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

DRDC | RDDC
technologysciencetechnologie

Public Safety Broadband Network (PSBN)

Technical Considerations on Security (TCS)

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

Defence Research and Development Canada

Scientific Report

DRDC-RDDC-2018-R240

February 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

The public safety community deals with the safety and security of people, property, our institutions, and our country on a daily basis. In the course of their work they access and generate information that is critical to the success of their missions. They expect their communications networks to be reliable, available, and secure.

A Public Safety Broadband Network (PSBN) would undoubtedly be a target for cyber-attacks, espionage, and conventional attempts to disrupt and deny the availability of this critical asset to first responders. It is, therefore, imperative that robust measures be taken to secure the network and the information carried over it. This document presents a number of considerations that are structured within a security architecture that serves as a reference for next generation communications networks.

The security measures contained in this document are those that are deemed to support the proposed security posture for the PSBN. A security risk assessment would likely identify other security controls that would be required to support the security posture.

The consideration statements in this document are derived from similar efforts undertaken in the U.S. to support FirstNet[1] and from the experience of subject-matter-experts and practitioners that participated in cross-disciplinary work groups.

The Public Safety Broadband Network Use-Cases and User Requirements [1] contains a set of scenarios, referred to as “use-cases,” that typify the way subscribers of the PSBN are expected to use the PSBN in their day-to-day work and during extra-ordinary events, as well as a list of User Requirements (UR) that are phrased in terms of what the users need to be able to do or accomplish.

The technical considerations contained in this Technical Considerations on Security document (TCS) were derived with those URs in mind, and they reflect the capabilities that PSBN would offer to satisfy the security needs of the users of a Public Safety Broadband Network (PSBN). The statements express “what is needed” in operationally relevant terms. The contributors to the TCS refrained as much as possible from stating “how” to satisfy the needs of the users.

The TCS does not sequence the technical considerations in the manner of a roadmap of features. It is expected that the features and capability roadmap will be developed by the operators of the PSBN as part of their strategic planning process.

What public safety needs in an emergency is…

“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

[1] FirstNet refers to “First Responder Network Authority.” It is the entity responsible for building and operating the US public safety broadband network.

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." [2]

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 broadband mobile in their hands will greatly increase their ability to anticipate, respond to and recover from emergencies, disasters and acts of terrorism by increasing their situational awareness 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 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.

The technical considerations on security contained in the TCS describe a modern mobile broadband communications network that provides users with the ability to securely access their information and applications from anywhere in the nationwide footprint of the PSBN and over partner networks in Canada, the U.S., and internationally. This TCS, together with its companion Scientific Reports, the Use Cases and User Requirements Document (URD) [1], the Technical Considerations on Operability (TCO) [3], the Network Architecture Description (NAD) [4], and the Technical Considerations on Interoperability (TCI) [5] documents, are expected to contribute to the successful implementation of a nationwide interoperable mobile broadband network in Canada.

Résumé

Chaque jour, les membres de la communauté de la sécurité publique veillent à la sécurité et à la protection de la population, des biens, de nos institutions et de notre pays. Dans le cadre de leur travail, ils génèrent et traitent de l'information essentielle à la réussite de leurs missions. Ils s'attendent donc à ce que leurs réseaux de communication soient accessibles, sécuritaires et fiables.

Un réseau à large bande pour la sécurité publique (RLBSP) serait à n'en point douter la cible de cyberattaques, d'opérations d'espionnage ou encore de tentatives conventionnelles pour perturber ou bloquer l'accès à cet outil crucial pour les premiers intervenants. Il est donc essentiel de prendre des mesures énergiques pour sécuriser le réseau et les données. Dans ce document, nous présentons bon nombre de facteurs à considérer dans une architecture de sécurité pouvant servir de référence pour la prochaine génération de réseaux de communication.

Les mesures décrites dans le présent document sont celles que nous jugeons les plus appropriées pour appuyer la posture de sécurité suggérée pour le RLBSP. L'évaluation des risques de sécurité pourrait sans doute permettre de déterminer des contrôles supplémentaires. Les énoncés relatifs aux différents facteurs à considérer découlent d'efforts semblables déployés aux États-Unis pour soutenir FirstNet[2] et de l'expérience d'experts et de professionnels ayant participé à des groupes de travail interdisciplinaires.

Le document intitulé *The Public Safety Broadband Network Use-Cases* and *User Requirements* [1] présente un ensemble de scénarios typiques sur l'utilisation du réseau à large bande par les abonnés (cas d'application) dans le cadre de leur travail quotidien ou lors d'événements extraordinaires. Il présente aussi une liste des besoins des utilisateurs en fonction de leurs tâches.

Les facteurs techniques à considérer mentionnés dans le document *Technical Considerations of Security (TCS)* découlent des besoins des utilisateurs. Ils correspondent aux capacités du RLBSP requises pour satisfaire aux exigences de sécurité de leurs utilisateurs. Les énoncés décrivent les besoins en fonction des activités. Les auteurs de ce document ont évité le plus possible d'indiquer la façon de répondre à ces besoins.

Dans le document, les facteurs techniques à considérer ne sont pas présentés comme dans une feuille de route. On s'attend à ce que les utilisateurs du RLBSP établissent eux-mêmes une feuille de route pour développer les fonctions et les capacités requises dans le cadre de leur processus de planification stratégique.

EN SITUATION D'URGENCE, SÉCURITÉ PUBLIQUE A BESOIN…

« Les organismes d'intervention d'urgence de tous les ordres du gouvernement doivent assurer des communications harmonieuses et interopérables afin de gérer les interventions, d'établir une structure de commandement et de contrôle, de conserver une connaissance de la situation et d'exercer leurs activités au sein d'un cadre opérationnel commun. On profitera ainsi de capacités d'intervention améliorées et

[2] FirstNet (First Responder Network Authority) est l'entité responsable de la mise sur pied et de l'exploitation du réseau à large bande pour la sécurité publique des É.-U.

d'une approche plus globale de la gestion des opérations en cas de catastrophe, d'où une plus grande sécurité pour les Canadiennes et les Canadiens. »

« L'information est l'élément vital des opérations quotidiennes dans le milieu de la sécurité publique. Les agents responsables prennent chaque jour d'innombrables décisions et doivent avoir rapidement accès à des renseignements opportuns, exacts et complets. Il est devenu évident qu'un processus décisionnel efficace nécessite un échange fréquent d'information entre une multitude de systèmes, d'organismes et d'administrations. » [2]

Importance pour la défense et la sécurité

Le RLBSP sans fil sera un réseau cellulaire national destiné surtout à la sécurité publique, ainsi qu'aux communautés de la sécurité et de la défense. Cet instrument de transformation révolutionnera les communications et l'échange de renseignements entre les premiers intervenants et le personnel de la défense durant des décennies. Les services mobiles à large bande à portée de la main augmenteront considérablement la capacité de prévoir les urgences, les sinistres et les actes terroristes, d'intervenir et de rétablir les choses. Le fait d'améliorer ainsi leur connaissance de la situation permettra au bout du compte de protéger et de sauver des vies, de limiter les dommages et les pertes matérielles, et rendra les collectivités plus sûres. Les services cellulaires commerciaux sont certes suffisants pour l'utilisation quotidienne par les agents de la sécurité publique, mais en cas d'incident grave, ils deviennent vite incapables de répondre à la demande car ils s'engorgent sérieusement. La disponibilité des réseaux commerciaux est principalement dictée par des facteurs économiques. En revanche, celle du RLBSP devrait essentiellement viser à garantir la sécurité de la population.

Les facteurs techniques relatifs à la sécurité qui figurent dans le document *Technical Considerations of Security (TCS)* visent à favoriser l'instauration d'un réseau moderne de communication mobile à large bande qui permettra aux utilisateurs d'avoir accès à leur information et à leurs applications de façon sécuritaire à partir de n'importe où sur le RLBSP ou sur des réseaux partenaires au Canada, aux É.-U. et ailleurs dans le monde. Le TCS, les rapports scientifiques connexes ainsi que les documents *The Public Safety Broadband Network Use-Cases and User Requirements Document* (URD) [1], *Technical Considerations on Operability* (TCO) [3], *Network Architecture Description* (NAD) [4] et *Technical Considerations on Interoperability* (TCI) [5] favoriseront la réussite de la mise en œuvre du réseau cellulaire à large bande interopérable à l'échelle du Canada.

Table of contents

List of figures

List of tables

Acknowledgements

This Scientific Report on PSBN Technical Considerations on Security supersedes a previous unpublished Report on PSBN Security in 2014. 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, academia, federal/provincial/territorial emergency management officials, and first responders. The recommendations were reviewed by the 700 MHz Technical Advisory Group[3] (700TAG). The authors of this report acknowledge the invaluable contributions and dedication of all 700TAG members and the participants in the work sessions.

The authors of this Report also acknowledge the following members of the 700TAG who were key contributors, directly involved in the production of the original draft report:

- Jacob Gurnick, Communications Research Centre Canada
- Eric Lafond, Communications Research Centre Canada
- Charles Auger, Communications Research Centre Canada
- Simond Arcand, Communications Security Establishment Canada
- Dr. Stephen Braham, Simon Fraser University

[3] 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 Center of Canada, Simon Fraser University, and technical experts from Federal/Provincial/Territorial/Municipal agencies.

1 Purpose

The purpose of this Scientific Report is to inform the public safety community on a variety of considerations related to the security of a Public Safety Broadband Network (PSBN) in Canada. To do so, a possible architecture, described in the PSBN Network Architecture Description [4], is used to draw out such considerations. The architecture is based on a two-tier service delivery model and was selected to serve as the basis for the operability considerations in this report insofar as it introduces modes of operation between the actors in the service delivery fabric that are unusual and are, thereby, uncommon in the industry. Other architectures could also have been considered in producing this report, but it is the opinion of the authors that the one selected, while not exclusive, represents a valid approach 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 the position of the federal government on PSBN.

The Technical Considerations on Security (TCS) is one in a series of PSBN reports issued by Defence Research and Development Canada Centre for Security Sciences (DRDC CSS) that also includes the PSBN Network Architecture Description (NAD) [4], the PSBN Technical Considerations on Interoperability (TCI) [5] and the Technical Considerations on Operability (TCO) [3] 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.

While the NAD was published by DRDC in 2013, the TCI, TCO and TCS remained in draft form and were not re-visited until 2017. When the first drafts were produced, 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.

The considerations expressed in this document state mostly “what-can-be-considered” rather than “how-to-achieve” the Technical Considerations on Security. This document does not define PSBN policies and procedures. At times, industry best practices and standard-based protocols and solutions may be provided when they are considered the best-proven or the only implementation that would lead to an interoperable and secure PSBN.

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 PSBN. As such, they do not represent actual requirements of the PSBN but simply information points on technical aspects of the PSBN.

As this Scientific Report is part of a series, it is recommended that the NAD be read before this TCS Report, as it contains assumptions and more detailed technical descriptions that are not fully provided in this report. The NAD will therefore serve as the foundational basis for the technical considerations found herein.

2 Introduction

This Scientific Report examines and highlights the technical considerations on security regarding the PSBN. The ability for users to communicate and access information is dependent on the integrity of the PSBN that is enabled by adhering to industry-accepted standards, best practices and taking certain measures that allow the PSBN to operate and perform as one network from a user-centric perspective. The network architecture of the PSBN [4] impacts Security Considerations (SC). A two-tiered network architecture serves as the basis for the interoperability considerations in this report insofar as it introduces modes of inter-working between the actors in the service delivery fabric that are unusual and are, thereby, uncommon in the industry. It is the opinion of the authors that this architecture yields the most complete analysis of security considerations, and as such, any other architecture that may be selected for the PSBN would nevertheless be covered by the contents of this report. The network architecture, consisting of Regional Service Delivery Entities (RSDE) and a national entity acting as a federating layer for the RSDEs, is selected for examination because it introduces distinct interoperability considerations that are not present in monolithic single-operator service delivery models.

The public safety community deals with the safety and security of people, property, our institutions, and our environment on a daily basis. In the course of their work they access and generate information that is critical to the success of their missions. They expect that this information will be secure in terms of confidentiality, availability, and integrity. They also expect their communications networks to be reliable, available, and secure.

The future public safety broadband network (PSBN) will undoubtedly be a target for cyber-attacks, espionage, and conventional attempts to disrupt and deny the availability of this critical asset to first responders. It is therefore imperative that robust measures be taken to secure the network and the information carried over it. This document presents a number of considerations that are structured within a security architecture that serves as a reference for communications networks.

For the stakeholders of the PSBN, a standard of security and mandatory compliance that is based on commonly-accepted practices and standards is required. Business and systems requirements must be met in order to achieve the appropriate level of security while allowing access to only those users that need the information to perform the full range of duties required of their roles. Access controls notwithstanding, interoperability between users wherever they may be located in Canada or outside of Canada must be assured.

The PSBN is intended to serve a broad range of users with widely varying needs for security of the PSBN. Examples are: the volunteer fireman needing access to a hazardous materials database, an RCMP officer needing access to criminal records, and a Canadian Armed Forces deployment sharing situational awareness with local responders in support of a major disaster. As permitted by the Federal Government [6], commercial users may share the spectrum on which the PSBN operates. The network architecture (NAD) for the PSBN [4] has considered this possibility in that only the Radio Access Network (RAN) could be shared, but not the core network. This approach is supported by the Third Generation Partnership Program (3GPP) and is referred to as
Multi-Operator Core Network (MOCN), which is discussed in greater detail in the NAD. The consideration statements in this report are stated without regards to distinction between commercial users

and public safety users. However, as commercial users cannot access the PSBN core nor the PSBN services, the related security considerations do not apply to commercial users.

The cost of implementing security controls are likely to be determined by the residual risk that the operators of the PSBN will tolerate and the point at which additional investment in security controls results in diminishing returns. It is possible that some security controls could be applied selectively for those users that require them, whereas the rest of the security controls would form the minimum set for the PSBN. The security considerations contained in this document would establish the minimum set of security controls for the PSBN. The result of a security risk assessment of the PSBN and its use-cases could potentially alter the baseline minimum security controls. A thorough review of the potential impacts on interoperability should be undertaken at the outset and within the life cycle of security controls.

Security considerations for telecommunication networks and services should follow industry-accepted standards for security, as it increases interoperability as well as avoids duplication of effort. The security services and mechanisms that can benefit telecommunication networks or service providers are related to protection against malicious attacks such as denial of service, eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting, or re-ordering of messages), repudiation or forgery. Protection includes prevention, detection and recovery from attacks, measures to prevent service outages due to natural events (weather, etc.) as well as management of security-related information.

The PSBN should be planned and implemented with accepted integrated security measures for all dimensions, layers and planes of the communications system as articulated in the International Telecommunications Union (ITU) “Security architecture for systems providing end-to-end communications”—ITU-T Rec. X.805 (10/2003) Recommendation from the International Telecommunication Union [7].

3 Scope of document

To understand the scope of this document, it is important to consider certain assumptions as described in the NAD Report.

A first assumption is on a service delivery model for a mobile network such as the PSBN, which identifies the actors and their interactions in the delivery of services—in this case, mobile broadband communications services, to its "customers." The PSBN is based on a service delivery model [8] whereby it is posited that the users of the PSBN are clients of the network operator, 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. In Figure 1 the PSBN service delivery model [8] shows how each of the three principal actors—a National Entity (NE), Regional Service Delivery Entities (RSDE), and the End-User Agencies (EUA) fit into the overall chain of connecting users (e.g., machine or humans) to their information networks or to each other. The NE and the RSDEs are depicted as being distinct from the users and the EUAs to which they pertain. The EUAs own the information networks, whereas the National Entity and RSDE own the PSBN infrastructure. Applications can be hosted by the NE, RSDEs, and by EUAs. The PSBN operators will interconnect the PSBN with external networks and applications, such as commercial carriers, FirstNet, existing LMR and WiFi networks and the applications that are hosted on those networks.

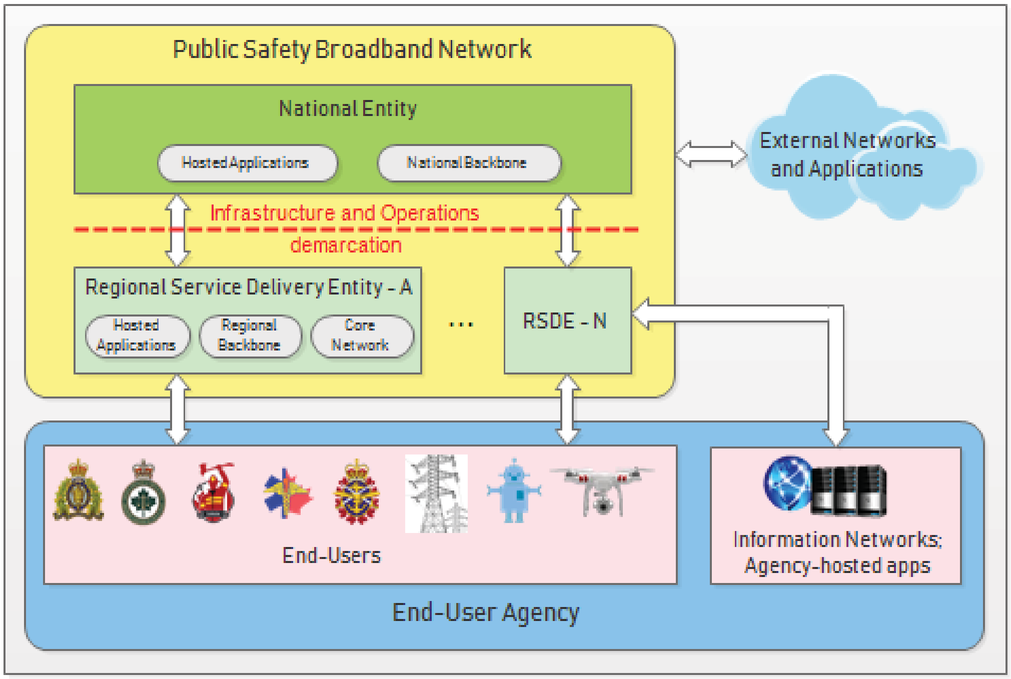

Public Safety Broadband Network
National Entity
Hosted Applications
National Backbone
Infrastructure and Operations
demarcation
Regional Service Delivery Entity - A
Hosted Applications
Regional Backbone
Core Network
...
RSDE - N
External Networks and Applications
End-Users
Information Networks; Agency-hosted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

***Figure 1:** PSBN service delivery model.*

A second assumption in this report is with regards to the functional scope of the PSBN. With reference to Figure 2, the items in the central, yellow rectangle represent the functions that are assumed to be in the scope of the PSBN. The items in the blue region, outside the inner rectangle, are assumed to be out of scope of the PSBN. Together, they comprise the public safety communications ecosystem. This report presents the security considerations for the interactions that are within the PSBN and the interactions of the PSBN with external networks and functions. The in-scope functions are examined in this report.

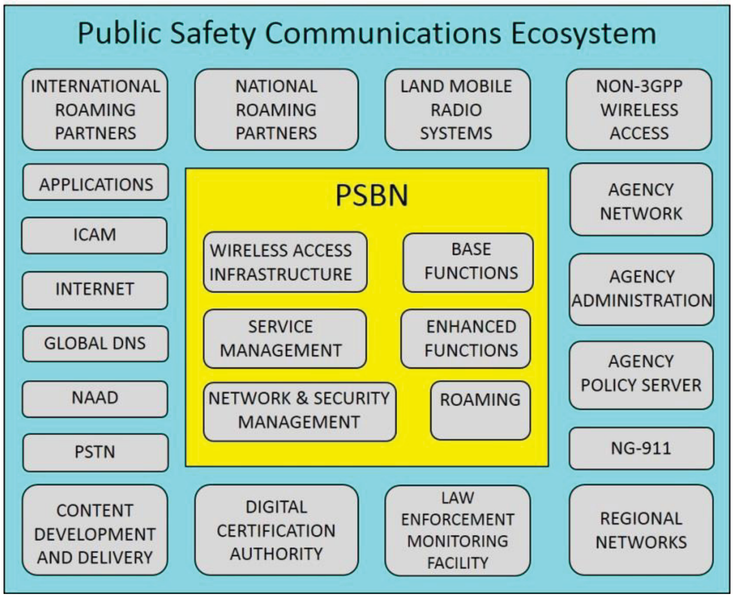

Public Safety Communications Ecosystem
INTERNATIONAL ROAMING PARTNERS
NATIONAL ROAMING PARTNERS
LAND MOBILE RADIO SYSTEMS
NON-3GPP WIRELESS ACCESS
APPLICATIONS
PSBN
AGENCY NETWORK
ICAM
WIRELESS ACCESS INFRASTRUCTURE
BASE FUNCTIONS
INTERNET
AGENCY ADMINISTRATION
GLOBAL DNS
SERVICE MANAGEMENT
ENHANCED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

Figure 2: *Public safety communications ecosystem.*

While considering the above, the scope of this document includes:

- PSBN up to its demarcation points to external networks such as Public Safety Agency Networks, the Public Switched Telephone Network (PSTN), roaming networks, and the internet;
- Technical protocol-based security considerations that can contribute to the formulation of security solutions Technical system-based security considerations that can contribute to the formulation of security solutions.

The following are out-of-scope of this document:

- Networks with no demarcation points with the PSBN, such as computer and server entities that are off-PSBN Network, office laptops, and intranet server;
- Process-based security measures such as security assessment, audit, testing, monitoring, training, education, certification, compliancy, Software (SW) development process, mobile app lifecycle management, Incident Response Process, Systems on a Chip (SoC)-based Processes, and others;[4]
- Security policies and security governance model;
- Fraud Prevention and Revenue Assurance;
- Legal Intercept;
- Business Continuity Planning, Disaster Recovery Planning, and Crisis Management;

[4] Although out-of-scope of this TCS, it is recommended that the PSBN implement industry best practices and standards in those areas.

- People and Personnel Security;
- Pros and cons analysis of security mechanisms, mitigations, or measure.

4 Public safety user requirements

The Public Safety Broadband Network Use-Cases and User Requirements document [1] contains a set of scenarios, referred to as “use-cases,” that typify the way subscribers of the PSBN are expected to use the PSBN in their day-to-day work and during extra-ordinary events. Each use-case contains a set of statements, referred to as “User Capability Needs” (UCN) that express the users’ needs, gaps in capabilities and what the users want to be able to do with this communications tool, namely the PSBN. The UCNs have been consolidated into a list of non-recurring statements that comprise the User Requirements (UR).

The technical considerations contained in this TCS were derived with those security-related URs in mind. UR statements are phrased in terms of what the users need to be able to do or accomplish, whereas the technical considerations are expressed in terms of what is required of the PSBN to satisfy the users’ needs.

Section 3.5 of the Public Safety Broadband Network Use-Cases and User Requirements document contains the consolidated set of security-related URs that have been derived from the User Capability Needs (UCNs). To ensure the completeness of technical requirements, the Security Considerations (SC) in this report have been mapped to the PSBN user requirements by conducting a traceability analysis with the operability considerations, the latter being outside of the scope of this report.

5 Security vulnerabilities, threats and countermeasures in PSBN

This section presents an overview of the main threats and mitigation measures, or countermeasures, pertaining to the many different components of the PSBN. While not always explicitly stated, it is assumed that if a threat exists, some level of vulnerability exists as well. A more extensive catalogue of threats to mobile devices and infrastructure has been compiled by the National Institute of Standards and Technology (NIST) [9].The associated NIST Interagency Report 8144 [10] provides context and describes the mobile threat catalogue. In the Department of Homeland Security (DHS) report Study on Mobile Device Security [11], a subset of the threats from the catalogue is analyzed and defences against the threats are validated.

It is expected that new vulnerabilities and threats will be uncovered over the lifespan of the PSBN, and that the operators of the PSBN will need to remain abreast of these discoveries, evaluate the risks and impacts, and decide on what actions to take.

5.1 Physical site

The physical site layer of the PSBN includes the physical facilities hosting the PSBN network elements, as well as facilities-based elements, such as power supply, heating, ventilation and air conditioning systems, that are essential to the availability of the PSBN.

In this area, threats include:

- Unauthorized access
- Physical attacks

Countermeasures to these threats include:

- Strong access control security to the PSBN facilities and network equipment with centralized monitoring and alarming systems
- Strong environmental monitoring and alarming systems for all key environmental factors that could affect proper operations of the PSBN network and equipment

Section 7.1 details the set of security considerations that could implement those countermeasures.

5.2 User Equipment (UE)

User Equipments (UE) are the subscriber entry points into the PSBN. As specified by 3GPP, UEs are composed of two sub-elements:

- Universal Integrated Circuit Card (UICC): UICCs are small cards that are removable from mobile devices. The UICC is commonly referred to as a Subscriber Identity Module (SIM) card[5] since, among other applications, it contains the SIM application. By design, cellular services for a given

[5] The Universal Subscriber Identity Module (USIM) is commonly referred to as the SIM.

subscriber is tied to the UICC, and UICCs can be moved from one piece of mobile equipment to another. The UICC holds the keys to authenticate the UE to the network;

- Mobile Equipment (ME): provides cellular connectivity and user interfaces.

UEs come in different form factors, are designed for different types of users (personal UE and machine UE), and are equipped with different capabilities, some of which expose the UE to specific security vulnerabilities.

Mobile devices come with multiple built-in wired and wireless interfaces, any one of which can potentially pose serious security threats. As mobile devices are designed to make it easy to install and use third-party applications from mobile device application stores, security risks can be introduced from mobile device platforms and application stores that do not place security restrictions on third-party application publishing.

While users prefer the convenience of having one device for both their personal and business activities, enterprises and governments are wary of security issues if Bring-Your-Own-Devices (BYOD) are used for both personal and business use. In response, some UE device manufacturers have partitioned UE devices into two separate logical spaces—one for personal data and the other space for business data. Such devices are referred to as “dual-personality” devices.

5.2.1 Personal UE

A personal UE is a handheld cellular radio device that includes all of the following features: (i) a mobile operating system; (ii) the capability to use mobile software applications, access and browse the internet, use text messaging, use digital voice service, and send and receive e-mail; (iii) cellular network connectivity. Examples of personal UEs are smartphones, where threats include:

- Physical attacks (theft, loss, tampering):
  - Personal UEs are inherently prone to loss and theft; in such cases, they can be physically tampered with and used to access and attack the PSBN;
  - Intruders may use stolen UEs and UICCs to gain unauthorized access to services.
- Data loss / loss of privacy:
  - Long Term Evolution (LTE) UEs are designed to store large amount of data, which make them vulnerable to data loss or theft.
- Application layer attacks (virus, malware, phishing):
  - As IP devices, UEs are susceptible to IP-based vulnerabilities and attacks. Downloaded applications and content can expose the UE to viruses, malware, spam, phishing and similar threats that compromise the integrity of the device, as well as the security of the PSBN; malware installed on a mobile device, or infecting a mobile device’s operating system and other firmware, could:
    - be part of a botnet launching a Distributed Denial of Service (DDoS) attack against a carrier’s radio network infrastructure;
    - prevent a UE from accessing a cellular network, therefore, causing a Denial of Service

        - modify, insert or delete applications and/or data stored by the Universal Subscriber Identity Module (USIM).

Countermeasures to the above threats include:

- A Device Anti-Theft and Disablement System to protect against tampered and compromised devices and/or stolen devices; this is covered in Section 7.9;
- The hardening of the UE; this is covered in Section 7.14;
- Strong authentication, authorisation, and encryption mechanisms; this is covered in Section 7.4:
    - strong mechanisms to authenticate users accessing the UE;
    - local user authentication to the USIM via a Personal Identification Number (PIN) configured on a UICC;
    - restricting access of a device to an authorized UICC (USIM) only;
    - devices with Operating System (OS) encryption, remote wipe capabilities, as well as options for encryption of data stored on the device.
- The most up-to-date anti-virus, anti-malware software installed on UEs and kept up to date as a basic protection mechanism for the device; this is covered in Section 7.10.

5.2.2 BYOD UE

For BYOD UEs, additional vulnerabilities that introduce threats include:

- Lack of physical security controls;
- Use of untrusted mobile devices, networks, content and applications;
- Interaction with untrusted systems;
- Unsecure use of location services.

Countermeasures to address these security threats include:

- Device security services that are commonly provided by the mobile device operating system, an enterprise Mobile Device Management (MDM) software, or other security controls; this is covered in Section 7.10;
- Applying the best practices in mobile device security for BYOD; this is covered in Section 7.10.

5.2.3 ProSe-enabled UEs

Similar to the Land Mobile Radio (LMR) direct communication, ProSe-enabled public safety UEs can establish the communication path directly between two or more ProSe-enabled public safety UEs, regardless of whether the ProSe-enabled UEs are served by eNodeBs.

With ProSe-enabled UEs, attackers can take advantage of the direct communication between the UEs (which is outside the UE-to-network security domain) with regards to user identity, user location, or eavesdropping; threats include:

- Eavesdropping
- Man in the Middle attack (MitM)
- Breach of privacy

Countermeasures to address these security threats include:

- Implementing 3GPP security specifications around the Proximity-based Services for both UE-to-Network as well as for UE-to-UE communication; this is covered in Section 7.6.

5.2.4 Machine UE (MTC UE or M2M UE)

A machine UE is a UE equipped for Machine Type Communication (MTC), which communicates through the PSBN with MTC server(s), other MTC device(s), and personal UEs. Within this document the terms Machine-to-Machine (M2M) and MTC (3GPP term for M2M) are interchangeable.

In contrast to personal UEs, which are carefully held and protected by a person, machine UEs can be located either in remote areas, or inside buildings and infrastructure. In such installations, machine UEs can remain untouched after installation for many years. Because they are not regularly physically monitored, these devices can be more susceptible to tampering by unauthorized persons.

A high number of MTC UEs may become active almost simultaneously after a period of power outage or other such events, or some MTC applications may generate recurring data transmissions at precisely synchronous time intervals, creating radio network congestion and generating an unintentional Distributed Denial of Service (DDoS).

Specific threats for machine UEs include:

- Theft
- Tampering
- Unauthorized access
- DDoS (unintentional)

Countermeasures include:

- MTC Device anti-theft and Disablement System; this is covered in Section 7.9;
- MTC application security mechanisms as specified by 3GPP; this is covered in Section 7.6;
- High-availability MTC network design; this is covered in Section 7.17:
    - to enable and sustain a mass of machine UEs in a particular area to transmit data almost simultaneously;
    - to design the MTC system to spread over time the peaks in the signalling traffic;
    - to enforce a maximum rate for the data sent/received by the group of MTC devices;
    - to apply congestion control mechanisms to MTC traffic.

5.3 Internet of Things (IoT)

It is expected that public safety agencies will make use of the Internet of Things (IoT) technology via a network of microphones, videos, and a wide variety of other sensors to enhance public safety and provide critical visibility to public safety users.

IoT in essence requires a Machine-to-Machine (M2M) communication network to interconnect the M2M devices with the centralized M2M server where “raw data” collected by devices is processed, or sent for processing. M2M devices are also foreseen to provide local processing in some cases. M2M is referred to as Machine Type Communication (MTC) within the 3GPP, and as such, both terms are interchangeable within this document. A MTC network is typically composed of wireless and wireline technologies that allow MTC devices, also called MTC endpoints, to interconnect with MTC servers in the cloud. For example, MTC devices can either be wired directly to the local area network (LAN), be connected over wireless LAN or other short range radio access technologies (RAT) such as Bluetooth, IEEE 802.15.4 or emerging 802.11 technologies, or directly to the wireless wide area networks (WAN) if the MTC endpoints have that capability. When connected to wireless LAN or short range technologies, access to the cloud servers is either over a wireline network or a WAN, usually a cellular network, via MTC gateways.

In the context of the PSBN within this document, the MTC local connectivity consists of:

- A set of MTC endpoints comprised of the sensors that provide the “raw data,” and which can communicate locally (wirelessly or via a hardwired connection) to a MTC gateway;
- MTC gateway: providing connectivity between the MTC endpoints and the MTC cloud-based server.

MTC endpoints can be motion sensors, digital door-locks, automotive telematics systems, sensor-driven industrial control systems, and more. Endpoints gather measurements from the physical environment around them, and push that data in different formats typically via LAN or a cellular network to the MTC servers, receiving instructions or actions in return.

MTC endpoints have the following characteristics which have particular security vulnerabilities, or challenges associated to them:

- Low power consumption translating into limited cryptographic capabilities;
- Low cost, meaning devices with low processing and memory capabilities;
- Long life (>10 years) making it hard to manage security vulnerabilities over time;
- Being physically accessible to attackers;
- In some cases, no Internet Protocol (IP) capabilities to transfer data to the local MTC gateway, complicating the process of securing the end-to-end communication.

Threats include:

- Physical attacks
- Tampering
- Unauthorized access

Countermeasures include:

- Implementing authentication, confidentiality and integrity on the connectivity between MTC endpoints and the MTC gateway. This is covered in Section 7.5.
- Implementing authentication, confidentiality and integrity on the connectivity between MTC gateway and the MTC server. This is covered in Section 7.6.
- Hardening the MTC endpoints and the MTC gateway. This is covered in Section 7.14.

5.4 Radio Access Network (RAN)

The radio access network layer of the PSBN is composed of the following network elements:

- Macro-cell (eNodeB): outdoor cell with a large cell radius;
- Small-cell (eNodeB): functionally similar to a macro-cell, and thus identified by the same network function by 3GPP, it provides a smaller form factor, lower power and coverage area than a macro-cell; typically installed in easy-to-access and less secure physical locations;
- Femtocell (HeNodeB): designed to be installed on customer premises and typically limited to serve a closed subscriber group; 3GPP has specified a new functional element called the Home eNodeB referred to as H(e)NodeB, HeNodeB, or HeNB;
- Non-3GPP Access Point (e.g., WiFi);
- Relay Node: Relay Nodes (RN) are low power eNodeBs that provide enhanced coverage and capacity at cell edges;
- Deployable systems (deployable eNodeBs);
- Serving access network (3G or LTE) while roaming.

5.4.1 eNodeB

The radio interface between the UE and the serving eNodeB represents a significant point of attack in the PSBN. The vulnerabilities and threats associated with attacks on the radio interface include:

- Eavesdropping, Man in the Middle (MitM) attacks; possible if the user plane LTE traffic on the Uu interface[6] between the UE and the eNodeB is not encrypted;
- Denial of Service (DoS) via radio jamming by transmitting static and/or noise at high power levels across the PSBN Band14;[7]
- Rogue eNodeBs; although a rogue eNodeB cannot authenticate itself successfully to the UE, it can force a UE to downgrade to GSM, where significant weaknesses exist in GSM cryptographic algorithms;

[6] The Uu interface is the over-the-air interface between the UE and the eNodeB.

[7] The spectrum band designated for PSBN is designated by the 3GPP as Band 14. Specifically, the spectrum includes the PSBB (758–763 and 788–793 MHz) and the D Block (763–768 and 793–798 MHz) for a total of 20 MHz (758–768 MHz downlink and 788–798 uplink).

- Breach of privacy (device and identity tracking); a subscriber's permanent identity, the IMSI on the UICC or the IMEI on the device, is, in some unavoidable scenarios, sent in clear text over the air interface when a UE attaches to the LTE network.

The countermeasures against these threats include:

- Enabling cryptographic protection of the user plane; this is covered in Section 7.2;
- Network monitoring using Wireless Intrusion Detection and Prevention systems to identify wireless attacks quickly and neutralize impacts; this is covered in Section 7.15;
- Configuring the UEs to only attach to secure radio technologies such as 3G HSPA and LTE, i.e., "Use LTE or 3G only" option; this is covered in Section 7.8;
- 3GPP defines the Globally Unique Temporary UE Identity (GUTI) which unambiguously identifies the UE without revealing the UE or the user's permanent identity; GUTIs need to be implemented in a manner that they are periodically refreshed via the Non-Access Stratum (NAS) GUTI reallocation command to ensure that it is truly a temporary identifier;
- While complying with the maximum permissible handover delay, implementing to the extent possible the several handover authentication approaches to achieve secured seamless handovers between the 3GPP E-UTRAN and the non-3GPP access networks as specified by TS 33.402 [12]; this is covered in Section 7.2.

5.4.2 Small-cell and Femtocell

Small-cells and femtocells may be installed outside the secure locations of the PSBN sites. Femtocells can be installed on customer's premises and typically connect back to the core network via an internet connection provided by an Internet Service Provider (ISP). Installation of small-cells (eNodeBs) and femtocells (HeNodeBs) in unsecure locations are vulnerable to physical tampering allowing for unauthorized access to the network. In addition, the radio equipment and other electronics required to operate the eNodeB or HeNodeB may be physically destroyed. The threats associated with small-cells and femtocells include:

- Physical attack
- Breach of privacy

Countermeasures to these threats include:

- Hardening of the small-cell or femtocell; this is covered in Section 7.14;
- Implementing 3GPP specifications to provide authentication, confidentiality and integrity measures on the HeNodeB network access via IP Security (IPSec) established through a Security GateWay (SeGW); this is covered in Section 7.2.

5.4.3 Non-3GPP access point

The threats associated with the non-3GPP access points include:

- Eavesdropping, MitM attack; an eavesdropping attack is possible on unsecure or untrusted access networks.

Countermeasure includes:

- Implementing 3GPP security mechanisms during inter working between non-3GPP accesses (both trusted and untrusted) and the Evolved Packet System (EPS); this is covered in Section 7.2.

5.4.4 Relay Node (RN)

Relay Node (RN) was introduced in LTE Release 10 of the 3GPP standards to enable traffic/signalling forwarding between an eNodeB and UE to improve the coverage of high data rates, cell edge coverage and to extend coverage to heavily shadowed areas in the cell or areas beyond the cell range. It provides throughput enhancement especially for the cell edge users. The relay nodes are wirelessly connected to the radio access network via a Donor eNodeB (DeNodeB). The RN is connected to the DeNodeB via the Un[8] interface and UEs are connected to the RN via the Uu interface.

The introduction of a RN into the network introduces some additional security threats to E-UTRAN, namely:

- Impersonation of a RN to attack the UE(s) attached to the RN or attack the network
- Attacks on the Un interface between RN and DeNodeB
- Man in the Middle attack
- DoS attacks

Countermeasures to these threats include:

- Implementing 3GPP security mechanisms for Relay Node; this is covered in Section 7.2.

5.4.5 Deployable eNodeB in IOPS mode

A deployable eNodeB operates in connected mode when it has a backhaul connection with the PSBN macro network. In connected mode, the eNodeB security mechanisms described earlier in this section apply to the deployable eNodeB as well.

A deployable eNodeB can also operate in stand-alone mode, also called Isolated E-UTRAN Operations for Public Safety (IOPS) mode by 3GPP, when it does not have a backhaul connection to the PSBN macro network or has experienced a failure of the backhaul link. When a deployable eNodeB operates in IOPS mode, it provides local IP connectivity and public safety services to IOPS-enabled UEs via a local EPS.

Subscriber credentials are provisioned in all local Home Subscriber Servers (HSS) within the local EPSs supporting IOPS operation where the public safety authority requires that the UE be provided service in the event of a loss of backhaul communication. If one of these local HSSs was compromised by an attacker, for all subscribers whose credentials were stored in the compromised local HSS, the USIMs out in the field would have to be swapped and the subscriber credentials would have to be re-provisioned in all local HSSs.

[8] The Un interface is the over-the-air interface between the Relay Node (RN) and the Donor eNodeB (DeNodeB).

As described in Section 7.2, 3GPP defines a USIM application dedicated exclusively for IOPS operation which uses a distinct set of security credentials separate from those used for *normal* operation. These credentials are configured in the local HSS and in the UICC prior to the commencement of IOPS operation.

5.4.6 Serving access network (3G or LTE) while roaming

The threats associated with the serving access network while roaming include:

- Eavesdropping, MitM attack; an eavesdropping attack is possible on unsecure or untrusted access networks.

As countermeasures, particularly applicable when the user is roaming on a network that is not encrypting the user's traffic:

- The ciphering indicator feature alerting the user if voice or data calls are made over an unencrypted connection; this is covered in Section 7.8;
- In this case, using an end-to-end Mobile Virtual Private Network (MVPN) solution can provide strong authentication, integrity and confidentiality protection for user data; this is covered in Section 7.13.

5.5 Core network

The core network layer of the PSBN, which includes the Evolved Packet Core (EPC), is composed of the following network elements:

- Serving Gateway (S-GW)
- Packet Data Network Gateway (P-GW)
- Mobility Management Entity (MME)
- Policy and Charging Rules Function (PCRF)
- Home Subscriber Server (HSS)
- Authentication Centre (AuC)

The core network of the PSBN presents multiple network demarcation points toward other security domains whether those points are towards external networks or within the PSBN. PSBN network demarcation points include:

- PSBN E-UTRAN
- Network-to-Network Interconnection (NNI) with partners' networks such as FirstNet or national roaming partners
- Roaming interconnection to an IP eXchange (IPX) provider
- public safety agency networks
- Public internet
- Public Switched Telephone Network (PSTN)

All these network demarcation points carry some threats to the PSBN core network, where key security threats/risks include:

- Unauthorized access to services
- Denial of Service
- Unauthorized disclosure (eavesdropping)
- Threats to integrity

The PSBN must interconnect its authentication systems to allow PSBN users to access their services even when roaming. Unless security protocols are enabled by the visited network, (IPSec, IKE, EAP/TLS), the control plane traffic and the user plane traffic are neither encrypted nor is integrity protected between the visited E-UTRAN and the PSBN EPC. This leaves the traffic vulnerable to eavesdropping or modification.

DoS and Distributed DoS (DDoS) attacks can be launched on the network demarcation points of the core network targeting specific nodes of the PSBN. A large number of simultaneous signalling requests may prevent core network components (e.g., HSS) from functioning properly. Intruders may prevent user or signalling traffic from being transmitted on any system interface, whether wired or wireless, by inducing protocol failures. These protocol failures may themselves be induced by physical means.

Intruders may eavesdrop, modify, insert, replay, or delete user plane data or control plane data on any interface flowing through a PSBN demarcation point. Intruders may masquerade as a network element in order to intercept, modify, insert, replay, or delete user plane data or control plane data on any system interface, whether wired or wireless. Intruders may observe the time, rate, length, sources or destinations of messages on any system interface to obtain access to information.

Preventative measures include:

- Implementing Virtual Local Area Networks (VLANs) and secure IP protocols to limit or pre-empt damage by unauthorized access, eavesdropping, spoofing and other attacks; this is covered in Section 7.12;
- Implementing authorization, authentication, integrity and confidentiality protection mechanisms on interfaces between security domains to protect the core network interfaces; this is covered in Section 7.3;
- Implementing network monitoring via Intrusion Detection and Protection System (IDPS). This is covered in Section 7.15;
- Protecting the PSBN from traffic surges directed at any of the elements of the EPC via network load balancing and congestion control mechanisms. This is covered in Section 7.17.

5.6 Transport and IP

The Transport and IP components, or layers of the PSBN is composed of the following network elements:

IP Elements

- Router
- Aggregation routers/devices

- Firewall
- Domain Name System (DNS) servers
- Diameter Routing Agent (DRA) / Diameter Edge Agent (DEA)

Transport

- Backhaul Transport System (eNodeB-EPC)
- Backbone Transport System (between core network elements)

Key security threats/risks include:

- Eavesdropping
- DoS

If the LTE network is not using confidentiality protection on the backhaul interface, the communication being sent to and received from eNodeBs is vulnerable to eavesdropping. The same is true for backbone connections used between distant core network elements. Both backhaul and backbone transport resources could be provided by untrusted service providers, or be used across different security domains of the PSBN.

A DoS via poisoning of DNS cache is an attack in which the attacker breaks the process of discovering a service node through DNS by poisoning the DNS cache so that a fake IP or domain name is returned to the UE. The result is that the UE cannot register to the service network or is registered with a rogue server.

Countermeasures to such threats include:

- Encryption of the S1 interface to secure the backhaul connection; this is covered in Section 7.3;
- Encryption of the exposed interfaces between core network elements that make use of a backbone transport system; this is covered in Section 7.3;
- Use of static entries in DNS; this is covered in Section 7.12;
- Use of separate internal DNS (iDNS) and external DNS (eDNS); this is covered in Section 7.12;
- Use of IPsec for all telecom flows across security domains (control plane, user plane); this is covered in Section 7.12.

5.7 Network service

The Network service aspect of the PSBN is composed of the following network components, which typically reside within the domain of the cellular network and should not be hosted outside the PSBN. The following list is not exhaustive:

- IP Multimedia Sub-system (IMS);
- Voice over LTE (VoLTE) and Video over LTE (ViLTE) application servers;
- Short Message Service Center (SMSC) and Multi-Media Service Center (MMSC);
- enhanced Multimedia Broadcast / Multicast Service (eMBMS) servers;

- PSBN-hosted MTC servers;
- PSBN-hosted MVPN server;
- Proximity Service (ProSe) function;
- Mission-Critical Push-To-Talk (MCPTT), Mission-Critical Video (MCVideo), and Mission-Critical Data (MCData) servers;
- Group Communication servers.

Key security threats/risks include:

- Theft of service, for instance via a compromised UE;
- Eavesdropping attacks performed on both service-level signalling and media planes;
- DoS attacks saturating service resources by sending a massive number of malicious requests in a short period of time.

Countermeasures to these threats include:

- Enabling service-level security protocols (i.e., between client and server); this is covered in Section 7.6;
- Implementing strong UE and user authentication at the service level; this is covered in Sections 7.6 and 7.11;
- Implementing Security Gateways between security domains; this is covered in Section 7.3.

5.8 Application layer

The application layer of the PSBN is composed of the following network elements:

- USIM for USIM-based application clients
- UE for UE-based application clients
- PSBN-hosted application servers
- Service Delivery Platform (SDP) encompassing Application Programming Interface (API) and a Service Capability Exposure Function (SCEF)

Key security threats/risks include:

- Unauthorized access (applies to both user access and application access)
- Virus and malware
- DoS
- Application Programming Interface (API) hacking
- Eavesdropping and spoofing

Since applications are typically hosted on networked servers running conventional operating systems, they are vulnerable to the same type of threats that enterprise businesses experience such as viruses, or worms' proliferation that ultimately can impact uptime and service availability for the PSBN.

DoS attack risks exist in both the control plane and the user plane. Any device that uses IP to communicate with the application servers or entities can send control plane traffic to this layer and launch an attack. In the user plane, a flood of data packets that consume a network's entire bandwidth can cause it to underperform. This type of flood can occur using any of the available network protocols such as a Transmission Control Protocol (TCP) flood (also known as a synchronization "SYN" flood) or a User Datagram Protocol (UDP) flood, among several others.

The PSBN capabilities and services will expose specific APIs to enable new applications. These APIs, services, and applications will allow for new capabilities such as dynamic control of Quality of Service, priority, pre-emption (QPP), local control, agency home page status, and public safety analytics. APIs give developers—both legitimate developers and potential system hackers—more finely grained access into an application than a typical Web application.

Eavesdropping and spoofing attacks include (i) identity attacks that exploit authentication, authorization, and session tracking, and (ii) Man in the Middle (MitM) attacks that intercept legitimate transactions and exploit unsigned and/or unencrypted data.

Countermeasures to these threats include:

- Strong User Access and Control Management (for both user-to-application and application-to-network); this is covered in Section 7.11;
- Network protocol security at the application layer; this is covered in Sections 7.6 and 7.10;
- Device Security Solution; this is covered in Section 7.10;
- Application server hardening; this is covered in Section 7.14;
- High-availability and resilient application server; this is covered in Section 7.17;
- Applications ecosystem security.

5.9 Telecommunications Management Network

Among others, the Telecommunications Management Network (TMN) layer of the PSBN is composed of the following network elements:

- Operations Support Systems (OSS):
  - Element Management System (EMS);
  - Network Management System (NMS).
- Business Support Systems (BSS):
  - Billing Systems;
  - SIM Over-The-Air (SIM-OTA), Mobile Application Management (MAM), and Mobile Device Management (MDM);

- Customer Relationship Management (CRM);
- Legal Intercept;
- Service Provisioning System.

The TMN is a vital part of an operational cellular network, providing remote access into geographically distributed components of the network. The TMN interfaces provide quick access to network components, allowing the network operator to manage network elements from one central location. Poor design and lack of hardening of these TMN interfaces create a serious security vulnerabilities and associated risks to the networks operational stability. Unauthorized access to management interfaces can potentially allow malicious and unintentional misconfigurations of critical network systems. Attacks may be launched from inside the network by insiders and also from external sources such as hackers, leading to risks such as masquerading, data loss or theft, eavesdropping and repudiation.

Security threats commonly associated with the TMN infrastructure are related to both human-to-server and server-to-server communication, as follows:

- Unauthorized access by a manager application to an agent application, causing unexpected disclosure of information and even damage to agent application and the Network Elements under its control;
- Entity masquerade where one entity can masquerade as a client or a server;
- Loss or corruption of information including bulk data;
- Eavesdropping on sensitive management information;
- Repudiation, where a client and/or a manager denies the fact that it has sent or received some management information.

Countermeasures to these threats include:

- Implement strong User Access and Control Management on TMN systems and interfaces; this is covered in Section 7.11;
- Implement 3GPP security mechanisms on the management plane via secure protocols; this is covered in Section 7.7;
- Implement security monitoring and alarming on TMN systems to track and log user activity, to trigger response, and to perform forensic analysis; this is covered in Section 7.16;
- Harden TMN servers; this is covered in Section 7.14.

6 ITU security framework

The PSBN is expected to be designed with integrated security measures for all dimensions, layers, and planes for all facets of the system that are articulated in the ITU “Security architecture for systems providing end-to-end communications” [7] and as illustrated in Figure 3.

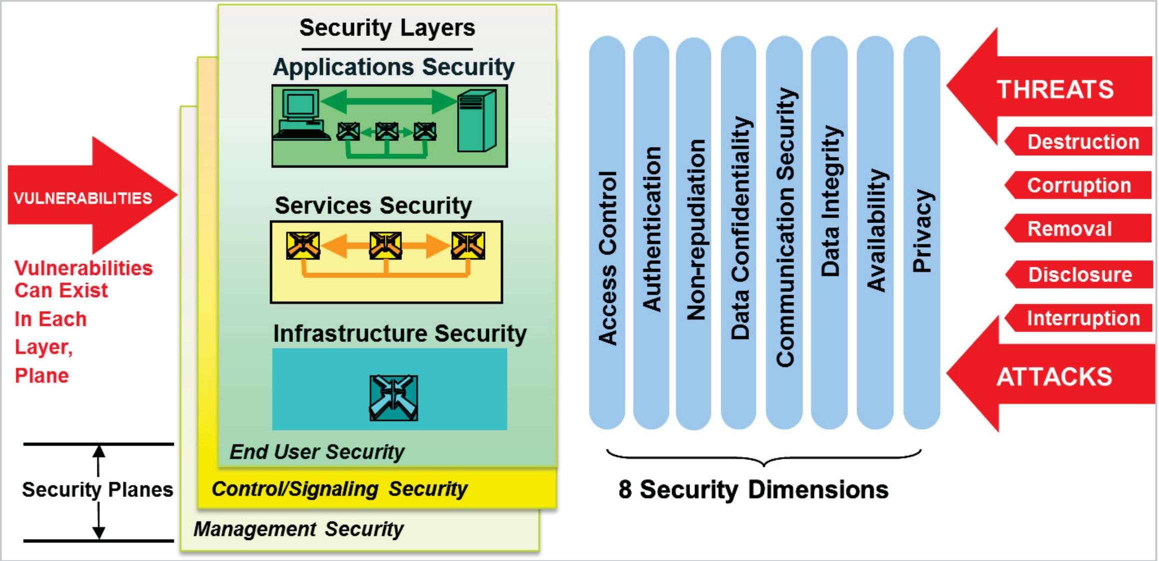


Figure 3: *Security architecture according to ITU X.805 Recommendation [7].*

6.1 Security dimensions

A security dimension is a set of security measures designed to address a particular aspect of network security and information security. There are eight such sets that protect against the five security threats as shown in Figure 3. The security measures associated with the eight dimensions apply to: (i) applications that are served across the PSBN, (ii) services provided by the PSBN, and (iii) the infrastructure itself. In addition, there are three security planes that represent the following types of information carried over the PSBN: (i) end-user information, (ii) control/signalling information, which is typically not user-accessible, and (iii) management information, which is accessible to network administrators. The eight security dimensions are summarized below.

6.1.1 Access control

The security measures that fall under this dimension protect against unauthorized use of the PSBN resources, access to information networks, configuration control functions, and performance and status information. Access control also applies to physical security to ensure that only authorized personnel may gain entry to the PSBN facilities.

6.1.2 Authentication

The set of measures under the dimension of “authentication” are intended to confirm the identities of the persons, machines, and applications that request access to network resources and information networks. Authentication security measures also assign a confidence level to the determination of the identity. Access control measures may use the confidence level factor as one of the criteria to either grant or deny access to the specific request. The US National Institute of Standards and Technology (NIST) published a guideline on assigning a confidence factor to the identity of users by electronic sign-on systems. An assurance level is designated by one of four categories listed below, as extracted from NIST SP 800-63 [13]:

Level 1—Although there is no identity-proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed.

Level 2—Provides single factor remote network authentication. At Level 2, identity-proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. For single factor authentication, Memorized Secret Tokens, Pre-Registered Knowledge Tokens, Look-up Secret Tokens, Out of Band Tokens, and Single Factor One-Time Password Devices are allowed.

Level 3—Provides multi-factor remote network authentication. At least two authentication factors are required. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol. Multi-factor Software Cryptographic Tokens are allowed.

Level 4—Intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. At this level, in-person identity-proofing is required. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed. The token is required to be a hardware cryptographic module validated at Federal Information Processing Standard (FIPS) 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security.

6.1.3 Non-repudiation

The set of security measures under the dimension of “non-repudiation” are intended to provide undeniable confirmation of any action that was taken by network administrators, or any services that were accessed by users. If pertinent, time and location would also be logged. The security measures would ensure that the logs cannot be tampered with and that the robustness of the non-repudiation measures can be trusted to preserve evidence of the actions that were taken.

6.1.4 Data confidentiality

The set of security measures that pertain to “confidentiality” are intended to protect data from unauthorized disclosure. Encrypting the data is a common way to impart a measure of confidentiality. Encryption processes plaintext into ciphertext in such a way that an eavesdropper who has captured the ciphertext cannot easily extract the plaintext.

6.1.5 Communication security

The set of security measures associated with "communication security" are intended to prevent information from being diverted or intercepted while in transit over the PSBN.

6.1.6 Data integrity

The set of security measures under the dimension of "data integrity" are intended to protect data against unauthorized modification, deletion, and replication. If such tampering should occur, data security measures would be able to detect that occurrence and signal the proper alert.

6.1.7 Availability

The set of security measures associated with "availability" are intended to ensure that the services offered over the PSBN are accessible to authorized users when they need them. This includes measures to harden the PSBN against service disruption due to disasters. The ability to restore services in case of a catastrophic event is part of the set of measures to maintain a high level of availability.

6.1.8 Privacy

The set of measures that are associated with "privacy" are intended to protect information, patterns of usage, location, etc., from being revealed to observers who aren't authorized to know this information. The security measures would prevent such insight to be gained from the observation of network activities.

6.2 Security planes

The International Telecommunication Union (ITU) X.805 Recommendation [7] categorizes information into three distinct planes as summarized in Table 1:

Table 1: *ITU security framework—security planes.*

Plane	Description
End-User	The End-User plane represents the information that a user originates or consumes.
Control	The control plane represents information that the network creates or uses to initiate/terminate sessions, route traffic, and modulate the priority of sessions, such as Radio Resource Request and various acknowledgments.
Management	The management plane represents information that is used to monitor the status of the network. It enables the workflow processes for moving information from one point to another in response to stimulus. An example of the latter is the process to provision services for users, which involves checking availability of bandwidth, checking authorization level, marking the bandwidth as having been allocated upon granting access, collecting usage records, etc.

The notion of security planes implies that security requirements can be defined for each plane independently. Furthermore, the separation of security planes according to the type of information carried over the network allows security measures to be applied that isolate the addressing space of each layer so attacks against one plane are less likely to affect the security posture of the other two planes.

6.3 Security threats

The ITU X.805 Recommendation lists five threat categories described in Table 2:

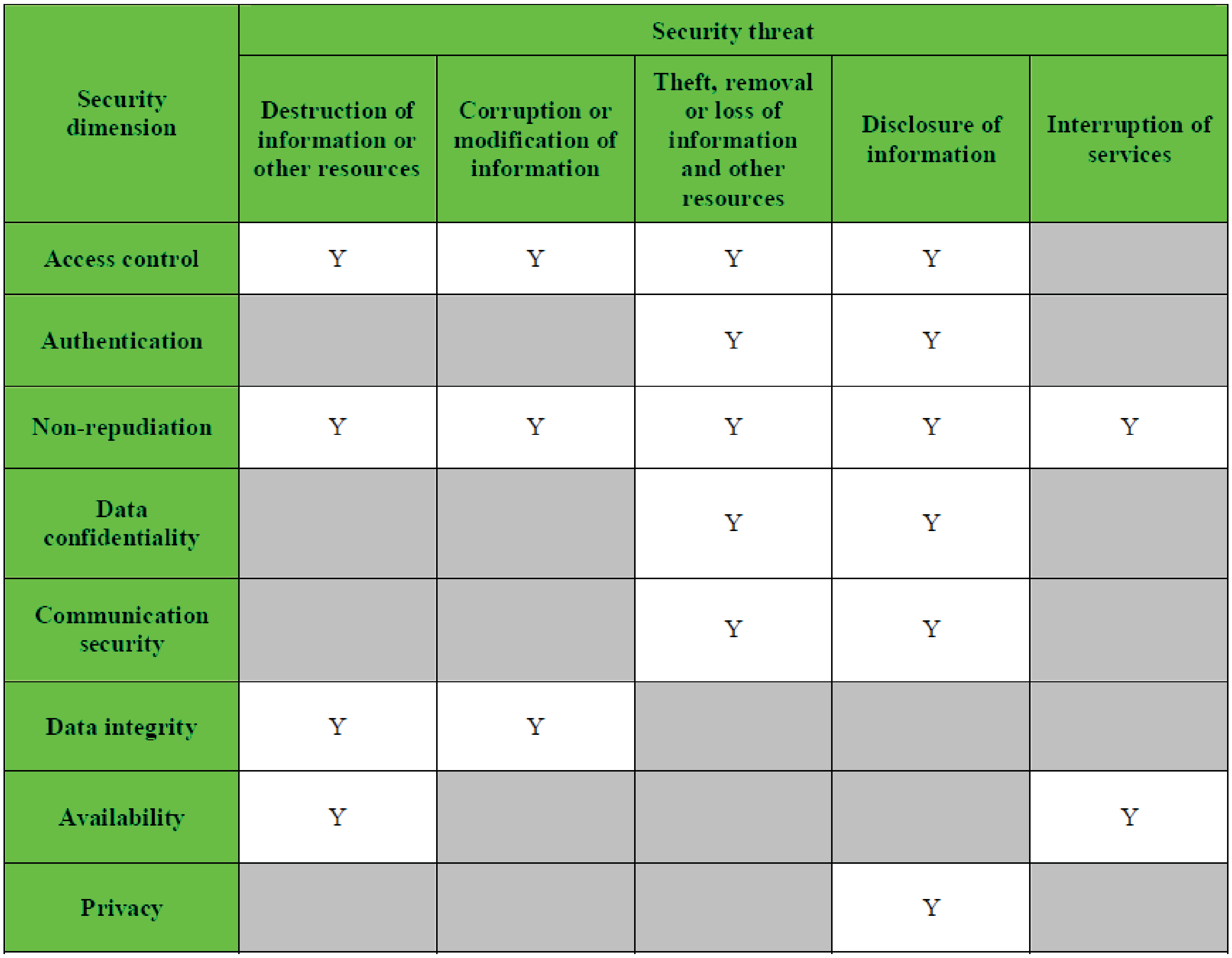
Table 2: *ITU security framework—threat categories.*

Threat	Description
Destruction	Destruction of information or other resources: the destruction of information or communications such that it can no longer be used. This attacks the availability of information. An example would be erasing the contents of a database.
Corruption	Corruption or modification of information: changing the information such that it is no longer accurate. This is attacking the integrity of the information. Examples would be an unauthorized modification of a database record or rendering a message unintelligible. Note that someone authorized to access the records or message file may not have permission to undertake the change action. Hence, security measures need to consider the threat of malicious intent by a person who is authorized to manipulate records and files.
Removal	Theft of information and other resources: An example would be downloading of personal medical records by persons that are not authorized to have this information, or inappropriate downloads of information by persons that may otherwise be authorized to access it. Theft does not necessarily destroy the information at the source.
Disclosure	Disclosure of information: releasing confidential information. An example is exposing the medical records of individuals. Note that theft does not automatically result in exposure of the information but it may be stolen under threat of exposure pending a ransom. This attacks the confidentiality of information.
Interruption	Interruption of services: interfering with communications such that authorized users cannot use the network when needed. An example would be jamming the radio access network using an RF interference source, where the source could be a compromised User Equipment (UE). Another example would be disconnecting the back-up power system to a cell site such that when mains power is lost, the back-up is unavailable. This attacks the availability of information.

The ITU X.805 Recommendations [7] illustrate an example of a possible mapping of threats to the security dimensions as shown in Table 3. The "Y" at the intersections of security threats and security dimensions, indicate where the security threats apply. This implies that for the intersections that are blank, the associated security threats would not apply. The actual mapping of threats to security dimensions for the PSBN would be done as part of a security risk assessment of the PSBN. The Communications Security Establishment Canada (CSEC) has published a guideline [14] on how to conduct a risk assessment of communications networks in order to determine what security measures (controls) should be implemented.

There are many standards and documents that describe the attacks and risks in telecommunications networks. As mentioned earlier, this paper uses the security framework defined by the ITU-T X.800 [15] and X.805 [7] recommendations.

Table 3: *ITU X.800 security threat versus security dimension (source: ITU [15]).*



Security dimension	Security threat				
	Destruction of information or other resources	Corruption or modification of information	Theft, removal or loss of information and other resources	Disclosure of information	Interruption of services
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data confidentiality			Y	Y	
Communication security			Y	Y	
Data integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

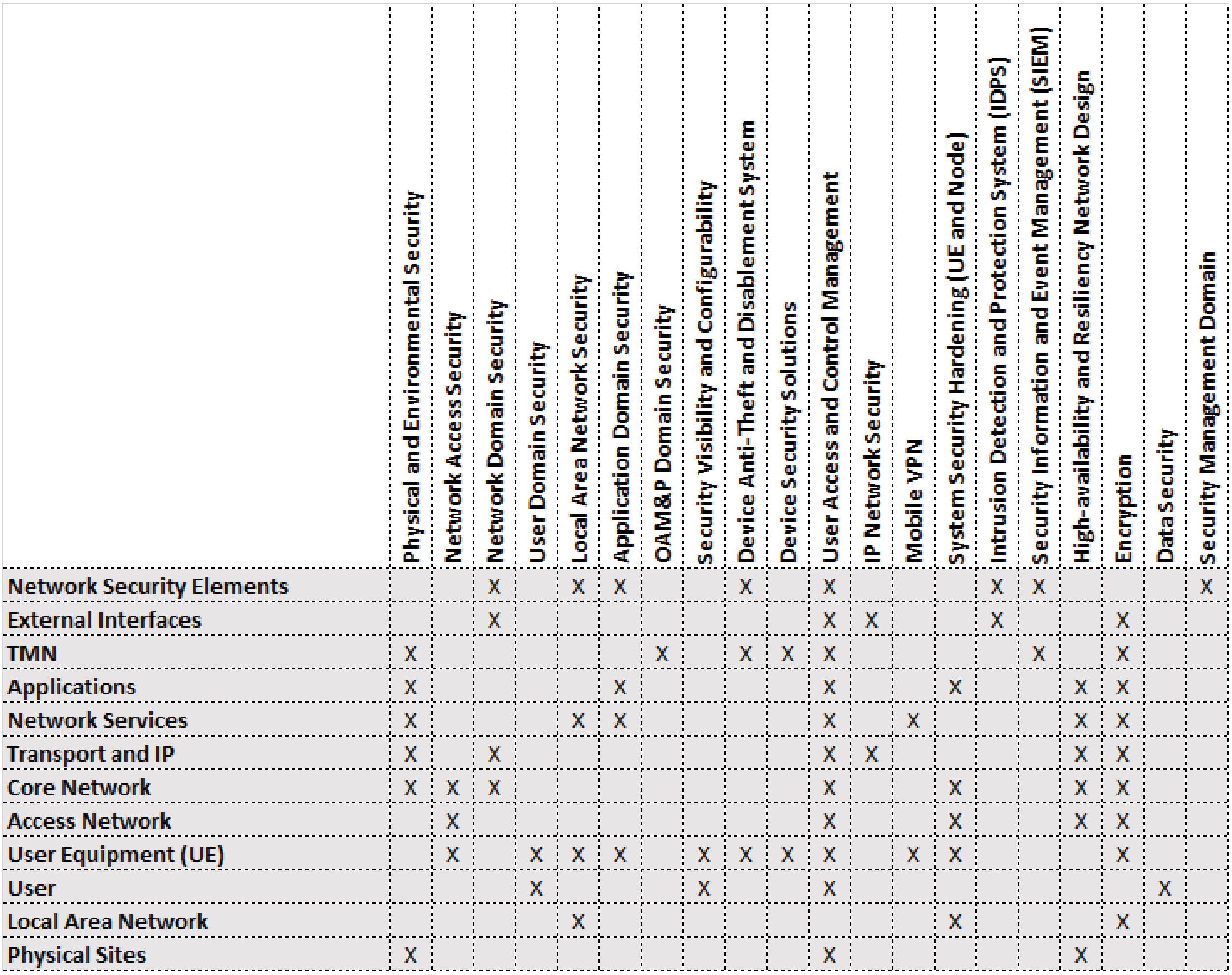
7 PSBN security architecture and considerations

A security feature is a service capability that meets one or several security requirements. A security mechanism is an element that is used to realize a security feature. All security features and security mechanisms taken together form the security architecture. An example of a security feature is user data confidentiality. A security mechanism that may be used to implement that feature is a stream cipher using a derived cipher key.

This section defines the security architecture, i.e., the security features and the security mechanisms, for the PSBN, and contains the minimum set of security considerations for the PSBN. The security considerations contained herein can potentially address the security risks and deliver the countermeasures described in Section 4. In order to determine which security features and mechanisms apply to which PSBN network components, Figure 4 has been created by the authors of this report. It shows a high-level coverage grid of the PSBN security architecture, where an “x” indicates which of the security features and mechanisms described in this section provide security for the different PSBN network components.

It is possible that a security risk assessment would identify additional requirements for the PSBN—applied at large or applied selectively in order to satisfy the need for a heightened security posture for specific groups of users. The considerations stated in this document should, therefore, be considered as the minimum set of security measures and may be augmented following a formal risk assessment.

Many of the security considerations listed in this section are taken directly from similar work conducted by other organizations such as the National Public Safety Telecommunications Council (NPSTC) [16], [17].



	Physical and Environmental Security	Network Access Security	Network Domain Security	User Domain Security	Local Area Network Security	Application Domain Security	OAM&P Domain Security	Security Visibility and Configurability	Device Anti-Theft and Disablement System	Device Security Solutions	User Access and Control Management	IP Network Security	Mobile VPN	System Security Hardening (UE and Node)	Intrusion Detection and Protection System (IDPS)	Security Information and Event Management (SIEM)	High-availability and Resiliency Network Design	Encryption	Data Security	Security Management Domain
Network Security Elements			X		X	X			X		X				X	X				X
External Interfaces			X								X	X			X			X		
TMN	X						X		X	X	X					X		X		
Applications	X					X					X			X			X	X		
Network Services	X				X	X					X		X				X	X		
Transport and IP	X		X								X	X					X	X		
Core Network	X	X	X								X			X			X	X		
Access Network		X									X			X			X	X		
User Equipment (UE)		X		X	X	X		X	X	X	X		X	X				X		
User				X				X			X								X	
Local Area Network					X									X				X		
Physical Sites	X										X						X			

Figure 4: *PSBN security architecture—coverage grid.*

Table 4 below presents the main protocol-based security specifications for the PSBN interfaces as discussed in this document. All references to “TS xx-xxx” specifications are from the 3GPP.

Table 4: *PSBN interfaces—security specifications.*

Network Layer	Entity A	Entity B	Interface	Specifications
UE				
	USIM	ME		TS 33.187 [18] TS 22.022 [19]
	USIM	SIM-OTA		TS 33.102 [20] TS 33.110 [21] TS 33.116 [22]
	User	USIM		TS 31.101 [23]
LAN				
	Endpoint	GW		TS 33.259 [24]
WLAN				
	UE	WLAN		TS 33.402 [12]
	UE	WLAN		IEEE 802.11i [25]

Network Layer	Entity A	Entity B	Interface	Specifications
3G RAN				
	UE	3G RAN		TS 33.102 [20]
LTE RAN				
	UE	eNB	Uu	TS 33.401 [26]
	eNB	eNB	X2	
	UE	MME	S1-MME	
	HeNB	SeGW		TS 33.320 [27]
Security Domains				
	SeGW	SeGW	Za	TS 33.210 [28] TS 33.310 [29]
	SS7-SeGW	SS7-SeGW		TS 33.204 [30]
IMS				
	UE	P-CSCF	Gm	TS 33.203 [31]
	UE	IMS-AGW		TS 33.328 [32]
	UE	Presence Server	Ut	TS 33.141 [33]
MTC				
	UE	HSE (Home Security Endpoint)		TS 33.163 [34]
	UE	MTC-AS		TS 33.187 [18]
	UE	SCS		
	MTC-IWF	SCS	Tsp	
	MME	SCEF	T6a	
Mission Critical Applications				
	User	MCPTT Server		TS 33.180 [35]
	User	MCData Server		
	User	MCData Server		
	UE (MC)	UE (MC)		
	MCPTT Server	IWF	IWF-1/2/3	TS 23.283 [36]
Proximity Service (ProSe) Application				
	ProSeApp	ProSeAS	PC1	TS 33.303 [37]
	ProSeFunction	ProSeAS	PC2	
	ProSeUE	ProSeFunction	PC3	
	ProSeFunction	HSS	PC4a	
	ProSeFunction	SLP	PC4b	
	ProSeUE	ProSeUE	PC5	
	ProSeFunction	ProSeFunction	PC6	
	HProSeFunction	VProSeFunction	PC7	
	ProSeUE	ProSeKMS	PC8	
MBMS				
	UE	BM-SC (NAF)		TS 33.246 [38]
GENERIC CLIENT-SERVER APPLICATION				
	UE	NAF	Ua	TS 33.220 [39]
	UE	BSF	Ub	TS 33.222 [40] TS 33.223 [41] TS 33.224 [42]
	UE	PKI	Ua	TS 33.221 [43]
Service Delivery Platform (SDP)				
	CAPIF	API Invoker	CAPIF-1e/2e	TS 23.222 [44]
OSS				
	EMS	NMS	Itf-N Type 2	TS 32.371 [45] TS 32.372 [46] TS 32.376 [47]
	UE	MDM/MAM		OMA DM Security [48]

7.1 Physical and environmental security

7.1.1 Physical security

Physical security is critical to security planning for any information or telecommunications systems. Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources. Physical security involves the use of multiple layers of interdependent systems which include Closed Circuit Video Equipment (CCVE) surveillance, security guards, protective barriers, locks, access control protocols, and many other techniques. Physical security systems should be capable of monitoring alarms, centrally displaying and reporting the alarm status of the entire system and all sub-components, and forwarding critical alarm notifications to appropriate personnel within the Network Operations Center (NOC) or Security Operations Center (SOC).

The PSBN physical security solution should take into consideration the following access security elements:

- Access control to and within a facility
- Monitoring, recording and alarming of activity within a facility to include egress/ingress
- Movement activity within a facility after hours or in restricted areas
- Building door alarms
- Closed Circuit Video Equipment (CCVE) surveillance systems
- Cabinet door alarms

The physical infrastructure of the PSBN must be protected from unauthorized access to enter the sites or various areas of a site. A main site such as a Network Management Centre (NMC) or data centre may have multiple secure zones. Figure 5 illustrates an example of a site that contains areas where different levels of authorizations are required depending on which zone one wishes to access. The Treasury Board of Canada has published a guideline for implementing physical access controls [49].

Access control security measures address the ability to access the facilities of the PSBN and the network elements themselves.

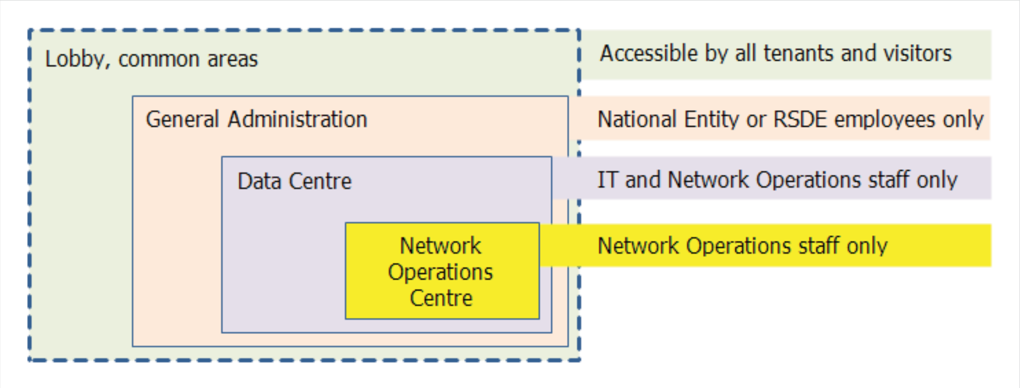

Lobby, common areas
General Administration
Data Centre
Network Operations Centre
Accessible by all tenants and visitors
National Entity or RSDE employees only
IT and Network Operations staff only
Network Operations staff only

Figure 5: *Example of a site containing multiple security zones with progressively more restrictive access requirements.*

7.1.2 Site hardening

Site hardening is critical to security planning for any information and telecommunications systems. The PSBN facilities should follow public-safety grade guidelines in site hardening so that equipment is protected from disruptions caused by failures in supporting utilities such as Heating, Ventilation, and Air Conditioning (HVAC) and power supply, as well as from damage from fire, flood, wind, earthquake, ice storm, extreme temperatures, or explosion. Facilities to be hardened shall include antenna support structure, outdoor equipment shelters, and buildings.

There are a number of standards that apply to the construction and protection of physical sites [16]. Some are intended for commercial communications sites, while others contain more stringent requirements for life-safety applications. The NPSTC report on Public-Safety Grade includes a contribution from the Association of Public Safety Communications Officials (APCO) on site hardening [16]. The dimensions of site hardening that are recommended in that report cover:

- Physical security: site perimeter security, access control to the site, cable feeds for power and communications, fuel storage;
- Antenna support structures: guy wires, lightning protection and grounding;
- Equipment enclosures: shelters, cabinets;
- Climate control systems;
- Power source: redundancy, battery system, generator, transfer switch;
- Monitoring and alarms: intrusion detection, status monitoring, actuators, cameras, siren;
- Tolerance to wildfires (especially rural/remote sites);
- Avoid flood-prone areas, elevate the site, ensure rapid drainage;
- Tolerance to wind forces;
- Tolerance to ice build-up;
- Tolerance to seismic events;
- Autonomous operation for extended periods in case of power failure.

7.1.3 Environmental security

Environmental security systems should be capable of monitoring alarms, centrally displaying and reporting the alarm status of all environmental security elements, and forwarding critical alarm notifications to appropriate personnel within the NOC or SOC. The following environmental events should be considered:

- Power and generator failure;
- Fire and smoke detection;
- Humidity and temperature detection;
- Heating, ventilation, and air conditioning system failure or degradation;

- Low generator fuel;
- Low battery.

Furthermore, on the exterior of the sites there may be vulnerabilities that need to be addressed such as power feeds that are easily detectable and/or accessible.

This subsection addresses the security considerations with regards to PSBN premises and equipment. It does not cover logging the instances when services and applications are accessed by end-users. It is assumed that each EUA would implement suitable mechanisms to record access-events by users accessing their premises and equipment.

SC-7.1.1 The PSBN SHALL support multi-level access controls to restrict access to the physical infrastructure of the PSBN according to the relevant security policies adopted by the operator of the PSBN and the EUAs.

SC-7.1.2 The PSBN SHALL provide administrators the ability to monitor alarms and other status indicators of the PSBN sites in their respective jurisdictions.

SC-7.1.3 PSBN sites SHALL be equipped with physical and/or electronic means to detect, monitor, and deter unauthorized entry.

SC-7.1.4 The PSBN SHALL record entry and exit times, by location, of all personnel going into and coming out of PSBN facilities.

SC-7.1.5 PSBN sites SHALL be equipped with physical and/or electronic means to detect, monitor, and alarm on critical environmental indicators.

SC-7.1.6 All alarms and monitoring tools SHALL be connected and monitored by the Security Operations Center.

SC-7.1.7 The PSBN SHOULD follow NPSTC's recommendations and requirements on Public-Safety Grade Systems and Facilities.

7.2 Network access security

The Network access security is a set of security features that provide public safety users with secure access to the PSBN services by protecting the radio air interface.

The UE interfaces (over-the-air radio interfaces) to either the eNodeB or EPS arethe most exposed interfaces and therefore represent heightened security vulnerability. In order to ensure interoperable communication between multiple vendors of infrastructure and device equipment, compliance and certification testing to 3GPP security specifications is necessary.

3GPP specifications have defined a suite of security related specifications for LTE systems. The following 3GPP specifications and reports provide authentication, confidentiality and integrity measures on 3G, LTE and non-3GPP network access.

7.2.1 LTE (eNodeB)

3GPP TS 33.401 [26] and related documents define the security architecture for LTE. It provides authentication, confidentiality and integrity protection on the air interface for both the UE-eNodeB and the UE-MME interfaces. It further recommends protection for the control, user and management planes at the transport network layer of the EPS as per TS 33.210 [28] with security services that include integrity, confidentiality and anti-replay.

Key functions that implement network access security for LTE are described in the following table:

Table 5: *Key functions of network access security.*

Function	Description
Authentication	The UE/USIM and the PSBN mutually authenticate each other through the use of a cryptographic authentication algorithm that relies on shared key material in both the UE and the HSS. To perform this authentication, both the USIM and the HSS must agree on the same authentication algorithm and share a common set of keys.
Access Control	The eNodeB ensures that only authenticated UEs are permitted to transmit user data to the eNodeB. UEs that do not successfully authenticate will be prevented from requesting resources from the network to transmit user data.
Non-Repudiation	Successful authentication by a UE proves to the LTE network that the device has possession of the physical USIM. USIMs are manufactured utilizing strong physical security techniques to protect the keys used for authentication.
Data Confidentiality and Privacy	To ensure that information is not disclosed to any unauthorized users via the LTE air interface, both control plane and user plane traffic can be encrypted utilizing 128-bit Advanced Encryption Standard (AES). Enabling cryptographic protection of the user plane traffic over the Uu interface is performed via the UPenc key at the Packet Data Convergence Protocol (PDCP) layer as per TS 33.401- 5.1.3.1 [26].
Data Integrity	The 3GPP defines integrity algorithms for all UE-eNodeB and UE-MME signalling messages.

7.2.2 LTE Relay Node

Relay Nodes (RN) introduce security challenges that are addressed in Annex D of TS 33.401 [26].

7.2.3 Femtocell (HeNodeB)

3GPP TS 33.320 [27] specifies the security architecture for the Home eNode Bs (HeNodeB) sub-system. This includes security requirements on HeNodeBs, and other HeNodeB-associated network nodes (e.g., SeGW and HeNodeB management system), as well as the procedures and features which are provided to meet those requirements. It provides device validation, authentication, authorization; protection of the management plane between the HeNodeB and HeNodeB management system; protection of the user plane and control plane traffic between the HeNodeB and the SeGW.

7.2.4 LTE deployables

To provide voice, video, and data communication service for public safety officers who are out of LTE network coverage, public safety authorities may deploy a dedicated eNodeB(s) for nearby public safety UEs beyond what is provided by Proximity Services in UE-to-UE direct communication mode.

Alternatively, where an unexpected incident interrupts the backhaul and/or the link(s) between the eNodeBs, it is also important to ensure the ability of public safety users to communicate. If such a situation arises the eNodeBs are expected to provide isolated operation with rapid dynamic reconfiguration of the system in support of mission critical operations. Deployables can operate in different network states, or modes as described in Table 6.

Table 6: *PSBN deployable system mode of operation.*

Mode	Description
Connected	Deployables that are operating in connected mode have a backhaul connection with the PSBN macro network. Therefore, connected mode operations allow a full extension of PSBN services to first responders.
Stand Alone	Deployables that are operating in stand-alone mode do not have a backhaul connection to the PSBN macro network or have experienced a failure of the backhaul link. Deployables may be activated in stand-alone mode to support a localized public safety mission that does not require services from the PSBN core. Those services would be provided by local application servers on the deployable. 3GPP has developed requirements for the stand alone mode, which is referred to as Isolated E-UTRAN Operations for Public Safety or “IOPS.” [50]
Cluster	Certain emergency incidents span large geographic areas in which a single deployable may not provide sufficient coverage for the incident area. This may require the activation of two or more deployables. This simultaneous use of more than one deployable is called Cluster Operations. Deployable clusters may operate with or without a backhaul connection to the PSBN macro network.

Deployables in connected mode shall support the same security features and mechanisms as an eNodeB.

For deployables in stand-alone or disconnected mode, 3GPP specifies that a USIM application be dedicated exclusively for IOPS mode. LTE security procedures for IOPS networks are described in 3GPP TS 33.401 Annex F. The adopted mechanism for *subscriber key separation* is transparent to MEs, eNodeBs, and MMEs.

The USIM application dedicated exclusively for IOPS operation, in an IOPS-enabled UE, has a distinct set of security credentials which contains at least:

- A permanent key K (uniquely assigned for IOPS operation)
- The Public Land Mobile Network (PLMN) identity assigned for IOPS network operation
- An IMSI (uniquely assigned for IOPS operation)
- Access Class status of 11 or 15 (subject to regional/national regulatory requirements and operator policy)

These credentials are provisioned in all Local HSSs within the Local EPSs supporting IOPS operation where the public safety authority requires that the UE be provided service in the event of a loss of backhaul communication.

Storage of the IOPS network security credential set in the Local HSS is only performed for UEs authorized for operation in the IOPS network.

In order to minimize the impact of a compromised local HSS supporting IOPS operations, 3GPP TS 33.401 Annex F recommends that the credentials for a given IOPS-enabled UE be different across all local HSSs on which the UE is authorized access.

This is done by using a key derivation function that derives the IOPS-specific UE credentials using:

- **The UE master key for IOPS operations**, which is provisioned only on the IOPS USIM and not in the local HSSs;
- **The local HSS identification number ranging from 1 to 256 maximum**; if the number of possible local HSSs exceeds 256, then the local HSSs have to be segregated into sub-classes where the same identification number (and therefore the same UE credentials) is used;
- **A configurable USIM parameter that is specific to the HSS identification number**; this parameter is configured in the IOPS-enabled UE and can be updated/incremented via SIM-OTA (in case the local HSS has been compromised); this allows the re-use of the HSS identification number even after the local HSS has been compromised.

If a local HSS is compromised, all UE credentials provisioned in the compromised local HSS have to be re-configured as follows:

- For all compromised UEs, the configurable USIM parameter specific to the identification number of the compromised local HSS has to be updated/incremented on their IOPS USIM via SIM-OTA; this may require coordination among RSDEs;
- All local HSSs (whether within one or multiple RSDEs) that were configured with the compromised UEs and that were bearing the same identification number as the compromised HSS one have to be re-configured with the new credentials of the compromised UEs.

The definition of the key derivation function as well as the use of local HSS identification numbers shall be done in accordance with the applicable PSBN security policy. If a local HSS is compromised, the OTA updates of affected UEs and the reconfigurations of affected local HSSs need to be coordinated across all impacted RSDEs.

7.2.5 3G

3GPP TS 33.102 [20] defines 3G security procedures performed within 3G-capable networks. Those procedures are applicable when the UE is roaming on a 3G network.

7.2.6 Non-3GPP access

3GPP TS 33.402 [12] specifies the security architecture, i.e., authentication, confidentiality and integrity protection during inter-working between non-3GPP accesses like a Wireless Local Area Network (WLAN) e.g., WiFi access point (both trusted and untrusted) and the Evolved Packet System (EPS). It covers authentication, confidentiality and integrity protection between the UE and the Access Network Discovery and Selection Function (ANDSF). The ANDSF is an optional element in the 3GPP architecture and provides network access discovery, inter-system mobility policy, and assistance data as per operators' policy. The ANDSF is specified in TS 23.402 [51].

WiFi is a wireless local area network (WLAN) technology based on the IEEE 802.11 [52] series of standards. WiFi is used by most mobile devices as an alternative to cellular data. NIST Special Publication 800-153 [53] provides guidance for the installation, configuration, deployment, and security of WiFi, while NIST Special Publication 800-97 [54] provides guidelines on WiFi security via IEEE 802.11i [25].

SC-7.2.1 The PSBN SHALL assign radio resources only to authorized UE devices.

SC-7.2.2 The PSBN SHALL employ mechanisms to alert commercial service providers, sharing the PSBN spectrum, if a compromised commercial UE interferes with the operation of the PSBN, in accordance with relevant policies.

SC-7.2.3 The PSBN SHALL use a nationwide common security profile for user plane and control plane traffic between UEs, eNodeBs and MMEs, in accordance with TS 33.401 [26], with, as a minimum, the specification of ciphering algorithms (for example, use of Advanced Encryption Standard (AES)-128 vs. SNOW 3G [55]).

SC-7.2.4 To enable interoperable authentication, the USIM and HSS SHALL be capable of supporting the same key derivation functions, such as MILENAGE per TS 35.205 [56] and 35.206 [57].

SC-7.2.5 While roaming on 3G networks, PSBN UEs SHALL support/use a security profile for user plane and control plane traffic, in accordance with TS 33.102 [20].

SC-7.2.6 The PSBN SHALL use a nationwide common security profile for user plane and control plane traffic for non-3GPP access like WLAN between UEs and EPC as specified on TS 33.402 [12].

SC-7.2.7 The PSBN SHALL implement the best guidelines with regards to 802.11 security such as documented in NIST SP 800.97 [54] and 800.153 [53].

SC-7.2.8 PSBN LTE Relay Nodes SHALL support security measures as described in TS 33.401 [26] Annex D.

SC-7.2.9 PSBN HeNodeBs SHALL support security measures as described in TS 33.320 [27].

SC-7.2.10 PSBN deployables SHALL support security measures as described in TS 33.401 [26] Annex F.

SC-7.2.11 The deployables SHALL allow an authorized user to disable the unit in a secure manner in accordance with PSBN policy (e.g., during an emergency situation or compromise of the deployables security).

SC-7.2.12 The deployables SHALL provide security mechanisms through encryption or other means to protect information passing through the network in accordance with PSBN Security Policy.

SC-7.2.13 A deployable system SHALL comply with the same PSBN security requirements that are present on the macro network, including relevant components of physical, information, network, and communications security policies. This applies to all modes of operation, including when operating in, or transitioning to, Stand-Alone mode.

SC-7.2.14 The PSBN SHALL encrypt user traffic carried over a commercial network in accordance to relevant security policies.

7.3 Network domain security

Due to interconnect and roaming, the core network of the PSBN is exposed to other networks. Consequently, measures to securely allow partners to interconnect in a controlled way have to be deployed, without revealing confidential information. Network Domain Security (NDS) protects the core network (EPS) of the PSBN.

The NDS provides the set of security features that enable nodes in the PSBN to securely exchange user and signalling data, and to protect against attacks on the wireline portion of the PSBN. This domain covers protection of the network, network elements and all internal (control and signalling) traffic against security threats.

Typically, NDS features are implemented between security domains. A security domain is a network that is managed by a single administrative authority. Within a security domain, the same level of security and usage of security services are expected. Normally, a network operated by a single network operator or a single transit operator will constitute one security domain although an operator may, at will, subsection its network into separate sub-networks (internal security domains). The network elements can belong to a single operator (intra-operator) or to different operators (inter-operator).

External interfaces that would most likely delimit the security domain of the PSBN and therefore benefit from the NDS include:

- Network-to-Network Interface (NNI) with partner networks such as FirstNet, national roaming partner, or public safety agencies networks;
- Interfaces to IPX for roaming interfaces such as S8, S9 and S6a;

- Public network interfaces such the Public Switched Telephone Network (PSTN) and the internet.

Internal interfaces that could cross security domains within the PSBN include:

- EUTRAN-to-EPC interfaces such as S1;
- eNodeB Operations, Administration, and Maintenance (OAM) interfaces;
- Ud interface between application front ends (e.g., HSS, MC servers) and user data in the User Data Repository (UDR) as specified by TS 23.335 [58].

Although the LTE-based PSBN is an all IP network, it is assumed that the PSBN will need to support SS7-based interfaces via a PSBN-hosted Inter-Working Function (IWF) towards SS7-based 3G roaming partners' networks. Thus, in addition to IP-based security features, SS7-based security features are also required.

The Network Domain Security (NDS) features of the PSBN include 3GPP-based security protocols as well as industry best-practices and guidelines as documented by GSMA guidelines. The following 3GPP specifications provide data integrity, data origin authentication, anti-replay protection, confidentiality (optional), and limited protection against traffic flow analysis when confidentiality is applied.

As per TS 33.210 [28], the 3GPP system and its network domains shall be logically and physically divided into security domains in order to protect IP based control plane signalling. These security domains typically coincide with operator borders. The interface between different security domains is protected by Security Gateways (SeGW) on the borders of IP security domains, which are responsible for enforcing the security policy of a IP security domain towards other SeGWs in the destination IP security domain. All IP traffic to be protected via TS 33.210 shall pass through a SeGW before entering or leaving a security domain. Additional security measures implemented between security domains may include filtering policies and firewall functions, which are not specified in TS 33.210. In this document, such additional security features for IP infrastructure are covered in Section 7.12.

As per TS 33.210 [28], the interfaces between network entities are to be secured using IPsec security associations. The Za interface is used to interface two security domains and the Zb interface is used to interface between the various network entities within a single security domain.

The Za-interface covers all NDS/IP traffic between security domains. On this interface, authentication/integrity protection is mandatory and encryption is recommended. According to TS 33.210 [28] the provisioning of a Za interface applies only to signalling traffic. Integrity and confidentiality is ensured by an IPsec tunnel between the two security domains. The required IPsec ESP tunnel functionality is:

- integrity, authentication and anti-replay protection (mandatory)
- confidentiality by encryption (optional)

The Zb-interface is located between the SeGWs and network elements and between network elements within the same security domain. The Zb-interface is optional for implementation, but if implemented, authentication and integrity protection is always provided. The intra-domain Zb interface shall be encrypted unless it is in physically secure and fully trusted environment.

The network domain security of an NDS/IP-network does not extend to the user plane and consequently the security domains and the associated security gateways towards other domains do not encompass the user plane Gi-interface towards other, possibly external, IP networks.

TS 33.310 [29] complements TS 33.210 [28] to cover the authentication of network elements via a Public Key Infrastructure (PKI). The specification includes both the authentication of SeGWs at the corresponding Za-interfaces and the authentication between network elements and between network elements and SeGWs at the Zb-interface. Authentication of end entities (i.e., network entities and SeGWs) in the intra-operator domain is considered an internal issue for operators.

TS 33.204 [30] covers the security mechanisms and procedures necessary to protect all Transaction Capabilities Application Part (TCAP) user messages that are sent between different security domains. TCAP in the SS7 protocol are functions that control non-circuit-related information transfer between two or more signalling nodes via a signalling network. TCAP provides transaction capabilities to the Mobile Application Part (MAP) for mobile services. The complete set of enhancements and extensions to facilitate security protection for the TCAP protocol is termed TCAPsec and it covers transport security in the TCAP protocol itself and the security management procedures.

For TCAP where IP is used as the transport protocol, the use of SeGW as per TS 33.210 [28] and 33.310 [29] could partially achieve the same goals. However, whenever inter-working with networks using SS7-based transport is necessary, protection with TCAPsec shall be used. TCAPsec can be applied between different types of SS7 networks: between two PLMNs, between a PLMN and an SS7-carrier, or between two
SS7-carriers. The security services provided by TCAPsec are data integrity, data origin authentication, anti-replay protection, and confidentiality (optional).

Within the scope of the NDS features, the following GSMA documents provide further guidelines for security services and implementation.

GSMA IR.88 "LTE and EPC Roaming Guidelines" [59] outlines LTE related security measures and contains a toolbox for security for Diameter, Stream Control Transmission Protocol (SCTP), GPRS (General Packet Radio Service) Tunnelling Protocol (GTP) and interface specific recommendation, (e.g., S6a, S6d, S9, S8, Gy).

GSMA IR.34 "Guidelines for IPX Provider networks" [60] defines a GRX/IPX as a dedicated roaming/interworking network that is separate from the internet, and which is thought to be reliable and more secure than the internet. Thus, no extra security features are needed in the service provider to service provider interface in addition to those that are standardised for the protocols in use.

GSMA IR.77 "Inter-Operator IP Backbone Security Requirements" [61] concentrates on IP layer security in inter-service provider IP backbone networks and associated peering points. Security issues at the service provider level are covered if those are provided via a direct link to achieve the aims of a secure and quality orientated, inter-working network between service providers. It addresses confidentiality, integrity and protection against DoS attacks.

GSMA IR.61 "WiFi Roaming Guidelines" [62] describes the WiFi access to the EPC as defined in the 3GPP specifications. It concentrates on the roaming scenarios but also includes some non-roaming scenarios between E-UTRAN and pre-E-UTRAN 3GPP radio access technologies, policy control and charging, and authentication. The main focus of the current version of the document is the S2b and S2a interfaces using the GPRS Tunneling Protocol (GTP).

SC-7.3.1 Network Domain Security SHOULD be implemented in accordance with 3GPP TS 33.210 [28], which stipulates the use of IPSec to protect IP communication between administrative domains (including all network connections used to interconnect the domains).

SC-7.3.2 The PSBN SHOULD consider using IPSec interfaces that utilize IKEv2 and utilize PKI to authenticate the peers of the IPSec security associations.

SC-7.3.3 The PSBN MAY comply with TS 33.310 [29] as the authentication framework for Public Key Infrastructure to authenticate these network interfaces between security domains.

SC-7.3.4 When PSBN network elements are located in trusted locations without wide area communication links between them, the use of Network Domain Security SHOULD be optional.

SC-7.3.5 The PSBN SHALL connect to the public internet via security gateways.

SC-7.3.6 To protect IP-based Roaming and Interworking Network Interfaces, the PSBN SHOULD apply GSMA guidelines as per GSMA PRD-IR.34 [60] and PRD-IR.77 [61].

SC-7.3.7 To protect LTE Roaming Interfaces, the PSBN SHOULD apply GSMA guidelines as per GSMA PRD-IR.88 [59].

SC-7.3.8 All DIAMETER-based interconnection points SHOULD be protected according to industry best practices.

SC-7.3.9 To protect WiFi roaming interfaces, the PSBN SHALL apply GSMA guidelines as per GSMA PRD-IR.61 [62].

SC-7.3.10 To protect SS7-based Roaming and Interworking Network Interfaces, the PSBN SHOULD comply with TS 33.204 [30].

SC-7.3.11 The PSBN SHALL monitor SS7 interconnection points and implement SS7 according to industry best practices.

SC-7.3.12 The PSBN SHALL protect all Signaling Transport (SIGTRAN)-based SS7 interconnection points according to industry best practices.

SC-7.3.13 Security mechanisms layered by a jurisdiction on top of the PSBN SHOULD NOT inhibit interoperability for users visiting from outside of the security domain in which it is implemented.

SC-7.3.14 As the national entity enters into roaming agreements with commercial partners, security policies SHOULD be implemented that ensure integrity of the PSBN and that PSBN security practices are not compromised.

7.4 User domain security

User domain security is a set of security features that provides users with secure access to mobile stations and related subscribed services and applications.

3GPP TS 33.102 [20] specifies two security features. The first is the User-to-USIM authentication. With this feature, access to the USIM can be restricted to an authorized user or to a number of authorized users. To accomplish this feature, the user and USIM must share a secret (e.g., a PIN) that is stored securely in the USIM. This security feature is implemented by means of the mechanism described in TS 31.101 [23]. The second feature is the USIM-Terminal Link, which ensures that access to a terminal or other user equipment can be restricted to an authorized USIM. To this end, the USIM and the terminal must share a secret that is stored securely in the USIM and the terminal. If a USIM fails to prove its knowledge of the secret, it will be denied access to the terminal. This security feature is implemented by means of the mechanism described in TS 22.022 [19].

SC-7.4.1 A UE device’s user interface SHOULD be disabled after it is idle for a pre-set (configurable) period of time.

SC-7.4.2 A UE device whose user interface has been disabled due to idle time-out SHOULD require the user to re-authenticate in order to enable the user interface.

SC-7.4.3 UEs SHOULD implement user domain security in accordance with TS 33.102 [20], TS 31.101 [23] and 22.022 [19].

SC-7.4.4 The PSBN SHALL apply security measures to protect signalling and addressing information carried over the PSBN up to the network domain border of the PSBN, as derived from a security risk and vulnerability assessment.

7.5 Local Area Network (LAN) and IoT security

The Local Area Network (LAN) security includes security features to protect the communication between a UICC Hosting Device and a Remote Device connected via a local interface. The communication over the local interface could take place via for example Bluetooth, USB, IR or a serial cable.

In this document, the LAN security is presented in the context of MTC, i.e., to secure the interface between the MTC endpoints and the MTC gateway. However, the LAN security features in this section are not limited to the MTC application.

TS 33.259 [24] describes the security features and mechanisms to provision a shared key between a UICC hosting device and a remote device connected via a local interface. The shared secret is then intended to be used to secure the interface between the remote device and the UICC hosting device. The solution is built on the existing infrastructure defined by the Generic Bootstrapping Architecture (GBA) as specified in TS 33.220 [39]. GBA is covered in more details in Section 7.6 on application security, as GBA is a generic security solution applicable to any client-server application, including an MTC application.

In the MTC context, as the security is ultimately required between the MTC endpoint and the MTC server, the local link between the MTC endpoint and the MTC gateway needs to be secured with a comparable level of security as the wide area network to keep the same overall level of security. With GBA, the authentication and security are extended from the MTC gateway to the MTC endpoint device, creating a secure channel from the given MTC endpoint device up to the MTC server.

GBA also leverages the USIM-based infrastructure to generate pre-shared keys which are then used to generate time-limited keys (tokens) as a basis of both authentication and encryption between devices and network-based applications referred to by 3GPP as Network Application Functions (NAFs). This authentication infrastructure has the virtue of providing not only authentication, but also encryption capabilities based on pre-shared secrets.

Additional security features applicable to the local interface between the endpoint and the gateway, specific to the technology of the local interface, is not within the scope of this document.

SC-7.5.1	The connectivity between MTC endpoints and the MTC gateway SHALL implement the security measures as specified in TS 33.259 [24].

7.6 Application domain security

The Application domain security encompasses a set of security features that enable network services and applications in the UE and in the PSBN to securely exchange messages.

This section covers the following three types of applications:

- 3GPP applications or services that are fully specified by 3GPP with built-in protocol-based security features including:
    - USIM applications;
    - IMS applications such as VoLTE and ViLTE;
    - Mission-Critical Services: MCPTT, MCData, and MCVideo;
    - MTC applications;
    - Presence service;
    - eMBMS.
- Non-3GPP applications that run on PSBN-hosted servers; although not specified by 3GPP, such applications could nonetheless make use of the 3GPP generic UE-server security measures specified by the 3GPP GBA;
- Non-3GPP applications that make use of the PSBN Service Delivery Platform (SDP).

The following 3GPP specifications provide data integrity, data origin authentication, anti-replay protection, and confidentiality (optional).

7.6.1 USIM Applications

The USIM Application Toolkit, as specified in TS 31.111 [63], provides the capability for operators or third-party providers to create applications that are resident on the USIM (similar to the SIM Application Toolkit in GSM). Security features for the USIM Application Toolkit implemented by means of the mechanisms described in TS 23.048[9] [64] provide secure messages between the network and applications on the USIM, with the level of security chosen by the network operator or the application provider. The security mechanisms include mutual authentication between network and UICC, message integrity, replay detection, proof of receipt, and message confidentiality.

7.6.2 IMS Applications

The IP Multimedia Sub-system (IMS) supports IP Multimedia applications such as video, audio and multimedia conferences. 3GPP has chosen Session Initiation Protocol (SIP) as the signalling protocol for creating and terminating multimedia sessions. The IP Multimedia Services Identity Module (ISIM) is a mandatory application on the UICC (alongside the USIM) required to provide access to the IMS network. The ISIM contains the security data and functions for IMS.

In the Packet Switched (PS) domain, the service is not provided until a security association is established between the UE and the network. IMS is essentially an overlay to the PS domain and a separate security association is required between the IMS client and the IMS before access is granted to multimedia services. The security termination point from the UE towards the IMS network is in the Proxy Call Session Control Function (P-CSCF) utilising IPsec Encapsulating Security Payload (ESP).

TS 33.203 [31] specifies the security features and mechanisms for secure access to the IMS. This specification deals with how the UE is authenticated and how the UE authenticates the IMS through the use of IMS Authentication and Key Agreement (AKA), and how the SIP signalling is confidentiality and integrity protected between the UE and the IMS P-CSCF. The security of SIP messages is then implemented based on Transport Layer Security (TLS) with the agreed keys.

When IMS control plane traffic is routed across different security domains, the applicable Network Domain Security, as described in Section 7.3, shall be implemented.

TS 33.328 [32] specifies IMS media plane security for real-time media, where the media plane can be protected end-to-end.

7.6.3 Mission Critical Services (MCS)

TS 33.180 [35] specifies the security architecture, procedures and information flows needed to protect Mission Critical Services (MCS). The architecture includes mechanisms to protect the Common Functional Architecture (CFA) and security mechanisms for mission critical applications. This includes Push-To-Talk (MCPTT), Video (MCVideo) and Data (MCData). Additionally, security mechanisms relating to on-network use, off-network use, roaming, migration, interconnection, interworking and multiple security domains are described. The security architecture provides signalling and application plane security mechanisms to protect metadata and communications used as part of the MC Service.

The following signalling plane security mechanisms are used by the MC Service:

- Protection of the signalling plane used by the MC Service
- Protection of inter/intra domain interfaces

[9] At Release 5, TS 23.048 has been split into TS 31.116 [65] and TS 31.115 [66].

The following application security mechanisms are used by the MC Service:

- Authentication and authorisation of users to the MC Service;
- Protection of sensitive application signalling within the MC Service;
- Security of Real-Time Control Protocol (RTCP) (e.g., floor control, transmission control) within the MC Service;
- Security of data signalling within the MCData Service;
- End-to-end security of user media within the MC Service.

Security mechanisms in the signalling plane and application layer are independent of each other, but may both be required for a secure MCPTT system.

To use MCPTT, the UE performs authentication and authorization after LTE attach as defined in TS 33.180 [35], which consists of three processes: MCPTT user authentication, SIP Registration and Authentication, and MCPTT Service Authorization.

The Identity Management (IdM) functional model for MCPTT consists of the identity management server located in the MCPTT common services core and the identity management client located in the MCPTT UE. The IdM server and the IdM client in the MCPTT UE establish the foundation for MCPTT user authentication and user authorization. It supports interchangeable MCPTT user authentication solutions, such as Web Single-Sign-On (SSO), SIP digest, GBA, biometric identifiers, username+password. The 3GPP IdM server would need to be integrated into the PSBN Identity, Credential, and Access Management (ICAM) Framework which is described in Section 7.11.

For a period of time after MCPTT capabilities are deployed in the PSBN, legacy LMR systems will continue to be in operation. An interface between PSBN-based MCPTT systems and legacy LMR systems will be required to preserve interoperability, as the timeline of transition from LMR to MCPTT may vary among public safety agencies. TS 23.283 [36] specifies the interworking between MCPTT and LMR systems, including the mechanisms to securely share encryption keys between the two systems.

7.6.4 Proximity-based Services (ProSe)

TS 33.303 provides authentication, confidentiality and integrity services for the UE-ProSe function; network element to network element, as well as UE-to-UE in direct communications. Based on the common security procedures for interfaces between network entities (using NDS), configuration of ProSe-enabled UEs, and data transfer between the ProSe Function and a ProSe enabled UE (PC3 interface), security for the following ProSe features is covered:

- Open ProSe Direct Discovery in network coverage
- One-to-many ProSe direct communication for ProSe-enabled Public Safety UEs
- EPC-level Discovery of ProSe-enabled UEs
- EPC support for WLAN Direct Discovery and Communication
- One-to-one ProSe direct communication for ProSe-enabled Public Safety UEs
- Prose Public Safety Discovery

- Prose UE-to-network relays

7.6.5 MTC Application

The following 3GPP specifications provide authentication, confidentiality and integrity measures on MTC UE and the Home PLMN Security Endpoint.

TS 33.163 [34] defines communication security processes designed for very low throughput MTC devices that are battery constrained. These processes consist of:

- A Key agreement service for end-to-middle and end-to-end security use
- An end-to-middle secure transport service that includes the ability to verify and confidentiality protect low throughput data
- An end-to-end secure transport service that includes the ability to verify and confidentiality protect low throughput data

TS 33.187 [18] specifies the security architecture enhancements (i.e., enhancements to the security features and the security mechanisms) to facilitate Machine-Type and other mobile data applications Communications enhancements (MTCe) as per the use cases and service requirements defined in TS 22.368 [67] and the architecture enhancements and procedures defined in TS 23.682 [68].

The PSBN, whether acting as a communication network for a public safety MTC service provider or acting as a full-fledged public safety MTC service provider itself, shall implement the best practices in security guidelines as documented in GSMA CLP.14 “IoT Security Guidelines for Network Operators” [69], including the following fundamental security mechanisms:

- Identification and authentication of the entities involved in the MTC Service (i.e., gateways, endpoint devices, home network, roaming networks, service platforms);
- Access control to the different entities that need to be connected to create the IoT Service;
- Data protection in order to guarantee the security (confidentiality, integrity, availability, authenticity) and privacy of the information carried by the network for the MTC Service;
- Processes and mechanisms to guarantee availability of network resources and protect them against attack (for example by deploying appropriate firewall, intrusion prevention and data filtering technologies).

7.6.6 Presence service

3GPP-based proximity application and services enable proximity-based discovery and communications between PSBN UEs such as with the LMR-based “talk around.” 3GPP proximity services require the presence service.

The presence service makes use of the Ut reference point between the Presence User Agent and the Presence Server. The Ut reference point is not covered in the IMS security specification TS 33.203 [31]. TS 33.141 [33] provides authentication, confidentiality, and integrity services to the Ut reference point used in the Presence Service.

7.6.7 Enhanced Multimedia Broadcast / Multicast Service

Multimedia Broadcast / Multicast Service (MBMS) introduces the concept of a point-to-multipoint service into a 3GPP system. The enhanced version of MBMS (eMBMS) is an important component in providing efficient support for Group Call for Public Safety services as part of Release 12. Point-to-multipoint broadcast offered by the LTE MBMS technology is well suited for group communications, which form a major part of public safety related communications.

A requirement of a MBMS User Service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a MBMS User Service. TS 33.246 [38] specifies the usage of Generic Bootstrapping Architecture (GBA) for MBMS. GBA is used to provision the keys that are needed to run an MBMS User Service. If protection for the MBMS User Service is required, then the UE needs to share GBA-keys with the BM-SC that is acting as a Network Application Function (NAF) according to TS 33.220 [39]. The MBMS Service Keys for an MBMS User Service shall be stored on either the UICC if the UICC is capable of MBMS key management or the ME if the UICC is not capable of MBMS key management.

The GBA is part of the Generic Authentication Architecture (GAA), as shown in Figure 6. With GAA, there are two types of authentication mechanisms available to mobile applications:

- the Generic Bootstrapping Architecture, which is based on a secret shared between the communicating entities, as specified in TS 33.220 [39];
- the Support for Subscriber Certificates (SSC), which is based on (public, private) key pairs and digital certificates, as specified in TS 33.221 [43].

The choice of one authentication mechanism over the other depends on the specific requirements and applicable security policies related to authentication. The following should be taken into consideration when selecting one authentication mechanism:

- SSC makes use of asymmetric encryption technology which requires more computational effort than symmetric key operations like GBA;
- SSC requires a Public Key Infrastructure (PKI);
- As SSC makes use of public key technique where the private key is only held by the sender, SSC provides non-repudiation provable to a third party;
- GBA can also be used in conjunction with SSC, where GBA is used to authenticate the UE to the PKI portal.

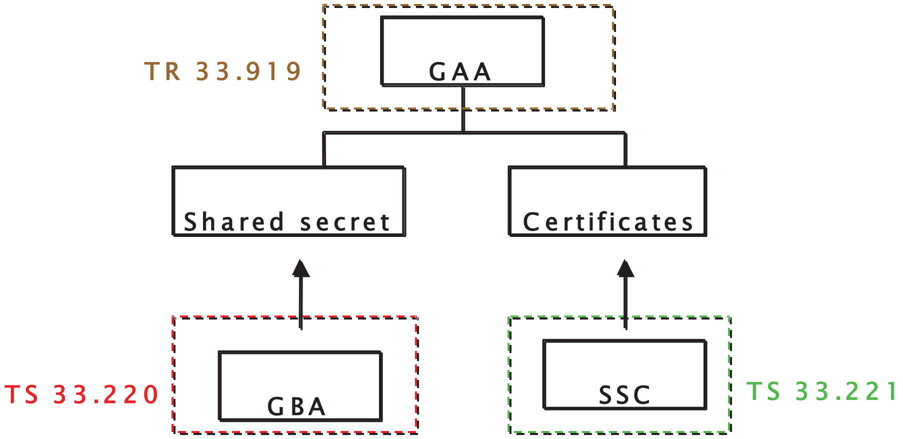


Figure 6: *GAA schematic overview (source: 3GPP TR 33.919 [70]).*

7.6.8 Generic Bootstrapping Architecture (GBA)

3GPP Generic Bootstrapping Architecture (GBA) provides a secure and reliable method to establish (aka bootstrap) a security association between a client and a server. With 3GPP GBA, the 3GPP authentication infrastructure including the 3GPP Authentication Centre (AuC), the USIM or the ISIM, and the 3GPP Authentication and Key Agreement (AKA) protocol that runs between them can be leveraged to enable application functions in the network and on the user side to establish shared keys.

GBA uses long term security associations that are stored in the Home Subscriber Server (HSS) of the mobile network operator. Based on this long-term security association, a short-term server specific security association is created during a bootstrapping procedure between the client and a server. The following 3GPP documents specify GBA.

TS 33.220 [39] describes the security features and mechanisms to bootstrap authentication and key agreement for application security. GBA provides a general mechanism based on 3GPP Authentication and Key Agreement (AKA) to install a shared secret between a UE and a server. The GBA includes three parties:

- A user who is trying to obtain network services using User Equipment (UE);
- Application server (called Network Application Function or NAF);
- A trusted entity (called Bootstrapping Server Function or BSF), which is involved in authentication and key exchange between two other entities.

The GBA enables authentication of a user, who is using a UE, to an application server (NAF) without revealing the user’s long-term credentials and secrets to the NAF by using a trusted entity BSF.

The BSF has an interface with the HSS and the UE runs AKA with the HSS via the BSF. From the resulting keys, a session key is derived in the BSF and UE. An application server called Network Application Function (NAF) can fetch this session key from the BSF together with subscriber profile information. In this way, the application server (NAF) and the UE share a secret key that can subsequently be used for application security, in particular to authenticate the UE and NAF at the start of the application session (possibly also for integrity and/or confidentiality protection). The communication between the UE and the BSF as well as that between NAF and BSF and between BSF and HSS are application independent.

TS 33.222 [40] specifies secure access methods to NAF using Hypertext Transfer Protocol over Transport Layer Security (HTTPS).

TS 33.223 [41] specifies the GBA-Push function that allows a NAF to initiate the establishment of a shared security association between itself and a UE without forcing the UE to contact the BSF to initiate the bootstrapping. GBA-Push is closely related to and builds upon GBA as specified in TS 33.220 [39].

TS 33.224 [42] specifies a Generic Push Layer (GPL) that makes use of the GBA-Push Function as specified in TS 33.223 [41]. With GPL, network-based applications can rely on a secure session with a UE, and benefit from pushing more than one message based on the same security association. An example could be a virus signature update server. It is possible that the virus signatures are delivered in multiple pushed messages (for size limitation reasons of the underlying push transport mechanism), and it would then be inefficient to establish a new security association for each message. A special case of a network initiated service is the case where the operator may want to securely update information on the terminal (e.g., device management or client provisioning). GPL provides replay protection in addition to integrity protection (and possibly confidentiality protection). Furthermore, a secure push would also allow protection against replay and DoS attacks.

The Open Mobile Alliance (OMA) GBA Profile [71] defines an OMA profile of the GBA specified in 3GPP and also an OMA profile of GBA-Push specified in 3GPP.

7.6.9 Support for Subscriber Certificates (SSC)

Use of asymmetric encryption technology requires a digital certificate that is created by a Certification Authority (CA). Such a certificate binds a public key to the identity of its legitimate owner and certifies the validity of the public key. TS 33.221 [43] specifies a mechanism to dynamically issue a digital certificate to a mobile subscriber. Once a mobile subscriber has a (public, private) key pair and has obtained a certificate for it, he can use the certificate together with the corresponding key pair to produce digital signatures but also to authenticate to a server.

7.6.10 3GPP Service Delivery Platform (SDP)

The PSBN will need to deliver PSBN services and expose specific Applications Programming Interfaces (APIs) to enable new applications. These APIs, services, and applications will allow for new capabilities such as dynamic control of QoS, priority, pre-emption, local control, and the creation of public safety analytics. Network services such as location information and usage records can be supplied to applications in order to render the information meaningful to users. Typically, this means that the applications would correlate data sets such as location coordinates with map layers, or usage information with rating data to prepare bills, etc.

3GPP has created TS 23.222 [44] to specify a Common API Framework (CAPIF) for 3GPP northbound APIs, including security requirements, so that all northbound APIs function similarly. The northbound API is in effect the interface between an application server (either in the PSBN or external to it operated by an EUA) and the 3GPP system via specified functions in the PSBN.

7.6.11 Application vetting

Although not in scope of this document, the PSBN should ensure the security of applications with the following process-based security measures:

- Applications ecosystem security
- Application audit
- Application security in software development life-cycle
- Application security certification
- Application developer certification

Applications can request information and services from the PSBN. It is expected that applications will be vetted prior to being approved. Vetting would include the verification of what services the application needs. For example, a blue-force tracking application should not require usage records and therefore not request this information from the PSBN. The PSBN SDP can provide a report on the services that were requested and by which application. This could be used as part of the vetting process for applications.

The NIST Special Publication 800-163 Vetting the Security of Mobile Applications [72] can help (i) understand the process for vetting the security of mobile applications, (ii) plan for the implementation of an application vetting process, (iii) develop application security requirements, (iv) understand the types of application vulnerabilities and the testing methods used to detect those vulnerabilities, and (v) determine if an application is acceptable for deployment on the organization’s mobile devices. The NIST Interagency Report 8136 [73] is a high-level investigation of application vetting services with the goal of enumerating the traits exhibited that may be useful to public safety.

SC-7.6.1 The PSBN SHALL apply access control measures to applications attempting to access network services.

SC-7.6.2 The PSBN network services layer SHALL record requests by applications for services.

SC-7.6.3 The PSBN SHALL offer a time reference service synchronized to an approved source.

SC-7.6.4 The PSBN SHALL apply time and geo-location stamping of captured data (video, still images, audio tracks, etc.), events, records, and logs.

SC-7.6.5 The PSBN SHALL encrypt network services layer information (e.g., location, usage, passwords).

SC-7.6.6 The PSBN SHALL ensure that the records of the network services requested by applications SHALL be preserved in a protected manner such that the records can be accessed by authorized personnel only.

SC-7.6.7 The PSBN SHALL ensure that only approved applications will be accessible on the PSBN.

SC-7.6.8 The PSBN SHALL employ measures to verify the security posture of approved applications at intervals and/or trigger events as defined by relevant policy.

SC-7.6.9 The PSBN SHALL provide secure voice and data communications between end-users, as required by EUAs.

SC-7.6.10 The PSBN SHALL ensure that applications software cannot be modified except by authorized persons.

SC-7.6.11 The PSBN SHALL ensure that applications software cannot be installed on, or deleted from host servers except by authorized persons.

SC-7.6.12 The PSBN SHALL disable access to UE-hosted and network-hosted applications whose code integrity has been compromised.

SC-7.6.13 The PSBN SHALL be able to restrict the information that applications request from network services.

SC-7.6.14 The PSBN SHALL be able to prevent applications from accessing specific websites anywhere on the worldwide web.

SC-7.6.15 USIM-based applications that require messaging between the USIM and network components SHALL comply with TS 31.116 [65] and TS 31.115 [66] to provide secure messaging between the USIM and the network.

SC-7.6.16 The PSBN SHALL comply with TS 33.203 [31] and TS 33.328 [32] to provide security on both signalling and media planes between the UE and the IMS network.

SC-7.6.17 The PSBN SHALL comply with TS 33.141 [33] to provide security on the signalling plane between the UE and the IMS-based Presence server.

SC-7.6.18 The PSBN SHALL comply with TS 33.163 [34] and 33.187 [18] to provide security between a MTC UE and the network.

SC-7.6.19 The PSBN SHALL comply with TS 33.180 [35] to provide security on the signalling plane between the UE and the IMS-based Mission Critical application servers.

SC-7.6.20 The PSBN SHALL comply with TS 23.283 [36] to provide security for interworking between MCPTT systems and LMR systems.

SC-7.6.21 The PSBN SHALL comply with TS 33.303 [37] to provide security for the Proximity-based services.

SC-7.6.22 The PSBN SHALL comply with TS 33.246 [38] to provide security for the MBMS services.

SC-7.6.23 The PSBN MAY comply with TS 33.220 [39], TS 33.222 [40], TS 33.223 [41] and TS 33.224 [42] to provide GBA-based security mechanisms to PSBN-hosted application servers.

SC-7.6.24 The PSBN MAY implement the best-practices in IMS security guidelines, as defined by GSMA PRD IR.92 [74] and IR.51 [75].

SC-7.6.25 The MCPTT Service SHALL employ compliant open standards for encryption and authentication, subject to applicable national policy.

SC-7.6.26 The MCPTT Service SHALL provide a mechanism to encrypt all PTT Group transmissions, both user and control plane data (for example, audio, Talker ID).

SC-7.6.27 A UE SHALL provide a mechanism for an authorized user to select what services are available on the UE prior to full authentication on the UE (for example, 911 calls on commercial UEs).

SC-7.6.28 The MCPTT, MCData, and MCVideo services SHALL provide a mechanism to accommodate ongoing security algorithm improvements, which could include over the air key management.

SC-7.6.29 The PSBN SHALL monitor for any security breach and non-standard ports used by an application.

SC-7.6.30 The PSBN SHALL provide protections to ensure applications protect data while at rest, in use, and in transit.

SC-7.6.31 The PSBN SHALL provide the capability to detect text and multimedia messaging infected with malware and prevent its delivery to the intended target.

SC-7.6.32 The PSBN SHALL monitor all common infrastructure components, servers, routers, gateways, and other vulnerable equipment using appropriate malware and virus protection mechanisms.

SC-7.6.33 The PSBN SHALL use monitoring tools to detect and analyze the various delivery methods used for distribution of malware, bugs, and virus software over including SMS, MMS, email, and other applications.

SC-7.6.34 PSBN applications SHOULD provide a logging and auditing capability for any additions, deletions, and updates to support non-repudiation.

SC-7.6.35 The PSBN SHOULD use industry standard practices to validate application and UE security postures against policies at relevant intervals.

7.7 OAM&P domain security

The Operations, Administration, Maintenance, and Provisioning (OAM&P) domain security protects the Telecommunication Management Network (TMN) and provides the protection of all the operation and maintenance traffic, authentication of users, applications and access control to the nodes. It protects the resources of network elements and management applications from intentional and unintentional destructive manipulation.

According to ITU X.1205 [76], the following components are necessary to secure the management plane of a network:

- Secure activity logs; this is covered in Section 7.16;
- Network operator authentication; this is covered in Section 7.11;
- Access control for network operators; this is covered in Section 7.11;
- Protection of network management traffic; covered in this section;
- Secure remote access for operators; covered in this section;
- Firewalls; this is covered in Section 7.12;
- Intrusion detection; this is covered in Section 7.15;
- OS hardening; this is covered in Section 7.14;
- Virus free software; this is covered in Section 7.14.

In the context of a Multi-Operator Core Network (MOCN) environment, the PSBN operator needs not only be concerned about protecting its own TMN but also reach agreements with the MOCN partners at TMN-level interconnection points on configuration management, performance management, fault management and security management. To address the protection of network management traffic, 3GPP specifies a series of security measures described below.

TS 32.371 [45] specifies the necessary security features, services and functions to protect the network management data across the 3GPP defined integration reference points and their supporting protocol stacks.

It is recommended to provide baseline infrastructure security between machines communicating across the Itf-N, as shown in Figure 7, through the use of IP network security protocols such as IPSec (Internet Protocol security suite), Secure Shell (SSH), and Secure Socket Layer / Transport Layer Security (SSL/TLS). These IP network security protocols employ security services through the use of cryptographic mechanisms and provide services including data confidentiality, data integrity, machine-to-machine authentication, and others. Note that the NE reference in Figure 7 refers to *network element* and not *national entity*.

Although the recommendations of TS 32.371 [45] apply specifically to management interfaces of Type 2, or EMS-NMS Interface also known as Interface N, including the underlying IP transport network used to support this interface, the recommendations and guidelines may also be considered to provide security for other interfaces such as the Type 1 (i.e., EMS-NE Interface) or even Type 3, 4, and 5, as shown in Figure 7. While TS 32.371 [45] specifies the security requirements for the IP transport layer of the OAM&P traffic, TS 32.372 [46] specifies the following security services to protect the management plane at the application layer: Authentication Security Service, Authorization Security Service, Activity Log Security Service, and File Integrity Security Service.

TS 32.376 [47] specifies the Solution Set for the Integration Reference Point (IRP) whose semantics is specified in 3GPP TS 32.372 Security Service for IRP Information Service.

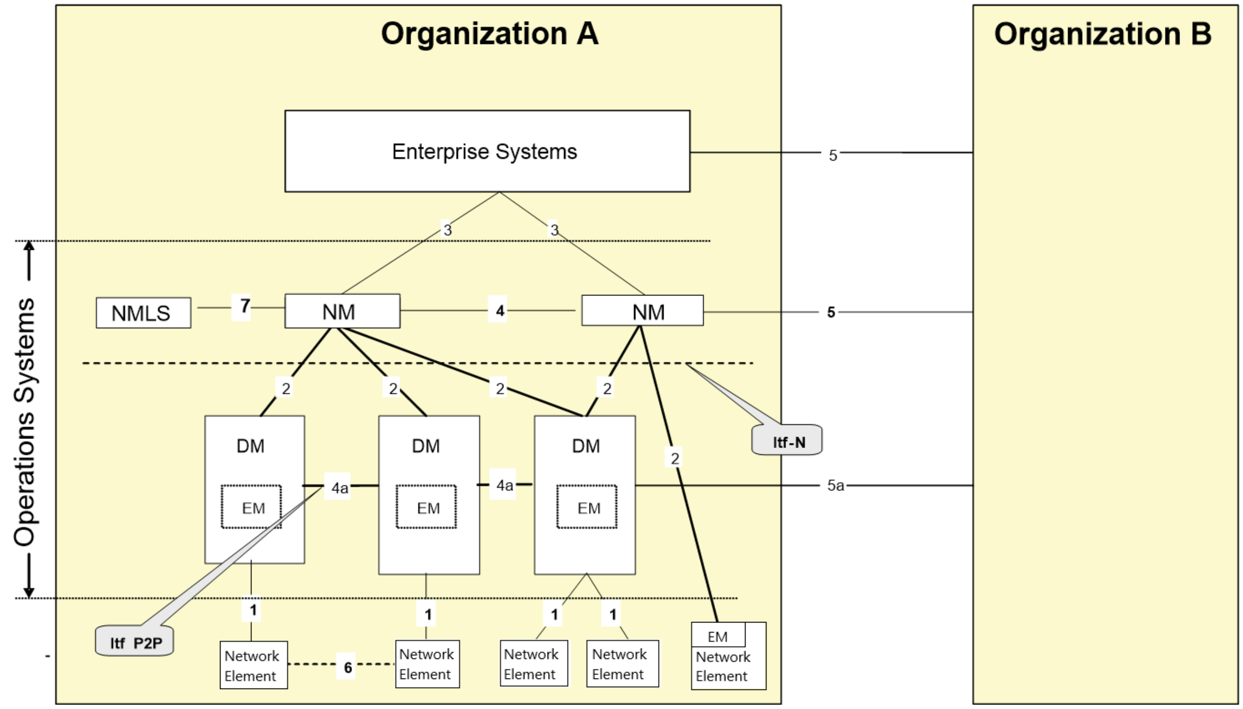


Figure 7: *3GPP management system interactions (adapted from TS 32.101, Section 5.1 [77]).*

7.7.1 Secure remote access

The PSBN will have networks, systems and facilities that rely on outside vendors for maintenance and support service. Vendors might require physical access and/or dedicated remote network access. Secure remote access to the network can be accomplished through either a Secure Shell (SSH) Tunnel, a Virtual Private Network (VPN) or a dedicated point-to-point line. Remote access should be granted only to the network elements that are under the scope of the maintenance activities. Security patches need to be kept up to date on those remote access connections. Vendor staff should meet the PSBN security policies with regards to background check requirements.

SC-7.7.1 The PSBN SHALL require that secure and encrypted connections be established for all remote monitoring and control sessions by the administrators.

SC-7.7.2 The PSBN SHALL comply with TS 32.371 [45], TS 32.372 [46] and 32.376 [47] to provide security in the OAM&P domain between Network Elements, Element Management Systems and the Network Management Systems.

SC-7.7.3 The PSBN SHALL provide remote access to vendors using secure technologies such as SSH, VPN, or dedicated point-to-point connection.

SC-7.7.4 The PSBN SHALL secure the OAM&P information according to the security requirements for the PSBN.

7.8 Security visibility and configurability

For end-users, security visibility and configurability is a set of features that enables the user to confirm whether a security feature is in operation or not, and whether the use and provision of services should depend on the security feature.

7.8.1 End-user visibility and configurability

In some public safety use cases, it is desirable or even necessary to provide user feedback concerning the security level in which a user device is operating. 3GPP standards provide mechanisms for:

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

The ciphering indicator feature specified in TS 22.101 [78] allows the UE to detect and indicate to the user that the 3GPP radio interface ciphering (user plane) is not switched on.

TS 33.102 [20] specifies configurability whereby the end-user can configure a service so that it depends on security features to be in operations. With configurability, a service can only be used if all security features that are relevant to that service and are required by the configurations of the user, are in operation. The following configurability features are possible:

- Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication for some events, services or use;
- Configuring the UE to only attach to secure radio technologies such as 3G HSPA and LTE, i.e., “Use LTE or 3G only” option;
- Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;
- Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;
- Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.

7.8.2 Operator-user visibility and configurability

For operator-users, security visibility and configurability is a set of features that enables network administrators to:

- Set and verify security settings on devices in their networks
- Set and verify security parameters consistently across multiple network nodes

ITU X.1205 [76] discusses configuration management techniques that allow the PSBN security administrators to set and verify security settings on devices in their networks. It also discusses policy management that enables the PSBN security administrators to define business-driven security and QoS policies, and enforce these across the organization without having to understand all the device-specific rules and settings that are needed to enforce these policies.

SC-7.8.1 The UE device SHALL conspicuously alert the end-user if a session is not encrypted.

SC-7.8.2 The PSBN SHALL give administrators the ability to derive reports of the security status of the PSBN as it relates to the availability of the services offered by the PSBN, in accordance to relevant policies.

SC-7.8.3 The PSBN SHALL provide any end-user and EUA the ability to black-list messaging contacts such that the messaging service will filter messages originating from black-listed contacts.

SC-7.8.4 The PSBN SHALL provide any end-user and EUA the ability to white-list messaging contacts such that only white-listed contacts can pass through the message filter.

SC-7.8.5 The PSBN SHALL support both black-listing and white-listing message filters at the same time and independently for any EUA.

SC-7.8.6 The PSBN SHALL allow an end-user to block his/her UE from transmitting his/her location information, according to relevant policies.

SC-7.8.7 The PSBN SHALL permit an authorized user to enable voice and data communications for end-users to occur in the clear, in accordance to relevant policies.

SC-7.8.8 In such cases where security visibility is required for devices on the PSBN, the implementations MAY comply with TS 22.101 [78].

SC-7.8.9 The PSBN SHALL implement solutions to provide visibility and configurability of network security configuration to the PSBN network administrators.

SC-7.8.10 In such cases where security configurability is required for devices on the PSBN, the implementations MAY comply with TS 33.102 [20].

7.9 Device anti-theft and disablement

The device anti-theft and disablement system provides a range of security-related capabilities including:

- UE location detection capabilities to alarm when the UE is positioned outside its expected or authorized area of operations;
- For stationary UEs (e.g., MTC UEs), capabilities to detect and report UE motion as a potential sign of theft;
- Anti-theft measures including the most prevalent network based anti-theft measure in use, which is the Equipment Identity Register (EIR) as defined in the TS 22.016 [79] and TS 29.002 [80];

- UE disablement capabilities with all required security (user, operator, server authentication) around the disabling request, data and applications backup, wipe-out and restore functions, screen and device lock, UE re-initialization prevention function; this is covered in Section 7.10.

The EIR is the logical entity responsible for storing the International Mobile Equipment Identities (IMEIs) allowed on the PSBN. The equipment is classified as “white listed,” “grey listed,” “black listed” or “unknown.” During the UE attach procedure, the MME initiates the UE identity check procedure towards the EIR via the S13 interface.

A device or class of devices should be able to be blacklisted or un-blacklisted either manually or automatically. However, the automatic blacklisting must not jeopardize the safety mission of first responders.

All recommended capabilities are described in the GSMA Guidelines SG.24 “Anti-Theft Device Feature Requirements [81].”

SC-7.9.1	The PSBN SHALL enable an administrator to remotely lock and wipe a UE device, according to policies and operating procedures.
SC-7.9.2	The PSBN SHALL support automatic detection of location change and subsequent UE disablement for stationary MTC UEs.
SC-7.9.3	The PSBN SHALL provide a UE anti-theft and disablement system based on the GSMA SG.24 [81].
SC-7.9.4	The PSBN SHALL enable alarming when a UE is positioned outside its expected or authorized area of operations.

7.10 Device security solutions

Device security solutions for the PSBN include capabilities to mitigate and eliminate risks related to the UE. It is comprised of security-related considerations to be provided by the Mobile Malware Security, the Mobile Device Management (MDM) and the Mobile Application Management (MAM) applications that are expected to form part of the PSBN infrastructure as a module of the Operations Support Systems (OSS).

Additional security countermeasures around the UE include a process for vetting of mobile applications to check for vulnerabilities and malware, and digitally sign apps that have been approved, as well as a process to guarantee the hardening of the UE, as covered in Section 7.14.

7.10.1 Mobile malware security

Mobile malware can be grouped into different classes: viruses, trojans, worms, botnets and spyware applications. There are several technical countermeasures that can be taken to enhance security related to mobile malware. These are:

- Device-based security solutions: software on a device that analyses applications or other content on a device for malware; such software may receive regular updates to remain capable of detecting the latest emerging threats;

- Server host-based security filtering: defence measures directly implemented on network element service hosts such as the email servers, instant messaging server, MMSC, or SMSC;
- Network-based security solutions such as the Intrusion Detection and Protection System; this is covered in Section 7.15;
- Application certification and trust models; this is covered in Section 7.14;
- Device management; covered later in this section;
- Application store application removal: ability for administrators of application stores to remotely "kill" malicious or perceived malicious applications on users' phones which have been downloaded from application stores;
- Device hardened configuration; this is covered in Section 7.14.

7.10.2 Mobile Device Management (MDM)

A Mobile Device Management (MDM) is key to mitigate threats to mobile devices by enabling controlled device configuration, security policy enforcement, compliance monitoring, and response (e.g., remotely lock and/or wipe a mobile device that has been reported as lost or stolen). MDM solutions include a server component and a client application installed on the mobile device to manage device configuration and security, and report device status to the MDM.

The device management application shall allow an authorized administrator to remotely perform a number of functions "over the air" such as: (i) track the inventory of UE devices that have been activated, (ii) track the configurations of UE devices, (iii) push OS and firmware upgrades, (iv) activate or deactivate various functions of the UE devices, (v) disable UEs, (vi) restrict user and application access to UE hardware and interfaces, (vii) enforce encryption of data at-rest and in-transit, (viii) lock and unlock the UE, (ix) wipe UEs, (x) enforce authentication of the device owner using his PSBN credentials.

7.10.3 Mobile Application Management (MAM)

Based on the PSBN security policies with regards to mobile applications, a Mobile Application Management (MAM) solution is required for mobile application management, monitoring, and distribution to the PSBN UEs and the application store. The MAM needs to interface with the MDM to provide application whitelisting and blacklisting services, and to provide applications and updates for installation on managed mobile devices.

The MAM shall provide the PSBN administrators with the ability to: (i) set up an application store, (ii) distribute mobile applications from a dedicated mobile application store, (iii) provision and control access to internally developed and commercially available mobile applications, (iv) enforce application policy, (v) monitor integrity and behaviour of installed applications, (vi) restrict which applications may be installed through whitelisting (preferable) or blacklisting, (vii) restrict the permissions (e.g., camera access, location access) assigned to each application, (viii) restrict which app stores may be used, (ix) verify digital signatures on application, (x) and remotely install, upgrade or uninstall applications as necessary.

7.10.4 UE to MDM/MAM server communications

OMA Device Management (OMA-DM) security [48] describes the security requirements, the transport layer security, and application layer security of the OMA-DM protocol used for UE to MDM/MAM server interface. It also describes security mechanisms that are used to provide integrity, confidentiality and authentication. OMA-DM is a protocol based upon SyncML where its purpose is to allow remote management of any device supporting the OMA-DM protocol.

Consideration of the following standards and best practices is very important for a successful implementation of MDM and MAM solutions:

- NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise [82].
- NIST Special Publication 1800-4b—Cybersecurity Practice Guide - Mobile Device Security - Cloud and Hybrid Builds [83].

NIST Special Publication 1800-4b proposes a system of commercially available technologies that provide protection for mobile platforms accessing and interacting with enterprise resources. MDM and MAM can be used to define a set of policies, push those policies to a mobile device, and then enforce these policies on a mobile device via an enforcement mechanism on the device (e.g., OS, mobile application). Before policies can be pushed to a given device, an enterprise must enroll that device into the management services. Once a UE is enrolled in the MDM and MAM, security policies are defined and then pushed to the device via a secure communications channel. Publication 1800-4b makes further references to the following documents:

- CIO Council, Government Mobile and Wireless Security Baseline [84];
- NIAP, Protection Profile for Mobile Device Management [85];
- NIAP, Protection Profile for Mobile Device Fundamentals [86].

Bluetooth capabilities are common on UEs today. NIST Guide to Bluetooth Security [87] describes Bluetooth threats and countermeasures for mobile devices. The PSBN should enforce the strongest Bluetooth security mode that is available for their Bluetooth-enabled devices.

7.10.5 Bring Your Own Device (BYOD)

There are some technical solutions for achieving degrees of trust in BYOD devices, such as running the organization’s software in a secure, isolated sandbox/secure container on the mobile device, or using device integrity scanning applications.

As described in the DRDC CSS publication “Public Safety Grade Mobile Application Management Framework” [88], potential strategies to protect public safety information on BYOD are:

- To provide a way to separate personal information from public safety information on the same BYOD device. This can be achieved by adopting mechanisms like “Lockbox” that support the idea of containerization. Furthermore, these mechanisms support the ability to encrypt and lock the public safety information on the BYOD device and the user’s personal information as well. Hence, information owners have the ability to control access (e.g., revoke, access, or wipe) their information if the BYOD is believed to have been compromised. By doing so, if a device is lost or stolen, the information owner has confidence that their information is protected from disclosure.

- Information owners can use policy enforcement techniques to limit access to information according to agencies’ pre-defined policies. For example, the information owner’s policy may require device storage encryption and a device access PIN following particular rules. Also, the BYOD owner can be allowed to use a generic browser to access non-public safety information, while using a specific browser to access public safety information. Furthermore, an information owner can control access of multiple users sharing a device by enforcing access control over information such that only approved users can access an information owner’s information.
- Use Root of Trust to establish a chain of trust and provide the device with the ability to send device state assertions to the IT management, then to the information owner.

SC-7.10.1 The PSBN SHALL enable an administrator to remotely install, update, and remove applications from user devices, according to policies and operating procedures.

SC-7.10.2 The PSBN SHALL enable an administrator to remotely push virus definition files to user devices.

SC-7.10.3 The PSBN MDM SHOULD enable authentication for access to the collection of secured applications on the device.

SC-7.10.4 The PSBN SHALL enable an administrator to remotely upgrade a user device’s operating system.

SC-7.10.5 The PSBN SHALL enable an administrator to disable the UE transmitting function of a public safety user in order to prevent a compromised UE from interfering with the operation of the PSBN, in accordance to relevant polices.

SC-7.10.6 The PSBN SHALL enable an authorized administrator to remotely upgrade a user device’s application client software.

SC-7.10.7 The PSBN MDM SHALL enable the administrator to enforce device and application password policies remotely.

SC-7.10.8 The PSBN SHALL allow an EUA administrator to wipe or lock a lost or stolen device.

SC-7.10.9 The PSBN SHALL implement mobile malware solutions as per industry guidelines such as GSMA GS.19.

SC-7.10.10 The PSBN SHALL host a mobile device management (MDM) solution allowing authorized administrators to track, monitor, update, configure, lock and wipe, and secure UEs.

SC-7.10.11 The PSBN SHALL host a mobile application management (MAM) solution allowing authorized administrators to distribute, monitor, configure, restrict, install and uninstall mobile applications on UEs as per the PSBN security policies.

SC-7.10.12 The PSBN SHALL monitor the integrity of the UE device operating systems.

SC-7.10.13 The PSBN SHALL disable a UE device from accessing any resources or services on the PSBN if its operating system has been rendered non-compliant to the approved configurations, according to relevant policies.

SC-7.10.14 The PSBN SHALL re-enable a UE device's ability to access resources and services on the PSBN when its operating system has been restored to an acceptable configuration.

SC-7.10.15 The PSBN SHALL ensure that dual-personality UE devices encrypt all data that is stored on the business side, if such devices are permitted.

SC-7.10.16 The PSBN SHALL ensure that dual-personality UEs maintain complete separation of personal and business data, if such devices are permitted.

SC-7.10.17 If public safety UE devices are shared among multiple end-users, the PSBN SHALL ensure that the private data that is stored on the device can be encrypted using an encryption key that is unique to each end-user, such that any end-user cannot access the private data that pertains to the other end-users sharing that same public safety UE device.

SC-7.10.18 The UE SHALL support user-defined encryption algorithms to be used for data that is to be kept private, in accordance with policies that govern when user-defined encryption algorithms are to be used.

SC-7.10.19 The PSBN SHALL provide protections to ensure only approved applications are installed and used on a UE.

SC-7.10.20 The device local storage of PSBN UEs must be encrypted with capability based on the UEs operating system.

SC-7.10.21 PSBN UEs SHALL be able to verify digital signatures of PSBN's and partners' signed applications.

SC-7.10.22 The PSBN SHOULD enforce the strongest Bluetooth security mode on UEs as per the PSBN security policies.

SC-7.10.23 The PSBN SHALL implement security solutions to address BYOD.

SC-7.10.24 The PSBN SHALL record log-on/off details of the end-users of shared data sessions.

SC-7.10.25 The PSBN SHALL provide protections to ensure applications cannot bypass OS security on devices.

SC-7.10.26 The PSBN SHALL provide a secure method of coexistence among PSBN-certified applications and commercially available applications on a device.

SC-7.10.27 Certificate or token-based authentication of certified applications SHOULD be available.

SC-7.10.28 Device-specific biometric authentication (e.g., fingerprint, retina) MAY be integrated for supplemental authentication of certified access to the application.

SC-7.10.29 Internal embedded clients SHOULD use non-exposed Access Point Names (APNs) for access to all certified applications or for EUA network access.

7.11 User access control management

User access control management includes solutions to effectively secure the credentialing, the authentication and the authorization of users in the following areas related to identity assurance:

- End-user to PSBN UEs, services, and applications;
- Non-person-user to PSBN UEs, services and applications;
- Operator-user to PSBN TMN applications and systems.

7.11.1 End-user and non-person user

Typically, 3GPP standards implement security mechanisms such as authentication from a device’s perspective, specifically the UE. Because public safety is likely to have many situations where equipment will be shared amongst different users during different shifts or even during different incidents, an authentication framework that extends beyond LTE device authentication is required. This framework must take into consideration that a single user may in fact share a device amongst different users (e.g., shift-by-shift) or utilize more than one LTE device simultaneously (e.g., vehicular modem, handheld, tablet).

For Mission-Critical Services (MCPTT, MCData and MCVideo), the 3GPP has introduced user-based authentication and authorization procedures in addition to the UE-based LTE and IMS authentication procedures [35]. The user-based authentication and authorization procedures make use of an identity management server to support interchangeable user authentication solutions, thereby allowing implementations to use different means to authenticate the user, (e.g., Web SSO, SIP digest, GBA, biometric identifiers, username+password).

The granting of access privileges requires that an individual requesting access must be accurately identified. Authentication is the process of correlating the credentials with stored user profiles. Various authentication methods can be used, ranging from user-name and password combinations, PIN numbers on a scrambled key pad, ID cards with bar codes and RFID, smart ID cards with embedded PKI certificates, random number tokens with or without PIN entry to decrypt the random code, biometric vectors, etc. Each method imparts a different level of confidence that the person presenting the credentials is who he/she says they are.

The NIST publication Considerations for Identity Management in Public Safety Mobile Networks [89] analyzes approaches to identity management for public safety networks.

The process of capturing credentials is not the same as authentication. It is assumed that the method to capture credentials is the purview of each EUA, the RSDEs, and the national entity for the end-users. It is expected that the end-users would be sponsored and “on-boarded” by the EUAs. Each EUA could implement its own method to capture the credentials of their users. The determination of confidence level is expected to be nationally harmonized in order to be able to establish access privileges on a common basis of acceptability. The EUAs are expected to have a critical role in vetting the users, capturing and maintaining the user' credentials, and revoking access privileges in a timely manner when warranted.

During emergencies first responders may need to access information and applications to which they may not have suitable credentialing at the time of the incident. For example, access to health records may not normally be accessible to law enforcement personnel. But, a life-threatening emergency may require that such records be accessible to him/her. However, bypassing access control measures could at times create significant security issues. It is expected that security policies and operational procedures will define when bypassing accessing controls is permitted, by whom, how the use of the PSBN is monitored during bypass conditions, and when/how normal access controls are to be restored.

7.11.2 Operator-user

To ensure the security of access to administrative accounts on the PSBN, the PSBN should consider:

- Managing the initiation, capturing, recording and management of operator-user identities and their related access permissions;
- Managing the process of operator-user provisioning and account setup;
- Providing administrators with the ability to instantly view and change access rights;
- Ensuring that operator-users are properly authorized to access applications, data, and services through the use of Attribute Based Access Controls (ABAC), Policy-Based Access Controls (PBAC), Role-Based Access Control (RBAC), and similar methods; access should be granted according to the rules set by the information security policy.

The PSBN security policy should identify and define the various roles of operator-users or processes. Each role is assigned those permissions needed to perform its functions. Each permission specifies a permitted access to a particular resource (such as "read" and "write" access to a specified file or directory, "connect" access to a given host and port, etc.). Unless a permission is granted explicitly, the user or process should not be able to access the protected resource. Additionally, identifying the roles/responsibilities that, for security purposes, should remain separate (commonly termed "separation of duties"). The concept of limiting access, or "least privilege," is simply to provide no more authorizations than necessary to perform required functions. The goal is to reduce risk by limiting the number of people with high-privilege access to critical system security controls. Best practices suggest that it is better to have several administrators with limited access to security resources rather than one person with "super user" permissions.

The PSBN security policy should include a policy to remove or restrict rights, which involves removing access once it has been granted or restricting access based on user roles. This occurs when users change roles over the course of their employment, either working in different departments or on different systems.

The NIST Guide to Attribute Based Access Control (ABAC) Definition and Considerations [90] provides a definition of ABAC and a description of the functional components of ABAC. It also provides planning, design, implementation, and operational considerations for employing ABAC.

The PSBN security policy should also ensure that all user actions are properly monitored and audited including: (i) create, protect , and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions; (iii) send privileged account data to Security Information and Event Management (SIEM) solutions; (iv) send alerts on potentially compromised accounts and automatically rotate the impacted credentials; (v) evaluated for security breaches for events such as unauthorized access, unusual application activity, and excessive incorrect login attempts should be. The considerations on the SIEM solution are covered in Section 7.16.

7.11.3 Identity, Credential, and Access Management (ICAM)

To cover all its needs related to user access and control management, the PSBN would need to set-up an Identity, Credential, and Access Management (ICAM) framework consisting of tools, policies, and systems that allows the PSBN to enable the right individual to access the right resource at the right time and for the right reason. The ICAM framework would also allow the PSBN to manage, monitor, and secure access to protected resources that may include network systems, application servers, or physical resources such as server rooms and buildings. Figure 8 depicts a conceptual view of ICAM. The process of associating a confidence level of the credentials to the method that is used to capture the credentials is assumed to be part of the PSBN ICAM framework process.

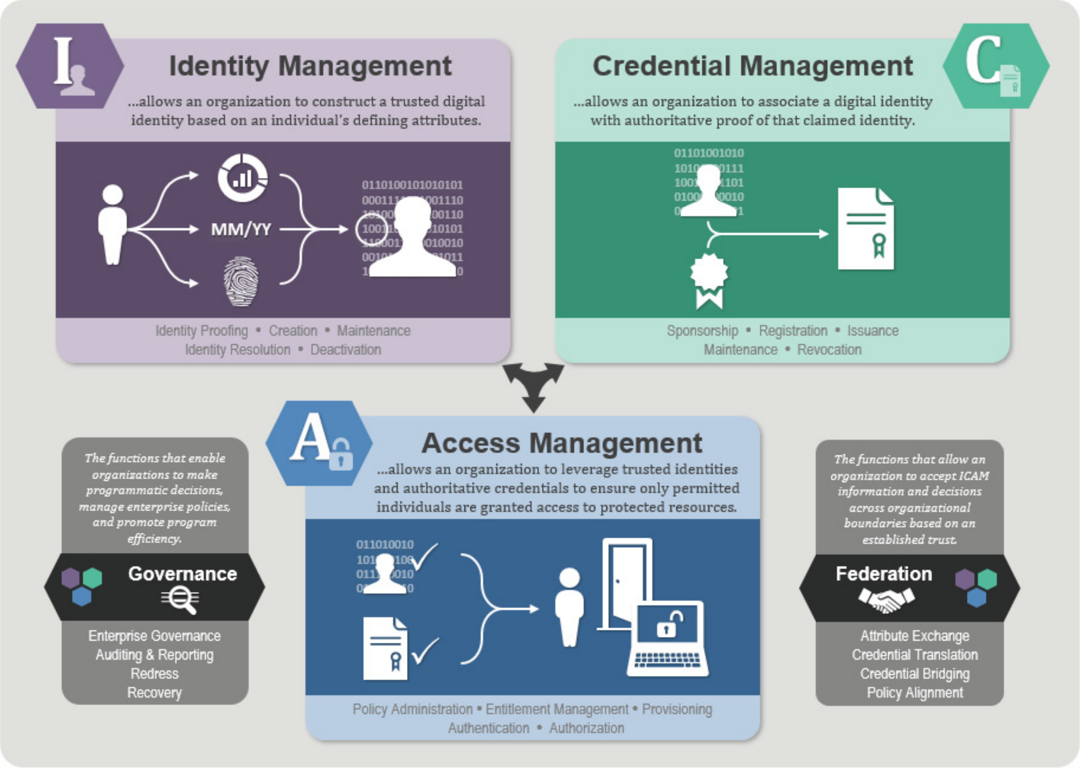

Identity Management
...allows an organization to construct a trusted digital identity based on an individual's defining attributes.
MM/YY
Identity Proofing • Creation • Maintenance
Identity Resolution • Deactivation
Credential Management
...allows an organization to associate a digital identity with authoritative proof of that claimed identity.
Sponsorship • Registration • Issuance
Maintenance • Revocation
Access Management
...allows an organization to leverage trusted identities and authoritative credentials to ensure only permitted individuals are granted access to protected resources.
Policy Administration • Entitlement Management • Provisioning
Authentication • Authorization
The functions that enable organizations to make programmatic decisions, manage enterprise policies, and promote program efficiency.
Governance
Enterprise Governance
Auditing & Reporting
Redress
Recovery
The functions that allow an organization to accept ICAM information and decisions across organizational boundaries based on an established trust.
Federation
Attribute Exchange
Credential Translation
Credential Bridging
Policy Alignment

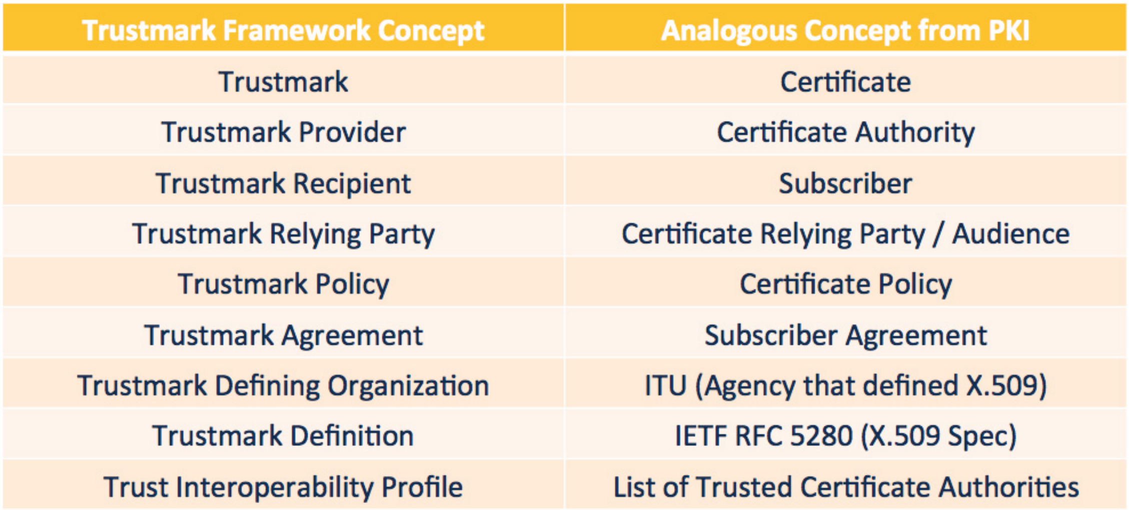
Figure 8: *Conceptual view of ICAM (source: IDMANAGEMENT.GOV [91]).*

Further to the set-up of an ICAM framework, it is recommended that the PSBN supports the establishment of a Federated ICAM (FICAM) service providing the means by which digital identity management credentials can be exchanged securely across boundaries between the EUAs, the RSDEs, and the national entity. Without a FICAM, application authentication would require unique credentials for each application or applications within an administrative domain and between administrative domains. Such proliferation of access credentials would quickly become a barrier to usability and therefore interoperability if first responders are expected to manage credentials for many different such networks and applications.

The FICAM framework comprises the programs, processes, technologies, and personnel used to create trusted digital identity representations of end-users and non-person users, bind those identities to credentials that may serve as a proxy for the end-users and non-person users in access transactions, and leverage the credentials to provide authorized access to an agency's resources. As most agencies currently have some form of ICAM for their organizations, re-using these systems in a federating trust framework would be cost-effective and allow identities to be shared across agencies. The FICAM performs the function of certifying the identities of the subscribing agencies and shares the digital representation of those identities among the subscribing agencies.

The Georgia Tech Research Institute has developed the concept of Trustmark Framework [92] that could apply to FICAM to build trust among autonomous actors for the purpose of sharing and reusing identities. Many aspects of the Trustmark concept have parallels in the well-understood concept of a Certificate Authority for a Public Key Infrastructure (PKI). The table below illustrates how various concepts from a Trustmark Framework map to similar concepts from PKI.

Table 7: *Parallels between the Trustmark Framework concept and the PKI concept (source: GTRI Trustmark [92]).*



Trustmark Framework Concept	Analogous Concept from PKI
Trustmark	Certificate
Trustmark Provider	Certificate Authority
Trustmark Recipient	Subscriber
Trustmark Relying Party	Certificate Relying Party / Audience
Trustmark Policy	Certificate Policy
Trustmark Agreement	Subscriber Agreement
Trustmark Defining Organization	ITU (Agency that defined X.509)
Trustmark Definition	IETF RFC 5280 (X.509 Spec)
Trust Interoperability Profile	List of Trusted Certificate Authorities

The following are some of the obvious conceptual similarities between the Trustmark model and the PKI model:

- A Trustmark (Certificate) represents a specific set of facts asserted to a Trustmark Relying Party (Certificate Relying Party, or Audience) about a Trustmark Recipient (Subscriber);
- The roles, responsibilities, and terms of use for a Trustmark (Certificate) are described in a Trustmark Policy (Certificate Policy);

- The scope and terms of the legal agreement between the Trustmark Provider (Certificate Authority) and the Trustmark Recipient (Subscriber) are delineated in a Trustmark Agreement (Subscriber Agreement).

The US government has published a roadmap for FICAM implementation in the US [93]. The Government of Canada has also published a report on how the concept of federation could apply to identity management within the Government of Canada context [94].

SC-7.11.1 The PSBN SHALL implement security measures such that only authorized administrators may configure and monitor the network elements of the PSBN, in accordance to policies established by the operator of the PSBN and the EUAs.

SC-7.11.2 The PSBN SHALL implement security measures such that only authorized administrators may intercept end-user data and metadata, in accordance with privacy policies and in conformity to legal statutes.

SC-7.11.3 The authentication method SHALL be able to ascertain the identity of the individual and assign a degree of confidence to the identity corresponding to the method that is used to capture the credentials.

SC-7.11.4 The PSBN SHALL implement nationally-harmonized definitions and levels of assurance for the credentials of users.

SC-7.11.5 The PSBN SHALL host an authentication service for applications that require network services.

SC-7.11.6 The PSBN SHALL host an authentication service for non-human (machine) users, such as sensors.

SC-7.11.7 The PSBN SHALL implement the means to determine the identity confidence level associated with the methods that end-user agencies employ to capture users' credentials, in accordance to relevant policies.

SC-7.11.8 The PSBN SHALL use the identity confidence level as a factor in the decision to grant or deny access requests by users.

SC-7.11.9 The PSBN SHALL ensure that user credentials are not viewable by unauthorized users.

SC-7.11.10 Identity assertions SHALL be cryptographically protected when being transmitted from one entity to another in the network.

SC-7.11.11 The PSBN services and applications SHALL authorize access to information based on the identity of users, their roles, and other attributes based on policies for the services and applications.

SC-7.11.12 The PSBN SHALL host an identity, credential, and access management (ICAM) system that can operate with the credentialing services that would be used by the EUAs.

SC-7.11.13 The PSBN ICAM framework SHOULD enable a set of guidelines and rules for applications to participate in the ICAM framework.

SC-7.11.14 The PSBN ICAM framework SHALL enable the PSBN-based applications and services to verify the identities of users irrespective of authorized administrator (both PSBN and EUA) management of the user's authentication credentials.

SC-7.11.15 The PSBN ICAM framework SHALL manage privileges for person and non-person entities.

SC-7.11.16 The PSBN ICAM framework SHALL enable applications and services to securely verify the identity of users.

SC-7.11.17 The PSBN ICAM services SHALL support industry standard authentication interfaces for mobile and fixed infrastructure components.

SC-7.11.18 The PSBN ICAM framework SHALL be standards based.

SC-7.11.19 The PSBN ICAM framework SHALL support identities being issued to non-person entities on the network.

SC-7.11.20 The PSBN ICAM framework SHALL enable non-person entities to authenticate to applications and services where authorized.

SC-7.11.21 The PSBN ICAM framework SHALL enable the process and procedures necessary for organizations (municipal, provincial, territory, and federal) to gain approval to join the ICAM framework.

SC-7.11.22 The agency, organization or entity that utilizes the PSBN ICAM framework SHOULD be responsible for enforcing authorization constraints on access to information as per their own security policy.

SC-7.11.23 The PSBN ICAM framework SHALL integrate with the PSBN SIEM for monitoring and reporting on user activity and security events.

SC-7.11.24 The PSBN ICAM system SHALL manage the initiation, capturing, recording and management of operator-user identities and their related access permissions.

SC-7.11.25 The PSBN ICAM system SHALL enable the process of operator-user provisioning and account setup.

SC-7.11.26 The PSBN ICAM system SHALL provide administrators with the ability to instantly view and change access rights.

SC-7.11.27 The PSBN ICAM system SHALL support all user authentication methods defined in the PSBN security policies.

SC-7.11.28 The PSBN ICAM system SHALL ensure that operator-users are properly authorized to access applications, data, and services through the use of Attribute Based Access Controls

(ABAC), Policy-Based Access Controls (PBAC), Role-Based Access Control (RBAC), and similar methods, as per the PSBN security policies.

SC-7.11.29 The PSBN SHOULD support implementation of a national Federated Identity Credential and Access Management (FICAM) framework to enable interoperability of user access management across administrative domains within the PSBN as well as between the PSBN and EUAs, where authorized.

SC-7.11.30 The PSBN SHALL ensure that only authorized personnel can provision services to end-users. This includes revoking services to users.

SC-7.11.31 The PSBN SHALL accept service requests from authorized users and UE devices only.

SC-7.11.32 The PSBN SHALL operate in a “Default Deny” security posture.

SC-7.11.33 The PSBN SHALL deny end-users the ability to modify the time on a UE device.

SC-7.11.34 The PSBN SHALL ensure that user profile data is accessible only to those administrators whose users pertain to their own agencies.

SC-7.11.35 The PSBN SHALL provide administrators with the means to restrict access to applications to authorized users only.

SC-7.11.36 The PSBN SHALL provide administrators the ability to set the access control rules and policies on a per-user basis.

SC-7.11.37 The PSBN SHALL provide administrators the means to restrict access to end-user data to authorized users only. For example, access to email mailboxes.

SC-7.11.38 The PSBN SHALL restrict access to the suite of Operations Support Systems (OSS) applications to authorized administrators only, and only to those applications that an administrator is authorized to access.

SC-7.11.39 The PSBN SHALL support the ability for users, when authorized, to override access control mechanisms during a state of emergency, in accordance to relevant policies.

7.12 IP network security

IP network security comprises best-practices in securing the IP network such as firewalls, use of secure IP protocols, VLAN segregation, and public internet isolation, as well as securing higher-level IP applications such as DNS. It includes the following key components.

7.12.1 Firewalls

Since the Internet Protocol (IP) is not secure, the PSBN should implement adequate security tools and procedures to prevent, monitor, log and correct any potential security breaches at all levels. This means implementing a firewall (FW) or border gateway (BG) as typically used in Mobile Network Operator (MNO) networks to enable Access Control Lists (ACL) or similar mechanisms.

A firewall is a fundamental security building block that provides network isolation at boundaries between network segments or between different networks. Security can be improved through the use of perimeter and distributed firewall filtering capabilities at strategic points within the network. A firewall performs isolation based on specific traffic filtering rules configured onto the firewall. It examines both inbound and outbound traffic, and should be configured to deny all traffic unless specifically allowed by the firewall rules. A firewall may also provide logging of traffic and trigger alarms when unauthorized packets are detected. Any of the following firewall capabilities may be used to provide protection on a given interface, and the choice will depend on security risks and impact on network performance.

- Static packet filtering, typically based on the packet source and destination IP addresses, the protocol type, and the TCP source and destination ports, thus providing an Access Control List (ACL);
- Application layer, which runs applications on behalf of the machines in the network they are protecting, and are often called "proxy" firewalls. Application layer firewalls can detect any anomalous activity and if found, do not pass the data onto the machines they are protecting;
- State aware packet filtering firewalls, which maintain information about the state of traffic connections allowing the firewall to make better decisions about whether to allow or deny particular traffic;
- Congestion control that provides signalling rate limiting and DoS/DDoS prevention for all IP protocols.

The NIST publication "Guidelines on Firewalls and Firewall Policy" [95] provides guidelines on firewalls and firewall policy.

7.12.2 VLAN

The PSBN should implement the security practice to separate/segregate management, control and user data traffic into different VLANs. VLANs serve the role of traffic separation and broadcast domain limitation and are used in almost every segment of the network. A VLAN is a group of network devices, such as servers and other network resources, that is configured to behave as if they were connected to a single network segment. In a VLAN, the resources and servers of other users in the network are invisible to each member of the other VLANs. The use of VLAN "tags" allows the segregation of traffic into specific groups such as user plane, control plane, and management-plane traffic. Separation of data without "leakage" between the VLANs is an important element for security.

In the context of MOCN where common backhaul is likely to be used, VLANs shall be used to segregate the traffic flows between a shared eNodeB and the core networks of the MOCN partners.

7.12.3 Secure IP protocols

To the extent possible, the PSBN should implement the most secure IP protocols available on both intra-network and inter-network IP interfaces, for instance:

- SNMPv3 providing authentication, integrity and encryption for network management traffic;
- IPSec protocol runs between the network layer (Layer 3) and the transport layer (Layer 4), and can be used to protect any type of data traffic (TCP or UDP), and is independent of applications. The set of security services offered by IPsec includes:
  - Data integrity
  - Data origin authentication based on IP address

    - Machine-to-machine authentication
    - Anti-replay protection
    - Data confidentiality
    - Cryptographic key exchange
- The Secure Sockets Layer (SSL/TLS) security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection at the transport layer (Layer 4).

7.12.4 DNS security

The PSBN will be required to host the following types of Domain Name Systems (DNS):

- An external DNS to be used for resolution of domain names into public IP addresses to access internet resources;
- An internal DNS to be used intra-network for resolution of domain name, load-sharing and failover scenarios, as well as zero-configuration service discovery.

The PSBN security practice should maintain completely separate DNS servers (internal DNS vs external DNS) that have no knowledge of each other. The external DNS server shall have no records of the internal DNS server.

The PSBN DNS security policy should also consider the following elements:

- Because external DNS data is meant to be public, preserving the confidentiality of DNS data pertaining to publicly accessible IP resources is not a concern. The primary security goals for DNS are data integrity and source authentication, which are needed to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit. The PSBN shall follow the best practices in maintaining data integrity and performing source authentication.
- Availability of DNS services and data is also very important; DNS components are often subjected to denial-of-service attacks intended to disrupt access to the resources whose domain names are handled by the attacked DNS components. The PSBN shall follow the best practices in configuring the DNS to prevent many denial-of-service attacks that exploit vulnerabilities in various DNS components.

The GSMA document “DNS Guidelines for Operators” [96] provides recommendations on DNS to facilitate successful interworking of inter-Service Provider services.

The NIST publication “Secure Domain Name System (DNS) Deployment Guide” [97] provides security guidelines with regards to DNS deployment in enterprise.

7.12.5 Public internet isolation

Most hackers initiate attacks towards private networks via poorly secured internet connections or gateways from the public internet. The inter-operator IP backbone and service provider networks used by the PSBN shall not be advertised to the public internet and shall not be accessible from the internet. Ideally, the infrastructure used to carry inter-operator IP backbone traffic shall be separate from the one used to provide access to the public internet. Detection systems should be used to identify unauthorized network access attempts and should produce full audit logs for any event, tracing and resolution.

SC-7.12.1 The PSBN SHALL implement separate addressing spaces for user plane data, management plane data, and control/signalling plane data within the core network such that any one data plane cannot be accessible from either of the other two data planes.

SC-7.12.2 The PSBN SHALL implement non-publicly routable IP address spaces for the PSBN network elements, including user devices.

SC-7.12.3 The PSBN SHALL implement IP security mechanisms according to industry standards to protect the information that crosses network and sub-network security boundaries.

SC-7.12.4 PSBN servers that are exposed to the internet SHALL be protected from Denial of Service attacks.

SC-7.12.5 The PSBN SHALL employ security measures to prevent duplicate IP addresses from being present on any IP address space.

SC-7.12.6 Internal IP address information SHALL be available to authorized personnel only.

SC-7.12.7 The PSBN SHALL encrypt IP address headers for packets containing management information and signalling/control information that is specific to the PSBN, when such information traverses security domains.

SC-7.12.8 The PSBN SHALL provide a Certificate Validation service and directory service for the management of encryption keys and X.509 certificates [98].

SC-7.12.9 The PSBN SHALL hide the topologies and address spaces of the PSBN IP networks.

SC-7.12.10 The PSBN SHALL create a firewall policy that specifies how firewalls handle inbound and outbound network traffic.

SC-7.12.11 The PSBN SHALL implement firewalls to separate external networks as well as internal networks across different security domains and follow industry best practices with regards to firewall policies such as outlined in NIST 800-41 “Guidelines on Firewalls and Firewall Policy.” [95]

SC-7.12.12 Within a security domain, the PSBN SHOULD make use of VLANs to segregate traffic from different contexts or domains such as between control, user, and management planes.

SC-7.12.13 To the extent possible, the PSBN SHOULD implement the most secure IP protocols and versions available, (e.g., SSL, SNMPv3, SSH, TLS, HTTPS, IPSec).

SC-7.12.14 The PSBN SHALL implement industry best practices with regards to DNS policies such as outlined in NIST Special Publication 800-81-2 Secure “Domain Name System (DNS) Deployment Guide.” [97]

SC-7.12.15 The PSBN SHALL follow industry best practices with regards to security guidelines for DNS interworking between service providers as outlined in GSMA DNS Guidelines for Operators [96].

SC-7.12.16 The PSBN SHALL maintain completely separate DNS servers (internal DNS vs external DNS) that have no knowledge of each other.

SC-7.12.17 The PSBN SHALL deploy a secure DNS solution with completely separate and distinct DNS domains/zones for transport networks, the evolved packet core, the roaming network, and the SGi interface.

SC-7.12.18 The PSBN SHOULD exclusively use inter-operator IP networks that are not accessible from the internet.

7.13 Mobile VPN

Today, public safety agencies that use commercial services to access restricted data on their agency's network secure the communications using a mobile VPN. A VPN is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between the UE and a VPN endpoint in the network. A VPN can provide several types of data protection, including confidentiality, integrity, data origin authentication, replay protection and access control.

Since the commercial cellular network may serve as a backup service to the PSBN service, the use of mobile VPN service will continue for some agencies. Public safety agencies should plan their mobile device security on the assumption that the networks between the mobile device and the organization may not be always trusted. Risk from use of untrusted networks can be reduced by using mobile VPN to protect the confidentiality and integrity of communications, as well as using mutual authentication mechanisms to verify the identities of both endpoints before transmitting data.

The PSBN shall host a mobile VPN endpoint to support a mobile VPN service.

The NIST publication "Guide to IPsec VPNs" [99] provides guidelines on IPsec VPNs.

SC-7.13.1 The PSBN SHALL support an agency's ability to perform a secondary authentication before allowing an PSBN user to connect with an EUA network.

SC-7.13.2 The PSBN SHALL support a communication path between an agency's PSBN user and the EUA network without imposing a NAT.

SC-7.13.3 The PSBN SHALL support local IP applications in the EUA network.

SC-7.13.4 The PSBN SHALL support transport of VPN traffic from an PSBN user to the EUA network.

SC-7.13.5 The PSBN SHALL support transport of prioritized traffic from/to the EUA network.

SC-7.13.6 The PSBN SHALL host a mobile VPN endpoint to support a mobile VPN service.

SC-7.13.7 The PSBN MAY implement industry best practices with regards to IPSec VPNs such as outlined in NIST publication “Guide to IPsec VPNs.”

7.14 System security hardening (UE and node)

In general computing terms, hardening is usually the process of securing a system by reducing its surface of vulnerability. Hardening includes measures implemented during the development lifecycle as well during the initial installation of the system. The PSBN shall implement or enforce industry-recognized best practices on system security hardening.

7.14.1 Network node hardening

The LTE infrastructure runs off of commodity hardware and software, and is therefore susceptible to hardware and software flaws pervasive in any general purpose operating system or application. One approach is to reduce, via a secure system development lifecycle, the amount of potential entry points for an attacker by hardening nodes against attacks. 3GPP has been working on specifying hardening for network nodes so that their security can be tested and certified. This kind of hardening reduces the attack space for an attacker substantially and offers better protection for the network infrastructure in general from unauthorized usage. The specifications are:

- TS 33.117 [100] provides a catalogue of security requirements and related test cases that are deemed applicable, possibly after adaptation, to several network product classes.
- TS 33.116 [22] contains objectives, requirements and test cases that are specific to the MME network product class. It refers to TS 33.117 [100] and formulates specific adaptations of the requirements and test cases given there, as well as specifying requirements and test cases unique to the MME network product class.
- TS 33.216 [101] contains objectives, requirements and test cases that are specific to the eNodeB network product class. It refers to TS 33.117 [100] and formulates specific adaptations of the requirements and test cases given there, as well as specifying requirements and test cases unique to the eNodeB network product class.
- TS 33.250 [102] contains requirements and test cases that are specific to the P-GW network product class. It refers to TS 33.117 [100] and formulates specific adaptations of the requirements and test cases given there, as well as specifying requirements and test cases unique to the P-GW network product class.

The GSMA Security Assurance Group (SECAG), a sub-group of the Fraud and Security Group (FASG), is expected to administer the Network Equipment Security Assurance Scheme (NESAS), based on 3GPP Security Assurance Methodology (SECAM) security requirements.

7.14.2 Application server hardening

The NIST Special Publication Guide to General Server Security [103] is intended to assist organizations in installing, configuring, and maintaining secure servers. More specifically, it describes in detail the following practices to apply:

- Securing, installing, and configuring the underlying operating system;
- Securing, installing, and configuring server software;
- Maintaining the secure configuration through application of appropriate patches and upgrades, security testing, monitoring of logs, and backups of data and operating system files.

7.14.3 UE hardening

PSBN mobile devices shall be capable of providing strong security assurances to public safety end-users and agencies. For that purpose, the PSBN shall enforce the best-in-class guidelines with regards to security primitives and capabilities on mobile devices.

The NIST Publication Guidelines on Hardware-Rooted Security in Mobile Devices [104] is centred on three security capabilities to address known mobile device security challenges. They are device integrity, isolation and protected storage. A tablet or phone supporting device integrity can provide information about its configuration, health and operating status that can be verified by the organization whose information is being accessed. Isolation capabilities are intended to keep personal and organization data components and processes separate. That way, personal applications should not be able to interfere with the organization's secure operations on the device. Protected storage keeps data safe using cryptography and restricting access to information.

To attain the security capabilities, NIST guidelines recommend that every mobile device implement three security components. These are foundational security elements that can be used by the device's operating system and its applications. They are:

- Roots of Trust, which are combinations of hardware, firmware and software components that are designed to provide critical security functions with a very high degree of assurance that they will behave correctly;
- An application programming interface that allows operating systems and applications to use the security functions provided by the roots of trust;
- A policy enforcement engine to enable the processing, maintenance and policy management of the mobile device.

7.14.4 IoT devices (M2M/MTC devices)

GSMA has published a series of security guidelines specifically targeted at IoT and MTC devices.

GSMA CLP.17 IoT Security Assessment [105] provides a flexible framework enabling suppliers to build secure IoT devices and solutions via a comprehensive set of best practices promoting the secure end-to-end design, development and deployment of IoT solutions.

GSMA CLP.12 IoT Security Guidelines for Iot Service Ecosystem [106] shall be used to evaluate all components in an IoT product or service from the Service Ecosystem perspective. The Service Ecosystem includes all components that make up the core of the IoT infrastructure. Components in this ecosystem are, for example, services, servers, database clusters, network elements, and other technologies used to drive the internal components of any product or service.

GSMA CLP.13 IoT Security Guidelines for IoT Endpoint Ecosystem [107] shall be used to evaluate the components of an IoT Service from the IoT Endpoint Device perspective. An Endpoint, from an IoT perspective, is a physical computing device that performs a function or task as a part of an internet connected product or service. An Endpoint, for example, could be a wearable fitness device, an industrial control system, an automotive telematics unit or even a personal drone unit. All technologies used to drive the physical device shall be evaluated for security risks. The result is a practical set of design guidelines that allow the reader to identify and remediate almost all potential risks to the IoT Service.

SC-7.14.1 PSBN UEs SHALL be hardened so that boot loaders, which initiate the Operating System (OS) of the device, SHALL not be allowed to be tampered with by malware.

SC-7.14.2 PSBN UEs SHALL be hardened so that every application and even large portions of the OS run inside their own isolated sandbox also called an AppContainer.

SC-7.14.3 PSBN UE's secured container solution SHOULD be used to protect agency applications and user data in mobile devices.

SC-7.14.4 PSBN UEs SHOULD be continuously monitored both online and offline to ensure the OS is not compromised and that devices have not been "jail broken" or "rooted."

SC-7.14.5 The PSBN SHALL follow 3GPP system security hardening practices for LTE network elements as specified in TS 33.117 [100], 33.116 [22], 33.216 [101], and 33.250 [102].

SC-7.14.6 The PSBN SHALL implement the industry best practices with regards to server hardening such as described in NIST 800-123 [103].

SC-7.14.7 The PSBN SHALL implement the industry best practices with regards to UE hardening such as described in NIST 800-164 [104] and 1800-4b [83].

SC-7.14.8 The PSBN SHALL implement the industry best practices with regards to IoT device and system hardening such as described in GSMA CLP.17 [105], CLP.12 [106], and CLP.13 [107].

7.15 Intrusion detection and prevention system

As per the NIST definition, an Intrusion Detection System (IDS) is a software that automates the process of detecting possible security incidents, which are violations or imminent threats of violation of the network's security policies. An Intrusion Prevention System (IPS) is a software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. An integrated IDS and IPS is referred to as IDPS in this document.

IDPSs are primarily focused on:

- Identifying possible incidents, by comparing network traffic and hosting log entries to match data signatures, traffic patterns and host address profiles indicative of hackers;
- Logging and recording information about them;

- Attempting to head them off, either by stopping the attack itself, changing the security environment, such as by modifying firewall rules or router filters, or changing the attack's content;
- Reporting the suspicious activities to security administrators or other security systems via alarms or other configurable responses.

IDPSs are a necessary addition to the security infrastructure of the PSBN particularly at security boundaries such as the internet access points. They can be network-based or host-based: a network-based IDPS typically involves one or many devices running on pre-configured appliances and installed at critical points on the network to monitor particular network segments or devices; a host-based IDPS requires that software be installed directly on the servers to be protected, and monitors the network connections, the user activity, and the events occurring on those servers. Some host-based IDPSs are actually specified in some 3GPP functional entities, for instance the IMS-ALG (Application Level Gateway) specified in TS23.228 [108] which monitors SIP signalling in order to detect malicious attack. The IMS-ALG is a functional entity of the IBCF (Interconnection Border Control Function) in P-CSCF.

IDPSs can be wireline or wireless, with wireless IDPS monitoring wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves. IDPSs use signature-based and/or anomaly-based analysis to detect security problems within network traffic, which is more than stateful firewalls do.

The NIST Special Publication Guide to Intrusion Detection and Prevention Systems (IDPS) [109] describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining them.

SC-7.15.1 The PSBN SHALL employ probes and other monitoring measures to be able to detect intrusion of viruses and other forms of malware.

SC-7.15.2 The PSBN SHALL employ measures to monitor public safety traffic for the possible inclusion of malware, in accordance to privacy policies.

SC-7.15.3 The PSBN SHALL employ measures to block or filter malware from intruding into the PSBN.

SC-7.15.4 The PSBN SHALL be capable of removing malware from any of its servers and databases.

SC-7.15.5 The PSBN SHALL notify an intended recipient and an administrator of a message containing malware and of the action that was taken to remove the malware.

SC-7.15.6 The PSBN SHALL employ security measures to identify malware and to quarantine or delete malware.

SC-7.15.7 The PSBN interfaces at the network's perimeter as well as between trust domains and possibly security domains SHALL be monitored by Intrusion Detection and Prevention Systems (IDPS).

SC-7.15.8 The PSBN SHALL monitor and protect against threats at any provided internet access points within the PSBN trusted zone.

SC-7.15.9 The PSBN MAY inspect all network traffic based upon encryption level at security boundaries for malware and viruses.

SC-7.15.10 The PSBN MAY implement the industry best practices for Intrusion Detection and Prevention Systems (IDPS), such as outlined in NIST Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) [109].

7.16 Security Information and Event Management SIEM) system

The PSBN security architecture should include a Security Information and Event Management (SIEM) system—a tool focused on the security aspects of log management, which involves collecting, monitoring, and analyzing security-related data from computer and network element logs. Security-related data includes log data generated from numerous sources, including antivirus software, intrusion detection systems, file systems, firewalls, routers and switches, and servers. SIEM is responsible for the aggregation and normalization of security-related data and allows for analysis on a large number of logs in an efficient manner.

SIEM software is designed to import information from various security-related logs and correlate events among them. Log types commonly supported by SIEM software include IDPSs, firewalls, antivirus software, and other security software; OSs (e.g., audit logs); application servers (e.g., Web servers, e-mail servers); and even physical security devices such as badge readers. SIEM software generally works by receiving copies of the logs from the logging hosts over secure network channels, converting the log data into standard fields and values (known as normalization), then identifying related events by matching IP addresses, timestamps, usernames, and other characteristics. SIEM products can identify malicious activity such as attacks and malware infections, as well as misuse and inappropriate usage of systems and networks. Some SIEM software can also initiate prevention responses for designated events. SIEM products usually do not generate original event data; instead, they generate meta-events based on their analysis of the imported event data.

Ways in which SIEM software complements IDPSs include the following:

- SIEM software can identify some types of events that individual IDPSs cannot because of its ability to correlate events logged by different technologies.
- The consoles for SIEM software can make data from many sources available through a single interface, which can save time for users that need to monitor multiple IDPSs. SIEM consoles also may offer analysis and reporting tools that certain IDPSs' consoles do not.
- Users can more easily verify the accuracy of IDPS alerts because the SIEM may be able to link each alert to supporting information from other logs. This can also help users to determine whether or not certain attacks succeeded.

The NIST Special Publication Guide to Computer Security Log Management [110] seeks to assist organizations in understanding the need for sound security log management. It provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. The publication presents log management technologies from a high-level viewpoint.

SC-7.16.1 The PSBN SHALL record all log-on/off actions by personnel accessing the control and monitoring functions of network elements.

SC-7.16.2 The PSBN SHALL record all actions taken by authorized users engaged in the process of configuring or controlling any aspect of the PSBN, including user profiles.

SC-7.16.3 The PSBN SHALL preserve entry/exit logs in a protected manner such that the logs can only be accessed by authorized personnel.

SC-7.16.4 The PSBN SHALL preserve log-on/off records of personnel accessing the configuration and monitoring functions of network elements in a protected manner such that the records can only be accessed by authorized personnel.

SC-7.16.5 The PSBN SHALL preserve change history logs of the configuration and control actions taken by authorized users in a protected manner such that the records can only be accessed by authorized personnel.

SC-7.16.6 The PSBN SHALL host the means to preserve history logs of the services and applications that were accessed by end-users in a protected manner such that the records can only be accessed by authorized personnel.

SC-7.16.7 The PSBN SHALL host the means to preserve network administrator records and logs for a period of time in accordance with relevant policies.

SC-7.16.8 The PSBN SHALL include mechanisms to trace the path of messages in the PSBN from the network element that is the source of control messages to all the downstream network elements.

SC-7.16.9 The PSBN SHALL maintain a history log of PSBN-hosted applications that an end-user accessed on the PSBN, according to relevant policies for retention of such information.

SC-7.16.10 The PSBN SHALL maintain a history log of OSS and other management applications that administrator-users accessed on the PSBN, according to relevant policies for retention of such information.

SC-7.16.11 The PSBN SHALL establish methods and techniques to conduct security monitoring across the PSBN environment.

SC-7.16.12 The PSBN SHOULD host a Security Information and Event Management (SIEM) solution to enable security analysis of large volumes of collected data and enable interfaces for information sharing purposes.

SC-7.16.13 The PSBN SIEM solution SHOULD allow for real-time analysis of log files and for real-time alerting to the Security Operations Center with vital security reports and information.

SC-7.16.14 The PSBN SHALL store security-related records and logs in an infrastructure secure

	against unauthorized access or destruction.
SC-7.16.15	The PSBN SHALL follow industry best practices with regards to SIEM such as NIST 800-92 [110].

7.17 High availability and resiliency network design

High-availability and resiliency are key security attributes of the PSBN. The PSBN should be designed to minimize or entirely eliminate the impact of equipment or component failures that result in a loss of data throughput or coverage, and be designed in a manner that promotes the network's quick return to optimal performance. In case of failure of the servers that host applications, it is necessary to ensure that a fail-over to another server instance of the applications occurs in order to provide continuity of service to the end-users.

A potential risk that impacts the integrity of control/signalling information, configuration settings, and management information is the possibility of corruption due to events such as power failures during database write-cycles. Updates to the firmware of network elements that change the location of data fields in message strings could also corrupt data if the message parsing function is also not updated. Changes to the network elements' hardware or firmware that require coordination to simultaneously upgrade multiple components of the PSBN across jurisdictional domains (e.g., between National Entity and RSDEs) are a potential source of interoperability problems.

High-availability of the PSBN can be achieved by minimizing the probability of network faults. When faults occur, resiliency mechanisms minimize their impacts and their duration, thus improving network availability when faults are active. Resiliency is synonymous with survivability such that the PSBN may continue to operate during disasters.

Availability and resiliency can be achieved through several infrastructure strategies:

- Harden sites to withstand severe environmental conditions and long duration disaster events; this is covered in Section 7.1;
- Provide alternative coverage solutions such as deployables; this is covered in the TCO [3];
- Protect all active network elements with redundant network elements, eliminating single points of failure; this is covered in the TCO;
- Provide high-availability, fault-tolerant, low or no downtime UEs and applications; this is covered in the TCO;
- Protect against denial of service attacks and cyber-induced failures through predictive analytics, intrusion detection, and fault isolation techniques; this is covered in Section 7.15;
- Implement network congestion control mechanisms, this is covered in the TCO.

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

The Technical Considerations on Operability [3] document addresses resiliency and reliability of the PSBN through several approaches:

- Redundancy of the network elements, facilities, and backhaul;
- Hardening of the facilities;
- Layered resiliency by using alternative access technologies;
- Supplementing the PSBN with deployable systems.

The considerations in this section cover the security measures that impact the availability of the PSBN and the services it offers, complementing the considerations already covered in the Technical Considerations on Operability document.

SC-7.17.1 The PSBN SHALL enable an authorized network administrator the ability to ensure that the network elements used for the PSBN are approved for such use.

SC-7.17.2 The PSBN SHALL enable an administrator to isolate portions of the PSBN that are infected with malware or not operating properly until the issue has been resolved.

SC-7.17.3 The PSBN SHALL employ measures to detect radio interference levels from external sources that may negatively impact the availability of one or more base stations (eNodeBs).

SC-7.17.4 The PSBN SHALL report when the availability has been negatively impacted by external radio interference or by other means.

SC-7.17.5 The design plan and assignment of LTE Network Identifiers SHALL be available to authorized personnel only.

SC-7.17.6 The PSBN SHALL retain images of prior configuration settings and network elements' firmware so that the PSBN can be restored to a prior known operating state, if needed, in accordance to relevant policies.

SC-7.17.7 The PSBN SHALL prevent power failures, equipment failures and other service-disruptive events from corrupting the information that is in-transit or stored within the PSBN, according to availability and resiliency objectives for the PSBN.

SC-7.17.8 The PSBN SHALL ensure that, when any network element of the PSBN, including UE devices, has been upgraded, the new upgrades SHALL only become operative after suitable acknowledgements and integrity checks have been completed.

SC-7.17.9 The PSBN SHALL employ security measures to protect the network services against denial-of-service attacks from misbehaving applications. For example, the PSBN SHALL prevent a service-request flood from causing a particular service from freezing into an undetermined state.

SC-7.17.10 The PSBN SHALL employ measures to re-start network services into a known operating state such as when recovering from failures.

SC-7.17.11 The PSBN SHALL ensure that administrators can access their respective, authorized management and control functions in case the PSBN identity and credentials management systems are compromised.

SC-7.17.12 When a user device's operating system, application client, or virus definition files are being remotely updated, the user device SHALL continue to operate in its non-upgraded state until the download process has concluded the requisite integrity checks.

SC-7.17.13 The PSBN SHALL enable administrators to remotely reset network elements on the PSBN, including public safety UE devices, into a known configuration state, according to the jurisdictional authority of each administrator.

SC-7.17.14 The PSBN SHALL provide a secure data back-up and restoration service for all data that resides within the PSBN.

SC-7.17.15 The PSBN SHALL ensure that the mirrored copies of the applications will operate in the same manner as the original applications and access the same or equivalent network resources and databases they require to operate.

7.18 Encryption

All IP and 3GPP network security protocols rely on underlying cryptographic algorithms to provide the security services. The choice of particular cryptographic algorithms and key lengths for use within the PSBN will be based on the PSBN security policies and no specific recommendations can be made at this point in time in this document. However, at a minimum, radios should support AES encryption and 128- or 256-bit symmetric keys, via a randomly generated encryption combination. These combinations are created and negotiated between links using industry-standard key agreement methods, which supports modulo of at least 2048 bits. Payload Encryption should be implemented in compliance with FIPS-197, which provides the definition for AES encryption. AES is commonly regarded as one of the leading worldwide encryption schemes accepted by the most demanding entities such as US Government and US Military.

SC-7.18.1 The PSBN SHALL implement and enforce the encryption algorithms and key lengths as per the PSBN security policies.

7.19 Data security

All data in transit, accessed, or stored across the PSBN environment shall be encrypted, restricted, retained and destroyed as per PSBN security policies and the data owner requirements. Data in the PSBN should not be releasable to any external parties without compliance with applicable laws.

Many applications that are expected to be served by the PSBN will require information from the PSBN, such as location, usage, and user profiles. It is expected that administrators will access this information through a type of monitoring application, or as in the case of user profiles, via a service provisioning application. Some information such as the user profiles for all PSBN users will likely be contained in centralized databases.

The level of sensitivity of the information carried over the PSBN is a matter for the user community and the operators of the PSBN to determine and agree on. The Government of Canada has issued a policy document on the level of protection to apply to classified information [111]. The policy states that classified information is expected to be protected using suite-B algorithms.

SC-7.19.1 The PSBN SHALL implement security measures to protect the integrity of data on all three data planes—user data, control/signalling data, and management data.

SC-7.19.2 The PSBN SHALL employ measures that ensure privacy of the information that is processed or routed by the PSBN in compliance with applicable laws of the Government of Canada with respect to privacy and confidentiality.

SC-7.19.3 The PSBN SHALL employ measures to ensure the privacy of the information that is processed or routed by the PSBN commensurate with the classification of the information as determined by the Government of Canada.

SC-7.19.4 The PSBN SHALL encrypt all data that is transferred from the PSBN security zones onto removable media when such transfer is authorized.

SC-7.19.5 If protected or classified information is carried over the PSBN, the PSBN SHALL comply with the applicable Government of Canada policies.

7.20 Security management

Security management comprises all activities to establish, maintain and terminate the security aspects of the PSBN. Security management includes the following set of functions:

- Prevention via system hardening, secure communication protocols, security policies and processes;
- Detection via security event monitoring and reporting of activities that may be construed as a security violation (unauthorized user, physical tampering with equipment);
- Containment and recovery via disablement and backup and restore;
- Security administration and enforcement of user access and security key management.

The Security Operations Center (SOC) is a facility that houses an information security team responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported. The objectives of the PSBN SOC include but are not limited to:

- Situational awareness that includes collecting, maintaining, and sharing information related to threats to network infrastructure, devices, data, and applications;
- 24/7/365 cybersecurity monitoring of network infrastructure, devices, data, and applications;
- Monitoring and analysis of user, system, and network access;
- Assessment of system and data file integrity;
- Establishment of the baseline network activity and utilization;
- Recognition and analysis of activity patterns that are indicative of an incident or intrusion;
- Analysis of logs for abnormal use patterns;

- Information sharing and collaboration that integrates and disseminates information throughout the critical infrastructure partnership network;
- Processing and posting suspicious activity reports;
- Assessment and analysis that evaluates infrastructure data for accuracy, importance, and implications;
- Decision support that provides recommendations to partners and the PSBN leadership.

The PSBN security management should account for a Security Incident Response Team that will be responsible for managing incident response.

To implement the security management functions, the SOC infrastructure would include the following PSBN entities that provide security services:

- Key Management Server; covered in this section;
- Identity Management Server; this is covered in Sections 7.6 and 7.11;
- Bootstrapping Server Function (BSF); this is covered in Section 7.6;
- Network Application Functions (NAF); this is covered in Section 7.6;
- Equipment Identity Register (EIR); this is covered in Section 7.9;
- Security Gateway (SeGW); this is covered in Section 7.3;
- Firewall; this is covered in Section 7.12;
- VPN Server; this is covered in Section 7.13;
- Security Information and Event Management (SIEM); this is covered in Section 7.16;
- Intrusion Detection and Protection System (IDPS); this is covered in Section 7.15.

The technical security considerations related to the functions and entities mentioned above are covered in different sections of this document. The only exception is with regards to Key Management Server or Public Key Infrastructure discussed below.

Key management server—Public Key Infrastructure (PKI)
The PSBN shall consider implementing a public key infrastructure if a scalable key management is required for the inter-domain interfaces of the PSBN. To create a PKI, the PSBN would need to establish the policies, procedures, hardware, software and personnel responsible for creation, management, distribution, use, storage, and verification practices of the digital certificates that provide the key material for the network.

Different applications have different requirements on a PKI, and it is often easier to implement multiple and simpler PKIs for each purpose, rather than building one single PKI that addresses all needs.

There are two types of PKIs

- Certification Authorities for network entities within the PSBN
- Certification Authorities for network entities within and outside the PSBN

NIST Special Report 800-32 [112] provides an overview of PKI functions and their applications, and can assist in determining if a PKI is appropriate, and how PKI services can be deployed most effectively.

SC-7.20.1 The PSBN SHALL implement security controls that satisfy the PSBN security requirements.

SC-7.20.2 The PSBN SHALL enable the security policies encompassing prevention, detection, containment and recovery, and administration and enforcement.

SC-7.20.3 The PSBN SHALL establish a Security Operations Center (SOC) to prevent, detect, and resolve security incidents.

SC-7.20.4 The PSBN MAY establish a Public Key Infrastructure to be used to secure the interfaces crossing security domains.

8 Conclusion

Security is of utmost importance for the PSBN. The PSBN will be an IP-based LTE network, interconnected with both public and private networks, and possibly sharing the Band 14 spectrum with commercial users. As described in the TCO [3], the PSBN has characteristics that extend beyond those of a commercial mobile network, including:

- A network based on a single PLMN-ID but that is possibly operated by different operating entities;
- The support of mission-critical services and related service enablers;
- The support of deployable systems;
- The interworking between an LTE-based MCPTT system and an LMR-based system;
- The support of a Federated Identity, Credentialing, and Access Management (FICAM) service providing the means by which user's credentials can be can be exchanged securely across multiple devices, applications, and networks;
- QoS and Congestion Control (Priority and Pre-emption) mechanisms for mission-critical services and applications;
- A network with public-safety grade availability and resiliency;
- A local control granted to End-User Agencies with regards to service provisioning and management, QoS and priority, HeNodeB and deployables ownership, and user credentials.

As such, the PSBN will be exposed not only to security threats that commercial networks face today, but also to threats that will be specific to the PSBN. It is therefore recommended that the PSBN implement to the extent possible all security features that are available in the different protocols used in the PSBN, as well as security measures that are tailored to the security needs of the PSBN.

Security considerations in this document follow industry-accepted standards for security, as it increases interoperability as well as avoids duplication of efforts. The security considerations will need to be reviewed to align with the PSBN security policies.

While the recommendations contained in this document are broad in scope, they do not suggest that the full scope of what is described therein should be implemented at the outset of the PSBN or at one time. Indeed, it would be prudent to stage the implementation of the PSBN in a time-phased manner in support of a capability roadmap that the PSBN operators are likely to develop.

References

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

[2] Public Safety Canada, “Communications Interoperability Strategy for Canada,” Jan.2011. WEB. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/index-eng.aspx>, Accessed 14 April 2018.

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

[4] Defence Research and Development Canada Centre for Security Science, Scientific Report, DRDC-RDDC-2019-R236, “Public Safety Broadband Network (PSBN) - Network Architecture Description,” January 2019.

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

[6] Innovation, Science and Economic Development Canada, SNSE-014-17 “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 763–788 MHz and 793–798 MHz (PSBB Block),” June 2017, WEB. <https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11289.html>, Accessed 14 April 2018.

[7] International Telecommunications Union, Recommendation ITU-T X.805, “Security architecture for systems providing end-to-end communications,” October 2003.

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

[9] National Institute of Standards and Technology, Mobile Threat Catalogue, WEB. <https://pages.nist.gov/mobile-threat-catalogue>, Accessed 14 April 2018.

[10] J.Franklin, C.Brown, S.Dog, N.McNab, S.Voss-Northrop, M.Peck, B.Stidham, “Assessing Threats to Mobile Devices & Infrastructure – The Mobile Threat Catalogue,” National Institute of Standards and Technology, (Draft) NISTIR 8144, September 2016.

[11] US Department of Homeland Security, “Study on Mobile Device Security,” April 2017.

[12] 3GPP TS 33.402, “3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses,” v14.3.0, September 2017.

[13] W.Burr, D.Dodson, E.Newton, R.Perlner, W.Polk, S.Gupta, E.Nabbus, “Electronic Authentication Guideline,” National Institute of Standards and Technology, Special Publication 800-63-1, Dec. 2011.

[14] Communications Security Establishment Canada, ITSG-33 "IT Security Risk Management: A Lifecycle Approach," March 2012. WEB. <http://www.itsecurityguidance.ca/ITSG33%20Documentation/Forms/AllItems.aspx>, Accessed 14 April 2018.

[15] International Telecommunications Union, Recommendation ITU-T X.800, "Security Architecture for Open Systems Interconnection for CCITT Applications - Series X: Data Networks and Open System Communication Security," 22 March 1991.

[16] National Public Safety Telecommunications Council, "Defining Public Safety Grade Systems and Facilities," May 22, 2014.

[17] National Public Safety Telecommunications Council, "Public Safety Broadband High-Level Launch Requirements: Statement of Requirements for FirstNet Consideration," Dec. 7, 2012. WEB <http://www.npstc.org/download.jsp?tableId=37&column=217&id=1439&file=Public%20Safety%20700MHz%20Broadband%20SoR%20v0_6.pdf>. Accessed 14 April 2018.

[18] 3GPP TS 33.187, "Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements," v14.1.0, January 2018.

[19] 3GPP TS 22.022, "Personalisation of Mobile Equipment (ME); Mobile functionality specification," v14.0.0, March 2017.

[20] 3GPP TS 33.102, "3G security; Security architecture," v14.1.0, March 2017.

[21] 3GPP TS 33.110, "Key establishment between a Universal Integrated Circuit Card (UICC) and a terminal," v14.0.0, March 2017.

[22] 3GPP TS 33.116, "Security Assurance Specification (SCAS) for the MME network product class," v14.1.0, June 2017.

[23] 3GPP TS 31.101, "UICC-terminal interface; Physical and logical characteristics," v14.2.0, December 2017.

[24] 3GPP TS 33.259, "Key establishment between a UICC hosting device and a remote device," v14.0.0, March 2017.

[25] IEEE 802.11i-2004, "IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements," 24 June 2004.

[26] 3GPP TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture," v15.2.0, January 2018.

[27] 3GPP TS 33.320, "Security of Home Node B (HNB) / Home evolved Node B (HeNB)," v14.0.0, December 2016.

[28] 3GPP TS 33.210, “3G security; Network Domain Security (NDS); IP network layer security,” v14.0.0, December 2016.

[29] 3GPP TS 33.310, “Network Domain Security (NDS); Authentication Framework (AF),” v14.0.0, December 2016.

[30] 3GPP TS 33.204, “3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security,” v14.0.0, March 2017.

[31] 3GPP TS 33.203, “3G security; Access security for IP-based services,” v15.0.0, September 2017.

[32] 3GPP TS 33.328, “IP Multimedia Subsystem (IMS) media plane security,” v14.0.0, March 2017.

[33] 3GPP TS 33.141, “Presence service; Security,” v14.0.0, March 2017.

[34] 3GPP TS 33.163, “Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST),” v15.2.0, January 2018.

[35] 3GPP TS 33.180, “Security of the mission critical service,” v15.0.0, January 2018.

[36] 3GPP TS 23.283, “Mission Critical Communication Interworking with Land Mobile Radio Systems,” v15.0.0, April 2018.

[37] 3GPP TS 33.303, “Proximity-based Services (ProSe); Security aspects,” v14.1.0, June 2017.

[38] 3GPP TS 33.246, “3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS),” v14.2.0, September 2017.

[39] 3GPP TS 33.220, “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA),” v15.0.0, June 2017.

[40] 3GPP TS 33.222, “Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS),” v14.0.0, March 2017.

[41] 3GPP TS 33.223, “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function,” v14.0.0, March 2017.

[42] 3GPP TS 33.224, “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push Layer,” v14.0.0, March 2017.

[43] 3GPP TS 33.221, “Generic Authentication Architecture (GAA); Support for subscriber certificates,” v14.0.0, December 2016.

[44] 3GPP TS 23.222, “Common Application Programming Interface (API) framework for 3GPP northbound APIs,” v15.0.0, January 2018.

[45] 3GPP TS 32.371, “Telecommunication management; Security Management concept and requirements,” v14.0.0, March 2017.

[46] 3GPP TS 32.372, “Telecommunication management; Security services for Integration Reference Point (IRP); Information Service (IS),” v14.0.0, March 2017.

[47] 3GPP TS 32.376, “Telecommunication management; Security services for Integration Reference Point (IRP); Solution Set (SS) definitions,” v14.1.0, June 2017.

[48] Open Mobile Alliance “OMA Device Management Security,” May 2010.

[49] Treasury Board of Canada, “Operational Security Standard on Physical Security,” 18 February 2013, WEB. <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329&section=text#cha7>. Accessed 14 April 2018.

[50] 3GPP TS 22.346, “Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1,” v14.0.0, March 2017.

[51] 3GPP TS 23.402: “Architecture enhancements for non-3GPP accesses,” v15.2.0, December 2017.

[52] IEEE 802.11-2016, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 07 December 2016.

[53] M.Souppaya, K.Scarfone, “Guidelines for Securing Wireless Local Area Networks (WLANs),” National Institute of Standards and Technology, Special Publication 800-153, 2012.

[54] S.Frankel, B.Eydt. L.Owens, K.Scarfone, “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i,” National Institute of Standards and Technology, Special Publication 800-97, February 2007.

[55] ETSI/SAGE Specification, “Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification,” v1.1, 06 September 2006.

[56] 3GPP TS 35.205, “3G Security; Specification of the MILENAGE algorithm set; Document 1,” v14.0.0, March 2017.

[57] 3GPP TS 35.206, “3G Security; Specification of the MILENAGE algorithm set; Document 2,” v14.0.0, March 2017.

[58] 3GPP TS 23.335: “User Data Convergence (UDC); Technical realization and information flows,” v14.0.0, March 2017.

[59] GSMA IR.88, “LTE and EPC Roaming Guidelines,” V.09, 24 January 2013.

[60] GSMA IR.34, “Guidelines for IPX Provider networks,” v9.1, 13 May 2013.

[61] GSMA IR.77, “Inter-Operator IP Backbone Security Requirements,” v2.0, 15 October 2007.

[62] GSMA IR.61, “Wifi Roaming Guidelines,” v12.0, 27 September 2017.

[63] 3GPP TS 31.111, “(USIM) Application Toolkit (USAT),” v15.0.0, December 2017.

[64] 3GPP TS 23.048, “Security mechanisms for the (U)SIM application toolkit,” v5.9.0, June 2005.

[65] 3GPP TS 31.116, “Remote APDU Structure for (U)SIM Toolkit applications,” v14.0.0, March 2017

[66] 3GPP TS 31.115, “Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications,” v14.0.0, March 2017.

[67] 3GPP TS 22.368, “Service requirements for Machine-Type Communications (MTC); Stage 1,” v14.0.1, August 2017.

[68] 3GPP TS 23.682: “Architecture enhancements to facilitate communications with packet data networks and applications,” v15.3.0, December 2017.

[69] GSMA CLP.14, “IoT Security Guidelines for Network Operators,” v1.0, 08 February 2016.

[70] 3GP TR 33.919, “3G Security; Generic Authentication Architecture (GAA); System description,” v14.0.0, March 2017.

[71] Open Mobile Alliance, “OMA GBA Profile,” July 2012.

[72] S.Quirolgico, J.Voas, T.Karygiannis, C.Michael, K.Scarfone, “Vetting the Security of Mobile Applications,” National Institute of Standards and Technology, Special Publication 800-163, 26 January 2015.

[73] G.Howell, M.Ogata, “An Overview of Mobile Application Vetting Services for Public Safety,” National Institute of Standards and Technology, NISTIR 8136, 27 January 2017.

[74] GSMA PRD IR.92, “IMS Profile for Voice and SMS,” v11.0, 15 June 2017.

[75] GSMA PRD IR.51, “IMS Profile for Voice, Video and SMS over untrusted Wi-Fi access,” v5.0, 23 May 2017

[76] International Telecommunications Union, Recommendation ITU-T X.1205, “Overview of Cybersecurity,” April 2008.

[77] 3GPP TS 32.101, “Telecommunication management; Principles and high level requirements,” v15.0.0, September 2017.

[78] 3GPP TS 22.101, “Service aspects; Service principles,” v15.3.0, January 2018.

[79] 3GPP TS 22.016, “International Mobile station Equipment Identities (IMEI),” v14.0.0, March 2017.

[80] 3GPP TS 29.002, “Mobile Application Part (MAP) specification,” v15.2.0, January 2018.

[81] GSMA SG.24, “Anti-Theft Device Feature Requirements,” v3.0, 17 May 2016.

[82] M.Souppaya, K.Scarfone, “Guidelines for Managing the Security of Mobile Devices in the Enterprise,” National Institute of Standards and Technology, Special Publication 800-124 Revision 1, 21 June 2013.

[83] C.Brown, K.Bowler, S.Edwards, N.McNab, M.Steele, J.Franklin, “Mobile Device Security: Cloud and Hybrid Builds,” National Institute of Standards and Technology, Special Publication 1800-4b, November 2015.

[84] CIO Council, Government Mobile and Wireless Security Baseline, May 23, 2013. WEB. < <https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf >, Accessed 14 April 2018.

[85] NIAP, Protection Profile for Mobile Device Management Version 2.0, 31 December 2014, WEB. <https://www.niap-ccevs.org/MMO/PP/pp_mdm_v2.0.pdf >, Accessed 14 April 2018.

[86] NIAP, Protection Profile for Mobile Device Fundamentals Version 2.0, September 2014. WEB. < https://www.niap-ccevs.org/MMO/PP/pp_md_v3.0.pdf>, Accessed 14 April 2018.

[87] K.Scarfone, J.Padgette, “Guide to Bluetooth Security,” National Institute of Standards and Technology, Special Publication 800-121 Revision 2, 30 September 2008.

[88] N.Keshta, Y.Morgan, “Public Safety Grade Mobile Application Management Framework (PSG-MAMF),” Defence Research and Development Canada Centre for Security Science, Contractor Report DRDC-RDDC-2018-C203, October 2018.

[89] N.Hastings, J.Franklin, “Considerations for Identity Management in Public Safety Mobile Networks,” National Institute of Standards and Technology, NISTIR 8014, 30 March 2015.

[90] C.T.Hu, D.Ferraiolo, D.Kuhn, A.Schnitzer, K.Sandlin, R.Miller, K.Scarfone, “Guide to Attribute Based Access Control (ABAC) Definition and Considerations,” National Institute of Standards and Technology, Special Publication 800-162, 16 January 2014.

[91] IDMANAGEMENT.GOV (US), “Federal Identity, Credential, and Access Management Architecture,” [online]. WEB. <https://arch.idmanagement.gov>, Accessed 14 April 2018.

[92] Georgia Tech Research Institute, “Trustmark Technical Framework,” [online]. WEB. <https://trustmark.gtri.gatech.edu/technical-framework>, Accessed 14 April 2018.

[93] CIO Council (US), “Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance,” 02 December 2011. WEB. <https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf>, Accessed 14 April 2018.

[94] Treasury Board of Canada Secretariat, “Federating Identity Management in the Government of Canada - A Backgrounder,” [online]. WEB. <http://www.tbs-sct.gc.ca/sim-gsi/docs/2011/fimgc-fgigc/fimgc-fgigc04-eng.asp>, Accessed 14 April 2018.

[95] K.Scarfone, P.Hoffman, “Guidelines on Firewalls and Firewall Policy,” National Institute of Standards and Technology, Special Publication 800-41 Rev.1, 28 September 2009.

[96] GSMA PRD IR.67, “DNS Guidelines for Operators,” v14.0, 21 November 2016.

[97] R.Chandramouli, S.Rose, “Secure Domain Name System (DNS) Deployment Guide,” National Institute of Standards and Technology, Special Publication 800-81-2, 18 September 2013.

[98] International Telecommunications Union, Recommendation ITU-T X.509, “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,” October 2016.

[99] S.Frankel, K.Kent, R.Lewkowski, A.Orebaugh, R.Ritchey, S.Sharma, “Guide to IPsec VPNs,” National Institute of Standards and Technology, Special Publication 800-77, 01 December 2005

[100] 3GPP TS 33.117, “Catalogue of general security assurance requirements,” v14.2.0, June 2017.

[101] 3GPP TS 33.216, “Security Assurance Specification (SCAS) for evolved Node B (eNB) network product class,” v15.0.0, September 2017.

[102] 3GPP TS 33.250, “Security assurance specification for the PGW network product class,” v15.0.0, September 2017.

[103] K.Scarfone, W.Jansen, M.Tracy, “Guide to General Server Security,” National Institute of Standards and Technology, Special Publication 800-123, 25 July 2008.

[104] L.Chen, J.Franklin, A.Regenscheid, “Guidelines on Hardware-Rooted Security in Mobile Devices (Draft),” National Institute of Standards and Technology, Special Publication 800-164 (draft), October 2012.

[105] GSMA CLP.17, “IoT Security Assessment Checklist,” v2.0, 29 September 2017.

[106] GSMA CLP.12, “IoT Security Guidelines for IoT Service Ecosystem,” v2.0, 31 October 2017.

[107] GSMA CLP.13, “IoT Security Guidelines Endpoint Ecosystem,” v2.0, 31 October 2017.

[108] 3GPP TS 23.228: “IP Multimedia Subsystem (IMS); Stage 2,” v15.1.0, December 2017.

[109] K.Scarfone, P.Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” National Institute of Standards and Technology, Special Publication 800-94, 20 February 2007.

[110] K.Scarfone, M.Souppaya, “Guide to Computer Security Log Management,” National Institute of Standards and Technology, Special Publication 800-92, 13 September 2006.

[111] Communications Security Establishment Canada, ITSB-40A “Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms,” March 2011. WEB. <http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb40a-eng.html>, Accessed 14 April 2018.

[112] D.Kuhn, C.T.Hu, W.Polk, S.H.Chang, "Introduction to Public Key Technology and the Federal PKI Infrastructure," National Institute of Standards and Technology, Special Publication 800-32, 26 February 2001.

List of symbols/abbreviations/acronyms/initialisms

3G	3rd Generation
3GPP	3rd Generation Partnership Project
A	
AAA	Authentication, Authorization and Accounting
ABAC	Attribute Based Access Controls
ACL	Access Control List
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
ANDSF	Access Network Discovery Function
APCO	Association of Public Safety Communications Officials
API	Application Programming Interface
APN	Access Point Name
AS	Application Server
AuC	Authentication Center
B	
BG	Border Gateway
BM-SC	Broadcast Multicast Service Center
BSF	Bootstrapping Server Function
BSS	Business Support System
BYOD	Bring-Your-Own-Device
C	
CAD	Computer Aided Dispatch
CAPIF	Common API Framework
CCVE	Closed-Circuit Video Equipment
CIO	Chief Information Officer
CRM	Customer Relationship Management
CSCF	Call Session Control Function
CSEC	Communications Security Establishment Canada
CSS	Centre for Security Science (Canada)
D	

DEA	Diameter Edge Agent
DeNodeB	Donor eNode-B
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security (USA)
DM	Device Management
DNS	Domain Name System
DoS	Denial of Service
DRA	Diameter Routing Agent
DRDC	Defence Research & Development Canada
E	
EAP	Extensible Authentication Protocol
eDNS	external Domain Name Server
EIR	Equipment Identity Register
EM	Element Manager
EMS	Element Management System
eNodeB	evolved Node-B
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
EUA	End-User Agency
E-UTRAN	Evolved UMTS Terrestrial Radio Access
F	
FASG	Fraud and Security Group (GSMA)
FICAM	Federated Identity Credentials and Access Management
FIPS	Federal Information Processing Standard (USA)
FTP	File Transport Protocol
G	
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GIS	Geographic Information System
GPL	Generic Push Layer
GPRS	General Packet Radio Service

GSM	Global System for Mobile Communications or Groupe Spéciale Mobile
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
GUTI	Globally Unique Temporary UE Identity
GW	Gateway
H	
HeNodeB	Home evolved Node B
HSE	Home Security Endpoint
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HTTPS	Hypertext Transfer Protocol over Transport Layer Security
HVAC	Heating Ventilation and Air Conditioning
I	
IBCF	Interconnection Border Control Function
ICAM	Identity, Credentials, and Access Management
ID	Identifier
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IKE	Interent Key Exchange
IMEI	International Mobile Equipment 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
IPS	Intrusion Protection System
IPsec	IP security
IPX	IP eXchange
IR	Infra-Red
IRP	Integration Reference Point

ISP	Internet Service Provider
ITU	International Telecommunication Union
IWF	Inter-Working Function
L	
LAN	Local Area Network
LMR	Land Mobile Radio
LTE	Long Term Evolution
M	
M2M	Machine-to-Machine
MAM	Mobile Applications Management
MAP	Mobile Application Part
MC	Mission Critical
MCData	Mission-Critical Data
MCPTT	Mission-Critical Push-To-Talk
MCS	Mission Critical Services
MCVideo	Mission-Critical Video
MDM	Mobile Device Management
ME	Mobile Equipment
MHz	megahertz
MitM	Man in the Middle
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
MNO	Mobile Network Operator
MOCN	Multi-Operator Core Network
MTBF	Mean Time Between Failures
MTC	Machine Type Communication
MVPN	Mobile Virtual Private Network
N	
NAD	Network Architecture Description
NAF	Network Application Function
NAS	Non-Access Stratum

NAT	Network Address Translation
NDS	Network Domain Security
NESAS	Network Equipment Security Assurance Scheme (GSMA)
NIAP	National Information Assurance Partnership (USA)
NIST	National Institute of Standards and Technology (USA)
NM	Network Manager
NMC	Network Management Centre
NMLS	Network Management Layer Service
NMS	Network Management System
NNI	Network-to-Network Interface
NOC	Network Operations Centre
NPSTC	National Public Safety Telecommunications Council (USA)
O	
OAM	Operations Administration and Maintenance
OAM&P	Operations, Administration, Maintenance, and Provisioning
OMA	Open Mobile Alliance
OS	Operating System
OSS	Operations Support Systems
OTA	Over The Air
P	
PBAC	Policy-Based Access Controls
PCRF	Policy Charging and Rules Function
P-CSCF	Proxy Call Session Control Function
PDCP	Packet Data Convergence Protocol
P-GW	Packet Gateway
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Radio
PLMN ID	PLMN Identifier
PRD	Permanent Reference Document (GSMA)
ProSe	Proximity Service
PS	Packet Switched

PSBN	Public Safety Broadband Network
PSTN	Public Switched Telephone Network
Q	
QoS	Quality of Service
QPP	Quality of Service, Prioritization and Pre-emption
R	
RAN	Radio Access Network
RAT	Radio Access Technology
RBAC	Role-Based Access Control
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
RFID	Radio Frequency Identification
RMS	Records Management System
RN	Relay Node
RSDE	Regional Service Delivery Entity
RTCP	Real-Time Control Protocol
S	
SC	Security Consideration
SCEF	Service Capability Exposure Function
SCS	Services Capability Server
SCTP	Stream Control Transmission Protocol
SDP	Service Delivery Platform
SECAG	Security Assurance Group (GSMA)
SECAM	Security Assurance Methodology
SeGW	Security Gateway
SG	Security Group
S-GW	Serving Gateway
SIEM	Security Information and Event Management
SIGTRAN	Signaling Transport
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLP	Secure User Plane Location Platform

SMS	Short Message Service
SMSC	Short Message Service Centre
SNMP	Simplified Network Management Protocol
SOC	Security Operations Centre
SoC	System on a Chip
SP	Special Publication
SS7	Signaling System 7
SSC	Support for Subscriber Certificates
SSH	Secure Shell
SSO	Single Sign On
SW	Software
SYN	Synchronization
T	
TAG	Technical Advisory Group (Canada)
TCAP	Transaction Capabilities Application Part
TCI	Technical Considerations on Interoperability
TCO	Technical Considerations on Operability
TCP	Transmission Control Protocol
TCS	Technical Considerations on Security
TLS	Transport Layer Security
TMN	Telecommunication Management Network
TR	Technical Report
TS	Technical Specification
U	
UCN	User Capability Need
UDP	User Datagram Protocol
UDR	User Data Repository
UE	User Equipment
UICC	Universal Integrated Circuit Card
US	United States
USB	Universal Serial Bus
USIM	UMTS Subscriber identity Module

UTRAN	Universal Terrestrial Radio Access Network
UR	User Requirement
URD	User Requirements Document
V	
ViLTE	Video over LTE
VoLTE	Voice over LTE
VPN	Virtual Private Network
W	
WAN	Wide Area Network
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

Glossary

The following terms are used with this meaning in this document:

Reliability, Availability, Resiliency

Reliability is the probability of a system completing its predefined function during a specified period of time while availability is a measure of the % of time the equipment is in an operable state. A system can be available but not reliable; a reliable system is usually available.

There are two commonly used measures of reliability:

- Mean Time Between Failure (MTBF), which is defined as: total time in service / number of failures;
- Failure Rate (λ), which is defined as: number of failures / total time in service.

Resiliency is the ability of a system to withstand a disruption that would result in loss of availability and reliability, and the ability to recover from any such outage within a minimum period of time.

Security Terms

Security domain: A set of elements, a security policy, a security authority, and a set of security-relevant activities in which the elements are managed by a single administrative authority in accordance with the security policy. The environment of systems for which a unique security policy is applicable.

The PSBN may be implemented with one or more security domains. For example, the PSBN Core and RAN might exist in a single or two security domains; each RSDE can have their own distinct security domains.

3GPP Security Architecture in TS 33.210 [28] provides the following definitions for the Inter- and Intra-domain security. These definitions are applicable to components that are covered by the 3GPP standards and not to the broader security context that involves system elements outside the PSBN.

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

Threat consequence is a security violation that results from a threat action. It includes disclosure, deception, disruption, and usurpation.

The term Threat Agent or Actor is used to indicate an individual or group that can manifest a threat and who actually carry out the attack. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against the company.

A security feature is a service capability that meets one or several security requirements. A security mechanism is an element that is used to realize a security feature. All security features and security mechanisms taken together form the security architecture. An example of a security feature is user data confidentiality. A security mechanism that may be used to implement that feature is a stream cipher using a derived cipher key.

Services vs Applications

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.

Services range from basic transport and connectivity to service enablers like those that are necessary for providing internet access (e.g., AAA services, DHCP, DNS) to value-added services such as VoLTE, text messages, QoS, mission-critical push-to-talk, location services, instant messaging, etc.

In this document, services are provided and hosted by the PSBN, and almost exclusively 3GPP-specified. Users can be both human-users and applications-users.

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. Service enablers can serve both PSBN-hosted applications as well as EUA-hosted applications. Service enablers may be specified by other bodies than 3GPP.

An application is a functionality typically provided via a client and server architecture, although applications can also be client-less or client-only. Applications are enabled by network services and include basic file transport (e.g., FTP) and web browsing applications, as well as high-end applications such as Geographic Information System (GIS), Traffic advisories, Computer-Aided Dispatch (CAD), Records Management Systems (RMS), etc.

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 subscription-based data service offered by an MNO. Applications serve both end-users and administrative-users. In this TSC, only PSBN-hosted applications are in-scope.

Shall, Should, May

SHALL: The attribute, which is the object of the sentence with “shall” as the auxiliary verb, is essential or necessary to ensure that 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 recommendation for the standards that apply to the attribute. In light of other standards which may exist, the sentence conveys the recommendation 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.

Users, end-users, User Equipment

In this TCS, the terms “users” and “end-users” refer exclusively to public safety users and exclude commercial users that may have access to the Band-14 access network via the spectrum sharing agreement between the PSBN and the PSBN’s MOCN partner. Only public safety users have access to the PSBN’s core network. By extension, User Equipment (UE) devices refer exclusively to public safety UEs which have access to the PSBN core network.

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): Technical Considerations on Security (TCS)

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.)

February 2019

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

114

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

112

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-R240

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; network security; Public Safety Broadband Network (PSBN)

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

The public safety community deals with the safety and security of people, property, our institutions, and our country on a daily basis. In the course of their work they access and generate information that is critical to the success of their missions. They expect their communications networks to be reliable, available, and secure.

A Public Safety Broadband Network (PSBN) would undoubtedly be a target for cyber-attacks, espionage, and conventional attempts to disrupt and deny the availability of this critical asset to first responders. It is, therefore, imperative that robust measures be taken to secure the network and the information carried over it. This document presents a number of considerations that are structured within a security architecture that serves as a reference for next generation communications networks.

The security measures contained in this document are those that are deemed to support the proposed security posture for the PSBN. A security risk assessment would likely identify other security controls that would be required to support the security posture.

The consideration statements in this document are derived from similar efforts undertaken in the U.S. to support FirstNet[10] and from the experience of subject-matter-experts and practitioners that participated in cross-disciplinary work groups.

The Public Safety Broadband Network Use-Cases and User Requirements [1] contains a set of scenarios, referred to as “use-cases,” that typify the way subscribers of the PSBN are expected to use the PSBN in their day-to-day work and during extra-ordinary events, as well as a list of User Requirements (UR) that are phrased in terms of what the users need to be able to do or accomplish.

The technical considerations contained in this Technical Considerations on Security document (TCS) were derived with those URs in mind, and they reflect the capabilities that PSBN would offer to satisfy the security needs of the users of a Public Safety Broadband Network (PSBN). The statements express “what is needed” in operationally relevant terms. The contributors to the TCS refrained as much as possible from stating “how” to satisfy the needs of the users.

The TCS does not sequence the technical considerations in the manner of a roadmap of features. It is expected that the features and capability roadmap will be developed by the operators of the PSBN as part of their strategic planning process.

What public safety needs in an emergency is…

“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.” [2]

Chaque jour, les membres de la communauté de la sécurité publique veillent à la sécurité et à la protection de la population, des biens, de nos institutions et de notre pays. Dans le cadre de leur travail, ils génèrent et traitent de l’information essentielle à la réussite de leurs missions. Ils s’attendent donc à ce que leurs réseaux de communication soient accessibles, sécuritaires et fiables.

Un réseau à large bande pour la sécurité publique (RLBSP) serait à n’en point douter la cible de cyberattaques, d’opérations d’espionnage ou encore de tentatives conventionnelles pour perturber ou bloquer l’accès à cet outil crucial pour les premiers intervenants. Il est donc essentiel de prendre des mesures énergiques pour sécuriser le réseau et les données. Dans ce

[10] FirstNet refers to “First Responder Network Authority.” It is the entity responsible for building and operating the US public safety broadband network.

document, nous présentons bon nombre de facteurs à considérer dans une architecture de sécurité pouvant servir de référence pour la prochaine génération de réseaux de communication.

Les mesures décrites dans le présent document sont celles que nous jugeons les plus appropriées pour appuyer la posture de sécurité suggérée pour le RLBSP. L'évaluation des risques de sécurité pourrait sans doute permettre de déterminer des contrôles supplémentaires. Les énoncés relatifs aux différents facteurs à considérer découlent d'efforts semblables déployés aux États-Unis pour soutenir FirstNet[11] et de l'expérience d'experts et de professionnels ayant participé à des groupes de travail interdisciplinaires.

Le document intitulé *The Public Safety Broadband Network Use-Cases* and *User Requirements* [1] présente un ensemble de scénarios typiques sur l'utilisation du réseau à large bande par les abonnés (cas d'application) dans le cadre de leur travail quotidien ou lors d'événements extraordinaires. Il présente aussi une liste des besoins des utilisateurs en fonction de leurs tâches.

Les facteurs techniques à considérer mentionnés dans le document *Technical Considerations of Security (TCS)* découlent des besoins des utilisateurs. Ils correspondent aux capacités du RLBSP requises pour satisfaire aux exigences de sécurité de leurs utilisateurs. Les énoncés décrivent les besoins en fonction des activités. Les auteurs de ce document ont évité le plus possible d'indiquer la façon de répondre à ces besoins.

Dans le document, les facteurs techniques à considérer ne sont pas présentés comme dans une feuille de route. On s'attend à ce que les utilisateurs du RLBSP établissent eux-mêmes une feuille de route pour développer les fonctions et les capacités requises dans le cadre de leur processus de planification stratégique.

EN SITUATION D'URGENCE, SÉCURITÉ PUBLIQUE A BESOIN…

« Les organismes d'intervention d'urgence de tous les ordres du gouvernement doivent assurer des communications harmonieuses et interopérables afin de gérer les interventions, d'établir une structure de commandement et de contrôle, de conserver une connaissance de la situation et d'exercer leurs activités au sein d'un cadre opérationnel commun. On profitera ainsi de capacités d'intervention améliorées et d'une approche plus globale de la gestion des opérations en cas de catastrophe, d'où une plus grande sécurité pour les Canadiennes et les Canadiens. »

« L'information est l'élément vital des opérations quotidiennes dans le milieu de la sécurité publique. Les agents responsables prennent chaque jour d'innombrables décisions et doivent avoir rapidement accès à des renseignements opportuns, exacts et complets. Il est devenu évident qu'un processus décisionnel efficace nécessite un échange fréquent d'information entre une multitude de systèmes, d'organismes et d'administrations. » [2]

[11] FirstNet (First Responder Network Authority) est l'entité responsable de la mise sur pied et de l'exploitation du réseau à large bande pour la sécurité publique des É.-U.