Impact of NG9-1-1 on the 700 MHz Public Safety Broadband Network- a technical assessment

Claudio Lucente
Fiorel Telecommunications

Daniel Charlebois
DRDC Centre for Security Science

Pierre Meunier
DRDC Centre for Security Science

Jack Pagotto
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science

Scientific Literature
DRDC CSS SL 2013-003(E)
January 2013

Principal Author

Claudio Lucente

Fiorel Telecommunications

700MHz Tech Advisory Group

Approved by

Jack Pagotto

DRDC Centre for Security Science

Section Head

Approved for release by

Dr. Andrew Vallerand

DRDC Centre for Security Science

Document Review Panel

Government of Canada | Gouvernement du Canada

Canadian Safety and Security Program

Jan. 17, 2013
700TAG-TAN#9

TECHNICAL ADVISORY NOTE

Impact of NG 9-1-1 on the 700 MHz Public Safety Broadband Network – a technical assessment

700 MHz Mobile Broadband for Public Safety - Technology Advisory Group **Centre for Security Science - Public Security Science and Technology**

Federal Lead: The Technology Advisory Group for 700 MHz Public Safety Spectrum (700TAG) is composed of a collaborative group of technical experts led by Centre for Security Science and includes scientific authorities from the Communications Research Center, and technical experts from Federal-Provincial-Territorial-Municipal agencies.

Objective

The objective of this Technical Advisory Note (TAN) is to provide a technical perspective on the impact of Next Generation 9-1-1 (NG 9-1-1) systems on the 700 MHz Public Safety Broadband Network (PSBN) in response to the public consultation[1] of the Canadian Radio-television and Telecommunications Commission (CRTC) dated December 17, 2012. The CRTC requests public comments on (i) the current state of 9-1-1- systems and services and, (ii) the vision of NG 9-1-1.

General recommendations are proposed on technical matters that impinge on interoperability between NG 9-1-1 and the PSBN. They do not constitute a necessary and sufficient set of requirements.

This technical assessment and the recommendations and conclusions contained herein are based on information that is current as of the time of writing.

Introduction

Public Safety Canada - Emergency Management Branch - Interoperability Development Office has requested that the Centre for Security Science (CSS) - 700 MHz TAG conduct a technical assessment of the impact of NG 9-1-1 on the 700 MHz PSBN. Part of the scope of the request is to assess how NG 9-1-1 services can be supported by the PSBN.

Scope and assumptions

This TAN addresses the questions concerning NG 9-1-1 in the CRTC's Notice of Consultation (NoC), as listed in Figure 1, that have bearing on the PSBN. Several of the questions relate to policy matters and the architecture of the NG 9-1-1 system itself. This assessment does not address those aspects.

The PSBN will carry NG 9-1-1 messages from Public Safety Answering Point (PSAP) and dispatch operators to first responders. In the opposite direction, it is assumed that the emergency alarms initiated by first responders will be treated within a workflow that includes the PSAP.

It is assumed that commercial service providers will be permitted to lease capacity on the PSBN. It is, therefore, also assumed that subscribers served by these service providers will be able to initiate NG 9-1-1 sessions with the PSAP operator and transfer data files to the latter.

The aspects covered in this TAN are:

a) How NG 9-1-1 systems could interface with the PSBN.
b) How NG 9-1-1 messages traverse the PSBN to/from the PSAP and first responders.
c) Resiliency of facilities and information repositories.
d) Security considerations for NG 9-1-1 session flows.

In the absence of a standardized NG 9-1-1 architecture for Canada, this TAN considers the i3 Solution, as espoused by the US National Emergency Numbering Association (NENA) [1] and as noted by the *CRTC's Notice of Consultation (See Figure 1 para 3).*

[1] Telecom Notice of Consultation CRTC 2012-686 http://www.crtc.gc.ca/eng/archive/2012/2012-686.htm

B. Next-generation (NG) 9-1-1:

1. With NG 9-1-1, there is an opportunity to build a system that could provide new and enhanced features and capabilities. Provide your vision of an NG 9-1-1 system in terms of, but not necessarily limited to

- how Canadians could communicate with PSAPs and emergency response teams, for example using what types of devices and methods of communications, how specific needs and concerns of Canadians with disabilities could be met, etc.;
- the types of information and data, such as pictures, videos, medical records, etc., that could be transmitted to, and possibly shared between PSAPs;
- how, and to what degree of accuracy a caller's location could be determined; and
- how the implementation and ongoing operation of an NG 9-1-1 system could be funded.

2. The evolution to an all-IP architecture permits re-imagining the logical architecture of a 9-1-1 system. For example, certain back-up functions or databases could be national or provincial in scope, while service delivery could continue to be local or regional. Provide your views on what functions or databases could be provided on a national or provincial basis in order to promote robustness, resiliency and/or greater efficiencies.

3. The National Emergency Number Association (NENA) i3 solution has been proposed as the architecture for NG 9-1-1. To what extent has there been consensus in Canada that this is the way forward?

If it is determined that the i3 solution is to be implemented,

- what steps would need to be taken in Canada to achieve this architecture?
- what institutions (e.g. public safety organizations, standards bodies, the Commission, carriers, PSAPs, first responders) would be involved?
- what role(s) would they play?
- what would be the timing for each step?

If there has not been consensus, provide your views.

4. NG 9-1-1 will enable detailed data gathering and analysis of emergencies.

- What data would need to be collected to assist policy makers and operations managers in responding to emergencies and disaster relief planning?
- How would this data be collected?

Figure 1. *Excerpt from the CRTC's Notice of Consultation related to NG 9-1-1.*

Summary of recommendations

The following are the recommendations that have been made in the TAN:

R1: The NENA i3 Solution should be used as a candidate model to benchmark Canada's future NG 9-1-1 network.

R2: The IP Multimedia Subsystem (IMS) should be implemented as part of the PSBN.

R3: The PSBN operator should enter into roaming agreements with US and Canadian commercial operators and FirstNet[2].

R4: The NG 9-1-1 operator should specify service availability for the data repositories as part of its implementation for the NG 9-1-1 network. If it chooses to out-source the data hosting service, it should specify the availability to the service provider. The availability should state operational availability as well as availability during disaster events.

[2] First Responder Network Authority http://www.ntia.doc.gov/category/firstnet

R5: The IP eXchange (IPX) Clearinghouse's routers, the PSBN routers, and the IP backbone routers should conform to the Internet Engineering Task Force's (IETF) definition of Differentiated Services Code Point (DSCP) as contained in the RFC-2475. This is in order to have a consistent end-to-end assignment of Quality of Service (QoS) and priority to NG 9-1-1 messages.

R6: All operators of the inter- networking routers and nodes in the transmission path of NG 9-1-1 messages should configure the DSCP pre-hop behaviour (PHB) according to an agreed-upon association of DSCP and traffic type.

R7: IP Security (IPsec) should be used in the Border Control Function (BCF) in accordance with RCF-2401 to encrypt the information transported across network domain boundaries. The encryption algorithm should be equivalent to Advanced Encryption Standard (AES) 128 or higher.

Inter-networking NG 9-1-1 and the 700 MHz PSBN

The i3 Solution from NENA

The i3 Solution from NENA is modeled on a network of IP networks. The i3 Solution defines the standards for the Emergency Services IP Network (ESInet), which is illustrated in the block diagram of Figure 2.

Figure 2 illustrates two regions, each with their own NG 9-1-1 ESInet, are interconnected to form a network of networks. Within each region, PSAP operators connect to the regional network. Subscribers of commercial service providers could initiate emergency 9-1-1 calls through their handheld portable devices or fixed facilities. Machine devices such as on-board crash notification systems could also initiate emergency 9-1-1 calls. Commercial wireless networks provide location information of the calling party to ESInet. Location information may be derived by the commercial service providers' wireless network and/or assisted by the subscriber device's Global Positioning System (GPS) receiver. Location information for subscribers is stored in the service provider's Location Information Server (LIS).

NG 9-1-1 messages are passed to the Internet by the commercial service providers. Security considerations for NG 9-1-1 messages are covered in the chapter titled, "*Security and Information Assurance*". NG 9-1-1 packets contain a special header which uniquely identifies them among all other traffic on the commercial wireless networks, such that NG 9-1-1 packets can be routed with higher priority through those networks.

The first network element to receive the NG 9-1-1 packets in the ESInet is the Border Control Function (BCF). The BCF provides security between public networks and the ESInet as well as between different networks within ESInet. Immediately behind the BCF in the ESInet is the Emergency Services Routing Proxy (ESRP), which routes the NG 9-1-1 packets to the correct PSAP according to routing policies and the caller's estimated location.

ESInet uses Session Initiated Protocol (SIP) [2] for creating, modifying, and terminating data and voice sessions with one or more participants. Data sessions include multimedia distribution, and multimedia conferences. SIP makes use of elements called proxy servers to help route requests, authenticate users, and authorize access to services.

In summary, the i3 Solution encompasses a comprehensive set of standards and requirements for implementing ESInet - developed and endorsed by NENA, a well-established and respected standards-setting organization for 9-1-1 emergency communications in the US.

Recommendation #1

NENA i3 Solution should be considered as a candidate model to benchmark Canada's future NG 9-1-1 network.

Interface between ESInet and the PSBN

In defining the interface between the NG 9-1-1 network and the PSBN, it is useful to examine what the US has postulated as the interface between ESInet and the FirstNet Nationwide Public Safety Broadband Network (NPSBN). The US Federal Communications Commission's (FCC) Interoperability Board published its Minimum Technical Interoperability Requirements [3] for the NPSBN in May 2012. It submitted this document as its interoperability recommendations to FirstNet. The Interoperability Board proposed

an approach to interface the NPSBN with ESInet as shown in Figure 3. The diagram shows the ESInet interfacing with the Applications-Services function that supports telephony (voice), short message service (SMS), and multi-media messaging services (MMS). It also shows an alternative connection to the core network of the NPSBN through the public Internet.

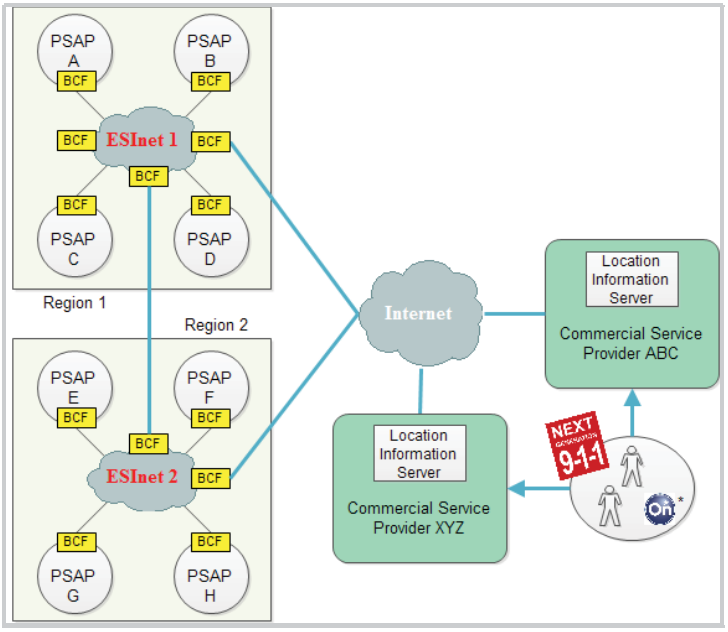

Figure 2. *Block diagram of ESInet and the interface to commercial service provider networks.* (* is a trademark of OnStar Corporation)

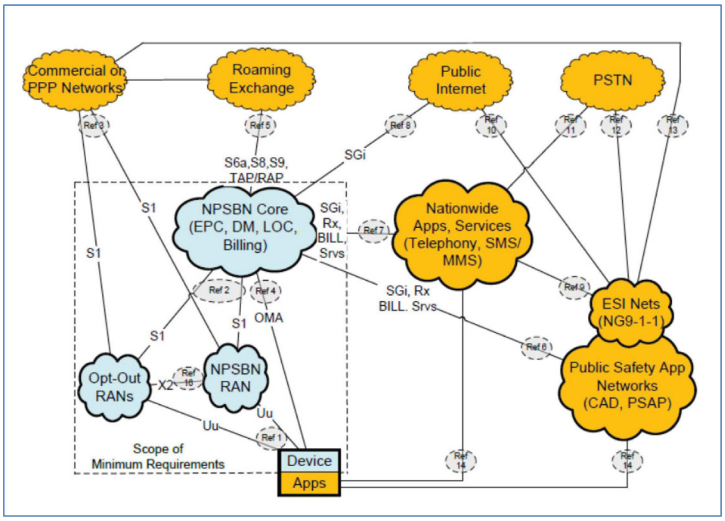

Figure 3. *US Landscape Model of public safety networks.* Source: [3]

In the Canadian context, Figure 4 shows how the PSBN could interface to a hypothetical Canadian implementation of ESInet based on NENA's i3 Solution. The block diagram illustrates the following:

a) The PSBN is partitioned into the National Entity and the Regional Service Delivery Entity (RDSE). The RSDE provides the Radio Access Network interface to first responders and commercial users[3]. The National Entity would host the LIS which provides location information of first responders and other subscribers. Security considerations for such information are discussed in the chapter titled, "*Security and Information Assurance"*.

b) The IP Multimedia Subsystem (IMS) [4] provides the ability to use SIP signalling headers to route the IP packets to the edge of the IMS, terminated by the Session Border Controllers (SBC). The IMS can be implemented within various different network architectures. For example, the IMS can be operated by the National Entity or can be out-sourced to a 3rd party IMS hosting service. The SBC, not shown in Figure 4, could be distributed among the RSDEs. In essence, the IMS provides the means to be able to be able to route multi-media IP packets that use SIP signalling to their destination addresses and to interface the PSBN with application hosting networks.

   The IMS could also facilitate voice and video connections between users on the commercial networks and users on the PSBN. It will add other capabilities such as traffic prioritization across network boundaries.

Recommendation #2

An IMS should be implemented as part of the PSBN.

c) The IPX Clearinghouse is a 3rd party service that provides the ability to exchange IP traffic, consisting of control and user information, between service providers. Roaming agreements between service providers are typically enabled by the IPX Clearinghouse. Sending emergency messages through multiple service providers is necessary in order to reach first responders, who may be outside the radio coverage of the PSBN, but whose user-equipment could be camped on a commercial service provider's network.

   In several instances along the Canada-US border, the closest first responder may be across the border. It is, therefore, important to be able to reach US first responders on their NPSBN and thus, a connection to FirstNet's NPSBN through the IPX Clearinghouse is envisaged. No consideration is made herein for policies and international agreements that are required to facilitate cross-border emergency response. But, suffice that the architecture can enable the agreements

Note that in Figure 4 emergency broadcasts are shown as originating from an Emergency Broadcast Aggregator to illustrate that the emergency broadcast network and ESInet can be separate networks. It is conceivable that the emergency broadcasts could be distributed through the NG 9-1-1 network, but that approach is not shown since the NENA i3 Solution specification does not cover emergency broadcasts in this manner.

Recommendation #3

The PSBN operator should enter into roaming agreements with commercial operators and FirstNet.

Location accuracy with 3GPP wireless networks

Locating the caller and the first responder is of paramount importance in the response to an emergency. As noted above, location information is stored in the LIS. To be specific, location pertains to the User Equipment (UE). The location of the UE is derived by network-based triangulation, measuring differences in time-of-arrival of polling signals, and augmented by GPS-assisted positioning of the UE.

[3] It is assumed that consumers are permitted to use the public safety network through a commercial retailer. This is to be confirmed by Industry Canada.

The CRTC has adopted a recommendation from its Emergency Services Working Group (ESWG) report [6] in Oct 2008 that the wireless service provider (WSP) will deliver unfiltered information to the PSAP regarding a caller's location consisting of (i) X,Y coordinates, (ii) confidence, and (iii) uncertainty. The text of the recommendation is in Figure 5..

On Feb.1, 2010 the CRTC announced the introduction of improved E9-1-1 services and that location accuracy is expected to be between 10m to 300m of the caller's actual location.

The FCC has mandated the accuracy of locating a wireless handset through its 3rd Report and Order in 1999 [5] which clarified the provisions for location accuracy for enhanced 9-1-1 calls. The mandated accuracy is stated in Table 1. The FCC has acknowledged that the degree of accuracy cannot be assured in all cases. The location accuracy is up to 300 meters for 95% of the E9-1-1 calls that are made, and up to 100 meters for 67% of the calls made. Device-based location is expected to be more accurate than network-based location

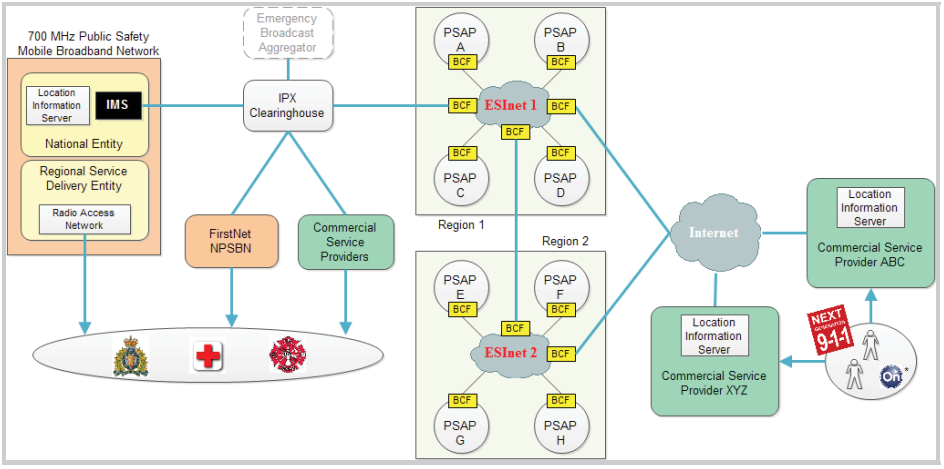

Figure 4. *Block diagram of the interface between the 700 MHz PSBN and ESInet.*

ESWG Recommendation

The ESWG recommends that Confidence (%) and Uncertainty (metres) values in addition to X,Y or an error message be transmitted to the PSAP during a wireless phase II E9-1-1 call. The ESWG further recommends that, the following location system parameters be utilized[5]:

- **Confidence value be set to 90%;**
- **Uncertainty value (metres) be calculated by the position determination equipment (PDE);**
- **The wireless phase II E9-1-1 information (X,Y, Confidence, Uncertainty or an error message) be sent within 30 seconds;**
- **At 30 seconds, available location information or an error message must be transmitted by the WSP's location server.**

Figure 5. *Excerpt from the ESWG report, "Technical and Operational Requirements of Wireless Phase II E911 Implementation". [6]*

percentage of E911 calls made	Location accuracy	
	Network-based	Device-based
67%	100 meters	50 meters
95%	300 meters	150 meters

Table 1. *FCC mandated location accuracy for E9-1-1 calls*

Resiliency strategy for transmission facilities and data repositories

Resiliency strategies generally include duplicating elements of the infrastructure such as servers and databases. The facilities would be located in geographically separate areas that are not subject to the same environmental conditions and, ideally, on separate power grids. Interconnectivity between facilities would be over redundant transmission paths carried over physically separated networks. In 1:1 redundancy one facility backs up the other. Additional degrees of redundancy can be implemented to tolerate multiple simultaneous failures. The concept of 1:1 redundancy is illustrated in Figure 6.

In Canada, a network such as ESInet could be implemented on a national scale in the form of a network-of-networks architecture. Each PSAP operator would connect to a national NG 9-1-1 network. Databases could be located anywhere on the network and replicated for added resiliency while at the same time providing local-level ownership of the data contained on the databases. In essence, with a network architecture similar to ESInet, ownership of the information is not tied to physical ownership of the repositories. Some level of consolidation of data repositories would offer operational cost efficiencies, though.

The PSAP may choose to purchase a cloud-hosted service for data repositories and would specify service availability, including availability during natural and man-made disasters.

Recommendation #4

The NG 9-1-1 operator should specify service availability for the data repositories as part of its implementation for the NG 9-1-1 network, or specify the same to the hosting service provider. The availability would need to account for normal operational availability as well as availability during disaster events.

Flow of NG 9-1-1 messages through the 700 MHz PSBN

The expected direction of NG 9-1-1 messages is from the citizen to the PSAP, and from the PSAP to the dispatcher to the first responder. It is, however, possible that first responders could initiate emergency alarm messages to alert the dispatcher of imminent threat to themselves or citizens. In some cases the PSAP may be in the operational workflow of the emergency alarm message from the first responder.

If commercial subscribers are served by the 700 MHz PSBN, then the message flow would originate from a subscriber on the PSBN, towards the PSAP, and be routed back to the PSBN from the PSAP to the closest first responder.

Priority and QoS for NG 9-1-1 messages

Emergency messages are to be carried with high priority so that in case there are capacity bottlenecks in the transmission path, whether it is in the radio network or the wired network, the emergency messages are minimally delayed. According to NENA's i3 Solution specifications, IP traffic within ESInet must implement DiffServ [7]. DiffServ is a way of marking the priority of IP packets according to an industry-accepted standard defined by the (IETF. The ESInet IP routers mark traffic through a 6-bit field in the IP header which defines the Differentiated Services Code Point (DSCP). DiffServ-enabled IP routers interpret the Code Point of the message and process the IP packet with the priority corresponding to the Code Point.

Recommendation #5

The IPX Clearinghouse's routers, the PSBN routers, and the IP backbone routers should conform to the IETF's definition of DSCP as contained in the RFC 2475 in order to have a consistent assignment of QoS and priority to NG 9-1-1 messages between network domains.

The NENA i3 Solution specifies a convention for assigning the type of information to a particular level of the DSCP per-hop-baviour (PHB). PHB is one of the configuration points by which a router or node assigns bandwidth resources to the IP packets and manages queues in buffers. The mapping of PHBs to traffic type according to NENA's i3 Solution is shown in Table 2

DSCP	Use	PHB
0	Routine traffic	Default
1	9-1-1 signaling	AF12
2	9-1-1 text media	AF12
3	9-1-1 audio media	EF
4	9-1-1 video media	AF11
5	9-1-1 non-human initiated call	AF21
6	Intra ESUnet events	AF21
7	Intra ESUnet other 9-1-1 traffic	AF22

Table 2. *DSCP mapping of traffic types to PHB values [8.8][4] according to NENA's i3 Solution*

Recommendation #6

All operators of the inter- networking routers and nodes in the transmission path of NG 9-1-1 messages should configure the DSCP PHB according to an agreed-upon association of DSCP and traffic type.

It is expected that the radio network portion of the PSBN will be implemented using Long Term Evolution[5] (LTE) technology. LTE provides a sophisticated set of Quality of Service (QoS) and prioritization tools to be able to identify and process NG 9-1-1 messages with high priority.

These parameters are known as Allocation Retention Priority (ARP) and QoS Class Identifier (QCI). The LTE network can map DSCP markings to the corresponding ARP and QCI parameters within the LTE domain and thus provide a consistent processing of priority for the NG 9-1-1 packets through the LTE network.

Security and Information Assurance

The security architecture recommended by the International Telecommunications Union (ITU) is currently under study by the TAG as a candidate framework within which to establish the security requirements for the PSBN. Recommendations ITU-T Y.2701 [9] and ITU-T X.805 [10] state that for multi-domain networks, each service provider is responsible for security within its domain and each service provider is responsible for designing and implementing security solutions to meet its own network-specific needs. In this context, the PSBN, the IPX Clearinghouse, the NG 9-1-1 network, and all other networks can be considered separate domains. This TAN does not address the measures that network operators should implement to secure their networks. The TAN covers the security of the information that traverses the boundaries between network domains.

Figure 7 illustrates the use of BCFs which each network owner would implement at the points where two or more networks meet. One of the functions of the BCFs is to encrypt the information carried between networks. The choice of encryption algorithm is the prerogative of the network operators. BCFs, as implemented, typically can support several algorithms within the same device

Recommendation #7

IP Security (IPsec) [11] should be used in the BCF in accordance with RCF 2401 to encrypt the information transported across network domain boundaries. The encryption algorithm should be equivalent to AES128 or higher.

[4] See RFC-2597 [8] for a definition of PHB..

[5] LTE is latest generation of wireless mobile technology from the 3rd Generation Partnership Project (3GPP). www.3GPP.org

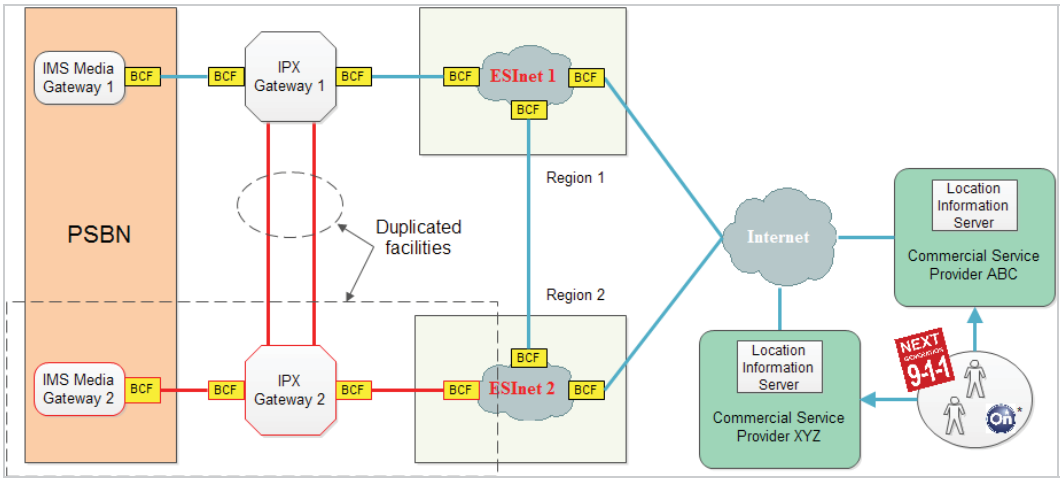

Figure 6. *Illustration of the concept of 1:1 protection of the ESInet sub-networks, the IPX Gateways, and transmission paths.*

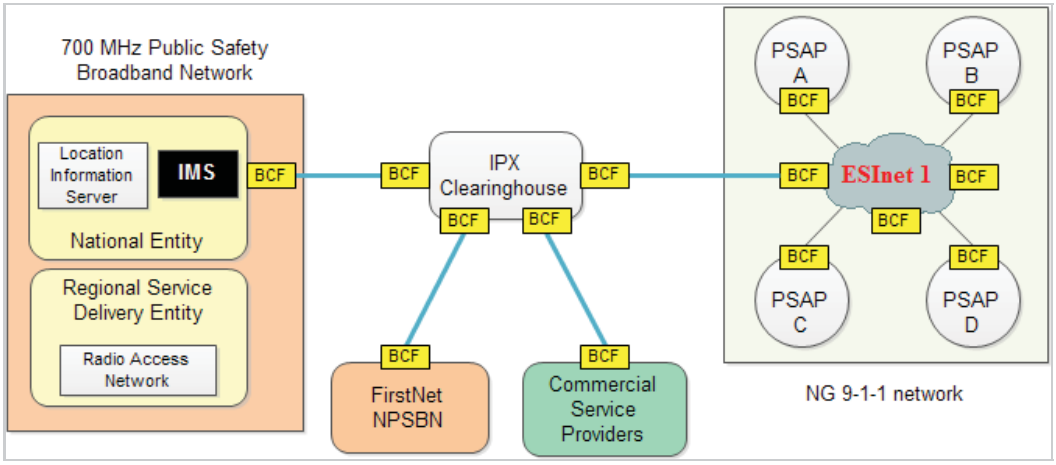

Figure 7. *Illustration on the use of Border Control Functions to protect the information transported between networks.*

IPsec imparts several degrees of protection to information. These are:

- Access Control.
- Data integrity, including rejection of replayed packets [6].
- Data origin authentication.
- Confidentiality through encryption.

Another important security dimension closely associated with information assurance is *non-repudiation*. IPsec does not impart any protection for this dimension. Additional measures over and above IPsec are required to ensure that data which has been received cannot be denied as having been received.

The trust model for sharing keys and digital certificates for securing the information transported between BCFs is a matter of agreement between network operators and should be based on an assessment of the operational needs and security risk. A method for defining security risks and suitable levels of controls to mitigate such risks for data communications networks is proposed by the Communications Security Establishment Canada (CSEC) [12].

Conclusion

NG 9-1-1 provides the citizen with a way of communicating an emergency to the PSAP using popular methods that people use to communicate today. That is, by means of text messages. It also allows rich content about the emergency to be communicated to the PSAP, which enhances the situational awareness of the PSAP operator, dispatcher, and first responders assigned to the emergency.

In addition to a textual description of the emergency, it is expected that other content will be transmitted as part of the message (e.g. location information tagged to the content). This would include still images, video files with an audio overlay, and VoIP voice. In order for the 700 MHz PSBN to be able to process the SMS, MMS, and VoIP emergency messages, the PSBN requires an IMS to be present within the public safety network or contracted as an out-sourced service.

NENA has specified the technical requirements for an IP-based emergency services network which is referred to as ESInet. The ESInet is intended to be a nationwide network-of-networks that interconnects local and regional PSAP networks. In this TAN, the NENA i3 Solution was used as the model for assessing the technical impacts of the NG 9-1-1 network on the PSBN.

The PSBN is but one network that first responders will need to have access to. It is expected, especially in the early stages of deploying the PSBN, that coverage gaps will be present. Given that this is highly likely to occur, it will be necessary to establish roaming agreements with commercial carriers so that first responders can be reached through commercial networks. Furthermore, if international agreements allow, US responders can be called upon to respond to an emergency. This requires roaming agreements be established with FirstNet and US and Canadian commercial carriers. The IPX Clearinghouse is a 3rd party service that facilitates the establishment and management of roaming agreements as well as provides the connectivity between roaming partner networks.

When a caller sends an emergency message, it is imperative that the caller be located as precisely as possible in the shortest period of time. Both Canada and the US have regulated the accuracy of correctly locating a wireless user making an emergency call. Although the regulations are not stated in the same way between Canada and the US, the essence is to achieve an uncertainty in locating the caller of between 10 metres and 300 metres.

Recent natural disasters in the US have exposed the vulnerability of current 9-1-1 networks to severe weather events. The FCC launched an inquiry into how to improve the resilience of 9-1-1 networks [12]. An IP-based network such as ESInet allows facilities to be duplicated in geographically separated areas that have a low correlated probability of exposure to the same risks at the same time. Furthermore, data repositories and back-up databases can also be separated by large distances while each jurisdiction retains ownership of the information contained in the databases. Third party cloud-hosting providers offer data warehousing services that can be purchased to specified levels of availability.

Emergency messages need to be carried across all networks that form part of the message

[6] A form of replayed packet is the masquerade attack [10].

transmission path with high priority. The flexibility that IP affords the network operator to mark and process emergency messages with high priority is a distinct advantage. However, the flexibility of the priority and QoS mechanisms also means that the network operators can choose different ways to configure them. This can lead to unpredictable behaviour of emergency message packets as they traverse from one network to the other. Hence, it is essential that all partnering network operators agree and conform to a standard approach to mark and process emergency packets.

All public safety communications networks will likely be subjected to cyber-attacks. Each network operator will need to implement their own measures to mitigate the risks and reduce vulnerabilities. The boundary between networks is a point of exposure and network operators will need to encrypt the information that traverses the boundaries

References

1. National Emergency Numbering Association (NENA), "Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3", v1, June 14, 2011.

2. Internet Engineering Task Force (IETF), "Session Initiated Protocol", RFC 3261, June 2002.

3. US Federal Communications Commission (FCC), Technical Advisory Board for First Responder Interoperability, "Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network", Final Report, May 22, 2012.

4. 3rd Generation Partnership Project (3GPP), "IP Multimedia Subsystem (IMS) Emergency Sessions (Release 10)", TS 23.167, December 2012.

5. US Federal Communications Commission (FCC), "Revision of the Commission's Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems", 3rd Report and Order, FCC 99-245; October 6, 1999.

6. CRTC, Interconnection Steering Committee, Emergency Services Working Group (ESWG), "Technical and Operational Requirements of Wireless Phase II E9-1-1 Implementation" Report Number: ESRE0046; October 31, 2008.

7. Internet Engineering Task Force (IETF), "An Architecture for Differentiated Services", RFC2475, December 1998.

8. Internet Engineering Task Force (IETF), "Assured Forwarding PHB Group", RFC-2597, June 1999.

9. International Telecommunications Union, "Security requirements for Next Generation Networks release 1", ITU-T Recommendation Y.2701, April 2007.

10. International Telecommunications Union, "Security architecture for systems providing end-to-end communications", ITU-T Recommendation X.805, October 2003.

11. Internet Engineering Task Force (IETF), "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

12. Communications Security Establishment Canada, Government of Canada, "IT Security Risk Management: A Lifecycle Approach", ITSG-33, November 2012.

13. FCC Public Notice, "PUBLIC SAFETY AND HOMELAND SECURITY BUREAU SEEKS COMMENT ON 9-1-1 RESILIENCY AND RELIABILITY IN WAKE OF JUNE 29, 2012, DERECHO STORM IN CENTRAL, MID-ATLANTIC, AND NORTHEASTERN UNITED STATES", DA 12-1153, July 18, 2012.

14. Internet Engineering Task Force (IETF), "Location Conveyance for the Session Initiation Protocol" RFC-6442, Dec.2011.

15. Dr. Walt Magnussen, "NG 9-1-1 and LTE: A Beneficial Union" Mission Critical Magazine, March 2012.

***700 MHz Mobile Broadband for Public Safety - Technology Advisory Group* Centre for Security Science - Public Security Science and Technology**

List of acronyms

3GPP	3rd Generation Partnership Project
AF	Assured Forwarding
AES	Advanced Encryption Standard
ARP	Allocation Retention Priority
BCF	Border Control Function
CRTC	Canadian Radio-television and Telecommunications Commission
CSS	Centre for Security Science
CSEC	Communications Security Establishment Canada
DiffServ	Differentiated Services
DSCP	Differentiated Services Code Point
EF	Expedited Forwarding
ESInet	Emergency Services IP Network
ESRP	Emergency Services Routing Proxy
ESWG	Emergency Services Working Group
FCC	Federal Communications Commission
FirstNet	First Responder Network Authority
GPS	Global Positioning System
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPX	IP eXchange
ITU	International Telecommunications Union
LIS	Location Information Server
LTE	Long Term Evolution
MMS	Multi-media Messaging Services
NENA	National Emergency Numbering Association
NG 9-1-1	Next Generation 9-1-1
NoC	Notice of Consultation
NPSBN	National Public Safety Broadband Network (USA)
PDE	Position Determination Equipment
PHB	Per-Hop Behaviour
PSAP	Public Safety Answering Point
PSMBN	Public Safety Mobile Broadband Network
QCI	Quality of Service Class Identifier
QoS	Quality of Service
RSDE	Regional Service Delivery Entity
SBC	Session Border Controller
SIP	Session Initiated Protocol
SMS	Short Messaging Service
TAG	Technology Advisory Group
UE	User Equipment
WSP	Wireless Service Provider

700 MHz Mobile Broadband for Public Safety - Technology Advisory Group Centre for Security Science - Public Security Science and Technology

DRDC Centre for Security Science warrants that this advisory note was prepared in a professional manner conforming to generally accepted practices for scientific research and analysis. This advisory note provides technical advice and therefore is not a statement of endorsement of Defence Research Development Canada, Department of National Defence, or the Government of Canada

Author:
Claudio Lucente, P.ENG. M.ENG.
Senior Technical Advisor – Technology Advisory Group
Defence R&D Canada (DRDC) - Centre for Security Science (CSS)

Scientific Authorities:
Dr. Daniel Charlebois
Portfolio Manager – Interoperable Communications
Defence R&D Canada (DRDC) - Centre for Security Science (CSS)

Pierre Meunier, MSC, PENG.
Head, Border and Critical Infrastructure Resilience Science & Technology
Defence R&D Canada (DRDC) - Centre for Security Science (CSS)

Jack Pagotto
Head, Muti-Agency Crisis Management, Canadian Safety & Security Program
Defence R&D Canada (DRDC) - Centre for Security Science (CSS)

Reviewers:
Doug Allport
Special Advisor - Public Safety Communications
Defence R&D Canada (DRDC) - Centre for Security Science (CSS)

Simon Arcand
High Assurance Evaluation – Canadian Security Establishment Canada (CSEC)

Dr. Stephen Braham
Director - PolyLab for Advanced Collaborative Networking, Simon Fraser University

Jacob Gurnick
Senior Research Engineer, Communications Research Centre (CRC), Government of Canada

Dr. Walt Magnussen
Director – Internet2 Technology Evaluation Center, Texas A&M University
Public Safety Advocate, US UCAN

Luc Samson
Technology Advisory Group
Defence R&D Canada (DRDC) - Centre for Security Science (CSS)

Approval for Release:
Dr. Andrew Vallerand
Director – Directorate Science & Technology Public Security (DSTPS)
Defence R&D Canada (DRDC) - Centre for Security Science (CSS)

DOCUMENT CONTROL DATA

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

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

DRDC Centre for Security Science
222 Nepean St.
Ottawa, ON

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

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

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

Impact of NG9-1-1 on the 700 MHz Public Safety Broadband Network- a technical assessment

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

Lucente, C.; Charlebois, D.; Meunier P.; Pagotto J.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
January 2013	13	15

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

Scientific Literature

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

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS SL 2013-003(E)	

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

Unclassified

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

Unlimited

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

The objective of this Technical Advisory Note (TAN) is to provide a technical perspective on the impact of Next Generation 9-1-1 (NG 9-1-1) systems on the 700 MHz Public Safety Broadband Network (PSBN) in response to the public consultation of the Canadian Radio-television and Telecommunications Commission (CRTC) dated December 17, 2012. The CRTC requests public comments on (i) the current state of 9-1-1- systems and services and, (ii) the vision of NG 9-1-1.
General recommendations are proposed on technical matters that impinge on interoperability between NG 9-1-1 and the PSBN. They do not constitute a necessary and sufficient set of requirements.
This technical assessment and the recommendations and conclusions contained herein are based on information that is current as of the time of writing.

La présente note consultative technique (NCT)) vise à donner un point de vue technique sur les répercussions des systèmes 9-1-1 de prochaine génération (PG) sur le réseau à large bande de sécurité publique (RLBSP) dans la bande du 700 MHz, à la suite de la consultation publique menée par le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), datée du 17 décembre 2012. Le CRTC souhaite recevoir les commentaires du public sur (i) l'état actuel des systèmes et des services 9 1 1 et (ii) la vision concernant les systèmes 9 1-1 PG.
Des recommandations d'ordre général sont proposées au sujet des questions techniques qui ont des répercussions sur l'interopérabilité entre les systèmes 9-1-1 PG et le RLBSP dans la bande du 700 MHz. Elles ne constituent pas un ensemble complet d'exigences qu'il est nécessaire d'adopter.
La présente évaluation technique et les recommandations ainsi que les conclusions qu'elle contient sont fondées sur des informations qui étaient à jour au moment de sa rédaction.

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

Emergency Management; 700MHz; NG 9-1-1; Public Safety Answering Point;