Réseau 4G privé pour les communications critiques

EFORT
http://www.efort.fr

La réalisation d'un système de télécommunication critique passe par l'acquisition de trois éléments fondamentaux qui forment le cœur technique de l'infrastructure de communication critique :
• une capacité d'accès à la couverture radio 4G (puis 5G) auprès de quelques opérateurs de réseaux mobiles ;
• l'acquisition des capacités techniques d'un opérateur de réseau mobile virtuel (MVNO) à savoir un « cœur » de réseau télécom, un système d'information de gestion du réseau privé et de ses abonnés, un centre d'opération du réseau et de service, une offre de terminaux mobiles ;
• l 'acquisition d 'une capacité à délivrer les services de téléphonie et d'Internet ;
• l'acquisition d'une capacité à délivrer des services applicatifs de communications pour missions critiques (MCx), permettant d'organiser des communications multimédias de groupe au profit des abonnés de l'infrastructure de communication critique en bénéficiant d'une qualité de service (QoS) avec priorité et préemption dans les réseaux aujourd'hui 4G et demain 5G.
Le but de ce tutoriel est de présenter un réseau privé 4G (demain 5G) pour prendre en charge les communications pour missions critiques.

1. PMR traditionnel à PMR 4G

Les réseaux mobiles professionnels (PMR / Professional Mobile Radio en anglais) sont des réseaux mobiles indépendants, distincts des réseaux mobiles ouverts au public (réseaux 3G, 4G et 5G). Comme leur nom l'indique, ils permettent de répondre à des besoins professionnels très spécifiques avec une couverture est le plus souvent locale ou régionale (campus, aéroports, industrie, etc).

Ils sont utilisés dans différents secteurs : transports (transports routiers, métros, bus, taxis, etc), industrie, BTP, sécurité, énergie, etc). Ils sont également utilisés par des services de l'état comme la police nationale avec ACROPOL (Automatisation des Communications Radioélectriques Opérationnelles de la Police nationale) ou la sécurité civile, les sapeurs-pompiers et les SAMU avec ANTARES (Adaptation Nationale des Transmissions Aux Risques Et aux Secours).

Leur moyen de communication emblématique est le talkie-walkie.

Sur les réseaux mobiles professionnels, deux technologies principales sont actuellement utilisées :

- **Tetra** (Terrestrial Trunked Radio), un standard défini en 1996 par l'ETSI (European Telecommunications Standards Institute),
- **Tetrapol** (Terrestrial Trunked Radio POLice), développé par Airbus Défence and Space.

Ces deux systèmes de radio numérique mobile ont la caractéristique d'être ouverts en permanence et réservés à un groupe d'utilisateurs spécifiques. Grâce à un talkie-walkie, un opérateur sur le terrain peut communiquer avec tous les autres membres du groupe concerné.

Les technologies Tetra et Tetrapol ne sont cependant plus adaptées aux besoins actuels, notamment en raison de leur faible débit de données et du nombre limité d'appareils qu'il est possible d'utiliser. Elles sont appelées à disparaître progressivement, entre 2026 et 2030.

Les principales qualités de la PMR sont :

- **Un haut niveau de sécurité**: c'est un réseau indépendant, résilient et confidentiel, qui est distinct des réseaux mobiles ouverts au grand public grâce à l'utilisation de bandes de fréquences réservées sous licence,
- **Un haut niveau de qualité**: les communications sont possibles à longues portées et ont une bonne couverture indoor (les bandes TETRA sont les bandes 410-430 MHz | 450-470 MHz | 870-880 MHz pour les applications civiles et privées).
- **Communication de groupe** : cette fonctionnalité « group talk» est essentielle et consiste à ouvrir un canal radio afin que tous les acteurs travaillant sur une même mission puissent recevoir quasiment instantanément et en même temps les mêmes communications.

Les réseaux PMR s'orientent vers le haut débit et la norme LTE sur le réseau 4G pour des raisons d'obsolescence de la technologie PMR classique et pour répondre aux besoins digitaux de leurs utilisateurs (ex : partage de fichiers, d'images, vidéo, chat, etc.). L'organisme de normalisation 3GPP travaille depuis plusieurs années sur la mise en place de la normalisation des services PMR sur les réseaux 4G.

2. Options de déploiement d'un réseau 4G privé pour les communications critiques

Il existe différentes options de déploiement d'un réseau privé 4G pour les communications critiques (Figure 1):

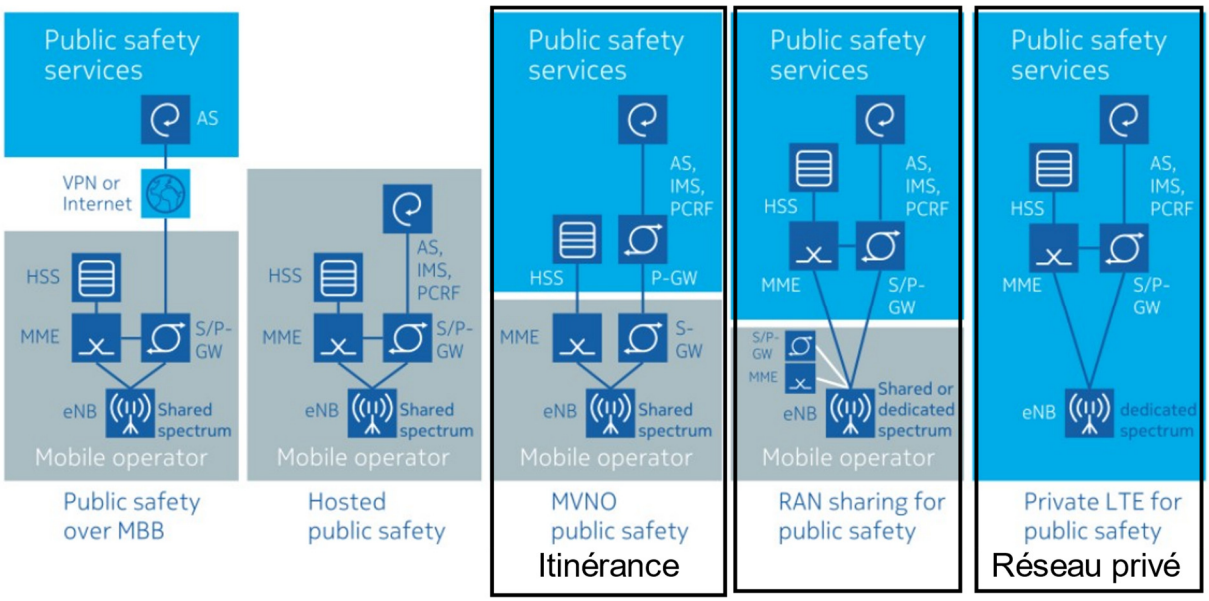

Figure 1 : Options de déploiement d'un réseau privé 4G pour les communications critiques

- Public safety over Mobile Broadband (MBB) : L'entreprise met le serveur pour les communications critiques appelé serveur MCX Server et s'appuie sur le réseau 4G d'un opérateur donné. Tous les terminaux mobiles MCX des agents de cette entreprise activent l'APN MCX dans le réseau 4G de l'opérateur et accèdent ainsi au serveur MCX pour établir des communications critiques voix, vidéo ou data.

- Hosted Public Saftey : L'entreprise utilise le service de bout en bout proposé par un opérateur. L'entreprise dispose donc de N souscriptions au service.
- MVNO public safety : L'entreprise met en place un réseau cœur 4G et le serveur MCX. Elle négocie des accords d'itinérance avec un ou plusieurs opérateurs. L'entreprise devient donc un MVNO pour les communications critiques.
- RAN sharing for public safety : L'entreprise met en place un réseau cœur 4G, le serveur MCX et dispose de ses fréquences qu'elle peut utilise via des sites radio et des antennes appartenant à un opérateur étable via un accord de RAN sharing.
- Private LTE for public safety : L'entreprise dispose d'un réseau 4G privé de bout en bout avec ses propre fréquence, propres antennes, propre réseau cœur et propre serveur MCX.

La figure 2 décrit plus en détail l'option MVNO public safety. L'entreprise dispose de son réseau cœur 4G appel EPC (Evolved Packet Core). Deux instances de cœur EPC virtuel peuvent être déployer dans deux data centers. Par ailleurs, l'entreprise dispose des serveurs Radius/DHCP/DNS pour l'accès Internet, serveurs IMS pour la VoLTE et serveur MCX pour les communications critiques voix, vidéo et data. L'entreprise met en place des accords d'itinérance au niveau national avec un ou plusieurs opérateurs mobiles.

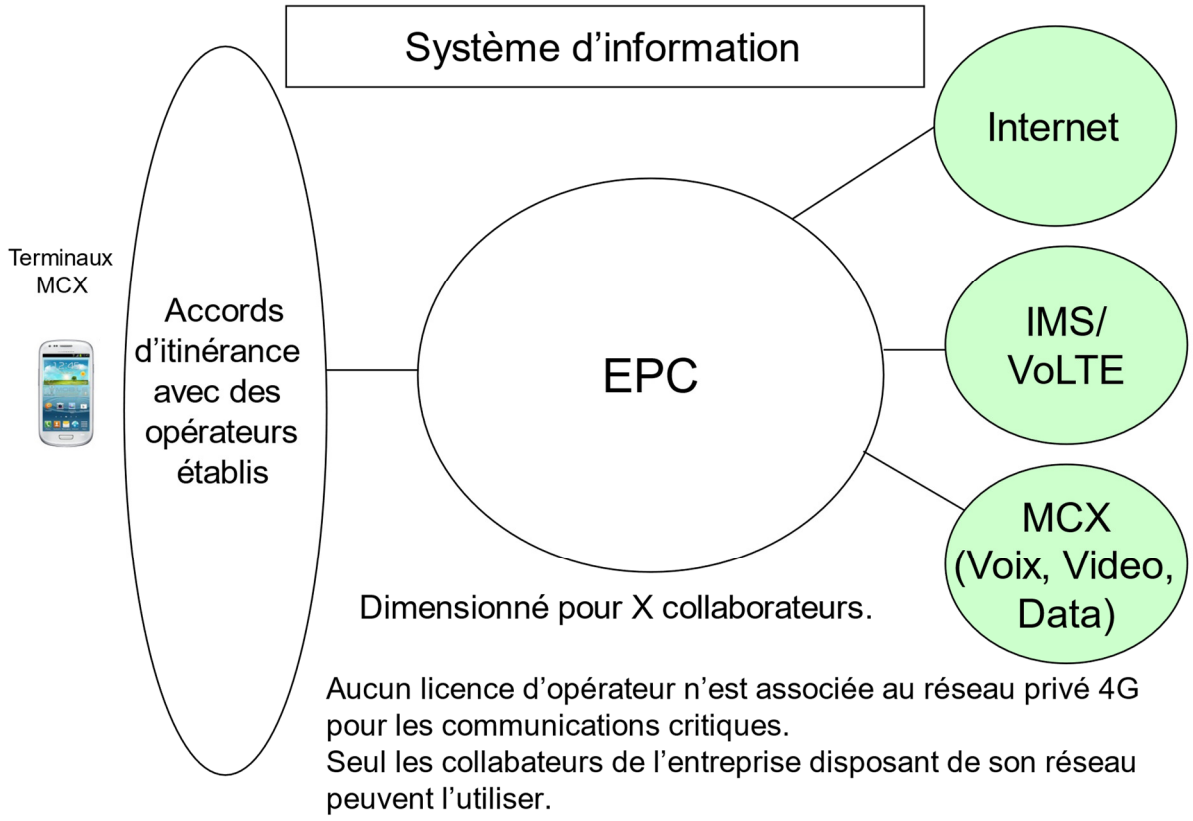

Figure 2 : Structure d'un réseau privé 4G pour les communications critiques (option MVNO public safety)

3. Connectivité 4G et APN

En 2G/3G, la voix ne peut être offerte que par le domaine circuit 2G/3G appelée R4.
L 'usager peut établir un contexte PDP 2G/3G via le domaine paquet GPRS et l 'APN

Internet et ainsi accéder à ses applications Internet. L 'application MCX n 'est pas accessible en 2G/3G.

En 4G, puisque le réseau mobile est tout-IP, les services Internet et la voix sont sur IP. A cela se rejoutent les services MCX sur IP. L 'usager peut établir trois bearers (Figure 3), l 'un pour la data Internet (APN Internet), le 2eme pour le service MCX (APN MCX) et le 3ème pour le service voix sur IP (APN IMS). Le service de voix sur IP depuis l 'accès 4G est appelé VoLTE (Voix over IP over LTE). Ainsi l'usager via son terminal pourra accèder norrmalement aux services Internet, établir des appels normaux VoLTE et établir des communications critiques MCX. Un client applicatif MCX est présent sur son terminal pour initier des communications critiques.

En 5G NSA, l 'usager doit utiliser les deux radios simultanément. La radio 4G est pour le service Voix sur IP et la radio 5G est pour les services data Internet. Le service MCX est considéré d 'un point de vue réseau mobile comme un APN Data. Le bearer MCX comme le bearer Internet seront utilisés depuis la radio 5G.

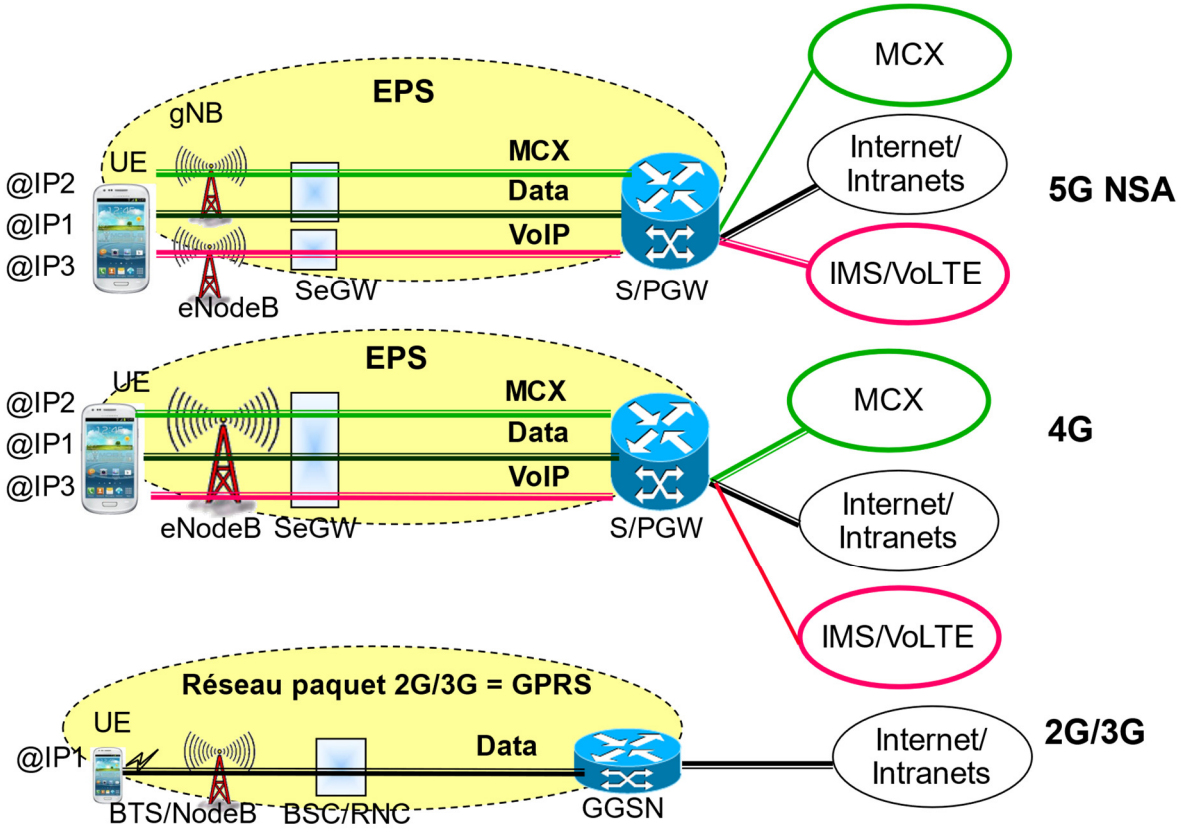

Figure 3 : Connectivités à établir dans le réseau 4G pour l'accès aux différents services

4. Serveur MCX

Le serveur MCX est représenté par différents serveurs chacun mettant en œuvre une fonctionnalité MCX (Figure 4):

- Le serveur MCPTT prend en charge les sessions groupe et sessions privées (i.e., point à point) MCPTT (communications audio)

- Le serveur MCVideo prend en charge les sessions groupe et sessions privées MCVideo (communications vidéo).
- Le serveur MCData prend en charge les conversations groupe et sessions privées MCData incluant les services SDS (Short Data Service) et FD (File Distribution).
- Le serveur Identity Management Server prend en charge l ’authentification de l ’usager MCX.
- Le serveur Group Management Server permet à un usager MCX de créer, modifier, supprimer et interroger des groupes.
- Le serveur Key Management Server permet à un usager MCX d ’obtenir son matériel de clé pour générer les clés requises pour protéger le trafic du plan usager et du plan contrôle.
- Le serveur Configuration Management Server prend en charge la configuration de l ’usager MCX.

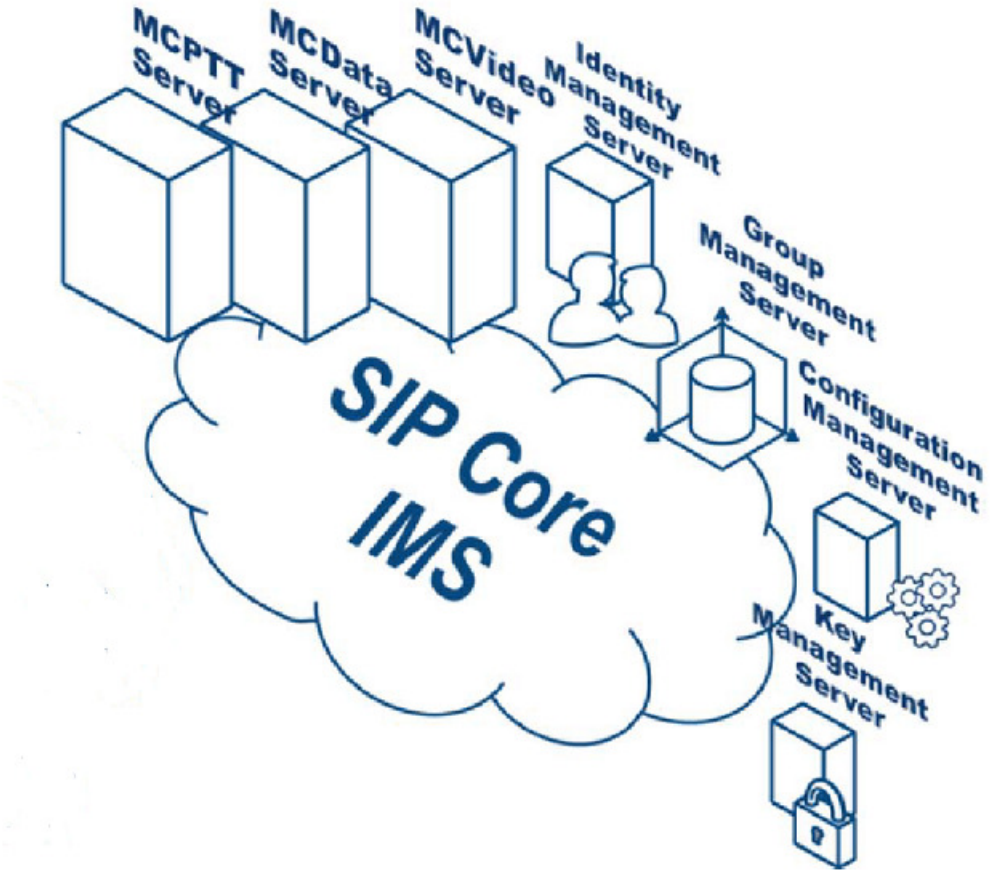

Figure 4 : Le serveur MCX

L’UE MCX doit réaliser les procédures suivantes lors de la mise sous tension du mobile pour accéder au service MCX (figure 5):

- S’identifier et s’authentifier (login et password) auprès de l’IdMS (Identity Management Server). Il obtient un jeton d’accès (autorisation) via le protocole HTTP (étapes 1-2)
- Obtenir sa configuration auprès du CMS (Configuration Management Server) via le protocole HTTP (Etapes 3-4-5)
- Obtenir ses groupes auprès du GMS (Group Management Server) via le protocole HTTP (Etapes 6-7-8)

- Obtenir son matériel de clé auprès du KMS (Key Management Server) via le protocole HTTP (Etapes 9-10-11)
- S'enregistrer et s'authentifier auprès du MCX Server via le protocole SIP et la commande SIP REGISTER (Etapes 12-13-14).

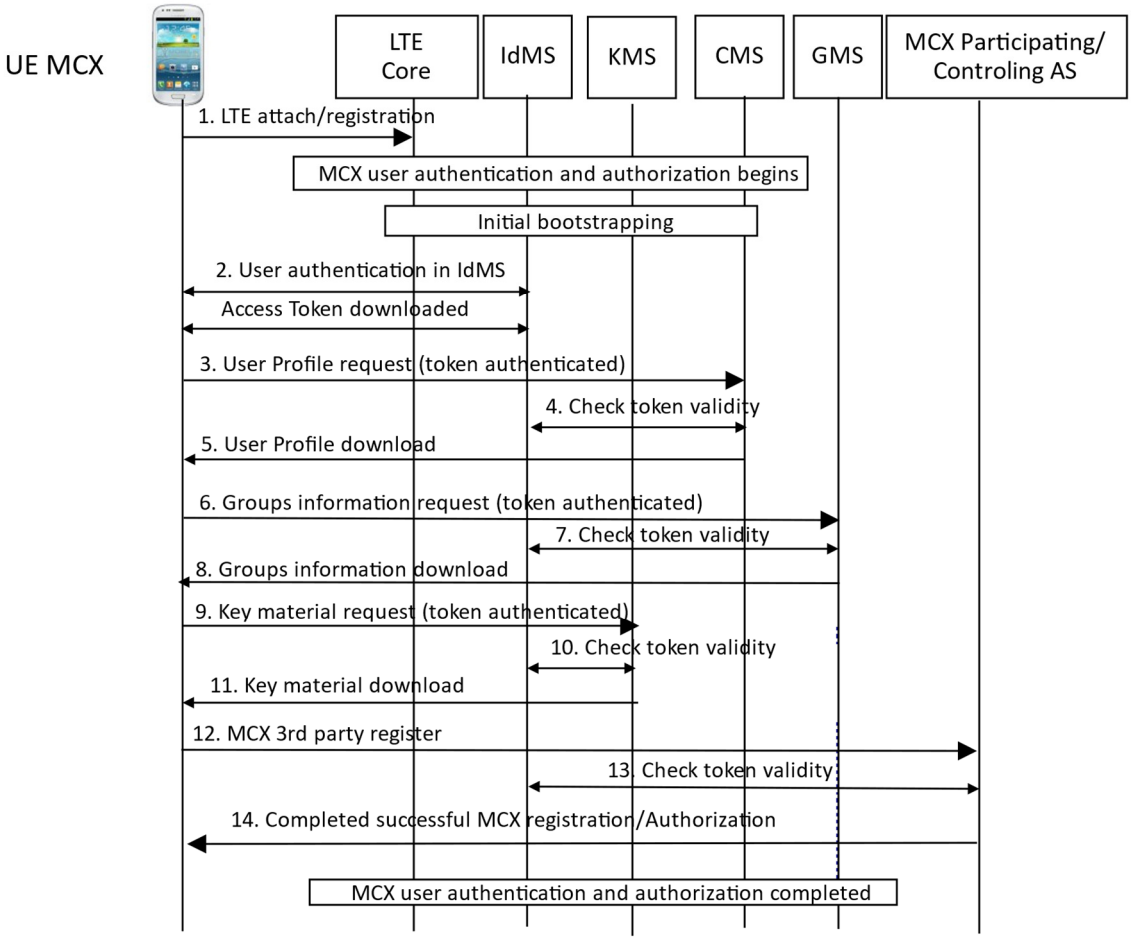

Figure 5 : Initialisation pour l'accès au service MCX

5. MCPTT

Le service Mission Critical Push-To-Talk Voice permet d'effectuer des appels de groupe voix indépendamment des services Mission Critical Video (MCvideo) et Mission Critical Data (MCdata) qui permettent d 'effectuer des appels de groupe vidéo et de partager des données.

Ces services sont intégrés dans les PMR 4G depuis les releases 3GPP 12 et 13 qui permettent d'avoir une garantie d'accès à la ressource à travers les classes d'usage et de service et la mise en œuvre des fonctionnalités dites MCPTT incluant les appels de groupe, les appels individuels, etc.

Ces services critiques sont présents pour la voix dans les réseaux PMR à bande étroite (e.g., TETRA).

- MCPTT est destiné à supporter une communication entre plusieurs utilisateurs (un appel de groupe), où chaque utilisateur a la possibilité d'obtenir le droit de parler de manière arbitrée. MCPTT prend également en charge les "appels privés" entre paires d'utilisateurs. MCPTT est supporté par le réseau EPS pour établir, maintenir et mettre fin au chemin(s) de communication (c'est-à-dire le plan usager) entre les utilisateurs.
- MCPTT permet aux utilisateurs de demander le « droit de parole » et fournit un mécanisme d'arbitrage entre les demandes qui entrent en conflit. Il s'agit du "Foor Control". En cas de plusieurs demandes, MCPTT détermine quelle demande d'utilisateur est acceptée et quelles demandes d'utilisateurs sont rejetées ou mises en file d'attente sur la base d'un certain nombre de caractéristiques telles que leurs priorités.
- MCPTT fournit un moyen pour un utilisateur hautement prioritaire (par exemple, en cas d'urgence) d'interrompre le locuteur actuel. MCPTT prend également en charge un mécanisme pour limiter le temps qu'un utilisateur puisse parler permettant ainsi aux utilisateurs de priorité identique ou inférieure de prendre la parole à leur tour.
- MCPTT permet à un utilisateur de surveiller plusieurs appels en parallèle et permet à l'utilisateur de basculer sur un appel sélectionné. Un utilisateur peut rejoindre un appel de groupe MCPTT déjà établi, appelé "late call entry". De plus, MCPTT permet d'identifier le locuteur actuel aux auditeurs.

5.1. Appels de groupe et appels privés MCPTT

MCPTT doit prendre en charge un certain nombre d'appels de groupe "spéciaux", notamment : **Broadcast Group Call, Emergency Group Call et Peril Group Call**.

- Pour les **Broadcast Group Call**, la diffusion ne fait pas référence au mécanisme de distribution utilisé sur la radio LTE mais au fait que l'utilisateur initiateur MCPTT n'attend aucune réponse des utilisateurs MCPTT récepteurs. Par conséquent, les utilisateurs récepteurs ne peuvent pas répondre dans un Broadcast Group Call. Les utilisateurs MCPTT destinataires prévus peuvent être un sous-ensemble de tous les utilisateurs MCPTT dans un système.
- Un **System Call** est un cas particulier de Broadcast Group Call qui est transmis à tous les utilisateurs d'une zone géographique définie dynamiquement.
- **Emergency Group Calls** sont initiés par des utilisateurs qui se trouvent, par exemple, dans une situation où leur vie est en danger, situation d'urgence pour appeler à l'aide et avoir la plus haute priorité sur toutes les autres transmissions de groupe MCPTT, à l'exception des System Calls et des autres Emergency Group Calls MCPTT. Par exemple, un pompier établit un emergency group call lorsque sa vie est en danger.
- **Imminent Peril Group Calls** sont des appels prioritaires en cas de menace immédiate, par exemple, feu de forêt sur le point d'encercler des campeurs, camion-citerne prêt à exploser près d'une école, victimes sur les lieux d'un attentat à la voiture piégée. Les Imminent Peril Group Calls ont une priorité sur toutes les autres transmissions de groupe MCPTT, à l'exception des System Calls, Emergency Group Calls et d'autres Imminent Peril Group Calls. Par exemple, un pompier établit un imminent peril group call lorsque la vie d'un occupant d'un appartement en feu est en danger.
- **Group Call** sont des appels groupe normaux moins prioritaires que imminent ou emergency group call.

MCPTT prend aussi en charge les **private call.**

Les **Private Calls** sont des appels bidirectionnels entre une paire d'utilisateurs MCPTT utilisant le service MCPTT avec ou sans Floor Control. Les Private Calls exploitent de

nombreuses fonctionnalités des appels de groupe MCPTT telles que la fourniture de l ’identité de l ’utilisateur MCPTT, les informations de localisation, chiffrement, priorité, etc.

Un Private call peut être de type normal ou emergency.

Emergency private call est établi lorsqu’il y a un danger immédiat pour la personne, et dispose d ’une priorité similaire à Emergency Group Call.