since 2009 when the first LTE networks appeared, the number of LTE mobile networks in operation world-wide has grown to 521. Yet, of these only 82 have launched VoLTE.[11] This is in part due to a general appreciation within the mobile communications industry that implementing IMS is costly and time consuming. However, the potential benefits of IMS are equally understood, where IMS allows MNOs to offer many advanced services that can bolster their service offering business. IMS is also required to route voice calls and multimedia messaging for next generation 9-1-1 using the PSBN.[12] There are numerous interfaces within an IMS subsystem as shown in the complex diagram of Figure 11. It is not the intention of this report to describe the functions of an IMS nor to describe the diagram in Figure 11, but merely to illustrate that implementing an IMS consists of a large number of interfaces that need to be configured and whose settings need to be managed and tested whenever changes within the IMS network or the interfaces to external networks are made.

In Figure 11 the UE is shown with an interface, Gm, to the proxy call session control function. This requires the UE to be configured with a session initiated protocol (SIP) user agent (UA). The SIP-UA is highly configurable. Since an entire subscriber base of mobile users need to have their SIP-UA's configured in the same way, it is not practical to configure them individually. The Internet Engineering Task Force (IETF) has recommended a set of procedures for how SIP-UAs can retrieve their configuration information from a configuration service [16]. While the referenced document is not a standards-track specification, it does provide guidance to the industry for a process to automatically configure SIP-UAs.

[10] https://webrtc.org/.

[11] The Global mobile Suppliers Association represents mobile suppliers worldwide, engaged in infrastructure, semiconductors, devices, services and applications development, and support services. https://gsacom.com/ .

[12] An MNO may be able to leverage the IMS in its commercial core network to serve public safety users. The considerations for QPP and reliability for doing so are not examined in this report. However, it remains that the implementation of IMS aggregated across all the regional MNOs as in Option-B and Option-C is more costly than an implementation of IMS by a single national MNO as in Option-A or centralized as a national function in Option-D.

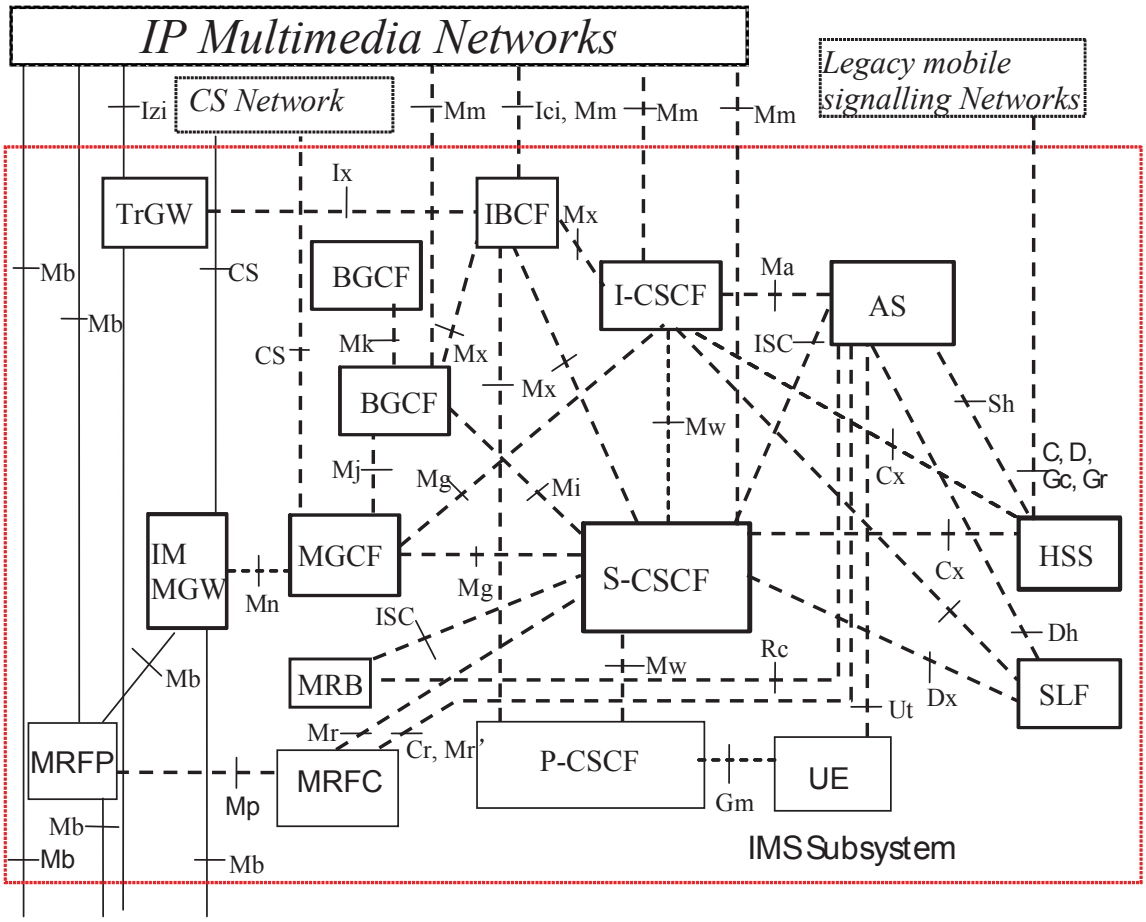

Figure 11: *Interface reference points within an IMS subsystem. (Source: [15] p. 24).*

To provide VoLTE services for users when they are roaming, the GSMA has defined three key operational requirements [17]. They are:

1. Routing of media for VoLTE when call originator is roaming should be at least as optimal as that of current circuit-switched (CS) domain.

2. The charging model for roaming used in CS domain shall be maintained in VoLTE.

3. Allow the HPLMN to decide, based on service and commercial considerations and regulatory obligations, to enforce the routing of the traffic to itself (home routing).

The reference architecture for VoLTE roaming that satisfies the above operational requirements is illustrated in Figure 12. The control plane information is exchanged between the home network and the visiting network, while the data plane information should be routed locally. This architecture assumes that all roaming partners will have implemented an IMS subsystem in their respective networks. If that is not the case then the data plane and control plane traffic could be routed to the home network's IMS. Since IMS is intended for voice and real-time multimedia services, routing user information to the home network could negatively impact the performance

of the application unless additional measures are taken by all the MNOs to ensure end-to-end quality of service, regardless of whether they host an IMS or not. These additional measures include the ability to re-direct traffic to the least congested path in real-time, which implies real-time traffic monitoring and dynamic marking of priority headers of multi-protocol label switched (MPLS) IP packets. The LTE networks would also require the application detection and control (ADC) function and traffic detection function (TDF) in order to gate OTT packets in favour of packets that carry more latency- and bandwidth-sensitive traffic [18]. In addition, all the MNOs would need to coordinate the establishment of Traffic Flow Templates (TFT) so that voice service flows are treated the same way in all the regional networks for consistent treatment of priority and QoS [19]. On-going coordination would be required to manage changes and upgrades to the networks and the configuration settings.

For national roaming partners that don't all support VoLTE, yet wish to provide a seamless handover for voice as their subscribers roam from one network to another, the MNOs must support enhanced Single Radio Voice Call Continuity (eSRVCC) and Circuit-Switched Fall Back (CSFB) to 2G and 3G networks [20]. However, eSRVCC voice quality is degraded because of the additional transcoding step that is necessary between the network domains. The transcoding step can be avoided by standardizing on the voice codecs that every MNO uses, but this requires an additional level of coordination burden on the MNOs [21]. Therefore, until all partner MNOs implement the IMS, those that are transitioning to VoLTE will each incur additional cost to support the CS voice network.

Supporting VoLTE services for roaming users entails additional cost, complexity and administration. The aggregated cost of multiple MNOs, each implementing its own IMS, is greater than the cost of implementing a centralized IMS for the PSBN nationwide. Hence, Options-B and Option-C would be less cost efficient than Option-A. Option-D would be as cost-effective as Option-A if the regional MNOs would agree to have an IMS CN hosted on their behalf as a national function.

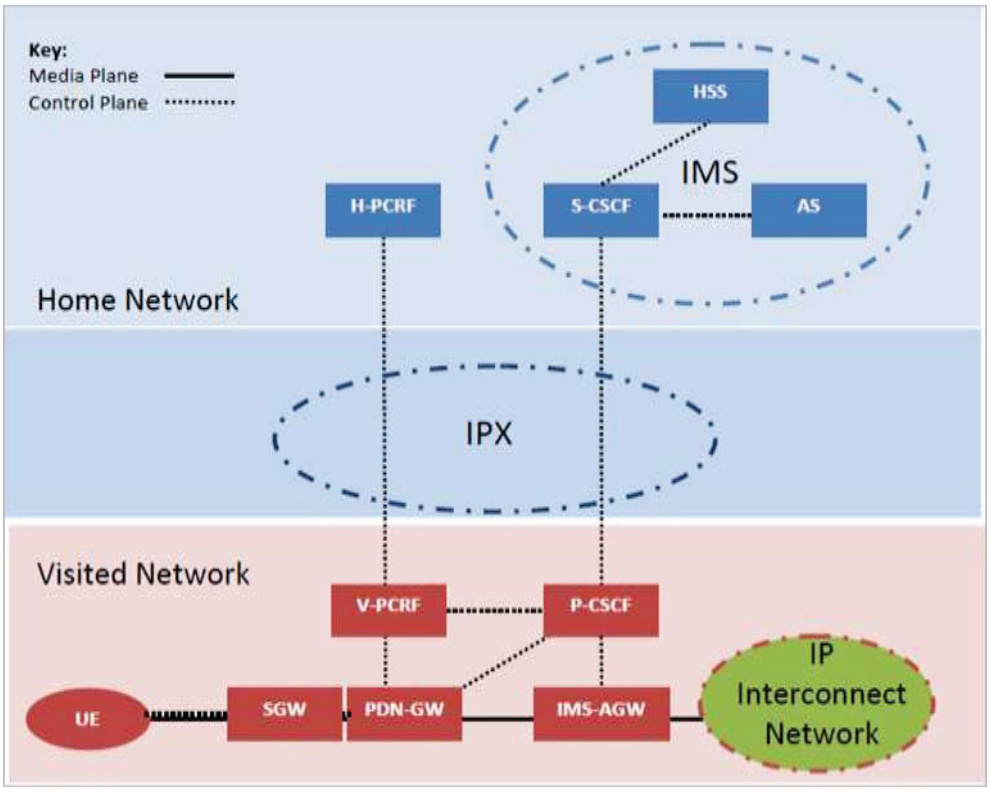

Figure 12: *Illustration of target voice roaming architecture. (Source: [17] p. 11).*

5.3.2 Proximity-based Services

One of the most important mission-critical capabilities demanded by emergency responders is the ability to communicate when they are out of range of the base station. Land mobile radio (LMR) systems have the "direct mode" feature which allows users to communicate with each other directly using a dedicated frequency designated as the "simplex channel". The 3GPP has released the specifications for ProSe, which is a feature that allows direct connection between users in proximity of each other without the assistance of the eNB to establish, maintain, or terminate the connection [22]. ProSe enables one-to-one and one-to-many direct device-to-device communications.

A ProSe-enabled UE can discover other ProSe-enabled UEs that are in proximity to it even if they belong to different PLMNs. This can be done with or without the assistance of the eNB. Figure 13 illustrates the non-roaming and roaming reference network architecture for ProSe.

With reference to Figure 13, the ProSe Function[13] is used to configure the UE so that it can use ProSe direct discovery and ProSe direct communication. It also enables visiting UEs to use ProSe services in the visited PLMN. The HPLMN is the authority for a UE to use ProSe direct discovery and ProSe direct communication, regardless of whether the UE is in its home PLMN or if it is outbound roaming. But authorization may be revoked by the VPLMN.

[13] In the context of this report, the ProSe Function is assumed to also contain the Key Management Server.

If a UE that intends to use ProSe is also in the coverage of an eNB, it will first check if the serving eNB is configured to provide radio resources for ProSe. If so, then the UE may use those radio resources for ProSe. If not, then it may not use that eNB's bandwidth allocated for ProSe. If the UE does not detect any PLMN through an eNB, then the UE may use the radio resources that are preconfigured in its universal integrated circuit card (UICC). ProSe-enabled UEs can operate on multiple PLMNs. The user profile in the HSS must be configured with the list of PLMNs where the user can operate ProSe direct discovery and ProSe direct communication.

In the case of Option-A, where there is one national PSBN operator, the entire network can be enabled for ProSe discovery and ProSe direct communications by the national operator. The administration of the configurations is managed at the national level. The only consideration for inter-PLMN device-to-device communications is with FirstNet where the two parties would need to coordinate with each other.

In the case of Option-B and Option-C, where the PSBN is constituted by multiple MNOs, they would need to coordinate the assignment of spectrum for ProSe operation among each other and with FirstNet in order to have multi-jurisdictional interoperable ProSe capabilities within their territories. Those MNOs that do not support ProSe would need to include a ProSe Proxy Function in their core networks so that a roaming UE may use a home-routed connection to the ProSe Application Server.

In the case of Option-D, the coordination can be performed as a national function, but would require that all the regional MNOs agree to a common set of configuration rules for ProSe services.

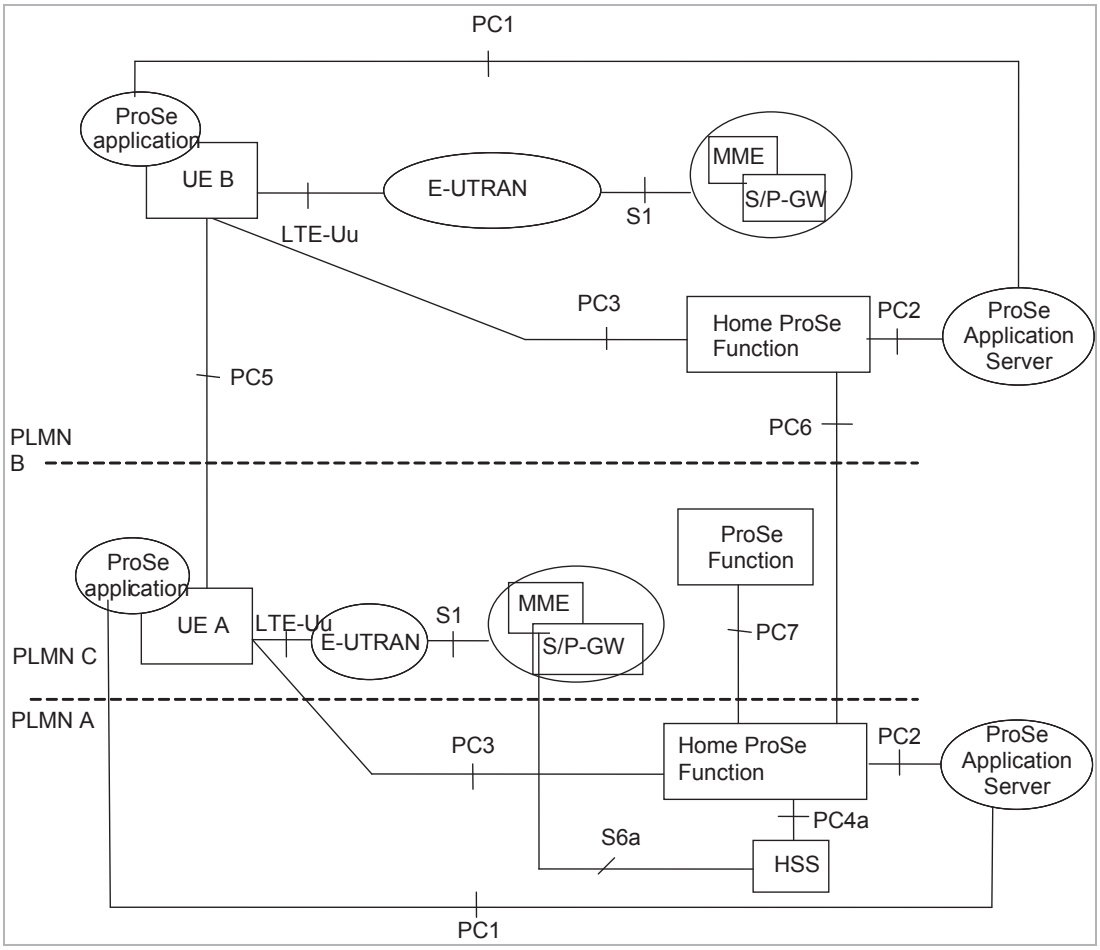

Figure 13: *Reference network architecture for ProSe showing roaming and non-roaming cases. (Source: [22] p. 14).*

5.3.3 Mission Critical Push-to-talk (MCPTT) and Group Communications

Mission Critical Push-to-Talk is a voice service that has been specified by 3GPP in order to enable similar capabilities that are found in Land Mobile Radio (LMR) systems. MCPTT utilizes aspects of ProSe, IMS, and Group Communications System Enablers (GCSE) for LTE [23]. MCPTT services have been specified for on-network (supported by the LTE core network), off-network (UE-to-UE direct mode) and UE-to-network relay modes. Service continuity is specified for on-network and UE-to-network relay modes. The on-network functional model for MCPTT is shown in Figure 14.[14] It illustrates the following client-server associations between the application functions and the UE:

- Media distribution function
- Floor control

[14] The interfaces and functions shown in Figure 14 are not described in this report. They are described in [24].

- Group management
- Configuration management
- Identity management
- Key management

The UEs must be configured with the above clients in order to support MCPTT.

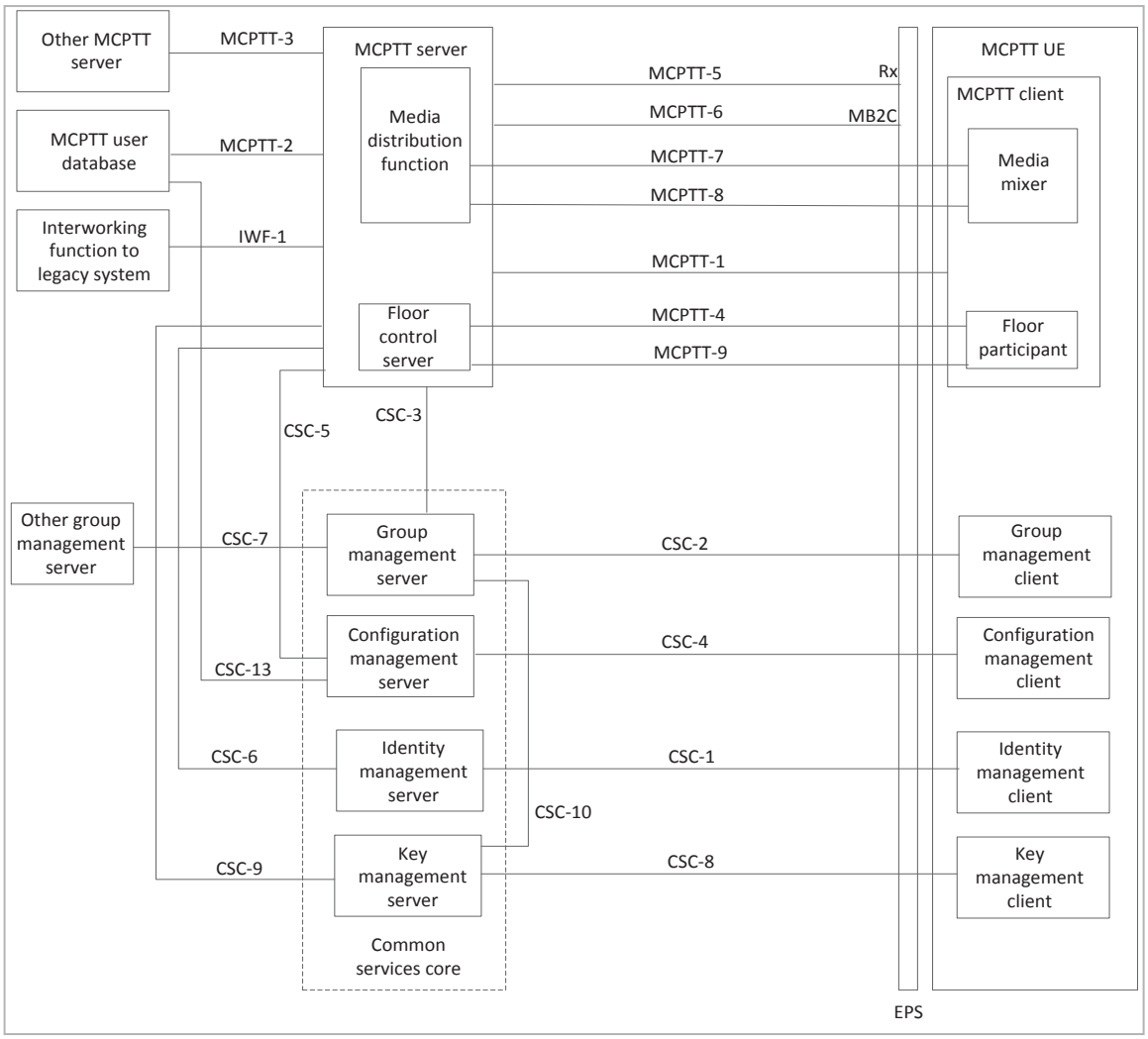

Figure 14: *On-Network Functional Model of MCPTT. (Source: [24]).*

Group Communications Services (GCS) are intended for voice, video, and messaging. Groups can consist of different users and can be members of different agencies. Users can also be in different regions. The 3GPP functional requirements state that groups shall be capable of receiving or transmitting group communication when they are roaming [23 §5.1.8] but it also states that enabling GCS for roaming users is by agreement between MNOs. In the case of Option-A only one agreement is required—between it and FirstNet. In the cases of Option-B and

Option-C, agreements between all regional MNOs would be required, as well as between each of them and FirstNet. With Option-D, since there is no roaming per se between regional MNOs, only an agreement with FirstNet is required to allow users from Canada and the U.S. to engage in cross-border group communications. The agreement can be managed as a national function.

With regards to priority and pre-emption, the 3GPP requires that the LTE network be able to support "n" priority levels for GCS [23 §5.3.4], where "n" has not been specified. The intent is that GCS traffic shall be able to pre-empt lower priority GCS traffic and non-GCS traffic. Each MNO may configure the priority and pre-emption parameters for GCS at its discretion. Interoperability between users within a group that pertain to different PLMNs would require that each MNO enables GCS and that all MNOs configure the priority and pre-emption parameters in the same way. This adds yet another level of coordination and associated cost among the regional MNOs in Option-B and Option-C.

5.3.4 Location Services (LCS)

Location services for public safety are typically associated with the ability to locate and track public safety assets, whether human or machine, and with the ability to locate citizens when they need help. Location data is associated with the UE rather than the actual user. The 3GPP has specified a number of ways that location can be determined for a UE in an LTE network [25]. There are five categories of positioning methods:

a) Network-assisted global positioning and global navigation satellite service (GPS/GNSS) methods. These methods make use of UEs that are equipped with radio receivers capable of receiving GPS/GNSS signals. Positioning computations are performed in the network.

b) Downlink positioning. The downlink observed time difference of arrival (OTDOA) positioning method makes use of the measured timing of downlink signals received by the UE from at least three eNB cells.

c) Enhanced cell ID method (eCID). In the eCID positioning method, the position of a UE is estimated with the knowledge of its serving eNB, the timing difference between transmit and receive signals of its serving eNB, and the receive signal levels from the neighbouring eNBs.

d) Uplink positioning. The uplink time difference of arrival (UTDOA) positioning method makes use of the measured timing at multiple location measurement units (LMU) of uplink signals transmitted from a UE. The LMU measures the timing of the received signals using assistance data received from the positioning server. The resulting measurements are used to estimate the location of the UE.

e) UE-based methods. The UE may contain an independent positioning function (e.g., GPS/GNSS) and thus be able to report its position independent of the E-UTRAN transmissions.

Each method presents performance trade-offs between (i) accuracy of fixing a location, (ii) speed to determine the location, (iii) power consumption of the UE, (vi) the ability to maintain performance over a large number of UEs, i.e., scalability, and (v) the ability to determine location indoors.

In some cases, the location of emergency responders engaged in certain missions can be classified as sensitive information. The Open Mobile Alliance has specified the requirements and architecture for protecting the transfer of location data over an IP-based mobile infrastructure [26]. The Secure User Plane Location (SUPL) architecture utilizes network-assisted GPS/GNSS methods to request location information from the UE or for UE-initiated location "push" data. The SUPL architecture introduces the following additional functional elements:

- SUPL Agent: the entity that initiates the request for location information. It may reside in the UE or in the network.
- SUPL Location Platform (SLP): the entity that is responsible for location service management and determining of the location of the UE. There are several variants of the SLP. The variants are not compared in this report since it is not relevant to its purpose.

The SUPL protocol also uses the Short Message Service Centre (SMSC) and the IMS core network.

Security in the SUPL architecture consists of mutual authentication between the UE and the SLP and the information is protected by transport later security (TLS) or pre-shared key cipher suites for TLS (PSK-TLS).

In the non-roaming case, where the network initiates the location update, the SUPL protocol involves the exchange of messages between four functional entities [26 p. 30]. In the roaming case there are six functional entities involved in the exchange of messages [26 p. 36].

The SUPL function can be hosted by an MNO or it can be outsourced to a 3rd party SUPL provider. In Option-B and Option-C, where the PSBN comprises multiple MNOs, it may be advantageous to outsource the SUPL function. In Option-B and Option-C, there are significantly more instances where users are roaming, hence the performance of LCS would be degraded for those users due to the greater number of communication steps in the SUPL protocol for roaming users.

5.4 Physical Layer Interoperability

Physical layer interoperability pertains to LTE networks that operate next to each other. This report assumes that the networks operate on the same frequency, that is Band-Class 14 (758–768 MHz downlink, 788–798 MHz uplink), which is the frequency band that has been set aside for public safety in Canada and the U.S. When different networks, operating on the same frequency, provide overlapping coverage such as at network boundaries, the signals interfere with each other and performance at these locations is significantly degraded [27].

A number of configuration parameters must be coordinated in order to maximize the probability of a successful hand-over between the eNB of one network and the eNB of an adjacent network [28]. These parameters are:

- physical cell identities (PCI): used in the LTE mobility initial attach and hand-off processes. The PCIs must be unique in all adjoining cells in order to avoid collisions and confusion for which cell the UE is to attach itself to during hand-over.
- uplink reference signals (UL-RS): used to assist in coherent detection and demodulation in the UL control and data streams; used to convey uplink channel quality information to the eNB that allows the eNB to adjust the UL scheduler and perform timing adjustments even in the absence of user data transmissions.
- physical random access channel (PRACH): used to synchronize the timing of the UEs' random access up-link (UL) transmissions to avoid collisions at the receiver of the eNB.

Interference Control

Typically, MNOs of adjoining networks will adjust transmitter power levels and antenna configurations to minimize the interference. But this approach tends to create coverage gaps. In either case, service is likely to be poorer in these locations. The performance at the cell edges can be improved through the use of the X2 interface that would enable enhanced Inter-Cell Interference Coordination. The X2 interface is a point-to-point link between two eNBs. If the eNBs belong to two different MNOs, the question of which MNO is responsible for establishing and maintaining the link should be resolved between them. Currently, such an arrangement between MNOs is rarely encountered since MNOs do not typically pool and coordinate the allocation of their networks' radio resources between them. The X2 interface of the eNBs can also be used to help balance the traffic load between eNBs.

Options comparison

In Option-A, where there is one national operator of the PSBN, the issue of coordinating the assignment of physical layer parameters and the ownership of the X2 links is moot. The national MNO would define the guidelines and the regional operations managers would comply. Since international coordination is required, and where it is desired to maximize the usable capacity of the available coverage along the Canada-U.S borders, the national MNO would need to coordinate the physical layer parameters with FirstNet and enter into an agreement for establishing and maintaining the X2 links.

In Option-B and Option-C, there is an added burden on each MNO to coordinate yet more parameters and guidelines. For the X2 interface the MNOs would need to develop multiple agreements, especially for regions that border more than one other region. Each MNO would also need to coordinate the configuration of physical layer parameters and the X2 links with FirstNet.

In Option-D, the assignment of physical layer parameters could be undertaken as a national function.

5.5 Self-Organizing Networks

The 3GPP has specified the Self Organizing Network (SON) function to help MNOs, intent on densifying their networks, to integrate new cells into their existing fabric in a cost-effective manner [29]. Among other functions, SON is used to optimize the hand-over performance when

the service of a mobile device is transferred from one eNB to another. There are many parameters in the eNBs that need to be adjusted and configured to accommodate the insertion of new ones into existing networks. SON algorithms are intended to automate the task of configuring and adjusting the relevant parameters. The reference architecture for SON is illustrated in Figure 15. It shows that the SON function can be distributed between the network management (NM) layer, the element management (EM) layer, and the network elements—the eNB in this case.

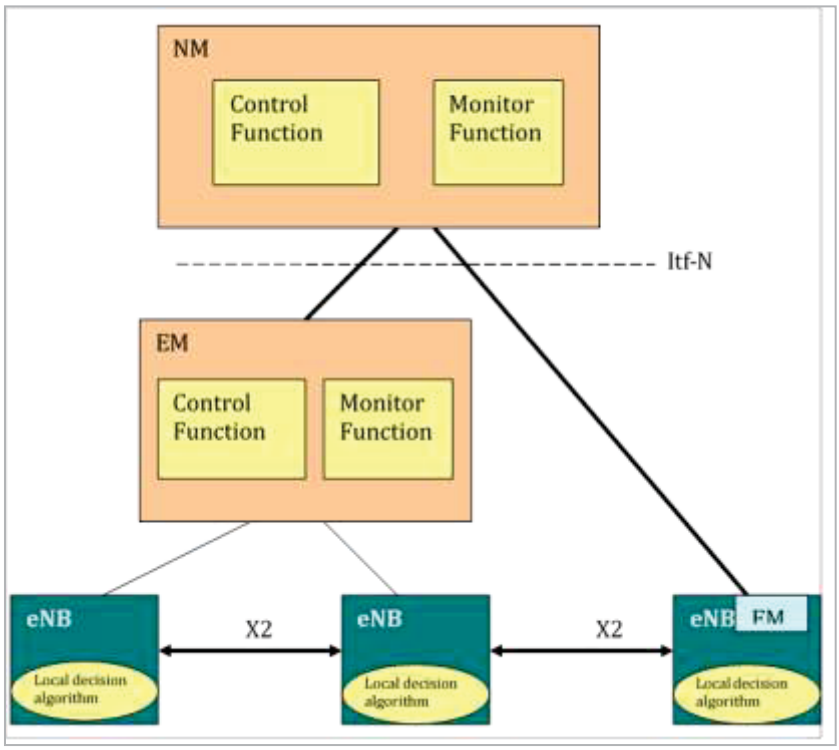

Figure 15: *Illustration of the Self-Organizing Network (SON) Reference Architecture (Source: [29]).*

A major challenge is how to apply SON to a network comprised of eNBs from different vendors. Most vendors of LTE infrastructure offer SON solutions that operate according to their proprietary algorithms[15] and are specific to their products because SON is tightly coupled with the provisioning function of those products. As such, the notion of a hybrid-SON solution is proposed by the 3GPP. The hybrid-SON operates at 2 levels—the distributed SON layer operates at the vendor-specific domain and the centralized-SON layer orchestrates the actions of the distributed-SON functions. The centralized-SON solution is, generally, customized to the requirements of the MNO.

In Option-A, the national MNO would control the design and implementation of the SON solution over a set of vendors that it also controls.

[15] The 3GPP has stated that the definition of the SON algorithms is beyond the scope of its standardization efforts [30].

For Option-B and Option-C, each regional MNO may implement SON solutions in their networks, but the overarching orchestration of the centralized-SON would need to be operated at a level that transcends the SON solutions of each MNO. With no central operating entity in either of these two options, the regional MNOs would need to determine how to procure and host the centralized-SON. If no MNO will host the centralized-SON, then, the MNOs would need to manually adjust and maintain the configurations of their eNBs at their jurisdictional borders where the coverage of their eNBs overlap.

In Option-D, there is the possibility for the centralized-SON function to be hosted as a national function. This is not to say that one national-level SON would orchestrate the distributed SONs for the entire PSBN. But, a number of centralized-SON functions could be instantiated and managed as a national function to orchestrate the vendor-specific SONs that would be implemented by the regional MNOs.

Use of SON with Deployable Systems

Deployable LTE Systems (DS) are expected to complement the PSBN assets and will be used to augment capacity and/or coverage of the PSBN on a temporary or quasi-permanent basis. When an event occurs in areas that are already served by the PSBN, DS can be used to augment the capacity at the incident scene. When an event occurs in areas that are already served by the PSBN but the PSBN has been compromised, DS can be used to provide coverage and capacity at the incident scene. In remote areas, where there may not be coverage from the PSBN or commercial MNOs at all, DS can be used to provide broadband communications services to the response team. When DS are inserted into areas where there is PSBN coverage from fixed sites, there is an expectation that the DS will not degrade the PSBN's performance at those locations. They are also expected to be turned up and operational in as short a time as possible and with the least amount of human intervention as possible.

DS can be dispatched to a site with advanced planning or in response to an unplanned emergency. When events are known to occur several days in advance there is time to plan the deployment, the backhaul, the location, etc. When an unplanned emergency arises, time does not favour planning, and rapid deployment and turn-up of the DS is essential. That means the siting of DS is not necessarily optimal for coverage or to minimize interference with other PSBN sites. In particular, if the event is along a jurisdictional border or between the coverage of separate regional MNOs, there is the possibility of interfering, not only with eNBs within the same jurisdiction of the DS, but across the border as well and with other MNOs.

Recent experiments with 700 MHz deployable LTE systems have shown that, under favourable conditions, a usable signal can propagate for many 10's of km from the DS [31]. While desirable for signal reception, such propagation characteristics also create a challenging interference environment. To further compound the issue, a major incident like a large forest fire or flood could require the dispatching of multiple DSs by multiple jurisdictions. Assuming that the DS can self-organize, another challenge is to be able to authenticate the emergency responders from the various agencies and jurisdictions to access the radio resources of any DS and to enable mobility (seamless hand-over) across the incident area and through the transition between the DS network and the fixed PSBN. Another challenge is to authorize the emergency responders to access the permissible information networks depending on whom the information assets belong to.

The matter of authentication and authorization is one of administrative coordination between jurisdictions. But the issue of inter-working of DS from different vendors and public safety agencies presents more significant technical, administrative, and financial challenges. The assumption that a SON function can operate in a multi-vendor and multi-jurisdictional environment is not currently supported by any standards development organization. Any SON-like solution to enable DSs, from various provenance, to be turned up rapidly with minimal impact on the neighbouring systems is likely to be a custom-designed solution specific to the group of vendors of deployable and fixed network assets that would be tested within a regimen of interoperability sustainment. New vendors' equipment would also need to be tested, as would upgrades to any of the systems within the qualified pool of systems. The systems need to be tested for interoperability with each other and with the SON function. This type of coordination requires deep technical knowledge supported by inter-jurisdictional, and if it were to be the case, inter-regional agreements on policies, procedures, and how funding is to be sourced and allocated.

It is expected that nationally-harmonized operational guidelines will be developed for admitting DS into the pool of qualified network elements of the PSBN. The guidelines would, as a minimum, require day-to-day management of configuration control, inventory, interoperability testing, and the supply chain. For Option-A the functions would be managed by the national MNO. For Option-B and Option-C, there is no actor in the service delivery fabric that would be capable of managing the day-to-day functions for DS at a national level. Hence, the regional MNOs would need to each assume this role. Option-D, on the other hand contains an actor that could undertake this function. This model provides the regional MNOs an avenue to delegate the responsibilities for the day-to-day implementation of the guidelines that would apply to DS.

6 Service Delivery Efficiency

The level of operational efficiency of a network has a direct impact on the costs incurred by a network operator, which in turn affects the price charged for the wireless service. The price charged then affects the long term sustainability of the network since a higher price translates to lower service take-up, and fewer subscribers adds pressure to increase prices for the service. The market dynamic seeks an equilibrium point among the return on investment of the service provider, the price it can charge for the value it delivers, and the size of the pool of subscribers that is willing to pay that price. If an equilibrium point is reached, then the venture is viable. If an equilibrium point cannot be reached, then the venture is not viable.

The service delivery options that are examined in this report are not equal in terms of the cost to carry out their primary mission of enabling nationwide communications interoperability among users with mobile broadband services. Some options are more efficient than others—primarily by reducing duplication of infrastructure and functions across all the regional MNOs. Some options are more amenable to centralizing certain functions that are common across all the regions, thus reducing their capital and operating expenses. Streamlining the operations of the regional MNOs means centralizing the common functions and infrastructure nationally.

The principal infrastructure elements of a PSBN are listed below.

A. LTE Radio Access Network (RAN) elements:

   a) eNB (fixed and deployable)

   b) User equipment

B. LTE Core Network elements—required:

   a) SGW

   b) MME

   c) PGW

   d) PCRF (may be contained in the PGW)

   e) HSS

   f) Authentication Authorization and Accounting (AAA) server

   g) Delivery Function (DF)—support lawful intercept

   h) Deployable RAN and EPC systems

C. LTE Core Network elements for value-added services:

a) ePGW (interface with un-trusted network domains such as public WiFi networks)

b) ProSe Function
c) ProSe Application server

} support Proximity Services

d) MCPTT server
e) MCPTT user database
f) Group Management server
g) Identity Management server
h) Key Management server

} support MCPTT and Group Communications

i) Enhanced Multimedia Broadcast Multicast Services (eMBMS)—support broadcast/multicast

j) User Data Convergence (UDC)—access control of user profile data by applications

k) Service Capability Exposure Function (SCEF)—access control of network services by applications

D. Non-LTE Core Network elements—required:

a) IMS—support VoLTE, MMS

b) Short Message Service Centre (SMSC)—support SMS messaging

c) MVPN server—support MVPN services

d) Network Time server

e) Diameter Routing Agents

f) Dynamic Host Configuration Protocol (DHCP)

g) Domain Name Service (DNS)

E. Non-LTE Core Network elements for value-added services:

a) SUPL Location Platform—support sensitive location services

b) Location Measurement Unit (LMU)—support UTDOA location methods

c) Cell Broadcast Centre (CBC)—support Cell Broadcast Service

d) ICAM service

F. Operations/Business Support Systems and Network Management:

   a) SON (distributed function and central function)

   b) Billing system

   c) Performance Management

   d) Trouble Ticketing and Fault Management

   e) Inventory and Configuration Management

   f) Provisioning system

   g) Mobile Device Management system

   h) IP address management

   i) Network Identifiers management

G. Network Security elements:

   a) Security Information and Event Management (SIEM) server

   b) Intrusion Protection, Intrusion Detection Systems

   c) Network Address Translation

   d) Security Gateways

   e) Routers/Firewall

The determination of which PSBN entities are responsible for which functions and PSBN infrastructure is driven by the service delivery model. For all Options A, B, C and D, the radio access network (A) of the PSBN would be the responsibility of the regional component of the network (Regional Operations in Option -A and MNOs in Option-B to Option-D). For all functions and infrastructure pertaining to the Core Network, both required and value-added, as well as the OSS/NM and Network Security (B–G), ownership of responsibility is driven primarily by the choice of the service delivery model. In the case of Option -A, it would be assumed by the national MNO. In Option-B and Option-C, it would be the regional MNOs. In the case of Option-D, some CN functions could be operated nationally, but would need to be coordinated between the MNOs.

Table 2: *PSBN infrastructure elements for each Option.*

PSBN Infrastructure Elements	Option-A		Option-B		Option-C		Option-D	
	Regional Operation	National MNO	Regional MNOs	National Proxy	Regional MNOs	National Proxy	Regional MNOs	National Proxy
LTE Radio Access Network (RAN)	✓		✓		✓		✓	
LTE Core Network elements		✓	✓		✓		✓	✓
LTE Core Network elements for value-added services		✓	✓		✓		✓	✓
Non-LTE Core Network elements		✓	✓		✓		✓	✓
Non-LTE Core Network elements for value-added services		✓	✓		✓		✓	✓
Operations/Business Support Systems/Network Mgmt		✓	✓		✓		✓	✓
Network security elements		✓	✓		✓		✓	✓

Option-A, as a single national MNO, represents the most streamlined service delivery model of the four that are considered in this report. The MNO is singularly responsible for operating the PSBN and, as such, can centralize as much of the infrastructure and functions of the PSBN and reduce as much duplication as it deems necessary while satisfying its regulatory and contractual obligations. Assuming the national MNO offers commercial mobile services, many of the organizational functions required to operate the PSBN can be shared with its commercial operations. The cost impact of operating the PSBN, as an addition to its overall operations, can be allocated to its public safety line of business. Despite its apparent advantage for streamlining operations, important concerns for Option-A are associated with the lack of regional autonomy and vendor lock-in, as discussed later in this report.

Option-B and Option-C are the least efficient service delivery models since the national coordination body would not assume any day-to-day operational functions and would not host any network infrastructure. Hence, each MNO must host all the infrastructure components of a fully independent stand-alone network and employ the associated staff to operate and manage those functions. Furthermore, Option-C imposes a non-standard roaming model that, besides the risk that it will not be acceptable to potential roaming partners, entails greater operating expenses with regards to the IPX.

Option-D offers the possibility to centralize a portion of the CN infrastructure and operating functions, but must be done in concert by all the regional MNOs. In the most streamlined state of this option, the regions can be solely responsible for the RAN. However, since it is assumed that the PSBN would be shared with commercial users, it is the authors' opinion that it would be unlikely for the regional MNOs to relinquish the operations and management of the PSBN CN in its entirety to a 3rd party, even if that 3rd party were to be a joint-venture created by them.

Vendor Lock-in

An important consideration for service delivery efficiency is "vendor lock-in". Vendor lock-in is equivalent to a monopoly, which is generally not conducive to operational efficiency and is less responsive over time to user needs due to the lack of competitive pressures. It is posited by the authors that a service delivery option is more efficient if multiple players are allowed to compete for operating the PSBN on behalf of the regional licensees. The barrier to re-compete or re-tender the operation of the PSBN at the regional, multi-regional or indeed, national level is not the same

for every service delivery option. This section examines the relative barriers to competition for each option.

With Option-A, the national MNO would have likely obtained a contract to implement and operate the PSBN for a significantly long period of time. By way of comparison, Airwave Solutions obtained a 20-year contract for the United Kingdom's Terrestrial Trunked Radio (TETRA) network. FirstNet's Request For Proposal (RFP) states that the duration of the Covered Lease Agreement with its contractor would be 25 years.[16] The contracts may include incentives to achieve certain objectives and penalties for those that are missed, but, fundamentally, this arrangement removes a significant amount of negotiating leverage from public safety to deviate from a service roadmap once it is set in the contract—and for a considerably long time. This is not to suggest that no changes can be made, but the public safety community's leverage would be weak. Assuming that the contract allowed for it to be re-competed for whatever reason, the barrier to re-compete a national contract is the highest among the four options—requiring agreement by all or a majority of the stakeholders to re-compete and select the winning bidder. The contractor would need to implement new PSBN infrastructure nationwide. Transitioning the service from one MNO to a new one would be highly complex, especially because the frequency band is unchanged from the incumbent MNO to the new MNO.

With Option-B, Option-C and Option-D the barrier to re-compete a service delivery contract is lower because it needs only to be considered at the regional level. Option-D would have a marginally lower barrier than Option-B and Option-C because part of the infrastructure would be operated as a national function. As a result, the capital cost for the regional portion of the PSBN would be lower with Option-D, and the residual depreciated value of the regional infrastructure, being a function of the capital cost, would also be lower at any point in time.

An interesting competitive scenario would arise for Option-B, Option-C and Option-D in the case that the regional MNOs would be prohibited from charging roaming fees to public safety users from other regions. In this case, by allowing public safety agencies the freedom to purchase their service from whichever regional MNO gives them a better offer, it would reduce the ramifications of vendor lock-in. However, an important barrier is that the UICCs in all the user devices would need to be changed. But that barrier is likely to fall when embedded UICC (eUICC) modules will migrate from Machine-2-Machine applications to smartphones. eUICC allows the home MNO to be changed without having to physically replace the UICC module. The change can be performed remotely and is effected over the air [32].

[16] Airwave Solutions: https://www.airwavesolutions.co.uk/home/FirstNet: http://www.firstnet.gov/news/firstnet-issues-rfp-nationwide-public-safety-broadband-network.

7 National Interoperability Functions for the PSBN

The previous section described the essential elements of an LTE network for public safety. It examined how those service delivery options that are more conducive to centralizing some of the infrastructure of the PSBN would improve service delivery efficiency. This section examines the national functions that are required to support interoperability and for which interoperability standards should be developed. These national functions are either administrative or operational in nature.

All the service delivery models that are described in §3 contain a national coordination body with an implied national scope of responsibility with regards to interoperability standards. The actual functions of the national coordination body are administrative in nature, whose scope depends on the service delivery option. In service delivery Option-A, these administrative functions would be shared between the national coordination body and the MNO, whereas all operational functions would be the responsibility of the MNO. In service delivery Option-B and -C, all the administrative functions would be the responsibility of the national coordination body. Furthermore, from an operational perspective, there is no national actor that can assume a central role in day-to-day interoperability functions. In these options, it is already a significant undertaking for an MNO to ensure that all the network elements, user devices, software and applications are able to function together in its own service domain and to maintain interoperability over time as vendors change, as products change and as new features are introduced. Achieving and sustaining nationwide interoperability would be even more challenging due to the lack of an operational function at the national level as well as the increased scope of responsibility of the national coordination body. This is further compounded if the PSBN service were to be delivered by multiple independent MNOs where each has its own regional focus. In service delivery Option-D, the administrative functions would be shared between the national coordination body and the regional MNOs' national proxy, whereas all national operational functions would be the responsibility of the national proxy.

The following lists the fundamental functions for national interoperability.

NF.1. The allocation of MSIN, International Mobile Equipment Identity (IMEI), and Mobile Station International Subscriber Directory Number (MSISDN) ranges for each region.

NF.2. The allocation of LTE Network Identifiers:

i. E-UTRAN Cell Global Identifier (ECGI),

ii. Tracking Area Identity (TAI),

iii. Globally Unique MME Identity (GUMMEI), and

iv. MME Group Identifier (MMEGI).

NF.3. Assignment of Access Point Names (APN).

NF.4. Manage the assignment of Physical Cell Identities to eNBs, Up-Link Reference Signals, Zadoff Chu root sequences for Random Channel preambles to optimize the hand-over success rate when moving between cells pertaining to different regions.

NF.5. Define the assignment of Quality of Service (QoS) parameters:

i. Allocation Retention Priority (ARP),

ii. QoS Class Identifier (QCI),

iii. Access Class Control (ACC),

iv. Differentiated Services Code Point (DSCP),

v. Multiprotocol Label Switching (MPLS) Traffic Class (TC),

vi. Policy Control and Rules Functions (PCRF), and

vii. Traffic Flow Templates (TFT).

NF.6. Manage the configuration parameters of Session Initiated Protocol (SIP) User Agents in UEs (for VoLTE).

NF.7. Manage the assignment of the IP Multimedia Private Identity and the IP Multimedia Public Identity in the UICC; used for IMS.

NF.8. Manage the requirements for Application Programming Interfaces (APIs).

NF.9. Manage the data models for the exchange of user subscriber information between regions (User Data Convergence—Ud interface).

NF.10. Manage the requirements for Location Services.

NF.11. Manage the requirements and interfaces to external networks for Lawful Intercept.

NF.12. Apply for the MNC and maintain compliance with the obligations of the associated Agreement.

NF.13. Manage the requirements that enable MCPTT and Group Communications on all regional networks.

NF.14. Manage the configuration parameters for the ProSe Function in the core network.

NF.15. Manage the configurations of the Key Management Server in the core network for ProSe.

NF.16. Manage the configurations of the inter-regional Security Gateways.

NF.17. Manage the requirements for multi-vendor and multi-jurisdictional interoperability of Self Organizing Networks applications.

NF.18. Manage the IP Addressing scheme.

NF.19. Manage the contract with the IP Exchange and Clearinghouse for international roaming.

NF.20. Manage the spectrum sharing agreement with FirstNet.

NF.21. Provision the S10 interconnections (MME-MME) for service continuity during hand-over between regions.

NF.22. Provision the X2 interconnections for enhanced Inter-Cell Interference Coordination (eICIC)—interference mitigation at the inter-regional coverage overlap areas.

NF.23. Provision the inter-regional transport networks. Tendering and managing the contracts with 3rd party providers of high capacity backbone networks.

NF.24. Monitor the performance of the inter-regional transport networks.

NF.25. Manage the requirements and the supply chain for user devices.

NF.26. Manage the requirements and the supply chain for deployable systems.

NF.27. Provision the ProSe parameters in the UICC.

NF.28. Host the national IMS core network—VoLTE, Multi-Media Service (MMS) and Short Message Service (SMS).

NF.29. Host a national HSS. (Avoids inter-regional roaming.)

NF.30. Host a national Identity Credentials and Access Management (ICAM) solution.

NF.31. Host a national PSBN MVPN solution.

NF.32. Synchronize the national PSBN VPN servers with FirstNet VPN servers to enable incident-specific interoperability during cross-border mutual aid.

NF.33. Host a national Security Operations Centre.

NF.34. Manage a national Security Policy for the PSBN.

NF.35. Conduct audits of regional partners for adherence to the Security Policy.

NF.36. Provision and manage the interconnection of Federal information networks to the PSBN.

NF.37. Host the Change Control Board to verify requests for changes to hardware, firmware, applications and configurations of network elements that could impact interoperability.

NF.38. Manage an Interoperability Test facility to support the Change Control Board.

Each national interoperability function would be associated with one or more interoperability standard. Standards would serve as the basis of agreements between the parties on how the functions will be performed such that nationwide interoperability is achieved. It limits the degrees of freedom for each party to deploy and manage the regional networks for those configuration points that impact interoperability. As an example, NF6 from the above list of functions addresses the configuration parameters for the SIP User Agent (SIP-UA) contained in the user devices. As explained in §5.3.1, there needs to be a nationwide standard for how the SIP-UA should be configured in order for users to be able to engage in voice-over-LTE (VoLTE) sessions with other PSBN users. Furthermore, if it is desirable for public safety users from the USA to engage in VoLTE sessions with Canadian users when they are operating in Canada, their devices needs to be configured the same way. Hence, the agreement on interoperability standards is not only between the implicated actors in Canada, it may also include FirstNet in the USA. Clearly, the actors are not free to decide how to configure as they wish many parameters that pertain to their networks, where SIP-UA is but one example. An additional important consideration on interoperability standards is that they will evolve over time, especially during the infancy of the PSBN as the MNOs discover errors and gaps that need to be addressed quickly. In service delivery Option-A the responsibility to maintain the interoperability standards would be held within its internal operations. With Option-B and Option-C, it could be undertaken by the national coordination body assuming it is suitably staffed and funded to assume this role. Option-D allows for the responsibility to be shared between the national coordination body and a national proxy of the regional MNOs.

The adherence to interoperability standards also has financial considerations for the MNOs. While some administrative coordination of the interoperability standards could be done by multi-functional bodies, interoperability sustainment requires physical space, tools, assets, and dedicated resources. In Option-A, where there is one national PSBN operator, it would factor the cost of interoperability sustainment into its business plan. Even if the function is out-sourced there would be a role in the MNO's organization that would be accountable for ensuring interoperability. In Option-B and Option-C, where the PSBN is realized by multiple independent MNOs, interoperability assurance is more complicated due to the multiple parties involved and hence, the potential for different approaches to operating and maintaining their networks. Within these options there is no identifiable actor where a joint responsibility and accountability for interoperability sustainment could be assigned. As this requires on-going investment, the sustainment roadmap would need to be aligned across all the regional MNOs. The authors of this report contend that such an alignment would be very challenging due to uncorrelated business strategies driven primarily by their separate commercial business interests, desires to achieve competitive differentiation, and differences in their balance sheets. As a practical example, some MNOs may have rural expansion higher in priority while others may have operation support systems (OSS) productivity improvements higher in priority.

Option-D could be designed so that a national proxy would be empowered, funded and held accountable for interoperability sustainment. In this way, a nationally-harmonized strategy would be achievable, albeit a negotiated one because of the disparity in the capacity of each regional MNO to invest in interoperability sustainment.

8 Conclusion

The four service delivery options that are examined in this report have been evaluated primarily from the perspectives of interoperability, a critical requirement of PSBN. A comparative assessment of service delivery efficiency has also been done. A common thread throughout this report is the notion of delivering sustainable value to the stakeholders. This is a key consideration since any service delivery model imposes a cost structure that affects the price to the subscriber and ultimately, the economic viability of the PSBN. Although sharing the PSBN with commercial users will greatly contribute to its viability and sustainability, the MNO's cost of operations must also be optimized to the greatest extent possible. Some service delivery models limit what is possible to accomplish in terms of operational efficiency and hence, are at greater risk of not being viable. While there may be other dimensions that could have been factored into the analysis, the authors posit that the ones considered in this report are extensive and allow for an effective comparison of the service delivery options.

A national proxy that centralizes some of the functions of separate MNOs is a novel construct that does not currently exist in the commercial wireless space. The effectiveness of having independent MNOs coordinate their service delivery through a national coordination body is also untested and, therefore, unproven and as such, all four options described herein are untested and unproven. Nevertheless, a model that facilitates cooperation among MNOs would present less risk to asserting and sustaining interoperability over the lifespan of the PSBN. At the limit, the PSBN served by a single MNO presents the lowest risk to interoperability but could experience an increasing erosion over time of value-to-price ratio.

Table 3 summarizes the analysis that is presented in this report and compares the 4 service delivery models for 3 key attributes:

A. Interoperability,

B. Service delivery efficiency, and

C. Viability and sustainability.

While attributes B and C are related, there is an important distinction to be made with regards to being able to deliver services efficiently and the ability to do so while delivering value over the long term. This is explained more fully in the discussion of the attributes for each dimension that follows.

A.1 Interoperability Risk: This attribute addresses the ease with which interoperability standards can be established and complied with by the MNOs. It also addresses the ability to sustain interoperability over time. Accountability for compliance is also a consideration. Option-B and Option-C would present a greater risk to interoperability than Option-A and Option-D. Option-A would have the least risk because interoperability standards are managed within a single organization. There is no need to coordinate between multiple actors. Although not as low risk as Option-A, Option-D also presents low risk since interoperability standards would be managed by the national proxy.

A.2 Interoperability with FirstNet and Commercial Carriers: This attribute consists of the ease with which the standards that impact interoperability with FirstNet and carrier partners can be harmonized. It consists of being able to converge effectively to agreement on those standards and to be able to address issues as effectively. The service delivery options that require multiple PSBN MNOs to negotiate the standards with FirstNet and other partners is not as effective as the service delivery options that only require one entity from Canada, representing the PSBN, to interact with them. That entity should be empowered to bind the PSBN MNOs in the agreement with their partners. Option-D, by virtue of the national proxy, can be as effective as Option-A if the MNOs would allow their national proxy to enter into such agreements.

A.3 Inter-regional Inter-working (Network Level): This attribute consists of the ease with which interoperability standards that apply to overlapping coverage of adjoining regional networks can be managed. It also addresses the interconnection of interfaces that are not standard roaming interfaces. As such, the MNOs would need to deviate from what they normally do with other commercial partners. Examples are the interconnection of the S10 interface between MMEs and the X2 interface between eNBs. These are not normally exposed by MNOs to their competitors. In Option-A there is no need to expose these interfaces, except to FirstNet. A national proxy in Option-D would alleviate the issue with the S10 if it was delegated the responsibility to operate the MMEs for the PSBN.

A.4 Ability to Support Federal Users: This attribute covers two aspects of support for Federal users. The first is the ability to provide a trusted connection to Federal information networks to the PSBN. This can be done at the PGW using a dedicated APN. The user plane traffic for each bearer in the LTE network is carried in its own separate tunnel from the SGW to the PGW using GPRS Tunneling Protocol (GTP).[17] One APN would be assigned for Federal information networks nationwide. For Option-B and -C one of the regional MNOs would need to provide the PGW for the Federal APN. Option-D allows for a national proxy to host the PGW that serves the Federal information networks. The architecture for the PSBN that supports this was proposed in the DRDC CSS' PSBN Network Architecture Description [5]. Option-A would have a PGW within the MNO's network to connect to the Federal information networks. The second consideration for Federal users deals with the MVPN service as discussed in §5.1. Option-B and Option-C are less able to support interoperability for MVPN-protected user data than Option-A and Option-D, assuming that the latter offer national MVPN hosted solutions.

A.5 Ability to Harmonize Network Operations Policies: This attribute addresses the ease with which network operations polices can be agreed upon and harmonized across all MNOs. The issue is similar to A.2 in that it becomes more difficult to reach an agreement in proportion the number of parties to the agreement, and it will undoubtedly be necessary to change the agreement from time-to-time. For Option-B and Option-C the national coordination body would need to broker the agreements between the regional MNOs. Option-D would make it easier to harmonize network operations policies, but only if the national proxy was empowered to oversee the development of the standard network operations procedures and ensure their implementation. Mainly those policies that have a direct bearing on interoperability would need to be harmonized. Those policies would, as a minimum, define the target states and objectives for the parameters listed in §7.

[17] GTP does not encrypt the user data.

A.6 Nation-wide Service Accessibility: This attribute addresses the ability for users to access PSBN services anywhere within the footprint of the PSBN in Canada and on Canadian commercial MNOs when they are out of reach of the PSBN. All options with the exception of Option-B can provide access through any regional MNO and by agreement with commercial MNOs. Option-B is limited because the eNB can only broadcast a maximum of 6 PLMN IDs. Option-B can potentially have up to 13 PLMN IDs.

B.1 Degree of Duplication of Infrastructure: The least amount of duplication in infrastructure is with Option-A. With Option-B and Option-C infrastructure can be duplicated by as many MNOs as there are in the PSBN and by the redundancy in each MNO for resiliency. Option-D can alleviate a substantial level of duplication but cannot be as streamlined as Option-A.

B.2 Ability to Offer Nationally-hosted Value Added Services (VAS): Some examples of VAS are MVPN, VoLTE, MCPTT, SMS and MMS, and LCS. To the extent that such services can be offered at the national level relieves the cost burden of having to host them regionally or at the agency level. Option-B and Option-C cannot offer any nationally-hosted services. Option-A and Option-D could offer them.

B.3 Ease of Inter-carrier Roaming: This attribute addresses how the MNOs would interface with roaming partner networks. By adhering to standard roaming interfaces, an IPX can facilitate the establishment of roaming agreements. Option-A would have no issue. Option-B is incompatible with the current CRTC guidelines for the assignment of MNC for the PSBN, which clearly state that only one MNC will be assigned for the PSBN. However, there is always the possibility that the CRTC can change the guidelines, however unlikely that may be given the limited number of available MNC resources remaining in Canada. Option-C is non-standard and requires special treatment by the IPX and also requires approval by whichever other network the regional MNOs would want to partner with. Option-D can present standard interfaces for roaming.

C.1 MNO Lock-in; Ease to Re-compete: Option-A presents the highest barrier for the stakeholders to re-compete the contract for PSBN services. If the MNOs were prohibited from charging roaming fees then Option-C and Option-D could facilitate competition among the MNOs. Option-B would require a change of UICC across the fleet of devices used by the agency that decides to switch MNO.

C.2 Viability of the Service Delivery Model: This attribute addresses the ability for an MNO to succeed commercially. If Option-A were to become a 4th national MNO in Canada, its viability is highly questionable based on the small number of public safety users and the likelihood that it would discount the price of service to commercial users because of priority and pre-emption encumbrance on the value of the spectrum for commercial use [34]. If Option-A were to be implemented by an existing national wireless carrier, the PSBN would form a separate network but the additional PSBN spectrum would be folded into its inventory. There is no recent precedent for a wireless carrier to be awarded a nation-wide concession on 20 MHz of spectrum. Option-B is highly unlikely due to wastefulness of MNC resources. Option-C and Option-D could be viable if MNOs can serve groupings of provinces and territories, hence there would be fewer than 13 MNOs but, Option-C would have a higher cost structure than Option-D as noted in B.1.

Table 3: *Comparison of the ability to support key attributes of the Service Delivery Models.*

		Option-A One National MNO One PLMN ID	Option-B Regional MNOs Multiple PLMN IDs	Option-C Regional MNOs Shared PLMN ID	Option-D National Entity; Regional MNOs; One PLMN ID
A	**Interoperability Considerations**				
A.1	Interoperability risk				
A.2	Interoperability with FirstNet				
A.3	Inter-regional inter-working (network)				
A.4	Ability to support Federal users				
A.5	Ability to harmonize Net.Ops Policies				
A.6	Nation-wide service accessibility				
B	**Service Delivery Efficiency**				
B.1	Degree of duplication of infrastructure				
B.2	Ability to offer nationally-hosted VAS				
B.3	Ease of inter-carrier roaming				
C	**Sustainable Value**				
C.1	MNO lock-in; ease to re-compete.				
C.2	Viability of the Service Delivery Model				

Legend: Green = most amenable to support the attribute.
Yellow = can support the attribute with reservations.
Red = least able to support the attribute.

In summary, Option-B and Option-C present significant risks to interoperability and are the least efficient ways to deliver mobile broadband services. Option-A, while presenting the least risk to interoperability and is the most cost-efficient model, has significant long-term viability concerns due to vendor lock-in and, fundamentally, a difficult business case for a new national carrier. Option-D, while not superior in all attributes, represents the best alternative and is anchored on the presumption that national functions and some core infrastructure can be centralized in support of the regional MNOs.

References

[1] Public Safety Canada, “Communications Interoperability Strategy for Canada”, 2013.

[2] Canadian Steering Committee on Numbering (CSCN), “Canadian International Mobile Subscription Identity (IMSI) Assignment Guideline”, version 5.0. Approved by Telecom Decision CRTC 2015-496, 06 November 2015.

[3] Conférence européenne des administrations des postes et télécommunications (CEPT) – Electronics Communications Committee (ECC), “Evolution in the Use of E.212 Mobile Network Codes”, ECC Report 212, 09 April 2014.

[4] 3GPP TS 23.251, “Network Sharing; Architecture and Functional Description”, (Release 13), V13.2.0, June 2016.

[5] DRDC CSS TR 2013-009, “Public Safety Broadband Network Architecture Description”, Defence R&D Canada, 01 August 2013.

[6] GSMA IR.88, “LTE and EPC Roaming Guidelines” Version 13.1, 16 June 2015.

[7] DRDC CSS, “Public Safety Broadband Network – Catalogue of Use-Cases and User Requirements”, unpublished draft.

[8] Internet Engineering Task Force (IETF), RFC 6733, Standards Track, “Diameter Base Protocol”, October 2012.

[9] GSMA IR.21, “Roaming Database, Structure and Updating Procedures”, Version 9.1, 05 July 2013.

[10] IETF RFC4301, “Security Architecture for the Internet Protocol”, December 2005.

[11] IETF, RFC4302, “IP Authentication Header”, December 2005.

[12] IETF, RFC4303, “IP Encapsulating Security Payload”, December 2005.

[13] NIST SP 800-63-1, “Electronic Authentication Guideline”, December 2011.

[14] Information Sharing Environment (ISE), “Introduction to ICAM Principles: Identity, Credentials, and Access Management”, Office of the Director of National Intelligence (USA).

[15] 3GPP TS 23.228: “IP Multimedia Subsystem (IMS); Stage 2 (Release 13)”, June 2015.

[16] IETF RFC6011, “Session Initiation Protocol (SIP) User Agent Configuration”, October 2010.

[17] GSMA IR.65, “IMS Roaming and Interworking Guidelines”, Version 8.0, May 9, 2012.

[18] 3GPP TS 23.203, “Policy and Charging Control Architecture (Release 13)”, June 2015.

[19] 3GPP TS 24.008, “Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (Release 13)”, June 2015.

[20] 3GPP, TS 23.216, “Single Radio Voice Call Continuity (SRVCC); Stage 2”, (Release 13), V13.1.0, December 2015.

[21] 3GPP TR 26.916, “Media handling and Quality aspects of SRVCC”, (Release 14), V14.1.0, June 2016.

[22] 3GPP TS 23.303, “Proximity-based Services (ProSe); stage 2 (Release 13)”, June 2015.

[23] 3GPP TS 22.468, “Group Communication System Enablers for LTE (GCSE_LTE (Release 13)”, December 2014.

[24] 3GPP, TS 23.179, “Functional architecture and information flows to support mission critical communication services; Stage 2”, (Release 13), V13.2.0, June 2016.

[25] 3GPP TS 36.305, “Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN (Release 12)”, December 2014.

[26] Open Mobile Alliance, “Secure User Plane Location Architecture”, OMA-AD-SUPL-V3_0-20110920-C, September 20, 2011.

[27] M. Rahman, H. Yanikomeroglu, and W. Wong, “Interference Avoidance with Dynamic Inter-Cell Coordination for Downlink LTE System”, IEEE Wireless Networking and Communications Conference, 2009.

[28] J. Salo, M. Nur-Alam, and K. Chang, “Practical Introduction to LTE Radio Planning”, 2010.

[29] 3GPP TS 32.522, “Telecommunication management; Self-Organizing Networks (SON) Policy Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS) (Release 11)”. September 2013.

[30] 3GPP TS 32.500 “Telecommunication Management; Self-Organizing Networks (SON); Concepts and requirements”, Release 12, V12.1.0, December 2014.

[31] S. Braham, “Field Operational Test Facility for Next-Generation Interoperable Mission-Critical Communications”, February 2015.

[32] GSMA, SPG.02, “Remote Provisioning Architecture for Embedded UICC Technical Specification”, Version 3.1, 27 May 2016.

[33] 3GPP TS 22.011 “Technical Specification Group Services and System Aspects; Service accessibility (Release 13)”, V13.1.0, September 2009.

[34] U.S. Office of the Inspector General Report to the FCC regarding “D Block Investigation”, 25 April 2008.

Annex A Public Land Mobile Network Identifier

The PLMN ID is a globally unique 6-digit number that is used to distinguish one public mobile network from any other public mobile network in the world. The structure of the PLMN ID is shown in Figure A.1 and a partial list of PLMN IDs assigned to Canadian wireless operators is given in Table A.1. The PLMN ID comprises a 3-digit (decimal) Mobile Country Code (MCC) and a 3-digit Mobile Network Code (MNC). The Telecommunications Standardization Bureau of the International Telecommunication Union assigns MCCs for public networks. Canada is assigned MCC = 302. In Canada, the MNC is administered by the Canadian Numbering Administrator by authority of the CRTC.

Roaming is the ability for a mobile device to continue to access services when travelling outside its home network, by means of using a visited network. It is either enabled or blocked according to information stored on user devices' (UE) universal mobile telecommunications system (UMTS) subscriber identity modules (USIM). The USIM contains the Home PLMN ID (HPLMN) to which the UE belongs, as well as a list of permitted PLMN IDs and a list of prohibited PLMN IDs. The permitted PLMN IDs represent the wireless networks that the UE is able to connect to. There is also the possibility to identify which operators are preferred among the permitted operators. The USIM may contain a list of Equivalent HPLMN (EHPLMN). When the EHPLMN list is present, any PLMN in that list shall be treated as the HPLMN in all the network and cell selection procedures [33 §3.2.2.1].

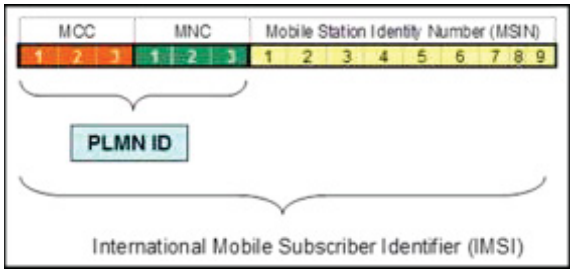

Figure A.1: *Structure of the PLMN ID.*

Table A.1: *Partial list of PLMN IDs assigned to Canadian wireless operators.*

PLMN ID						
MCC			MNC			Name of Operator
3	0	2	6	1	0	Bell Mobility
3	0	2	6	4	0	Bell Mobility
3	0	2	2	2	0	Telus Mobility
3	0	2	2	2	1	Telus Mobility
3	0	2	8	6	0	Telus Mobility
3	0	2	3	6	0	Telus Mobility
3	0	2	7	2	0	Rogers Wireless
3	0	2	4	9	0	Globalive Wireless
3	0	2	6	6	0	MTS Mobility
3	0	2	7	8	0	SaskTel Mobility

This page intentionally left blank.

Annex B Contents of GSMA Roaming Agreements

"The scope of the Roaming Exchange (RAEX) database is as follows (copied from GSMA IR.21):

- Organization Information:
  - The Organization Name
  - The Operators home country in abbreviated format
  - Information for each Network(s), Roaming Hubbing and Hosted Network belonging to the Organization
  - The Transferred Account Data Interchange Group (TADIG) code used by the operator according to TD.13[18]
- Network Information
  - SE.13[19] Database information: the Technology and the Frequency used by the operator, Presentation of Country initials and Mobile Network Name, the abbreviated Mobile Network name, the Network Colour code and the (U) SIM header information.
- Numbering Information
- International and Domestic signalling connection control point (SCCP) gateway (GW) information
- Type of SCCP protocol available at public mobile network (PMN)
- Information about Subscriber Identity Authentication
- The test number available at PMN for service testing
- The information concerning introduction of mobile application part (MAP), a list of the Application Context with the current version and the time planned for changing to the next higher version
- Addresses of network elements with Time Zone information
- Information about Unstructured Supplementary Service Data (USSD)[20] availability and the supported phase
- Customized Applications for Mobile networks Enhanced Logic (CAMEL) Application Part (CAP) version
- Information associated with general packet radio service (GPRS) network identifiers, such as access point name (APN) operator identifier, list of test APNs, Data Service supported with Class Capabilities etc.

[18] GSMA TD.13, "TADIG Code Naming Convention".
[19] Replaced by GSMA TS.25, "Mobile Network Codes and Names Guidelines and Application Form".
[20] 3GPP TS 22.090, "Unstructured Supplementary Service Data".

- Information associated with IP Roaming and IP interworking towards the GPRS roaming exchange (GRX) provider, such as domain name service (DNS) IP addresses/names (primary and secondary), IP address range(s), autonomous system (AS) Number, etc. of the PMN
- Mobile multimedia service (MMS) Inter-working and wireless local area network (WLAN) Information
- Detailed numbering information where needed
- Information about contact persons listed by service and troubleshooting contacts
- Information related to any type of Hosted Network, including non-terrestrial and satellite. Available information are: TADIG code, Global Title Addresses, Mobile Station Roaming Number (MSRN) Ranges and IP Address Ranges
- Information for LTE Roaming

Each category listed above is further composed of more detailed information. As an example, the last item in the above list "information for LTE Roaming" consists of:

- Roaming interconnection information: IP address of Diameter Edge Agent, information on S6a, S6d, S8, S9.
- Short Message Service (SMS) delivery mechanism: SMS over IP, SMS over SGs.
- Voice services: IP multimedia sub-system (IMS), circuit-switched fall-back (CSFB), other.
- Roaming retry.
- Roaming scenarios for LTE-only, 2G/3G roaming.
- QoS profiles: QoS Class Identifier (QCI), allocation retention priority (ARP), pre-emption vulnerability, pre-emption capability, maximum uplink and downlink bit rates, guaranteed uplink and downlink bit rates.
- IPv6 connectivity for mobility management entity (MME), serving gateway (SGW), packet gateway (PGW).
- IP address of IPsec gateways; availability of security certificates.

The roaming agreement template consists of 3 parts. They are,

a) AA.12 International/National Roaming Agreement: General Terms and Conditions

b) AA.13 International/National Roaming Agreement – Common Annexes: contains articles that are specific between the two roaming partners.

c) AA.14 International/National Roaming Agreement – Individual Annexes: published by an MNO and contains items that apply to all roaming that occurs on its network.

Examples of the contents (not exhaustive) of the roaming agreements are:

- Agreed settlement procedure (e.g., Direct Payment, Netting)

- Security
- Signaling Interconnection and/or IP Connectivity
- Data Privacy
- Fraud Prevention Procedures
- Contacts
- Services available
- Inter Operator Tariffs (IOT)
- Invoicing information
- Customer Care information
- Testing and testing contacts
- Billing and Transfer information
- Billing identifier (BID) Annexes”

This page intentionally left blank.

List of Symbols/Abbreviations/Acronyms/Initialisms

3GPP	3rd Generation Partnership Project
AAA	Authentication Authorization Accounting
ACC	Access Control Class
ADC	Application Detection and Control
API	Application Programming Interface
APN	Access Point Name
ARP	Allocation Retention Priority
AS	Autonomous System
BID	Billing Identifier
CAMEL	Customized Applications for Mobile networks Enhanced Logic
CAP	CAMEL – Applications Part
CBC	Cell Broadcast Centre
CEPT	Conférence européenne des administrations des postes et télécommunications
CFSB	Circuit Switched Fall Back
CID	Cell Identifier
CISC	CRTC Interconnect Steering Committee
CISC	Communications Interoperability Strategy for Canada
CN	Core Network
CNA	Canadian Numbering Administrator
CoL	Conditions of License
CRTC	Canadian Radio-television and Telecommunications Commission
CS	Circuit Switched
CSS	Centre for Security Science
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Network Service
DRDC	Defence Research and Development Canada
DS	Deployable System
DSCP	Differentiated Services Code Point
DSS	Diameter Signalling Service
ECGI	E-UTRAN Cell Global Identifier

eCID	enhanced Cell ID
EHPLMN	Equivalent HPLMN
eICIC	enhanced Inter-Cell Interference Coordination
EM	Element Management
eMBMS	enhanced Multimedia Broadcast Multicast Services
eNB	evolved NodeB
EPC	Evolved Packet Core
eSRVCC	enhanced Single Radio Voice Call Continuity
E-UTRAN	Evolved UMTS Terrestrial Radio Access
GCS	Group Communications Services
GCSE	Group Communications System Enablers
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRX	GPRS Roaming Exchange
GSM	Groupe Spéciale Mobile; Global System for Mobile
GSMA	GSM Association
GUMMEI	Globally Unique MME Identity
GW	Gateway
HMNO	Home Mobile Network Operator
hPCRF	Home Policy Charging Rules Function
HPLMN	Home PLMN
HSS	Home Subscriber Server
ICAM	Identity Credentials and Access Management
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identifier
IOT	Inter Operator Tariffs
IP	Internet Protocol
IPsec	IP security
IPX	IP Exchange

ISED	Innovation Science and Economic Development (Canada)
ISO	International Standards Organization
LCS	Location Services
LMR	Land Mobile Radio
LMU	Location Measurement Unit
LTE	Long Term Evolution
MAP	Mobile Application Part
MCC	Mobile Country Code
MCPTT	Mission Critical Push-to-Talk
MME	Mobility Management Entity
MMEGI	MME Group Identifier
MMS	Multi Media Service
MNC	Mobile Network Code
MNO	Mobile Network Operator
MOCN	Multi Operator Core Network
MPLS	Multi-Protocol Label Switched
MSIN	Mobile Subscriber Identity Number
MSISDN	Mobile Station International Subscriber Directory Number
MSRN	Mobile Station Roaming Number
MVNO	Mobile Virtual Network Operator
NM	Network Management
NTP	Network Time Protocol
OTDOA	Observed Time Difference Of Arrival
OTT	Over The Top
PCI	Physical Cell Identifier
PCRF	Policy Charging Rules Function
PDN	Packet Data Network
PGW	Packet Gateway
PLMN	Public Land Mobile Network
PLMN ID	PLMN Identifier
PMN	Public Mobile Network
PRACH	Physical Random Access Channel

ProSe	Proximity Services
PSBN	Public Safety Broadband Network
PSK-TLS	Pre-Shard Key cipher suites for TLS
P/T	Provincial/Territorial
QCI	QoS Class Indicator
QoS	Quality of Service
QPP	Quality of Service, Priority and Pre-emption
RA	Roaming Agreement
RAEX	Roaming Agreement Exchange
RAN	Radio Access Network
SCCP	Signalling Connection Control Point
SGW	Serving Gateway
SIEM	Security Information and Event Management
SIP	Session Initiated Protocol
SIP-UA	SIP User Agent
SLA	Service Level Agreement
SLP	SUPL Location Platform
SMS	Short Message Service
SMSC	Short Message Service Centre
SON	Self-Organizing Networks
SPR	Subscriber Profile Repository
SUPL	Secure User Plane Location
TADIG	Transferred Account Data Interchange Group
TAI	Tracking Area Identity
TAN	Technical Advisory Note
TC	Traffic Class
TDF	Traffic Detection Function
TETRA	Terrestrial Trunked Radio
TFT	Traffic Flow Template
TLS	Transport Layer Security
UDC	Unified Data Convergence
UE	User Equipment (examples: handheld devices, external dongles and set top boxes, embedded modems in computing platforms and sensors)

UICC	Universal Integrated Circuit Card
UL	Up Link
UL-RS	Up Link Reference Signals
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
USSD	Unstructured Supplementary Service Data
UTDOA	Uplink Time Difference of Arrival
VMNO	Visited Mobile Network Operator
VoIP	Voice over IP
VoLTE	Voice-over-LTE
VPLMN	Visited PLMN
VPN	Virtual Private Network
WebRTC	Web Real Time Communications
WLAN	Wireless Local Area Network
WSP	Wireless Service Provider

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

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.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

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 DECEMBER 2013

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.)

Implications of service delivery model options on interoperability and operational efficiency in a public safety mobile broadband network

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

Fournier, J.; Lucente, C.

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.)
March 2017	72	34

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.)

Scientific Report

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

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

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.)

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-RDDC-2017-R038	

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

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.)

Delivering broadband services to the subscribers of the Public Safety Broadband Network (PSBN) can be achieved by several different approaches. Each approach entails different sets of actors in the service delivery fabric and different distributions of functions between the actors. Four approaches (options) are examined and compared for how they could satisfy fundamental requirements for (i) nationwide and agency-wide interoperability and (ii) operational efficiencies in delivering broadband service. The evaluation was based to a large degree on previous work by DRDC CSS that examined the technical underpinnings to achieve inter-working at the network level and interoperability at the service and user levels. In general, nation-wide interoperability can be more easily achieved by centralizing the functions that are implicated in delivering the services than by replicating those functions among independent regional actors. Furthermore, centralizing those key functions also leads to service delivery efficiencies because of reduced capital costs for the infrastructure and reduced costs to operate and maintain those functions. A hybrid option, between a fully centralized model and one consisting solely of independent regional actors, can be an efficient way to operate the PSBN and facilitate interoperability. The hybrid option consists of a national proxy of the regional actors to whom they would have delegated their authority to perform some of their functions. In all the options, a centralized coordination function is required that acts as the custodian of the interoperability standards for the PSBN.

On peut assurer de diverses façons la prestation de services à large bande aux utilisateurs du Réseau à large bande de sécurité publique (RLBSP); chacune présente des groupes d'intervenants différents dans la structure de prestation des services et une répartition différente des fonctions entre ces mêmes intervenants. Quatre démarches (options) sont analysées et comparées en fonction de leur capacité à répondre aux exigences de base visant (i) l'interopérabilité à l'échelle de l'Agence et du pays, ainsi que (ii) l'efficacité opérationnelle de la prestation des services à large bande. Cette analyse se fonde dans une large mesure sur des travaux précédents du CSS de RDDC, dans lesquels on a étudié les fondements techniques pour assurer l'interopérabilité à l'échelle du réseau, sur le plan des services et au niveau de l'utilisateur. En règle générale, centraliser les fonctions qui entrent en jeu dans la prestation des services permet d'assurer l'interopérabilité à l'échelle nationale plus aisément que répartir ces mêmes fonctions entre des intervenants régionaux indépendants. La centralisation des fonctions essentielles permet égalent d'assurer l'efficacité de la prestation des services, autant grâce à une capitalisation moindre pour l'infrastructure qu'à une réduction des coûts d'exploitation et de maintenance des fonctions. Une option hybride à mi-chemin entre le modèle entièrement centralisé et un groupe formé d'intervenants indépendants peut être aussi un moyen efficace d'exploiter le RLBSP et d'assurer l'interopérabilité. Dans ce modèle, les intervenants régionaux délèguent leur autorité d'exécuter certaines fonctions à un mandataire national. Toutes les options analysées, cependant, exigent une fonction de coordination centralisée qui assure l'application des normes d'interopérabilité du RLBSP.

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.)

Wireless; Broadband; Long Term Evolution (LTE); Communications networks; Roaming