Répercussions du système 9-1-1 de prochaine génération sur le réseau à large bande de sécurité publique dans la bande du 700 MHz – Évaluation technique

Claudio Lucente
Fiorel Télécommunications

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(F)
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

NOTES CONSULTATIVES TECHNIQUES

17 janvier 2013
GCT700-NCT-n°9

Répercussions du système 9-1-1 de prochaine génération sur le réseau à large bande de sécurité publique dans la bande du 700 MHz – Évaluation technique

Large bande mobile pour la Sécurité publique dans la bande du 700 MHz - Groupe consultatif technique du Centre des sciences pour la sécurité - Sciences et technologie de la sécurité publique

Responsable fédéral : Le Groupe consultatif de la technologie sur les communications de sécurité publique dans la bande du 700 MHz (GCT700) est composé d'un groupe de collaborateurs experts techniques dirigé par le Centre des sciences pour la sécurité et comprend des responsables scientifiques du Centre de recherches sur les communications et des experts techniques d'organismes fédéraux/provinciaux/territoriaux/municipaux.

Objectif

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[1] 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.

1. Avis de consultation de télécom CRTC 2012-686 http://www.crtc.gc.ca/fra/archive/2012/2012-686.htm

Introduction

Le Bureau du développement de l'interopérabilité du Secteur de la gestion des urgences de Sécurité publique Canada a demandé à ce que le GCT700 conduise une évaluation technique des répercussions des systèmes 9-1-1 PG sur le RLBSP du 700 MHz. La demande vise partiellement à évaluer comment le réseau à large bande de sécurité publique peut appuyer les services 9-1-1 PG.

Portée et hypothèses

On examine dans la présente NCT les questions relatives au système 9-1-1PGabordées dans l'avis de consultation du CRTC, tel que mentionnées au tableau 1, qui ont des répercussions sur le RLBSP. Plusieurs des questions sont liées à des enjeux de politiques et à d'architecture du système 9-1-1 PG. La présente évaluation ne traite pas de ces aspects.

Le RLBSP diffusera les messages des services 9-1-1 PG provenant du centre d'appel de sécurité publique et répartiteurs vers les premiers intervenants. Dans la direction opposée, on suppose que les alertes d'urgence lancées par les premiers intervenants seront traitées dans le cadre d'un flux de travail qui comprend le centre d'appel de sécurité publique (CASP).

On suppose que les fournisseurs de services commerciaux pourront louer une partie des ressources du réseau à large bande de sécurité publique. On croit donc également que les abonnés aux fournisseurs de services seront capables d'ouvrir une session dans les services 9-1-1 de PG avec l'opérateur du CASP et de lui transférer des dossiers de données.

La présente NCT traite :

a) de la façon dont les systèmes 9-1-1 PG pourront interagir avec le RLBSP;

b) des moyens par lesquels les messages des systèmes 9-1-1 PG passent par le RLBSP entre un CASP et les premiers intervenants;

c) de la résilience des installations et des dépôts d'information;

d) des facteurs dont on tient compte du point de vue de la sécurité pour le flux des sessions sur les systèmes 9-1-1 PG.

Puisqu'il n'existe aucune architecture normalisée pour les services 9-1-1 PG au Canada, la présente NCT étudie la solution i3, adoptée par la US National Emergency Numbering Association (NENA) [1] et mentionnée dans l'*Avis de consultation du CRTC* (voir le tableau 1, paragr. 3).

B. Services 9-1-1 de prochaine génération

1. Avec les services 9-1-1 de prochaine génération, nous avons la possibilité de bâtir un système qui comporte de nouvelles fonctions évoluées. Indiquer comment le système 9-1-1 de prochaine génération devrait fonctionner en abordant les points suivants et tout autre point pertinent :

- comment les Canadiens pourraient communiquer avec les CASP et les équipes d'intervention d'urgence, par exemple les types d'appareils utilisés et les moyens de communication privilégiés, comment répondre aux besoins précis des personnes handicapées, etc.;
- les types d'information et de données, comme les photos, les vidéos, les dossiers médicaux, etc., qui pourraient être transmis aux CASP et échangés entre ces derniers;
- comment, et avec quel degré de précision, l'emplacement de l'appelant devrait être déterminé;
- comment financer la mise en oeuvre et l'exploitation continue du système 9-1-1 de prochaine génération.

2. La transition à une architecture fondée sur la technologie IP permet de réinventer la structure logique du système 9-1-1. Par exemple, certaines fonctions de secours ou bases de données pourraient avoir une portée nationale ou provinciale, tandis que la prestation de services pourrait continuer de se faire à l'échelle locale ou régionale. Indiquez les fonctions ou les bases de données qui, selon vous, devraient être fournies à l'échelle nationale ou provinciale afin de promouvoir la solidité, la résilience et l'efficacité du système.

3. On a proposé la solution i3 de la National Emergency Number Association (NENA) pour l'infrastructure du système 9-1-1 de prochaine génération. Cette solution a-t-elle fait l'objet d'un consensus au Canada? Si on a déterminé que la solution i3 est appropriée :

- quelles mesures le Canada doit-il prendre pour mettre en oeuvre cette infrastructure?
- quelles institutions (p. ex. organismes de sécurité publique, organismes de normalisation, le Conseil, entreprises, CASP, premiers intervenants) devraient participer à la mise en oeuvre de l'infrastructure?
- quels rôles occuperaient ces institutions?
- quel serait le calendrier des étapes du projet?

S'il n'y a pas consensus, donnez votre point de vue.

4. Le système 9-1-1 de prochaine génération permettra de recueillir des données détaillées et d'analyser les cas d'urgence.

- Quelles données devrait-on recueillir pour aider les décideurs et les directeurs de l'exploitation à réagir aux situations d'urgence et à planifier les secours en cas de catastrophe?
- Comment devrait-on recueillir ces données?

Tableau 1. *Extrait de l'avis de consultation du CRTC sur les systèmes 9-1-1 de prochaine génération.*

Résumé des recommandations

Recommandations formulées dans la NCT

R1 : La solution i3 de la NENA devrait servir de modèle pour comparer l'architecture du futur réseau de systèmes 9-1-1PG du Canada.

R2 : Le IP Multimedia Subsystem (IMS) devrait être mis en place comme une composante du RLBSP.

R3 : L'opérateur du RLBSP devrait conclure des accords d'itinérance avec des opérateurs commerciaux canadiens et américains ainsi qu'avec FirstNet[2].

R4 : L'opérateur des systèmes 9-1-1 PG devrait préciser la disponibilité requise de l'accès à des dépôts de données dans le cadre de la mise en œuvre du réseau de systèmes 9-1-1PG. Si l'opérateur choisit de confier l'hébergement des données à un partenaire externe, il devrait préciser la disponibilité requise de l'accès à des dépôts de données au fournisseur de services en tenant compte de la disponibilité opérationnelle et de la disponibilité pendant des catastrophes.

R5 : Les routeurs du centre d'échange pour le fournisseur de service IPX, les routeurs du RLBSP et ceux de l'infrastructure IP devraient correspondre à la définition d'un code d'accès aux services différenciés (CASD) du Groupe de travail d'ingénierie et de l'Internet (GTIE), contenue dans le RFC-2475. Cela permettrait d'assurer l'uniformité de la qualité des services et de hiérarchiser les priorités dans les messages liés au système 9-1-1 PG.

R6 : Tous les opérateurs des routeurs et des nœuds interréseautage qui font partie du trajet de diffusion des messages du système 9-1-1 PG devraient configurer les CASD de type Per Hop Behaviour (PHB) conformément à une association de codes d'accès aux services différenciés et de type de trafic ayant fait l'objet d'une entente entre les opérateurs.

R7 : La sécurité IP devrait être utilisée dans la fonction de contrôle de la frontière du réseau conformément à la RFC-2401 pour chiffrer l'information transmise dans les limites du domaine du réseau. L'algorithme de chiffrement devrait être équivalent à la Norme de chiffrement avancé 128 ou à un niveau plus élevé.

Interréseautage du système 9-1-1 de prochaine génération et du réseau à large bande de sécurité publique dans la bande du 700 MHz

Solution i3 de la NENA

La solution i3 de la NENA est fondée sur un réseau de réseaux IP. Elle définit les normes pour le réseau IP des services d'urgence (ESInet), illustré dans le schéma fonctionnel du tableau 2.

Le tableau 2 illustre deux régions, qui possèdent leur propre ESInet 9-1-1 PG et qui sont interconnectées pour former un réseau de réseaux. Dans chaque région, des opérateurs du CASP se branchent au réseau régional. Les abonnés aux fournisseurs de services commerciaux pourraient lancer des appels d'urgence 9-1-1 à l'aide de leurs appareils portables ou de leurs installations fixes. Les appareils automatiques comme les systèmes d'alerte de collision installés dans les véhicules pourraient aussi lancer des appels d'urgence aux services 9-1-1. Les réseaux sans fil commerciaux fournissent des informations sur l'emplacement du demandeur à ESInet. Ces informations peuvent être obtenus à l'aide du réseau sans fil des fournisseurs de services commerciaux ou de la fonction GPS de l'appareil de l'abonné. Les informations sur l'emplacement pour les abonnés sont sauvegardées sur le serveur d'information sur les emplacements (SIE).

Les fournisseurs de services commerciaux diffusent les messages des services 9-1-1 PG sur Internet. Le chapitre intitulé « Sécurité et assurance de l'information » traite des facteurs associés à la sécurité relatifs aux messages du système 9-1-1 PG. Les paquets de données du système 9-1-1 PG contiennent un en-tête unique qui permet de les distinguer de tout autre trafic sur les réseaux sans fil commerciaux. Cela permet de les acheminer dans ces réseaux en leur accordant une priorité plus élevée.

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

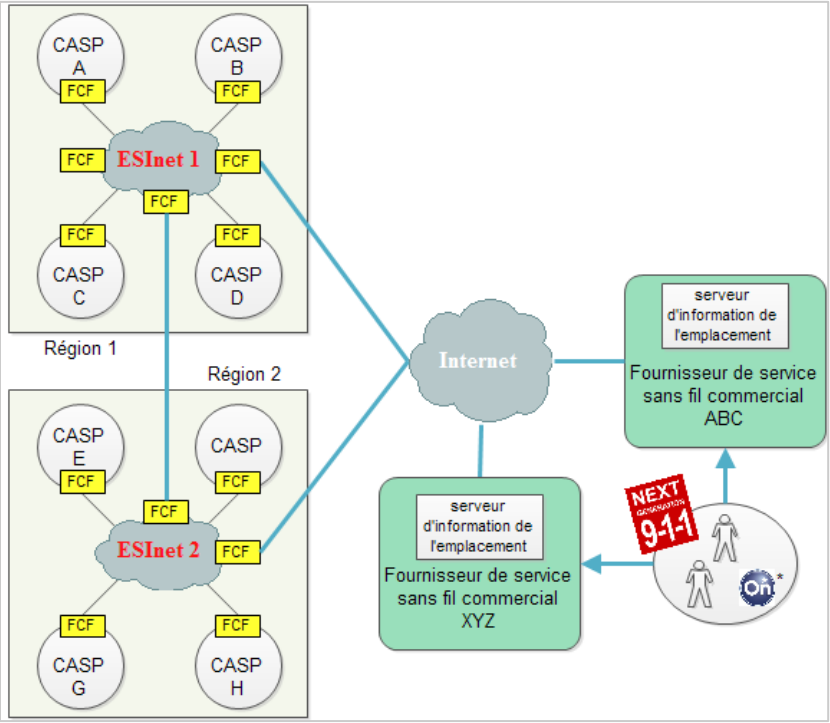

Tableau 2. *Schéma fonctionnel de l'ESInet et de l'interface des réseaux des fournisseurs de services commerciaux.* (* Marque déposée de OnStar Corporation)

Le premier élément du réseau qui reçoit les paquets de données du système 9-1-1 PG dans l'ESInet, la fonction de contrôle de la frontière, assure la sécurité entre les réseaux publics et l'ESInet ainsi qu'entre les divers réseaux au sein de celui-ci. Tout juste derrière la fonction de contrôle de la frontière dans l'ESInet se trouve le proxy de routage des services d'urgence, qui achemine les paquets de données du système 9-1-1 PG au CASP approprié, conformément aux politiques en matière d'acheminement et en fonction de l'emplacement estimé du demandeur.

ESInet utilise un protocole d'initiation de session [2] pour créer, modifier et terminer les sessions de transmission de données et de voix avec un ou plusieurs participants. Les sessions de transmission de données comprennent la distribution multimédia et les conférences multimédia. Le protocole d'initiation de session utilise des éléments appelés serveurs proxy pour aider à acheminer les demandes, à authentifier les utilisateurs et à autoriser l'accès aux services.

En résumé, la solution i3 comprend un ensemble complet de normes et d'exigences relatives à la mise en place d'ESInet, conçu et approuvé par la NENA, une organisation bien établie et respectée d'établissement de normes applicables aux communications des services d'urgence 9-1-1 aux États-Unis.

Recommandation n° 1

On devrait songer à utiliser la solution i3 de la NENA comme modèle pour comparer l'architecture du futur réseau de systèmes 9-1-1 PG du Canada.

Interface entre l'ESInet et le réseau à large bande de sécurité publique

Quand vient le temps de définir l'interface entre le réseau des services 9-1-1 de prochaine génération et le réseau à large bande de sécurité publique, il est utile d'examiner l'interface que le gouvernement américain a proposé entre l'ESInet et le réseau national à large bande de sécurité publique de Firstnet (NPSBN). Le Bureau d'interopérabilité de la Commission fédérale des communications des États-Unis a publié ses exigences techniques en matière d'interopérabilité pour le NPSBN en mai 2012. Il a présenté ce document, qui contenait ses recommandations en matière d'interopérabilité, à FirstNet.

Le tableau 3 illustre l'approche que les membres du Bureau d'interopérabilité ont proposée pour l'interface entre le NPSBN et l'ESInet. Le diagramme montre l'interface entre l'ESInet et la fonction d'applications et de services qui appuient la téléphonie (voix), les services d'envoi de messages courts et les services de messagerie multimédia. Il montre aussi une solution alternative pour la connexion du NPSBN au réseau principal à l'aide de l'Internet public.

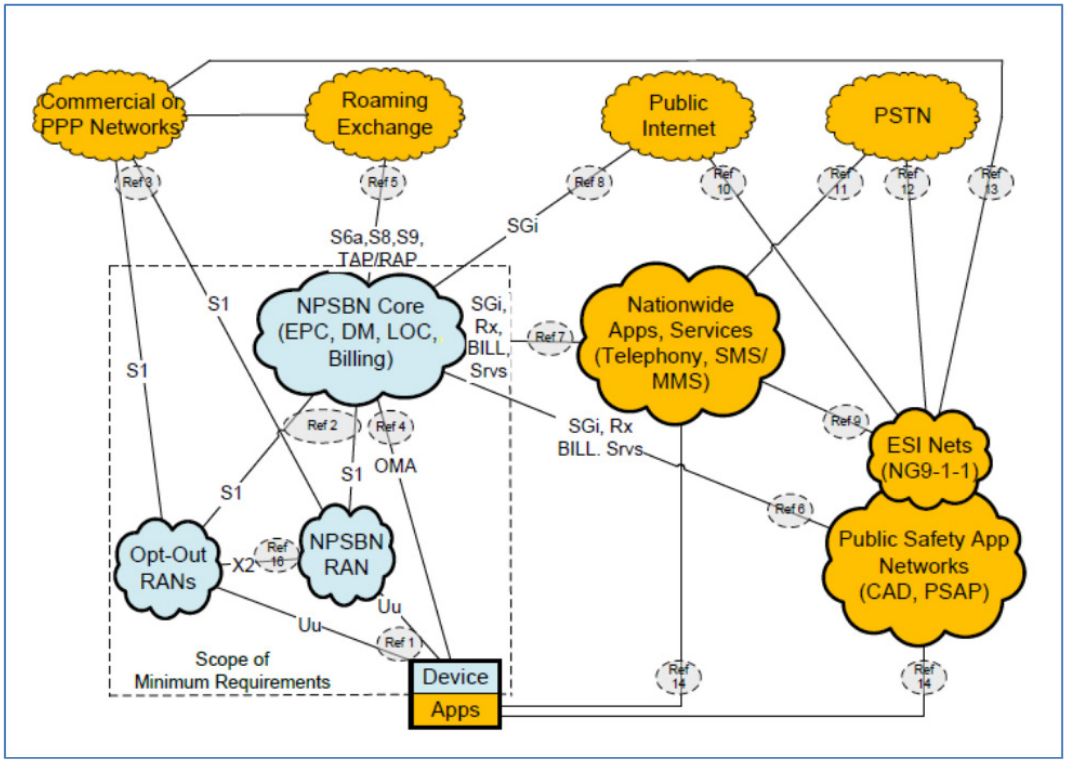

Tableau 3. *Le plan des réseaux environnants qui font interface avec le réseau de la sécurité publique des États-Unis tel que suggéré par le Bureau d'interopérabilité.* Source: [3]

Dans le contexte canadien, le tableau 4 montre comment le RLBSPpourrait être en liaison avec un projet de mise en œuvre du genre ESInet au Canada fondé sur la solution i3 de la NENA. Le schéma fonctionnel illustre ce qui suit :

a) Le RLBSPest réparti entre l'entité nationale et l'entité de fourniture de services régionale (EFSR). Cette dernière fournit l'interface du Réseau d'accès radio aux premiers intervenants et aux utilisateurs commerciaux[3]. L'entité nationale accueillerait le SIE qui fournit l'information sur l'emplacement aux premiers intervenants et aux autres abonnés. Le chapitre intitulé « Sécurité et assurance de l'information » traite des facteurs relatifs à la sécurité associés à de l'information de cette nature.

b) Le IP Multimedia Subsystem (IMS) [4] permet d'utiliser les en-têtes de signalisation du protocole d'initiation de session pour acheminer les paquets IP vers les contrôleurs de session en périphérie du IP Multimedia Subsystem, qui peut être mis en œuvre dans diverses architectures de réseau. Par exemple, il peut être géré par l'entité nationale ou être confié à un service d'hébergement externe. Les contrôleurs de session en périphérie, qui ne sont pas illustrés dans le tableau 4, peuvent être distribués parmi les EFSR. Essentiellement, l'IMS donne les moyens d'acheminer les paquets IP multimédia qui utilisent la signalisation du protocole d'initiation de session vers leurs adresses de destination ainsi que d'assurer l'interface entre le RLBSPet les réseaux qui hébergent les applications.

   L'IMS pourrait aussi faciliter la transmission de données vocales et vidéo entre les utilisateurs sur les réseaux commerciaux et ceux sur le RLBSP. Il ajoutera d'autres capacités comme l'établissement des priorités du trafic dans l'ensemble du réseau.

[3] On suppose que les consommateurs peuvent utiliser le réseau de sécurité publique par l'entremise d'un détaillant. Industrie Canada doit confirmer cette hypothèse.

Recommandation n° 2

Un IMS devrait être mis en œuvre pour faire partie du réseau à large bande de sécurité publique.

c) Le centre d'échange de données d'IPX est un service tiers qui permet l'échange de trafic IP, composé d'information sur le contrôle et sur les utilisateurs, entre les fournisseurs de services. Le centre d'échange de données d'IPX permet habituellement la conclusion d'ententes d'itinérance entre les fournisseurs de services. Il est nécessaire d'envoyer des messages d'urgence à l'aide de plusieurs fournisseurs de services afin de joindre les premiers intervenants, qui peuvent être à l'extérieur de la zone de couverture radio du RLBSP, mais dont l'équipement peut être hébergé sur le réseau d'un fournisseur de services commerciaux.

   À plusieurs endroits, le premier intervenant le plus près pourrait se trouver de l'autre côté de la frontière canado-américaine. Il est donc important d'être en mesure de joindre les premiers intervenants américains sur leur NPSBN. Pour ce faire, on envisage d'établir une connexion au NPSBN de FirstNet par l'intermédiaire du centre d'échange de données d'IPX. Le présent document ne tient pas compte des politiques et des ententes internationales nécessaires pour faciliter les interventions transfrontalières en cas d'urgence. Il suffit par contre de permettre à l'architecture de mettre les ententes en œuvre.

Il est important de noter que dans le tableau 4, les messages d'urgence proviennent d'un diffuseur de messages d'urgence afin de montrer que le réseau de diffusion de messages d'urgence et l'ESInet peuvent être des réseaux distincts. On peut penser que les messages d'urgence pourraient être distribués à l'aide du réseau du système 9-1-1 de PG, mais cette approche n'est pas illustrée puisque la solution i3 de la NENA ne couvre pas les messages d'urgence de cette façon.

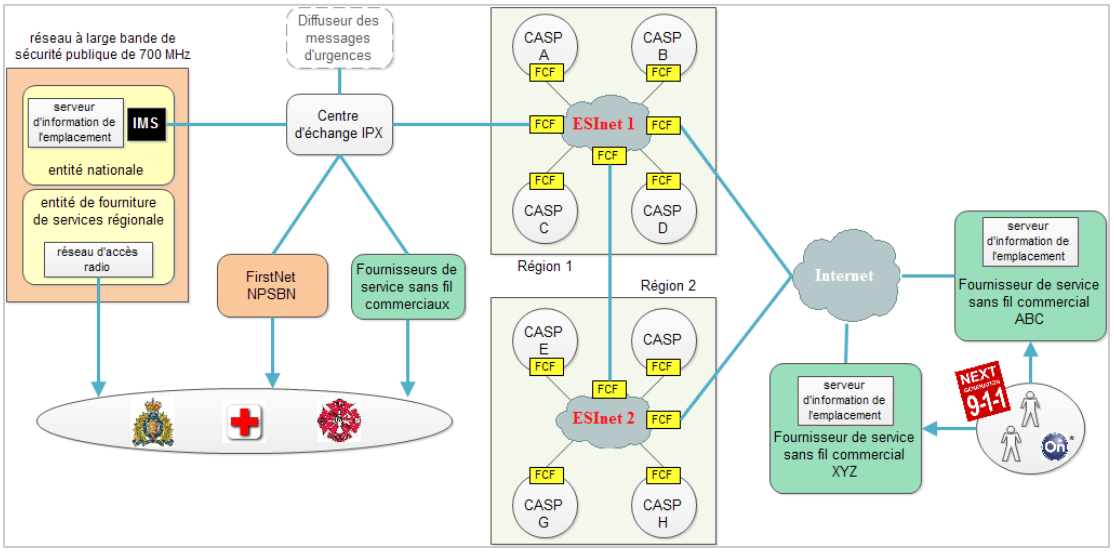

Tableau 4. *Schéma fonctionnel de l'interface entre le réseau à large bande de sécurité publique dans la bande du 700 MHz et ESInet.*

Recommandation n^{o} 3

L'opérateur du réseau à large bande de sécurité publique devrait conclure des ententes d'itinérance avec des opérateurs commerciaux ainsi qu'avec FirstNet.

<u>Précision de l'information sur l'emplacement avec les réseaux sans fil du 3GPP</u>

Il est essentiel, lors d'une intervention en cas d'urgence, de localiser l'emplacement du demandeur et du premier intervenant. Tel que mentionné plus haut, l'information sur l'emplacement est sauvegardée dans le serveur d'information sur l'emplacement. Plus précisément, l'emplacement a trait à l'équipement de l'usager. On obtient l'emplacement de l'équipement de l'usager par triangulation sur l'ensemble du réseau, c'est-à-dire en mesurant la différence entre les temps d'arrivée des signaux provenant de diverses tours. Ce calcul est rendu plus précis grâce aux données recueillies à l'aide de la fonction GPS de l'appareil de l'utilisateur.

Le CRTC a adopté une recommandation présentée dans le rapport de son Groupe de travail sur les services d'urgence [6], daté d'octobre 2008, selon laquelle le fournisseur de services sans fil fournira au CASP, au sujet de l'emplacement d'un demandeur, de l'information non filtrée qui indiquera (i) les coordonnées X et Y (ii) le niveau de confiance envers l'information et (iii) le degré d'imprécision. Le tableau 5 présente cette recommandation.

Le 1er février 2010, le CRTC a annoncé l'introduction de services d'urgence 9-1-1 améliorés, qui devaient permettre de trouver l'emplacement du demandeur dans un rayon de 10 à 300 mètres.

La Commission fédérale des communications des États-Unis (FCC) a défini la précision avec laquelle on devait déterminer où se trouve un combiné sans fil dans son troisième rapport et décret [5] (1999), qui énonçait les exigences en matière de précision pour les services d'urgence E9-1-1 améliorés. Le degré de précision demandé est mentionné dans le tableau 6. La FCC a reconnu que le degré de précision ne peut être garanti dans tous les cas. La précision peut atteindre un rayon de 300 mètres pour 95 % des appels faits aux services E9-1-1, et de 100 mètres dans 67 % des cas. L'emplacement établi à l'aide d'un appareil devrait être plus précis que celui déterminé à l'aide d'un réseau.

Recommandation du GTSU

Le GTSU recommande que les valeurs de confiance (%) et de l'imprécision (en mètres) en plus de les coordonnées X, Y ou un message d'erreur soient transmis au CASP pendant un appel sans fil de E911 phase II. Le GTSU recommande en outre que les paramètres qui suivent soient utilisés:

1. Valeur de confiance réglée à 90%;
2. Valeur de l'imprécision (m) devra être calculée par l'équipement de détermination de localisation ;
3. L'information du sans-fil E9-1-1 de la phase II, soit les coordonnées X Y, la confiance et l'imprécision ou un message d'erreur, seront envoyés en moins que 30 secondes;
4. À 30 secondes, les informations de localisation ou un message d'erreur doit être transmis par le serveur à l'emplacement du FSSF.

Tableau 5. *Extrait du rapport du Groupe de travail sur les services d'urgence, Exigences techniques et opérationnelles liées à la mise en œuvre du service E-9-1-1 sans fil de la Phase II.* [6]

Pourcentage d'appels du genre E911	précision de l'emplacement	
	dérivé par le réseau	dérivé à l'aide de l'appareil
67%	100 mètres	50 mètres
95%	300 mètres	150 mètres

Tableau 6. *Précision exigée par la FCC pour les appels aux services E9-1-1*

Stratégie en matière de résilience pour les installations de transmission et les dépôts de données

Les stratégies en matière de résilience comprennent généralement la multiplication des éléments des infrastructures, comme les serveurs et les bases de données. Les installations seraient situées dans des secteurs géographiques distincts qui ne sont pas sujets aux mêmes conditions environnementales et, idéalement, qui ne sont pas desservis par le même réseau électrique. L'interconnectivité entre les installations serait assurée par des trajets de transmission redondants hébergés sur des réseaux distincts. Dans une redondance 1:1, une installation est l'auxiliaire de l'autre. D'autres degrés de redondance peuvent être mis en place afin de tolérer de multiples pannes simultanées. Le tableau 8 illustre le concept de la redondance 1:1.

Au Canada, un réseau comme ESInet pourrait être mis en œuvre dans l'ensemble du pays sous la forme d'un réseau de réseaux. Chaque opérateur d'un CASP serait branché à un réseau

national de services 9-1-1 PG. Les bases de données pourraient être situées n'importe où sur le réseau, et être multipliées pour améliorer la résilience tout en assurant une prise en charge à l'échelle locale des données qu'elles contiennent. Essentiellement, avec une architecture de réseau similaire à ESInet, la prise en charge de l'information n'est pas liée à la prise en charge physique des dépôts. Un certain regroupement des dépôts de données permettrait cependant de réduire les coûts d'exploitation.

Les représentants du CASP peuvent choisir d'acheter un service hébergé dans un nuage pour les dépôts de données, et ils préciseraient la disponibilité des services, notamment au cours d'une catastrophe naturelle ou humaine.

Recommandation n^{o} 4

L'opérateur des services 9-1-1 PG devrait préciser la disponibilité des services pour les dépôts de données dans le cadre de la mise en œuvre du réseau de services 9-1-1 PG, ou préciser cette information au fournisseur de services d'hébergement. On devrait alors tenir compte de la disponibilité pendant les opérations normales et pendant les catastrophes.

Flux de messages des services 9-1-1 PG sur le RLBSP dans la bande du 700 MHz On s'attend à ce que les messages envoyés aux services 9-1-1 de PG soient acheminés du citoyen au CASP, puis du CASP au répartiteur, puis de ce dernier au premier intervenant. Il est toutefois possible que les premiers intervenants lancent des messages d'alarme d'urgence pour informer le répartiteur d'une menace imminente pour eux ou pour la population. Dans certains cas, le CASP pourrait faire partie des destinataires d'un message d'alarme d'urgence fait par le premier intervenant.

Si des abonnés commerciaux sont desservis par le RLBSPdans la bande du 700 MHz, le message proviendrait d'un abonné, serait dirigé vers le CASP, puis acheminé vers le réseau à large bande à l'intention du premier intervenant le plus près.

Priorités et QDS pour les messages des systèmes 9-1-1 PG

Les messages d'urgence doivent être diffusés avec une haute priorité afin d'être retardés le moins possible en cas de congestion du chemin de transmission, soit sur le réseau radio ou sur le réseau filé. Selon les caractéristiques de la solution i3 de la NENA, le trafic IP sur ESInet doit mettre des services différenciés en place [7]. Les services différenciés est une façon de marquer la priorité des paquets IP selon une norme acceptée par l'industrie, définie par le Groupe de travail d'ingénierie et de l'Internet. Les routeurs IP de l'ESInet marquent le trafic à l'aide d'un champ de 6 bits dans l'en-tête IP qui définit le code d'accès aux services différenciés. Les routeurs IP équipés de services différenciés interprètent le code d'accès du message et traitent le paquet IP en lui accordant la priorité qui correspond au code d'accès

Recommandation n^{o} 5

Les routeurs du centre d'échange pour le protocole IPX, les routeurs du RLBSPe et ceux de l'infrastructure IP devraient correspondre à la définition d'un code d'accès aux services différenciés du Groupe de travail d'ingénierie et de l'Internet, contenue dans le RFC-2475. Cela permettrait d'assurer l'uniformité de la qualité des services et de hiérarchiser les priorités dans les messages liés au système 9-1-1 PG entre les domaines de réseau.

La solution i3 de la NENA établit une convention pour assigner le type d'information à un niveau particulier de comportement Per Hop Behaviour (PHB) du code d'accès aux services différenciés. Le PHB est l'un des points de configuration par lequel un routeur ou un nœud attribue la bande passante aux paquets IP et gère les queues dans les mémoires tampons. Le tableau 7 montre la répartition des PHB en fonction du type de trafic, selon la solution i3 de la NENA.

CASD	Utilisation	PHB
0	trafic ordinaire	default
1	signalisation du message 9-1-1	AF12
2	contenu texte du message 9-1-1	AF12
3	contenu audio du message 9-1-1	EF
4	contenu vidéo du message 9-1-1	AF11
5	message 9-1-1 initité par un non-humain	AF21
6	événements intra-ESInet	AF21
7	message autre 9-1-1 intra-ESInet	AF21

Tableau 7. *Répartition des types de trafic, par CASD, en fonction des valeurs de PHB [8][4], selon la solution i3 de la NENA.*

Recommandation n^{o} 6

Tous les opérateurs des routeurs et des nœuds interréseautage qui font partie du trajet de transmission des messages du système 9-1-1 devraient configurer les comportements de type DSCP Per Hop Behaviour PHB conformément à une association de points de code d'accès aux services différenciés et de type de trafic ayant fait l'objet d'une entente.

La portion du réseau radio du RLBSP sera probablement mise en œuvre à l'aide d'une technologie d'évolution à long terme (LTE)[5]. Cette technologie fournit tout un ensemble de qualité de service et d'établissement des priorités qui nous permettent de relever et de traiter les messages des services 9-1-1 PG avec une haute priorité.

Ces paramètres sont appelés « priorité de rétention des attributions (PRA) » et « identificateur de classe de QDS ». Le réseau LTE peut établir des liens entre les marquages du code d'accès aux services différenciés et les paramètres de priorité de rétention des attributions et de classe de qualité de service correspondants du domaine LTE, et donc permettre le traitement uniforme des priorités pour les paquets associés aux services 9-1-1 PG.

Sécurité et assurance de l'information

Le Groupe consultatif de la technologie examine actuellement l'architecture de sécurité recommandée par l'Union internationale des télécommunications (UIT), qui pourrait devenir le cadre dans lequel serait établi les exigences de sécurité relatives au RLBSP. Selon les recommandations ITU-T Y.2701 [9] et ITU-T X.805 [10], dans le cas des réseaux multidomaines, chaque fournisseur de services est chargé de la sécurité dans son domaine, et chacun d'eux doit concevoir et mettre en œuvre des solutions de sécurité permettant de répondre aux besoins propres à son réseau. Dans ce contexte, le RLBSP, le centre d'échange de l'IPX, le réseau des services 9-1-1 PG et d'autres réseaux peuvent être considérés comme des domaines distincts. Le présent avis technique ne traite pas des mesures que les exploitants de réseaux devraient mettre en place pour assurer la sécurité de leurs réseaux. Il traite de la sécurité de l'information qui traverse les frontières entre les domaines de réseau.

Le tableau 9 illustre l'utilisation des fonctions de contrôle de la frontière que chaque exploitant de réseau mettrait en place aux endroits où au moins deux réseaux se rencontrent. L'une des fonctions de contrôle de la frontière est de chiffrer l'information transmise entre les réseaux. Le choix de l'algorithme de chiffrement revient aux exploitants des réseaux. Les fonctions de contrôle de la frontière, telles que mise en œuvre, peuvent habituellement soutenir plusieurs algorithmes dans le même appareil.

Recommandation n^{o} 7

La sécurité IP [11] devrait être utilisée dans la fonction de contrôle de la frontière conformément au RCF-2401 pour chiffrer l'information transmise dans les limites du domaine du réseau. L'algorithme de chiffrement devrait être équivalent à la Norme de chiffrement avancé 128 ou à un niveau plus élevé.

[4] Le RFC-2597[B] donne la définition de PHB.

[5] La technologie d'évolution à long terme représente la dernière génération de technologie mobile sans fil du Projet de partenariat de troisième génération. http://www.3GPP.org

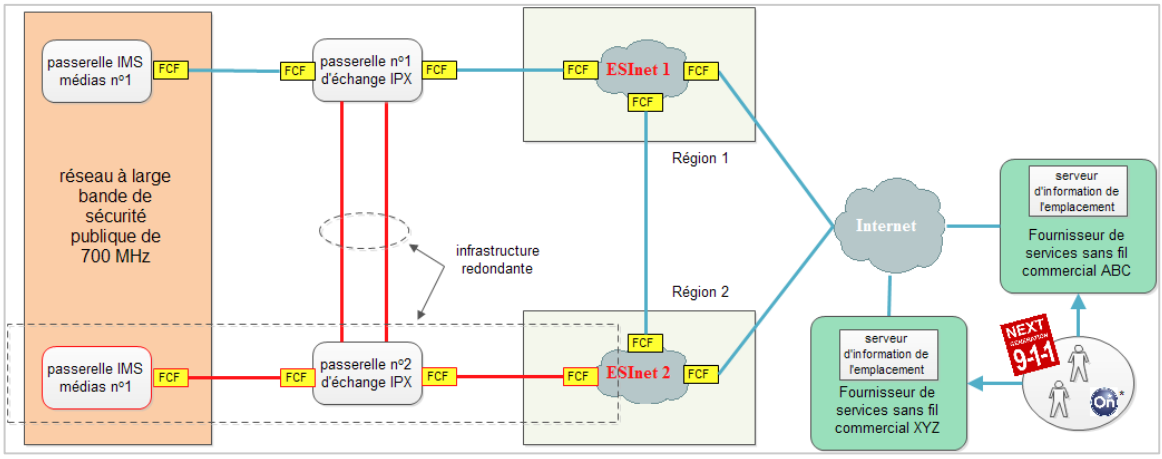

Tableau 8. *Illustration du concept de la protection 1:1 des sous-réseaux ESInet, des passerelles IPX et des chemins de transmission.*

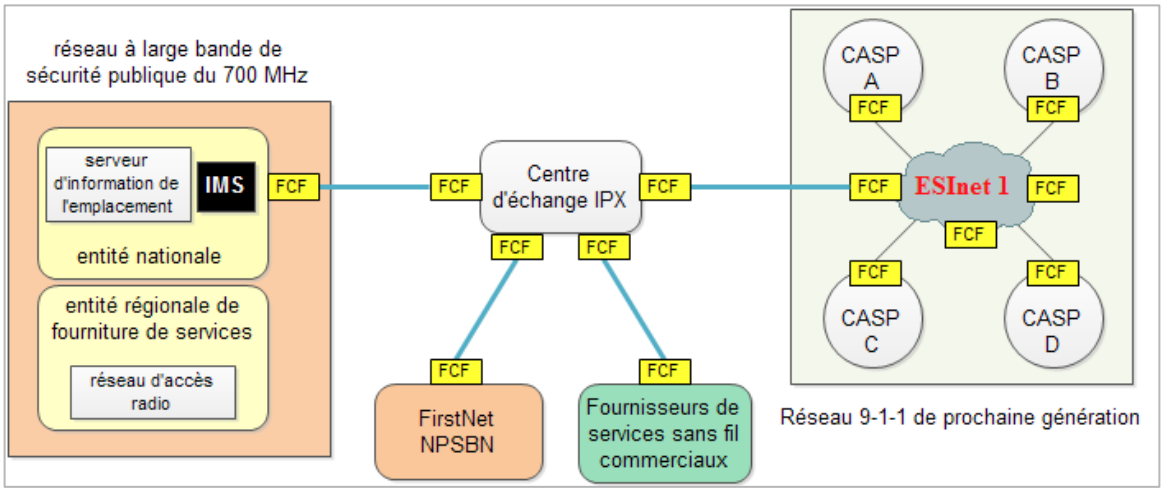

Tableau 9. *Illustration de l'utilisation des fonctions de contrôle de la frontière pour protéger l'information transmise entre les réseaux.*

IPsec offre plusieurs degrés de protection de l'information :

- Contrôle d'accès;
- Intégrité des données, donc le rejet des paquets repris[6];
- Authentification de l'origine des données;
- Assurance de la confidentialité grâce au chiffrement.

Une autre dimension importante relative à la sécurité associée de près à l'assurance de l'information est la *non-répudiation*. IPsec n'offre aucune protection en ce qui a trait à cette dimension. Des mesures additionnelles qui vont au-delà d'IPsec sont nécessaires pour s'assurer

[6] L'attaque par mascarade est une forme de paquet repris [10].

que la réception des données ne puisse être niée.

Le modèle de confiance servant à partager les clés et les certificats numériques destinés à protéger l'information transmise entre les fonctions de contrôle de la frontière dépend des ententes conclues entre les opérateurs de réseaux, et il devrait être fondé sur une évaluation des besoins opérationnels et des risques pour la sécurité. Le Centre de la sécurité des télécommunications Canada (CSTC) propose une méthode permettant de définir les risques pour la sécurité et les degrés de contrôle souhaitables pour atténuer de tels risques pour les réseaux de communication de données [12].

Conclusion

Le système 9-1-1 de PG permet aux citoyens de signaler une situation d'urgence au CASP à l'aide de méthodes répandues que la population utilise actuellement pour communiquer, c'est-à-dire par messagerie texte. Il permet aussi de communiquer un contenu riche au sujet de l'urgence qui doit être signalée au CASP, ce qui améliore la connaissance de la situation de l'opérateur du CASP, du répartiteur et des premiers intervenants qui répondent à l'urgence.

En plus d'une description textuelle de l'urgence, on s'attend à ce que d'autres informations soient transmis dans le message (c.-à-d. de l'information sur l'emplacement jointe au reste du contenu). Ces informations seraient, entre autres, des images, des fichiers vidéo accompagnés d'un message audio superposé et de voix par IP. Un système IMS devra être intégré au réseau à large bande de sécurité publique dans la bande du 700 MHz, ou ce service devra être imparti, afin de permettre au réseau de traiter les messages courts, les messages multimédia et les messages d'alerte par voix sur IP.

La NENA a défini les exigences techniques auxquelles devra répondre un réseau de services d'urgence sur IP, appelé ESInet. L'ESInet est destiné à devenir un réseau national de réseaux qui établira une connexion entre les CASP locaux et régionaux. Dans le présent avis technique, la solution i3 de la NENA sert de modèle pour l'évaluation des répercussions sur le CASP, au plan technique, du réseau 9-1-1 PG.

Le CASP n'est que l'un des réseaux auxquels les premiers intervenants devront avoir accès. On s'attend à ce qu'il y ait des lacunes liées à la couverture lors du déploiement du réseau à large bande de sécurité publique, surtout lors des étapes initiales. Il sera nécessaire d'établir des ententes d'itinérance avec les fournisseurs commerciaux afin que les premiers intervenants puissent être joints à l'aide des réseaux commerciaux. De plus, si les ententes internationales le permettent, on pourrait demander à des intervenants américains de répondre à une urgence. Pour cela, des ententes d'itinérance doivent être conclues avec FirstNet ainsi qu'avec des fournisseurs commerciaux canadiens et américains. Le centre d'échange pour le protocole IPX est un service offert par un tiers et qui facilite l'établissement et la gestion d'ententes d'itinérance en plus de fournir une connectivité entre les réseaux des parties aux ententes.

Lorsqu'un demandeur envoie un message d'urgence, il est impératif de le localiser aussi précisément que possible dans un très court laps de temps. Le Canada et les États-Unis ont adopté des règlements sur la précision avec laquelle on doit localiser un appareil sans fil à partir duquel un appel d'urgence est fait. Ces règlements ne sont pas énoncés de façon identique au Canada et aux États-Unis, mais ils visent essentiellement à localiser le demandeur dans un rayon de 10 à 300 mètres.

Les catastrophes naturelles survenues récemment aux États-Unis ont permis de constater la vulnérabilité des réseaux 9-1-1 actuels en cas de phénomènes météorologiques violents. La FCC a amorcé une enquête sur la façon d'améliorer la résilience des réseaux 9-1-1 [12]. Un réseau IP comme ESInet permet la multiplication des installations dans des régions géographiques distinctes qui ont peu de chances d'être exposées au même risque simultanément. De plus, les dépôts de données et les bases de données de secours peuvent aussi être séparées par de grandes distances et permettre à chaque administration de demeurer néanmoins propriétaire de l'information contenue dans ces bases de données. Les fournisseurs externes de services hébergés dans un nuage offrent des services de sauvegarde de données qui peuvent être achetés aux niveaux précisés de disponibilité.

Les messages d'urgence doivent être transmis, avec une haute priorité, dans tous les réseaux qui font partie du chemin de transmission. La flexibilité qu'offre la technologie IP à l'opérateur du réseau lorsque celui-ci accorde une haute priorité aux messages d'urgence et les traitent avec cette même priorité représente un avantage distinct. Toutefois, la flexibilité des mécanismes liés à la priorité et à la QDS signifie aussi que les opérateurs de réseaux peuvent choisir de les configurer différemment. Cela peut mener au comportement imprévisible des paquets de messages d'urgence lorsqu'ils passent d'un réseau à un autre. Il est donc essentiel que les opérateurs de réseaux qui établissent un partenariat conviennent d'une approche uniforme servant à marquer et à traiter les paquets, et qu'ils s'y conforment.

Tous les réseaux publics de sécurité des communications seront probablement la cible d'attaques cybernétiques. Chaque opérateur de réseau devra mettre en œuvre ses propres mesures d'atténuation de ces risques et vulnérabilités. La frontière entre les réseaux est un point vulnérable et les opérateurs de réseau devront chiffrer l'information qui la traverse.

Références

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

2. Groupe de travail d'ingénierie et de l'Internet, *Protocole d'ouverture de session*, RFC-3261, juin 2002.

3. Comité consultatif technique sur l'interopérabilité des premiers intervenants, Commission fédérale des communications des États-Unis (FCC), *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*, rapport final, 22 mai 2012.

4. Projet de partenariat de troisième génération (3GPP), *Multimedia Subsystem (IMS) Emergency Sessions (Release 10)*, TS 23.167, décembre 2012.

5. Commission fédérale des communications des États-Unis (FCC), *Revision of the Commission's Rules To Ensure Compatibility with Enhanced 9-1-1 Emergency Calling Systems*, 3e rapport et ordonnance, FCC 99-245, 6 octobre 1999.

6. Comité directeur du CRTC sur l'interconnexion, Groupe de travail Services d'urgence, *Exigences opérationnelles et techniques concernant la mise en œuvre de la Phase II du service E9-1-1 sans fil*, rapport numéro ESRE0046, 31 octobre 2008.

7. Groupe de travail d'ingénierie et de l'Internet, *An Architecture for Differentiated Services*, RFC2475, décembre 1998.

8. Groupe de travail d'ingénierie et de l'Internet, *Assured Forwarding PHB Group*, RFC-2597, juin 1999.

9. Union internationale des télécommunications, *Security requirements for Next Generation Networks release 1*, recommandation Y.2701, ITU-T, avril 2007.

10. Union internationale des télécommunications, *Security architecture for systems providing end-to-end communications*, recommandation X.805, ITU-T, octobre 2003.

11. Groupe de travail d'ingénierie et de l'Internet, *Security Architecture for the Internet Protocol*, RFC-2401, novembre 1998.

12. Centre de la sécurité des télécommunications Canada, gouvernement du Canada, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, ITSG-33, novembre 2012.

13. Avis public de la FCC, Public Safety and Homeland Security Bureau seeks comment on 911 resilience and reliability in wake of June 29, 2012, derecho storm in central, mid-Atlantic, and northeastern United States, DA 12-1153, 18 juillet 2012.

14. Groupe de travail d'ingénierie et de l'Internet, *Location Conveyance for the Session Initiation Protocol*, RFC-6442, dèc. 2011.

15. Walt Magnussen, PH.D, *NG 9-1-1 and LTE: A Beneficial Union*, *Mission Critical Magazine*, mars 2012

Liste d'acronymes

3GPP	Projet de partenariat de troisième génération
AF	« Assured Forwarding »
NCA	Norme de chiffrement avancé
PRA	Priorité de rétention des attributions
FCF	Fonction de contrôle de la frontière
CRTC	Conseil de la radiodiffusion et des télécommunications canadiennes
CSS	Centre des sciences pour la sécurité
CSTC	Centre de la sécurité des télécommunications Canada
DiffServ	Services différenciés
CASD	Code d'accès aux services différenciés
EF	« Expedited Forwarding »
ESInet	Réseau IP des services d'urgence
PRSU	Proxy de routage des services d'urgence
GTSU	Groupe de travail sur les services d'urgence
FCC	Commission fédérale des communications (É-.U.)
FirstNet	First Responder Network Authority (FirstNet)
GPS	Système mondial de localisation
IETF	Groupe de travail d'ingénierie et de l'Internet
IMS	Sous-système IP multimédia
IP	Protocole Internet
IPX	IP eXchange
UIT	Union internationale des télécommunications
SIE	Serveur d'information sur les emplacements
LTE	Technologie d'évolution à long terme
MMS	Services de messagerie multimédia
NENA	National Emergency Numbering Association
9-1-1 PG	Système 9-1-1 de prochaine génération
AC	Avis de consultation
NPSBN	National Public Safety Broadband Network (É.-U.)
EDE	Équipement de détermination de l'emplacement
PHB	Per-Hop-Behaviour
CASP	Centre d'appel de la sécurité publique
RMLBSP	Réseau mobile à large bande de sécurité publique
QCI	Indicateur de classe de qualité de service
QDS	Qualité du service
EFSR	Entité de fourniture de services régionale
CSP	Contrôleur de session en périphérie
PIS	Protocole d'initiation de session
SMS	Service de messagerie texte
GCT	Groupe consultatif de la technologie
EU	Équipement de l'utilisateur
FSSF	Fournisseur de services sans fil

Le Centre des sciences pour la sécurité de RDDC garantit que la présente NCT a été préparée avec professionnalisme, conformément aux pratiques généralement reconnues pour la recherche et l'analyse scientifiques. Ce document présente un avis technique et ne constitue donc pas une déclaration d'appui de la part de Recherche et développement pour la défense Canada, du ministère de la Défense nationale ou du gouvernement du Canada.

Auteur

Claudio Lucente, ing., M.Ing.
Conseiller technique principal - Groupe consultatif de la technologie
Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC)

Autorités scientifiques

Dr. Daniel Charlebois, Ph.D.
Gestionnaire de portefeuille, Communications interopérables
Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC)

Pierre Meunier, ing, M.Sc.
Chef, Sciences et technologie, Résilience de la frontière et des infrastructures essentielles
Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC)

Jack Pagotto
Chef, Gestion multiorganismes des crises
Programme canadien pour la sûreté et la sécurité
Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC)

Vérificateurs

Doug Allport
Conseiller spécial – Communications à Sécurité publique Canada
Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC)

Simon Arcand
Évaluation de l'assurance élevée – Centre de la sécurité des télécommunications Canada (CSTC)

Dr. Stephen Braham, Ph.D.
Directeur – PolyLab for Advanced Collaborative Networking, Université Simon Fraser

Jacob Gurnick
Ingénieur de recherche principal, Centre de recherches sur les communications Canada, gouvernement du Canada

Dr. Walt Magnussen, Ph.D.
Directeur – Internet2 Technology Evaluation Center, Université Texas A&M
Champion de la sécurité publique, US UCAN

Luc Samson
Groupe consultatif de la technologie
Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC)

Approbation pour publication

Dr. Andrew Vallerand, Ph.D.
Directeur – Direction générale de la science et de la technologie, Sécurité publique
Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC)

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.)

Répercussions du système 9-1-1 de prochaine génération sur le réseau à large bande de sécurité publique dans la bande du 700 MHz – Évaluation technique

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(F)	

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.)

Gestion des situations d'urgence; 700MHz; 9-1-1 PG; Centre d'appel de sécurité publique (CASP);