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

DRDC | RDDC
technologyssciencetechnologie

Public Safety Broadband Network (PSBN)

Network architecture description

Joe Fournier
Claudio Lucente
Dean Skidmore
Luc Samson
DRDC – Centre for Security Science

Defence Research and Development Canada

Scientific Report

DRDC-RDDC-2018-R236

January 2019

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

Disclaimer: Her Majesty the Queen in right of Canada, as represented by the Minister of National Defence ("Canada"), makes no representations or warranties, express or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

Endorsement statement: This publication has been peer-reviewed and published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada. Inquiries can be sent to: Publications.DRDC-RDDC@drdc-rddc.gc.ca.

Abstract

This Scientific Report provides guidance on possible architectures for the Public Safety Broadband Network (PSBN) initiative in Canada. The architecture considers Service Delivery Model (SDM) concepts and 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE), and is supplemented by various other technologies that, in its ensemble, forms the PSBN. The described architectures contained herein are intended to provide Science and Technology (S&T) advice to those ultimately responsible for the implementation of the PSBN in Canada, and the decision to consider the contents of this Scientific Report rests with them.

This report is a revision of the initial PSBN architecture that was developed in 2013. It has been expanded beyond the network aspects and now includes additional architectural aspects for mission critical communication services, machine type communications, better known as Internet of Things (IoT), operations support, business support, telecommunications management, PSBN planning and service architecture. The information and views that are contained in this document are those of the authors and are only intended as guidance to the implementers of the PSBN.

What public safety needs in an emergency is…

The ability of emergency personnel to communicate between jurisdictions, disciplines, and levels of government, using a variety of systems, as needed and as authorized… a national emergency communications based on common user requirements, open standards and a system of systems approach… a public safety controlled mobile broadband communications network expected to operate in the 700 megahertz (MHz) band [1].

Significance to defence and security

The wireless PSBN will be a nationwide cellular network primarily for the 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 secure mobile broadband 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 and ability to communicate, 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 unreliable, or even unavailable, when major incidents occur, and networks become severely congested. The availability of commercial networks are primarily driven by economic considerations whereas it is expected that the availability objectives for the PSBN will be strongly influenced by life-safety considerations.

This network architecture description is intended to inform the public safety and defence communities on possibilities for how the PSBN could be structured either as a single nationwide network consisting of a national component and a federation of regional sub-networks, or a single nationwide network with regional operations. In the case of the former, a national entity and regional service delivery entities could structure the national and regional networks and determine how service delivery could be performed over

that nationwide service delivery fabric. In the case of the latter, service delivery would be the responsibility of the single nationwide mobile network operator.

The PSBN user experience is shaped by various aspects of the PSBN, including its design and implementation choices. This network architecture description will also illustrate how achieving greater interoperability contributes directly to achieving a consistent and reliable user experience. Together with its companion reports that cover PSBN technical considerations on operability, interoperability and security, it is anticipated that this network architecture description could significantly contribute to the successful implementation of a nationwide interoperable mobile public safety broadband network in Canada.

Résumé

Ce rapport fournit des conseils sur des architectures possibles pour un réseau à large bande pour la sécurité publique (RLSP) au Canada. L'architecture RLSP considère des concepts de modèle de prestation de services (MPS) et le Projet de Partenariat de 3^{e} Génération (3GPP) évolution à long terme (LTE) et est complétée par diverses autres technologies qui, dans leur ensemble, forme le RLSP. Les architectures décrites ont comme but de fournir des conseils S&T à ceux qui seront ultimement responsable pour la mise en oeuvre du RLSP, et la décision de considérer les contenus de ce rapport, ou pas, est la leur.

L'architecture RLSP initiale qui a été développée en 2013, a été élargie au-delà de seulement les aspects du réseau et comprend maintenant des aspects architecturaux supplémentaires pour le développement des services, les services de communication critique de mission, les communications de type machine mieux connu comme « Internet of Things » (IoT), le soutien des opérations, le soutien aux entreprises, la gestion des télécommunications et la planification RLSP. Les informations et points de vue contenus dans ce document sont ceux des auteurs et sont seulement destinés à guider les metteurs en cause du RLSP.

Importance pour la défense et la sécurité

Le RLSP sans fil sera un réseau cellulaire national principalement pour les communautés de sécurité publique, de sécurité et de défense. Ce sera une capacité transformationnelle qui révolutionnera la façon dont les premiers intervenants et le personnel de la défense communiquent et partagent l'information les uns avec les autres pendant des décennies à venir. Mettre les mobiles à large bande sécurisés dans leurs mains augmentera considérablement leur capacité à anticiper, à réagir et à se remettre des urgences, des catastrophes et des actes de terrorisme en augmentant leur conscience de la situation et leur capacité de communiquer, ce qui ultimement aidera à protéger et sauver des vies, limiter les dommages matériels et les pertes, et rendre les communautés plus sûres. En effet, même si le service cellulaire commercial est en mesure de fournir des services à large bande aux usagers de la sécurité publique pour une utilisation quotidienne, il devient rapidement peu fiable ou même indisponible lorsque des incidents majeurs surviennent, et les réseaux deviennent gravement encombrés. La disponibilité des réseaux commerciaux est principalement motivée par des considérations économiques, alors qu'on s'attend à ce que les objectifs de disponibilité pour le RLSP soient fortement influencés par les considérations de sécurité-vie.

Cette description de l'architecture informera les communautés de la sécurité publique et de la défense sur la façon qu'un seul RLSP national peut être structuré soit avec une entité nationale et des entités régionales de prestation de services ou avec un tissu national de prestation de service.

L'expérience utilisateur RLSP est façonnée par divers aspects de la RLSP, y compris les choix de conception et de mise en œuvre. Cette description de l'architecture du réseau illustrera également comment la réalisation d'une expérience utilisateur cohérente et fiable contribue directement à la réalisation d'une plus grande interopérabilité. Avec ses rapports complémentaires qui couvrent l'influence de l'accès et du partage de l'information sur l'opérabilité, l'interopérabilité et la sécurité, il est anticipé que cette description d'architecture contribuera de manière significative à la mise en œuvre réussie d'un réseau à large bande mobile interopérable à l'échelle nationale au Canada

Table of contents

List of figures

List of tables

Acknowledgements

This version of the PSBN Network Architecture Description supersedes the previous published version—DRDC CSS TR 2013-009, August 2013 [2]. It builds upon the technical considerations found in the original published version. The previous version was created based on recommendations derived from comments and feedback from a work group composed of representatives from the vendor community, wireless carriers, consultants, federal government representation, academia, federal/provincial/territorial emergency management officials, and first responders. The recommendations were reviewed by the 700 MHz Technical Advisory Group[1] (700TAG). The former 700TAG acknowledges the invaluable contributions and dedication of all the participants in the work sessions.

[1] The 700TAG was composed of a collaborative group of technical experts led by Centre for Security Science and includes scientific authorities from the Communications Research Centre of Canada, Simon Fraser University, and technical experts from Federal/Provincial/Territorial/Municipal agencies.

This page intentionally left blank.

1 Purpose

The purpose of this Scientific Report is to inform the public safety community on a variety of considerations related to the network architecture of a Public Safety Broadband Network (PSBN) in Canada. To do so, two possible architectures and a variant of both are used to draw out such considerations. One is based on a two-tiered service delivery model involving both national and regional network operator components, and the other is a single-tiered service delivery model involving a single national network operator. Other architectures could also have been considered in producing this Scientific Report, but it is the opinion of the authors that those included, while not exhaustive, represent valid approaches to a PSBN. The technical information provided in this report is that of Defence Research and Development Canada Centre for Security Sciences (DRDC CSS) and does not necessarily represent any endorsement or specific position of the federal government on PSBN.

The Network Architecture Description (NAD) is one in a series of PSBN Reports issued by DRDC CSS. Other reports include the PSBN Technical Considerations on Interoperability (TCI) [3], the PSBN Technical Considerations on Operability (TCO) [4] and the PSBN Technical Considerations on Security (TCS) [5] Reports. These documents were originally drafted in the 2012–2014 timeframe under different titles in some cases by a federally-led Technical Advisory Group (TAG) while considering input from technical and operational PSBN work groups comprised of participants from government, public safety, industry and academia. Not all input from these workgroups was considered by the TAG in producing the documents, where the decision to include or exclude information was the responsibility of DRDC CSS.

The NAD was published by DRDC in 2013, whereas the other three reports referenced above remained in draft form and were not re-visited until 2017. At the time, these documents were intended to serve as references for federal, provincial, territorial, and municipal public safety stakeholders and agencies. They were expected to contribute to the establishment of technical requirements, features and capabilities of the PSBN by the entity(ies) ultimately responsible for the implementation and operation of a PSBN in Canada. The current variants of the documents have a similar purpose, which is to inform the public safety community on a variety of technical considerations related to network architecture, the operability, interoperability and security of a potential PSBN in Canada.

The technical information contained herein should ***not*** be construed as requirements or recommendations for a PSBN. This information is simply intended to complement and add to various other sources of information that will inevitably be considered in devising an implementation plan for a PSBN in Canada. These other sources of information may include other technical approaches to a PSBN, business plans, cost-benefit analyses, feasibility assessments and trade-off decisions. The information contained in this document may be considered either in its entirety, partially or not at all in the development of such a plan.

In the cases of the TCO, TCI and TCS, while they include statements containing the auxiliary verbs “shall,” “should” and “may,” it is important to note that they are simply considerations in the form of statements that are conditional and only pertinent if parts or all of the architecture described in this NAD are considered by those ultimately responsible for the implementation of a PSBN. As such, they do not represent actual requirements of the PSBN but simply information points on technical aspects of the PSBN.

2 Introduction

The world of mobile communications is experiencing massive growth in the creation and consumption of data. Consumers have an insatiable appetite for information delivered to their fingertips, enabled by the availability of a wide range of smart mobile devices and the sophisticated feature-rich applications that they support. Access to information in a timely, i.e., immediate manner, and in any location has had, and continues to have, an enormous impact on our lives—from increased productivity for businesses to accelerated social development.

Wireless technology re-invents itself with ever shrinking product life-cycles. Application developers keep churning out new tools, while consumers continuously invent more ways to use them. The commercial world has moved from voice-only mobile communications to multi-media, pervasive, content-rich, adaptive, personalized information delivery platforms. Yet, public safety communications have not advanced much beyond the walkie-talkie push-to-talk style of voice-centric networks from decades ago. Certainly, first responders have better radios today, but they are still used for the same purpose and have limited capabilities. That is, to transmit and acquire information through the spoken word, and very limited data communications.

The advent of broadband mobile communications is expected to be of significant benefit to public safety and security communities by improving their ability to communicate and share valuable information, particularly at times when they need it most. There are currently a growing number of public safety broadband initiatives worldwide that intend to leverage the technological advancements of broadband mobile. Such broadband networks herald the era of advanced communications capabilities for first responders. The public safety community will be able to take advantage of new applications to improve the effectiveness with which they conduct their missions, increase their safety, and that of the citizens whom they serve. The networks will provide high-capacity mobile communications for first responders and will support applications that deliver the kinds of information and experience on par with commercial users, but with greater reliability and security. In Canada, the notion of a PSBN has been considered for many years now, driven by the potential enhanced capabilities, and its ability to deliver truly interoperable communications at all times.

"Emergency response agencies, at all levels of government, must have seamless interoperable communications to manage response, establish command and coordination, maintain situational awareness and function within a common operating framework. This will lead to improved response capabilities and provide a more comprehensive approach to disaster management, which will lead to increased safety for all Canadians. ... Information is the lifeblood of effective day-to-day operations within the public safety community. In making countless decisions every day, officials must have immediate access to timely, accurate, and complete information. It has become clear that effective decision making requires information that must often be shared across a broad landscape of systems, agencies, and jurisdictions. For example, the adoption of common tools such as open standards is a key element in enabling public safety agencies to deal with this growing and complex problem [1]."

To this end, part of the valuable 700 MHz band of radio frequency spectrum has been designated for public safety broadband use. Specifically, the spectrum includes the Public Safety Broadband (PSBB) (758–763 and 788–793) and the D Block (763–768 and 793–798) for a total of 20 MHz (758–768 MHz downlink and 788–798 uplink). Collectively, this is known as Band 14 in the 3rd Generation Partnership

Project (3GPP). This document will provide technical considerations on possible network architectures for a PSBN. In order to capture and describe these considerations, two such architectures are described in this document and serve as the foundation and basis for the technical considerations described herein. The first architecture is based on a single, nationwide Mobile Network Operator (MNO) with, potentially, a number of regional operations. The second contains two tiers of operational responsibility—a National Entity (NE) and multiple Regional Service Delivery Entities (RSDE) that, while linked together as a single network, can be separate from one another from an operational perspective.

Both architectures are aligned with a service delivery model [6] whereby it is posited that the users of the PSBN are clients of the national or regional operators, depending on the architecture, and End-User Agencies (EUA) are owners of the information networks. The PSBN is used to link users with their information networks and ensures they can access their information from any region in Canada. Facilitated by roaming agreements, users would also be able to access their information when they are on other networks). As the information networks are assumed to be owned and managed by the various agencies to which the end-users pertain, it would be within the purview of the end-user agencies to grant appropriate access to their information networks as required during day-to-day operations and for the specific interoperability needs during incidents. The end-user agencies would control the profiles of the end-users within their jurisdictional authority.

For the purposes of this Scientific Report, the components that are considered to be part of the PSBN are shown inside the yellow block in Figure 1and make up the primary focus of this Scientific Report. The PSBN will interface with several external networks, systems, services and applications that are captured in the blue space, and this Scientific Report describes, at a high level, how the PSBN could interface with many of these external components. The TCI, TCO and TCS also describe such interfaces (reference points).

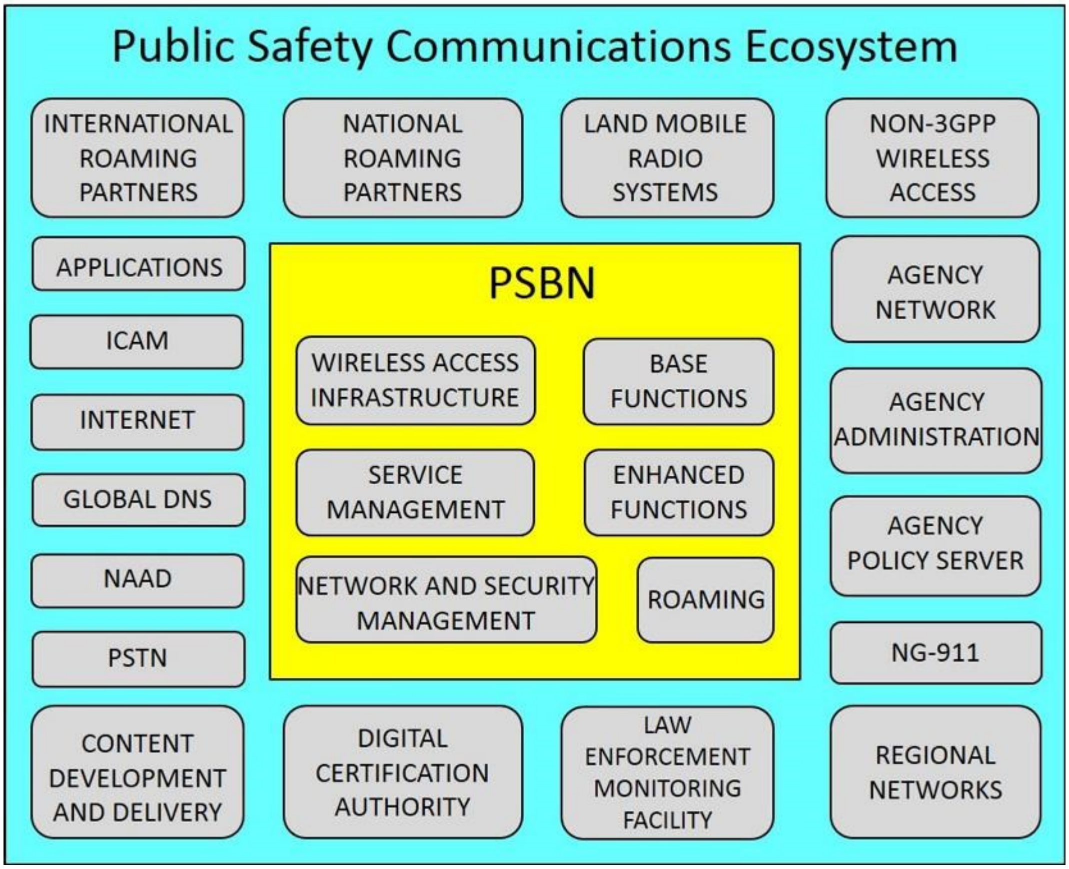

Public Safety Communications Ecosystem
INTERNATIONAL ROAMING PARTNERS
NATIONAL ROAMING PARTNERS
LAND MOBILE RADIO SYSTEMS
NON-3GPP WIRELESS ACCESS
APPLICATIONS
ICAM
INTERNET
GLOBAL DNS
NAAD
PSTN
PSBN
WIRELESS ACCESS INFRASTRUCTURE
BASE FUNCTIONS
SERVICE MANAGEMENT
ENHANCED FUNCTIONS
NETWORK AND SECURITY MANAGEMENT
ROAMING
AGENCY NETWORK
AGENCY ADMINISTRATION
AGENCY POLICY SERVER
NG-911
CONTENT DEVELOPMENT AND DELIVERY
DIGITAL CERTIFICATION AUTHORITY
LAW ENFORCEMENT MONITORING FACILITY
REGIONAL NETWORKS

Figure 1: *Public safety communications ecosystem.*

Section 3 of this Scientific Report lists PSBN architecture technical assumptions, definitions and service delivery model considerations. Section 4 describes three possible network architectures for the PSBN: a single-tiered architecture, a two-tiered and a variant of the two-tiered Sections 5 through 10 provide additional detail on each component of the PSBN within the yellow in Figure 1. Section 11 presents the Conclusion. It is followed by Annex A and the List of Acronyms.

It is expected that the technical considerations on PSBN architecture will evolve over time and as such, this document is a snapshot in time of the needs of the public safety community as they are understood today.

3 PSBN architecture assumptions and definitions

Given that, at the time of writing, the PSBN does not exist and other technical and operational parameters are not yet fully defined, it is necessary to table certain assumptions for these and other aspects that impact a network architecture. The assumptions that are stated in this section are those that are deemed relevant to setting the baseline for possible architectures. In addition to these assumptions, key terms related to PSBN are defined.

For user requirements, this Scientific Report considers user requirements derived from a number of public safety and security use cases that have been produced (or amassed) over the past few years, and validated and updated through a series of outreach sessions held from June 2017 to February 2018 throughout Canada [7].

3.1 PSBN service delivery model assumptions

A Service Delivery Model (SDM) identifies the actors and their interactions in the delivery of services—in this case, mobile broadband communications services, to its "customers." The PSBN technical architectures described in this document have considered possible PSBN SDM options described in a DRDC CSS Scientific Report [6]. Specifically, the two SDM options considered are a service delivery model with a single national MNO and one with a number of regional MNOs and a national operational entity. Both options consider a single Public Land Mobile Network IDentifier (PLMN ID).

In the case of the former, Figure 2 illustrates a possible single-tiered service delivery model. In this particular case, it shows how each of three possible actors—a national mobile network operator, EUAs and end-users fit into the overall chain of connecting users to their information networks. The national operator is depicted as being distinct from the end-users and the EUAs they pertain to. The EUAs own the information networks, whereas the national MNO owns the PSBN infrastructure. Applications can be hosted by the national operator and by end-user agencies. The PSBN operator interconnects the PSBN with external networks and applications, such as commercial carriers, FirstNet, existing Land Mobile Radio (LMR) and WiFi networks and the applications that are hosted on those networks.

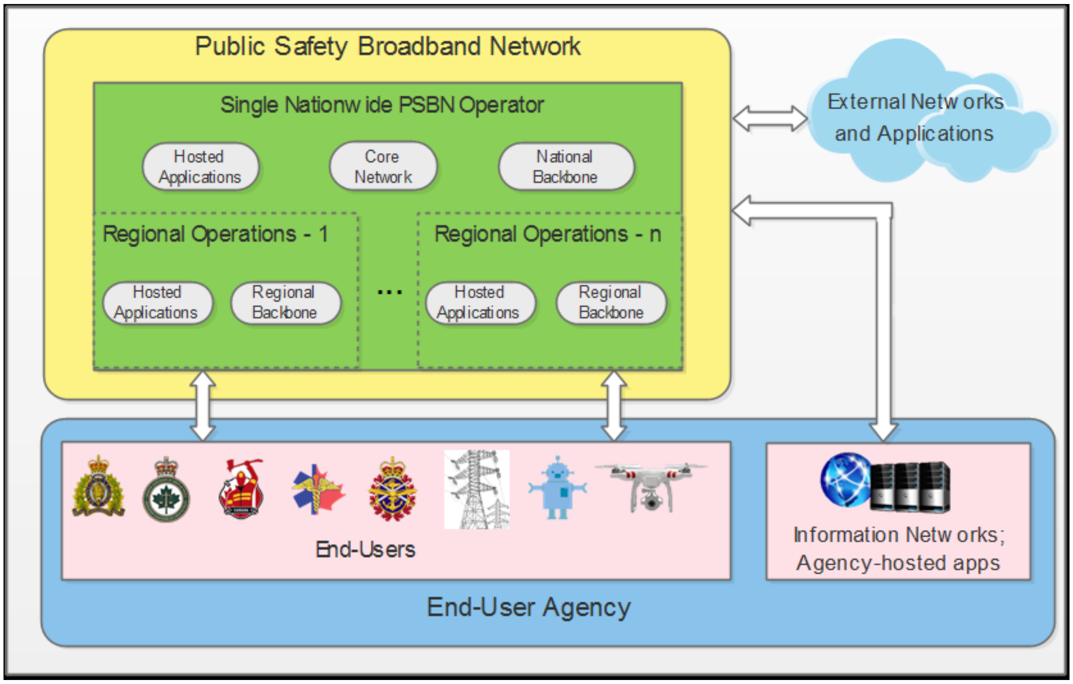


***Figure 2:** Single national operator service delivery model.*

In the case of the latter, Figure 3 illustrates a possible two-tiered service delivery model. In this particular case, it shows how each of four possible actors—NE, RSDEs, EUAs and end-users fit into the overall chain of connecting users to their information networks. Similar to the previous model, the national entity and the RSDEs are depicted as being distinct from the end-users and the EUAs they pertain to. The EUAs own the information networks, whereas the NE and RSDEs own the PSBN infrastructure. An exception may be with regards to the possibility that some EUA may operate deployable systems,[2] which are extensions of the infrastructure of the PSBN. The EUA would be active participants in the use of the PSBN in terms of provisioning the services to their subscribers and, to some degree, adapting the service to the communications needs of their users during incidents. Applications can be hosted by the NE, RSDEs, and by EUAs. The PSBN operators interconnect the PSBN with external networks such as commercial carriers, FirstNet, existing LMR and WiFi networks and the applications that are hosted on those networks.

In this approach, each region can implement its portion of the PSBN with its selected vendors/partners according to its budgets and timelines. However, it is expected that each regional sub-network will comply with a set of nationally-harmonized requirements in order to achieve nationwide interoperability such that end-users from any region in Canada can be served over the PSBN regardless of which region they are in. A national network layer serves as the host for nationwide applications and interconnects the regional sub-networks.

[2] The EUA are presumed to have been granted permission to operate deployable systems under a licensing framework and governed by agreements with the NE and/or the RSDEs.

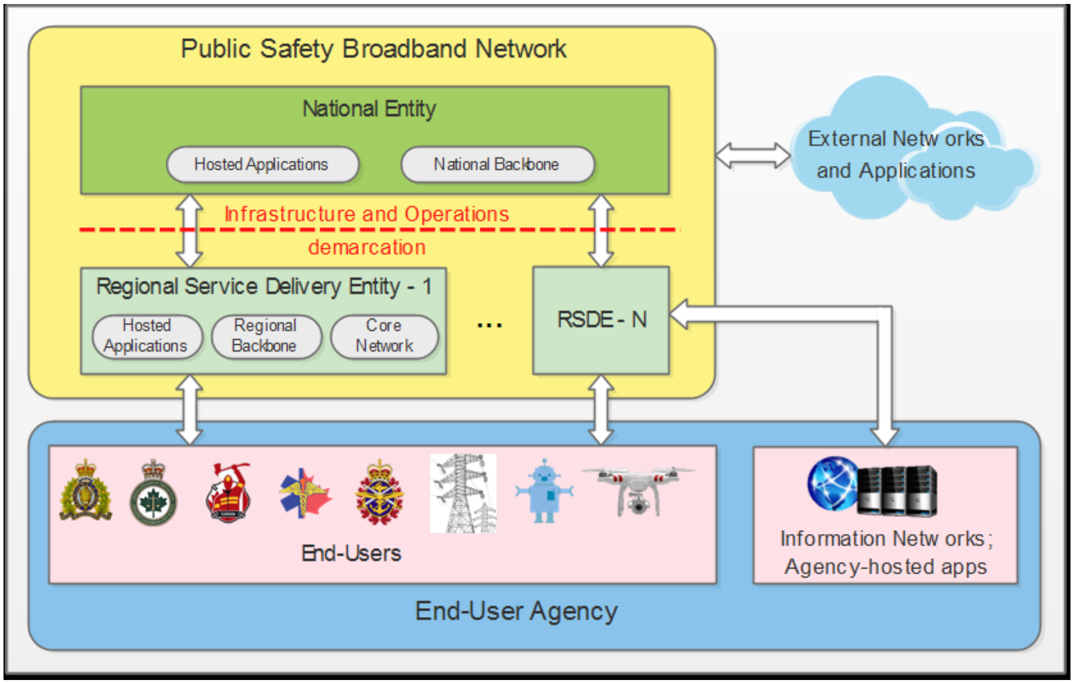

Public Safety Broadband Network
National Entity
Hosted Applications
National Backbone
Infrastructure and Operations
demarcation
Regional Service Delivery Entity - 1
Hosted Applications
Regional Backbone
Core Network
...
RSDE - N
External Netw orks and Applications
End-Users
Information Netw orks; Agency-hosted apps
End-User Agency

Figure 3: *Two-tier service delivery model.*

Key assumptions for a service delivery model are listed below.

a. The PSBN is managed and operated either jointly by the NE and “n” number[3] of RSDE, or by a single national operator (n=1).

b. As applicable, a national operator or a RSDE will enter into a contract with its mobile network operator partner.

c. The nation-wide PSBN is constituted by either the NE and all the RSDEs or the national operator, as well as the communications assets that may be owned and operated at the agency level such as user devices and deployable systems.

d. A RSDE is a municipality, a province or territory, or any combination thereof.

e. Mobile network operators will be implicated in building, operating and maintaining the PSBN, either as sub-contractors to the NE and RSDEs (or national operator) or in a public-private partnership arrangement with the NE and RSDEs.

f. There may be more than one mobile network operator for the PSBN.

g. The PSBN spectrum will be shared with commercial users.

[3] “n” may be greater than or equal to 1. If “n” = 1, then the RSDE is the de facto national PSBN service provider.

h. Interoperability policies and standards that apply to the PSBN nationwide are established and managed at the national level.

3.2 Technical assumptions

The assumptions listed in this section are intended to set the hypothetical technical and operational boundaries for the PSBN. While the assumptions are based on the two-tiered SDM, in the case of a single national operator, all references to NE and RSDE can be replaced by the "national PBSN operator."

a. For the two-tiered SDM, the NE specifies, procures, operates and manages the inter-regional backbone network that interconnects the RSDEs.

b. Billing (due to roaming) will be reconciled at the national level. For the two-tiered model, the national entity will settle the inter-carrier charges. It will collect or credit the amount attributed to the specific regional service delivery entities.

c. The NE manages policies regarding spectrum sharing with FirstNet and commercial mobile network operators.

d. The NE manages the national and international roaming agreements.

e. The NE offers value-added nationally hosted applications and services.

f. The NE configures the mobile devices / Universal Subscriber Identity Module (USIM) with national configuration parameters.

g. The NE provides connections for federal network access at agreed-upon demarcation points.

h. The RSDE adheres to nation-wide interoperability standards.

i. The RSDE delivers value-added services through regionally-hosted applications.

j. The RSDE provides a connection point for agency information networks at agreed-upon demarcation points.

k. The RSDE provides access to the public Internet.

l. The RSDE provides connection points for roaming exchange networks.

m. The RSDEs will be able to assert selective Local Control (LC)[4] on the PSBN, in accordance with national policies.

n. The RSDE configures the mobile devices / USIM with regional configuration parameters.

[4] National Public Safety Telecommunications Council (U.S.) recommendations for Local Control are contained in the report "Public Safety Entity Control and Monitoring Requirements for the Nationwide Public Safety Broadband Network," Final Report, October 2015 [8].

o. The RSDE provides an LTE-LMR interworking function to support inter-domain Push-to-Talk (PTT) talk groups in accordance with national standards.

p. Each EUA provisions the services for its own subscribers.

q. The EUA establishes and manages the access control policies and rules for their information networks.

r. The EUA will be able to assert selective Local Control on the PSBN, in accordance with national policies.

s. The EUA may procure, own and operate its own deployable systems in accordance with national policies.

t. The EUA may procure, own and operate its own mobile devices in accordance with national policies.

u. The EUA may activate the services and mobile devices / USIM.

v. The EUA provides access to the Internet for the users and user devices under its authority. This enables the EUA to apply its Internet access policies.

w. The user requirements for the PSBN are articulated in the “PSBN Use-Case and User Requirements” Report [7].

x. The end users have a common quality of experience when they are connecting to a nationwide PSBN service regardless of which RSDE that they are accessing.

y. All authorized users served by the Public Safety Broadband Network may attach to any region of the Public Safety Broadband Network regardless of which agency they pertain to. There is no roaming required for such users when anywhere on the Public Safety Broadband Network.

z. The minimum 3GPP feature set and specifications for the PSBN will be LTE Release 14.

aa. There will be one PLMN ID for the PSBN. There may be a separate PLMN ID assigned for all deployable systems for when they are isolated from the macro network.

bb. 20 MHz of spectrum is allocated for the PSBN in the 700 MHz band (downlink: 758–768 MHz and uplink: 788–798 MHz).

cc. Public safety traffic of the PSBN will flow through a dedicated public safety core network.

dd. Commercial Band-14 traffic is carried on the commercial core network only. In effect, commercial traffic and public safety traffic will be kept separate when both are using Band 14 spectrum.

ee. Public safety traffic may flow over a commercial network in the absence of the PSBN.

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

gg. The RSDEs may be able to operate, serving the users in their regions, in case of disconnection from the National entity.

hh. The minimum PSBN content of an RSDE is the Radio Access Network (RAN).

ii. The PSBN, except for UEs, will not store user-traffic, except if required by regulations.

jj. There will be service continuity and session (LTE bearers) persistence during hand-over between RSDE-to-RSDE, RSDE-to-commercial partner, RSDE-to-FirstNet/AT&T.

kk. The PSBN MNOs have enabled Quality of Service, priority and pre-emption mechanisms on the PSBN.

ll. The PSBN will support Wireless Public Alerting [10].

mm. The PSBN will support Next Generation 911 (NG 911) in accordance with the National Emergency Number Association's (NENA) i3 solution [11].

nn. RAN-sharing may be used in the regional networks.

3.3 Definitions

A complete list of definitions and acronyms pertaining to the PSBN will be in the forthcoming "Integrated Dictionary of Terms" [12]. For the purposes of the present document, the 3GPP terms and definitions are described in 3GPP Vocabulary TR 21.905 [13]. A term defined in the present document takes precedence over the definition of the same term as may be defined in other documents.

For clarity, the following definitions are used to convey the strength of the interoperability, operability and security considerations in the companion reports to this Scientific Report.

Shall
The attribute, which is the object of the sentence with "SHALL" as the auxiliary verb, is essential or necessary to ensure that the effect of the attribute is achieved. It is assumed that the realization of the attribute is entirely within the control of the operators of the PSBN.

Should
The attribute, which is the object of the sentence with "SHOULD" as the auxiliary verb, is essential or necessary to ensure that the effect of the attribute is achieved. But, it is assumed that the realization of the attribute is not entirely within the control of the operators of the PSBN.

May
The attribute, which is the object of the sentence with "MAY" as the auxiliary verb, is proffered as guidance or as a consideration for the standards that apply to the attribute. In light of other standards

which may exist, the sentence conveys the consideration of the authors for what standards to apply to the PSBN. The use of other standards could impede the attainment of the intended effect of the attribute due to lack of significant adherents to the alternative standards, or pending obsolescence, or other similar risks.

Other definitions:

Service
A service is a component of the portfolio of choices offered by service providers to a user; a functionality offered to a user. A service entails that a subscriber is engaged in a subscription with a service provider. A subscriber is associated with one or more users. In this document, services are network-based, provided by the MNO, and almost exclusively 3GPP-specified (e.g., Voice over LTE (VoLTE), Short Message Service (SMS)). Users can be human-users, machine-users and application-users.

Service Enablers
Services can also act as "enablers" when complemented with appropriate logic and exposure building blocks, so that it can be reused by other services or applications through well-defined functional and operational interfaces. These service enablers are typically not directly visible to end-users, but rather made available to end-user applications or administrative-user applications via Application Programming Interfaces (API). Service enablers can serve both PSBN-hosted applications as well as EUA-hosted applications. Service enablers may be specified by bodies other than 3GPP.

Application
An application is a functionality typically provided via a client and server architecture, although applications can also be client-less or client-only. Application servers can be hosted by the PSBN, the EUAs, or the cloud. An application differs from a service as it doesn't necessarily require a subscription, although mobile applications typically make use of a data subscription-based service offered by an MNO. Applications serve both end-users and administrative-users. In this Scientific Report, only PSBN-hosted applications running on PSBN devices or servers are in-scope.

Interoperability
The ability for two or more systems to exchange information and to mutually use the information that has been exchanged [14].

Interworking
The means whereby terminals connected to a telecommunication network may communicate with terminals of another network [15].

User Data
User Data is data about the user, such as agency, role, rank, personally identifying information, etc.

User Plane Traffic
User Plane Traffic is data that is created or consumed by a user. Examples: audio communications, email, camera feeds, etc.

Network Elements
Network Elements are physical or logical components of a communications network. They are referred to by labels that identify them within a network architecture or block diagram of a communications network. Network elements perform functions, either individually or as a group.

Functions
Functions are manifestations of the processes that are conducted by the network elements or groups of network elements. They are identified by what they do or what actions they perform within a communications network.

Capabilities
Capabilities are manifestations of functions that are perceptible by a user or an application.

4 PSBN base network architecture

This section describes three base network architectures that can meet the user requirements described in the PSBN Use Cases and User Requirements report [7]. One network architecture is based on a single nationwide MNO service delivery model (Figure 3), while two other architectures are based on a two tiered service delivery model with a national entity and regional service delivery entities (Figure 2). These last two still constitute a single nationwide PSBN. The architectures are presented by first illustrating the base network block diagram of the PSBN with a high level description, followed by a description of the components and roles of each service delivery entity in each base architecture. The block diagrams are primarily based on 3GPP's System Architecture Evolution (SAE) and LTE.

4.1 PSBN architecture options

4.1.1 Single national PSBN mobile network operator

The first possible architecture is based on a PSBN service delivery model that is operated by a single operator, as described in Figure 3, providing nationwide coverage, services, applications, gateways, operations support and business support. Figure 4 illustrates a single operator providing service delivery for the nationwide PSBN.

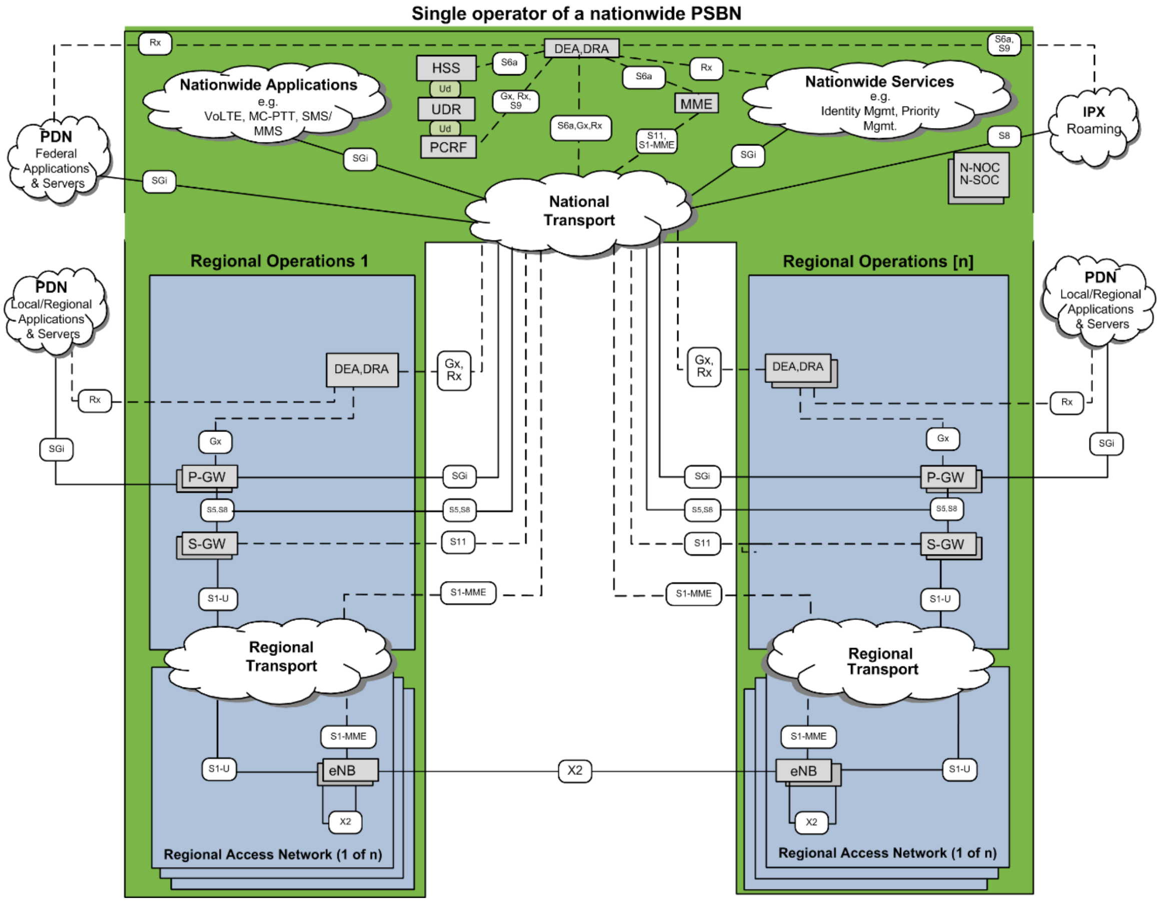


Figure 4: *Single national operator of the PSBN.*

A single PSBN national operator, with potentially a number of regional operations, would provide all national, regional and gateway functions of the PSBN. The single network operator could nevertheless have multiple regional operations that would provide Packet Data Network (PDN) gateway functions for connecting the local/regional/federal applications and servers. For purposes of accessing external commercial roaming networks and services, the regional operations would provide bilateral interconnect with commercial roaming partners as described in Group Spécial Mobile Association (GSMA) IR.34 [16]. Furthermore, international access to other external international networks would be made possible by contracting with an Internet Protocol (IP) eXchange (IPX) provider. All nationwide applications and nationwide services would be provided by a central function.

In the case of a single nationwide operator architecture, responsibilities would be assumed by the national operator and its regional operations. The network elements and functions of the PSBN, as listed in Table 1, would be deployed, managed and maintained by the national operator.

Table 1: *National mobile network operator—network elements and functions.*

Element / Function	Description
Spectrum Responsibility	Innovation, Science and Economic Development (ISED) has allocated 20 MHz of nationwide spectrum for the PSBN in the 700 MHz band (downlink: 758–768 MHz and uplink: 788–798 MHz).
Core Network	The national operator is responsible for the deployment and operation of the Mobility Management Entity (MME) of the Evolved Packet Core (EPC), Home Subscriber Server (HSS), User Data Repository (UDR) and Policy and Charging Rules Function (PCRF) components.
National Transport	The national transport interconnects the regional operations and allows them to connect to the master subscriber database and to national services, applications and data networks. The Quality of Service (QoS)-aware national transport can consist of multiple transport, network, and data link technologies. These can include satellite backhaul links.
User Data Repository	The UDR contains subscriber information for every user in the PSBN. Authorized EUA administrators must have access to the UDR in order to enter, modify, or delete user profiles.
National services	National services are services such as user location displays or identity management databases that can be used by end-user agencies, regardless of where they operate in Canada.
National applications	National applications are applications such as user VoLTE, SMS and mission critical applications that can be used by end-user agencies, regardless of where they operate in Canada. The testing and certification of the national applications is expected to be the responsibility of the national operator.
Regional, national and international roaming agreements	The national operator would enter into and manage the agreements for roaming and interconnection to partner networks. This includes inter-working agreements with FirstNet. The inter-working gateways with the external roaming exchanges and interconnections would be hosted at the regional operations level.
Bilateral interconnect commercial networks	The national operator, through its regional operations, would operate and manage the bilateral interconnect functions with commercial MNOs to provide the ability for end-users to non-seamlessly roam between PSBN and commercial networks. In some cases, it would be possible to implement seamless mobility between the PSBN and commercial networks.

Element / Function	Description
International roaming via IP exchange (IPX)	The national operator would put into operation a connection to an IPX service provider that would support an international roaming exchange. The physical attachment between the RSDE and the IPX service provider would be done using GSMA IR.34 guidance [16].
Network Operations Centre	National operator would operate the Network Operations Centre (NOC).
Security Operations Centre	National operator would operate the Security Operations Centre (SOC).
Operation Support System	The national operator will have the necessary operations, administration, management and provisioning functions to manage the resources of the PSBN.
Business Support System	The national operator is likely to contract with partner MNO(s) for operating the PSBN. In any MNO, it is necessary to provide Business Support System functions such as customer billing and customer relationship management.

The network elements and functions listed in Table 2 would be deployed, managed and maintained by the regional operations.

Table 2: *Regional operations functions.*

Function	Description
EPC - Gateways	The regional operations would deploy and operate the EPC Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW) components.
Radio Access Network(s)	The radio access network (RAN) is composed of evolved Node Bs (eNodeB), trusted WiFi access points and possibly other RAN technologies that are distributed across the region.
Regional Transport	The regional transport interconnects the regional operations multiple radio access networks with the main core components. It allows clients in the Access Networks (AN) to connect to regional services, applications and data networks. The QoS-aware regional transport can consist of multiple transport, network, and data link technologies. These can include satellite backhaul links. The regional transport shall abide by the same QoS requirements as the national transport.

Function	Description
Connection to End User Agency and federal agency networks	End-user agencies and federal agencies can attach their network or part of their network to the PSBN. The regional operations would provide an Access Point Name (APN) and configure a packet gateway and a firewall to connect to these particular packet data networks. The end-user agency and federal agency administrators would then be able to select that APN for their users. It is expected that the specific agency network would only be available to the users of that particular agency, though this does not preclude the agency from allowing access to other users.

4.1.2 Multiple RSDE operators with a national entity

The second possible architecture is based on a two-tiered service delivery model as described in Figure 2, and is made up of a NE and multiple RSDEs. A national entity is an operational entity assumed to have the responsibility to establish and manage the national interoperability standards for the PSBN. A RSDE is a municipality, a province or territory, or any combination thereof. It is assumed that RSDEs will be required to abide by a common set of policies, regulations and minimum interoperability standards. RSDEs would manage all users within their respective geographic regions to ensure adherence to those national standards. It is also assumed that RSDEs will enter into contracts with partner mobile network operators, as could the NE for operational components.

Each RSDE would provide their respective full RAN, core, gateways, applications, services, telecommunications management network, operations support and business support. These multiple RSDEs would be interconnected to each other and to a NE which provides a master UDR, a master HSS, national services, and national applications. The NE would not provide any RAN or other subscriber access network functions. This is illustrated in Figure 5.

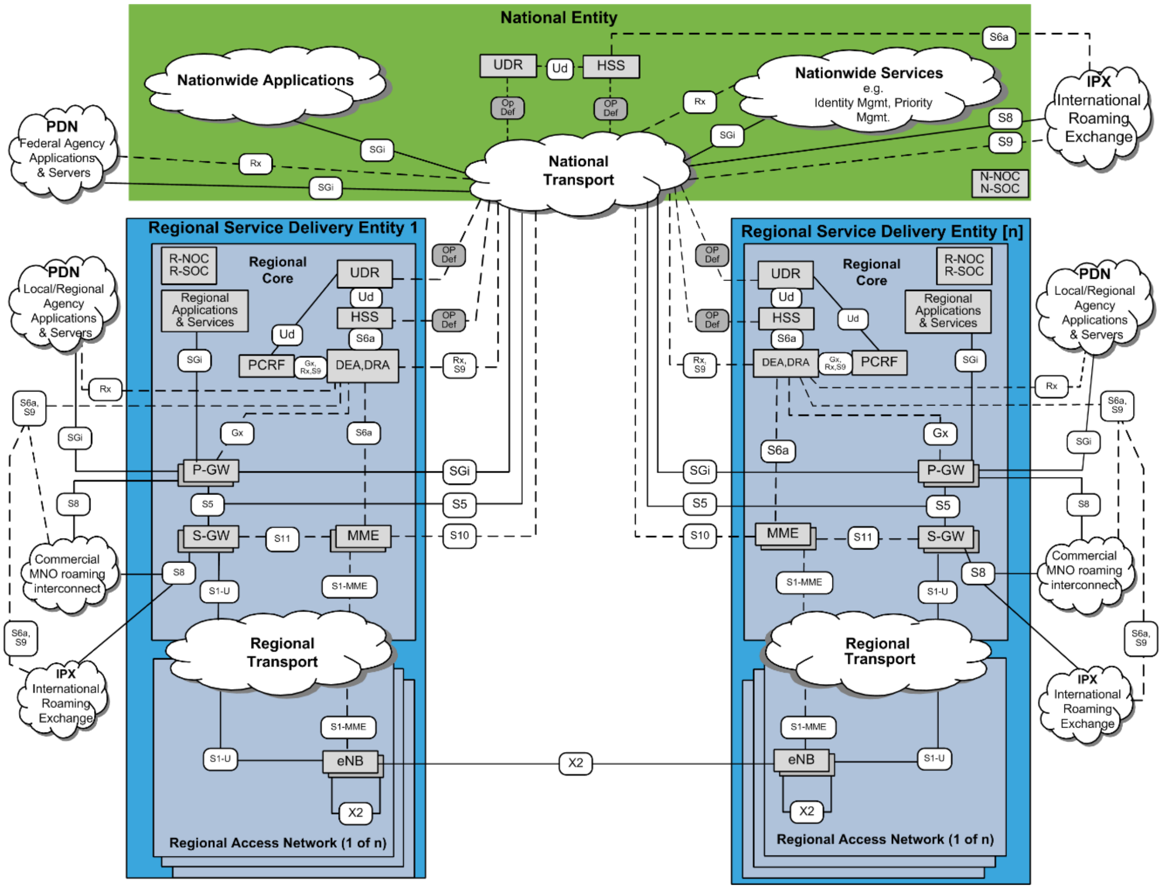

National Entity
Nationwide Applications
UDR
Ud
HSS
Op Def
OP Def
Nationwide Services
e.g. Identity Mgmt, Priority Mgmt.
S6a
IPX International Roaming Exchange
PDN Federal Agency Applications & Servers
Rx
SGi
National Transport
S8
S9
N-NOC N-SOC
Regional Service Delivery Entity 1
Regional Service Delivery Entity [n]
R-NOC R-SOC
Regional Core
Regional Applications & Services
PDN Local/Regional Agency Applications & Servers
PCRF
Gx, Rx,S9
DEA,DRA
S6a
Rx, S9
S6a, S9
Gx
P-GW
S5
S-GW
S11
MME
S10
Commercial MNO roaming interconnect
S1-U
S1-MME
Regional Transport
eNB
X2
Regional Access Network (1 of n)

Figure 5: *Multiple RSDE operators with National Entity.*

The national entity would provide national functions, such as national applications and services. The national entity would provide external network attachment for federal agency networks via the RSDE gateways, FirstNet interconnection and a national transport network. The RSDEs may partner with regional MNOs and would provide regional functions. RSDEs would also provide regional services, applications, NOC, SOC and gateways to external regional networks. RSDEs would provide connection to external networks such as local/regional agency networks, regional commercial roaming partners, IPX commercial roaming points of attachment for regional, national and international networks.

The national entity would provide a central repository for all PSBN user data such as subscriber profiles and other user data. This user data is stored in the UDR. Each RSDE would have its own UDR and would synchronize with a national entity UDR for all subscriber and subscription information. The connection shown between the NE UDR and RSDE UDR is used to indicate the interface for synchronization. This interface is labelled as the OP-Def interface which stands for operator defined. At the time of this writing, multiple standards for the inter-UDR synchronization exist and as such, the national and regional operators would need to agree upon a single standard and the associated interfaces, and the procedures for synchronizing the UDRs (e.g., using Lightweight Directory Access Protocol (LDAP) to communicate between the UDRs).

The national entity would also host a national level HSS that contains an aggregation of information from each RSDE HSS. The NE HSS and the RSDEs' HSSs need to be synchronized. The connection shown between the NE HSS and RSDEs' HSSs is used to indicate the interface for synchronization. This interface is also labelled as an OP-Def interface since at the time of this writing, multiple standards exist for inter-HSS synchronization. As such, the national and regional operators would need to agree upon a single standard and its associated interfaces, and the procedures for synchronizing the NE HSS and RSDEs' HSSs.

Within the PSBN, it is assumed that the NE will deploy, manage, and maintain the following functions:

Table 3: *National Entity functions.*

Function	Description
Spectrum Responsibility	ISED has allocated 20 MHz of nationwide spectrum for the PSBN in the 700 MHz band (downlink: 758–768 MHz and uplink: 788–798 MHz).
National Transport	The national transport interconnects the RSDEs and allows these entities to connect to the master subscriber database and to national services and applications. The QoS-aware national transport can consist of multiple transport, network, and data link technologies. These can include satellite backhaul links.
Master User Data Repository	The master UDR contains subscriber information for every user in the PSBN. Authorized EUA administrators must have access to the UDR in order to enter, modify, or delete user profiles. The NE UDR will be synchronized with the RSDEs' UDRs.
Master Home Subscriber Server	The master HSS stores the information of each user in the network and performs the authentication and authorization of the users and services provided to them. It contains users' subscription data such as the subscribed QoS profile and any access restrictions for roaming. It also holds information about the PDNs to which the user can connect. The NE HSS will be synchronized with the RSDEs' HSSs.
National Services	National services are services such as user location displays or identity management databases that can be used by End User Agencies, regardless of where they operate in Canada.
National Applications	National applications are applications such as user VoLTE, SMS and Mission Critical Applications that can be used by End User Agencies, regardless of where they operate in Canada. The testing and certification of the national applications is expected to be the responsibility of the NE.

Function	Description
Regional, national and international roaming agreements	NE would enter into and manage the agreements, on behalf of the PSBN, for roaming and interconnection to partner networks. This includes inter-working agreements with FirstNet. The inter-working gateways with the external roaming exchanges and interconnections would be hosted at the regional level.
International roaming via IP exchange (IPX)	Through a RSDE, the national entity would put into operation a connection to an IPX service provider that would support international roaming exchange. The physical attachment between the RSDE and the IPX service provider would be done using the GSMA IR.34 guidance [16].
National Network Operations Centre	NE would operate the national Network Operations Centre (NNOC).
National Security Operations Centre	NE would operate the national Security Operations Centre (NSOC).

Within the PSBN, the regional service delivery entity will deploy, manage, maintain, and operate the core network and access networks as described in the following table.

Table 4: *Regional service delivery entity functions.*

Function	Description
Core Network	The RSDE is responsible for the deployment and operation of the EPC, HSS/UDR, PCRF components.
Radio Access Network(s)	The radio access network is composed of evolved eNodeBs, WiFi access points and possibly other RAN technologies that are distributed across the region.
Regional Transport	The regional transport interconnects the regional operations multiple radio access networks with the main core components. It allows clients in the access networks to connect to regional services, applications and data networks. The QoS-aware regional transport can consist of multiple transport, network, and data link technologies. These can include satellite backhaul links. The regional transport shall abide by the same QoS requirements as the national transport.

Function	Description
Connection to End User Agency and federal agency networks	End user agencies and federal agencies can attach their network or part of their network to the PSBN. The RSDE would provide an APN and configure a packet gateway and a firewall to connect to these particular packet data networks. The end-user agency and federal agency administrators would then be able to select that APN for their users. It is expected that the specific agency network would only be available to the users of that particular agency, though this does not preclude the agency from allowing access to other users.
Bilateral interconnect with national and regional commercial networks	Each RSDE would operate and manage the bilateral interconnect functions with national and regional commercial MNOs to provide the ability for end-users to non-seamlessly roam between PSBN and the commercial network. In some cases, it would be possible to implement seamless mobility between the PSBN and the commercial networks.
International roaming via IP exchange (IPX)	Each RSDE, working with the national entity, would put into operation a connection to an IPX service provider that would support international roaming exchange. The physical attachment between the RSDE and the IPX service provider would be done using the GSMA IR.34 guidance.
Regional Services	Regional services are services that are critical to the operation of the PSBN in that region.
Regional Applications	Regional applications are applications such as user VoLTE, SMS and Mission Critical applications that can be used by Canadian End User Agencies, if the national entity is not reachable.
Operation Support System	Each RSDE will have the necessary operations, administration, management and provisioning functions to manage the RSDE resources of the PSBN.
Business Support System	Each RSDE is likely to contract with a partner MNO for operating the RSDE's part of the PSBN. In any MNO, it is necessary to provide Business Support System functions such as customer billing and customer relationship management.
Regional Network Operations Centre	Each RSDE will be able to operate their own Regional Network Operations Centre (RNOC).
Regional Security Operations Centre	Each RSDE will be able to operate their own Regional Security Operations Centre (RSOC).

4.1.3 Multiple RSDEs, national entity with regional RAN operation

Similar to the second architecture, this one is based on the two-tiered service deliver model described in Figure 3 but differs in that the NE, whose function is to provide a federating layer for the RSDEs, is now able to provide the regional core and gateways on behalf of RSDEs that have elected to delegate this operation to the NE. In this architecture, an RSDE would deploy only the RAN while other RSDEs would deploy the RAN and a core network. In effect, this “hybrid” architecture illustrates that the PSBN network architecture can be flexible and adapted to the needs to each region.

This is illustrated in Figure 6.

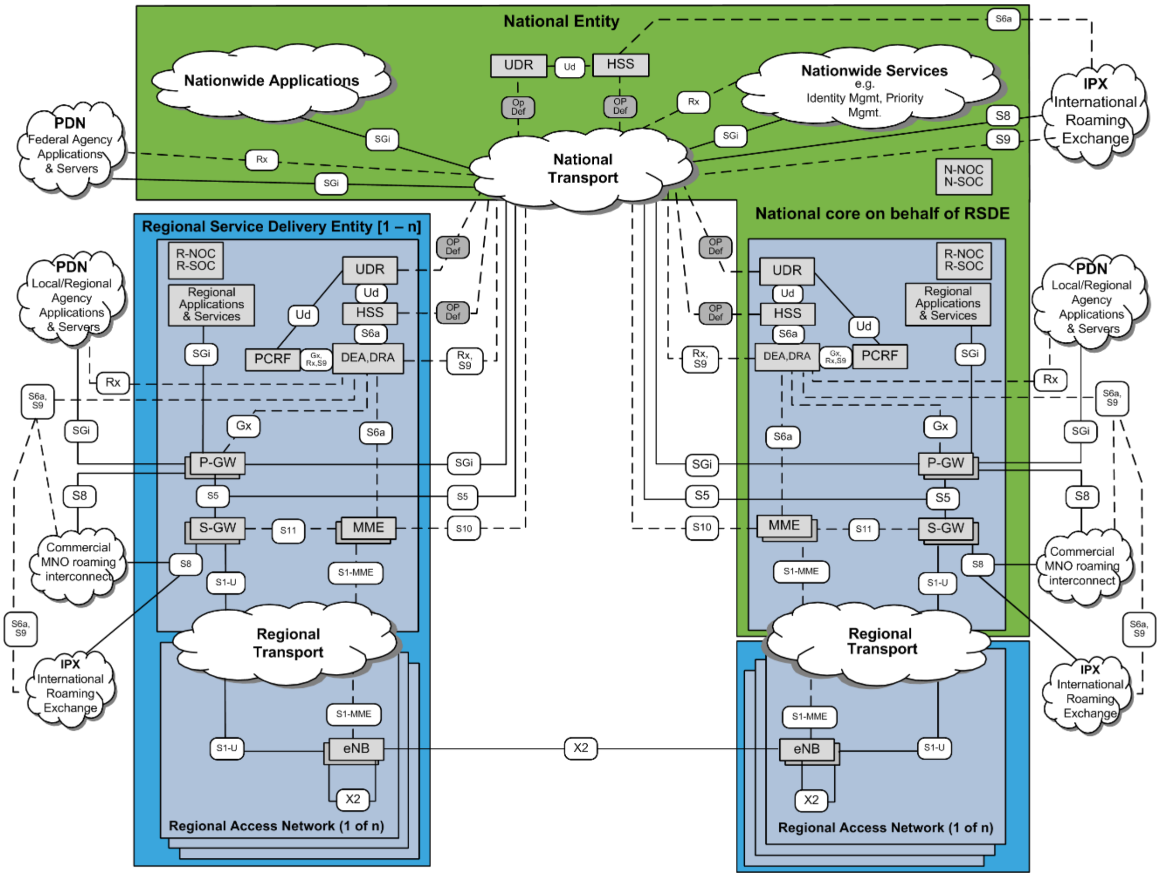


Figure 6: *Multiple RSDEs, national entity with regional RAN operation.*

Figure 6 illustrates a close variant to the architecture shown in Figure 5. The difference here is that the national entity, on behalf of a particular region(s) of Canada and upon request of the region(s), may partner with a regional MNO to provide regional transport, core, services, gateways, applications, operations support, business support, a Network Operations Centre, and a Security Operations Centre (SOC). The RSDE is still responsible for providing and operating the regional access networks (e.g., Band 14 LTE RAN, trusted WiFi).

Figure 6 represents simply one example of a variation of the architecture presented in Figure 5. Other such variations could be where the national entity also provides and operates the RAN on behalf of the region, through partnership with a regional MNO. Yet another could be where the region arranges to join an existing RSDE, thereby alleviating the need for support from the national entity.

4.2 PSBN base architecture components and reference points

Table 5 and Table 6 respectively list and describe the components and reference points (interfaces) for the three network architectures shown in Figure 4to Figure 6.

Table 5: *PSBN network block diagram components.*

Component	Name	Description
EPC	Evolved Packet Core	The EPC of an LTE network consists of the Serving Gateway, the Packet Data Network Gateway and the Mobile Manager Entity. When complemented by the Home Subscriber Server and the Policy and Charging Rules Function (PCRF), the whole is referred to as the Evolved Packet System (EPS).
S-GW	Serving Gateway	The S-GW is the point of interconnect between the radio-side and the EPC; all user IP packets are transferred through the S-GW. The S-GW routes and forwards user data packets and serves as the local mobility anchor for the data bearers when the User Equipment (UE) moves between eNodeBs. It also retains the information about the bearers when the UE is in the idle state and temporarily buffers downlink data while the MME initiates paging of the UE to re-establish the bearers. In addition, for certain roaming approaches, the PSBN S-GW can perform some administrative functions in the visited network such as collecting information for charging (for example, the volume of data sent to or received from the user) and lawful interception. It also serves as the mobility anchor for interworking with other 3GPP technologies such as General Packet Radio Service (GPRS) and Universal Mobile Telecommunications System (UMTS).
P-GW	Packet Data Network Gateway	The P-GW is the point of interconnect between the EPC and the external IP networks. It provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. It is responsible for IP address allocation for the UE, as well as QoS enforcement and flow-based charging based on rules from the PCRF. It also serves as the mobility anchor for interworking with non-3GPP technologies such as WiFi.
MME	Mobility Management Entity	The MME is the key control-node for the LTE access-network. It is responsible for idle mode UE tracking and paging procedure including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW for a UE at the initial attach and at time of intra-LTE handover involving core network node relocation. It is responsible for authenticating the user by interacting with the HSS.

Component	Name	Description
PCRF	Policy and Charging Rules Function	The PCRF is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities which resides in the P-GW. It provides the QoS authorization that decides how a certain data flow will be treated by the P-GW and ensures that this is in accordance with the user's subscription profile.
UDR	User Data Repository	The UDR is a database that stores all user related information. As specified in 3GPP Technical Specification (TS) 23.335 [17], each network element or application that employs user related data implements a Front End (FE) then connects the frontend via the Ud interface to the UDR.
HSS	Home Subscriber Server	The HSS is a data base that stores the information of each user in the network and performs the authentication and authorization of the users and services provided to them. It contains users' subscription data such as the subscribed QoS profile and any access restrictions for roaming. It also holds information about the PDNs to which the user can connect. In addition, the HSS holds dynamic information such as the identity of the MME to which the user is currently attached or registered. In the case where both a HSS and UDR are in the same core network, the HSS will then not store any user data in its database, but store that information in the UDR using the HSS frontend and the Ud interface to access the UDR.
DRA	Diameter Routing Agent	The DRA provides routing capabilities for the Diameter control protocol used by many LTE core network components to exchange information about end-user device tracking, session tracking, session management, data usage, entitlements and other details. The DRA allows for the centralization of the Diameter routing functionality, therefore avoiding a Diameter mesh between core network components. While not required in the EPC, DRAs simplify network deployment and facilitate future expansions.
(N/R) NOC	Network Operation Centre	The Network Operations Centre is the organizational function from where the PSBN is administered and monitored. There are two instances: national NOC (NNOC) and regional NOC (RNOC). The NNOC and RNOC have full control and monitoring of their respective PSBN resources.

Table 6: *PSBN network block diagram reference points.*

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

The remaining sections of this Scientific Report expound on the groupings of functional components that make up the PSBN, as captured in the yellow block in Figure 2. The groupings of components consist of:

- Wireless access network
- Roaming

- Base functions
- Enhanced functions
- Network and security management
- Service management

From this point forward in the Report, the architecture described in Figure 5 will serve as the basis for all technical considerations and descriptions that follow. This approach is taken since that option is sufficiently comprehensive such that technical information relevant to derivative architectures can be extracted.

5 PSBN wireless access network

Broadband mobile networks based on fourth generation 3GPP standards have a Core Network (CN) and a Radio Access Network.

5.1 Core Network (CN)

The PSBN architecture is based on existing wireless communication standards. More specifically, the architecture is designed according to 3GPP's System Architecture Evolution (SAE) to provide Internet Protocol (IP) based voice and data services to users including the first responder community. In 3GPP TS 23.002 [18], Section 6, there is a listing of the PLMN basic interfaces and reference points. The core components of the architecture include the EPC, a high-capacity, all-IP core network capable of providing real-time and media-rich sessions for mobile users. The EPC is responsible for the overall control of the UE, the establishment of the bearers, and configuring the communication channels with QoS or flow-based data transmission characteristics.

As shown in Figure 4, most of the CN components are in the national operator with gateways located in the regional operations of the network. In Figure 5 the core network components are located within the national RSDE level in the area identified as the regional core. Additionally, the national entity may host the core network on behalf of one or more of the RSDEs as described in Figure 6. However, if an RSDE elects to have the NE host the core network as is the case in the architecture described in Figure 6, the RSDE would still be responsible to deploy the RAN to provide cellular coverage for its region's subscribers.

For the PSBN architecture in Figure 5, which serves as the basis for this Scientific Report, the HSS and UDR would exist at the RSDE level, but also at the NE level. The NE UDR would act as a centralized (master) UDR that is synchronized with the RSDEs. This allows for the centralization of subscriber information for every user in the PSBN, thereby providing a single point of entry for provisioning, authentication and authorization regardless of the jurisdiction that the user belongs to. The same would apply to a centralized (master) HSS synchronized with the RSDEs' HSSs.

Each RSDE would be expected to deploy, maintain and operate a regional core to meet the communication requirements of public safety entities in the region, while maintaining interoperability with networks of other RSDEs. This model provides flexibility for the regions to develop and deploy their respective regional core based on their timelines and according to their operational requirements and financial abilities. It also allows for regions to control the equipment provider selection process and to enter into agreements with regional commercial operators for purposes of building, operating, and/or entering into various sharing arrangements. It is common practice that all core network components are duplicated and monitored regularly. These should be duplicated in a geographically separate location such that the RSDE can remain operational if the main components become damaged or disconnected. The duplicate components should be located in a region that is not subject to the same environmental hazards as the main network components, and should be powered from a separate power grid. This level of redundancy can tolerate the simultaneous failures of two serial network elements and the catastrophic failure of the main components. All components should be interconnected by a redundant backbone network where each fibre (assuming a fibre optic backbone) should be carried on a different physical bundle and each bundle should be routed on a different geographic path. This is to avoid the possibility that a disruptive event cuts one fibre bundle thereby taking out the entire backbone network. Regional networks should also have redundant connections to the backbone network.

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

5.1.1 Evolved Packet Core (EPC)

In 3GPP TS 23.401 [19], the named EPC network elements are the S-GW, P-GW and MME. Often, the industry has considered the EPC to include the HSS and PCRF, but for the purposes of this Scientific Report, both are treated separately. The S-GW serves as the mobility anchor for 3GPP roaming and handover operations as well as some packet forwarding and administrative functions. The P-GW provides PDN connection end point services for UEs and external Packet Data Networks, and provides mobility anchor for external non-3GPP networks. The MME deals solely with the control plane. It handles the signalling related to mobility and security for the Evolved Universal Terrestrial Radio Access Network (E-UTRAN)[5] access. The MME is responsible for the tracking and the paging of UEs in idle mode. It is the termination point of the Non-Access Stratum (NAS).[6]

5.1.2 PSBN Home Subscriber Server (HSS)

Within the PSBN, the HSS is implemented in the national entity, the RSDEs and certain types of deployable systems. These HSS implementations would support an additional interface, referred to as Ud that connects to the UDR. An important consideration within the two-tiered PSBN is that these HSS/UDR instances need to be kept in synchronization with each other. The master of record user information will be kept in the NE UDR. The RSDE HSSs and the deployable system HSSs will each contain a subset of the user information, but as stated in the assumptions section of this document, it is expected that any PSBN user device that is authorized will be able to access the set of services, applications and information by accessing any RSDE or deployable system. In 3GPP TS 29.336 [20], "Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications," describes interactions between the HSS and a range of networks, applications and the Service Capability Exposure Function (SCEF).The SCEF is further described in Section 10.1.1.

5.1.3 Policy and Charging Rules Function (PCRF)

In 3GPP TS 23.203 [21], the PCRF is the Policy and Charging Rules Function that controls differentiated services for subscribers accessing and communicating with other users, services and applications.

The PCRF is used for assigning QoS, Priority retention and Pre-emption attributes to specific authorized LTE bearers that support different classes of users, services and applications. The PCRF can be used during handover and roaming operations to ensure that the proper policy and charging rules are provided during the user mobility operation.

[5] E-UTRAN consists of the LTE UE and eNodeB.

[6] The NAS is a functional layer within the EPS that manages the establishment of communication sessions and maintains continuous communications with the user equipment as it moves.

5.1.4 User Data Repository (UDR)

The User Data Repository (UDR) is a database that stores all user related information. As specified in 3GPP TS 23.335 [17], each network element or application that employs user related data implements a FE and connects the front end via the Ud interface to the UDR.

5.1.4.1 User Data Convergence (UDC)

The PSBN contains many ways to store and retrieve user related information from many different network elements and applications. As shown in the previous PSBN architecture diagrams, e.g., Figure 5, the User Data Convergence (UDC) concept has been introduced into the RSDE and into the NE. All network elements (e.g., HSS), services (e.g., IMS/VoLTE) and applications (e.g., Mission-Critical Push-to-Talk) will use the UDC front ends to gain access to user related information that is stored in the UDR.

In keeping with the 3GPP network architecture (3GPP TS 23.002 [18]) and service principles (TS 22.101 [22]), 3GPP has created service requirements, (3GPP TR 22.985 [23]) and technical architecture specifications, (3GPP TS 23.335 [17]) for UDC. The benefit of incorporating the UDC into the PSBN versus a network that does not use UDC is shown in Figure 7. When UDC is not used then data that pertains to users is contained in many different network elements, thus making the job of maintaining this data more difficult and increasing the possibility of storing the same user data inconsistently across the network. With UDC, the UDR acts as a central repository for user-related data, instead of having it stored in different parts of the network. With the UDR containing all the user-related data in a network then each network element and application will implement a front end which provides the necessary support to access the UDR to store and retrieve the data.

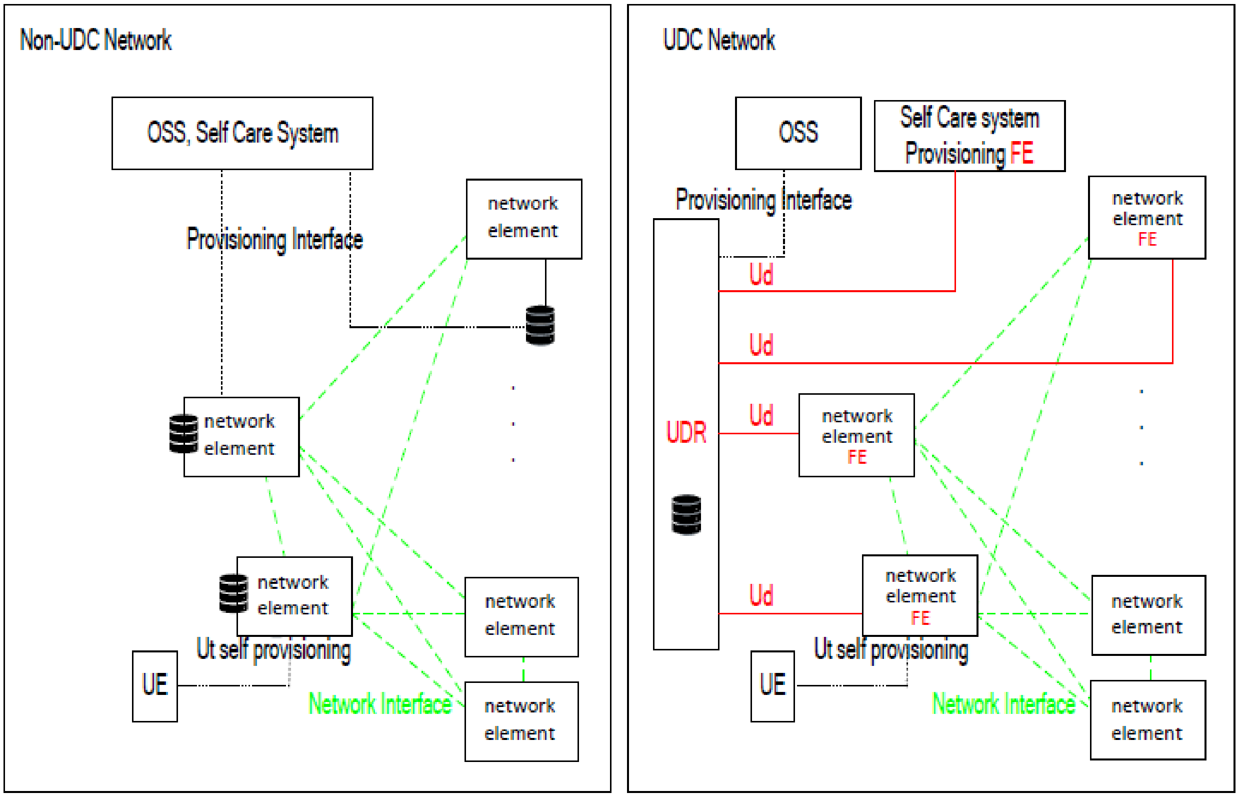


Figure 7: Comparison of non-UDC network to UDC network (adapted from 3GPP TS 23.335 [17]).

5.1.4.2 User Data Convergence (UDC) architecture

The UDC method supports a layered architecture, separating the data from the application logic in the 3GPP system. By doing so, user-related data is stored in a logically unique repository allowing access from core entities and service layer entities, named network element FE and application FE, respectively. Entities that do not store user data but need to access user data stored in the UDR are collectively known as application front ends. Network elements and functionalities should be designed to access user-related data remotely and without storing them permanently locally i.e., the front ends shall work in a subscriber data-less configuration. In the UDC architecture, the UDR is a functional entity that acts as a single logical repository of user-related data. In Table 7, the UDC architectural components and corresponding descriptions are provided.

***Table 7:** User Data Convergence (UDC) components.*

Component	Description
User Data Repository	The User Data Repository (UDR) is a functional entity that acts as a single logical repository that stores converged user data. The user-related data that traditionally has been stored in the HSS, Home Location Register (HLR), Authentication Centre (AuC), application servers, etc., is now stored in the UDR according to a UDC information model. UDR facilitates the sharing and the provisioning of user-related data

Component	Description
	throughout services of 3GPP systems.
Application Front End	Functional entities such as the HLR/HSS/AuC, application servers, the Access Network Discovery and Selection Function in home network (H-ANDSF), any other Core Network nodes, provisioning systems, etc., keep the application logic, but they do not locally store user-related data permanently when the UDC architecture is applied. These data-less functional entities are collectively known in the UDC architecture as application FEs. The application that is handled by a FE determines the type of FE. A HSS Front End may implement a full or a part of the HSS functionalities as listed in 3GPP TS 23.002 [18], this choice being implementation dependent. The reference points between the different FE and the core and service layers are not affected by the UDC architecture.
Provisioning Front End	A provisioning FE is an application FE for the purpose of provisioning the UDR. A provisioning FE provides means to create, delete, modify and retrieve user-related data. However, the provisioning should not be allowed to manipulate on the common baseline information model.[7]
Network Element Front End	Other network elements, which in their original form represent pure application logic with no persistent data storage functionality but with user data access towards an external database, may be assumed to perform the functionality of an application front end when the UDC architecture is applied. For example, for Mission Critical Services (MCS) (see 3GPP TS 23.280 [24]), the MCS server, and Configuration Management server may be considered as application FEs accessing MC Service user profile data via the Ud interface from the UDR.

5.2 Radio Access Network (RAN)

The PSBN's Radio Access Network is based on E-UTRAN's LTE standard, described in 3GPP TS 36.300 [25]. The main component of this standard is the evolved Node B, or eNodeB, or eNB. This network node communicates directly with the User Equipment and to the EPC. There are multiple types of radio access technologies (RAT) that are available for the RSDEs to consider for their RAN implementation: i) Band 14 LTE eNB, ii) Band 14 home eNB (HeNB), iii) Band 14 deployable LTE, iv) trusted WiFi access points and v) partner LTE RAN. The first two types of radio access technology options would be owned, operated and managed by the PSBN. The third and fourth could be owned and operated by the PSBN but EUAs could also assume this responsibility. The last one may be owned, operated and managed by a partner carrier.

The RSDEs are responsible for deploying and maintaining the dedicated Band 14 RAN, RAN sharing and wireless access networks within their region (Sections 7–10). It is expected that they will deploy

[7] The common baseline information model (CBIM) of the UDC is an abstract, formal representation of entity types common to many applications using the UDR. CBIM provides flexibility in its data structure and content, extensibility and multi-application approach. In particular, CBIM provides support for the concepts of Subscription, Service Profile, End User, Identifiers, End User Group, and End Device, among others.

sufficient RAN components to serve their respective region, though exact coverage goals and strategies will depend on timelines, funds, national or regional policies, conditions of spectrum licence, etc.

The RAN components use the regional transport network to connect back to the regional core. In some cases, these components will be deployed in remote and rural areas which may not have a fixed backhaul link. These areas may have to rely on a satellite link or some other remote communications technology to connect back to the core. These scenarios are further described in Section 5.2.3.

RSDEs may also opt to use other RAN technologies such as WiFi in order to offload data or to allow users to access locally available hot-spots. Although this option is not shown in the network block diagrams, it is discussed in more detail in Sections 5.2.4 and 8.5.

5.2.1 Band 14 eNodeB

The main component of the PSBN's RAN is based on radio equipment operating in the 3GPP-designated Band 14. This was enabled by a decision paper issued by the Canadian Government's Innovation, Science and Economic Development (ISED) department in June 2017. The document, titled "Decision on Policy, Technical and Licensing Framework for Use of the Public Safety Broadband Spectrum in Bands 758–763 MHz and 788–793 MHz (D Block) and 763–768 MHz and 793–798 MHz (PSBB Block)" (SMSE-014-17) [26], effectively confirmed the designation of Band 14 radio spectrum for public safety use. Other important decisions on public safety spectrum that impact the PSBN architecture are stated in decisions D4 and D5 in the document.

> D4: Commercial use of unused capacity will be allowed provided that public safety users will have higher QoS, priority and pre-emptive rights over any form of commercial usage.
>
> D5: ISED will not mandate specific technology, though any technology employed on the 700 MHz public safety broadband spectrum must ensure national and cross-border interoperability and ensure priority and pre-emption capability for public safety services and must be consistent with the interoperability solution "sharing standards-based systems."

Decision D4 is of importance to the PSBN network architecture in that spectrum and network sharing become an important aspect of the architecture, as does the need to implement a Quality of Service (QoS), Prioritization and Pre-emption (QPP) strategy. Decision D5 is of importance in that, while no specific technology is being mandated, it states the need for cross-border interoperability. Since the US equivalent to the PSBN in Canada, FirstNet, is using Band 14 LTE in their network rollout, the interoperability requirement then suggests the use of LTE for the PSBN in Canada as well. As such, the main PSBN RAN technology considered in this Scientific Report is Band 14 LTE. In fact, no other alternative could be considered at present since all products currently being developed worldwide in Band 14 are based on LTE.

5.2.2 Home eNodeB

The PSBN may provide the ability to support a coverage extension option referred to as home eNodeB (HeNodeB), whose service requirements are described in the 3GPP TS 22.220 [27]. The following diagram illustrates how public safety agencies may consider using HeNodeB to extend cellular coverage. Essentially, it establishes a coverage area that is separate from the PSBN macro eNodeB coverage area, thereby offloading the local cellular traffic onto the HeNodeB and alleviating the load on PSBN macro eNodeBs.

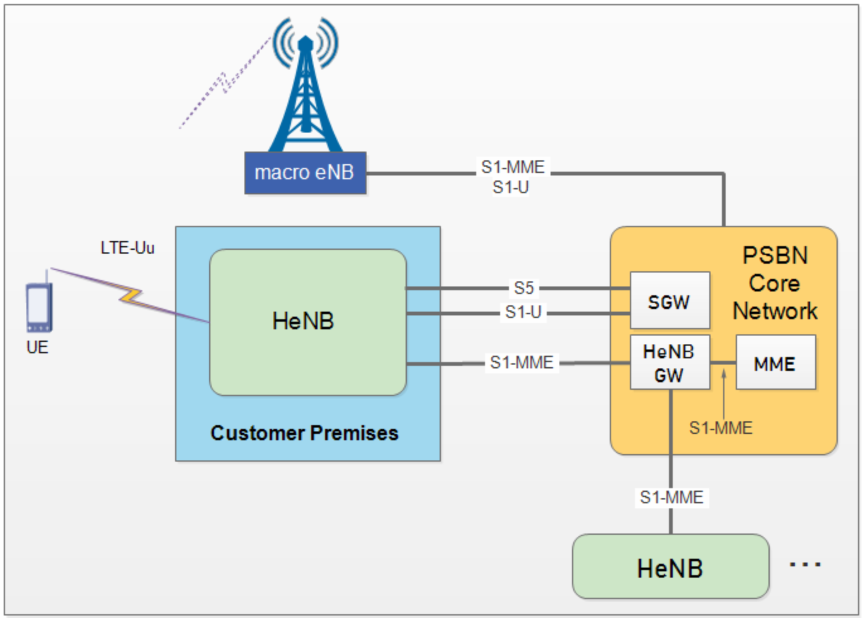


Figure 8: *HeNB service as an extension of the PSBN mobile operator's Radio Access Network (RAN).*

As illustrated in Figure 8, a HeNodeB extends the coverage of the RSDE Radio Access Network. This type of access may be provided by the PSBN Public Land Mobile Network (PLMN) by means of HeNodeB and the HeNodeB Gateway in the RSDE core. The HeNodeB is connected to the mobile operator core network using IP backhaul via any suitable backhaul access technology. All the service requirements for installation, Operations, Administrations, Maintenance and Provisioning (OAM&P), access control, mobility management, emergency services and interworking with other networks can be found in 3GPP TS 22.220 [27]. Typically, the PSBN MNO would be responsible for all aspects of an HeNB as it is an integral part of the network. The PSBN support of HeNodeB is based on reference architecture defined in TS 23.401 [19] and TS 36.300 [25].

5.2.3 Deployable PSBN

It is expected that Canada's public safety community will rely on deployable systems to deliver broadband services to isolated areas of the country where no broadband communications infrastructure exists, to areas where the infrastructure has been damaged, and to augment coverage and/or capacity at planned events or during emergency incidents. In the case of the former, deployables may also be considered to provide longer term coverage when no permanent infrastructure exists.

Deployable systems are expected to be used in the following circumstances:

- Extensions of the PSBN fabric to remote regions
- Augmenting the existing PSBN
- Isolated E-UTRAN Operation for Public Safety (IOPS)

Two types of broadband deployable systems (BBDS) that are considered to satisfy the above circumstances are: core-ready BBDS (CR-BBDS) and core-enabled BBDS (CE-BBDS) [28]. The former consists essentially of a radio access network, which can be an eNodeB, a Relay Node (RN), or a HeNodeB. There may be some ancillary functions contained within the CR-BBDS such as a security gateway for the S1 and X2 connections and a protected network management interface. The CR-BBDS requires a suitable backhaul connection to the macro PSBN network. The CE-BBDS contains all the core network functions and application servers in addition to what is in the CR-BBDS. The CE-BBDS should be able to deliver mission-critical services to users when it is isolated from the macro PSBN network. As such, the network elements and reference points that are associated with MCS would also be contained in the CE-BBDS. Note that even when the CE-BBDS is connected to the macro PSBN, there are advantages to using the local Mission Critical Services (MCS) capabilities and application servers in order to minimize traffic on the backhaul. Both types will be described in the following sections.

Furthermore, in any of the above circumstances where there is a need for the use of deployables, it can be surmised that commercial mobile service may also be unavailable. Deployable systems could then be shared with commercial MNOs to offer their commercial services to consumers of their respective commercial mobile network while at the same time serving public safety users. In this case, only the spectrum is shared. Traffic would be carried on two separate cores—one for public safety traffic; the other for commercial traffic. The option is mentioned in this Scientific Report to illustrate the possibility that spectrum sharing can extend to deployable systems as well. It is not suggested by the authors that such a configuration be typical of deployable systems.

The three circumstances where the use of deployables can be considered are described in the following sections.

5.2.3.1 Deployable PSBN systems in remote regions

Broadband deployable systems can be used to extend the footprint of the PSBN into areas that are difficult or not economical to serve with permanent infrastructure. These systems may not have terrestrial backhaul and are typically connected by satellite to the PSBN fabric. It is assumed that this satellite backhaul connection has increased latency and a lower data rate than urban-deployed backhaul infrastructure. It may also have a higher Packet Loss Rate (PLR).[8] Due to this high latency and possible low availability of the satellite channel, a consideration is that an "anchor" deployable system could be configured as an EPC, as in the case for the CE-BBDS. Other deployable systems configured as eNodeBs may be connected to the anchor deployable system. These systems may be required to fulfill dual roles. That is, to provide fixed services during day-to-day operations and then to be transported to incident areas in their relative vicinity when incidents arise.

Figure 9 illustrates a network architecture for a fixed remote implementation of the PSBN (CE-BBDS). The network architecture assumes a satellite connection is available, which could be substituted by high-performance microwave backhaul. All authentication services (HSS) are supplied either locally by the remote system or by the RSDE with corresponding interfaces and protocols traversing the satellite/remote link. The fixed remote system could be operating in a totally disconnected or connected mode. In the disconnected mode, the deployable system contains the necessary network elements to host local application servers and packet data networks, and as such, all service comes from the fixed remote

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

system. This can alleviate the need to use satellite backhaul. In the connected mode, where there is sufficient backhaul capacity, the fixed remote system could connect the RAN directly to the RSDE core network and services.

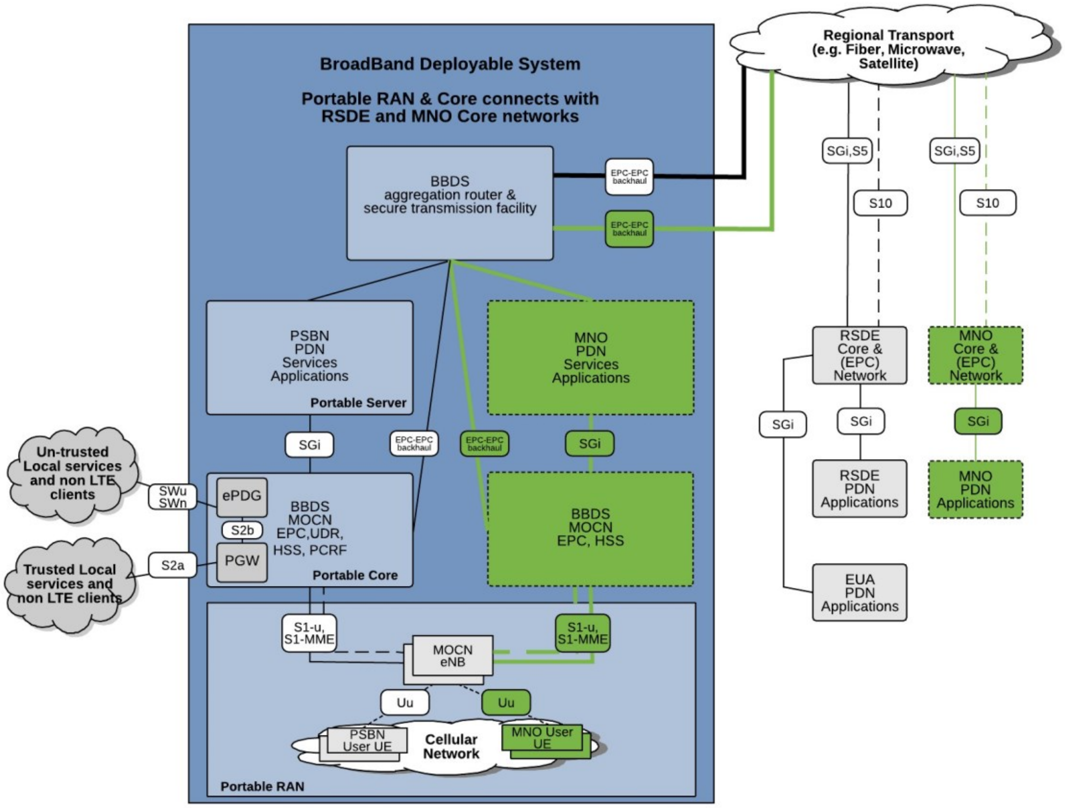

BroadBand Deployable System
Portable RAN & Core connects with RSDE and MNO Core networks
Regional Transport (e.g. Fiber, Microwave, Satellite)
BBDS aggregation router & secure transmission facility
EPC-EPC backhaul
EPC-EPC backhaul
SGi,S5
S10
SGi,S5
S10
PSBN PDN Services Applications
Portable Server
MNO PDN Services Applications
RSDE Core & (EPC) Network
MNO Core & (EPC) Network
SGi
SGi
SGi
SGi
EPC-EPC backhaul
EPC-EPC backhaul
SGi
RSDE PDN Applications
MNO PDN Applications
Un-trusted Local services and non LTE clients
SWu SWn
ePDG
S2b
BBDS MOCN EPC,UDR, HSS, PCRF
PGW
Portable Core
Trusted Local services and non LTE clients
S2a
BBDS MOCN EPC, HSS
EUA PDN Applications
S1-u, S1-MME
S1-u, S1-MME
MOCN eNB
Uu
Uu
PSBN User UE
Cellular Network
MNO User UE
Portable RAN

Figure 9: *Core-enabled deployable system containing MOCN-shared eNodeB and local core networks connected to public safety and commercial macro core networks and remote packet data networks.*

As illustrated in Figure 9 an additional capability has been added to the deployable system for enabling commercial MNO operators and their respective MNO users to share band 14 spectrum. This is enabled by using the 3GPP specified option called the Multiple Operator Core Network (MOCN) [29]. The MOCN capability can be optionally supported in the deployable system portable RAN via the supporting MOCN enabled eNodeBs connecting to two or more core networks. As the figure depicts, both PSBN subscriber UEs and commercial subscriber UEs can share the Band 14 spectrum. The traffic that is generated from each of the respective users stays on its respective core network, including across the backhaul by using Virtual Local Area Network (VLAN) encryption. This is required for security as well as performance reasons. MOCN is further described in Section 7.10.1.

In addition to separate portable core networks, the deployable system could support portable servers that could host applications and services from each respective operator. There is no minimum list of hosted applications at this time, as it is the responsibility of the EUA to specify what services and applications should be hosted on the deployable system.

Also shown are two potentially independent components that can be used to anchor and provide access to trusted and un-trusted data or services such as WiFi. The evolved Packet Data Gateway (ePDG) allows for an IPSec-based (SWu) interface between authenticated clients and services on the un-trusted network and the PSBN. This allows non-LTE wireless clients to be connected at the trusted and un-trusted levels. A description of the reference points can be found in Table 34.

In situations where the PSBN is deployed in remote regions, the reference points in Table 8 may be required to travel over satellite connections or another remote communications technology. The interfaces between the PSBN fabric and the remote deployable systems used in this manner need to be tolerant of high latency and relatively low grade of interconnection service.

Table 8: *Fixed remote deployments: reference points over satellite and other remote access technologies.*

Reference Point	Description
S2a	Proxy Mobile IP interface to and from remote trusted non-3GPP systems via a remote field P-GW. The non-3GPP trusted access network accesses the local P-GW and does not transit the backhaul transmission link.
S2b	Interface to and from the RSDE ePDG and remote field P-GW for un-trusted access to the remote field network from PSBN.
S5	Data interface for S-GW to RSDE, NE, or EUA interface. Uses GPRS Tunneling Protocol (GTP) or Duel Stack Mobile Internet Protocol version 6 (DS-MIPv6) protocol.
S6a	Signalling interface between HSS and remote field MME.
S10	Signalling interface to support handoffs between MMEs in multiple remote deployable systems.
SWu	Data interface for IPSec-secured communications between remote field un-trusted networks to ePDG within the RSDE or from RSDE, NE or EUA un-trusted networks to remote field network (via remote field ePDG).
Gx	Signalling interface for QoS configuration from remote field PCRF to RSDE, NE or EUA P-GWs, and from RSDE PCRFs to remote field P-GW.
Rx	Signalling interface for QoS requests from PSBN applications to remote field PCRF, and from remote field applications to RSDE PCRFs.

In some cases, the number of users in an area may not be significant. In these cases, small, localized, "EPC in a Box" solutions, consisting of a single hardware platform providing all core network functions, may be appropriate. However, many small Canadian communities have complex topographies and will require LTE deployments that are capable of providing for multiple eNodeBs, with corresponding RAN functionalities. Furthermore, even an "EPC in a Box" must provide for all the required 3GPP external interfaces to allow it to fully communicate with the PSBN core and thus provide full inter-agency interoperability. These solutions are typically offered as low-footprint/transportable form factors suitable for rapid deployment.

5.2.3.2 Deployable systems to augment PSBN

During an emergency or a planned event, initial response teams may need to establish a quick means of communication in areas where the PSBN is either not available, or does not provide the minimum communication requirements. Deployable PSBN systems can then be used to augment or extend coverage in order to increase capacity, or to restore communications service to areas where the macro PSBN has been taken out of service, which may result from severe natural events or man-made events. It is expected that these deployable systems can be connected to the regional core network with low latency backhaul. In such cases, rapidly deployable systems such as eNodeB-only Cell-on-Wheels (COW) or Cell-on-Light-Trucks (COLT) can be used in these cases. Where the incident areas are not accessible by road the deployable systems may be configured as "Cell in Backpacks" or "Cell in Fly-Away Kits." Although deploying these solutions may improve local communications, special care should be taken to ensure that the rapidly deployed network does not impact or disrupt other nearby PSBN cells.

As described in the previous section, deployable systems can be configured to be able to operate autonomously in case the backhaul cannot be easily or readily established. However, in cases where deployables are used to augment, extend or restore the PSBN within the macro PSBN coverage, CR-BBDS may be considered as an option. Figure 10 illustrates the use of the CR-BBDS. Since CR-BBDS does not contain a core network, the backhaul must be suitable to support the traffic and signalling requirements. All the information networks are remotely located from the BBDS and all traffic flows across the backhaul.

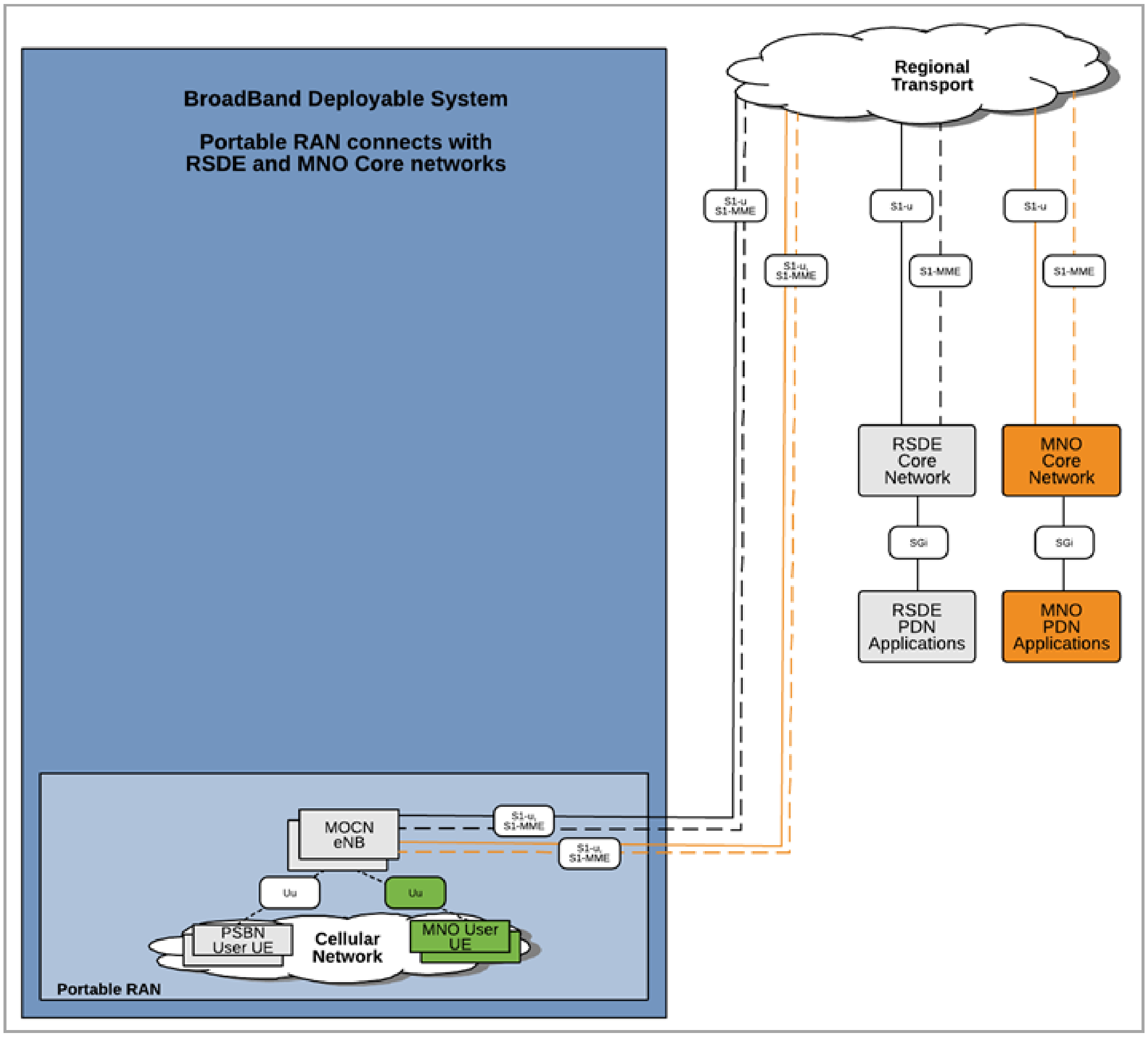


Figure 10: *Deployable system containing MOCN-shared eNodeB connected to public safety and commercial macro core networks and remote packet data networks.*

An extensive study of public safety use cases and user requirements for deployable systems has been conducted by DRDC CSS jointly with National Public Safety Telecommunications Council (NPSTC) [28].

5.2.3.3 Deployable systems used in isolation

When there is no macro PSBN fabric that can be used to anchor the deployable systems and there is no backhaul available to connect them to a regional core network, the BBDS are deemed to operate in isolation. In such a case, it is not possible to authorize users with the RSDE HSS, and it is therefore necessary to use a local UDR, HSS and PCRF as shown in Figure 11. The deployed network can thus operate in a fully self-contained fashion. The UDR, HSS and PCRF components allow other deployed components to operate without an external remote connection. This UDR and HSS may contain a subset of the national entity’s user credential database or may be temporarily left blank to allow for immediate communication requirements (e.g., while a remote connection to the NE’s HSS is being setup).The deployable system provides full, localized data services, alternate localized communication technologies, and 700 MHz UE access. When used in an isolated mode, the interfaces that are exposed are the ones that connect with other local networks such as WiFi and LMR networks. Core components highlighted in green are optional and would support negotiated service with a commercial MNO that wants to share Band 14 spectrum using MOCN during normal operation and also with IOPS

In this scenario, deployable systems can be expected to operate autonomously or in concert with other locally deployed systems. The key technical consideration is that there is no connection with the PSBN fabric or regional core network for the deployable systems used in this manner. However, the deployable systems would need to interconnect in order to coordinate radio resource assignments and transmit power levels in order to maximize the use of the available capacity. 3GPP TS 23.401 Annex K is an informative annex that provides implementation and operational guidance for a 3GPP Rel.14 functionality called "Isolated E-UTRAN Operations for Public Safety" (IOPS) [19].

When the deployable system operates in the IOPS mode, the deployable system is configured with a unique PLMN ID that is different from the one that is used by the PSBN and by BBDS that are connected to the PSBN core network. In addition, the UEs will have two USIM profiles on the Universal Integrated Circuit Card (UICC) that will be used to access the RSDE E-UTRAN and the BBDS E-UTRAN when operating in a standalone IOPS mode. The 3GPP TS 23.401 Annex K provides further guidance on this IOPS mode.

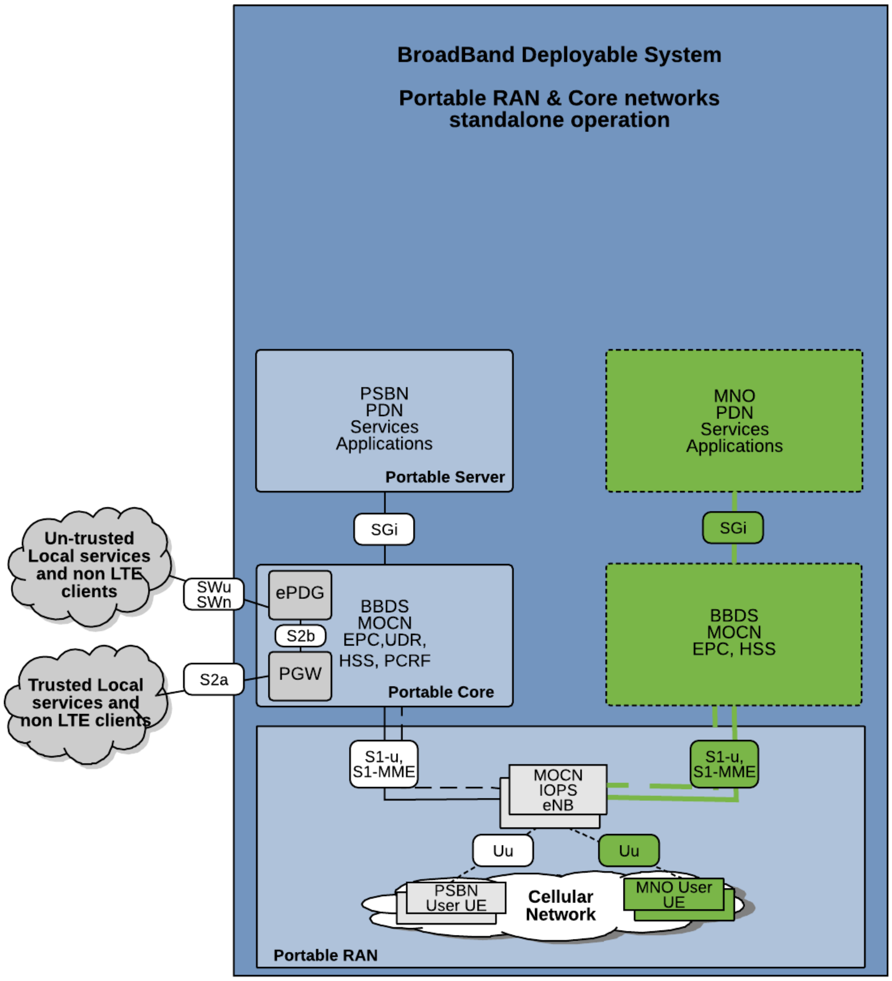

BroadBand Deployable System
Portable RAN & Core networks standalone operation
PSBN PDN Services Applications
Portable Server
MNO PDN Services Applications
SGi
SGi
Un-trusted Local services and non LTE clients
SWu SWn
ePDG
S2b
PGW
BBDS MOCN EPC,UDR, HSS, PCRF
Portable Core
BBDS MOCN EPC, HSS
Trusted Local services and non LTE clients
S2a
S1-u, S1-MME
S1-u, S1-MME
MOCN IOPS eNB
Uu
Uu
PSBN User UE
Cellular Network
MNO User UE
Portable RAN

Figure 11: *Deployable system in isolated mode of operation.*

If a communications link to the RSDE core becomes available at a later point (through satellite or other remote communication systems), the local UDR, HSS and PCRF may be disabled if necessary and if this does not impact local communication. The further aspects of clustering of BBDS instances, visibility of BBDS to the Network Operations Centre (NOC), local control and remote management of the BBDS are for further study.

5.2.4 Trusted WiFi wireless access

The 3GPP specifications define how interworking is achieved between an E-UTRAN (LTE and LTE-Advanced), and UTRAN (radio access network of UMTS-based technologies Wide Band Code Division Multiple Access (WCDMA) and High Speed Packet Access (HSPA)). All are within the scope of 3GPP. In addition to this, the PSBN should also support the use of non-3GPP wireless networks to which UEs can connect. 3GPP has specified support of other access technologies as well as the handover between these other access technologies. The notion of supporting other radio access technologies is to bring convergence using a unique core network providing various IP-based services over multiple access technologies.

Non-3GPP access networks are IP access networks that use access technology whose specification is out of the scope of 3GPP. These non-3GPP access networks can be used to quickly extend the coverage or improve the capacity of the PSBN when needed by offloading the LTE cellular RAN. PSBN devices can access such networks if they are interconnected with the PSBN RSDEs. The most common of such non-3GPP access networks include WiFi Hotspot 2.0 Release 2, which is a WiFi Alliance specification [30] (i.e., not 3GPP) that specifies network discovery, authentication, and roaming. 3GPP and the WiFi Alliance have been working together to integrate the following WiFi and cellular aspects: seamless mobility, access network selection and offloading from 3GPP Network to WLAN.

Non-3GPP access networks can be trusted or un-trusted from a PSBN perspective. Normally, the decision on whether a non-3GPP IP access network is trusted or un-trusted is not a characteristic of the access network. Rather, the decision is based on the PSBN operator's policy. While considering 3GPP TS 33.402 [31], Section 4.2, the following paragraphs summarize the differences between trusted and un-trusted non-3GPP access networks.

- For the trusted non-3GPP access network, it is the home operator policy decision that determines if a non-3GPP access network is treated as a trusted non-3GPP access network. When all the security feature groups provided by the non-3GPP access network are considered sufficiently secure by the home operator, the non-3GPP access network may be identified as a trusted non-3GPP access network for that operator. However, this policy decision may additionally be based on reasons not related to the security feature groups. Typically, trusted non-3GPP access networks are managed by a single administrative authority and use the same level of security and usage of security services.
- For the un-trusted non-3GPP access network, it is the home operator policy decision if a non-3GPP access network is treated as un-trusted non-3GPP access network. When one or more of the security feature groups provided by the non-3GPP access network are considered not sufficiently secure by the home operator, the non-3GPP access may be identified as an un-trusted non-3GPP access for that operator. However, this policy decision may additionally be based on reasons not related to security feature groups.

Trusted WiFi is the only non-3GPP wireless access technology considered to be part of the PSBN. To enable trusted WiFi, EUAs would request that the PSBN network administrators activate their WiFi access points after complying with the regional and national policies. In addition, the RSDE may own its own network of WiFi access points that are made available to the EUAs. The primary 3GPP architecture specification for supporting trusted or un-trusted non-3GPP access is TS 23.402 [32]. Within TS 23.402, there are different PSBN core network components that support attachment of a non-3GPP trusted or un-trusted networks. For trusted WiFi access points that connect to the PSBN RSDE via a land based connection, the 3GPP TS 23.139 [33] defines the system description of the security, mobility, policy, QoS aspects between the PSBN (based on 3GPP standards) and a fixed broadband access network such as WiFi, as well as the respective interactions with the Policy Charging Control (PCC) frameworks. The BroadBand Forum (BBF) has defined the architecture functions for land-based access and has worked with 3GPP to include them within the TS 23.139.

Figure 12 illustrates the architecture functions of the Broadband Network Gateway (BNG), the Broadband Policy Control Function (BPCF) and the Broadband Authentication, Authorization and Accounting (AAA) functions. These are the main network elements used to attach a fixed based access network to the PSBN.

The PSBN may not own or manage these non-3GPP access network elements but provides support for the 3GPP specified interfaces that provide access to the RSDE cores. As indicated in the figure, there are specific 3GPP specified interfaces that are used to connect with the EPS that is in the PSBN RSDE. The red dotted line in the figure delimits the 3GPP network and non-3GPP network boundary.

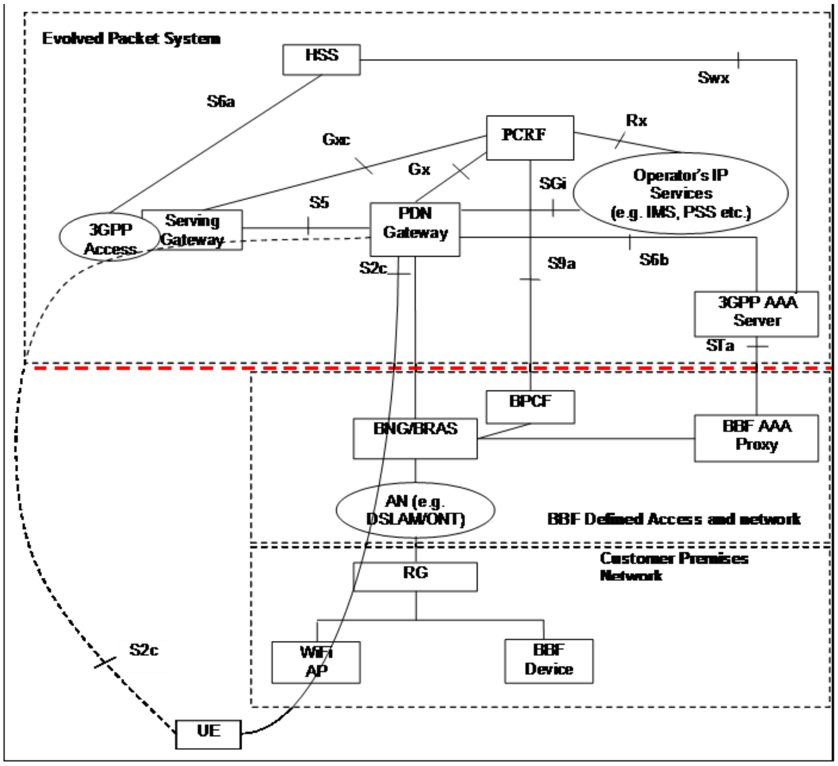


Figure 12: *Non-roaming architecture for trusted fixed broadband (source: 3GPP TS 23.139 [33]).*

5.2.5 Partner commercial mobile network

Within the PSBN, each RSDE could enter into an agreement with a partner MNO for operating the PSBN RSDE mobile network. The partner MNO that builds a separate LTE network for the PSBN RSDE mobile network could also have a commercial LTE network. Public safety users shall be able to attach to the partner's commercial mobile network when there is no PSBN connectivity in that coverage area. When the PSBN user goes outside of the PSBN coverage area, then LTE inter-PLMN handover is expected between the PSBN and the partner commercial mobile network. This capability is made possible by the PSBN and partner MNO putting in place the needed service level agreement and using the LTE inter-PLMN handover feature, as explained in 3GPP TS 23.401 [19]. Both networks will need to interconnect their respective cores using the 3GPP S10 reference point. This interconnect only serves the PSBN users that will be handed over to and from the partner MNO network, it does not enable commercial users to be handed over from the commercial network to the PSBN RSDE network. Traditional roaming, such as home routed or local breakout roaming does not apply to the partner MNO.

5.3 User Equipment (UE)

Within the PSBN, User Equipment (UE) is defined as those devices that are used by EUAs' personnel for the purposes of communicating with services and applications both within the PSBN and outside of the PSBN. The RSDEs are responsible for configuring the mobile devices with regional configure parameters. The EUAs are responsible for the procurement, ownership and operation of its own mobile devices in accordance with national policies. EUA administrators will also activate the services and mobile devices (e.g., UICC, USIM, International Mobile Subscriber Identifier (IMSI)).

Figure 13 illustrates the three layers of device functions. User device functions are indicated on the left-hand side of the figure and the management domains are on the right-hand side. The top layer indicates that application clients are in device memory and that these clients are part of the service infrastructure that comprises a server-side component. The right side set of EUA application clients are owned and managed by the EUA and managed by the mobile device management service. The left side set of PSBN application clients are managed as part of the service infrastructure using the PSBN mobile device management. In the middle layer, the left-hand side of the figure illustrates the device operating system and configuration parameters, and these also are administered by the PSBN administrator and managed by the mobile device management system. On the right-hand side of the middle layer, the Mobile Virtual Private Network (MVPN) client and the set of security policies are administered by the EUA administrator using the mobile device management system.

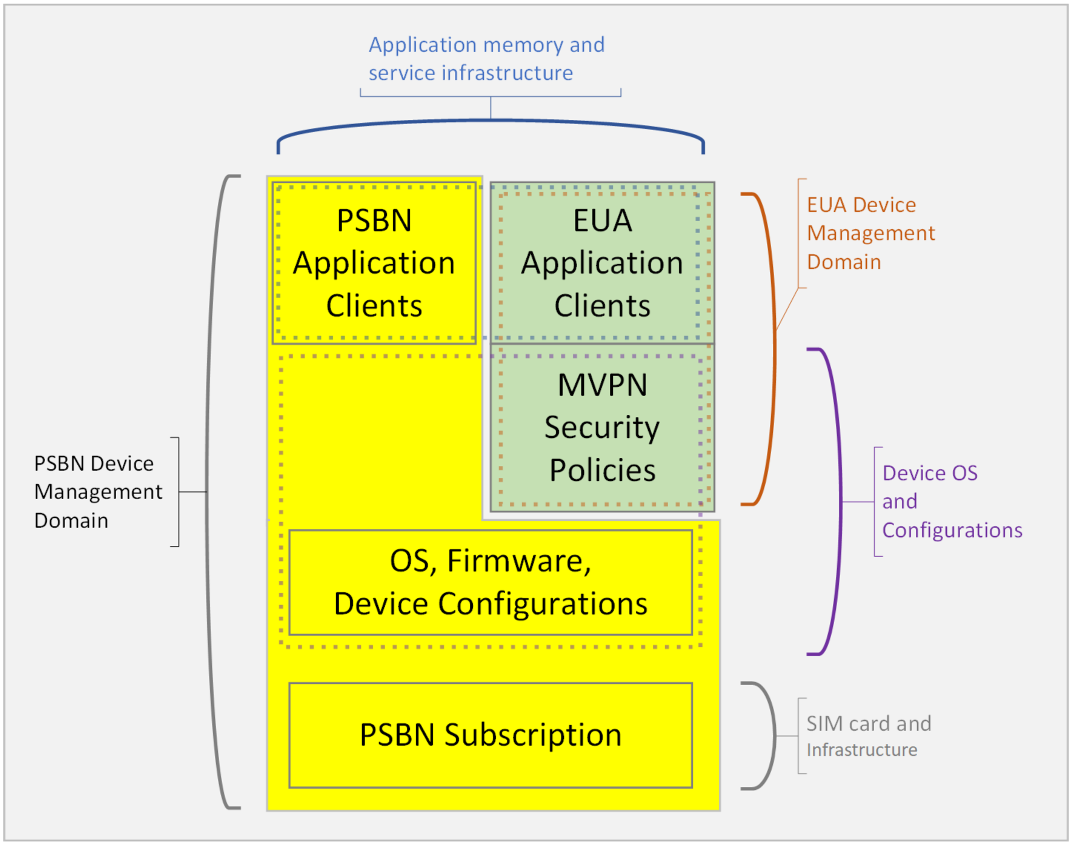

Application memory and service infrastructure
PSBN Application Clients
EUA Application Clients
EUA Device Management Domain
MVPN Security Policies
Device OS and Configurations
PSBN Device Management Domain
OS, Firmware, Device Configurations
PSBN Subscription
SIM card and Infrastructure

***Figure 13:** User device functions and management domains (adapted from NPSTC Local Control report [8]).*

5.3.1 Public safety mobile devices

PSBN Mobile Devices would use a UICC and USIM application. These devices also may be supporting IMS based Services, so an ISIM application is also integrated with the UICC and USIM.

5.3.2 Machine Type Communications (MTC) via sensors

The PSBN will have Band 14 sensors that will connect to the PSBN RSDE RANs and establish connections for uploading sensor data to analytics applications that are hosted in the EUAs, RSDEs or NE. The definition of a Machine Type Communications (MTC) device is a UE equipped for machine type communications, which communicates through a PLMN in real-time with MTC server(s) and/or other MTC device(s), also referred to as Machine to Machine (M2M) communications. The MTC service requirements and architecture are described in 3GPP TS 22.368 [34], TS 23.682 [35] and TS 29.368 [36].

5.3.3 Bring-Your-Own-Device (BYOD) support in the PSBN

Public safety entities and mutual aid volunteers could be using their own authorized mobile devices, referred to as Bring-Your-Own-Device (BYOD) to gain access to the PSBN network, services and applications. Using BYOD types on the PSBN will depend greatly on the NE, RSDEs and EUAs defining what the specific policy and rules are for use of BYODs on the PSBN and specific RSDE partner mobile networks. This document does not recommend a specific technical approach to support BYOD on the PSBN since it is so highly dependent on how the BYOD policy will be mandated by the EUA and PSBN.

5.4 Backbone and backhaul network

The separate domains of the PSBN will be interconnected via some form of backbone network. Similarly, eNodeBs will be connected to the Serving Gateways via backhaul network connections. These can be high capacity microwave, fiber, leased lines, or other media. It is beyond the scope of this document to specify the performance requirements (e.g., capacity, latency, availability) for the inter-domain backhaul.

5.4.1 IP interconnection nodes

Since the national entity and the RSDEs will deploy and maintain their respective networks, networking elements such as routers, switches, and firewalls are required in order to interconnect these networks into a single PSBN. To avoid service interruption, these devices are normally redundant and secure.

Table 9 describes the main IP network components used within the PSBN.

Table 9: *IP network components.*

Component	Description
Router	Routers interconnect different subnets together and allow one segment of a network to connect to another. Routers and firewalls can be combined in a single unit. The national entity is responsible for managing the network Identifiers (IDs). It is expected that the national entity will assign an IP address block to each RSDE. Each RSDE will then be able to set up and configure their respective network. In this scenario, each region would use one or more router within or at the borders of their network in order to connect to remote areas within their territory, to other entities via the national transport, or to other external networks.
Switch	Switches are used to distribute traffic within a respective network. Some switches include routing capabilities. For the purpose of this example, such switches are treated as routers as per the description above. It is expected that multiple switches will be deployed within each entity network in order to distribute traffic across the network. It is also expected that some if not all will use VLANs to separate and differentiate certain traffic flows.
Firewall	Firewalls protect the internal PSBN networks and are located at every ingress point within the network and in front of devices or networks which require more limited access. Firewalls rely on various access control lists (ACLs) to block incoming or outgoing traffic with specific ports or addresses. These ACLs may be different depending on the location and purpose of the firewall, though they should be tailored based on the policies and regulations of the National entity and the RSDEs.

6 PSBN roaming

Public safety users should be able to roam onto commercial mobile networks if an area of interest is not served by the PSBN or if the local PSBN does not meet the minimum connectivity requirements for the user. Roaming to or from Third Generation (3G) networks should also be supported as long as the 3G-LTE Internetwork Function (IWF) is implemented in the PSBN. The rule is that the most advanced network provides the IWF function. It is also possible for the IP eXchange (IPX) to provide the Signalling System 7 (SS7) modified application part (MAP)-DIAMETER IWF. In this scenario, an IPX service is used for international roaming and a bilateral interconnect service via a secure border gateway is used for national and regional roaming as the framework for mobile data roaming.

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

Table 10 lists the EPC reference points that must be shared to support roaming.

Table 10: *Reference points to support roaming onto commercial networks.*

Reference Point	Components	Description
S6a	Visited MME to home HSS	Required to authenticate users when roaming on commercial networks. Uses Diameter protocol.
S8	Visited S-GW to home P-GW	Required to allow users to connect back to PSBN networks and application networks when roaming.
S9	Visited PCRF to home PCRF	S9 is used if local breakout scenarios are used and dynamic charging and QoS policies are implemented between the home PLMN (HPLMN) and visited PLMN (VPLMN).

The 3GPP describes roaming and handover in TS 23.401 [19] between home PLMN and visited PLMN. When seamless handover is to be supported between PLMNs, then the MME-to-MME S10 reference point also needs to be supported.

From a PSBN user perspective, they should be able to move seamlessly and without disruption between the coverage areas of the RSDE macro LTE RAN, RSDE WiFi, deployable systems, partner commercial MNO networks and the FirstNet NPSBN. While it would be technically feasible to move seamlessly between the PSBN and non-partner commercial MNOs (regional, national or international), the actual realization could be more challenging as the MNOs involved could be commercial competitors. Of all possibilities, only FirstNet and non-partner MNOs would require roaming mechanisms.

Roaming to or from the PSBN is achieved using any of the following approaches:

- EPC-level roaming as defined in 3GPP TS 23.401 [19] and implementation guidelines provided in GSMA International Roaming (IR).88 LTE Roaming [37].

- IMS-level roaming as defined in 3GPP TS 23.228 [38] and GSMA IR.65 [39] IMS roaming guidelines.
- Non-3GPP Access (ex. WiFi) to 3GPP network roaming as defined in 3GPP TS 23.402 [32] and GSMA IR.61 [40] WLAN roaming guidelines.
- 3GPP has specified IP Flow Mobility (IFOM). There are two modes of IFOM. Network Based IFOM (NBIFOM) as defined in 23.161 [41] and Device Based IFOM (DBIFOM) in 23.261 [42].
    - In 3GPP TS 23.161 [41], a PDN connection supporting NBIFOM provides simultaneous access to a single PDN via different access networks: a 3GPP access network and a WiFi access network. It is used by multi-radio (i.e., 3GPP and WiFi) capable UEs that can simultaneously connect to a given PDN via different access systems (3GPP and WiFi). To enable NBIFOM, the UE can establish and maintain a PDN connection over both 3GPP access and WiFi access simultaneously. When a PDN connection is established over both simultaneously, there is one default bearer for each access. On a PDN connection established over both 3GPP access and WiFi access, it is possible to move individual IP flows from one access network to another, when policies determine that flows should be moved, and the multiple access network paths are available for the UE.
    - As explained in TS 23.261 [42], the granularity of access system connectivity and inter system mobility based on TS 23.402 [32] and TS 23.327 [43] is per PDN connection basis. This implies that when a handover occurs, all the IP flows belonging to the same PDN connection are moved from the source access system to the target access system. With IP flow mobility it is possible to have a finer granularity in access system connectivity and inter system mobility: the handover procedures can be applied to a single or multiple IP flows belonging to the same PDN connection. This implies that some IP flows of one PDN connection can be routed via one access system while simultaneously some IP flows of the same PDN connection can be routed via another access system. To achieve IP flow mobility the inter-system mobility signalling is enhanced in order to carry routing filters.

PSBN international roaming and interconnect requirements using an IPeXchange (IPX) service provider are described in GSMA IR.34 [16] guidelines for IPX provider networks and service provider networks. The GSMA has also produced IMS roaming and interconnect guidelines in GSMA IR.65 [39]. The roaming capability makes it possible to use IMS services even though the user is not geographically located in the service area of the HPLMN. 3GPP architecture specifications define multiple deployment configurations and these are also illustrated in the GSMA IR.65 document.

6.1 Roaming with non-partner regional, national and international commercial MNOs

In early deployments of the PSBN, it is expected that the geographic coverage of the public safety spectrum will be less than the more mature deployments of the commercial MNOs. As such, the ability for first responders to be served over commercial mobile networks should be considered. It is envisaged that roaming agreements will be established between the PSBN national entity and non-partner regional, national and international commercial MNOs.

While roaming on non-partner commercial networks, first responders will want to reach their EUA data networks and application servers with the same level of security as they have on the PSBN. First responders will desire to have priority service[9] on commercial networks during emergencies. However, mobility achieved via roaming does not provide service continuity and session persistence.

Additional national roaming partners may include un-trusted public WiFi network providers, 3G/HSPA MNOs and IMS connected network operators, such as in support of VoLTE. The commercial cellular MNO roaming partners inside of Canada would be directly connected to the PSBN via the RSDEs using a bilateral interconnect that is specified in the GSMA IR.34 guidance. The international roaming partners would primarily use the service of an IPX service provider to provide roaming from commercial MNOs outside of Canada.

6.2 FirstNet nationwide public safety broadband network roaming

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

An IMS is required to support voice for both Mission Critical Push-to-Talk (MCPTT) service and VoLTE service. Voice roaming between the FirstNet NPSBN and the PSBN can use either home routed or local breakout approaches.

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

Table 11: *Reference points to support roaming onto FirstNet.*

Reference Point	Components	Description
S6a	Visited MME to home HSS	Required to authenticate users when using either home or local routing mechanisms. Uses Diameter protocol.
S8	Visited S-GW to home P-GW	Required to provide services to users when using home routing mechanisms.

[9] Equivalent Mapping of QoS Class Indicator (QCI) and Allocation Retention Priority (ARP) by both PSBN and commercial networks are according to roaming agreements.

Reference Point	Components	Description
S9	Visited PCRF to home PCRF	Required to retrieve appropriate QoS settings when using either home or local routing mechanisms. Uses Diameter protocol.
S10	PSBN MME to FirstNet MME	If FirstNet and PSBN agree to support seamless mobility between their networks, then the S10 is needed to exchange tracking area information about UE location within respective coverage areas.
Mw	Visited Proxy Call Session Control Function (P-CSCF) to home Serving Call Session Control Function (S-CSCF)	Required for voice sessions when using local routing mechanisms. Uses Session Initiated Protocol (SIP) protocol.
Mm (*)	S-CSCF (a) to S-CSCF (b)	Required for voice session when using either home or local routing mechanisms. Uses SIP protocol.
Mb (*)	IMS Access Gateway (AGW) (a) to IMS AGW (b)	Required for voice session when using either home or local routing mechanisms. Uses Real-Time Control Protocol (RTCP) / Real-Time Transfer Protocol (RTP) protocol.

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

7 PSBN base functions

This section describes the base functions of the PSBN.

The PSBN will provide access to essential network services and application networks. Figure 14 illustrates an example of how the national entity and the RSDEs interconnect and connect to services and application networks. This example is for illustration purposes only. The PBSN may require more network elements or provide more services than what is shown here.

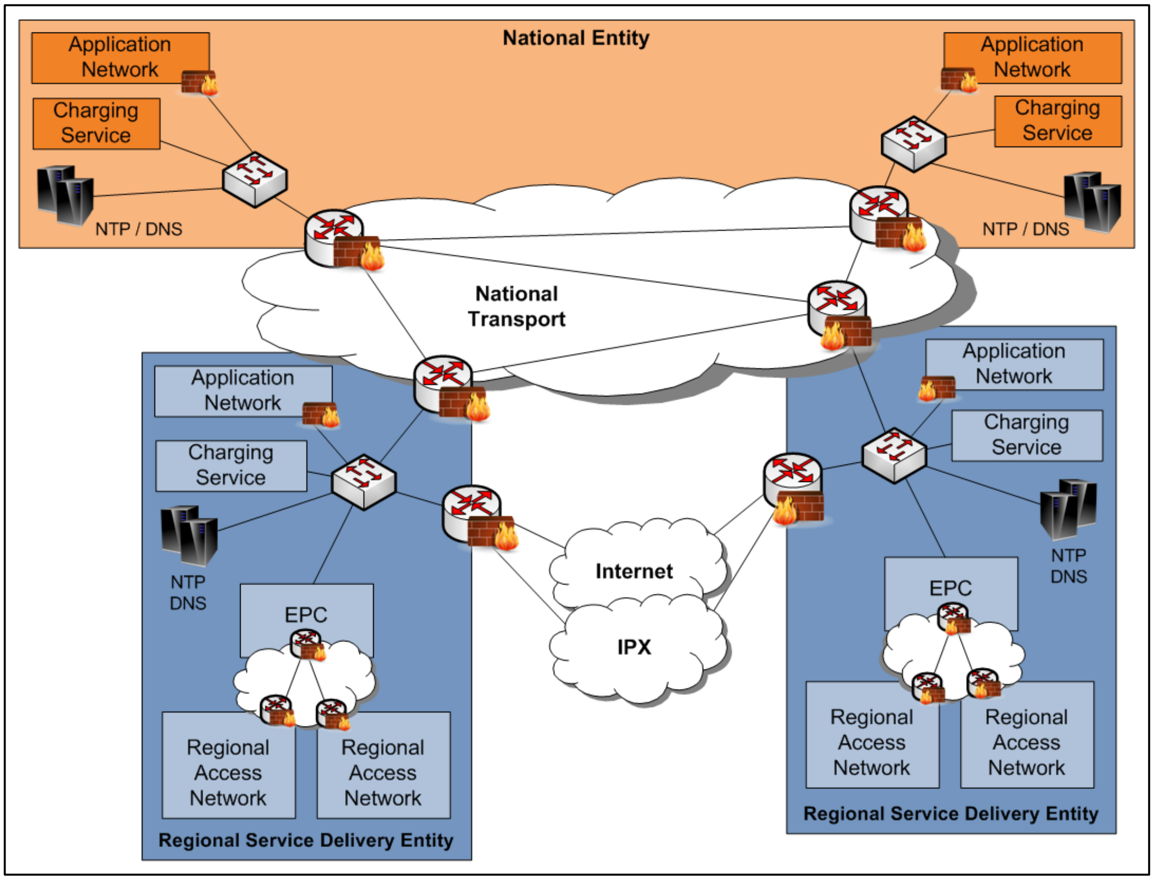


Figure 14: *Example of network services provided by PSBN.*

In this example, RSDEs connect to each other and to the national entity by means of routers. Each router uses a firewall to limit particular IP addresses or ports based on the policies and regulations in place. Once inside the network, switches distribute the traffic to the proper device, service, or application network. Each of these may have their own firewall to limit access as required. The following sub-sections briefly describe the essential network services provided by the PSBN.

7.1 Location service

Location Services (LCS) is specified in 23.271 [44]. IMS based location information services needed for 911 is specified in 23.167 [45].

7.2 Network time service

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

Although many solutions exist, Figure 14 illustrates one possible implementation of a network time service. In this example, Network Time Protocol (NTP) servers within the national entity provide the main network time source for the PSBN using either Global Positioning System (GPS) time or a very accurate clock. Regional NTP servers then synchronize to one or both to obtain the precise time. Local users and devices subsequently obtain the time from the regional NTP servers.

7.3 Domain Name Service (DNS)

Domain name services (DNS) allow users and devices to connect to particular services, equipment, or users by name instead of by an IP address.

Figure 14 shows a basic example where the national entity and the RSDEs each have their own DNS. Each entity is thus able to customize and tailor their respective DNSs according to their needs.

Even with the introduction of VoLTE, the use of standard telephone numbers (International Telecommunication Union-Telecommunication (ITU-T) Recommendation E.164) is not going away. ENUM (tElephone NUMber Mapping) is a specific usage of the DNS protocol used for mapping telephone numbers to IP resources.

7.4 Voice over LTE (VoLTE)

The SAE and LTE is completely IP based, and as such, analog voice is not supported. Instead, SAE uses VoLTE, a special type of Voice over IP (VoIP) technology which relies on an IMS to manage and control signalling and media transcoding messages between the network and the PSTN.

7.4.1 IP Multimedia Sub-system (IMS)

IMS is an architectural framework for offering multimedia and voice over IP services. It consists of session control, connection control and an applications services framework layered over an existing network infrastructure (e.g., LTE). IMS enables new converged voice and data services, while allowing for the interoperability of these converged services between internet and cellular subscribers using open standard IP protocols. It is access independent as it supports multiple access technologies such as GSM, WCDMA, Code Division Multiple Access 2000 (CDMA2000), WLAN, and LTE.

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

As the name implies, the IP Multimedia Sub-system consists of various components. These are listed and described in Table 12 below. The IMS reference points are subsequently described in Table 13.

Table 12: *IMS components.*

Component	Name	Description
P-CSCF	Proxy Call Session Control Function	The P-CSCF is responsible for security of the messages between the network and the user and allocation of resources for the media flows.
I-CSCF	Interrogating Call Session Control Function	The I-CSCF is a session control entity for endpoint devices that maintains session state. It is responsible for querying the HSS to determine the S-CSCF for a user.
S-CSCF	Serving Call Session Control Function	The S-CSCF is responsible for processing registrations to record the location of each user, user authentication, and call processing (including routing of calls to applications). The operation of the S-CSCF is controlled by policy stored in the HSS.
MRFC	Media Resource Function Controller	The MRFC is a signalling plane node that interprets information coming from an application server and S-CSCF to control the MRFP.
MRFP	Media Resource Function Processor	The MRFP is a media plane node used to mix, source or process media streams. It can also manage access right to shared resources.
BGCF	Breakout Gateway Control Function	The BGCF is a SIP proxy which processes requests for routing from an S-CSCF when the S-CSCF has determined that the session cannot be routed using DNS or ENUM/DNS. It includes routing functionality based on telephone numbers.
MGW	Media Gateway	The MGW interfaces with the media plane of the circuit switched network, by converting between RTP and PCM. It can also transcode when the codecs[10] are not equivalent (e.g., IMS might use AMR[11], PSTN might use G.711[12]).
MGCF	Media Gateway Controller Function	The MGCF controls the resources in a MGW and manages the distribution of sessions across MGWs.
IP-SM-GW	IP Short Message Gateway	The IP Short Message Gateway function is used for two functions: to deliver SMS messages over the IP network and to provide interworking between SMS users and Instant Messaging users. The interworking function translates between MAP or Diameter based

[10] https://en.wikipedia.org/wiki/Codec [46].

[11] http://en.wikipedia.org/wiki/Adaptive_Multi-Rate [47].

[12] http://en.wikipedia.org/wiki/G.711 [48].

Component	Name	Description
		signalling and SIP signalling to convey messages and responses between the two systems. Both functions are described in TS 23.204 [49].

__Table 13:__ IMS reference points.

Reference Point	Description
Cr	Used by MRFC to fetch documents (e.g., scripts, announcement files, and other resources) from an application server. Also used for media control related commands. Uses the SCTP protocol.
Cx	Used to send subscriber data to the S-CSCF, including authorization, authentication, filter criteria and their priority. Uses the Diameter protocol.
Iq	Conveys the necessary information needed to allocate and release transport addresses. Uses the H.248 protocol [50].
ISC	Reference point between S-CSCF and application servers. Main functions are to notify the application server of the registered IP Multimedia Public Identity (IMPU) and UE capabilities and supply the application server with information to allow it to execute multiple services. Uses the SIP protocol.
Mb	Interface to exchange RTP packets between the MGW and the IMS-AGW.
Mg	Integrated Services Digital Network (ISDN) User Part (ISUP) signalling to SIP signalling and forwards SIP signalling to I-CSCF. Uses the SIP protocol.
Mi	Used to exchange messages between S-CSCF and BGCF. Uses the SIP protocol.
Mj	Used for the interworking with the PSTN/circuit switched domain, when the BGCF has determined that a breakout should occur in the same IMS network to send SIP message from BGCF to MGCF. Uses the SIP protocol.
Mn	Allows control of user-plane resources. Uses the H.248 protocol.
Mr	Used to exchange information between S-CSCF and MRFC. Uses the SIP protocol.
Mw	Used to exchange messages between CSCFs. Uses the SIP protocol.
Rx	Used to exchange policy and charging related information between P-CSCF and PCRF. Uses the Diameter protocol.
SGi	Reference point between the P-GW and a packet data network. It may be an operator external public or private packet data network or an intra operator packet data network, e.g., for provision of IMS services.

Reference Point	Description
Sh	Used to exchange User Profile information (e.g., user related data, group lists, user service related information or user location information or charging function addresses (used when the AS has not received the third-party REGISTER for a user)) between an Application Server (AS) (SIP AS or Open Services Access (OSA) Services Capability Server (SCS)) and HSS. Also allow AS to activate/deactivate filter criteria stored in the HSS on a per subscriber basis. Uses the Diameter protocol.

In the PSBN, these components are expected to be deployed within the RSDEs networks as shown in Figure 15 below.

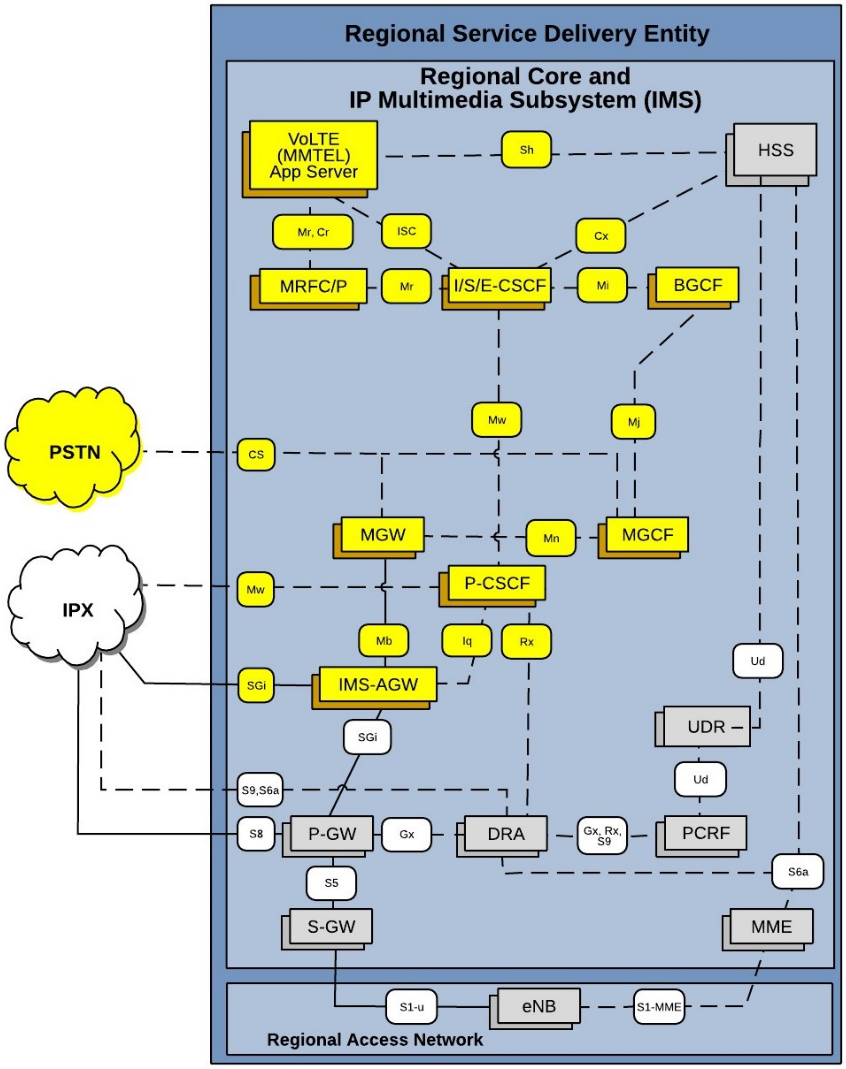


Figure 15: *IMS block diagram.*

7.4.2 IMS to IMS Network to Network Interface (NNI)

Within the PSBN, it is expected that the NE and each of the RSDEs will host their own IMS and VoLTE service. Therefore, in order to support inter-RSDE IMS to IMS communications, the following architecture will apply. The Inter-IMS Network-Network Interface (II-NNI) is illustrated in Figure 16. Referring to that figure, each Interconnect Border Controller Function (IBCF) will connect to each other over the national backbone. The SIP User-Network Interface (UNI) based signalling interactions between IMS Core Network (CN) elements may be different than SIP based signalling between the UE and the CSCF. II-NNI is specified in 3GPP TS 23.228 [38] Annex K and is required to support worldwide interoperable communication between IMS networks. II-NNI helps IMS networks to comply with the interoperability requirements defined within national and international regulatory frameworks.

3GPP TS 23.228 is the main IMS architecture specification. In addition, 3GPP TS 29.165 [51] "Inter-IMS Network to Network Interface (NNI)" specifies interconnection scenarios between two different IMS CN subsystems in order to support end-to-end service interoperability across multiple operators' IMS CN subsystems. Several RSDEs will implement IMS CN subsystems in support of IMS-based services like VoLTE. These RSDEs operate independently but will be interconnected. There are two approaches to interconnection between RSDEs. All the RSDEs IMS CN subsystems could be interconnected with the national entity or they could be interconnected to each other. In either case, they will use the II-NNI described in the Figure 16 below. While most of these 3GPP IMS reference points have already been described in the IMS section, there are a few new components and reference points that are described in the Table 14 and Table 15, respectively.

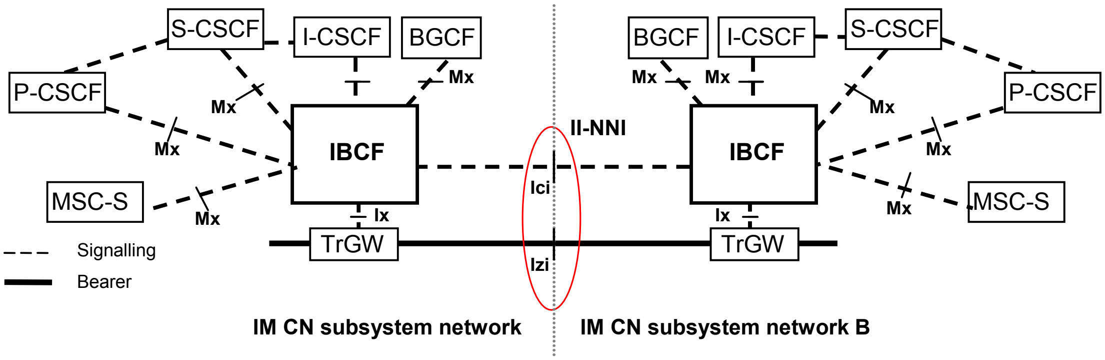


Figure 16: *Inter-IMS Network-to-Network Interface (II-NNI) (source: 3GPP 23.228 Annex K [38]).*

Table 14: *IMS connected network-to-network components.*

Component	Name	Description
IBCF	Inter Border Control Function	Based on operator preference, border control functions may be applied between two IMS CN subsystem networks or between an IMS CN subsystem network and other SIP based multimedia network. These functions are provided by the IBCF.
TrGW	Transfer Gateway	The IP Multimedia Subsystem has the option to deploy media functions such as TrGWs on the media path associated with each media stream associated with a session. These media functions can perform only transport level functions such as firewall or Network Access Translation (NAT), or can also perform application level functions such as transcoding or conferencing. IBCFs at the boundary of a network allocate TrGWs to protect media functions within the network or to provide address translation to the private address space used within the network, however it might be determined later during session establishment that no media resources are needed within the network, thus making the TrGWs unnecessary.

Table 15: *Inter-IMS network-to-network interface reference points.*

Reference Points	Description
Ici	The Ici reference point allows IBCFs to communicate with each other in order to provide the communication and forwarding of SIP signalling messaging between IMS CN subsystem networks. Furthermore, Ici reference point allows IBCF to be the entry/exit point towards other SIP networks and provide border control functions. The functionality of the reference point is specified in TS 24.229 [52].
Izi	The Izi reference point allows TrGWs to forward media streams between IMS CN subsystem networks.

7.5 Wireless public alerting

The Canadian Radio-television and Telecommunications Commission (CRTC) published Telecom Regulatory Policy 2017-91 for implementation of the National Public Alerting System by wireless service providers to protect Canadians [10]. That policy states that the Commission ***directs*** wireless service providers to implement wireless public alerting capability on their long-term evolution networks by 6 April 2018. Concurrent with this implementation, the Commission ***directs*** the CRTC Interconnection Steering Committee (CISC) to resolve several outstanding issues before the mandatory distribution of emergency alert messages begins. A Wireless Public Alerting System (WPAS) is the vehicle by which local, regional or national authorities can alert the public of an impending emergency using their cell phones. Figure 17 provides a block diagram of a Canadian WPAS system architecture [53]. It illustrates how alerting authorities feed the National Alert Aggregator and Disseminator (NAAD), which then feeds the Wireless Service Providers (WSP) over a Canadian standardized C-interface. The WSPs use cell broadcast technology to distribute the alerts to their wireless subscribers. In Canada, the closest equivalent to a National Public Alerting System (NPAS) solution is the NAAD system owned and operated by Pelmorex Communication Inc.

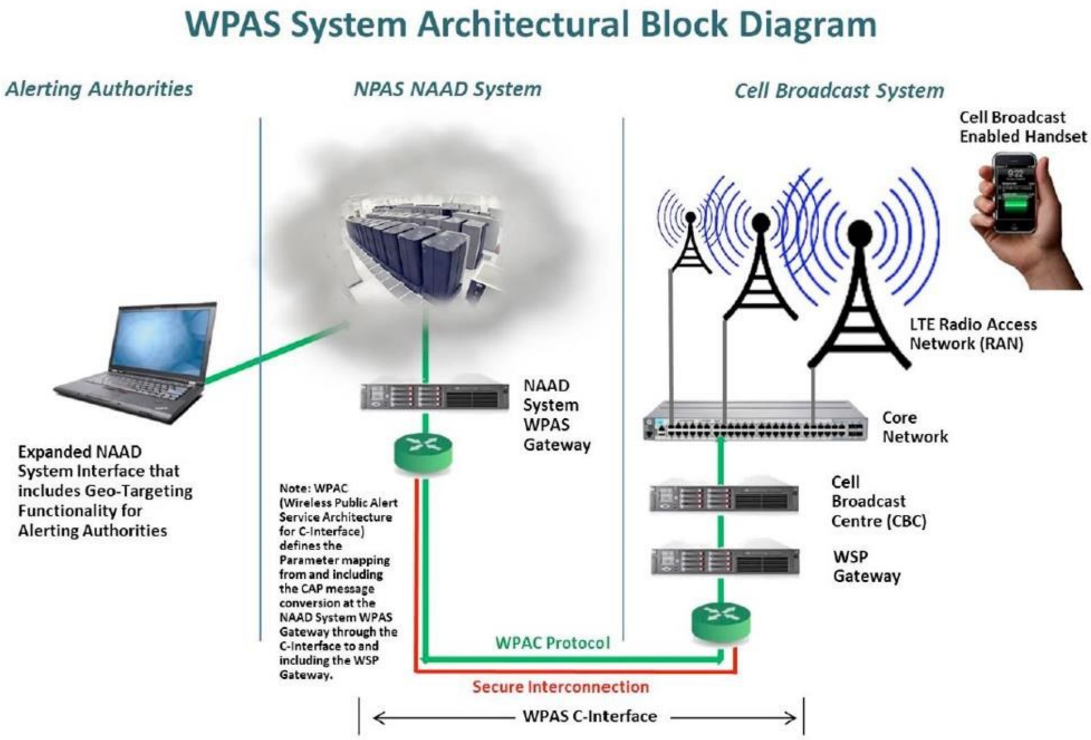

WPAS System Architectural Block Diagram
Alerting Authorities
NPAS NAAD System
Cell Broadcast System
Cell Broadcast Enabled Handset
LTE Radio Access Network (RAN)
NAAD System WPAS Gateway
Core Network
Expanded NAAD System Interface that includes Geo-Targeting Functionality for Alerting Authorities
Note: WPAC (Wireless Public Alert Service Architecture for C-Interface) defines the Parameter mapping from and including the CAP message conversion at the NAAD System WPAS Gateway through the C-Interface to and including the WSP Gateway.
Cell Broadcast Centre (CBC)
WSP Gateway
WPAC Protocol
Secure Interconnection
WPAS C-Interface

Figure 17: *Wireless public alerting service reference architecture (source: CRTC CISC-NTWG, "WPAS C-Interface Specification" [53]).*

Being a mobile network operation, the PSBN will need to interface with a Canadian WPAS to enable public safety users to receive emergency warning notifications on their user devices. In the context of 3GPP LTE, the Public Warning System (PWS) is the mechanism by which emergency alerts are distributed to end-users. As a result, the PSBN will also require PWS functionality.

It is important to note that while PWS functionality is achieved by using sub-components of the cell broadcast service (CBS), this does not enable cell broadcast functionality in the LTE network. PWS can only be used to broadcast emergency warning notifications. Furthermore, PWS-enabled UEs are required in order to receive and properly display emergency warning notifications. A number of key components are required to enable PWS functionality in LTE and thus in the PSBN and are listed and briefly described in Table 16 below. The PWS reference points are subsequently listed and described in Table 17.

Table 16: *Public alerting system components.*

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

Table 17: *Reference points to support the public alerting system.*

Reference Point	Description
SBc	Interface between MME and CBC. SBc is used for the delivery of warning messages and control information signalling.
C-Interface	The WPAS C-Interface represents the physical and communication protocol interconnection between the NAAD System WPAS Gateway and the wireless service provider (WSP) Gateway. The WPAS C-Interface is used to fulfill the following functions: a) Provides information for the authentication and validation of actions across this reference point. b) Supports delivery of a new or updated wireless alert message by the NAAD System WPAS Gateway (i.e., CBE) in a format that is suitable for ingestion by the WSP Gateway, the mobile devices and the wireless alert delivery technology or technologies employed by the WSP. c) Supports delivery of a cancellation wireless public alerting message by the NAAD System WPAS Gateway whereby the cancellation message terminates the delivery of the associated alert message currently being delivered by the wireless alert delivery technology or technologies employed by the WSP. d) Supports delivery of a test public alerting message by the NAAD System WPAS Gateway whereby the test message is delivered by the wireless alert delivery technology or technologies employed by the WSP using a special test channel. e) Provides acknowledgement from the WSP Gateway to the NAAD System WPAS Gateway that the new, updated, or cancelled wireless alert message has been received by the WSP Gateway. f) Provides periodic C-Interface interface testing.

Figure 18 illustrates an example where an RSDE uses PWS components (highlighted in yellow).

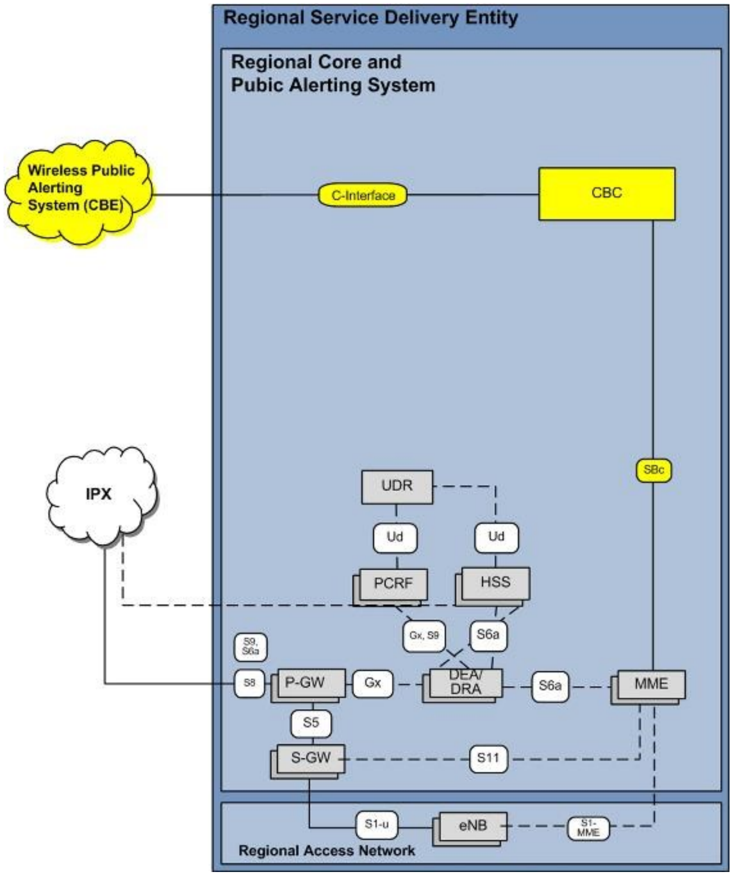


Figure 18: *RSDE core and public alerting system.*

7.6 Lawful intercept

The PSBN may have to provide lawful intercept capabilities depending on national or regional policies and regulations. In such cases, it will need to interface with various law enforcement agency networks in order to securely receive intercept commands and to relay intercept records and data as per 3GPP TS 33.107 [54].

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

Figure 19 illustrates how lawful interception can be implemented in the PSBN. This example shows the Administration Function (ADMF) within the RSDE. This provides a regional administration point for law enforcement agencies to submit their lawful intercept requirements. The ADMF then coordinates with regional delivery functions in order to deliver the proper intercept records to the appropriate enforcement agency.

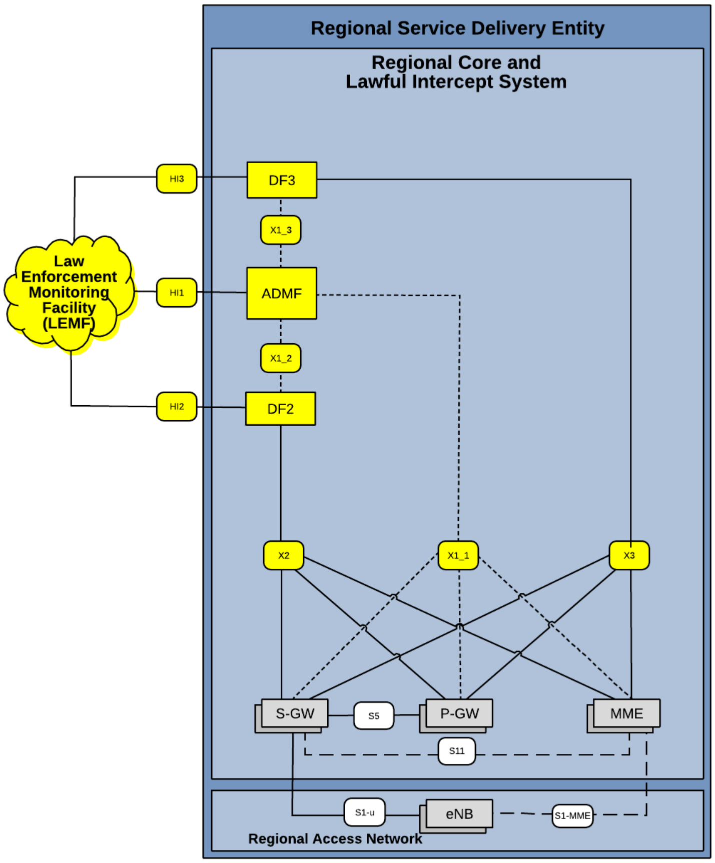


Figure 19: *Lawful intercept block diagram.*

Alternatively, it may also be possible for the NE to provide a single ADMF for the entire country. However, each RSDE would need to use the NE's ADMF.

Table 18 and Table 19 list and describe the lawful intercept components and reference points, respectively.

Table 18: *Lawful intercept system components.*

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

Component	Name	Description
DF3	Delivery Function 3	Delivers Content of Communication to law enforcement agency. Also responsible for call control (signalling) and bearer transport for the content of communication.

Table 19: *Reference points to support lawful intercept.*

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

7.7 Agency network access

It is expected that public safety users will use the PSBN to access their agency’s network or services from anywhere in the PSBN. This link may be encrypted and protected by means of a mobile VPN-type connection in addition to the LTE over-the-air encryption. The respective agencies may require dynamic control of the QoS policies for PDN data transfers. As shown in Figure 20, connections to agency network PDNs will be realized through the SGi of the P-GW for data transfer and the Rx interface of the PCRF for session control and QoS information.

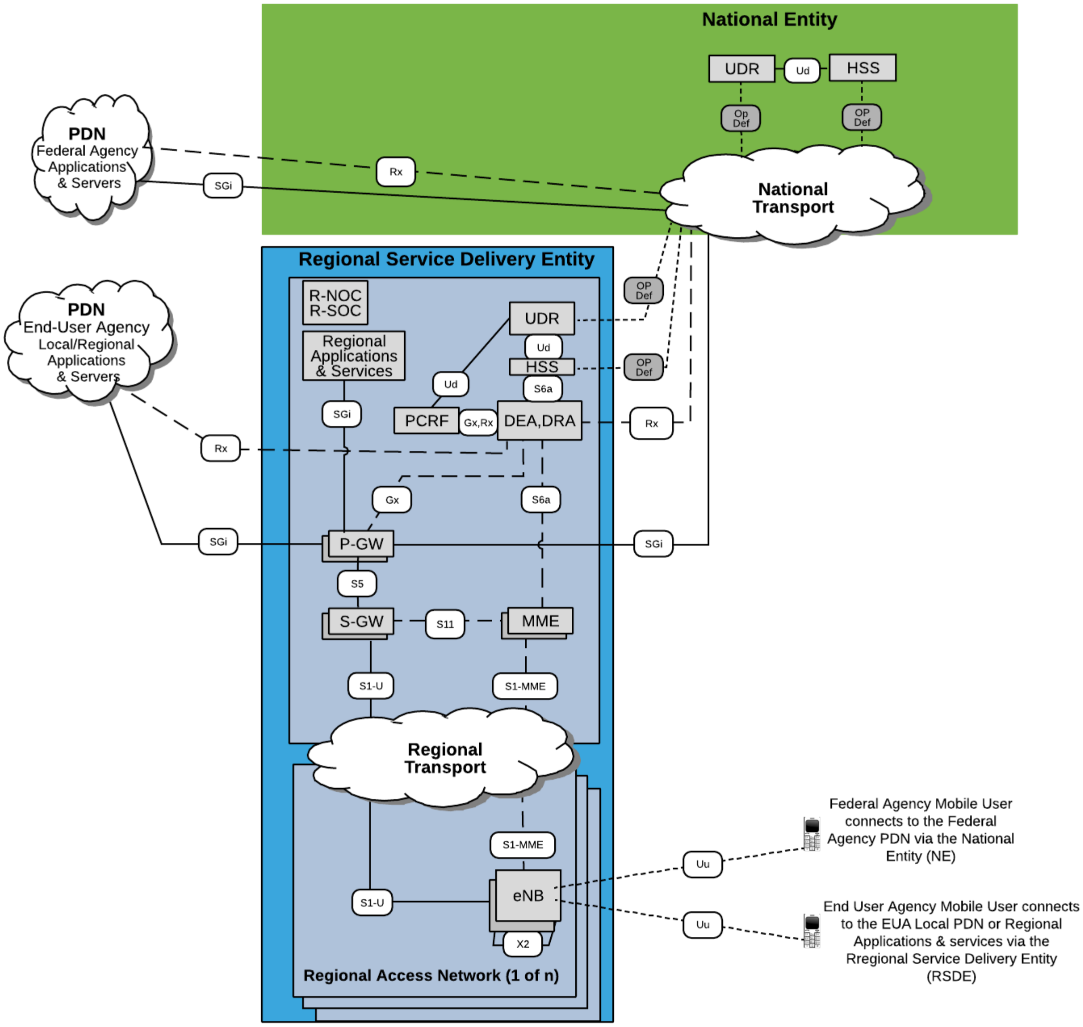


Figure 20: *Connection to agency networks.*

7.8 Internet

PSBN users should have access to the Internet through the EUAs so that the agencies' policies with regards to Internet usage would apply. The PSBN could nevertheless provide Internet access if it is done on behalf of an EUA. The internet APN connection passes through a P-GW, via the SGi interface to the EUA packet data networks which will provide controlled access to the Internet.

7.9 Inter-RSDE mobility

The RSDE operates independently for its regional users and applications but must also provide support for visiting users from other RSDEs. In essence, PSBN users can be transparently served anywhere on the PSBN network.

For any user, the parenting of eNodeBs, MMEs, and S-GWs is done within a single RSDE. When a UE makes a request with a specified Access Point Name (APN), a P-GW is assigned dynamically to that APN and can require inter-entity bearer establishment inside the PSBN. The following table lists some of the RAN and EPC interfaces and states whether they need to be open (i.e., accessible) between RSDEs to support visiting users.

Table 20: *Inter-RSDE entity gateway reference points.*

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

7.10 Commercial networks—spectrum sharing

It is expected that the national entity and the RSDEs may form partnerships with commercial carriers to deploy, maintain, and operate parts of the PSBN. As part of such partnerships, public safety entities may allow the commercial partner to use some, or all, of their 20 MHz public safety band when the band is not in use or in low use by public safety. Different types of partnerships are possible and will depend on the needs of the public safety entity and the level of service that the commercial partner can provide.

Regardless of the nature of the partnerships, the agreements would detail the services that the PSBN users or commercial MNO users would receive. Figure 21 illustrates one example where an RSDE partners with a commercial carrier to provide commercial MNO subscribers access to Band 14 coverage in their region using the Multiple Operator Core Network (MOCN). There are other possible configurations, but they are not illustrated here.

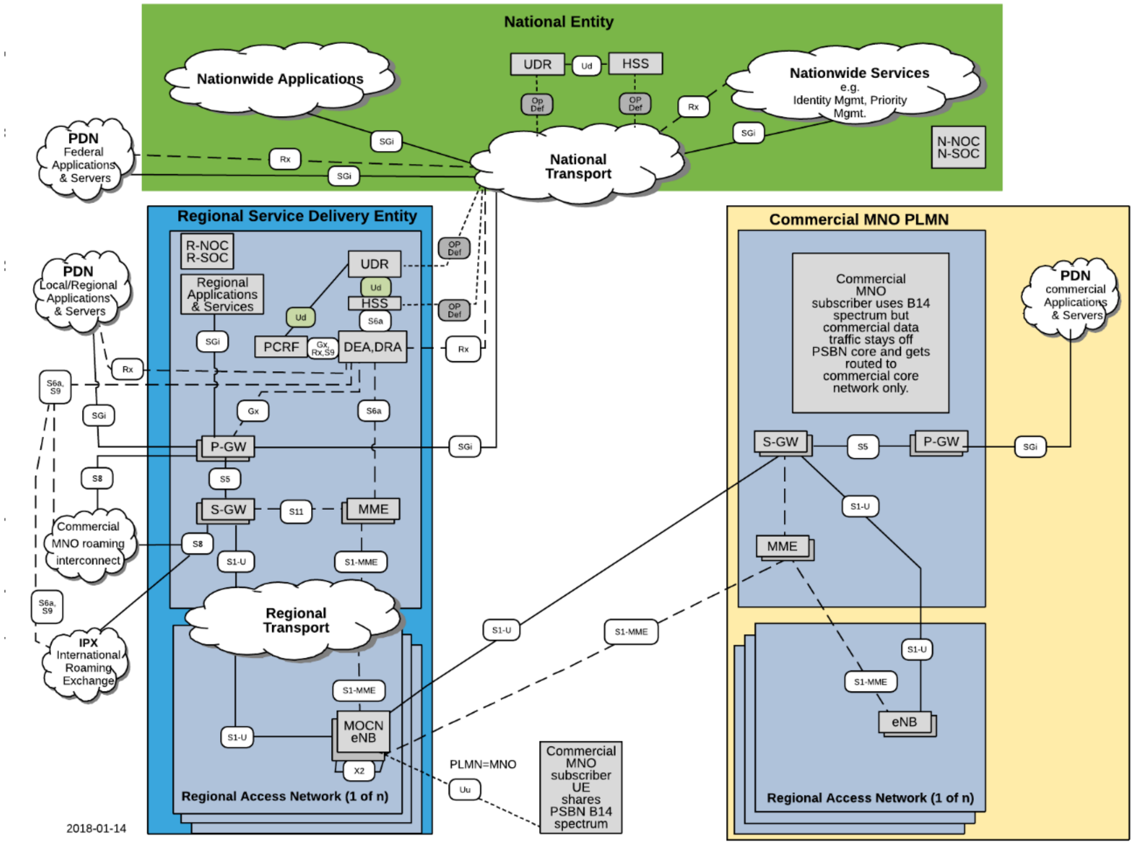

National Entity
Nationwide Applications
UDR
Ud
HSS
Op Def
OP Def
Rx
Nationwide Services
e.g.
Identity Mgmt, Priority Mgmt.
SGi
N-NOC
N-SOC
PDN
Federal Applications & Servers
Rx
SGi
SGi
National Transport
Regional Service Delivery Entity
R-NOC
R-SOC
UDR
OP Def
Regional Applications & Services
Ud
HSS
OP Def
Ud
S6a
SGi
PCRF
Gx, Rx,S9
DEA,DRA
Rx
PDN
Local/Regional Applications & Servers
Rx
S6a, S9
SGi
Gx
S6a
P-GW
SGi
S8
S5
S-GW
S11
MME
Commercial MNO roaming interconnect
S8
S1-U
S1-MME
S6a, S9
Regional Transport
IPX
International Roaming Exchange
S1-MME
S1-U
MOCN eNB
X2
Regional Access Network (1 of n)
2018-01-14
S1-U
S1-MME
PLMN=MNO
Uu
Commercial MNO subscriber UE shares PSBN B14 spectrum
Commercial MNO PLMN
Commercial MNO subscriber uses B14 spectrum but commercial data traffic stays off PSBN core and gets routed to commercial core network only.
PDN
commercial Applications & Servers
S-GW
S5
P-GW
SGi
S1-U
MME
S1-U
S1-MME
eNB
Regional Access Network (1 of n)

Figure 21: *Example of spectrum sharing.*

7.10.1 Multiple Operator Core Network (MOCN)

As shown in Figure 22, the RSDE's MOCN eNodeBs connect to both the RSDE core and the commercial MNO core. This MOCN eNodeB access allows commercial MNO subscribers to have access to the public safety 700 MHz band 14 radio access network in the RSDE regional access network. The commercial MNO subscribers are then able to use the Band 14 RAN to access their commercial MNO core and the commercial applications and servers.

In 3GPP TS 23.251 [29] and 36.300 [25], the coverage extension options are explained for multiple operators to use RAN sharing. For the purposes of the PSBN functional architecture, the architecture approach that has been assumed is the MOCN configuration.

In Figure 21, the MOCN configuration illustrates the relationships between the participating operators' core networks that share a single RAN. Each operator also has its own non-shared eNodeBs, but this not addressed in this Scientific Report. In the shared zone, the PLMN IDs of both operators' networks are broadcast to the UEs and it is up to the UEs to select the correct PLMN.

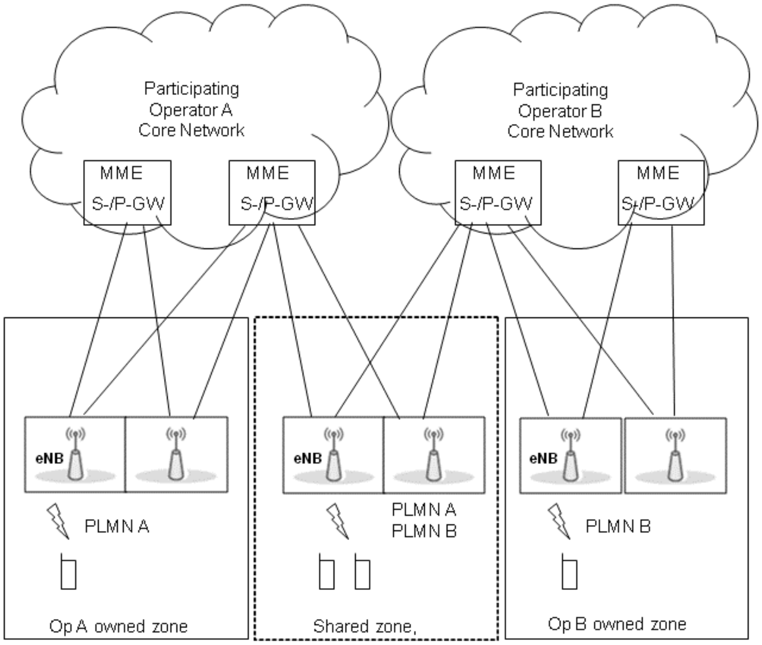


Figure 22: *Multiple Operator Core Network (source: 3GPP TS 32.130 [55]).*

3GPP TS 32.130 [55] specifies the telecommunication management of MOCN based network sharing configurations. For the PSBN RSDE, the telecommunication management architecture is based on assigning roles that each operator will play in coordinating and establishing the shared arrangement. This involves the designation of a master operator (MOP) and then participating operators (POP). The responsibilities of each operator are explained further in the 3GPP TS 32.130.

8 PSBN enhanced functions

This section describes the enhanced functions of the PSBN.

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

8.1 Mission Critical (MC) communications

In the PSBN, the functions for Mission Critical (MC) communications will be hosted in the RSDE and may also be hosted in deployable systems that can operate in stand-alone mode, i.e., without backhaul to the macro core network. It is expected that MC communications can occur between RSDEs for mutual aid reasons.

A platform for MC communications and MC Services has been a key priority of public safety and Standards Development Organizations (SDOs) in recent years and is expected to evolve into the future by specifying more requirements for this MC system platform.[13]

The MC Services that are described in this chapter are mission critical to the command, management and operation of a public safety incident. These functions provide voice, video, data and multimedia broadcast capabilities for on-network communications and in more limited off-network communications based on device-to-device direct mode of operations.

8.1.1 LTE device-to-device communications and Proximity Services

During public safety operations, PSBN users need to be able to communicate directly in a direct peer-to-peer communications mode. Public safety users require the capability to communicate even if the macro LTE network is not available. This capability is called Proximity Services or ProSe, which is the 3GPP way of specifying off-network communications between two or more LTE UEs. This off-network communication can be assisted by the macro network or can be conducted without the LTE network. In assisted mode, the network can assist with discovery of the target user. In direct mode, the ProSe UEs must be in close enough radio coverage or proximity so that they can discover each other and establish communications.

3GPP TS 23.303 [56] describes the specification for devices to act independently of the macro network. Additionally, this 3GPP technical specification explains how the LTE macro RAN would provide directory assistance and bridging capability through the ProSe Function to assist in setting up direct mode capabilities when two or more user equipments are out of range of each other. In Table 21, the names and descriptions are provided for all of the components that are involved in proximity services when used to provide off-network communications. In Table 22, the reference points between parts of ProSe system are named and described.

[13] A recent 2017 article on Mission Critical specifications in 3GPP, written by the Chair of the 3GPP SA6 [57].

Table 21: *Proximity Services components.*

Component	Name	Description
ProSe Function	Proximity Services Function	The ProSe Function is the logical function that is used for network related actions required for ProSe. The ProSe Function plays different roles for each of the features of ProSe. In this version of the specification it is assumed that there is only one logical ProSe Function in each PLMN that supports Proximity Services.
ProSe UE	ProSe-enabled User Equipment	A ProSe-enabled UE supports exchange of control information with the ProSe Function.
ProSe Network Relay	ProSe UE-to-Network Relay for Public Safety	The ProSe UE-to-Network Relay entity provides the functionality to support connectivity to the network for Remote UEs. A UE is considered to be a remote UE for a certain ProSe UE-to-Network relay if it has successfully established a PC5 link to this ProSe UE-to-Network Relay. A remote UE can be located within E-UTRAN coverage or outside of E-UTRAN coverage.
ProSe Application Server	ProSe Application Server	Application server can store EPC ProSe user IDs, map ProSe application layer user IDs to EPC ProSe user IDs, and maintains permission information for the restricted ProSe direct discovery capabilities.

Table 22: *ProSe reference points.*

Reference Points	Description
PC1:	The reference point between the ProSe application in the UE and in the ProSe Application Server. It is used to define application level signalling requirements.
PC2:	The reference point between the ProSe Application Server and the ProSe Function. It is used to define the interaction between ProSe Application Server and ProSe functionality provided by the 3GPP EPS via ProSe Function (e.g., name translation) for ProSe Direct Discovery and EPC-level ProSe discovery.
PC3:	The reference point between the UE and the ProSe Function. PC3 relies on the EPC user plane for transport (i.e., an "over IP" reference point). It is used to authorize ProSe Direct Discovery and EPC-level ProSe Discovery requests, and perform allocation of ProSe Application Codes / ProSe Restricted Codes corresponding to ProSe Application Identities used for ProSe Direct Discovery. It is used to define the authorization policy per PLMN for ProSe Direct Discovery (for public safety and non-public safety) and communication (for public safety only) between UE and ProSe function.

Reference Points	Description
PC4a:	The reference point between the HSS and ProSe Function. It is used to provide subscription information in order to authorize access for ProSe Direct Discovery and ProSe Direct Communication on a per PLMN basis. It is also used by the ProSe Function (i.e., EPC-level ProSe Discovery Function) for retrieval of EPC-level ProSe Discovery related subscriber data.
PC4b:	The reference point between the Secure User Plane Location (SUPL) Location Platform (SLP) defined in Open Mobile Alliance (OMA) AD SUPL and the ProSe Function. It is used by the ProSe Function (i.e., EPC-level ProSe Discovery Function) in the role of LCS client to query the SLP defined in OMA AD SUPL.
PC5:	The reference point between ProSe-enabled UEs used for control and user plane for ProSe Direct Discovery, ProSe Direct Communication and ProSe UE-to-Network Relay. The aspects of the radio layers for the PC5 reference point are defined in RAN specifications.
PC6:	The reference point between ProSe Functions in different PLMNs (EPC-level ProSe Discovery) or between the ProSe Function in the HPLMN and the ProSe Function in a Local PLMN (ProSe Direct Discovery). With ProSe Direct Discovery this reference point is used for HPLMN control of ProSe service authorization. It is also used to authorize ProSe Direct Discovery requests, retrieve the Discovery Filter(s) corresponding ProSe Application ID name(s) and translate the ProSe Application Code to the ProSe Application ID Name.
PC7:	The reference point between the ProSe Function in the HPLMN and the ProSe Function in the VPLMN. It is used for HPLMN control of ProSe service authorization. It is also used to authorize ProSe Direct Discovery requests, retrieve the Discovery Filter(s) corresponding ProSe Application ID name(s) and translate the ProSe Application Code to the ProSe Application ID Name.
S6a:	In addition to the relevant functions defined in TS 23.401 [19] for S6a, in the case of ProSe, S6a is also used to download ProSe related subscription information to the MME during E-UTRAN attach procedure or to inform the MME subscription information in the HSS has changed.
S1-MME	In addition to the relevant functions defined in TS 23.401 [19] for S1-MME, in case of ProSe, it is also used to convey the ProSe direct services authorization from MME to eNodeB.

8.1.2 Common Functional Architecture (CFA) to support Mission Critical (MC) services

A Common Functional Architecture (CFA) to support MC services includes a common application plane and signalling plane entities. Each MC Service supports several types of communications amongst the users (e.g., group call, private call). There are several common functions and entities (e.g., group, configuration, identity) that are used by the MC services (e.g., MCPTT, MCVideo, MCData). A summary of each plane and MC service is provided below.

Both the application plane and signalling plane reference points for the MC system are described in 3GPP TS 23.280 [24]. The common functional architecture to support MC services utilizes aspects of the IMS architecture defined in 3GPP TS 23.228 [38], the ProSe architecture defined in 3GPP TS 23.303 [56], the Group Communication System Enablers for LTE (GCSE_LTE) architecture defined in 3GPP TS 23.468 [58] and the PS-PS access transfer procedures defined in 3GPP TS 23.237 [59].

The MC_Service_UE primarily obtains access to a MC Service via E-UTRAN, using the EPS architecture defined in 3GPP TS 23.401 [19]. Certain MC Service functions such as dispatch and administrative functions can be supported using either MC service UEs in E-UTRAN or using MC Service UEs via non-3GPP access networks such as LMR. External applications usage (e.g., PSAP console) of MC services can be enabled via E-UTRAN or non-3GPP access networks.

8.1.2.1 Common services core architecture—application plane

Figure 23 illustrates the common components and associated reference points between intra-system components and inter-system components.

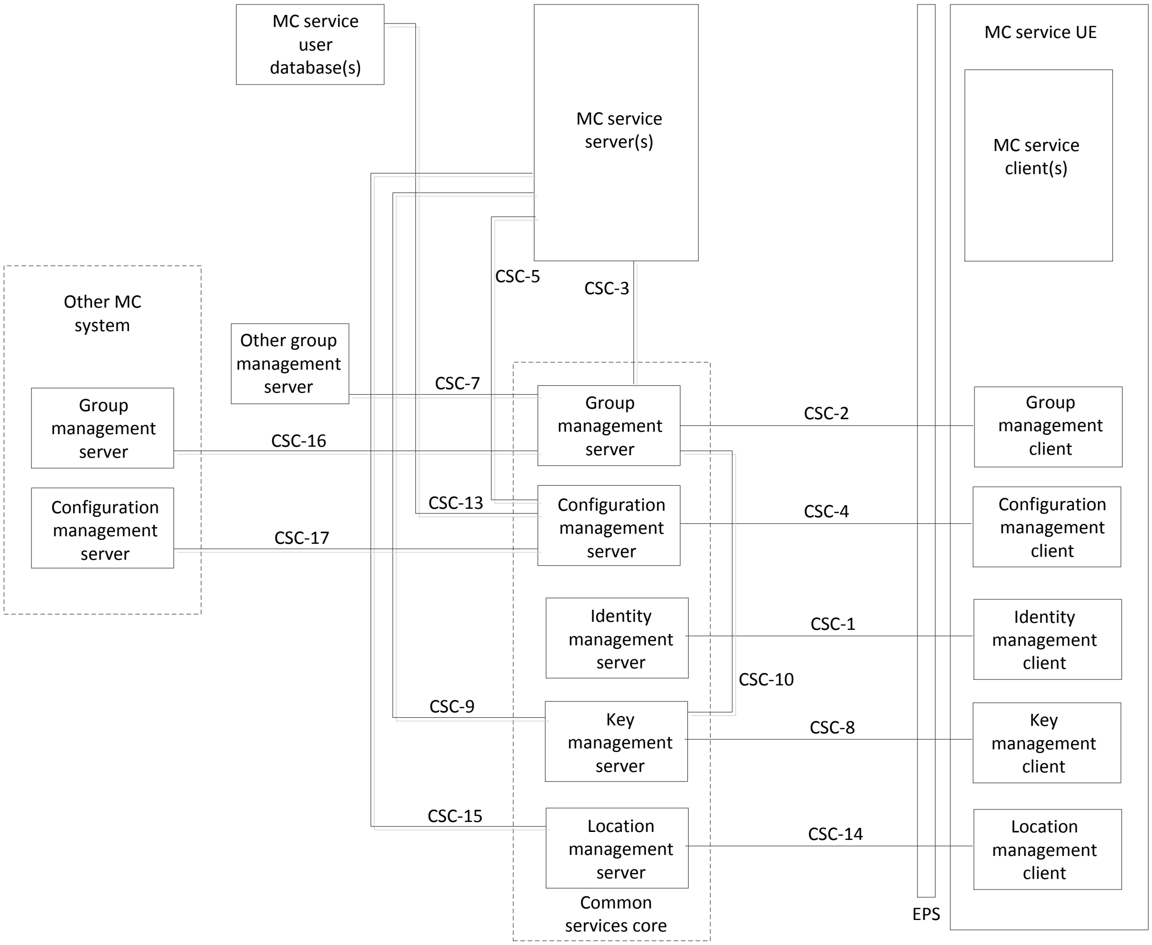


Figure 23: *Mission Critical Common Functional Architecture—application plane (source: 3GPP TS 23.280 [24]).*

The common services core functions and reference points are shown in Figure 23 and are shared across each MC Service. The description of the functions and reference points specific to an MC service is contained in the corresponding MC service 3GPP specifications for MCPTT (TS 23.379) [60], MCVideo (TS 23.281) [61] and MCData (TS 23.282) [62]. These are explained in later sections of this document.

Table 23: *Components for the application plane for an MC system.*

Component	Name	Description
Application Plane	MC Application Plane	The application plane provides all the services (e.g., call control, floor control, video control, data control) required by the user together with the necessary functions to support MC service. It uses the services of the signalling control plane to support those requirements.
MC Core	Common Services Core	Each MC service (e.g., PTT, Video, Data) can be represented by an application plane functional model. The functional model across MC

Component	Name	Description
		services may be similar but is described by the individual functional entities and reference points that belong to that MC service. Within the application plane for an MC service there is a common set of functions and reference points. The common set is shared across services. This common set of functions and reference points is known as the common services core.
MC Service	MC Service specific	A generic name for any one of the three mission critical services: either MCPTT, or MCVideo, or MCData.
MC Service Server	Server-side functions	The MC service server is a functional entity that provides centralized support for specific MC services.
MC Service UE	User Equipment	The MC service UE primarily obtains access to a MC service via E-UTRAN, using the EPS architecture defined in 3GPP TS 23.401. Certain MC service functions such as dispatch and administrative functions can be supported using either MC service UEs in E-UTRAN or using MC service UEs via non-3GPP access networks. External applications usage of MC services can be enabled via E-UTRAN or non-3GPP access networks.
MC Service Client	Client-side functions	The MC service client functional entity acts as the user agent for all MC service transactions. For a specific MC service, the detailed description of functions of the MC service client is contained in the corresponding MC service TS.
MC Database	MC Service User Database	The database contains information concerning the SIP subscriptions and corresponding identity and authentication information required by the SIP core, and such information as application service selection.

8.1.2.2 Common services core architecture—signalling plane

The following diagram, Figure 24, illustrates the functional model for signalling control plane of the MC system.

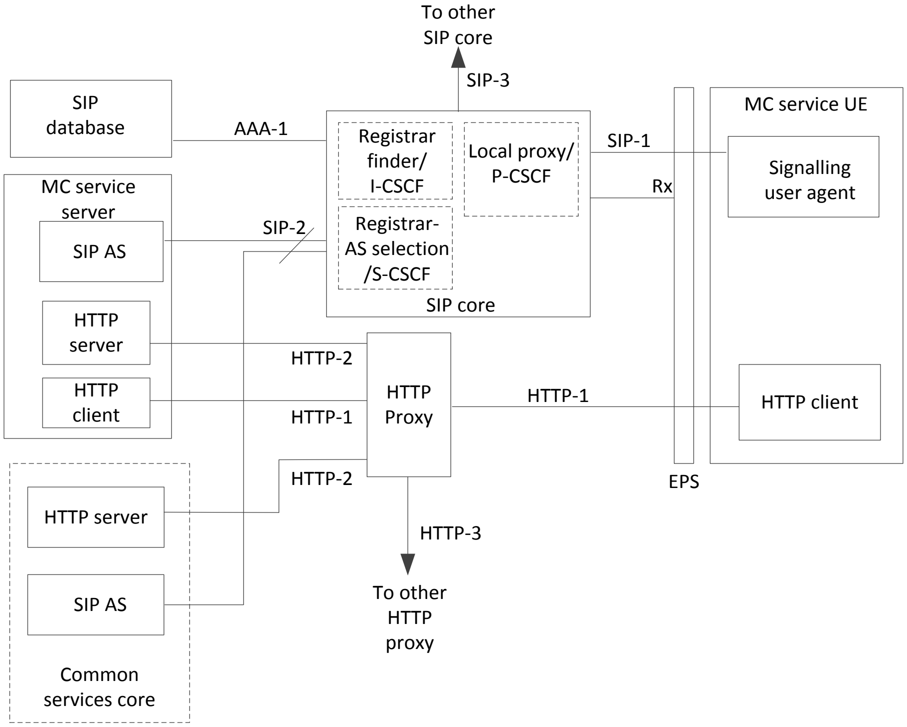


Figure 24: *Functional model for signalling control plane of the MC system (source: 3GPP TS 23.280 [24]).*

Table 24: *Components that describe the signalling control plane.*

Component	Name	Description
Signalling Plane	MC Signalling Plane	The signalling control plane provides the necessary signalling support to establish the association of users involved in an MC service, such as an MCPTT call or other type of MC services. The signalling control plane also offers access to and control of services across MC services. The signalling control plane uses the services of the bearer plane.
User Agent	Signalling user agent	This functional entity acts as the SIP user agent (both client and server) for all SIP transactions.
SIP AS	SIP Application Server	The SIP AS functional entity supports the following functions on behalf of the MC service: - influencing and impacting the SIP session; and - supporting event subscription and event notification.
SIP Core	MC Signalling Core	The SIP core contains many sub-entities responsible for registration, service selection and routing in the signalling control plane. The alternative to using a SIP Core is to use a fully compliant, specified TS 23.228 [38] IMS CSCF that are used as a proxy CSCF at the entry to

Component	Name	Description
		the IMS, an interrogating CSCF which is used to locate the Serving CSCF for a specific Application Service, and a serving CSCF which is used as a registrar for the IMS user that is selecting an IMS application service.
MC Signalling Database	MC Service User Database	The SIP database consists of the following functionalities: - support for control functions of the SIP core such as the registrar and registrar finder. This is needed to enable subscriber usage of the SIP core services. This functionality is independent of the access network used to access the SIP core; and authentication functionality required by the SIP core to authenticate the MC service UE.

8.1.2.3 MC services common off-network operations using proximity services

Within the PSBN, all of the MC Services can be available in a limited form as services between PSBN users without a supporting LTE network. When these users are not on the LTE macro network, they are said to be off-network. When they are off-network, the two UEs that support Proximity Services are referred as ProSe UEs. The ProSe UEs establish a direct device-to-device connection for the purposes of using Push-to-Talk (PTT) half-duplex voice, or MCVideo or MCData. Off-network communications is most helpful when access to the RSDE or BBDS LTE networks are not available.

3GPP TS 23.280 [24] describes that in off-network operation, an MC Service group ID is used for identifying the MC Service group while off-network. The MC Service group ID should be resolved to the ProSe group IP multicast address and ProSe Layer-2 group ID for the group communication. The MC service UE is able to make one or more MC service communications (as per the group configuration) with other member UEs whose users are of the same MC service group ID over ProSe direct communications based on ProSe Layer-2 Group ID and ProSe group IP multicast address, and utilising IP version 4 (IPv4) or IP version 6 (IPv6) as indicated by policy, as described in 3GPP TS 23.303 [56].

Figure 25 illustrates how the MC Service group ID, ProSe group IP multicast address and the ProSe Layer-2 group ID are mapped to each other. ProSe group IP multicast address and ProSe Layer-2 group ID are pre-configured in accordance with the MC Service group ID. Thus, they are pre-defined and associated. This mapping information should be provisioned through UICC in the UE or through ProSe function as specified in 3GPP TS 23.303, or be delivered from an application server. Mapping information is provisioned from group management server for online configuration, and provisioned from configuration management server for offline configuration.

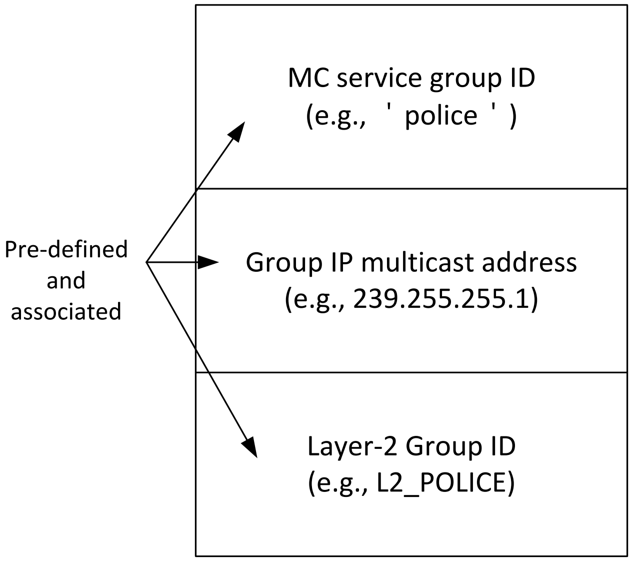


Figure 25: *MC Service group ID management in off-network operation (source: TS 23.280 [24]).*

8.1.3 Mission Critical Push-to-Talk Service (MCPTT)

The service requirements for MCPTT are specified in 3GPP TS 22.179 [63]. The MCPTT Service allows users to request the permission to talk (transmit voice/audio) and provides a deterministic mechanism to arbitrate between requests that are in contention (i.e., floor control). When multiple requests occur, the determination of which user's request is accepted, and which users' requests are rejected or queued is based upon many characteristics (including the respective priorities of the users in contention). MCPTT Service provides a means for a user with higher priority (e.g., MCPTT emergency condition) to override (interrupt) the current talker. MCPTT Service also supports a mechanism to limit the time a user talks (hold the floor) thus permitting users of the same or lower priority a chance to gain the floor.

The MCPTT Service provides the means for a user to monitor activity on many separate calls and enables the user to switch focus to a chosen call. An MCPTT Service user may join an already established MCPTT group call (late call entry). In addition, the MCPTT Service provides the user ID of the current speaker(s) and user's location determination features.

The MCPTT service supports communication between several users (i.e., group call), where each user has the ability to gain access to the permission to talk in an arbitrated manner. The MCPTT service also supports private calls between two users. The MCPTT service can operate in an on-network mode and in an off-network mode. When the MCPTT UE is connected to the MCPTT server that is referred to as on-network. When the MCPTT UE is communicating directly with another MCPTT UE that is referred to as off-network. Both MCPTT modes of operation are explained later in this section.

The MCPTT architecture utilizes the MC common functional architecture to support mission critical services over LTE defined in 3GPP TS 23.280 [24] and aspects of the IMS architecture defined in 3GPP TS 23.228 [38], the ProSe architecture defined in 3GPP TS 23.303 [56], the Group Communication System Enablers for LTE (GCSE_LTE) architecture defined in 3GPP TS 23.468 [58] and the PS-PS access transfer procedures defined in 3GPP TS 23.237 [59] to enable support of the MCPTT service.

The MCPTT UE primarily obtains access to the MCPTT service via E-UTRAN located in the RSDE, using the EPS architecture defined in 3GPP TS 23.401 [19]. Certain application functions of MCPTT service such as dispatch and administrative functions can be supported using either MCPTT UEs in E-UTRAN or using MCPTT UEs via non-3GPP access networks defined in 23.402 [32]. Dispatch consoles and devices used by MCPTT service administrators are considered MCPTT UEs in the MCPTT architecture. MCPTT UEs that use non-3GPP access can only support a subset of the functionality specified in this specification that is supported by the non-3GPP access network. The MCPTT system provides the function to support interworking with LMR systems defined in 3GPP TS 23.283 [64]. This MCPTT interworking function (IWF) is in the PSBN and is used to interwork with the EUA LMR System.

8.1.3.1 MCPTT on-network functional model—application plane

In the Mission Critical common functional architecture, there are descriptions for the application plane and a signalling plane. For each of the MC Services that have been specified by 3GPP, there is only an application plane since the MCPTT signalling plane uses the common functional architecture signalling plane. Figure 26 illustrates the MCPTT application plane. Table 25 provides an explanation of the service components within the MCPTT application plane.

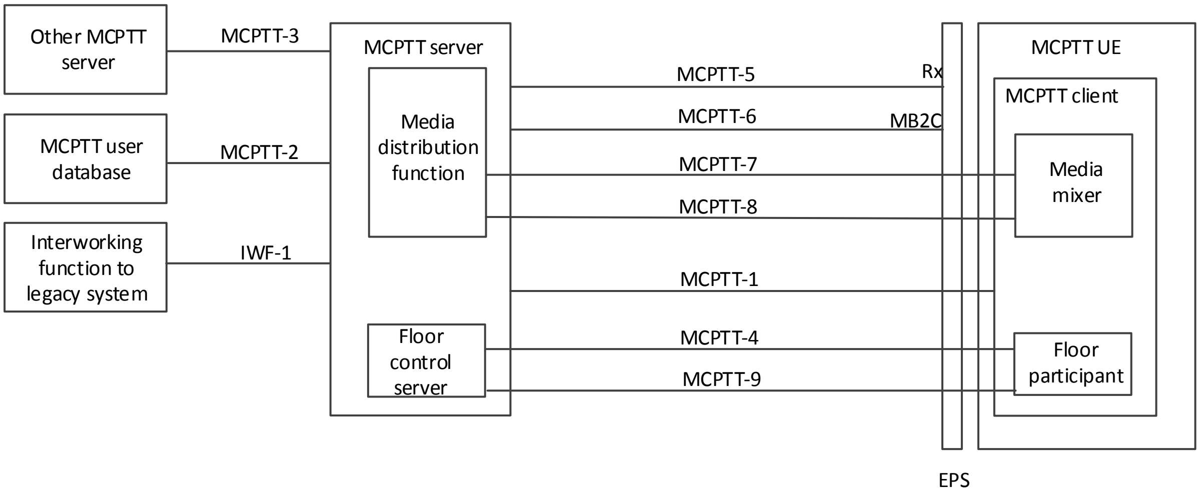


Figure 26: *Functional model for application plane of the MCPTT service (source: 3GPP TS 23.379 [60]).*

Table 25: *MCPTT Service components—application plane.*

Component	Name	Description
User Agent	MCPTT Application Service Client	The MCPTT client functional entity acts as the user agent for all MCPTT application transactions. The client reports the information of where the client is currently located.
Server	MCPTT Central Services support	The MCPTT server functional entity provides centralized support for MCPTT services. The MCPTT server functional entity represents a specific instantiation of the Ground Control Station (GCS) AS described in 3GPP TS 23.468 [58] [35] to control multicast and unicast operations for group communications.
Floor participant	MCPTT UE requester	The floor participant functional entity is responsible for floor requests. This functional entity is located in the UE for both on-network and off-network operations.
Floor Control Server	MCPTT Central Floor manager	This functional entity provides support for centralized floor control for on-network and distributed floor control for off-network operation. It may provide arbitration between floor control requests between different users, grant the floor in response to successful requests, and provide queuing in cases of contention. For on-network operation, this functional entity is located with the MCPTT server. For off-network operation, this functional entity is located in the UE.
Media distribution function	MCPTT Media Distribution Manager	The media distribution function is responsible for the distribution of media to call participants. By means of information provided by the MCPTT server (e.g., IP addresses, transport layer ports).
Media stream combiner	MCPTT UE Media Mixer	This functional entity exists on the UE and provides support for combining multiple media streams into one media stream through the enforcement of media policy information.
Interworking Function	MCPTT to LMR Gateway	The MCPTT-LMR gateway is detailed in 3GPP TS 23.283 [64]. It enables PTT groups to include participants from MCPTT and LMR systems.

Component	Name	Description
System Interconnection Function	MCPTT to MCPTT System Interconnect	The architecture for interconnect between MCPTT systems allows the affiliation of MCPTT users from an MCPTT system with MCPTT groups defined in another MCPTT system. When both MCPTT systems are served by different networks, interconnect of signalling and media is achieved using the interfaces defined for interconnect between PLMNs.
User Profile database	MCPTT ID information	This functional entity contains information of the MCPTT user profile associated with an MCPTT ID that is held by the MCPTT service provider at the application plane. The MCPTT user profile is determined by the mission critical organization, the MCPTT service provider, and potentially the MCPTT user.

8.1.3.2 MCPTT off-network functional model

During normal incident management or during incident operations that occur outside the coverage of the RSDE LTE networks, the MCPTT off network communications can enable direct PSBN user-to-user Push-to-Talk communications or enable talk group chat communications between many PSBN users. MCPTT off-network service is defined as the collection of functions and capabilities required to provide MCPTT using ProSe Discovery and the ProSe communication path for MCPTT using public safety ProSe-enabled UEs as a direct communication between UEs using evolved-Universal Terrestrial Radio Access (e-UTRA).

3GPP TS 22.179, “Mission Critical Push To Talk (MCPTT) over LTE; Stage 1,” [63] explains that to the extent possible, the end user’s experience should be similar when operating either under coverage of an EPC network, or based on ProSe without network coverage. To clarify this intent, the requirements are grouped according to applicability to on-network use, off-network use, or both. Figure 27 below illustrates the MCPTT functional model for off-network operation.

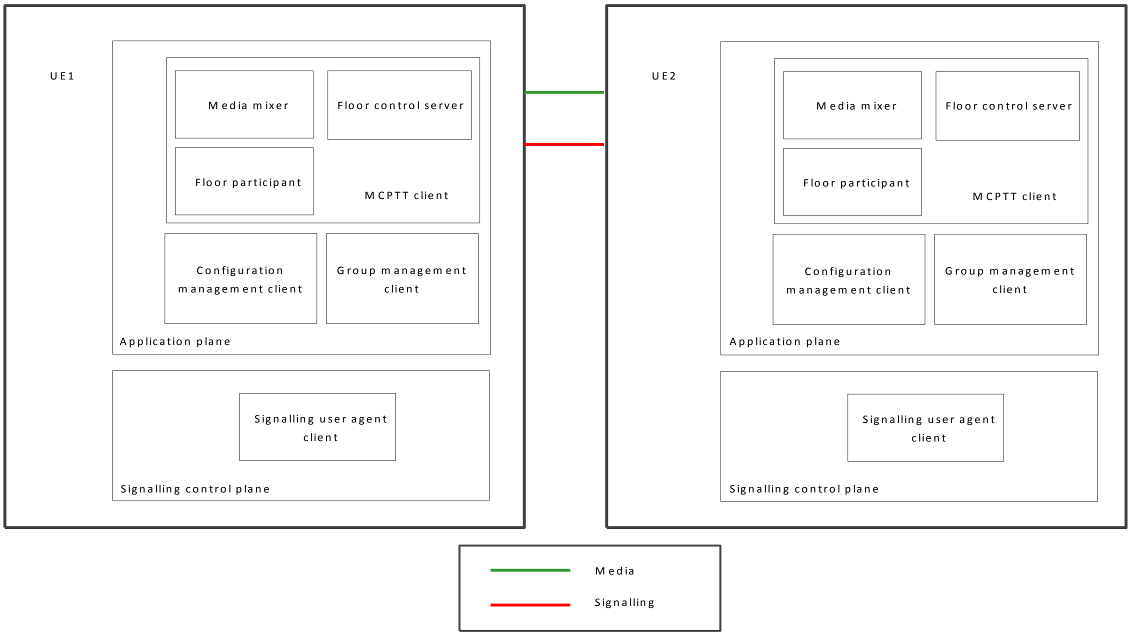


Figure 27: *Functional model for MCPTT off-network mode of operations (source: 3GPP TS 23.379 [60]).*

8.1.4 Mission Critical Video (MCVideo) service

The MCVideo service requirements are described in 3GPP TS 22.281 [65]. The MCVideo functional model is described in 3GPP TS 23.281 [61].

The MCVideo service supports video media communication between several users (i.e., group call), where each user has the ability to gain access to the permission to stream video in an arbitrated manner. The MCVideo service also supports private calls between two users.

8.1.4.1 MCVideo on-network functional model—application plane

Figure 28 shows the functional model for the application plane of MCVideo service for on-network operations.

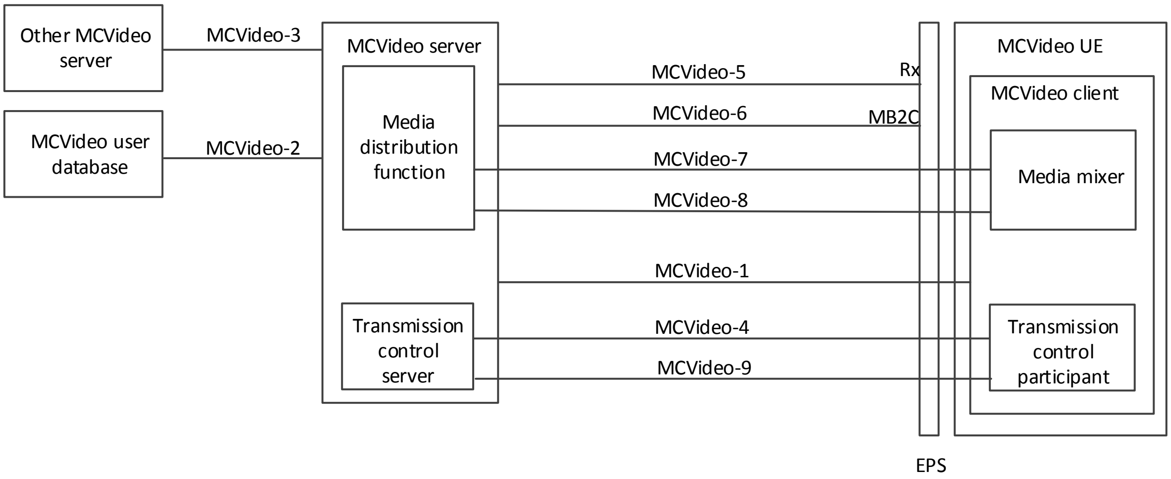


Figure 28: *Functional model for application plane of MCVideo service (source: 3GPP TS 23.281 [61]).*

The components for the MCVideo Service are listed below with brief description.

Table 26: *MCVideo Service components—application plane.*

Component	Name	Description
User Agent	MCVideo Service Client	The MCVideo client functional entity acts as the user agent for all MCVideo application transactions. The MCVideo client is responsible for remote device control. This functional entity is located in the UE for both on-network and off-network operations.
Server	MCVideo Central Services support	The MCVideo server functional entity provides centralized support for MCVideo services. This MCVideo server provides support for centralized media transmission control for on-network and distributed media transmission control for off-network operation. The MCVideo server is responsible for managing and providing the device information that can participate in MCVideo communications. The device information is further associated to MCVideo users to manage remote device control authorization. The device information is provisioned to the MCVideo server by the MCVideo service provider, mission critical organization and the MCVideo user.

Component	Name	Description
Transmission Control participant	MCVideo UE requester	The transmission control participant functional entity is responsible for handling outgoing transmission requests and the incoming video stream invitations and notifications. This functional entity is located in the UE for both on-network and off-network operations.
Transmission Control Server	MCVideo centralized Transmission Control	This functional entity provides support for centralized transmission control for on-network and distributed transmission control for off-network operation. It may schedule transmission requests according to uplink criteria from different transmission control participants, send a notification to all transmission control participants to allow them to receive the video according to downlink criteria if the transmission request is granted, and provides queuing in cases of contention. Transmission control applies to all MCVideo communications including group call and private call. For on-network operation, this functional entity is located with the MCVideo server. For off-network operation, this functional entity is located in the UE.
Media distribution function	MCVideo Media Distribution Manager	The media distribution function is responsible for the distribution of media to MCVideo clients. By means of information provided by the MCVideo server (e.g., IP addresses, transport layer ports).
Media stream combiner	MCVideo UE Media Mixer	This functional entity exists on the UE and provides support for sending and receiving one or multiple media streams. It also provides support for combining multiple media streams into one media stream through the enforcement of media policy information. It supports the storing of a media stream as MCVideo content files.
User profile database	MCVideo ID information	This functional entity contains information of the MCVideo user profile associated with an MCVideo ID that is held by the MCVideo service provider at the application plane. The MCVideo user profile is determined by the mission critical organization, the MCVideo service provider, and potentially the MCVideo user. The MCVideo user profile can be co-located with other MC service user profiles and stored in a common MC service user database.

8.1.4.2 MCVideo off-network functional model

Figure 29 shows the functional model for the application plane of MCVideo service for off-network operations. Each PSBN UE that supports the MCVideo off-network service will need to support these functions in the PSBN ProSe UE.

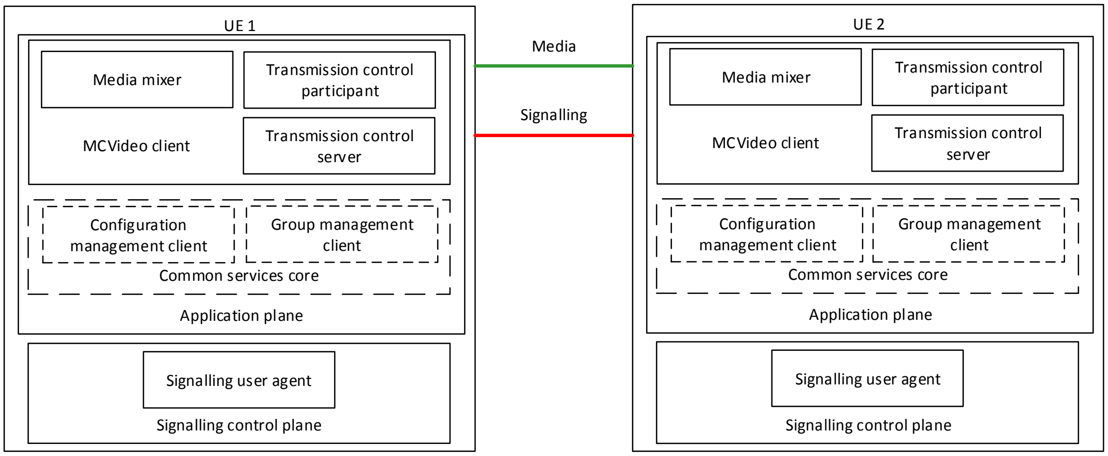


Figure 29: *Functional model for MCVideo off-network mode of operations (source: 3GPP TS 23.281 [61]).*

8.1.5 Mission Critical Data (MCData) service

The Mission Critical Data (MCData) Service requirements are described in 3GPP TS 22.282 [66]. The MCData functional model is described in 3GPP TS 23.282 [62].

MCData defines a service for MCData Service. As well as voice services, current mission critical users have been increasing their use of data services, including low throughput services on legacy networks and data services on commercial networks. This need will continue to grow with the creation of the new multimedia services. The MCData service needs to provide a means to manage all data connections of mission critical users in the field and provide relevant resources to the ones who need it. For example, mission critical users already use event manager software along with the voice system. The migration to LTE networks will allow mission critical users to operate current and new data services while relying on the fundamental capabilities of mission critical communication. The MCData Service provides a set of communication services that will be directly used by the user or functions that will be called by external applications in control rooms.

In addition, the MCData Service will provide a set of generic capabilities such as: messaging, file distribution, data streaming, IP proxy, etc. Also, the MCData Service will provide specific services such as conversation management, data base enquiries, internet access, robots control. The MCData Service is expected to have open interfaces in the network and is required to allow for the use of a variety of multimedia applications using the MCData Service.

MCData makes frequent use of a set of capabilities and enablers that allows for many end user services to be built on a common foundation. Several generic capabilities are defined for use in the MCData Service. These capabilities can be used on their own to transfer files, messages and other content to individuals and affiliated members of groups or combined with other services, through an application, to provide complete end users services as determined by the authorities implementing the service. The MCData generic capabilities are common for on-network and off-network.

8.1.5.1 MCData on-network functional model—application plane

Figure 30 shows the functional model for the application plane of MCData service for on-network operations.

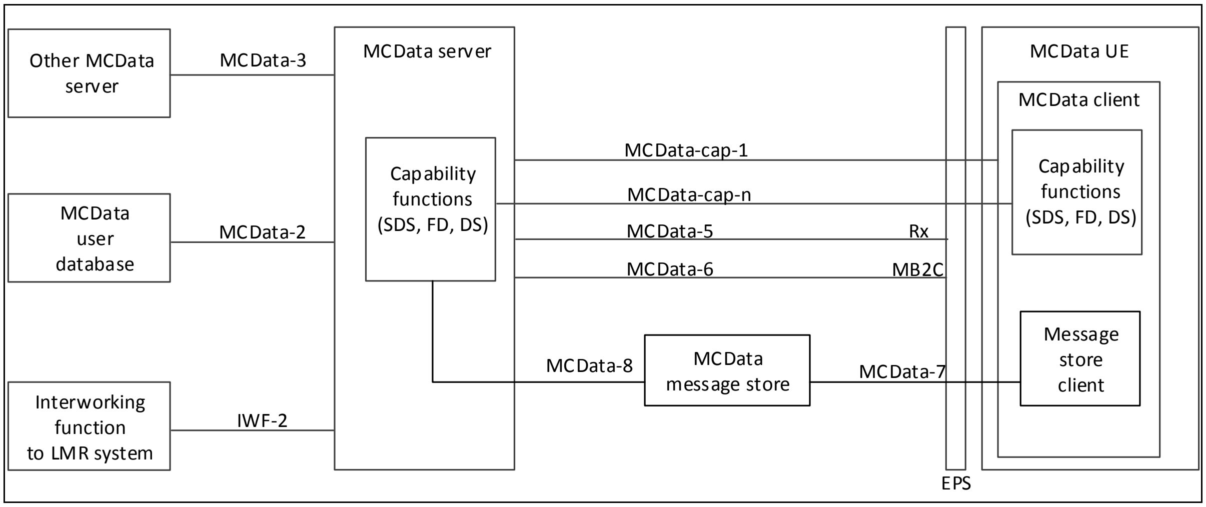


Figure 30: *Functional model for MCData Service—application plane (source: TS 23.282 [62]).*

The following table contains a list of the components of the MCData functional model.

Table 27: *MCData service components—application plane (excerpts from TS 23.282 [62]).*

Network Function	Description
MCData Client	The MCData client functional entity acts as the user agent for all MCData application transactions. The client supports SDS, file distribution, data streaming and IP connectivity. MCData capabilities utilized by MCData services like conversation management, robots control, enhanced status, database enquiries and secured internet.
MCData server	The MCData server functional entity provides centralised support for MCData services suite. Conversation management, robots, enhanced status, database enquiries and secured internet MCData services requiring one-to-one or group data communication are realized using SDS, file distribution, data streaming and IP connectivity MCData communication capabilities
MCData user database	This functional entity contains information of the MCData user profile associated with an MCData ID that is held by the MCData service provider at the application plane. The MCData user profile is determined by the mission critical organization,

Network Function	Description
	the MCData service provider, and potentially the MCData user.
MCData message store	The MCData message store is a network-based persistent store that allows mission critical organization to configure their MCData service users to permanently store their MCData communications. Once configured, a MCData service user will be allocated a secured storage area in the MCData message store that is only accessible by that configured MCData service user and any authorized users. The MCData service user can manage how and what will be stored in his/her personal message store with the support of management operations such as creating, deleting and merging folders, moving stored messages and files, as well as synchronizing all the user devices according to user preferences.

8.1.6 Mission Critical (MC) system interconnection

As public safety agencies deploy mission critical voice and data systems based on 3GPP Mission Critical communications specifications, each RSDE will implement a system which will interconnect to other MC systems located in the NE or other RSDEs. 3GPP is currently working on updating existing MC system specifications to support system interconnection. This will make it possible for a MC Service UE to access other RSDE jurisdiction's MC system. The set of updates to the 3GPP specifications for mission critical communications is expected to be completed in June 2018.

8.1.7 Mission Critical (MC) communication interworking

Many EUAs currently rely on LMR or other narrow band technologies to provide mission critical voice and low-throughput data communications to their users. Many of these systems are still being deployed or upgraded and will remain operational for the foreseeable future.

It is expected that EUAs will use a mixture of both LMR and PSBN for a period of time. Since both technologies will be in use, RSDEs may be able to bridge both systems together such that for a private or group call, a PSBN user can connect to a LMR user or group of users and vice versa for mission critical voice and data. 3GPP TS 23.283 [64] has specified the IWF as the bridge that is used between the PSBN Mission Critical system and the EUA LMR system. Figure 31 shows a high-level illustration of this concept.

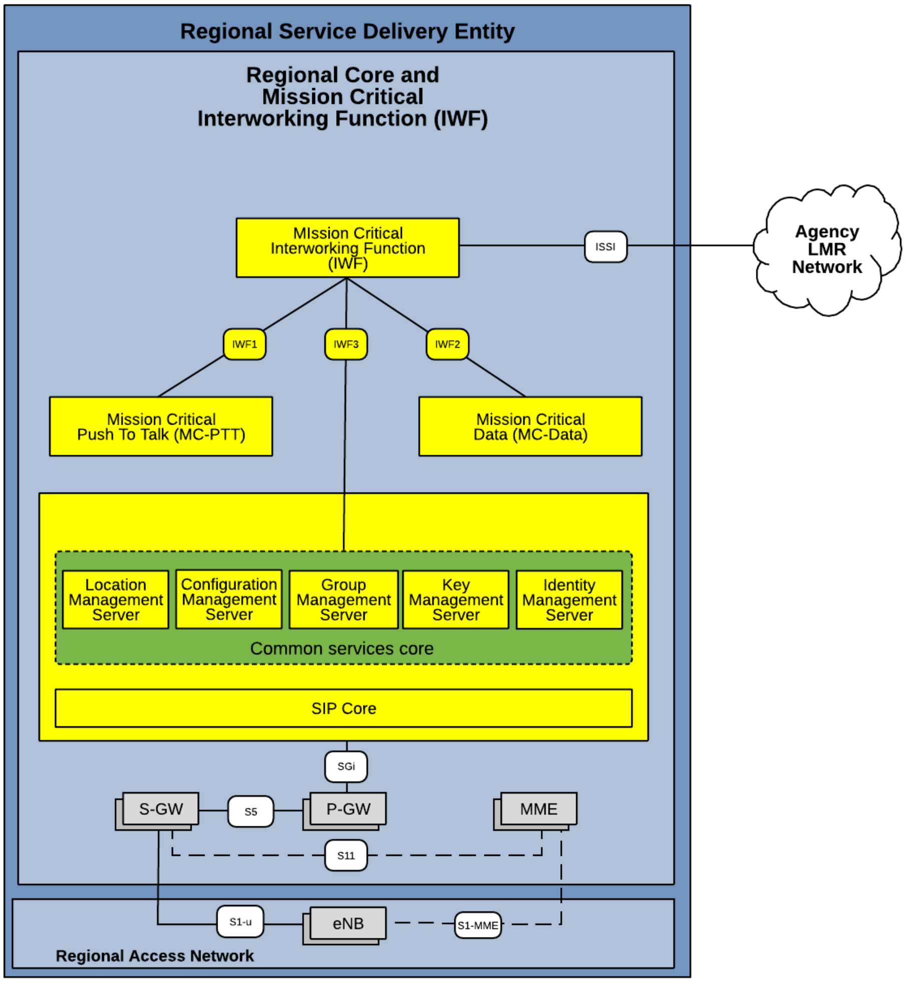

Regional Service Delivery Entity
Regional Core and Mission Critical Interworking Function (IWF)
MIssion Critical Interworking Function (IWF)
ISSI
Agency LMR Network
IWF1
IWF3
IWF2
Mission Critical Push To Talk (MC-PTT)
Mission Critical Data (MC-Data)
Location Management Server
Configuration Management Server
Group Management Server
Key Management Server
Identity Management Server
Common services core
SIP Core
SGi
S-GW
S5
P-GW
MME
S11
S1-u
eNB
S1-MME
Regional Access Network

Figure 31: *PSBN and LMR interconnection.*

The premise is to use the IWF that connects LMR data to the MCData service via the IWF2 interface and use the IWF to connect LMR voice services to the PSBN MCPTT service via the IWF1 interface. The IWF also supports MC-common services via the IWF3. NPSTC has published a report on LMR-LTE interoperability and interworking [67].

8.2 Evolved Multimedia Broadcast Multicast Service (MBMS)

The PSBN will require a Multimedia Broadcast Multicast Service (MBMS) if it plans to offer certain MC services and other point-to-multipoint services to users over LTE. Evolved MBMS (eMBMS) is another LTE broadcast service, but only provides broadcast services within the network. The same carrier frequencies are used to transmit both unicast and broadcast messages in LTE. As such, a portion of the total available bandwidth must be allocated for broadcast use in order to provide eMBMS services. 3GPP TS 22.246 [68] describes the service requirements for the eMBMS service and TS 23.246 [69] describes the eMBMS service requirements/architecture.

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

A number of key components are required in order to enable eMBMS functionality in the LTE network. They are listed and briefly described in Table 28 below. The eMBMS reference points are subsequently listed and described in Table 29.

Table 28: *eMBMS components.*

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

Table 29: *eMBMS reference points.*

Reference Point	Description
M1	User plane interface for the delivery of MBMS data (via IP) from MBMS GW to eNodeBs.
M2	Interface for the provision of radio configuration data and session control signalling between MCE and eNodeB.
M3	Interface to support MBMS Session control signalling (e.g., MBMS session initiation and termination) between MME and MCE.

Reference Point	Description
SGmb	Interface for the control plane between BM-SC and MBMS GW (e.g., MBMS session start, update and stop, and session attributes like service area, QoS).
SGi-mb	Interface providing MBMS data delivery function between BM-SC and MBMS GW.
Sm	Interface for the control plane between MBMS GW and MME.

Figure 32 illustrates an example where an RSDE uses eMBMS components that are highlighted in yellow.

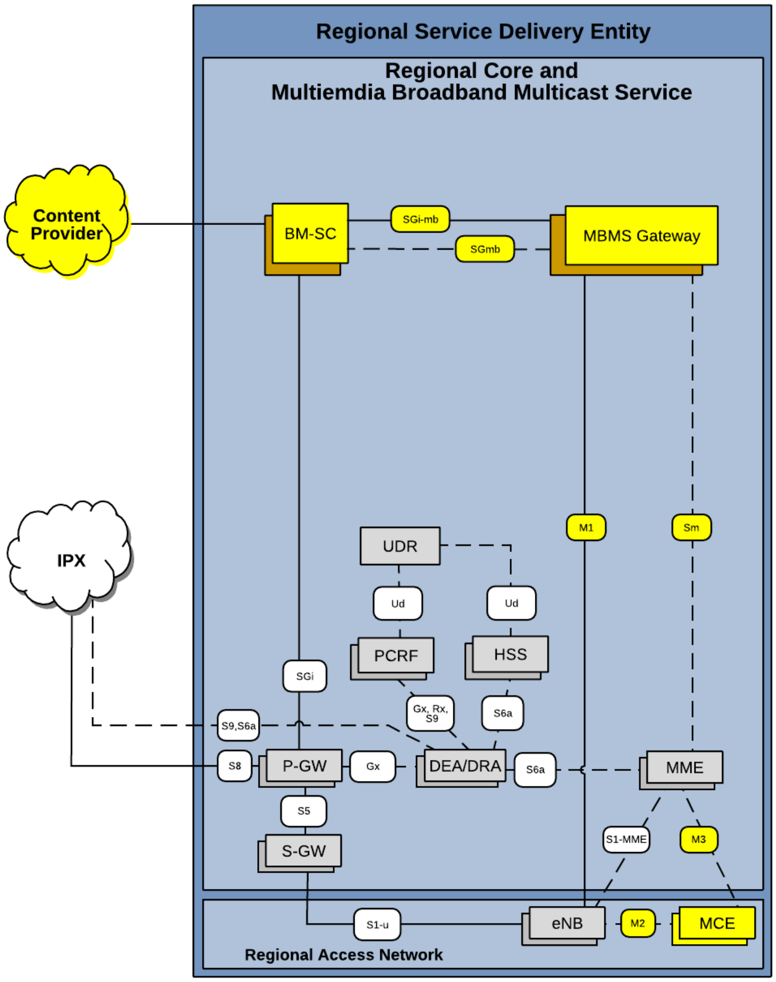


Figure 32: *eMBMS block diagram.*

8.3 Mobile Virtual Private Network (MVPN)

This section compares traditional virtual private network (VPN) technology to mobile VPN (MVPN) technology and then explains how MVPN client and server parts are used between the PSBN and the EUA.

A virtual private network is a network designed to secure remote network access. It extends the reach of EUA local area networks by using a public telecommunication infrastructure, such as the Internet, and does not require any owned or leased private lines. Companies use VPNs to provide telecommuting employees and branch offices with secure access to the corporate network and applications on internal servers. Traditional VPNs, based on IP Security (IPsec) and Secure Sockets Layer (SSL), provide a high level of security when properly configured and used. They use authentication and encryption technologies to protect networks from unauthorized users and to secure data transmissions to and from devices. These VPNs work well for fixed remote access but do not handle the challenges of mobile wireless communication and mobile devices well. These challenges include coverage gaps, inter-network roaming, bandwidth, battery life, and limited memory and processing power.

A MVPN provides the same level of security as the traditional wired VPN solution, but it is optimized for the mobile wireless network. Advanced data compression increases the throughput and provides significantly better performance in wireless networks with small bandwidth compared to a traditional VPN. It provides session persistence and seamless data roaming to create a reliable and seamless user experience when devices switch networks or move out of coverage. Although mobile VPN solutions can offer a certain level of session persistence on non-real-time data sessions, that level is not considered suitable for Mission Critical real-time communications. Additionally, a true mobile VPN has a much smaller memory footprint and uses less processing power than a traditional VPN, enabling applications to run faster while the battery lasts longer. Furthermore, a MVPN is a hosted application that encrypts user and routing information. It adds a header to the encrypted IP packets and provides privacy and confidentiality of the information. It can also buffer information during session breaks and re-establish the flow when the session resumes, even on different networks without the need for users to sign on again to their applications.

8.3.1 MVPN client and server

The typical PSBN application of a mobile VPN is between the PSBN UE acting as a MVPN client that is connected to the EUA Packet Data Network (PDN) via the RSDE Core. The EUA PDN would have a MVPN server which terminates the MVPN connection thereby providing a secure virtual tunnel over the PSBN.

Suppliers of MVPN client and server products draw a distinction between remote access and mobile environments. A remote access user typically establishes a connection from a fixed endpoint, launches applications that connect to EUA resources as needed, and then logs off. In a mobile environment, the endpoint changes constantly (for instance, as users roam between different cellular networks or WiFi access points). A mobile VPN maintains a virtual connection to the application at all times as the endpoint changes, handling the necessary network logins in a manner transparent to the user. In Table 30, a description is given of the functions which are used in building a MVPN service.

Table 30: *MVPN client/server functions.*

Function	Description
Persistence	Open applications remain active, open and available when the wireless connection changes or is interrupted. Also applies to idle mode operation with LTE devices.
QOS Indication	Specifies the priority that different applications or services should receive when contending for available wireless bandwidth; this is useful for ensuring delivery of the essential "mission-critical" applications (such as computer-assisted dispatch for public safety) or giving priority to streaming media or voice-over-IP.
Roaming	Underlying virtual connection remains intact when the device roams to a different network while the MVPN handles the logins automatically.
Application Compatibility	Software applications that run in an "always-connected" state will work on Mobile VPNs without modification.
Security	Enforces authentication of the user, the device or both, as well as the selected encryption of the data traffic in compliance with security standards such as FIPS 140-2. For authentication between MVPN Client and server peers, Internet Key Exchange version 2 (IKEv2) is the next generation standard for secure key exchange between peer VPN devices, as defined in RFC 7296, "Internet Key Exchange Protocol Version 2 (IKEv2)" [70]. An IKEv2 server requires a certificate to identify itself to clients. RFC 4945, "The Internet IP Security Public Key Infrastructure (PKI) Profile of IKEv1/ISAKMP, IKEv2, and PKIX" [71] provides a profile of IKE and PKIX that defines the requirements for using PKI technology in the context of IKE/IPsec.
Acceleration	Link optimization and data compression improve performance over wireless networks, especially cellular networks where bandwidth may be constrained.
Management Console	Displays status of devices and users, and offers the ability to quarantine a device if there is possibility that it may have been lost or stolen.
Policy Management	Enforces access policies based on the network in use, bandwidth of the connection, on layer-3 and layer-4 attributes (IP address, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port, etc.), time of day, and in some VPNs, the ability to control access by individual application software.
Network Access Control (NAC)	Evaluates the patch status, anti-virus and anti-spyware protection status, and other aspects of the "health" of the device before allowing a connection; and optionally may integrate with policies to remediate the device automatically.

8.4 Next generation 911

NG 911 is intended to replace the existing narrowband, circuit switched 911 networks with a system supporting seamless, end-to-end IP-based communication of emergency related voice, text, data, photos, and video between the public and public safety answering points (PSAP). NG 911 requires the implementation of emergency services IP networks (ESInets), which provide interconnectivity and interworking between originating wireless networks and PSAPs. The ESInet is intended to be a nationwide network-of-networks that interconnects local and regional PSAP networks.

The National Emergency Number Association (NENA) created the i3 set of requirement and architecture documents which define Session Initiation Protocol (SIP)-based interfaces to interact with the NG 911 system. The scope includes gateways for legacy wireline and wireless networks that are used to initiate emergency calls, and which do not create call signalling matching the interfaces defined for the ESInet. The NENA i3 architecture can be viewed and downloaded at [11].

The 3GPP standards body also published a specification on IMS emergency sessions (TS 23.167 [45]) that introduces an additional function in the IMS architecture called Emergency Call Session Control Function (E-CSCF), along with reference points to connect to PSAPs via IP or traditional PSTN links. This concept is illustrated generically in Figure 33 where the PSBN's data and voice (IMS) domains are connected to the NG 911 network via the IMS Interconnect-Network-to-Network Interface (II-NNI). In the IMS core, the Interconnection Border Control Function (IBCF) serves as the IMS point of attachment to the II-NNI. The E-CSCF is connected to the IBCF using the Mx interface. PSBN users that place 911 calls via the RSDE core will be handled by the IMS core and then routed to the E-CSCF which routes the call over the Emergency Services IP network (ESInet) to the PSAP. The PSBN will also provide location information of the UE that has initiated an emergency session to the ESInet.

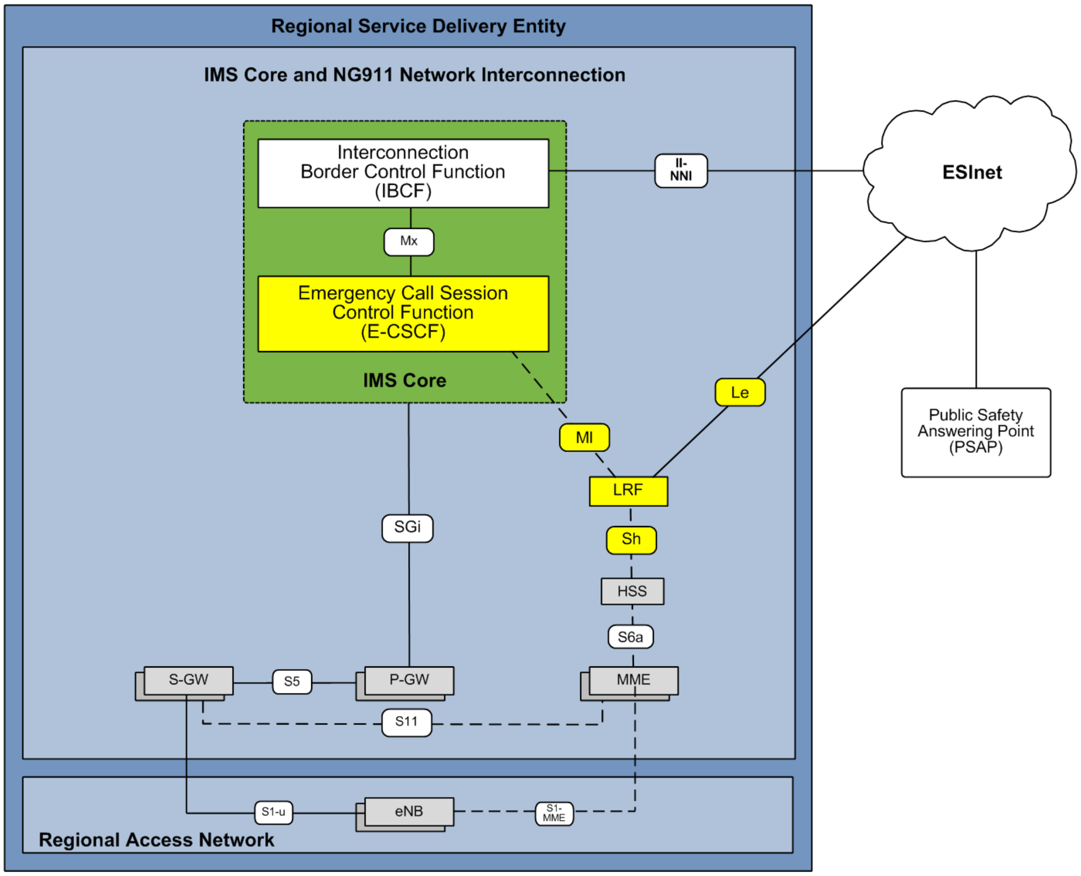

Regional Service Delivery Entity
IMS Core and NG911 Network Interconnection
Interconnection Border Control Function (IBCF)
Mx
Emergency Call Session Control Function (E-CSCF)
IMS Core
II-NNI
ESInet
Le
Ml
LRF
Public Safety Answering Point (PSAP)
SGi
Sh
HSS
S6a
S-GW
S5
P-GW
MME
S11
S1-u
eNB
S1-MME
Regional Access Network

Figure 33: *NG 911 interconnection to the RSDE IMS core.*

Table 31and Table 32 provide descriptions of the components and reference points of NG-911, respectively.

Table 31: *Components of NG-911.*

Component	Name	Description
LRF	Location Retrieval Function	The LRF handles the retrieval of location information for the UE including, where required, interim location information, initial location information and updated location information. The LRF may interact with a separate location server or contain an integrated location server in order to obtain location information.

Table 32: *NG-911 reference points.*

Reference Point	Description
Sh	Used to exchange user profile information between the HSS and an application server. The user profile information can consist of user related data, group lists, user service related information or user location information or charging function addresses. Uses the Diameter protocol.
Le	Used by the external LCS client to retrieve location information from the LCS server. Signalling on this interface may use the OMA Mobile Location Protocol (MLP) and Open Services Access Application Programming Interface (OSA-API).
Ml	Allows the E-CSCF to request the LRF to validate the location information received from the UE, to determine or query the LRF for routing information to emergency centres.

8.5 Non-3GPP wireless access networks

This section focuses on non-3GPP access technologies with the exception of trusted WiFi which is considered to be part of the PSBN radio access network and is described in Section 5.2.4.

In order to extend public safety broadband wireless coverage beyond the Band 14 PSBN footprint, it is expected that public safety agencies will want to take advantage of wireless technologies that extend their wireless coverage. Several agencies implement non-3GPP access networks in their respective offices and locations, many of which are based on WiFi. While the Evolved Packet System (EPS) consists of the UE, E-UTRAN and EPC, as explained in 3GPP TS 23.402 [32], it also allows UEs to interconnect with non-3GPP technologies such as WiFi. Non-3GPP simply means that these access network standards were not specified in the 3GPP and are categorized as either trusted or un-trusted from a PSBN's perspective. Section 5.2.4 describes the differences between trusted and un-trusted networks, but essentially, trusted networks can interact directly with the PSBN core whereas un-trusted networks interwork with the PSBN via a network entity called the evolved Packet Data Gateway (ePDG). The main role of the ePDG is to provide security mechanisms such as IPsec tunneling of connections with the UE over an un-trusted non-3GPP access network. 3GPP does not specify which non-3GPP technologies should be considered trusted or un-trusted. This decision is made by the operator.

In 3GPP TS 23.402 [32], there are many diagrams as to how to configure both non-roaming and roaming architectures for non-3GPP access to 3GPP EPS. Figure 34 and Figure 35 below represent a valid configuration that could be considered for the PSBN by the RSDEs since it provides support for both trusted and un-trusted non-3GPP access networks, depending on the operator's decision to implement one or the other or both.

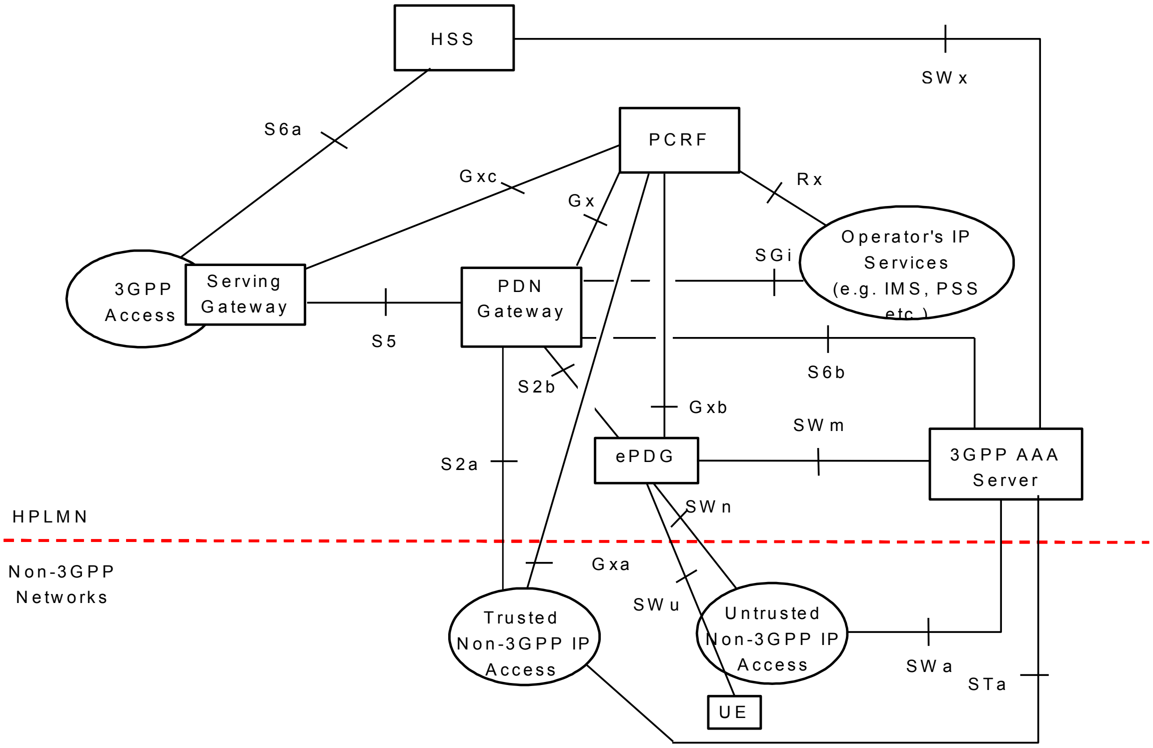


Figure 34: *Non-roaming architecture within EPS (source: 3GPP 23.402 [32]).*

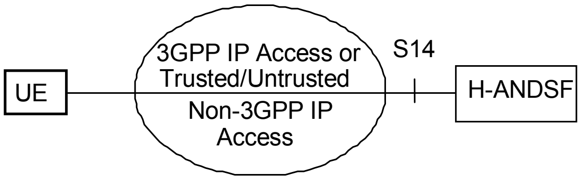


Figure 35: *Non-roaming architecture within EPS using H-ANDSF (source: 3GPP 23.402 [32]).*

Referencing the above figures, Table 33 and Table 34 list the components and reference points involved in the connection to trusted and un-trusted non-3GPP networks accessing the PSBN RSDE LTE Networks.

Table 33: *Components to support trusted and un-trusted wireless access networks.*

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

Table 34: *Reference points to support trusted and un-trusted wireless access networks.*

Reference Point	Description
S2a	Provides the user plane with related control and mobility support between trusted non 3GPP IP access and the Gateway.
S2b	Provides the user plane with related control and mobility support between ePDG and the Gateway.
S6b	Reference point between PDN Gateway and 3GPP AAA server/proxy for mobility related authentication if needed. This reference point may also be used to retrieve and request storage of mobility parameters and to retrieve static UE QoS profiles for non-3GPP access in case dynamic Policy and Charging Control is not supported.
Gx	Provides transfer of QoS policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the P-GW.
Gxa	Provides transfer of QoS policy information from PCRF to trusted non-3GPP accesses.

Reference Point	Description
Gxb	Provides transfer of QoS policy information from PCRF to the ePDG.
Gxc	Provides transfer of QoS policy information from PCRF to the S-GW.
SWa	Connects the un-trusted non-3GPP IP access with the 3GPP AAA Server/Proxy and transports access authentication, authorization and charging-related information in a secure manner.
STa	Connects the trusted non-3GPP IP access with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters and charging-related information in a secure manner.
SWm	Reference point located between 3GPP AAA Server/Proxy and ePDG used for AAA signalling such as transport of mobility parameters, tunnel authentication and authorization data. This reference point also includes the MAG-AAA interface functionality and Mobile IPv6 NAS-AAA interface functionality.
SWn	Reference point between the un-trusted Non-3GPP IP access and the ePDG. Traffic on this interface for a UE-initiated tunnel has to be forced towards ePDG. This reference point has the same functionality as Wn which is defined in TS 23.234 [72].
SWu	Reference point between the UE and the ePDG and supports handling of IPSec tunnels. The functionality of SWu includes UE-initiated tunnel establishment, user data packet transmission within the IPSec tunnel, tear down of the tunnel and support for fast update of IPSec tunnels during handover between two un-trusted non-3GPP IP accesses.
SWx	Reference point located between 3GPP AAA Server and HSS and used for transport of authentication, subscription and PDN connection related data.
S14	Reference point between UE and Home ANDSF or Visited ANDSF for direct queries via pull. It enables dynamic provision of information to the UE for access discovery and selection procedures related to 3GPP and non-3GPP accesses. This dynamic provision is supported with pull (UE-initiated session) and with push (ANDSF-initiated session), if feasible. Communication over S14 is secured as specified in TS 33.402 [31].

The procedures for 3GPP WLAN (WiFi) access selection and PLMN selection are defined in 3GPP TS 23.402 [32]. The 3GPP standards for non-3GPP access to 3GPP networks adds the following capabilities:

- Dynamic management and switching of individual IP-Flows (e.g., IFOM) from one radio interface to another based on QoS requirements, user subscription, and equipment type (TS 23.261 [42] via Dual Stack Mobile IP).
- The inter-system mobility policy (ISMP) to route IP traffic only over a single radio access interface at a given time in order to select the most preferable access technology type or access network that should be used to connect to EPC. The inter-system mobility policy is a set of operator-defined rules

that affect the inter-system mobility decisions taken by the UE in multi-access PDN connectivity (MAPCON) scenario.

- The inter-system routing policy (ISRP) rules to route IP traffic simultaneously over multiple radio access interfaces in order to meet the operator routing / offload preferences. The ISRP is a set of operator-defined rules that determines how the UE should route IP traffic across multiple radio access interfaces. The access network discovery and selection function (ANDSF) provides a list of ISRP rules to the UE independently of the UE capability to route IP traffic simultaneously over multiple radio access interfaces.
- Access network selection and traffic steering based on RAN-assisted WLAN interworking. (e.g., described in TS 23.401 [19] Section 4.3.23).
- ANDSF device client and server provides operator policies regarding discovery and selection of WiFi access. The 3GPP ANDSF specifications are described in the following table.

Table 35: *3GPP specification list for access network discovery and selection function.*

TS 23.402	Architecture enhancements for non-3GPP accesses
TS 24.302	Access to the 3GPP EPC via non-3GPP access networks
TS 24.312	ANDSF Management Object
TS 33.402	3GPP SAE; Security aspects of non-3GPP accesses
TR 23.853	OPIIS, Inter-APN Routing Policy
TR 23.890	Optimized Offloading to WLAN in 3GPP RAT
TR 23.865	Study on WLAN Network Selection (WLAN_NS)

8.5.1 Evolving standards for non-3GPP access to 3GPP networks

Efforts by 3GPP to further standardize WiFi to 3GPP interworking capabilities are the basis for enhancements in TS 23.402. Simultaneously, the cellular industry has converged on a single mobile broadband standard which has facilitated WiFi/Cellular integration work [73]. Historically, 2G and 3G mobile access technologies were fragmented. EIA/TIA-based TDMA and CDMA access dominated in North America; whereas 3GPP based networks were the preferred option in much of the rest of the world. Today LTE is the clear 4G evolution choice of all major operators. The global convergence towards 3GPP based standards for 4G facilitates integration with WiFi as there is greater economy of scale for mobile devices, more roaming partner opportunities, and hence increased incentives for operators to invest in WiFi/3GPP interworking infrastructure. Thus, many mobile operators are considering how WiFi can complement and enhance their existing infrastructure deployments.

More specifically, 3GPP has spent several years standardizing the ANDSF. ANDSF provides a framework for operators to customize network steering policies and distribute those policies down to devices.

Altogether, these newly standardized tools for simplified roaming, seamless handovers, and more intelligent network steering, are designed to enable users to continue using data services as they pass between cellular macro cells, small cells and WiFi hotspots, with no need for further authentication or user intervention. That is, these standards seek to provide a transparent and secure user experience regardless of the radio access technology used to serve a given subscriber.

9 PSBN network management

This section describes the network management aspects of a PSBN.

9.1 Telecommunications Management Network (TMN)

Telecommunications management networks (TMN) are used for the management of telecommunication networks operated by administrations, customers, or other organizations and individuals. When these telecommunication networks are inter-connected with each other, their TMNs provide the means of exchanging information required to manage end-to-end telecommunication services. All types of telecommunication networks and network elements—such as analogue networks, digital networks, public networks, private networks, switching systems, transmission systems, telecommunication software, and logical resources of the network (such as circuit, path, or telecommunication services supported by these resources) are candidates for management by a TMN.

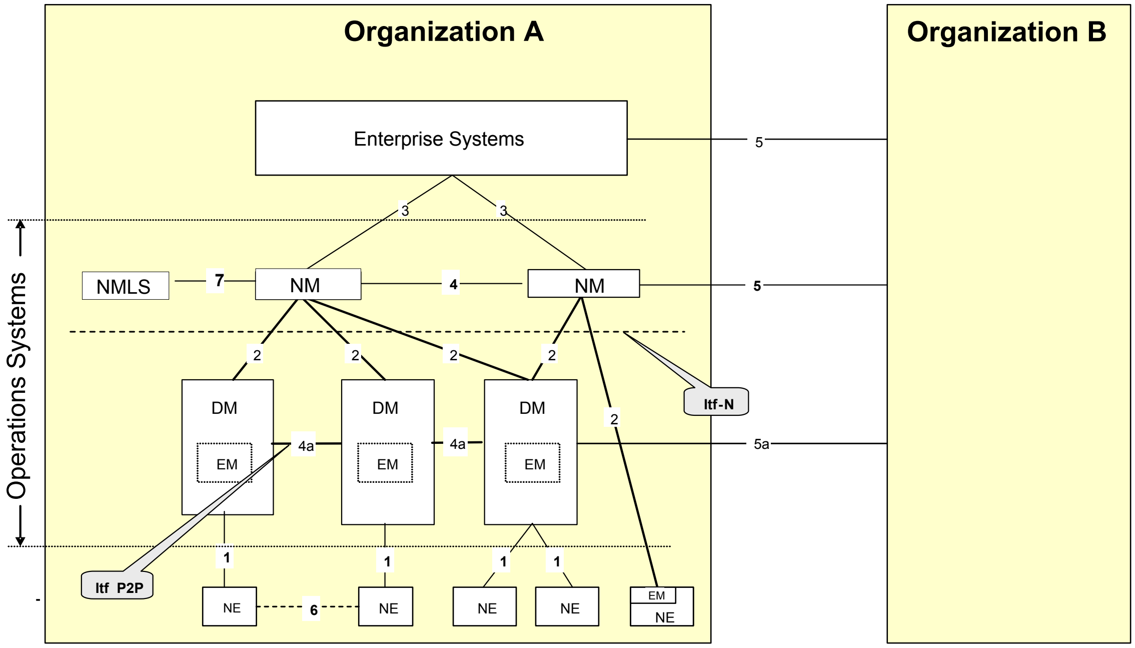


Figure 36: *The 3GPP telecommunication management model (source: TS 32.101 [74]).*

Based on these high-level requirements described in TS 32.101 [74], the 3GPP TMN architecture for managing the PSBN Public Land Mobile Network (PLMN) is specified in the 3GPP TS 32.102 [75]. For the PSBN, there are multiple TMNs, where each RSDE and national entity will have its own. As indicated in Figure 36, organizations (e.g., RSDEs or NE) are inter-connected using the interfaces 5 and 5a. At different layers of the TMN in each organization, these interfaces are used to interconnect the Operations Support Systems (OSS) and the Enterprise Systems (ES) that are in the national entity and each of the RSDEs. Within these OSSs, there are network management functions and element management functions. These element management functions provide for the management operation of the underlying network elements that are in the RSDE networks and national entity networks. Figure 37 illustrates the domains of Operations Support Functions (OSF) that provide management of the user equipment, access network, core network and service specific entities. Each of the RSDEs will implement these OSFs for each domain. Moreover, the national entity will implement these OSFs as well, if it is acting on behalf of an RSDE that has decided to not implement the PSBN core network functions for its respective regional network.

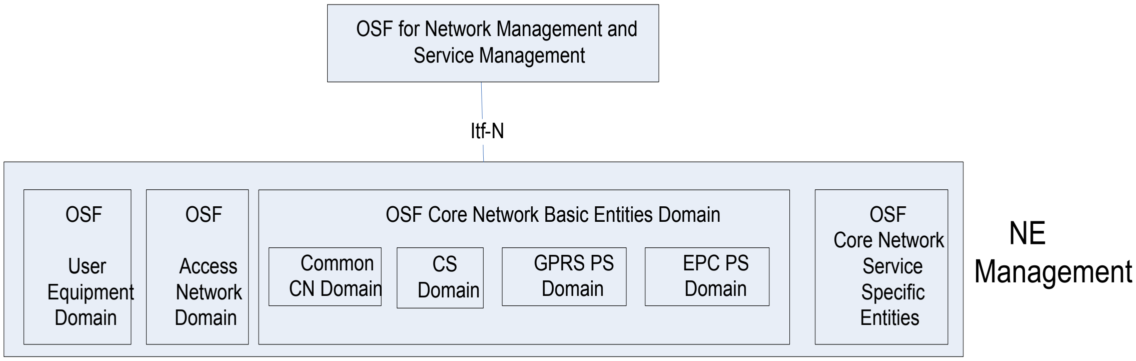

OSF for Network Management and Service Management
Itf-N
OSF User Equipment Domain
OSF Access Network Domain
OSF Core Network Basic Entities Domain
Common CN Domain
CS Domain
GPRS PS Domain
EPC PS Domain
OSF Core Network Service Specific Entities
NE Management

Figure 37: *Overview of 3GPP telecommunications management domains (source: 3GPP TS 32.102 [75]).*

9.2 Operations support system

The TM Forum (TMF) has released a complete blueprint for a platform for managing a multi-vendor hybrid infrastructure as part of its Agile OSS toolkit [76]. The blueprint brings together multiple elements into one set of tools in the TMF070 suite of documents [77]. The suite includes key practical assets such as Open APIs, information models, best practices and deployment guides. Together these provide the standard interface required for multi-vendor hybrid deployments.

9.2.1 Mobile device, MTC device and application management

The Open Mobile Alliance (OMA) maintains a registry of Device Management (DM) descriptions [78] and the values used for many Managed Objects (MO) implementing specific management functions. The Table 36 below provides a sample of the function names as Managed Objects and provides a short description of the MO.

Table 36: *OMA mobile device Managed Objects (functions).*

Function	Description
Firmware Update (FUMO)	The OMA device management Firmware Update Managed Object (FUMO).
Software Management (OMA DM SCOMO)	The Software Component Managed Object (SCOMO) allows not only the installation and the removal of applications on the mobile device, but also the retrieval of the inventory of software components already installed on the mobile device.

Function	Description
Management Policy (OMA DM Management Policy MO)	Allows the deployment on the device of policies which the DM client can execute and enforce independently: if some events happen, then perform some operations.
M2M / Internet of Things Technology	The OMA DM working group with its expertise in remote management addressed the Machine-to-Machine (M2M) environment with OMA Lightweight M2M protocol, which focuses on constrained cellular and sensor network M2M devices.
Device Capabilities (OMA DM DCMO)	Allows a management authority to remotely enable and disable device peripherals like cameras, Bluetooth, USB, etc.
Lock and Wipe (OMA DM LAWMO	Allows a management authority to remotely lock and/or wipe the device, for instance when the device is stolen or sold, or when personal or enterprise data are compromised.
Browser (OMA DM BMO)	Allows remote management of browser favorites and settings.
Diagnostics and Monitoring (OMA DM DiagMon MO)	Enables remote diagnostic, for example to query the device for memory and battery status or to collect radio measures and QoS parameters, and remote monitoring, by defining trap and reports.
Connectivity (OMA DM ConnMO)	Evaluates the patch status, anti-virus and anti-spyware protection status, and other aspects of the "health" of the device before allowing a connection; and optionally may integrate with policies to remediate the device automatically.

9.2.2 Inventory manager

As written in 3GPP TS 32.690 [79], the main task of network inventory management is to manage network inventory information about the various static resources of a mobile telecommunications network. It provides support to network planning, network operation and maintenance. Inventory management functions are distributed over different layers of a Telecommunications Management network (TMN). The main task of the inventory management function is to provide an efficient access for network management systems to the static inventory data of all related managed network elements.

In 3GPP TS 32.692 [80], Inventory Management (IM) actions have the objective to monitor the actual configuration on the network elements and network resources, and they may be initiated by the operator or by functions in the OSS or network elements. The final goal of IM is the establishment of an accurate and timely model of the actual inventory of the network elements or network resources.

IM actions may be requested to reflect changes initiated by configuration management actions or to make sure that the inventory model is in sync with the actual inventory. IM actions are initiated either as single actions on single network elements of the LTE network or as part of a complex procedure involving actions on many resources/objects in one or several network elements.

9.2.3 Configuration manager

In 3GPP TS 32.600 [81], Configuration Management (CfM), specifically provides the mobile network operator with the ability to assure correct and effective operation of the PLMN network as it evolves. CfM actions have the objective to control and monitor the actual configuration on the network elements and network resources, and may be initiated by the operator or by functions in the OSS or network elements.

9.2.4 Trouble ticket system

The TMF standard for a trouble ticket API provides a standardized client interface to trouble ticket management systems for creating, tracking and managing trouble tickets among partners as a result of an issue or problem identified by a customer or another system. Examples of trouble ticket API clients include customer relationship management (CRM) applications, network management or fault management systems, or other trouble ticket management systems (e.g., B2B). TMF661 Trouble Ticket API Conformance Profile R16.5.1 standard [82] is the REST API conformance for the trouble ticket API.

9.2.5 Self-Organizing Networks (SON)

The 3GPP has specified the Self Organizing Network (SON) function [83] to help MNOs with RAN network design and to facilitate inserting new cells into their existing fabric by automating some of the network planning, configuration and optimization processes. The SON function is used to optimize:

- Handover performance when the service of a mobile device is transferred from one eNodeB to another
- Load balancing between cells
- Capacity and coverage optimization
- UE attach optimization via the Random Access Channel (RACH) parameters

There are several parameters in the eNodeBs that need to be adjusted and configured to accommodate the insertion of new ones into existing networks, such as:

- neighbour relations list;
- physical cell identity;
- uplink reference signals; and
- uplink preamble.

SON algorithms automate the task of configuring and adjusting these parameters. It is important to note that certain SON aspects will not be specified by the 3GPP, especially the SON algorithms themselves.

The 3GPP has specified three stages for the roll-out of SON capabilities, as described in 3GPP TS 32.500 [84] and summarized in Table 37.

Table 37: *Self-organizing network functions.*

Function	Description
Self Configuration (Stage 1)	• Plug-n-play (PNP) • Faster rollout, automatic inventory, automatic software download • Consistency and PCI assignment • Licences, hardware inventory and software build efficient resource utilization
Self Optimization (Stage 2)	• Mobility Robustness Optimization (MRO) • Mobility Load Balance (MLB) and automatic neighbour relations • Minimization of Drive Testing (MDT) • Fast and proactive parameter optimization • Increased network performance
Self Healing (Stage 3)	• Fast, autonomous failure mitigation • Continuous performance monitoring • Faster network maintenance • More efficient resource utilization, less effort

The minimum 3GPP specifications that are relevant for SON are as follows:

- TS 32.500 Telecommunication management; Self-Organizing Networks (SON); Concepts and requirements [84];
- TS 32.521 Telecommunication management; Self-Organizing Networks (SON) Policy Network Resource Model (NRM) Integration Reference Point (IRP): Requirements [85];
- TS 32.522 Telecommunication management; Self-Organizing Networks (SON) Policy NRM IRP: Information Service (IS) [83];
- TS 32.526 Telecommunication management; Self-Organizing Networks (SON) Policy NRM IRP: Solution Set (SS) definitions [86];
- TS 32.511 Telecommunication management; Automatic Neighbor Relations (ANR) Management; concepts and requirements [87].

In 3GPP TS 32.500, the following SON functions and network capabilities are identified and require support from the EMS and NMS:

- SON in a multi-vendor network
- Self-establishment of a new eNodeB
- Automatic neighbour relation management
- Self-optimization, Self-healing
- Continuous optimization due to dynamic changes in the network

The 3GPP's reference architecture for the SON functions is illustrated in Figure 38. It shows that some SON functions are resident in the element and network management layers and use the reference point "ItF-N" to communicate requests for configuration information and assert changes to configuration parameters that are carried between Network Manager (NM) and Element Manager (EM). However, there is provision for the eNodeB to host a local SON decision algorithm and that the X2 reference point is intended to communicate the relevant parameters directly between the eNodeBs to overcome processing delays and enable a fast adaptation to changing conditions. The reference architecture accounts for a hybrid SON architecture, in which decisions can be taken locally, i.e., at the eNodeB level or centrally, at the EM and NM levels.

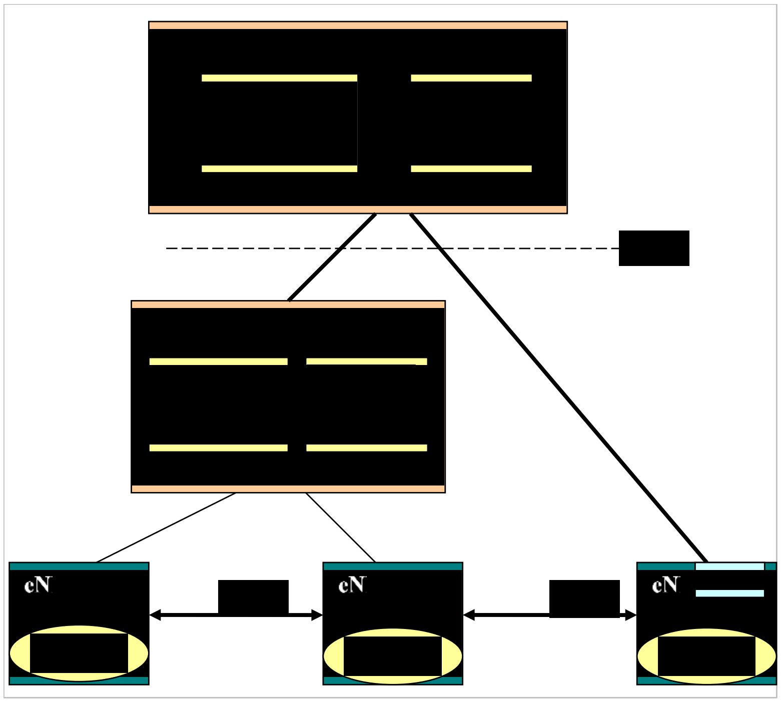


Figure 38: *Reference architecture for the SON functions illustrating coordination performed at the Network Manager layer (source: 3GPP TS 32.522 [83]).*

A significant challenge is how to apply SON to a network consisting of eNodeBs from different vendors. Most vendors of LTE infrastructure offer SON solutions that operate according to their proprietary algorithms and are specific to their products because SON is tightly coupled with the provisioning function of those products. The 3GPP has acknowledged the risk that SON algorithms from different vendors may conflict and worsen the interoperability between eNodeBs than if they were not present at all and has proposed ways to mitigate that risk. In 3GPP 32.500 [84] Section 6.1.2, titled "SON in a Multi-Vendor Network," the following requirements for MV-SON are described:

REQ-SON-CON-003 Self-establishment and self-optimization shall be supported in a multiple vendor environment. Standardized procedures and Operations, Administration and Maintenance (OAM) interfaces are needed to avoid cost-intensive mediation between different vendor nodes and side effects due to different detailed solutions (e.g., different optimization algorithm leads to ping-pong effects and swinging phenomena).

REQ-SON-CON-004 The standardized information made available to SON algorithms shall be consistent, independent of the vendor.

At the time of writing, there are no 3GPP guidelines answering these two requirements, but there are some industry efforts and proposals to address multi-vendor SON issues. For example, the 4G Americas publication "Self-Optimizing Networks: The Benefits of SON in LTE" dated October 2013 discusses multi-vendor SON architectures. Additionally, the Next Gen Mobile Network (NGMN) Alliance has written a summary review of a project called "P-Smallcell Work Stream 2 (WS2)" [88]. This Scientific Report is primarily focused on promoting multi-vendor deployment of heterogeneous networks, with a focus on SON interoperability. Of the many planning aspects covered in the NGMN report, the most important for the PSBN are "SON features description and analysis of multi-vendor deployments" and "Descriptions of potential interoperability issues for each SON feature and the recommended proposals for solving or reducing these issues." The Interoperability issues and recommended resolutions that are described therein cover:

- Physical Cell ID Optimization (PCI)
- Automatic Neighbour Relation (ANR)
- Mobility Robustness Optimization (MRO)
- Mobility Load Balancing (MLB)
- Coverage and Capacity Optimization (CCO)

In order for the benefits of SON to be achieved in the regions of the PSBN that span the coverage boundaries of adjoining RSDEs, the RSDEs must coordinate the requirements and management of the attributes of their respective networks that impact the proper functioning of SON. The performance of the algorithms is not specified by 3GPP and is out of scope of this Scientific Report. However, the operators of the PSBN should agree on the SON architecture and the algorithms that will be used for the SON functions, as well as coordinate any changes to the algorithms over time.

9.3 Network Operations Centre (NOC)

Within the PSBN, there will be two levels of Network Operation Centres (NOC). The national entity network operations centre (N-NOC) operates at a national level. At this level, the national entity is responsible for the national transport network, nationally-hosted applications, negotiations with international, national and regional roaming partners, and with the FirstNet/AT&T network. As well, it is assumed that the N-NOC's mission will monitor compliance to the governance and regulatory aspects of the PSBN. The RSDE level will be responsible for serving PSBN users directly, so they have the need for a robust implementation of a Regional Network Operation Centre (R-NOC).

A NOC monitors the telecommunications network for alarms or certain conditions that may require special attention in order to avoid impact on network performance. NOCs are capable of analyzing problems, performing troubleshooting, communicating with site technicians and tracking problems until they are resolved. Network operation centres serve as the main focal point for software troubleshooting, software distribution, and updating router and domain name management in coordination with affiliated networks and performance monitoring. All NOCs are mirrored at geo-redundant sites in order to protect against catastrophic failures that may occur at any one site. The sites are located in areas where the same threat cannot affect the mirrored sites. For example, a NOC that is located where hurricanes may occur would have a mirrored site in a location where hurricanes do not occur.

At the core of the NOC is the Network Management System (NMS). The NMS touches every network element either directly or indirectly through Element Management Systems (EMS). It monitors the status of those elements and correlates the data it collects into information that is presented in a human-understandable manner—often in a graphical, contextualized representation that can be easily and accurately interpreted by the NOC staff. Some key features of an NMS are:

- Support for drag and drop;
- Context sensitive menus;
- Real-time updates;
- Information overlaid on geographic and logical maps in various layers;
- Photorealistic equipment views;
- Ability to customize the views, alarms, workflow, and any other aspects that can simplify the daily work of NOC operators and allow faster network roll-out, identification and restoration of network and service issues.

10 Service management

This section describes the service management aspects of the PSBN.

10.1 PSBN services and applications architecture

The PSBN will be a nationwide interoperable wireless network consisting of cellular, and potentially non-cellular communications technologies used in the national and/or regional service delivery entities. In addition to basic communications, the PSBN also provides a set of services and applications that will offer enhanced communication and information services to public safety personnel.

As witnessed throughout this Scientific Report, the PSBN functional architecture leverages many network and service industry standards such as Open Mobile Alliance (OMA), Telecommunications Management Forum (TMF), GSM Association (GSMA) and several other standards development organizations. Moreover, a significant emphasis is placed on 3GPP service specifications. The 3GPP TS 22.101 [22] describes the service principles for PLMNs specified by 3GPP. As well, the principles and requirements for interworking with non-3GPP access networks are specified in 3GPP TS 23.402 [32]. Each RSDE could implement a telecommunication management network (TMN) based on the principles and high-level requirements that are specified in 3GPP TS 32.101 [74] with the TMN architecture specified in 32.102 [75].

The PSBN provides both network connectivity as well as voice, video and data services and applications to PSBN users. These services and applications could originate from inside the PSBN either at the national entity or at the RSDE. Additionally, some of these applications will originate externally from EUAs or 3rd parties. There are several types of applications that originate from within the PSBN. Some are directly consumed by PSBN users whereas other applications and services are used by operators to enable the functions that are needed to on-board new offerings to PSBN users. These types of on-boarding services and applications include OSS applications, Business Support System (BSS) applications, base and enhanced functions and services, and other PSBN applications. Furthermore, these PSBN applications could be mobile device based applications or server based applications that could be mission critical or non-mission critical that interact directly with the PSBN users.

Within the PSBN service architecture are the Service Delivery Platform (SDP) components that include the SCEF, Common Application Programming Interface Framework (CAPIF), Enterprise Service Bus (ESB), Service Orchestrator and Policy Management Framework. These components provide the necessary functions to enable network capabilities to be securely exposed as service capabilities via the SCEF and can be programmed through the CAPIF. Each of these APIs would be connected to the ESB to make these API services available to OSS applications, BSS applications, trusted operator applications and un-trusted 3rd party applications via a secure gateway. Figure 39 shows a layered view of a services architecture. The services layer is built upon the Evolved Packet System (EPS) network layer. Table 38 lists each of the components of the services layer with a description of that component.

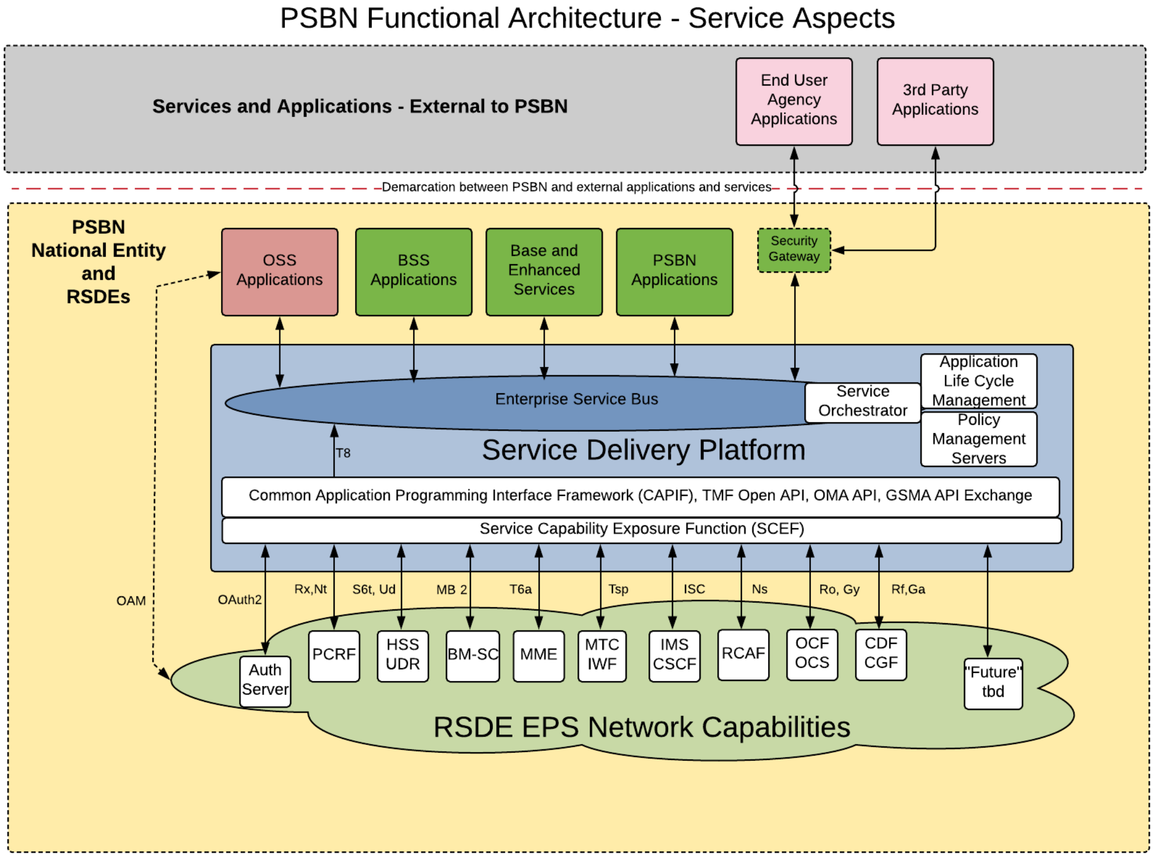

PSBN Functional Architecture - Service Aspects
Services and Applications - External to PSBN
End User Agency Applications
3rd Party Applications
Demarcation between PSBN and external applications and services
PSBN National Entity and RSDEs
OSS Applications
BSS Applications
Base and Enhanced Services
PSBN Applications
Security Gateway
Enterprise Service Bus
Service Orchestrator
Application Life Cycle Management
Policy Management Servers
T8
Service Delivery Platform
Common Application Programming Interface Framework (CAPIF), TMF Open API, OMA API, GSMA API Exchange
Service Capability Exposure Function (SCEF)
OAM
OAuth2
Rx,Nt
S6t, Ud
MB 2
T6a
Tsp
ISC
Ns
Ro, Gy
Rf,Ga
Auth Server
PCRF
HSS UDR
BM-SC
MME
MTC IWF
IMS CSCF
RCAF
OCF OCS
CDF CGF
"Future" tbd
RSDE EPS Network Capabilities

Figure 39: PSBN functional architecture—service aspects.

Table 38: PSBN functional architecture—component descriptions.

Component	Description
Service Oriented Architecture (SOA)	Adapted from 3GPP TS 32.101 [74], the basic building block of any SOA is a service. In the context of this document, the word service is used to denote the various kinds of PSBN services offered, provided or provisioned by and consumed by network elements and network applications. These types of services are combined and offered as composite services to PSBN mobile phone users. One example of this type of composite service is one that is used for locating a PSBN user during an incident and sending that information to the dispatcher. More information on SOA for telecommunications[14] is available online.

[14] SOA For Telecom, http://www.thbs.com/thbs-insights/soa-for-telecom [89].

Component	Description
Service Delivery Platform (SDP)	As shown in Figure 39, the SDP provides all the capabilities needed for new application enablement, service delivery and orchestration of sequenced execution of network and service capabilities that are needed for offering new user offerings.
Service Capability Exposure Function (SCEF)	The SCEF provides a means to securely expose the services and capabilities provided by 3GPP network interfaces and provides a means for the discovery of the exposed services and capabilities. The SCEF provides access to network capabilities through homogenous network application programming interfaces (e.g., network APIs) defined over the T8 interface. The SCEF abstracts the services from the underlying 3GPP network interfaces and protocols. Individual instances of SCEF may vary depending on what service capabilities are exposed and what API features are supported. The SCEF is always within the trust domain. An application can belong to the trust domain or may lie outside the trust domain. The SCEF functions are described in the 3GPP TS 23.682 [35]. In 4-2, there are a number PSBN EPS network capabilities that have defined interfaces into the SCEF.
Common Application Framework (CAPIF)	The 3GPP has conducted studies (e.g., Technical Report (TR) 23.722 [90]) and defined requirements on architecture (e.g., TS 23.222 [91]) to define what common functions must be supported in an API framework.
Industry based APIs	In addition to the 3GPP API Framework, other industry groups have been defining their own APIs for mobile application development. The use of APIs other than the 3GPP common API framework are considered in the PSBN service architecture. Examples of industry API programs are the GSM (Groupe Spéciale Mobile) Association (GSMA) API exchange, Open Mobile Alliance (OMA) API Program and Telecommunications Management Forum (TMF) Open API program.
Enterprise Service Bus (ESB)	Within the SDP, the ESB acts as a message flow management system to allow requests and responses to be exchanged by all systems and applications that are connected to the ESB.
Service Orchestrator (SO)	To help automate the rapid introduction of new PSBN offerings based on existing modular functions, the Service Orchestrator executes a sequenced set of scripted operations that enable composite services to be offered to the PSBN users. The Service Orchestrator is attached to the ESB and therefore has the ability to call services from other systems and application that are attached to the ESB.

Component	Description
Policy Management Framework	The PSBN policy management architecture, as described in Section 10.2.2 is a de-centralized framework. The policies are entered via a policy console and stored in a policy repository. The Policy Decision Point (PDP) server executes the policy and communicates the rules associated with a policy to a Policy Enforcement Point. An example of this system is the 3GPP Policy and Charging Control function that is described in TS 23.203 [21].
Application Lifecycle Management	Applications life cycle consists of all the stages in the usable life of an application – from the creation, on-boarding, through maintenance and support, to its retirement. The life cycle process is managed under various regimes that are administered by the owner of the application and the hosting service. The process includes various metrics and revenue sharing aspects. The application life cycle and its management are outside the scope of this Scientific Report.
Mobile AppStore	The PSBN may offer a public safety grade set of applications that can be used on a variety of mobile device form factors and with MTC devices. The application store (AppStore) would host software development tools for application developers that facilitate the certification and on-boarding processes of new applications. PSBN users would be able to browse this AppStore, and download and execute applications.
OSS, BSS, trusted and un-trusted Applications	Each of these types of applications would register, be authorized and connect to the Enterprise Service Bus, thus making their respective functions available to other systems, services and applications that are connected to the ESB. In the case of un-trusted applications, they would connect with an ESB gateway function that performs additional security operations.
EPS network element capabilities	In 3GPP TS 23.682 [35], enhancements to the EPS are described as a series of new reference points. Through these reference points, a network element would expose its capability through the SCEF. It is the intention of 3GPP to define more EPS network capabilities in the future and have those capabilities exposed through the SCEF and corresponding Common API Framework.

10.2 Policy management for a PSBN

As stated in the previous section, policy[15] management is an important consideration in the overall architecture of a mobile service offering. This section provides a further description on policy management for a PSBN.

[15] Policies are formalisms that are used to express business, engineering or process criteria represented by a combination of policy conditions and actions.

10.2.1 Policy management reference model

The International Telecommunications Union (ITU) has defined a reference model for policy management. The ITU X.1205 recommendation [92] specifies a three-layered approach, which is illustrated in Figure 40. This three-layered approach uses a policy repository component, policy server as the Policy Decision Point (PDP) component and the Policy Enforcement Point (PEP) function that is implemented by network devices. In addition to the functional elements, the figure also shows the protocols that can be used to support the communications between them. Lightweight Directory Access Protocol (LDAP), Common Open Policy Service (COPS), Simple Network Management Protocol (SNMP), and Command Line Interface (CLI) are examples of protocols that can be used. LDAP, specified in IETF RFC 3337 [93] is a client-server protocol for accessing a directory service. COPS is a simple query and response stateful TCP-based protocol that can be used to exchange policy information between a PDP and its clients' PEPs. It is specified in the Internet Engineering Task Force IETF RFC 2748 [94]. SNMP is a set of protocols that are used for network management and monitoring. It is specified by the IETF RFC 3410 [95]. CLI is intended for direct control of network elements and is normally specific to a network element or family of network elements sourced from the same vendor.

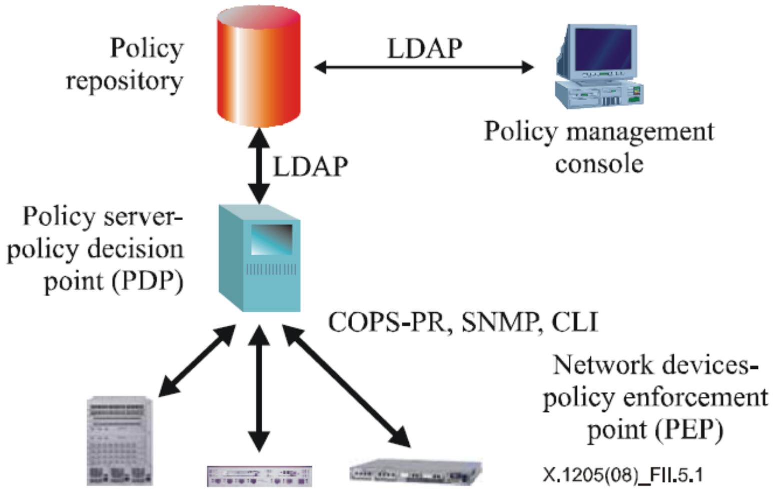

Policy repository
LDAP
Policy management console
LDAP
Policy server-policy decision point (PDP)
COPS-PR, SNMP, CLI
Network devices-policy enforcement point (PEP)
X.1205(08)_FII.5.1

Figure 40: *Policy management reference model (source: ITU X.1205 [92]).*

Components of the reference model are described in Table 39.

Table 39: *ITU reference model component.*

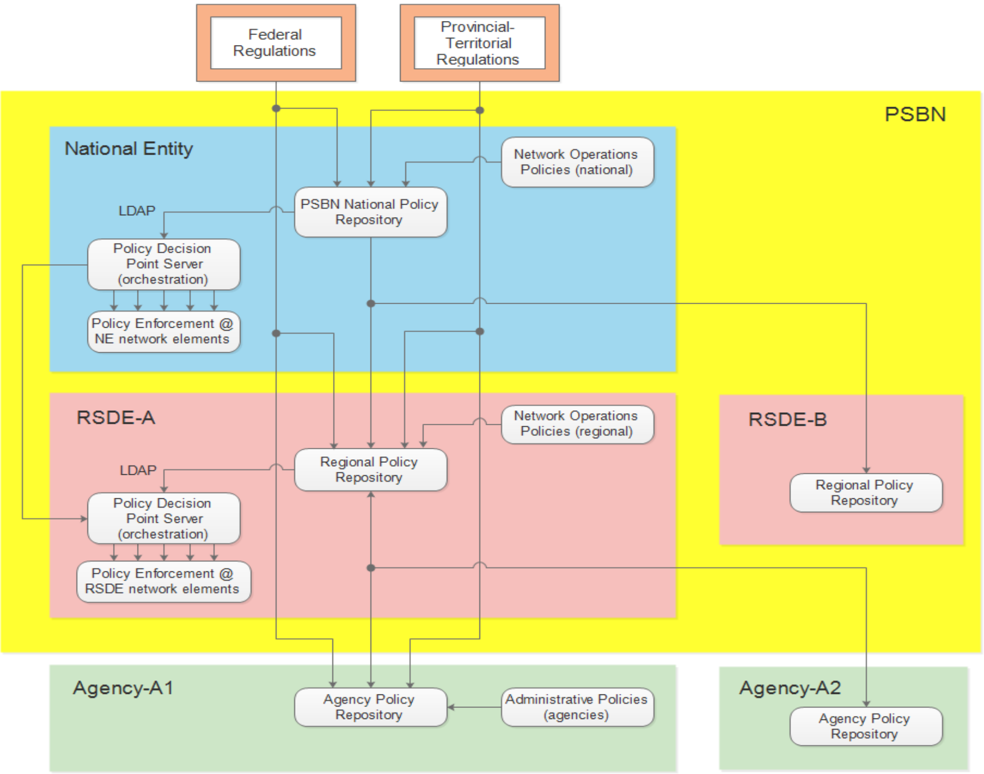
Component	Description
Policy Repository	The network directory is the repository for all policy information. It describes network users, applications, computers, and services (i.e., objects and attributes), and the relationships between these entities. There is a tight integration between the IP address and the end user, via the Dynamic Host Control Protocol (DHCP) and a Domain Name System (DNS). A directory is usually implemented on a special-purpose database machine. The policy repository is used to store relatively static information about the network (e.g., device configurations), whereas policy servers store more dynamic network state information (e.g., bandwidth allocation, information about established connections). The policy server retrieves policy information from the directory and deploys it to the appropriate network elements. There is no established standard to describe the structure of the directory database, i.e., how network objects and their attributes are defined and represented. A common directory *schema* is needed if multiple vendor applications are to share the same directory information; for example, all vendors need a common way to interpret and store configuration information about routers.
Policy Management Console	Human beings interact with the policy management system through a management console, generally running on a personal computer or workstation. Alternatively, a web browser can be used to provide management access from virtually anywhere, with policy object-level security used to limit which policies can be modified by a specific individual. It is through the management console that policies get instantiated in the directory. The console provides a graphical user interface and the tools needed for managers to define network policies as business rules. It may also give the operator access to lower-level security configurations in individual switches and routers.
Policy Decision Point	PDPs or policy servers abstract network policies into specific device control messages that are then passed to policy enforcement points. These policy servers are often stand-alone systems controlling all of the switches and routers within a particular administrative domain. The PDP communicates with the policy enforcement point network devices using a control protocol (e.g., COPS, SNMP set commands, telnet or the device’s specific command line interface (CLI)).

Component	Description
Policy Enforcement Point	A network or security device that accepts a policy (configuration rules) from the policy decision point and enforces that policy against the network traffic traversing that device. This enforcement leverages network and network-assisted security mechanisms as appropriate.

The elements of the policy management reference model interoperate to deliver closed loop policy management. This includes the configuration of edge devices, enforcement of policies in the network and verification of network functionality as seen by the end-user application. Enforcement of policies in the network includes admission controls of applications or users vying for access to network resources. Policy management can contribute to simplifying the configuration management environment inside enterprises, thereby minimizing opportunities for human error.

10.2.2 Policy management framework for the PSBN

While the previous section described a policy management reference model, this section applies the reference model to the PSBN. Figure 41 illustrates a possible policy management framework for the PSBN.



Federal Regulations
Provincial-Territorial Regulations
PSBN
National Entity
Network Operations Policies (national)
LDAP
PSBN National Policy Repository
Policy Decision Point Server (orchestration)
Policy Enforcement @ NE network elements
RSDE-A
Network Operations Policies (regional)
LDAP
Regional Policy Repository
Policy Decision Point Server (orchestration)
Policy Enforcement @ RSDE network elements
RSDE-B
Regional Policy Repository
Agency-A1
Agency Policy Repository
Administrative Policies (agencies)
Agency-A2
Agency Policy Repository

Figure 41: *Possible policy management framework for PSBN.*

10.2.2.1 National entity role in the policy management framework

The following list describes the roles of a national entity in a PSBN policy management framework.

- National level PSBN policies are based on federal, provincial and territorial (F/P/T) regulations and NE level operational policies.
- The NE Policy Decision Point (PDP) server orchestrates the settings and configurations for the network element Policy Enforcement Points (PEP) in the NE portion of the PSBN.
- The NE PDP does **not** communicate directly with the network elements at the RSDE level.
- The NE PDP communicates with the RSDE PDP server in cases where a policy enforcement action involves the network elements in both the NE and RSDEs.

10.2.2.2 RSDE role in the policy management framework

The following list describes the roles of a national entity in a PSBN policy management framework.

- Regional level policies are based on F/P/T regulations, national level policies, and are adapted to RSDE specific network operations policies.
- The RSDE PDP server orchestrates the settings and configurations for the network elements in the RSDE portion of the PSBN.
- There is no direct RSDE-RSDE orchestration.

10.2.2.3 Agency role in the policy management framework

- Agency level policies are based on F/P/T regulations, national and regional level policies, and are adapted to agency-specific administrative policies.[16]
- Agency level polices may affect the regional portion of the PSBN for those service aspects that are delegated to the agencies under "Local Control."[17]

10.2.3 Policy management using Open Mobile Alliance (OMA) policy evaluation, enforcement and management

Open Mobile Alliance's (OMA) Policy Evaluation, Enforcement and Management (PEEM) specifies ways to convey and enforce policies that can be used to manage resources, processes, and underlying systems. Relevant references are:

- Policy Evaluation, Enforcement and Management **Architecture** Approved Version 1.0 – 24 Jul 2012 [96].
- Policy Evaluation, Enforcement and Management **Requirements** Approved Version 1.0 – 24 Jul 2012 [97].

[16] Agencies don't operate any portion of the PSBN. But, they exercise administrative authority over user devices and BBDS.

[17] "Local Control" may grant Agencies the ability to adjust some configurations of the PSBN for those service aspects that are delegated to it. An example may be where the Incident Command staff (COM-L) can modify the QPP settings dynamically.

10.2.3.1 PEEM architecture

PEEM may be considered an implementation of the IETF PDP/PEP model. Figure 42 below illustrates the functions of the PEEM architecture and the corresponding Table 40 lists and describes the components of the architecture figure.

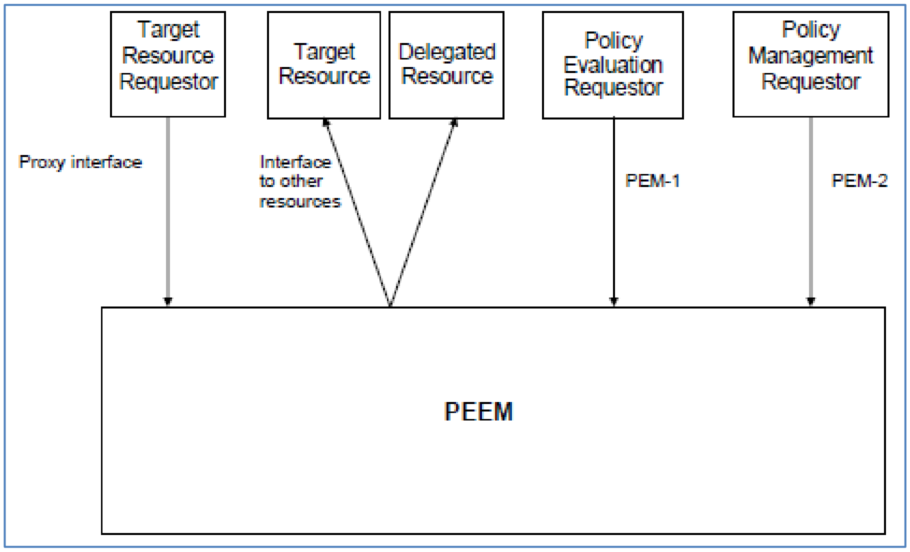

Target Resource Requestor
Target Resource
Delegated Resource
Policy Evaluation Requestor
Policy Management Requestor
Proxy interface
Interface to other resources
PEM-1
PEM-2
PEEM

Figure 42: *Policy evaluation, enforcement and management architecture (source: Open Mobile Alliance [96]).*

Table 40: *PEEM architecture logical components (source: OMA PEEM Architecture Description).*

Component	Description
Target Resource Requestor	Target Resource Requestor represents a resource (e.g., application, enabler) that issues a request to a target resource.
Target Resource	Target Resource represents the destination resource for a request made by another resource.
Delegated Resource	Delegated Resource represents the resource to which PEEM may delegate certain policy actions during the policy processing process.
Policy Evaluation Requestor	Evaluation Requestor represents a resource (e.g., application, enabler) that issues a request for policy processing to PEEM.
Policy Management Requestor	Management Requestor represents a resource (e.g., application, enabler) that issues a request for policy management to PEEM.

10.2.3.2 PEEM uses in the PSBN

Figure 43 illustrates how PEEM architecture supports the callable mode of using PEEM. The use case that is illustrated in the figure is between two PSBN users that are using the Short Message Service system. In the diagram the steps 2, 3 and 4 are the PEEM callable operations that illustrate the actions that can be made to PEEM architecture.

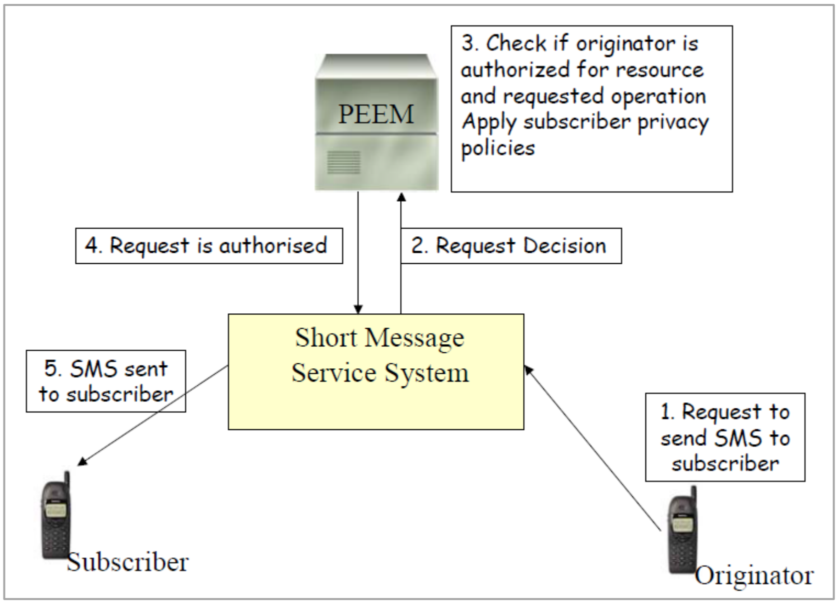

PEEM
3. Check if originator is authorized for resource and requested operation Apply subscriber privacy policies
4. Request is authorised
2. Request Decision
Short Message Service System
5. SMS sent to subscriber
1. Request to send SMS to subscriber
Subscriber
Originator

Figure 43: *Use case—policy evaluation and enforcement for short message service request (source: Open Mobile Alliance [97]).*

10.3 Business Support System (BSS)

A Business Support System (BSS) is used by mobile network operators to run their business operations towards customers. Both BSS and OSS are used to support end-to-end services, with the BSS being customer facing and the OSS being network facing. Typical responsibilities of a BSS include order taking, payment, business revenues, and applications. This section excerpts information from the Telecommunications Management (TM) Forum's program called Frameworx [76]. While not unique, Frameworx is one approach for the implementation of a BSS that has significant adoption in industry [98] and may be considered by PSBN operators. Other such BSSs exist that may also be considered for this purpose.

The industry is migrating towards platform architectures, where the support and management functions are provided by platform support services (such as the previously described SDP), rather than discrete applications. The trend amongst telecommunication service providers has been to integrate using APIs based on REST.[18] The Integration Framework has thus been expanded to include the suite of TM Forum REST APIs. This suite of APIs covers both the needs of integration between digital service providers, following the TM Forum Digital Services Reference Architecture, and the internal interfaces needed to create a complete end to end management system for a hybrid virtual and physical infrastructure using an automated, catalog-driven approach.

[18] A RESTful API—also referred to as a RESTful web service—is based on Representational State Transfer (REST) technology, an architectural style and approach to communications often used in web services development.

Table 41: *TMF Frameworx standards for operating a telecommunications business.*

Component	Name	Description
Best Practices	Frameworx	TM Forum Frameworx is a suite of best practices and standards that provides the blueprint for effective, efficient business operations. It enables an operator to assess and optimize performance using a service-oriented approach to operations and integration. The tools available in Frameworx help improve end-to-end management of services across complex, multi-partner environments. All of Frameworx, including the architecture best practices, Business Process Framework, the Information Framework, the Application Framework and Integration Framework are created and evolved by members of the TM Forum collaboration community.
SOA-based guidance	Architecture	Some of the most important parts of Frameworx are its guidelines for architecture that can be applied to building integrated management solutions. Frameworx architecture guides provide direction on how operational processes can be automated by utilizing standardized information definitions from the Information Framework to define standardized, reusable Service Oriented Architecture (SOA)-based Business Services.
Business Process Framework	enhanced Telecommunications Operations Map (eTOM)	The Business Process Framework called eTOM is a critical component of Framework. It is a comprehensive, industry-agreed, multi-layered view of the key BSS and OSS processes.
Logical Groupings of Applications	The Application Framework (TAM)	The Application Framework (TAM) provides a systems map which captures how business capabilities are implemented in deployable, recognizable applications. TAM provides a common language for communities who specify, procure, design, and sell systems, so that they can understand each other's viewpoints. It provides logical groupings of applications, then describes each application's functionality.
Information Framework	Shared Information Data model (SID)	The Shared Information Framework (SID) is a component of Frameworx. It provides standard definitions for all the information that flows through the enterprise and between service providers and their business partners.
Enterprise Service Bus	Integration Framework	The Integration Framework provides a set of standards to integrate existing legacy end-to-end management applications

Component	Name	Description
		as well as the platform for future services. Traditionally the integration framework contains a set of standards that support the integration and interoperability between applications defined in the Applications Framework. These standards are in current use in the telecoms industry. As well as the APIs, the framework contains other assets to support the creation of Orchestration Reference architectures and implementation guides.

10.3.1 Charging service

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

10.3.1.1 Offline and online charging

The 3GPP TS 32.240 [99] specifies the charging architecture and identifies two types of charging mechanisms that may be used simultaneously and independently for the same chargeable event; offline and online charging.

Offline charging is a process where charging information for network resource usage is collected concurrently with that resource usage, but which does not affect, in real-time, the service rendered. The charging information is then passed through a chain of logical charging functions which results in the creation of Charging Data Record (CDR) files that are then transferred to the network operator's billing domain for the purpose of subscriber billing or inter-operator accounting.

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

10.3.1.2 Event and session based charging

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

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

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

10.3.1.3 Charging support for roaming

The 3GPP TS 32.240 provides information on inter-PLMN accounting for roaming traffic, which would be required for scenarios where users (e.g., first responder users) roam between the PSBN and non-partner commercial cellular networks or FirstNet. The CDRs collected from the network also include details of the services employed by visiting and inbound roaming subscribers. The charges for Mobile Originated Calls (MOCs) and for supplementary services used are calculated as for home subscribers, converted to an agreed accounting currency and included in the CDRs which are exchanged with the commercial operator or FirstNet. For data sessions using home routing when roaming, PSBN-hosted charging systems can apply both online and offline charging. In roaming mode, it is important to distinguish between end-user charges and inter-operator charges.

10.4 QoS, priority and pre-emption policy management

3GPP TS 23.203 [21] defines the Policy and Charging Control (PCC) architecture that forms the basis for PSBN policy management for Quality of Service (QoS). In 2015, NPSTC produced a report that describes the Priority and QoS (PQOS) requirements for public safety agencies [100]. This National Public Safety Telecommunications Council (NPSTC) report describes a QoS, Priority, and Pre-emption (QPP) management system. The NPSTC report and the 3GPP PCC architecture can serve as a benchmark for how PSBN can specify its own PSBN QPP Policy Management Framework.

There are many facets to network planning. While most of these are not within the scope of this Scientific Report, radio access network planning is described in the following sections as it pertains to a PSBN architecture with the possibility for multiple operational entities.

10.4.1 Planning for MOCN between RSDE partner MNO and commercial MNO

In 3GPP TS 32.130 [55], Multiple Operator Core Network sharing has implications on the operations of the network. During network planning, the RSDE MNO and the partner commercial MNO need to coordinate several aspects of deploying MOCN based spectrum sharing. The following are examples of coordination aspects: alignment on operational priorities, congestion control, common network planning / evolution strategy, sharing end user data / subscription data and sharing performance data, alarms etc. Each needs to be considered carefully in the shared network. Privacy, security and competitive information are also important for the operations of the network elements that are shared.

10.4.2 Real-time cell coverage

The PSBN is expected to provide wireless coverage to a significant part of Canada. Planning for real-time cell coverage is a complex planning effort that involves using sophisticated coverage analysis tools, high resolution Geographic Information System (GIS) data sets and capacity planning and analysis tools.

Network planners need to make sure that the network is working as per the operator's standards and serving the users optimally, and as such, MNOs periodically perform drive tests. These tests are carried out to validate initial coverage predictions, to optimize the network, and when required, to debug certain issues in a particular areas. Periodic drive tests can be very costly to the network operator and consume valuable operational resources. To minimize these costs, 3GPP standardization groups have proposed new techniques to minimize the amount of drive tests by collecting information from mobile users. The types of information collected can be on signal strength, signal to noise+interference ratios, receiver noise floors, handover details, or signalling failures to name a few. The ability to gather this information effectively reduces the need to carry out periodic drive tests.

To help with measuring the RF characteristics in various locations throughout a RAN coverage area, a function called Minimization of Drive Testing (MDT) has been specified in 3GPP TS 37.320 [101], "Radio measurement collection for MDTs; Overall description." MDT solutions consist of the client/server applications and a graphic user interface (GUI) application overlaid on topographical maps that show the RF coverage. For network planners, they need a way to troubleshoot RF problems in real-time or analyze logged RF coverage data for troubleshooting purposes. When real-time data is not available, recorded data needs to be made available.

There are two different types of MDT; a) in immediate MDT, the mobile device performs measurements in "CONNECTED" state and reports the measurements to the LTE eNodeB; b) logged MDT is performed when the mobile device is in idle mode, where the measurements are time stamped and can include location information.

11 Conclusion

The public safety broadband network in Canada is a transformational initiative that will change the way first responders and other public safety stakeholders conduct day-to-day operations and respond to major incidents. Such a network will allow the public safety community to make use of sophisticated feature-rich broadband applications that will dramatically enhance its ability to communicate and access information at all times. In order to have the most impact nationwide, some of the key tenets of a PSBN are interoperability, availability anywhere at any time, affordability and sustainability. It is these driving principles, along with many other considerations, that have served as the foundation on this Scientific Report on a network architecture description for a PSBN.

The objective of this Scientific Report is not to be prescriptive about the required architecture of a PSBN in Canada, but rather to serve as a possible input to whoever is ultimately responsible for the establishment of a PSBN. The information contained herein can be considered in whole, in part, or not at all when planning the implementation of the PSBN.

This Scientific Report presented three possible single network architectures for a nationwide PSBN, although other architectures certainly could be considered. Of the three, one is more elaborate in structure that the other two, and as such was the main focus of the Report. If however, one of the other two are to be considered, or any other architecture that may be considered for that matter, it is opinion of the authors that portions of this report would still be relevant and of value. As an example, in an architecture where there is no regional service delivery entity (RSDE), the functions attributed to the RSDE could be subsumed by a national operator, or may not even be required.

In producing the network architecture description of a PSBN, it was important to make certain assumptions on what actually constitutes a PSBN. As indicated in Section 2, the PSBN is part of a much broader public safety communications ecosystem, albeit a key part. For the purposes of this Scientific Report, it was assumed that the PSBN is made up of the functions in the yellow part of Figure 1. The PSBN will interface with several external networks, systems, applications and services found in the blue outer area, and this Scientific Report describes, at a high level, how the PSBN could interface with many of these external components from a technical perspective.

Section 3 of this Scientific Report listed PSBN architecture technical assumptions, definitions and service delivery model considerations. Section 4 described three possible architectures for the PSBN. Sections 5 through 10 provided additional detail on each component of the PSBN within the yellow box in Figure 1. References, Annex A and the List of Acronyms follow this conclusion.

It is expected that the technical considerations on PSBN architecture will evolve over time and as such, this document is a snapshot in time of the needs of the public safety community as they are known today.

References

[1] Public Safety Canada, “Communications Interoperability Strategy for Canada,” January 2011. Web. <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/index-en.aspx>, [accessed 14 April 2018].

[2] “Public Safety Broadband Network Architecture Description”, Defence R&D Canada – Centre for Security Science, Technical Report, DRDC CSS TR 2013-009, August 2013.

[3] “Public Safety Broadband Network, Technical Considerations on Interoperability,” Defence Research and Development Canada, Scientific Report, DRDC-RDDC-2018-xxxx, 2019.

[4] “Public Safety Broadband Network, Technical Considerations on Operability,” Defence Research and Development Canada, Scientific Report, DRDC-RDDC-2018-xxxx, 2019.

[5] “Public Safety Broadband Network, Technical Considerations on Security,” Defence Research and Development Canada, Scientific Report, DRDC-RDDC-2018-xxxx, 2019.

[6] “Implications of Service Delivery Model Options on Interoperability and Operational Efficiency in a Public Safety Mobile Broadband Network,” Defence Research and Development Canada, Scientific Report, DRDC-RDDC-2017-R038, March 2017.

[7] “Public Safety Broadband Network, Use-Cases and User Requirements,” Defence Research and Development Canada, Scientific Report, DRDC-RDDC-2018-xxxx, 2019.

[8] National Public Safety Telecommunications Council, “Public Safety Entity Control and Monitoring Requirements for the Nationwide Public Safety Broadband Network,” Final Report, October 2015. Web. <http://www.npstc.org/download.jsp?tableId=37&column=217&id=3556&file=NPSTC_Local_Control_Report_Final_20151010.pdf>, [accessed 13 April 2018].

[9] Communications Security Establishment Canada, “Technology Supply Chain Guidelines – Contracting Clauses for Telecommunications Equipment and Services,” TSCG-01\G, October 2010. Web. <https://www.cse-cst.gc.ca/en/page/technology-supply-chain-guidance>, [accessed 13 April 2018].

[10] Canadian Radio-television and Telecommunications Commission, “Implementation of the National Public Alerting System by wireless service providers to protect Canadians,” Telecom Regulatory Policy CRTC 2017-91. 06 April 2017. Web. <http://crtc.gc.ca/eng/archive/2017/2017-91.htm>, [accessed 13 April 2018].

[11] National Emergency Numbering Association (NENA), “Detailed Functional and Interface Standards for the NENA i3 Solution”, NENA-STA-010.2-2016, 2016. Web. <https://www.nena.org/?page=i3_stage3>, [accessed 13 April 2018].

[12] “Public Safety Broadband Network—Integrated Dictionary of Terms,” Defence Research and Development Canada, in progress.

[13] 3GPP TR 21.905, "Vocabulary for 3GPP Specifications," v15.0.0, April 2018.

[14] ANSI IEEE Std 100-1984, "IEEE Standards Dictionary of Electrical and Electronic Terms," 1984.

[15] International Electrotechnical Commission, "Electricity, Electronics and Telecommunications," Elsevier, 1992.

[16] GSMA IR.34: "Guidelines for IPX Providers," v13.0, October 2016.

[17] 3GPP TS 23.335, "User Data Convergence (UDC); Technical realization and information flows; Stage 2," v14.0.0, March 2017.

[18] 3GPP TS 23.002, "Network Architecture," v14.1.0, March 2017.

[19] 3GPP TS 23.401, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access," v15.2.0, December 2017.

[20] 3GPP 29.336, "Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications," v15.1.0, December 2017.

[21] 3GPP TS 23.203, "Policy and charging control architecture," v15.1.0, December 2017.

[22] 3GPP TS 22.101, "Service Aspects and Principles," v15.3.0, January 2018.

[23] 3GPP TR 22.985, "Service requirements for the User Data Convergence (UDC)," v14.0.0, March 2017.

[24] 3GPP TS 23.280, "Common functional architecture to support mission critical services," v15.2.0, January 2018.

[25] 3GPP TS 36.300, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2," v15.0.0, January 2018.

[26] Industry Science and Economic Development Canada, "Decisions on Policy, Technical and Licensing Framework for Use of the Public Safety Broadband Spectrum in the Bands 758–763 MHz and 788–793 MHz (D Block) and 763–768 MHz and 793–798 MHz (PSBB Block)," SMSE-014-17, June 2017.

[27] 3GPP TS 22.220, "Service requirements for Home Node B (HNB) and Home eNode B (HeNB)," v14.0.0, March 2017.

[28] National Public Safety Telecommunications Council, "Broadband Deployable Systems in the NPSBN—A Report from the National Public Safety Telecommunications Council and the Defence Research and Development Canada's Centre for Security Science," April 2017. Web. <http://npstc.org/download.jsp?tableId=37&column=217&id=3903&file=NPSTC_CSS_BB_Deployable_Systems_Report_Final_170403.pdf>, [accessed 14 April 2018].

[29] 3GPP TS 23.251, "Network Sharing; Architecture and functional description," v14.1.0, September 2017.

[30] Wi-Fi Alliance, “Hotspot 2.0 (Release 2) Technical Specification,” Version 1.2, 08 December 2016.

[31] 3GPP TS 33.402, “3GPP System Architecture Evolution (SAE); Security aspects on non-3GPP accesses,” v14.3.0, September 2017.

[32] 3GPP TS 23.402, “Architecture enhancements for non-3GPP accesses,” v15.2.0, December 2017.

[33] 3GPP TS 23.139, “3GPP system - fixed broadband access network interworking; Stage 2,” v14.0.0, March 2017.

[34] 3GPP TS 22.368, “Service Requirements for Machine Type Communications (MTC); Stage 1,” v14.0.1, August 2017.

[35] 3GPP TS 23.682, “Architecture enhancements to facilitate communications with packet data networks and applications,” v15.3.0, December 2017.

[36] 3GPP TS 29.368, “Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS),” v14.3.0, December 2017.

[37] GSM Association IR.88, “LTE Roaming Guidelines,” V.09, Jan. 24, 2013.

[38] 3GPP TS 23.228, “IP Multimedia Subsystem (IMS); Stage 2,” v15.1.0, December 2017.

[39] GSMA IR.65, “IMS Roaming guidelines,” v22.0, 11 October 2016.

[40] GSMA IR.61, “WLAN Roaming guidelines,” v12.0, 28 September 2017.

[41] 3GPP TS 23.161, “Network-Based IP Flow Mobility (NBIFOM); Stage 2,” v14.0.0, March 2017.

[42] 3GPP TS 23.261, “IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2,” v14.0.0, March 2017.

[43] 3GPP TS 23.327, “Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems,” v13.1.0, September 2016.

[44] 3GPP TS 23.271, “Location based services,” v14.3.0, December 2017.

[45] 3GPP TS 23.167, “IP Multimedia Subsystem (IMS) emergency sessions,” v15.0.0, December 2017.

[46] Wikipedia contributors, “Codec,” Wikipedia, The Free Encyclopedia, 16 November 2018, 22:15 UTC. Web. <https://en.wikipedia.org/w/index.php?title=Codec&oldid=869177118> [accessed 14 December 2018].

[47] Wikipedia contributors, “Adaptive Multi-Rate audio codec,” Wikipedia, The Free Encyclopedia, 2 October 2018, 10:09 UTC. Web. <https://en.wikipedia.org/w/index.php?title=Adaptive_Multi-Rate_audio_codec&oldid=862125304>, [accessed 14 December 2018].

[48] Wikipedia contributors, “G.711,” Wikipedia, The Free Encyclopedia, 24 June 2018, 06:49 UTC. Web. <https://en.wikipedia.org/w/index.php?title=G.711&oldid=847286439>, [accessed 14 December 2018].

[49] 3GPP TS 23.204, “Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access; Stage 2,” v14.0.0, March 2017.

[50] Wikipedia contributors, “H.248,” Wikipedia, The Free Encyclopedia, 12 May 2018, 01:33 UTC. Web. <https://en.wikipedia.org/w/index.php?title=H.248&oldid=840768550>, [accessed 14 December 2018].

[51] 3GPP TS 29.165, “Inter-IMS Network-Network Interface,” v15.2.0, December 2017.

[52] 3GPP TS 24.229, “IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3,” v15.1.0, December 2017.

[53] CRTC Interconnection Steering Committee (CISC) – Network Working Group (NTWG), “Canadian Wireless Public Alerting Service (WPAS) C-Interface Specification,” V1.3, October 2016. Web. <https://crtc.gc.ca/public/cisc/nt/NTCO0648.pdf>, [accessed 11 April 2018].

[54] 3GPP TS 33.107, “Lawful interception architecture and functions,” v15.0.0, January 2018.

[55] 3GPP TS 32.130, “Network Sharing; Concepts and Requirements,” v14.1.0, January 2018.

[56] 3GPP TS 23.303, “Proximity-based services (ProSe),” v15.0.0, June 2017.

[57] Y.Lair, G.Mayer, 3GPP, “Mission Critical Services in 3GPP”, 20 June 2017. Web. <http://www.3gpp.org/news-events/3gpp-news/1875-mc_services>, [accessed 15 April 2018].

[58] 3GPP TS 23.468, “Group Communication System Enablers for LTE (GCSE_LTE); Stage 2,” v15.0.0, December 2017.

[59] 3GPP TS 23.237, “IP Multimedia Subsystem Service Continuity,” v15.1.0, December 2017.

[60] 3GPP TS 23.379: “Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT),” v15.2.0, January 2018.

[61] 3GPP TS 23.281: “Functional architecture and information flows to support Mission Critical Video (MCVideo),” v15.2.0, January 2018.

[62] 3GPP TS 23.282: “Functional architecture and information flows to support Mission Critical Data (MCData),” v15.2.0, January 2018.

[63] 3GPP TS 22.179: “Mission Critical Push To Talk (MCPTT) over LTE; Stage 1,” v15.2.0, January 2018.

[64] 3GPP TS 23.283, “Mission Critical Communication Interworking with Land Mobile Radio Systems,” v15.0.0, April 2018.

[65] 3GPP TS 22.281, “Mission Critical Video services over LTE,” v15.0.0, June 2017.

[66] 3GPP TS 22.282, “MCData over LTE requirements,” v15.0.0, January 2018.

[67] National Public Safety Telecommunications Council, “Public Safety Land Mobile Radio (LMR) Interoperability with LTE Mission Critical Push to Talk,” Final Report, 08 January 2018. Web. <http://www.npstc.org/download.jsp?tableId=37&column=217&id=4031&file=NPSTC_Public_Safety_LMR_LTE_IO_Report_20180108.pdf>, [accessed 15 April 2018].

[68] 3GPP TS 22.246, “Multimedia Broadcast/Multicast Service (MBMS) user services,” v14.0.0, March 2017.

[69] 3GPP TS 23.246, “Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description,” v15.0.0, December 2017.

[70] Internet Engineering Task Force, RFC 7296, “Internet Key Exchange Protocol Version 2 (IKEv2),” October 2014.

[71] Internet Engineering Task Force, RFC 4945, “The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX,” August 2007.

[72] 3GPP TS 23.234, “3GPP system to Wireless Local Area Network (WLAN) interworking: System description,” v13.1.0, March 2017.

[73] 4G Americas, “Integration of WiFi and Cellular Networks,” September 2013. Web. <http://www.2www.5gamericas.org/files/4414/0759/1568/Integration_of_Cellular_and_WiFi_Networks_White_Paper-_9.25.13.pdf>, [accessed 15 April 2018].

[74] 3GPP TS 32.101, “Telecommunications Management Network; Principles and high-level requirements,” v15.0.0, September 2017.

[75] 3GPP TS 32.102, “Telecommunications Management Network; Architecture,” v14.0.0, April 2017.

[76] Telecommunications Management Forum (TM Forum): “Framworx description,” Web. <https://www.tmforum.org/tm-forum-frameworx/>, [accessed 15 April 2018].

[77] Telecommunications Management Forum (TM Forum), “TMF070 Implementation and Deployment Blueprints for Hybrid Environments R17.0.1 Standard,” September 2017. Web. <https://www.tmforum.org/resources/specification/tmf070-implementation-and-deployment-blueprints-for-hybrid-environments-r17-0-1/>, [accessed 15 April 2018].

[78] Open Mobile Alliance (OMA), “OMA Device Management (DM) Management Object (MO) Registry.” Web. <http://www.openmobilealliance.org/wp/OMNA/dm/dm_mo_registry.html>, [accessed 05 January 2019].

[79] 3GPP TS 32.690, “Telecommunication management; Inventory Management (IM); Requirements,” v14.0.0, April 2017.

[80] 3GPP TS 32.692, “Telecommunication management; Inventory Management (IM) network resources Integration Reference Point (IRP); Network Resource Model (NRM),” v11.0.0, September 2012.

[81] 3GPP TS 32.600, “Telecommunication management; Configuration Management (CM); Concept and high-level requirements,” v14.0.0, April 2017.

[82] Telecommunication Management Forum, “TMF661 Trouble Ticket API Conformance Profile R16.5.1 Standard,” April 2017. Web. <http://www.tmforum.org/resources/specification/tmf661-trouble-ticket-api-conformance-profile-r16-5-1/>, [accessed 15 April 2018].

[83] 3GPP TS 32.522, “Self-Organizing Networks (SON) Policy Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS) (Release 11),” September 2013.

[84] 3GPP TS 32.500, “Telecommunication Management; Self-Organizing Networks (SON); Concepts and requirements,” v14.0.0, April 2017.

[85] 3GPP TS 32.521, “Telecommunication management; Self-Organizing Networks (SON) Policy Network Resource Model (NRM) Integration Reference Point (IRP); Requirements,” v11.1.0, December 2012.

[86] 3GPP TS 32.526, “Telecommunication management; Self-Organizing Networks (SON); Policy Network Resource Model (NRM) Integration Reference Point (IRP); Solution Set (SS) definitions,” v11.7.0, December 2013.

[87] 3GPP TS 32.511, “Telecommunication management; Automatic Neighbour Relation (ANR) management; Concepts and requirements,” v14.1.0, January 2018.

[88] Next Generation Mobile Network (NGMN), “Recommended Practices for Multi-Vendor SON Deployment,” 29 sept 2015. Web. <http://www.ngmn.org/fileadmin/user_upload/140930_NGMN_P-SmallCells_Multivendor_IOT_D4_v1_3.pdf>, [accessed 16 April 2018].

[89] Torry Harris Integration Solutions, Whitepaper, “SOA for Telecom,” 07 Sept 2016. Web. <https://www.thbs.com/thbs-insights/soa-for-telecom>, [accessed 16 April 2018].

[90] 3GPP TR 23.722, “Study on Common API Framework for 3GPP Northbound APIs,” v15.0.0, January 2018.

[91] 3GPP TS 23.222, “Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2,” v15.0.0, January 2018.

[92] ITU X.1205, “Overview of Cybersecurity,” 2008. Web. <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=en>, [accessed 16 April 2018].

[93] IETF RFC 3337: “Class Extensions for PPP over Asynchronous Transfer Mode Adaptation Layer 2 (AAL2),” December 2002.

[94] IETF RFC 2748: “The COPS (Common Open Service Policy) Protocol,” January 2000.

[95] IETF RFC 3410: “Introduction and Applicability Statements for Internet Standard Management Framework,” December 2002.

[96] Open Mobile Alliance, “Policy Evaluation, Enforcement and Management Architecture,” Approved Version 1.0, OMA-AD-Policy_Evaluation_Enforcement_Management-V1_0- 20120724-A, 24 Jul 2012. Web. <http://www.openmobilealliance.org/release/PEEM/V1_0-20120724-A/OMA-AD-Policy_Evaluation_Enforcement_Management-V1_0-20120724-A.pdf>, [accessed 25 June 2018].

[97] Open Mobile Alliance, “Policy Evaluation, Enforcement and Management Requirements,” Approved Version 1.0, OMA-RD-Policy_Evaluation_Enforcement_Management-V1_0- 20120724-A, 24 Jul 2012. Web. <http://www.openmobilealliance.org/release/PEEM/V1_0-20120724-A/OMA-RD-Policy_Evaluation_Enforcement_Management-V1_0-20120724-A.pdf>, [accessed 25 June 2018].

[98] TM Forum, “Framworx Adoption,” March 2015. Web. <https://www.tmforum.org/tm-forum-frameworx-2/adoption>, [accessed 16 April 2018].

[99] 3GPP TS 32.240, “Telecommunication management; Charging management; Charging architecture and principles,” v15.0.0, January 2018.

[100] National Public Safety Telecommunications Council, “Priority and Quality of Service in the Nationwide Public Safety Broadband Network, rev.1.4, August 2015. Web. <http://www.npstc.org/download.jsp?tableId=37&column=217&id=3515&file=PQoS15_003_PQoS_Definition_v1_4_20150817_GB_APPROVED.pdf>, [accessed 16 April 2018].

[101] 3GPP TS 37.320, “Radio measurement collection for Minimization of Drive Tests (MDT),” v14.0.0, March 2017.

Annex A 3GPP industry standards overview

The 3GPP has published an extensive set of specifications for LTE that have been developed by various committees and work groups. The 3GPP specifications development groups are organized as shown in Figure A.1. Each Technical Specification Group (TSG) has a specific scope for the System Architecture (SA), RAN, and Core Network and Terminals (CT). 3GPP follows a standards development process which involves specifying service aspects and requirements as Stage 1, specifying logical architecture as Stage 2 and specifying protocol implementation in Stage 3. Each stage in the process delivers technical studies or technical specifications, some of which have been referenced in this Scientific Report.

The LTE specifications continue to evolve as new features and capabilities are scheduled for future releases. There are currently more than 1,000 specifications across all the work groups that pertain to LTE Rel.14. This Scientific Report does not list the entire set of specifications, but only a sub-set, i.e., those specifications that are deemed most impacting on interoperability of the PSBN. From a practical perspective, manufacturers will implement the specifications that they anticipate will result in economically viable products. Therefore, it is unlikely that all the LTE specifications will be implemented. Furthermore, as stated earlier, compliance to standards and specifications does not, per se, ensure multi-vendor interoperability.

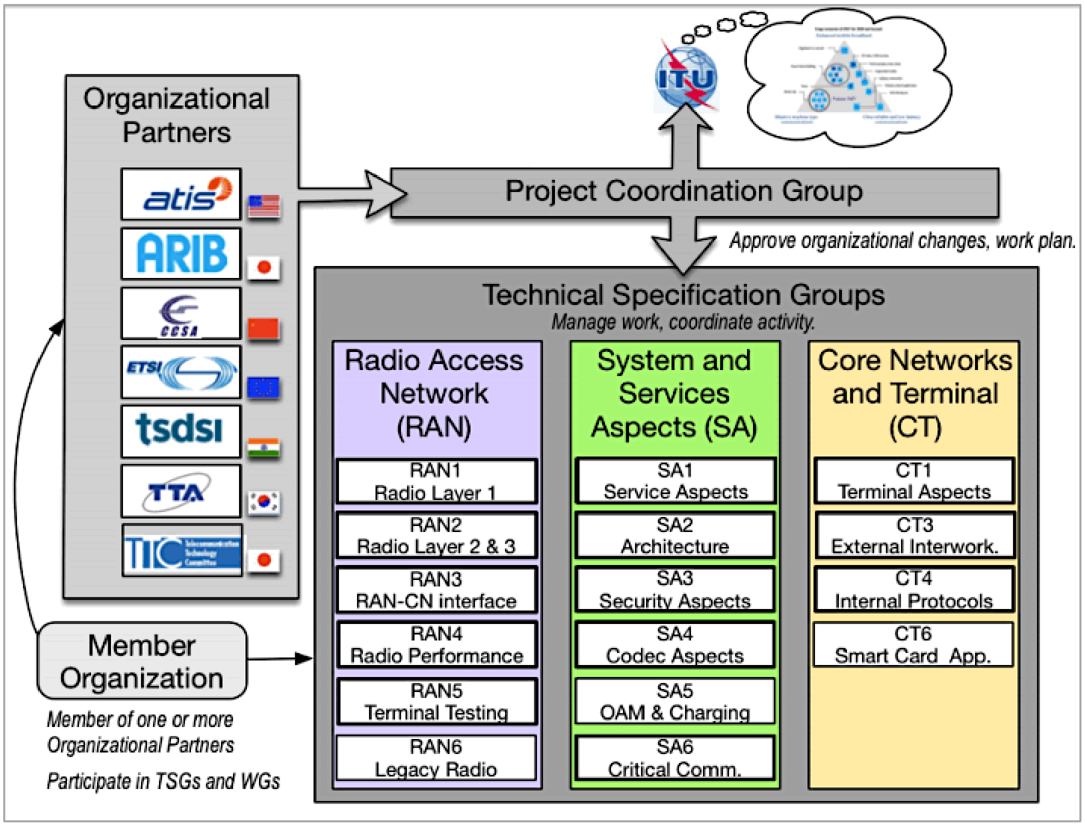


Figure A.1: *3GPP specifications development groups (source: www.3gpp.org).*

A.1 Specification numbering

All 3GPP specifications have a specification number[19] consisting of four or five digits (e.g., 09.02 or 29.002). The first two digits define the series, followed by two further digits for the 01 to 13 series or three further digits for the 21 to 55 series. The series of specifications are categorized as shown in Table A.1.

Table A.1: *3GPP specification numbering guide.*

Subject of specification series	3G and beyond / GSM (R99 and later)	GSM only (Rel-4 and later)	GSM only (before Rel-4)
General information (long defunct)			00 series
Requirements	21 series	41 series	01 series
Service aspects (“stage 1”)	22 series	42 series	02 series
Technical realization (“stage 2”)	23 series	43 series	03 series
Signalling protocols (“stage 3”) - user equipment to network	24 series	44 series	04 series
Radio aspects	25 series	45 series	05 series
CODECs	26 series	46 series	06 series
Data	27 series	47 series (none exist)	07 series
Signalling protocols (“stage 3”) -(RSS-CN) and OAM&P and Charging (overflow from 32.- range)	28 series	48 series	08 series
Signalling protocols (“stage 3”) - intra-fixed-network	29 series	49 series	09 series
Program management	30 series	50 series	10 series
Subscriber Identity Module (SIM / USIM), IC Cards. Test specs.	31 series	51 series	11 series

[19] http://www.3gpp.org/specifications/79-specification-numbering.

Subject of specification series	3G and beyond / GSM (R99 and later)	GSM only (Rel-4 and later)	GSM only (before Rel-4)
OAM&P and Charging	32 series	52 series	12 series
Access requirements and test specifications		13 series (1)	13 series (1)
Security aspects	33 series	(2)	(2)
UE and (U)SIM test specifications	34 series	(2)	11 series
Security algorithms (3)	35 series	55 series	(4)
LTE (Evolved UTRA), LTE-Advanced, LTE-Advanced Pro radio technology	36 series	-	-
Multiple radio access technology aspects	37 series	-	-
Radio technology beyond LTE	38 series	-	-

The 3GPP Technical Reports are of two classes:

1. Those intended to be issued by the Organizational Partners as their own publications; and

2. Those not intended for publication, but which are simply 3GPP internal working documents, used, for example, for documenting planning and scheduling of work, or for holding the interim results of feasibility studies.

The first category has numbers of the form: xx.9xx. The second category have numbers of the form: xx.8xx (feasibility study reports, etc.). Or, more rarely, 30.xxx / 50.xxx (planning and scheduling).

For some specification series, the stock of xx.8xx TRs has been exhausted, and in these cases, further internal TRs are allocated xx.7xx numbers.

For missing specifications[20]: The specifications not yet available following the most recent round of TSG meetings.

The 3GPP Specifications are stored on the file server as zipped MS-Word files. The filenames have the following structure:

SM[-P[-Q] -V.zip

where the character fields have the following significance:

[20] http://www.3gpp.org/ftp/Specs/html-info/MissingSpecs.htm.

S = series number—two characters (see the table above)
M = mantissa (the part of the spec number after the series number)—two or three characters (see above)
P = optional part number—one or two digits if present
Q = optional sub-part number—one or two digits if present
V = version number, without separating dots—three digits (six digits when any component of the three-digit range has been exhausted - see the fifth example below)

Some examples:

- 21900-320.zip is 3GPP TR 21.900 version 3.2.0
- 0408-6g0.zip is 3GPP TS 04.08 version 6.16.0
- 32111-4-410 is 3GPP TS 32.111-part 4 version 4.1.0
- 29998-04-1-100 is 3GPP TS 29.998-part 4 sub-part 1 version 1.0.0
- 29898-133601 is 3GPP TR 29.898 version 13.36.1

Latest version
The latest versions of the approved specifications in the "latest" directory. The latest version of draft specs (i.e., those not yet under change control) are in the "latest-drafts" directory.

Particular version
All older versions of specifications (where available) are stored in the **archive subdirectory**. All versions of all releases of a given specification are placed directly under the name of the specification.

Searching by title or subject
The complete list of all 3GPP specification numbers and titles are found here:
http://www.3gpp.org/DynaReport/SpecReleaseMatrix.htm

This list also shows the most recent version in each Release.

Searching for specifications related to a particular working group
Each 3GPP TSG Working Group has a home page, which lists the specifications under its responsibility. They can be found here:
http://www.3gpp.org/specifications-groups/specifications-groups

Official versions published by recognized Standards Development Organizations
The 3GPP Technical Specifications (and Technical Reports) which are publicly available from this site have, in themselves, no legal standing. They only become "official" when transposed into corresponding publications of the Partner Organizations.

List of acronyms/abbreviations/symbols/initialisms

3G	3rd Generation
3GPP	3rd Generation Partnership Project
700TAG	700 MHz Technical Advisory Committee
A	
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ADMF	Administrative Function
AF	Application Function
AGW	Access Gateway
AMR	Adaptive Multi-Rate
AN	Access Network
ANDSF	Access Network Discovery Function
ANR	Automatic Neighbour Relations
AP	Application Part
API	Application Programming Interface
APN	Access Point Name
ARP	Allocation Retention Priority
AS	Application Server
AuC	Authentication Center
B	
BBDS	Broadband Deployable System
BBF	Broadband Forum
BGCF	Breakout Gateway Control Function
BM-SC	Broadcast Multicast Service Center
BMO	Browser Managed Object
BNG	Broadband Network Gateway
BPCF	Broadband Policy Control Function
BSS	Business Support System
BYOD	Bring-Your-Own-Device

C

CAPIF	Common API Framework
CBC	Cell Broadcast Centre
CBE	Cell Broadcast Entity
CBIM	Common Baseline Information Module
CBS	Cell Broadcast Service
CC	Content of Communication
CCO	Coverage and Capacity Option
CDMA	Code Division Multiple Access
CDR	Charging Data Record
CE-BBDS	Core Enabled Broadband Deployable System
CFA	Common Functional Architecture
CfM	Configuration Management
CISC	CRTC Interconnect Steering Committee
CLI	Command Line Interface
CM	Configuration Management
CN	Core Network
CODEC	Coder-Decoder
COLT	Cell On Light Truck
ConnMO	Connectivity Managed Object
COPS	Community Oriented Policing Service
COW	Cell On Wheels
CR-BBDS	Core Ready Broadband Deployable System
CRM	Customer Relationship Management
CRTC	Canadian Radio-Television and Telecommunications
CSCF	Call Session Control Function
CSS	Centre for Security Science (Canada)
CT	Core Network & Terminals

D

D2D	Device to Device
DBIFOM	Device Based IP Flow Mobility
DCMO	Device Capabilities Managed Object

DeNodeB	Donor eNode-B
DF2	Delivery Function 2
DF3	Delivery Function 3
DHCP	Dynamic Host Configuration Protocol
DiagMonMO	Diagnostics and Monitoring Managed Object
DM	Device Management
DNS	Domain Name System
DRA	Diameter Routing Agent
DRDC	Defence Research & Development Canada
DS	Deployable Systems
E	
E-CSCF	Emergency Call Session Control Function
EM	Element Manager
eMBMS	enhanced Multimedia Broadcast Multicast Services
EMS	Element Management System
eNodeB	evolved Node-B
ENUM	(ITU-T) E.164 Number Mapping
EPC	Evolved Packet Core
ePDG	enhanced Packet Data Gateway
EPS	Evolved Packet System
ES	Entreprise Systems
ESB	Enterprise Service Bus
ESInet	Emergency Services IP network
eTOM	enhanced Telecommunications Operations Map
EUA	End-User Agency
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved UMTS Terrestrial Radio Access
F	
F/P/T	Federal/Provincial/Territorial
FE	Front End
FIPS	Federal Information Processing Standard (USA)
FTP	File Transport Protocol

FUMO	Firmware Update Managed Object
G	
GCS	Ground Control Station
GCSE	Group Communications System Enablers
GIS	Geographic Information System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications or Groupe Spéciale Mobile
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
GTP-C	GPRS Tunneling Protocol for the Control plane
GTP-U	GPRS Tunneling Protocol for the User plane
GUI	Graphical User Interface
GW	Gateway
H	
H-ANDSF	Home Access Network Discovery Function
HeNodeB	Home evolved Node B
HF	High Frequency
HLR	Home Location Register
HNB	Home Node B
HPLMN	Home Public Land Mobile Network
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Transport Layer Security
I	
IBCF	Interconnection Border Control Function
ICAM	Identity, Credentials, and Access Management
ICIC	Inter-Cell Interference Coordination
I-CSCF	Interrogating Call Session Control Function
ID	Identifier
IEEE	Institute of Electrical and Electronjc Engineers

IETF	Internet Engineering Task Force
IFOM	IP Flow Mobility
II-NNI	Inter-IMS Network to Network Interface
IM	Inventory Management
IMS CN	IP Multimedia Subsystem Core Network
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
IMS-AGW	IP Multimedia Sub-system – Access Gateway
IMSI	International Mobile Subscriber Identity
IOPS	Isolated E-UTRAN Operations for Public Safety
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IP-SM-GW	IP Short Message Gateway
IPsec	IP security
IPX	IP eXchange
IRI	Intercept Related Information
IRP	Integration Reference Point
IS	Inter-System
ISDN	Integrated Services Digital Network
ISED	Innovation, Science and Economic Development Canada
ISIM	IP Multimedia Service Identity Modules
ISMP	Inter-System Mobility Policy
ISRP	Inter-System Routing Policy
ISUP	ISDN User Part
ITU	International Telecommunication Union
IWF	Inter-Working Function
L	
LAN	Local Area Network
LAWMO	Lock and Wipe Managed Object
LC	Local Control

LCS	Location Services
LDAP	Lightweight Directory Access Protocol
LEMF	Law Enforcement Monitoring Facility
LMR	Land Mobile Radio
LRF	Location Retrieval Function
LTE	Long Term Evolution
M	
M2M	Machine-to-Machine
MAG	Mobility Access Gateway
MAG-AAA	Mobility Access Gateway – Authentication, Authorization and Accounting
MAP	Mobile Application Part
MBMS	Multimedia Broadcast Multicast Services
MBMS GW	Multimedia Broadcast Multicast Services Gateway
MC	Mission Critical
MCData	Mission-Critical Data
MCE	Multi-cell/multicast Coordination Entity
MCPTT	Mission-Critical Push-To-Talk
MCS	Mission Critical Services
MCVideo	Mission-Critical Video
MDT	Minimization of Drive Tests
MGCF	Media Gateway Control Function
MGW	Media Gateway
MHz	megahertz
MIP	Mobile Internet Protocol
MLB	Mobility Load Balance
MLP	Mobile Location Protocol
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MO	Managed Object
MOCN	Multi-Operator Core Network
MOP	Master Operator

MPS	Modèle de Prestation de Services
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MOC	Mobile Originated Calls
MRO	Mobility Robustness Optimization
MTC	Machine Type Communication
MV	Mobile Virtual
MVPN	Mobile Virtual Private Network
N	
NAAD	National Alert Aggregation & Dissemination
NAD	Network Architecture Description
NAS	Non-Access Stratum
NBIFOM	Network Based IP Flow Mobility
NE	National Entity
NENA	National Emergency Numbering Association
NG 911	Next Generation 911
NGMN	Next Generation Mobile Network
NM	Network Manager
NMS	Network Management System
NNI	Network-to-Network Interface
N-NOC	National Network Operations Centre
N-SOC	National Security Operations Centre
NOC	Network Operations Centre
NPAS	National Public Alerting System
NPSTC	National Public Safety Telecommunications Council (USA)
NRM	Network Resource Model
NTP	Network Time Protocol
O	
OAM	Operations Administration and Maintenance
OAM&P	Operations, Administration, Maintenance, and Provisioning
OCS	Online Charging System
OMA	Open Mobile Alliance

Op-Def	Operator Defined
OSA	Open Services Access
OSA-API	Open Services Access – Applications Programming Interface
OSF	Operations Support Functions
OSS	Operations Support Systems
P	
PCC	Policy and Charging Control
PCEF	Policy Charging and Enforcement Function
PCI	Physical Cell Identity
PCRF	Policy Charging and Rules Function
P-CSCF	Proxy Call Session Control Function
PDN	Packet Data Network
PDN ID:	Packet Data Network Identifier (same as APN)
PDP	Policy Decision Point
PEEM	Policy, Evaluation, Enforcement and Management
PEP	Policy Enforcement Point
P-GW	Packet Gateway
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Radio
PLMN ID	PLMN Identifier
PLR	Packet Loss Rate
PMIP	Proxy Mobile IP
PNP	Plug-n-Play
POP	Participating Operators
ProSe	Proximity Service
PSAP	Public Safety Answering Point
PSBB	Public Safety Broadband
PSBN	Public Safety Broadband Network
PSTN	Public Switched Telephone Network
PTT	Push To Talk
PWS	Public Warning System

Q	
QCI	Quality of Service Class Indicator
QoS	Quality of Service
QPP	Quality of Service, Prioritization and Pre-emption
R	
R&D	Research and Development
RACH	Random Access Channel
RAN	Radio Access Network
RAT	Radio Access Technology
REST	Representational State Transfer
RF	Radio Frequency
RLSP	Réseau à Large Bande pour la Sécurité Publique
RN	Relay Node
R-NOC	Regional Network Operations Centre
R-SOC	Regional Security Operations Centre
RSDE	Regional Service Delivery Entity
RTCP	Real-Time Control Protocol
RTP	Real-time Transfer Protocol
S	
SA	System Architecture
SAE	System Architecture Evolution
SCEF	Service Capability Exposure Function
SCOMO	Software Component Managed Object
SCS	Services Capability Server
S-CSCF	Serving Call Session Control Function
SCTP	Stream Control Transmission Protocol
SDM	Service Delivery Model
SDO	Standards Development Organization
SDP	Service Delivery Platform
SDS	Short Data Service
S-GW	Serving Gateway
SID	Shared Information Data model

SIP	Session Initiation Protocol
SLP	Secure User Plane Location Platform
SMS	Short Message Service
SNMP	Simplified Network Management Protocol
SO	Service Orchestration
SOA	Service Oriented Architecture
SOC	Security Operations Centre
SON	Self Organizing Network
SS	Solution Set
SS7	Signaling System 7
SSL	Secure Sockets Layer
SUPL	Secure User Plane Location
T	
TAG	Technical Advisory Group (Canada)
TAM	The Application Framework
TCI	Technical Considerations on Interoperability
TCO	Technical Considerations on Operability
TCP	Transmission Control Protocol
TCS	Technical Considerations on Security
TMF	TeleManagement Forum
TMN	Telecommunication Management Network
TrGW	Transfer Gateway
TR	Technical Requirement
TS	Technical Specification
TSG	Technical Specification Group
U	
UDC	User Data Convergence
UDP	User Datagram Protocol
UDR	User Data Repository
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System

UNI	User to Network Interface
USIM	UMTS Subscriber identity Module
UTRA	Universal Terrestrial Radio Access
UTRAN	Universal Terrestrial Radio Access Network
V	
VLAN	Virtual Local Area Network
VoIP	Voice-over Internet Protocol
VoLTE	Voice over LTE
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network
W	
WWCDMA	Wideband Code Division Multiple Access
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAS	Wireless Public Alerting System
WS2	Workstream 2
WSP	Wireless Service Provider

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

DRDC – Centre for Security Science
NDHQ (Carling), 60 Moodie Drive, Building 7
Ottawa, Ontario K1A 0K2 Canada

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

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Public Safety Broadband Network (PSBN): Network architecture description

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

Fournier, J.; Lucente, C.; Skidmore, D.; Samson, L.

5. DATE OF PUBLICATION (Month and year of publication of document.)

January 2019

6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)

152

6b. NO. OF REFS (Total references cited.)

101

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Scientific Report

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

DRDC – Centre for Security Science
NDHQ (Carling), 60 Moodie Drive, Building 7
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. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2018-R236

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Wireless; Broadband; Long Term Evolution (LTE); Communications Networks; Public Safety Communications; 700 MHz; Situational Awareness; Network Architecture and Design

13. ABSTRACT (When available in the document, the French version of the abstract must be included here.)

This Scientific Report provides guidance on possible architectures for the Public Safety Broadband Network (PSBN) initiative in Canada. The architecture considers Service Delivery Model (SDM) concepts and 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE), and is supplemented by various other technologies that, in its ensemble, forms the PSBN. The described architectures contained herein are intended to provide Science and Technology (S&T) advice to those ultimately responsible for the implementation of the PSBN in Canada, and the decision to consider the contents of this Scientific Report rests with them.

This report is a revision of the initial PSBN architecture that was developed in 2013. It has been expanded beyond the network aspects and now includes additional architectural aspects for mission critical communication services, machine type communications, better known as Internet of Things (IoT), operations support, business support, telecommunications management, PSBN planning and service architecture. The information and views that are contained in this document are those of the authors and are only intended as guidance to the implementers of the PSBN.

What public safety needs in an emergency is…

The ability of emergency personnel to communicate between jurisdictions, disciplines, and levels of government, using a variety of systems, as needed and as authorized… a national emergency communications based on common user requirements, open standards and a system of systems approach… a public safety controlled mobile broadband communications network expected to operate in the 700 megahertz (MHz) band [1].

Ce rapport fournit des conseils sur des architectures possibles pour un réseau à large bande pour la sécurité publique (RLSP) au Canada. L’architecture RLSP considère des concepts de modèle de prestation de services (MPS) et le Projet de Partenariat de 3e Génération (3GPP) évolution à long terme (LTE) et est complétée par diverses autres technologies qui, dans leur ensemble, forme le RLSP. Les architectures décrites ont comme but de fournir des conseils S&T à ceux qui seront ultimement responsable pour la mise en oeuvre du RLSP, et la décision de considérer les contenus de ce rapport, ou pas, est la leur.

L’architecture RLSP initiale qui a été développée en 2013, a été élargie au-delà de seulement les aspects du réseau et comprend maintenant des aspects architecturaux supplémentaires pour le développement des services, les services de communication critique de mission, les communications de type machine mieux connu comme « Internet of Things » (IoT), le soutien des opérations, le soutien aux entreprises, la gestion des télécommunications et la planification RLSP. Les informations et points de vue contenus dans ce document sont ceux des auteurs et sont seulement destinés à guider les metteurs en cause du RLSP.