

LE RÉSEAU RADIO DU FUTUR

by airphel

Le Réseau Radio du Futur (RRF) est un nouveau système de communication pour missions critiques conçu pour les services de sécurité publique et de secours.

Le RRF a été créé pour remplacer les réseaux radio bas débit actuels vieillissants et qui ne répondent plus aux besoins des forces de sécurité et de secours. En effet, s'appuyant sur une technologies pré-GSM (TETRAPOL), ces réseaux ne sont plus en phase avec les usages de ses utilisateurs actuels que les policiers, les gendarmes, les secouristes ou encore les pompiers. Seules les communications vocales et les messages textes peuvent transiter sur ces réseaux et le parc prenant de l'âge, les frais d'entretien et de maintenance s'accroissent d'année en année.

Ainsi l'objectif du RRF est de fournir d'ici 2024, un système de communication rapide, sécurisé, résilient et totalement interopérable aux forces de sécurité et d'urgence basé sur la norme de communication MCPTT (Mission Critical Push-to-Talk-Over Cellular LTE) dédiées aux missions critiques standardisées par le 3GPP.

(3rd Generation Partnership Project est une coopération entre organismes de normalisation en télécommunications tels que : l'UIT, l'ETSI, l'ARIB/TTC, le CCSA, l'ATIS et le TTA. Il produit et publie les spécifications techniques pour les réseaux mobiles de 3^e, 4^e et 5^e générations. Source Wikipédia)

Le RRF va permettre :

- des communications radio vocales Push-To-Talk,
- l'échange de données,
- des communications vidéo,
- d'utiliser des applications métiers,
- une priorité des communications des abonnés RRF par rapport aux utilisateurs grand public (accès prioritaire et débit garanti pour les échanges),
- la géolocalisation de ses utilisateurs,
- l'interopérabilité entre différents corps de métier/communautés,
- l'ajout d'une couverture réseau additionnelle en cas de crise, catastrophe.

Le RRF fonctionnera grâce aux infrastructures des opérateurs de réseaux mobiles et intégrera les technologies 4G et 5G. Le RRF sélectionnera deux opérateurs et ses utilisateurs bénéficieront d'un usage prioritaire par rapport au grand public. Ce dispositif de priorité leur évitera toute saturation de leurs communications en cas de congestion du trafic.

Contrairement aux réseaux critiques bas débit actuels qui limitent les communications à une zone géographique définie, grâce à l'itinérance offerte par les opérateurs téléphoniques, les communications transitant via le RRF n'auront plus de frontière. Des usagers situés dans des zones distinctes très éloignées l'une de l'autre, pourront communiquer sans problème.

Grâce au RRF les communications vidéo de groupe, individuelles et la géolocalisation des utilisateurs deviendront possibles contrairement au réseau privé actuel.

Aujourd'hui, les professionnels utilisent au moins une des solutions de communication suivantes:

1. une radio pour leurs communications opérationnelles fonctionnant sur une zone limitée,
2. un smartphone pour leurs appels et échanges de données (mails, SMS, MMS...etc.) utilisable sur l'ensemble du territoire national et international.

Le RRF offrira une solution tout en un avec un seul équipement.

Enfin, le RRF permet une innovation de taille : l'interopérabilité entre différents corps de métiers.

Le RRF permettra aux services de secours et de sécurité de davantage communiquer entre eux, en particulier dans le cadre d'opérations à grande échelle où leur coordination à tous les niveaux est nécessaire.

Ainsi, équipés d'un terminal adapté à une utilisation terrain et fonctionnant sur un réseau de nouvelle génération sécurisé et plus performant, les acteurs de la sécurité et des secours seront mieux armés pour assurer la continuité des communications et réaliser leurs missions critiques.

Dossier documentaire :

Document 1	LE RÉSEAU RADIO DU FUTUR Plan de Transformation Numérique Ministériel - Projet phare n°6 Source : MGMSIC 18 septembre 2018	Pages 1 à 2
Document 2	Extrait de la présentation du programme RRF Source : MGMSIC 2 avril 2019	Pages 3 à 4
Document 3	Le futur réseau de communications des forces de sécurité fait du bruit Publication du 11 juin 2013 https://sd-magazine.com/communications-securisees/le-futur-reseau-de-communications-des-forces-de-securite-fait-du-bruit	Pages 5 à 8
Document 4	Après des premiers essais au GIGN, la 4G débarque dans les forces d'intervention Publication du 14 juin 2018 https://lessor.org/operationnel/apres-des-essais-au-gign-la-4g-debarque-dans-les-forces-d-intervention/	Page 9
Document 5	LTE : architecture et éléments de sécurité MISC n° 068 juillet 2013 Carlos Aguilar Melchor - Léonard Dallot - Riadh Dhaou -	Pages 10 à 12
Document 6	Réseaux mobiles : exploration, outillage et évolutions MISC n° 068 juillet 2013 Loïc Habermacher	Pages 13 à 14
Document 7	Extrait du rapport d'étude RRF - Architecture multi-MCS Source : Cogisys 25 avril 2019	Pages 15 à 17
Document 8	Architecture du réseau national pour INPT IP Source : STSI ² 27 juillet 2016	Page 18

PTNM - Projet phare n°6 LE RÉSEAU RADIO DU FUTUR

Présentation du contexte et des besoins identifiés conduisant à la mise en œuvre du projet

Les réseaux radios actuels gérés par le ministère de l'Intérieur (INPT/RUBIS) reposent sur une technologie non-standard (TETRAPOL) comparable aux réseaux commerciaux de téléphonie mobile des années 90. Ils ne permettent que la transmission de courts messages textes et de la voix. Cette technologie propriétaire est annoncée par son équipementier de référence (Airbus Aerospace & Defense) comme en fin de vie en 2020 pour certaines zones, dont la plaque parisienne du réseau INPT, alors même que des jalons majeurs sont d'ores et déjà identifiés : ouverture de la ligne 15 sud du Grand Paris Express (2022), coupe du monde de Rugby (2023) et surtout les Jeux Olympiques (2024).

S'agissant de ce programme à vocation interministérielle, visant les communications opérationnelles et l'interopérabilité de l'ensemble des forces de sécurité intérieure et des unités en charge des missions de secours, trois moteurs majeurs induisent la nécessité d'une évolution : l'obsolescence technologique, l'émergence des besoins nouveaux (communications vidéo de groupe, accès haut débit au système d'information, etc.) et le rejet de plus en plus net exprimé par les utilisateurs au regard du niveau fonctionnel offert par les réseaux actuels.

Présentation des objectifs principaux et du périmètre du projet

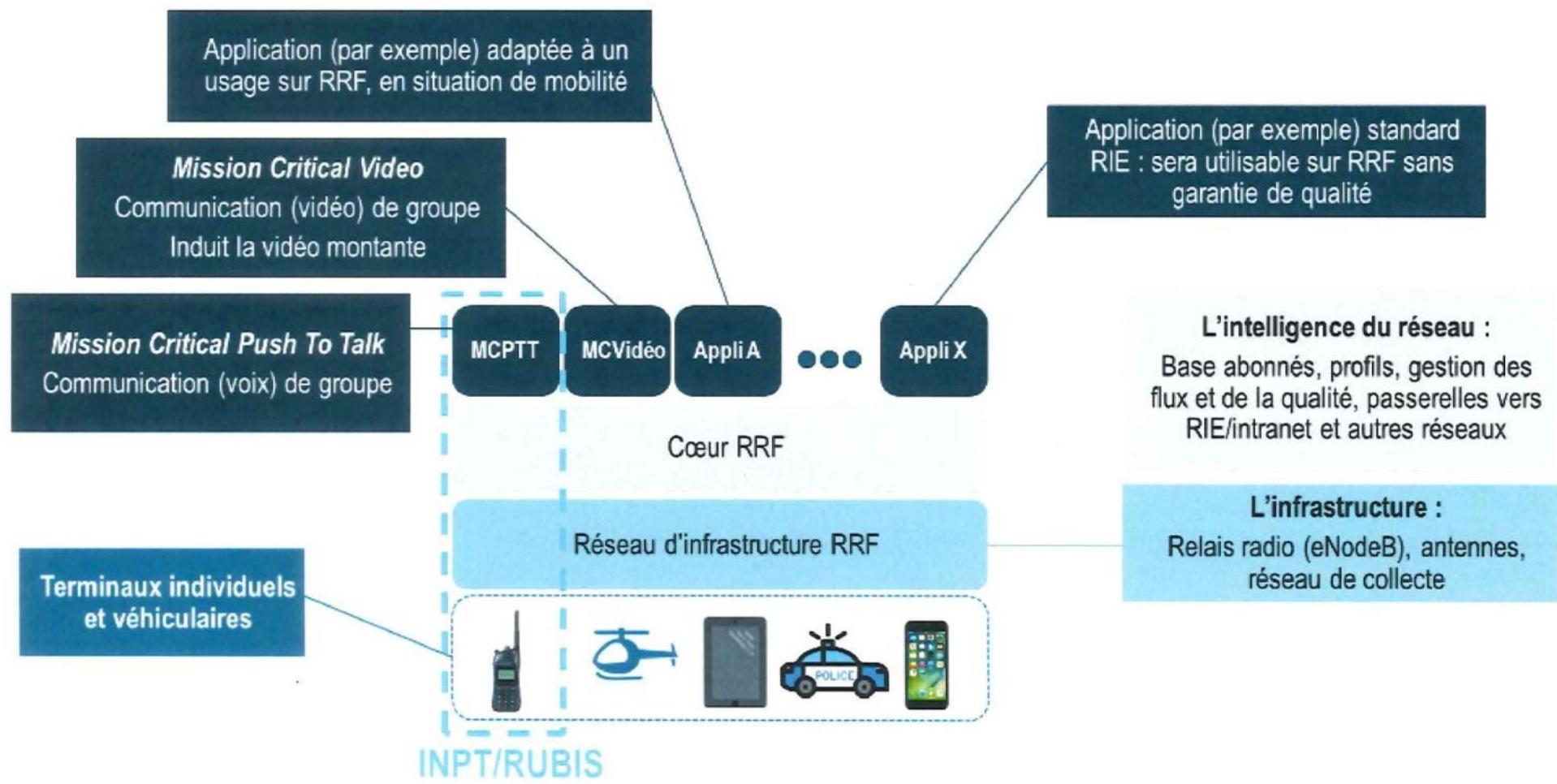
Le caractère hybride du réseau cible permet d'associer les opérateurs privés de la téléphonie mobile, sur la base d'un réseau national mutualisé, mettant en œuvre des fonctions avancées de priorité/préemption et de contrôle de qualité de service.

Des applicatifs spécifiques permettent de sécuriser les transmissions de toutes natures (sons, images, textes, accès aux SI) des agents de l'État ou d'organismes participant à des missions régaliennes.

Des dispositifs autonomes mobiles permettent de répondre à des événements critiques particuliers ou à une absence de couverture dans une zone géographique donnée (bulles tactiques véhiculaire ou portable, grande bulle tactique d'infrastructure, etc.), rendant l'ensemble fortement résilient. Le projet correspondant, PC STORM, engagé en avance de phase au sein du ministère, permet en outre de valider la technologie et d'identifier les adaptations à mettre en œuvre en termes de doctrine d'emploi.

De la mise en œuvre de la transformation ministérielle dans le domaine des moyens de radiocommunications opérationnelles

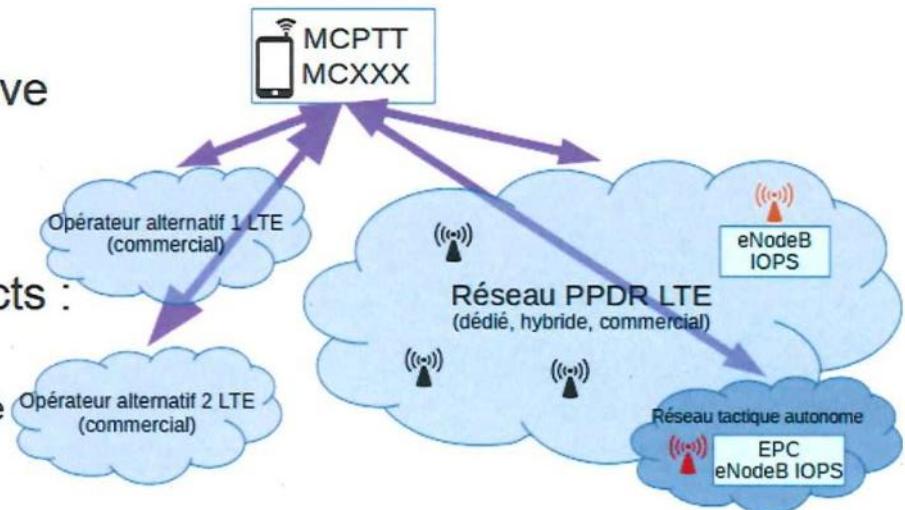
Le Réseau Radio du Futur (RRF) s'inscrit pleinement dans la feuille de route du ministère de l'Intérieur puisqu'il est clairement cité par le président de République dans son discours du 18 octobre 2017 aux forces de sécurité intérieure, en mettant en évidence la pertinence et l'opportunité de créer un réseau radio du futur à haut débit commun à la police, la gendarmerie et la sécurité civile (mais aussi au-delà : SAMU, douanes, pénitentiaires, militaires de l'opération « Sentinelle », OIV, etc.) et qui devra bénéficier d'un haut niveau de résilience en cas de crise et des meilleures technologies. En outre, la mutualisation de ce nouveau réseau a vocation à assurer l'interopérabilité des acteurs de la sécurité et du secours dans le cadre de la Police de Sécurité au Quotidien, afin de renforcer la déconcentration des politiques de sécurité, de re-dynamiser les partenariats locaux de prévention de la délinquance, et d'associer plus particulièrement les polices municipales et les agents de sécurité de transports.



MGMSIC - Extrait de la présentation du programme RRF

Programme RRF : Les fondamentaux en une planche

- Un nouveau réseau pour remplacer les réseaux Tetrapol existant (INPT et Rubis)
- Construit sur les technologies de la 4G commerciale, avec une architecture évolutive vers la 5G
- Phase 1 engagée sur les marchés PCSTORM, à compléter sur certains aspects :
 - Ouverture aux services de secours (pompiers, SAMU) et aux services de sécurité intérieure hors PN/GN (douanes, pénitentiaire, sentinelle)
 - Air-sol-air, partage de spectre (pour les bulles), gestion de parc/contrôle de conformité
 - Contrôle de la qualité de service



Un modèle de résilience assurant couverture et disponibilité en tout point du réseau, tout en limitant au maximum la vulnérabilité du réseau

1 Itinérance nationale

- Accès au **service de transport** de l'opérateur de référence
- **Multi-roaming** : possibilité de changer d'opérateur si panne / manque de couverture
- **Priorité et préemption** sur les réseaux commerciaux en cas de congestion



- Couverture 4G nationale des opérateurs (98%^(a) de la population)
- **Couverture permanente sur l'ensemble du territoire** (hors zones blanches)

Garantir la disponibilité du réseau sur les zones sensibles

2 Plaques de résilience

Couverture des sites sensibles : JO et axes structurants, Paris, petite couronne, métropoles (post JO)



Durcissement des infrastructures opérateur

Garantir la disponibilité du réseau de manière dynamique

3 Bulles tactiques véhiculaires et individuelles

Couverture réseau locale dans une zone peu couverte (e.g. zone blanche)



4 Bulles d'infrastructure

Couverture réseau locale sur une zone sinistrée, zone d'intervention large et peu couverte



(a) Obligation formulée par l'ARCEP de 98% de couverture 4G pour la population métropolitaine en 2024

Le futur réseau de communications des forces de sécurité fait du bruit

Dans un monde ultra connecté où la diffusion de l'information en temps réel est une évidence du quotidien, l'heure de repenser les systèmes de communications des forces de sécurité et de Défense est venue. Le but : répondre aux nouvelles exigences de notre société et donner les moyens aux acteurs opérationnels d'y parvenir. Plusieurs questions se posent alors. Celles de l'interopérabilité et de mobilité dans un monde décloisonné, celle du niveau de sécurité de diffusion des informations souvent sensibles ou confidentielles, celle du débit à l'heure où la 4G fait son entrée sur le marché, celles d'un réseau privé ou public, et enfin celle des budgets, toujours plus maigres... Mais qu'en est-il des besoins opérationnels des primo-intervenants ?

■ De l'avenir des réseaux de communication nationaux des primo-intervenants de la sécurité

Au début des années 1980, une rupture technologique a été opérée en France avec le choix concerté Délégation générale pour l'armement – Gendarmerie nationale du numérique pour le réseau de radiocommunication Rubis. Choix évident aujourd'hui, le numérique ayant relégué l'analogique au rang des technologies antédiluvien. Choix osé à l'époque. Ce dernier a permis le développement et le succès de la technologie TETRAPOL, le déploiement de deux réseaux nationaux Rubis pour la gendarmerie nationale et Acropol pour la Police nationale. Un succès industriel amplifié à l'international.

Si l'on peut se féliciter d'avoir été pionniers en matière technologique, force est de constater qu'il n'en est pas de même pour les choix d'architecture des réseaux des primo-intervenants français de la sécurité (polices, gendarmerie, douanes, pénitentiaire, ...). Ces réseaux sont, vingt ans après, disjoints en termes d'architecture et d'exploitation et hétérogènes technologiquement, alors que bon nombre de pays européens ou étrangers ont réussi à construire des réseaux partagés pour leurs forces de sécurité. *Témoignage de Bernard REFALO, actuel délégué général adjoint du GICAT en charge de la branche sécurité, a été directeur de programme RUBIS et manager des opérations de télécommunication de la gendarmerie au sein de la DGA de 1995 à 2003. Comment en sommes-nous arrivés là ?*

Et maintenant ?

Certes, les réseaux actuels fonctionnent et donnent satisfaction. Certes, il existe des solutions de passerelles palliant leur cloisonnement. Certes, il y a bien eu des avancées en matière de partage de réseaux qu'il faut saluer, notamment avec le réseau INPT (Infrastructure Nationale Partageable des Transmissions), mais au prix de beaucoup d'énergie, de frustrations, d'efforts financiers et avec des élongations calendaires bien trop importantes. Dans le contexte actuel marqué par la réduction des budgets publics d'investissement, la rapidité des évolutions technologiques et normatives, les demandes de nouveaux services de la part des utilisateurs opérationnels, un niveau d'exigence de services accru de nos concitoyens, ce serait non plus une erreur mais une faute de ne pas se pencher en temps et en heure sur l'étude et la définition des futurs réseaux.

...

Il est encore temps

Les choix qui seront opérés pour les futurs réseaux seront engageants pour des décennies. Les enjeux sont importants pour ne pas dire énormes. Les idées ne manquent pas, les solutions non plus, elles ont même tendance à foisonner.

Les réseaux actuels peuvent encore fonctionner quelques années.

La France a été un pionnier des technologies de radiocommunication numérique dans les années 90, avec le développement de TETRAPOL et la création de deux réseaux nationaux, Rubis et Acropol, destinés à sa gendarmerie nationale et à ses forces de police.

Le défi actuel est de définir et de concevoir le futur réseau de communication national des principaux acteurs de la sécurité. Le choix de son architecture, ses performances et ses technologies en font un projet complexe. Il présente des défis opérationnels et industriels considérables qui nécessitent une attention particulière.

Il est hautement préférable que ce futur réseau soit partagé par toutes les forces de sécurité, voire par d'autres utilisateurs, en raison de la réduction des budgets de l'État, de la nécessité de l'interopérabilité et de la rareté des points hauts et des fréquences rares. Ce concept de réseau exige que tout le monde soit membre et adopte une approche commune. Des références européennes et internationales concrètes montrent que la France peut atteindre cet objectif. Le GICAT est prêt à apporter son soutien pour en faire une réalité.

■ Les technologies de 4e génération de la téléphonie mobile comme solution d'avenir pour l'évolution des réseaux PMR

Les crises majeures, auxquelles les services du ministère de l'Intérieur ont été confrontés ces dernières années, confortent la pertinence des choix technologiques retenus, tout particulièrement dans le cadre des systèmes de radiocommunication mobile. Forts de cette expérience dans la gestion de crises et des besoins nouveaux des utilisateurs, les spécifications techniques d'un futur réseau de télécommunication au profit des services de l'État sont clairement définies. Ainsi, elles se doivent d'être prospectives et innovantes afin de répondre aux attendus technico-fonctionnels, tout en recherchant à optimiser au mieux le modèle économique de la solution cible.

Explication du général Bernard Pappalardo, chef du ST(SI)2, Service des technologies et des systèmes d'information de la sécurité intérieure du ministère de l'Intérieur.

Des réseaux adaptés

Les récentes catastrophes naturelles (Klaus 2009, Xynthia 2010, épisodes neigeux) tout comme les catastrophes technologiques (accidents ferroviaires, aériens, industriels, incendies, etc.), voire la menace terroriste, ont conforté les services d'urgence et de sécurité publique dans leurs choix technologiques. Ces services régaliens soulignent la nécessité de préserver des systèmes de communication propriétaires ou maîtrisés, seuls garants de la résilience et de la disponibilité indispensables à la bonne exécution des missions en toutes circonstances.

À ce titre, lors des tempêtes de 2009 et 2010, les réseaux d'infrastructure des opérateurs de téléphonie mobile se sont avérés dans l'incapacité de garantir la fiabilité et la qualité des services offerts aux utilisateurs. Ceci en raison des dégradations matérielles engendrées par des conditions climatiques exceptionnelles (destruction de pylônes, dégradation des aériens, défaut d'alimentation en énergie, ...), mais aussi au regard d'une saturation non maîtrisable du réseau (mouvement de panique, augmentation des appels d'urgence, concentration d'abonnés, ...). En cela, seuls les réseaux de radiocommunication privés (PMR) peuvent à ce jour offrir la garantie de service et les fonctionnalités spécifiques attendues (communication de groupe, appel de détresse, mode direct, ...) par les services d'urgence et de sécurité publique dans la gestion de crise.

Disposant de telles infrastructures pour couvrir l'ensemble du territoire national (RUBIS pour la Gendarmerie nationale et INPT pour la Police nationale, les pompiers, la sécurité civile et les SAMU), le ministère de l'Intérieur possède des systèmes de communication actuellement adaptés à ses besoins opérationnels. Parallèlement, pour la Gendarmerie nationale, la disponibilité d'une chaîne "SIC" pour le soutien opérationnel de proximité permet de faire face sans délais aux incidents ou dégâts matériels rencontrés grâce à une capacité d'intervention sur site renforcée et à la mise en œuvre immédiate de moyens complémentaires de circonstance.

Pour autant, même si ces choix technologiques et stratégiques satisfont aux besoins critiques de communication, la mise en adéquation des moyens matériels aux attendus opérationnels relève d'une analyse pragmatique et constante en vue d'identifier les axes d'amélioration.

Des événements riches d'enseignement

Ainsi, les grands événements récents (65e anniversaire du débarquement en 2009, le G8 et le G20 en 2011), par la mise en œuvre de systèmes d'information complémentaires, l'augmentation des ressources radio et l'optimisation de la couverture des réseaux, posent les bases d'une réflexion technique sur l'évolution des réseaux de communication ainsi que sur les nouveaux services à offrir à moyen terme aux utilisateurs.

À ce titre, les débits offerts par les réseaux de radiocommunication du ministère ne permettent pas de répondre pleinement à des besoins en transmission de données, en constante augmentation, notamment lors de crises majeures ou de grands événements. Pour autant, les demandes

d'informations enrichies pour les salles de commandement comme pour les autorités d'emploi (géolocalisation, remontées vidéo, intégration de nouveaux systèmes d'information, etc.) ou l'augmentation des capteurs d'informations sur le terrain (caméras autonomes, robots démineurs, drones de surveillance, etc.) rendent nécessaire la mise en œuvre de services haut débit de circonstance.

En outre, l'interopérabilité justifiée par la diversité et l'hétérogénéité des acteurs (services de secours, services de sécurité, forces armées, opérateurs d'importance vitale, etc.) est désormais un élément-clé de la gestion des réseaux. Car, étant impliqués dans la gestion d'une crise ou d'un événement majeur, ils invitent à s'appuyer, pour l'avenir, sur des solutions technologiques standardisées et à mutualiser les infrastructures pour satisfaire aux besoins fonctionnels tout en rationalisant les coûts et en optimisant les investissements.

...

Disposer d'un système modulaire et projetable

Reposant sur une combinaison opportuniste des moyens de communication aériens, terrestres et satellitaires existant afin de garantir la disponibilité du réseau, la configuration retenue pour la réalisation d'un premier prototype permet de disposer d'un système modulaire et projetable sans délais. Pour autant, la complexité de la solution se trouve tout autant dans les enjeux technologiques que dans les réponses techniques et matérielles à apporter pour répondre aux exigences de mobilité (poids, encombrement, mise en œuvre, etc.) et aux contraintes énergétiques.

L'architecture fonctionnelle du système doit permettre aux stations de base aéroportées d'établir un cœur de réseau d'opportunité tout en fédérant l'infrastructure terrestre présente sous la couverture radioélectrique. Parallèlement, le rôle de passerelles joué par les stations terrestres mobiles doit conduire à garantir l'emploi des moyens de communication à disposition des services engagés sur des catastrophes (TETRAPOL, TETRA, etc.) afin de répondre aux enjeux d'interopérabilité évoqués précédemment.

...

■ Le haut débit cherche sa fréquence !

À l'heure où le ministère de l'Intérieur prévoit pour juillet 2013 une réforme de l'administration centrale, jugée par ailleurs « ambitieuse » place Beauvau, les services de communication et systèmes d'informations ne sont pas en reste. La note de Manuel Valls prévoit notamment la création d'une équipe dédiée placée sous l'autorité directe du secrétaire général. Chargée de la « gouvernance stratégique » dans le domaine des systèmes d'information, elle aura pour fonction l'« arbitrage des évolutions techniques structurantes nécessaires » et la « validation du lancement des projets », dont le chantier du nouveau réseau des télécommunications des forces de sécurité pourrait bien faire partie. Un chantier destiné à améliorer le travail des forces de sécurité... À la problématique des objectifs opérationnels du nouveau réseau, tous s'accordent à dire qu'il faut offrir un réseau capable de traiter de la voix, des données images, de la vidéo ou encore d'accéder à des bases de données à distance ou à Internet. En somme, un réseau en phase avec son temps.

Pour cela, il faut donc offrir de la bande passante supplémentaire pour les flux de données et donc du haut débit. Consortium autour du LTE

Aujourd'hui, la norme LTE (Long-Term Evolution) est la technologie choisie par les opérateurs commerciaux pour augmenter la capacité de leurs réseaux et répondre ainsi aux nouveaux usages applicatifs, notamment à base de vidéo, très consommateurs de bande passante. « L'utilisation de plus en plus importante des systèmes d'information au sein de la sécurité et de la défense fait du LTE la technologie candidate pour répondre aux besoins opérationnels de transmission haut-débit », souligne Thales, rejoints par Guy Mans, responsable commercial Secteur public de Motorola Solutions, pour qui « la future technologie radio doit être et sera le LTE ». Le LTE fait donc l'unanimité et sert parallèlement l'implication sans faille de Thales dans le continuum sécurité/défense. En effet, le groupe précise « que l'étude de la norme LTE, technologie civile de pointe, s'inscrit parfaitement dans la politique du continuum sécurité/défense menée par le groupe. » Groupe retenu par ailleurs en mars dernier par la Direction générale de l'armement (DGA) pour conduire une étude technico-opérationnelle (ETO) portant sur l'Analyse de la norme LTE et son exploitation au sein des forces Armées (ALTEA). « Une étude qui devra permettre de mettre en évidence les capacités susceptibles d'être apportées par cette technologie lors d'opérations extérieures et sur le territoire national et ce, en collaboration avec les forces de sécurité », souligne Thales.

Une solution LTE, appropriée au milieu de la sécurité publique et de la défense, qui devra être adaptée

à un environnement où les contraintes d'utilisation et les performances à atteindre sont plus exigeantes. Aussi, cette solution devra être interopérable, une réponse essentielle à la mobilité dont ont aujourd'hui besoin les acteurs opérationnels. Cela implique notamment des outils plus faciles à transporter, à manier, autonomes et légers. Plus proches d'un smartphone que d'un PR4G donc... « Le réseau des policiers de demain et non pas du futur », précise Sébastien Sabatier, directeur Stratégie et Marketing au Service sécurité nationale C4I et PMR de Thales « doit permettre aux policiers et aux gendarmes, mais aussi aux sapeurs-pompiers ou encore aux agents des opérateurs d'intérêts vitaux, de pouvoir se connecter et échanger ensemble. Le système actuel, patrimonial, montre aujourd'hui ses limites sur ce sujet. Beaucoup d'intervenants ne sont pas connectés et connectables, engendrant les problèmes que l'on peut facilement imaginer. Aussi, le nouveau réseau doit être résilient, s'adapter aux changements, aux évolutions, il doit être un réseau crypté, étanche et non pénétrable, mais partagé », ajoute-t-il. Et Guy Mans de poursuivre, « partagé oui, indépendant des opérateurs publics oui, mais opéré ». Un opérateur qui pourrait être un consortium de plusieurs industriels, de plusieurs agences, d'opérateurs civils de confiance... Un réseau en somme fédérateur mais pas propriétaire qui trouverait sa place dans un environnement de standardisation avec des moyens et des technologies au goût du jour qui permettrait, on peut l'imaginer, la diffusion rapide de vidéos entre les "hommes de terrain" et le poste de commandement, la télémédecine pour les pompiers, ou encore une meilleure réactivité dans la conduite des enquêtes grâce à des accès à distance aux bases de données sécurisées...

Le déploiement du réseau LTE est aujourd'hui acquis par les États-Unis, qui viennent d'annoncer un budget de près de 10 milliards de dollars consacré pour les 10 prochaines années à la construction de ce réseau opéré par FirstNet. Thales Communications, Inc. société 100 % américaine du groupe Thales, participe notamment au programme Public Safety Communications Research (PSCR) qui vise à promouvoir l'interopérabilité des systèmes de communication de sécurité publique à l'échelle des États-Unis. « Cet essai d'interopérabilité dans le cadre du PSCR est un jalon important pour notre solution LTE de sécurité publique en réponse aux besoins spécifiques de nos clients », a ainsi déclaré Michael Sheehan, PDG de Thales Communications. Mené en proche collaboration avec des partenaires du secteur privé et du domaine de la sécurité publique, le programme PSCR met à la disposition des fabricants, opérateurs et agences de sécurité publique un banc d'essais de démonstration permettant d'évaluer les équipements et logiciels de communication haut débit en vue du déploiement d'un futur réseau de communication dédié aux services d'urgence dans la bande passante unique des 700 MHz. Bande de fréquence aujourd'hui à l'origine des discordances dans le traitement du dossier des futurs réseaux de communication des forces de sécurité de notre pays.

700 ou 400, les chiffres de la discorde

Question agnostique selon Guy Mans pour qui les deux fréquences présentent respectivement des avantages et des inconvénients. Du côté de Thales, la réponse est identique « toutes les gammes sont intéressantes. Reste que la réponse à cette question ne doit pas être imposée par l'industriel mais elle se trouve dans l'écosystème », ajoute Richard Kalczuga, directeur Comptes clés chez Thales. Un écosystème qui est en train de se former autour du 700 MHz avec les États-Unis qui semblent s'orienter vers ce choix, suivis par le Canada et l'Asie Pacifique. En Europe, la Conférence européenne des administrations des postes et télécommunications (CEPT) et la Commission européenne réfléchissent à l'établissement de nouvelles normes pour les télécommunications destinées aux forces de sécurité, et notamment à l'introduction de cette nouvelle plage à 700 MHz.

Gilles Brégant, directeur général de l'ANFR, soulignait déjà lors de ses voeux de début d'année : « La France n'est pas une île, et elle devra agir de concert avec ses voisins d'Europe occidentale ... ». Pour ce qui est des objectifs opérationnels du nouveau réseau, tous s'accordent à dire qu'il faut un système capable de traiter les voix, les données image, la vidéo et l'accès aux bases de données distantes et à Internet. Pour cela, il a besoin de plus de bande passante pour le flux de données et donc du haut débit.

Actuellement, les opérateurs commerciaux choisissent la technologie LTE (Long-Term Evolution) pour augmenter la capacité de leur réseau et gérer de nouvelles applications. Des fabricants tels que Motorola Solutions et Thales sont unanimes quant à l'utilisation de la technologie LTE.

La solution LTE doit être interopérable, résiliente, cryptée, scellée et impénétrable, partagée, indépendante des opérateurs publics et exploitée. Réseau commun non exclusif permettant la distribution rapide de vidéos entre « agents de terrain » et centres de contrôle, télémédecine pour les services d'incendie, réponse plus rapide pour les enquêtes par accès à distance à des bases de données sécurisées, etc.

Après des premiers essais au GIGN, la 4G débarque dans les forces d'intervention

Attendue depuis longtemps, la 4G va enfin débarquer dans les forces d'intervention françaises de la sécurité intérieure (BRI, GIGN, et Raid). Le ministère de l'Intérieur vient de notifier, ce mercredi 6 juin, la première attribution d'un lot d'un marché public très convoité dans les télécommunications, le [marché PC-Storm](#). La société française [Streamwide](#), spécialisée dans les logiciels de communication pour les opérateurs télémédias, va fournir une application de messagerie sécurisée permettant de géolocaliser, d'échanger des données, des flux vidéos, ou encore de consulter un annuaire enrichi constamment actualisé, le tout de manière hautement sécurisée.

Des fonctionnalités banales depuis la généralisation des smartphones, avec par exemple la messagerie grand public WhatsApp, mais dont les forces du ministère de l'Intérieur étaient privées, la faute à des réseaux radios d'ancienne génération. *"PC-Storm sera un outil complémentaire"*, corrige un membre du GIGN à *L'Essor*. *Mais à terme il deviendra indispensable*, avec la montée en puissance du très haut-débit mobile.

Un besoin révélé après 2015

Concrètement, la 4G va permettre à des forces d'intervention de transmettre des vidéos après une opération, d'envoyer des éléments de preuve au commandement ou de donner des premiers éléments d'ambiance. Le besoin d'une telle solution technique s'est révélé au grand jour en janvier 2015 lors de la traque des frères Kouachi à Dammartin-en-Goële (Seine-et-Marne), après l'attentat contre Charlie-Hebdo. Dans la campagne, le réseau téléphonique se révèle vite saturé. Le marché PC-Storm doit combler cette faille grâce à la mise en place de bulles tactiques radios pouvant pallier les défaillances des infrastructures des opérateurs.

Ce nouveau équipement ne devrait arriver qu'au début de l'année prochaine dans les forces d'intervention. Pourtant, il est déjà bien connu au GIGN. Le groupe teste depuis environ deux ans une autre version de l'application de Streamwide, antérieure à celle qui sera déployée. Elle a ainsi été expérimentée durant l'Euro de foot 2016, des matchs du championnat de handball à Nantes en 2017 ou le Tour de France. *"Cela nous a permis de constater la réelle plus-value de ce type d'outil"*, explique ce membre du GIGN. Le groupe a d'ores et déjà testé une centaine de fonctionnalités qui vont lui permettre de poursuivre sa transformation numérique – par exemple une check-list envoyée et validée avant un départ.

Faciliter le travail en commun des forces d'intervention

Demain, la mise en place de la nouvelle application devrait faciliter le travail en commun des différentes forces équipées (BRI, GIGN, Raid) de l'Intérieur mais aussi de la défense avec les commandos marine. Une innovation regardée de très près au ministère de l'Intérieur: ce marché constitue la première pierre vers le réseau radio du futur qui devra offrir aux policiers, pompiers et gendarmes, un réseau en 4G, résilient et sécurisé avec des applications métiers multimédia d'ici les Jeux Olympiques 2024. La Gendarmerie, précurseur avec le réseau radio Rubis à la fin des années 1980, aura un rôle central dans ce projet, avec le centre de données de PC-Storm qui sera hébergé à Rosny-sous-Bois. Une plateforme des *"communications critiques"* destinée à devenir une vitrine du savoir-faire français, une des premières solutions à être mises en oeuvre dans les services de sécurité dans le monde.

Gabriel Thierry

LTE : architecture et éléments de sécurité

LTE (de l'anglais Long Term Evolution) est la norme de téléphonie mobile la plus récente et performante utilisée en pratique. En France, le déploiement a commencé en 2012 et devrait pour certains opérateurs couvrir de nombreuses grandes villes, Paris inclus, vers la fin 2013. Au niveau de la sécurité, LTE apporte des grands chamboulements que nous présentons dans cet article : nouvelle architecture de sécurité, dérivations de clés en cascade pour permettre des handovers (i.e. le passage d'une antenne à un autre) rapides et sécurisés, utilisation d'algorithmes de chiffrement dernière génération comme AES, etc.

1. Architecture de sécurité et objectifs

L'architecture du réseau de l'opérateur dans LTE suit le modèle SAE (System Architecture Evolution) du 3GPP (3rd Generation Partnership Project), organisme de standardisation phare dans le monde du mobile.

1.1. Le modèle SAE

LTE propose une évolution des réseaux 3G. Parmi elles, l'abandon du circuit pour la voix même dans le cœur du réseau et le passage au tout IP ont un impact majeur sur l'architecture du réseau.

Toutefois, le passage des technologies 3G à LTE doivent éviter les écueils communs comme la complexité d'une nouvelle architecture et le coût en infrastructure. Le maître-mot est donc la simplification de l'architecture.

Un réseau LTE est constitué de deux grandes parties : d'une part le réseau d'accès radio dénommé e-UTRAN (evolved Universal mobile telecommunications system Terrestrial Radio Access Network) et d'autre part le cœur de réseau appelé EPC (Evolved Packet Core). La figure 1 présente une vision d'ensemble simplifiée de l'architecture LTE, bien moins complexe que l'architecture des réseaux 3G précédents.

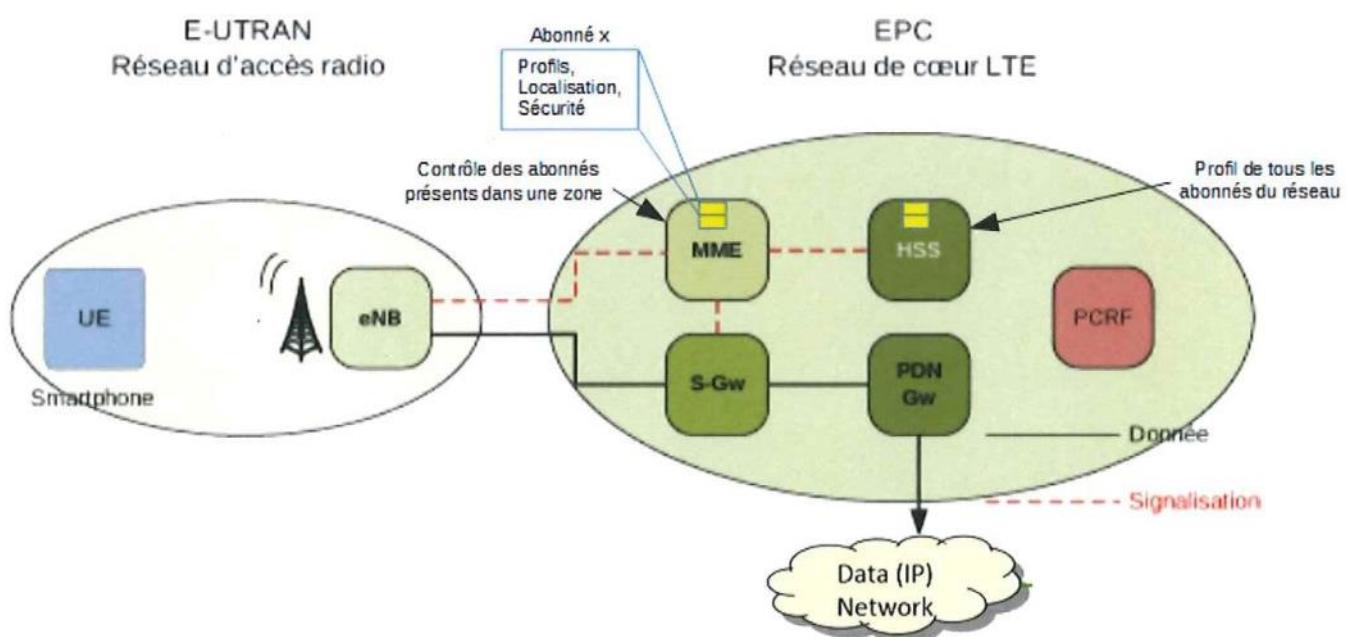


Figure 1 : Architecture de réseau LTE

Le rôle de l'e-UTRAN est de permettre aux équipements utilisateur (UE) d'accéder au réseau LTE. Les différentes fonctionnalités ont toutes été réunies dans un seul type d'équipement, l'eNode B (eNB). Chaque eNB s'occupe de la gestion radio d'une cellule comprenant les équipements de réception et d'émission mais aussi de toute la partie allocation de ressources sur l'interface air via la création des différents bearers de chaque utilisateur et l'affectation des ressources airs à chacun d'eux. Les eNB sont interconnectés entre eux généralement en fibre optique et avec le cœur de réseau. Ces communications utilisent IP.

Parmi les rôles de l'EPC, on trouve la gestion de l'accès des utilisateurs au réseau, la gestion de la mobilité des utilisateurs, la facturation, la mise en relation des utilisateurs entre eux, la mise à

disposition d'un grand nombre de services, ou encore l'accès à d'autres réseaux ou technologies (comme Internet). Pour mettre tout cela en place, LTE a besoin d'entités spécialisées dont les principales sont représentées sur la figure 1.

Comme dans beaucoup de technologies de l'ITU (Union Internationale des Télécommunications), la partie signalisation (appelée plan de contrôle) est séparée logiquement de la partie données (appelée plan utilisateur).

Dans le plan utilisateur, la Serving Gateway (S-GW) est en charge des communications entre les utilisateurs du même réseau LTE tandis que la Packet Data Network Gateway (PDN-GW ou P-GW) est une passerelle vers le monde extérieur : il est le premier routeur IP que rencontrent les flux d'un utilisateur et permet l'interconnexion avec d'autres réseaux et technologies, notamment l'Internet.

Les éléments du plan de contrôle sont au cœur de la sécurité dans LTE. La MME (Mobility Management Entity) est l'entité en charge de la mobilité des utilisateurs LTE mais aussi de leur authentification. Pour ce faire, elle a recours au Home Subscriber Server (HSS) qui est la base de données de tous les utilisateurs du réseau LTE, contenant leur profil avec notamment leurs informations de sécurité, leurs droits d'accès ou encore leurs crédits. Enfin, la Policy and Charging Rules Function (PCRF) est le cœur du système LTE quant à l'accès aux ressources.

Pour donner un meilleur aperçu des plans utilisateur et de contrôle, voici une description rapide des piles protocolaires, interfaces, et rôles des principaux protocoles concernés.

- Plan utilisateur

Les protocoles de l'interface radio LTE-Ue comme PDPC (Packet Data Convergence Protocol), RLC (Radio Link Control), MAC (Medium Access Control) ainsi que la couche physique sont communs aux plans utilisateur et de contrôle. PDPC est responsable de la transmission ordonnée des paquets de plus haut niveau, ainsi que pour le chiffrement des fonctions d'intégrité. RLC est en charge du format de trame et de délimitation tandis que MAC gère l'accès aux ressources radio. Dans l'EPC, les données du plan d'utilisateur sont transmises via le protocole GTP-U (GPRS Tunneling Protocol User plane) sur les protocoles UDP/IP.

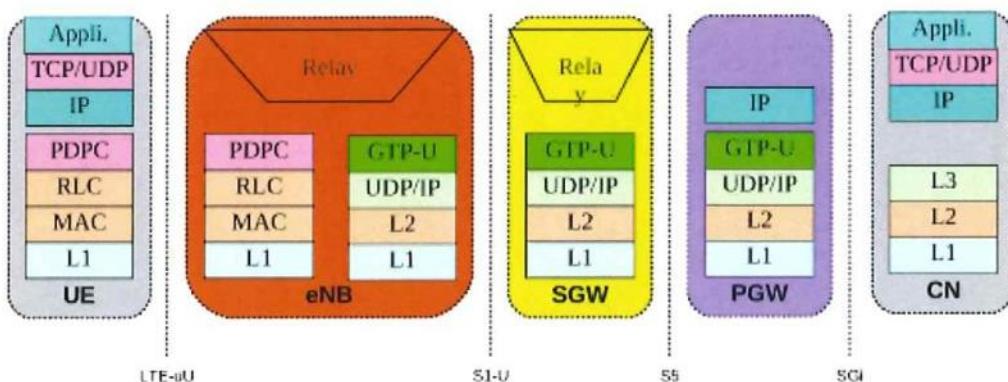


Figure 2a : Plan utilisateur

- Plan de contrôle

Pour le plan de contrôle, il y a une dissociation entre la gestion de la ressource radio qui est effectuée directement par l'eNB et la gestion de la présence et de l'AAA de l'UE qui est orchestrée par le MME. Le MME est l'entité de cœur du plan de contrôle. Dans le cœur de réseau, la gestion est assurée par le protocole GTP-C (GPRS Tunnelling Protocol for Control Plane). L'interaction entre le cœur de réseau et le réseau d'accès est effectuée par l'intermédiaire des protocoles de l'S1-AP (S1 Application Protocol). SCTP (Stream Control Transmission Protocol) assure la bonne réception des messages de ce protocole. S1-AP est responsable en particulier du transfert de la signalisation et offre également la possibilité de transmission transparente des messages NAS (Non-Access Stratum). Les messages NAS permettent une signalisation directe entre le MME et l'UE. En particulier, ce protocole gère certaines fonctions pour la mobilité des UE ainsi que des fonctions de gestion et de sécurité capitales. Sur l'interface air, LTE-Uu, le protocole principal pour le plan de contrôle est RRC (Radio Resource Control). Il a un rôle important dans la gestion de la mobilité.

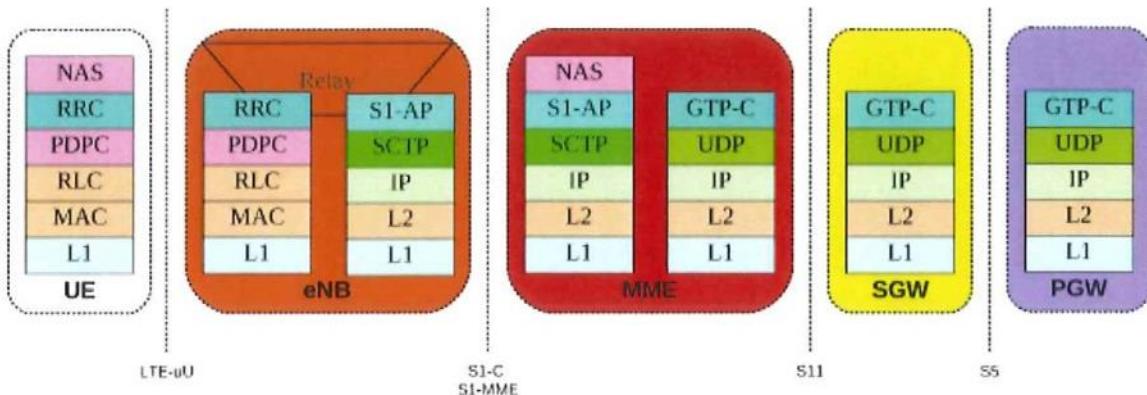


Figure 2b : Plan de contrôle

1.2. Objectifs de sécurité

Pour bien comprendre les apports au niveau des objectifs de sécurité dans LTE, nous présentons une évolution de ceux-ci depuis GSM jusqu'à LTE en passant par UMTS. Dans GSM, on peut (de façon relativement arbitraire) mettre en avant trois objectifs de sécurité :

- authentification de l'abonné avant de lui donner accès au service ;
- secret des identités des utilisateurs et terminaux pour limiter la traçabilité ;
- confidentialité des communications entre le portable et l'antenne relais (optionnel).

Bien que la confidentialité des communications entre les portables et les antennes relais ait été optionnelle dans la norme GSM, dans la plupart des pays industrialisés, cette option était activée. Les mécanismes mis en place pour atteindre ces objectifs étaient parfois limités, mais nous ne reviendrons pas sur la fragilité de ceux-ci ni sur les nombreuses attaques portant atteinte à ces objectifs de sécurité (voir, par exemple, [NP09] [Spaar09] ou [BBK03]).

La norme UMTS a introduit deux autres objectifs qui nous paraissent primordiaux. Premièrement, l'authentification du réseau auprès des cartes USIM devient obligatoire dans les échanges nécessaires à l'authentification. Cet objectif a été introduit pour éviter des attaques de deux types. Premièrement, les attaques par fausse station de base, où typiquement des choix cryptographiques faibles étaient proposés aux terminaux. Deuxièmement, les attaques de type oracle, où des échanges d'authentification étaient simulés pour forcer la carte USIM à répondre à des faux défis et ces réponses étaient utilisées pour extraire les secrets contenus dans la carte. Le deuxième objectif introduit par la norme UMTS est la sécurisation d'une partie de la signalisation (dite RRC et correspondant à la signalisation des antennes radio) par des mécanismes d'intégrité et anti-rejet.

Au niveau de LTE, le document de norme [TS 33.401] reprend les objectifs de sécurité de GSM et UMTS, et en ajoute d'autres parmi lesquels les suivants nous paraissent particulièrement importants :

- protection de l'intégrité et contre le rejet pour l'ensemble de la signalisation ;
- gestion allégée des échanges cryptographiques dans les handovers (changements d'antenne) ;
- sécurisation de l'architecture en cas de compromission d'une antenne.

Quand un appareil se connecte à un réseau sous la norme LTE, une série de procédures visant à sécuriser les échanges se met en place dès la première tentative de connexion. Tout commence par un envoi d'une identité temporaire suivi par une authentification et un échange de clés. Ensuite, il y a une négociation des algorithmes de sécurité par la mise en place d'associations, et un système de dérivation de clés. À la fin du processus, signalisation et données sont sécurisées, et l'UE peut commencer à communiquer à travers le cœur du réseau de l'opérateur.

...

Conclusion

LTE utilise des algorithmes standards en cryptographie, porte le chiffrement et le contrôle d'intégrité bien au-delà de ce qu'on avait dans les technologies précédentes, et utilise un système de dérivation de clés permettant de donner des bonnes garanties de sécurité en cas de compromission de différents éléments du réseau. Peut-on par conséquent espérer que LTE soit beaucoup plus sûr que les technologies précédentes ? Ce n'est pas si simple. En effet, il ne faut pas oublier que si un consortium comme le 3GPP a fait un grand effort en sécurité, c'est parce qu'il voit que les menaces ont fortement grandi.

Réseaux mobiles : exploration, outillage et évolutions

L'objectif de cet article est de présenter les différents points d'entrée des réseaux mobiles ainsi que les outils d'exploration disponibles en open source. Il couvrira toutes les générations de réseaux mobiles avec un focus particulier sur les réseaux de 4e génération (LTE/EPC).

1. Introduction

Les réseaux mobiles sont devenus ces dernières années un champ d'investigation privilégié pour hackers en quête d'un nouveau terrain de jeu loin de la recherche de vulnérabilités kernel Windows ou de l'exploitation de navigateur web. Le sujet ne manque en effet pas d'attraits : de nombreux équipements très interconnectés, des piles protocolaires complexes, un empilement de technologies à des fins de rétrocompatibilité et un accès depuis la voie radio font des réseaux mobiles un terrain d'exploration riche et varié.

L'accès à l'information et une montée en compétence rapide sont cependant rendus difficiles par cette complexité. Les architectures et protocoles sont décrits dans de très nombreuses normes de plusieurs centaines de pages, les acronymes sont indénombrables, les outils souvent parcellaires et en constante évolution, et l'accès aux équipements télécoms limité si l'on ne travaille pas pour un opérateur ou un constructeur... Le but de cet article est de guider le lecteur dans cette masse d'information, de présenter les différents points d'entrée pour un attaquant et de faire un rapide état de l'art des outils disponibles et des évolutions à venir.

2. Par où commencer

2.1. Prérequis

L'architecture d'un réseau LTE/EPC (Long Term Evolution/Evolved Packet Core) ainsi que les évolutions des interfaces et des propriétés de sécurité par rapport aux réseaux UMTS sont présentées dans le premier article réseau mobile de ce dossier.

2.2. Architecture et points d'entrée

Les normes pour toutes les générations de réseaux mobiles (2G, 3G, 4G) sont sous la responsabilité des groupes de travail du « 3rd Generation Partnership Project » (3GPP). Ces documents de références en constante évolution sont disponibles en accès libre et gratuit sur leur site web . Une référence condensée et moins indigeste est disponible sous forme de livre : à privilégier pour une première approche.

Pour se retrouver dans cette masse de documentation, une première précision de terminologie est utile. Les spécifications dites de « stage 1 » sont des spécifications de services, les spécifications de « stage 2 », les spécifications d'architectures implémentant ces services et les spécifications de « stage 3 » décrivent l'implémentation technique (format de messages bit par bit, piles protocolaires, ...) de ces architectures.

Quand il s'agit d'implémenter des outils de fuzzing ou de manipulation de paquet, on se tournera donc plutôt vers des spécifications de « stage 3 », alors que pour une vue globale d'architecture, les spécifications de « stage 2 » sont tout indiquées. Les spécifications de « stage 1 » sont peu techniques et décrivent principalement des services, mais permettent d'avoir de bonnes indications sur les futures évolutions des réseaux mobiles et peuvent être intéressantes pour identifier des axes de recherche.

La spécification qui décrit l'architecture d'un cœur de réseau 4G (de stage 2 donc) est la Technical Specification (TS) 23.401. L'accès radio est décrit dans la TS 36.300. L'architecture de sécurité est quant à elle décrite dans la TS 33.401 .

Pour identifier les principaux points d'entrée pour un attaquant, servons-nous de l'architecture de référence d'un réseau LTE sans roaming de la TS 23.401, adaptée en figure 1 ci-après. Les attaques peuvent être lancées :

- depuis un terminal ;
- depuis l'interface radio ;
- depuis un site avec un accès physique à une antenne (eNodeB) ;
- depuis le réseau de collecte (backhaul) reliant le réseau d'accès radio aux équipements de cœur de réseau ;

- depuis Internet ;
- depuis les réseaux d'administration des différents équipements ;
- depuis les interfaces de roaming ;
- directement dans le cœur de réseau.

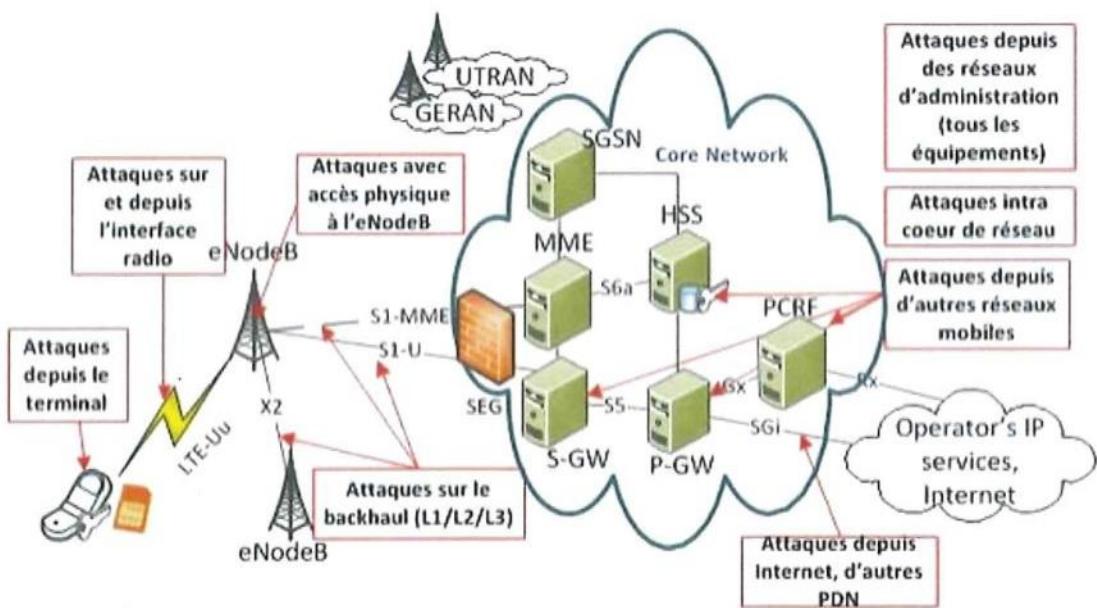


Figure 1 : Architecture d'un réseau LTE/EPC et points d'entrée pour un attaquant

Il est important de noter qu'à ce jour, aucune attaque pratique n'existe contre les algorithmes d'authentification, de chiffrement et de contrôle d'intégrité pour les réseaux 3G et LTE.

...

4.3. Rôle des opérateurs

Comme vu précédemment, de nombreuses tâches restent sous la responsabilité de l'opérateur et dépassent le périmètre des standards :

- déploiement et maintien opérationnel d'un réseau mobile dans une configuration sûre en appliquant les standards ;
- ingénierie IP et protection de son cœur de réseau pour limiter les attaques et réduire leurs impacts (déploiement de passerelles IPsec, pare-feu, DMZ, protocoles de management d'équipements sûrs, traçage et identification des attaquants, haute disponibilité, ...);
- évaluation des équipements qu'il intègre dans son réseau d'un point de vue sécurité (penetration testing, fuzzing, ...);
- **
- contribution au maintien et à l'évolution des standards de sécurité dans les groupes concernés (3GPP, IETF, GSMA).

Conclusion

Les réseaux mobiles de 3e et 4e générations en incluant « de base » des aspects sécurité dans leurs standards d'architecture et de services permettent un niveau de sécurité et de protection élevé par défaut, tant des utilisateurs et de leurs données que des infrastructures opérateurs. Ils ne sont cependant pas suffisants seuls. La complexité de ces réseaux, la variété des protocoles utilisés ainsi que le nombre de points d'entrée potentiels imposent chez les opérateurs la mise en place et le respect de processus de configuration, de validation et de maintien opérationnel de la sécurité.

Les outils d'exploration et d'attaque pour ces protocoles et interfaces deviennent de plus en plus accessibles. Pour la radio, bien que les outils soient aujourd'hui toujours principalement orientés 2G, ils évoluent rapidement et d'autres technologies pourraient être bientôt accessibles. Enfin, l'écosystème intègre en permanence de nouvelles interfaces qui n'ont de limites que l'imagination des groupes définissant les besoins de services et pour lesquels des standards de sécurité solides devront être créés et maintenus.

Extrait du rapport d'étude RRF - Architecture multi-MCS

Dans le cadre de travaux préparatoires à l'appel d'offres pour la fourniture du réseau RRF, Cogisys a été chargé d'une étude portant sur le chantier « Gestion des interfaces, architectures et applications ».

Le réseau RRF s'appuiera sur l'architecture Mission Critical définie par 3GPP « 3rd Generation Partnership Project » à partir de la release 13 et poursuivie en release 14 et 15. Cette architecture permet de fournir des services Mission Critical (MCPTT, MC Data, MC Video) via un réseau mobile LTE, aux différentes communautés utilisatrices.

Le nombre d'utilisateurs est estimé à 734 000.

Architecture générique d'un système MC

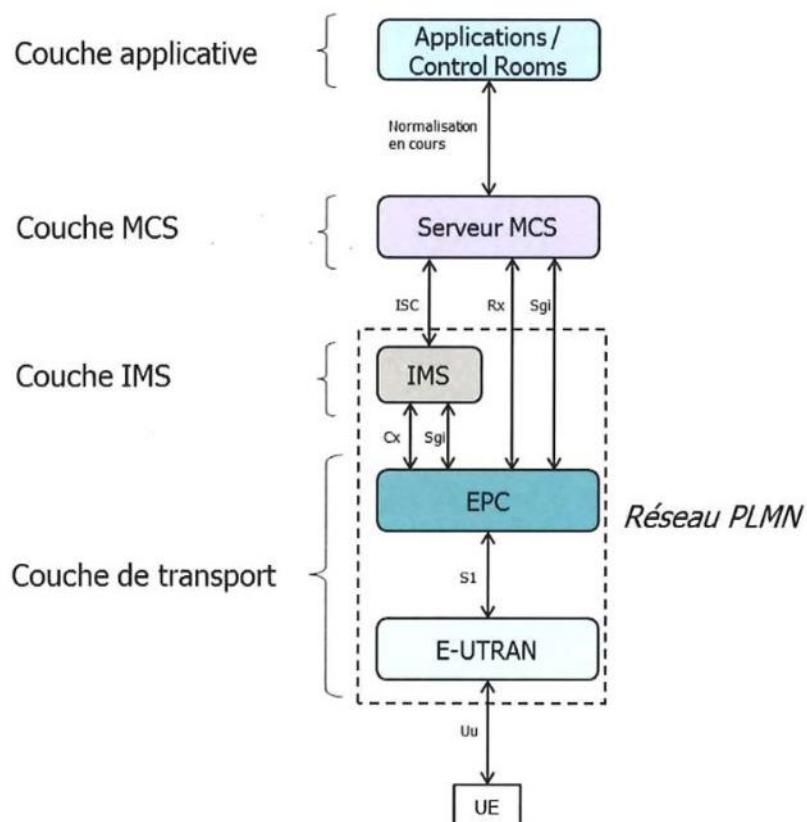
On entend par :

- « service MC » : l'un des trois services MCPTT, MCVideo, MCData.
- « serveur MCS » : l'ensemble des serveurs qui fournissent des services MC aux clients présents dans les UE.

Le « serveur MCS » contient des entités responsables de la gestion de la signalisation :

- SIP Application Server : gestion des sessions SIP appelées par le service MC.
- HTTP client, HTTP server : client et serveur de transactions http.

Blocs fonctionnels



Un système MC est constitué des blocs fonctionnels suivants :

- Un réseau PLMN de technologie LTE qui fournit au terminal la connectivité aux réseaux de données. Il se subdivise en :

- Un réseau d'accès radio (E-UTRAN)
- Un cœur paquet (EPC)

- Un système IMS qui gère la signalisation SIP sur laquelle s'appuient les services Mission Critical. L'IMS demande au serveur MCS de fournir des services, au travers de l'interface ISC (protocole SIP).
- Un ou plusieurs serveurs MCS qui offrent les différents services MC aux utilisateurs soit directement, soit via des applications externes. Compte tenu des besoins de communications de bout en bout, les MCS de différentes origines devront interopérer : le respect de la normalisation 3GPP est indispensable.
- Une couche applicative qui appelle les différents services MC : par exemple, application de salle de commandement (control room), application de cartographie.

Couche de transport LTE

Les terminaux utilisateurs accèdent aux serveurs MCS et à leurs applications métiers par le biais de plusieurs types de réseaux de transport LTE du RRF :

- Un ou plusieurs d'opérateurs mobiles commerciaux.
- Des réseaux tactiques (bulles) déployés à la demande pour faire face à la saturation des réseaux commerciaux lors d'événements ou pour pallier une couverture insuffisante. Ces réseaux devront pouvoir fonctionner en autonomie.

Interconnexion avec les réseaux extérieurs

RRF devra assurer l'interconnexion avec deux familles de réseaux critiques :

- Avec les réseaux critiques bande étroite de type Tetrapol (INPT, Rubis,), vu comme un autre système MCS.
- Avec les réseaux MC des OIV : certains OIV disposeront sans doute de leur propre réseau MC, comprenant : réseau de transport LTE, couche MCS et applications.

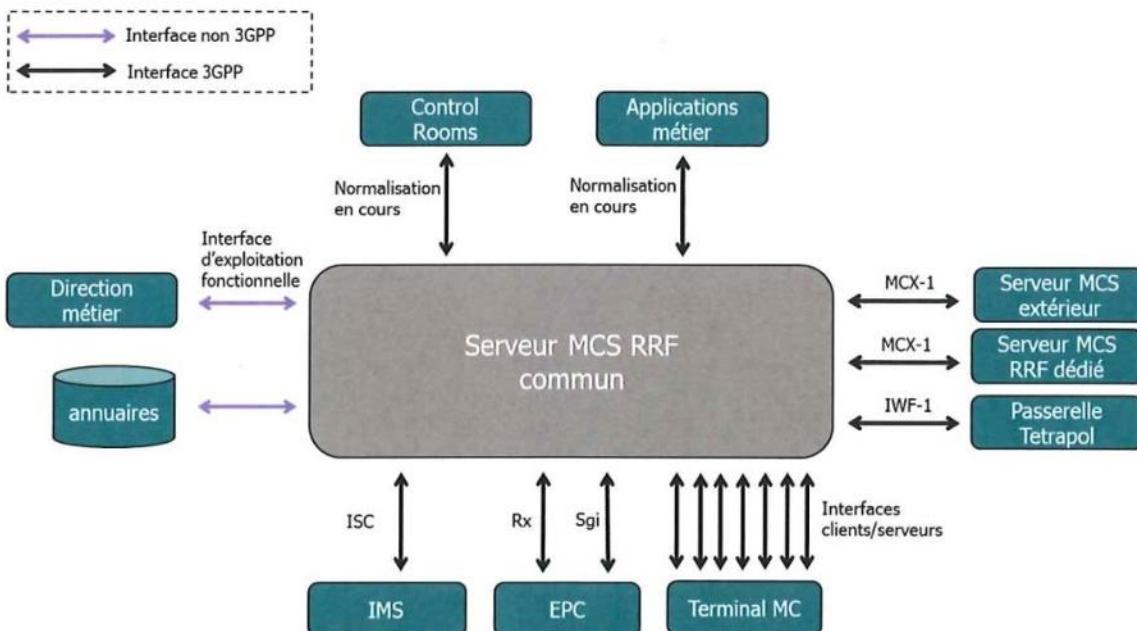
Interface avec les applications métiers et les control rooms

Les MCS devront s'interfacer avec les serveurs des applications métier et avec les control rooms (salles de commandement). Les control rooms accèdent aux serveurs MCS via l'interface nord en cours de normalisation au 3GPP (TS 23.222 : Common API Framework for 3GPP Northbound APIs). Les applications et control rooms sont spécifiques à une communauté donnée : ils devront donc dialoguer avec les utilisateurs RRF de cette communauté, par le biais du MCS RRF commun ou par le biais des MCS dédiés.

Synthèse des interfaces du MCS commun de RRF

La plupart de ces interfaces sont normalisées 3GPP.

Le schéma suivant synthétise les diverses interfaces du MCS RRF commun :

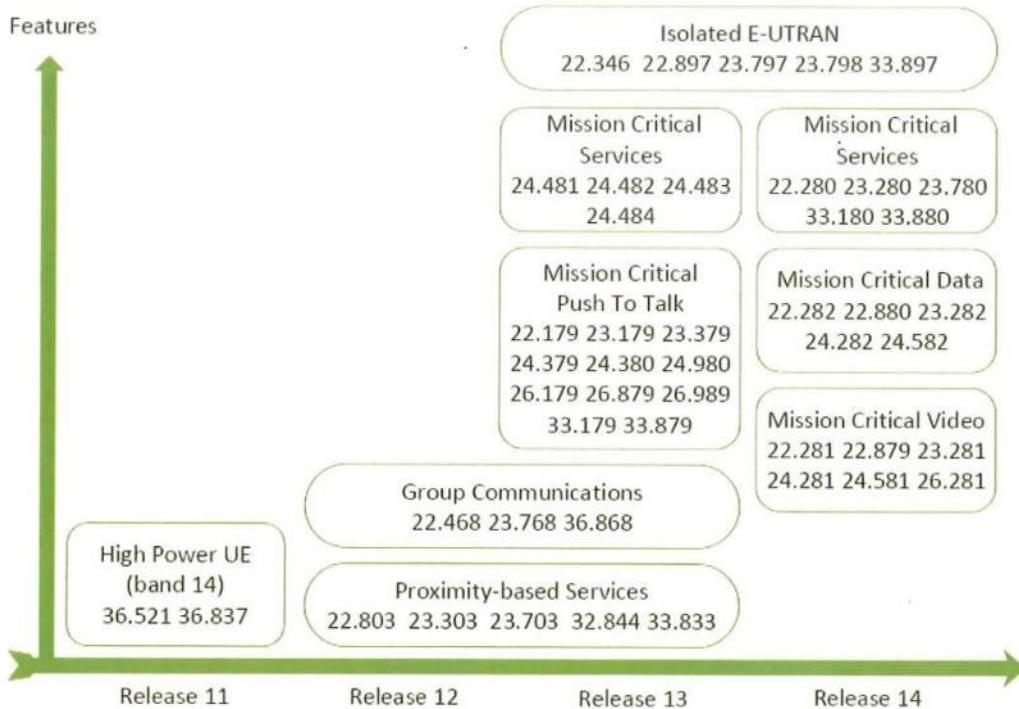


Annexe : définition d'un système 3GPP Mission Critical

État de l'art du LTE

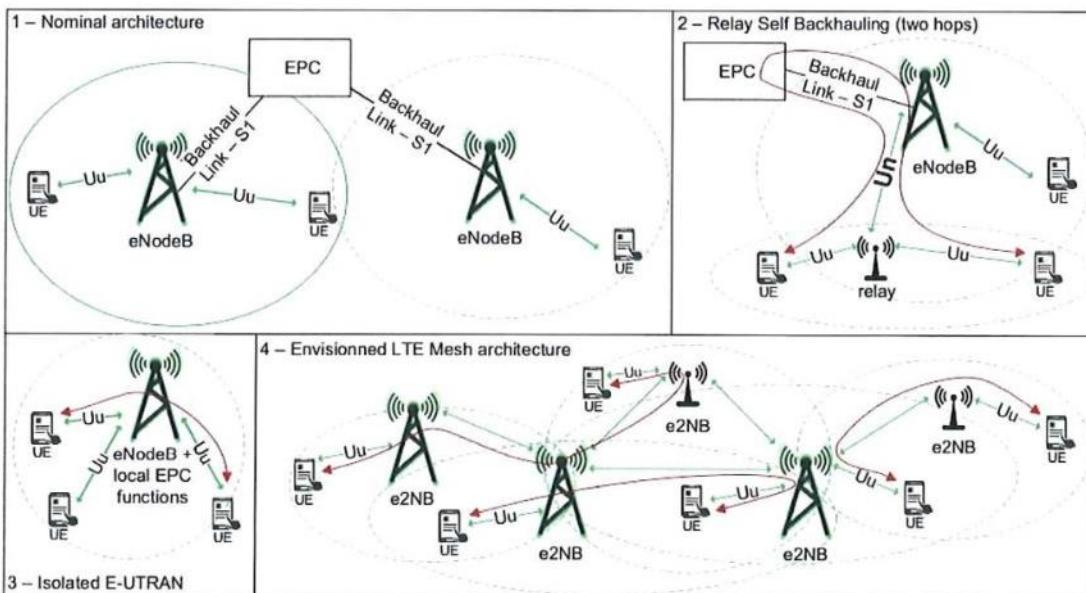
Les spécifications du LTE sont publiées par les groupes de travail du 3GPP. La première version, nommée "Release 8" a été publiée en 2008, et la "Release 10" a été la première version qui respectait les critères de l'Union Internationale des Télécommunications (UIT) pour être désignée comme technologie de quatrième génération (4G). Elles spécifient complètement l'interface radio entre les stations de base (eNBs) et les UEs depuis la couche physique jusqu'à la fourniture du service IP utilisateur.

En particulier, le 3GPP a commencé à travailler sur des fonctionnalités orientées "sécurité publique" à partir de la "Release 11".



Cependant, malgré tous ces travaux, un certain nombre de fonctionnalités d'importances pour les réseaux militaires et pour les réseaux de sécurité publique ne sont pas traités. Ainsi, bien que le 3GPP définisse un type d'eNB autonome (Isolated E-UTRAN) et les fonctions minimales qu'il doit remplir, les liaisons entre eNBs autonomes ne sont pas spécifiées. Il s'agit pourtant d'une fonctionnalité nécessaire à l'établissement d'un réseau autonome.

Ainsi, le LTE tel que spécifié permet de réaliser les topologies présentées sur les Figures (1), (2) et (3) mais ne permet pas de réaliser ce qui est présenté en Figure (4) qui correspond au réseau autonome visé.

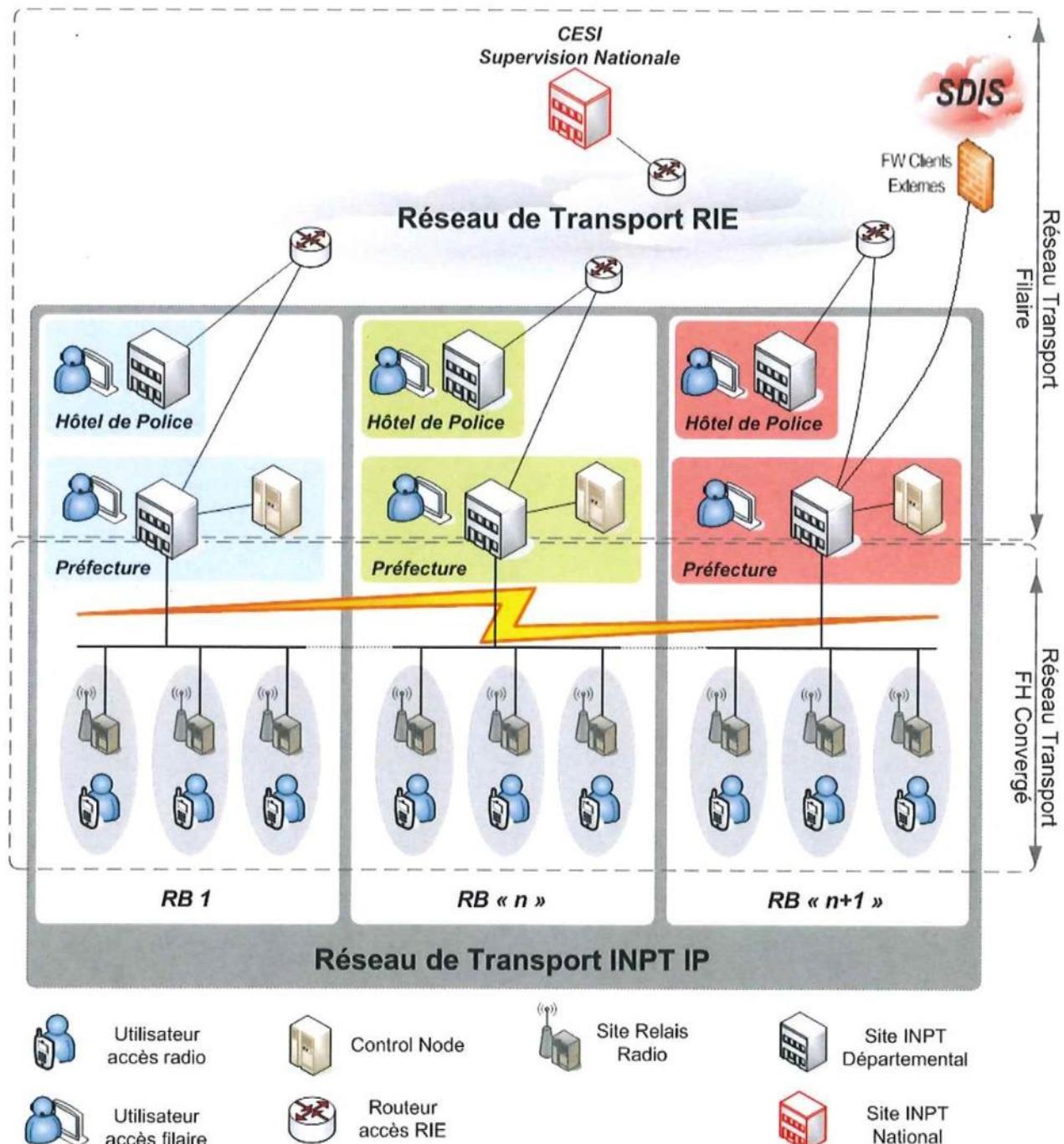


Architecture du réseau national pour INPT IP

Le réseau de transport RIE est une architecture de transmission opérée par Orange.

L'INPT est organisée en Réseaux de Bases départementaux interconnectés entre eux via le RIE. Ainsi, l'architecture RIE permet d'interconnecter les sites TETRAPOL nodaux tels que les Préfectures aux centres de commandement situés dans les Hôtel de Police et SDIS, ou les sites INPT nationaux tels que le centre de supervision CESI et la plate forme TETRAPOL à Lognes.

Le réseau de transport FH Convergé est une architecture de transmission à base de Faisceaux Hertziens reliant les sites radio mobile pour l'INPT et RUBIS.



Vue générique du réseau de transport pour INPT IP