RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ACMOSS
Agence des communications mobiles opérationnelles de sécurité et de secours

Diffusion contrôlée

Date : 12/11/2024

Référentiel interconnexion RRF-Réseaux partenaires

Version 0.1

agurre
ASSOCIATION DES GRANDS UTILISATEURS DE RÉSEAUX RADIO D'EXPLOITATION

TABLE DES MATIERES

INDEX DES ILLUSTRATIONS

INDEX DES TABLEAUX

INDEX LEXICAL

ACB	Access Class Barring
ACMOSS	Agence des Communications Mobiles Opérationnelles de Sécurité et de Secours
ANFR	Agence Nationale des FRéquences
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
APN	Access Point Name
ARCEP	Autorité de Régulation des Communications Electroniques et des Postes
ARP	Allocation and Retention Priority
AVP	Attribute-Value Pair
CPE	Customer Premise Equipment
DGE	Direction Générale des Entreprises
DNS	Domain Name System
DSCP	Differentiated Services Code Point
FQDN	Fully Qualified Domain Name
FTTB	Fiber To The Building
FTTH	Fiber To The Home
GBR	Guaranted Bit Rate
GTP	GPRS Tunelling Protocol
GTR	Garantie de Temps de Rétablissement
HLD	High Level Design
HO	Hand Over
HSS	Home Subscriver Server
INPT	Infrastructure Nationale Partageable des Télécommunications
IMS	Information Management System
IP	Internet Protocol
KPI	Key Parameters Indicator
LLD	Low Level Design
LTE	Long Term Evolution
MCPTT	Mission Critical Push To Talk
MCX	Mission Critical X
MME	Mobility Management Entity
MMS-C	Multimedia Message Service Center
MOCN	Multi Operator Core Network
MVNO	Mobile Virtual Network Operator
NSA	Non-StandAlone
OIV	Opérateur d'importance vital
OLT	Optical Line Terminal
PCI	Preemption Capability
PCRF	Policy and Charging Rules Function
PGW	Packet data network GateWay
PLMN	Public Land Mobile Network
PMP	Plan de Management de Projet
PMR	Private Mobile Radio
PPDR	Public Protection and Disaster Relief
PVI	Preemption Vulnerability
QCI	QoS Class Identifier
RACI	Responsible, Accountable, Consulted, Informed
RAN	Radio Access Network
RMP	Réseau mobile Privé
RRF	Réseau Radio du Futur
SA	StandAlone
SAMU	Service d'Assistance Médicale d'Urgence
SCTP	Stream Control Transmission Protocol
SDF	Service Data Flow
SGW	Serving GateWay
SLA	Service Level Agreement
SMS-C	Short Message Service Center
UDP	User Datagram Protocol
VoLTE	Voice over LTE
VPN	Virtual Private Network

1 INTRODUCTION

1.1 PREAMBULE

Ce document se base sur le livrable d'un groupe de travail technique constitué en 2015 du Ministère de l'Intérieur, des membres de l'AGURRE, du Ministère de la Défense, de l'ARCEP et de l'ANFR. Ce document n'avait pas fait l'objet d'une validation formelle.
Il est le fruit du Groupe de Travail « Technique » constitué de membres de l'AGURRE, du Ministère de l'Intérieur, de l'ACMOSS et de la DTNUM et obéit au mandat suivant :
« Il s'agit d'un référentiel qui a pour objectif de constituer la base de la convention d'exploitation des bandes de fréquences à 700MHz du Ministère de l'Intérieur par des acteurs externes. »

Le groupe de travail technique initial s'était fixé les objectifs suivants : *« sous conditions de faisabilité et de disponibilité techniques et dans le strict respect des normes, définir toutes les briques techniques qui composeront l'infrastructure radio de communications de sécurité et de secours dans son ensemble à savoir :*

- *Les conditions techniques d'interfaçage avec les réseaux de certains partenaires légitimes concourant au secours, à la sécurité ou à l'ordre publics et pouvant justifier une interconnexion avec le réseau régalien d'ensemble en raison d'un besoin :*
  - *De communications opérationnelles entre les acteurs de la sécurité du partenaire et de l'Etat ;*
  - *D'accueil de forces régaliennes qu'elles soient permanentes, régulières ou événementielles sur le réseau du partenaire ;*
- *Et définir la gestion régalienne qui intègrera tant les services étatiques que les partenaires légitimes extérieurs concourant aux mêmes missions et souhaitant souscrire à un service radio clef en main ».*

1.2 CONTEXTE

Les réseaux radio bas débit (INPT, RUBIS, ANTARES) du Ministère de l'Intérieur accueillent aujourd'hui les préfectures, les forces de police, de gendarmerie, de sécurité civile, des services de secours (SAMU) et, dans une moindre mesure, des services pénitentiaires et de la défense.

Ces réseaux reposent sur la technologie propriétaire TETRAPOL dite en bande étroite conçue pour transmettre la voix. Ces réseaux obsolètes ne peuvent répondre au besoin de transmission de données haut-débit et présentent des difficultés à s'interopérer. Les usages en sont limités, alors que les exigences d'accès aux systèmes d'information en situation de mobilité sont toujours plus grandes, à l'instar des services grands publics offerts par la téléphonie mobile sur la base technologies large bande.

En conséquence, le Ministère de l'Intérieur a engagé des réflexions sur le renouvellement de ses réseaux actuels bas débit par un réseau haut-débit pour répondre à ces nouveaux besoins et mène des actions conjuguées pour faire face à la fin de vie de la technologie TETRAPOL sur laquelle ils s'appuient à l'horizon 2025 :

- Il a pris une part active à l'obtention de ressources en fréquences dédiées pour les futurs usages de radiocommunications pour la protection du public et les secours en cas de catastrophe dits PPDR en haut débit. Concrétisée par l'obtention de 2 x 8 MHz. Cette démarche collaborative d'usage de ces fréquences est soutenue par les acteurs de réseaux privatifs via l'AGURRE ayant des intérêts convergents avec ceux du Ministère de l'Intérieur sur leurs emprises, par la mise à disposition de ces mêmes fréquences.
- Dans la continuité de l'action menée sur les réseaux actuels, il inscrit aussi sa perspective dans une démarche d'ouverture aux autres services d'État témoignant d'un besoin d'interopérabilité opérationnelle prégnant pouvant s'étendre aussi à certains exploitants de réseaux mobiles professionnels concourant au secours, à la sécurité ou à l'ordre publics. Ce nouveau réseau haut-débit pourra s'interconnecter avec des réseaux bâtis en propre par ces exploitants (appelés **réseaux partenaires**) en raison de convergences avec le Ministère de l'Intérieur dans la réalisation de missions de service public. L'objectif est de bâtir une infrastructure radio cohérente sur un territoire géographique donné, et partagée entre tous les acteurs de la sécurité.

- Afin de développer ce futur service radio haut débit dans un contexte économiquement favorable, le Ministère de l'Intérieur s'est naturellement tourné vers la technologie LTE et travaille, dans le cadre des instances internationales de réglementation et de normalisation, à inclure progressivement les fonctionnalités spécifiques des réseaux radios professionnels de sécurité dans les normes de cette technologie.

En raison de la difficulté pour financer le déploiement de l'ensemble du territoire national avec un réseau en propre dans la bande de 700MHz, le Ministère de l'Intérieur a fait le choix de créer son propre réseau mobile appelé Réseau Radio du Futur (RRF) opéré par l'ACMOSS (Agence des Communications Mobiles Opérationnelles de Sécurité et de Secours).

Le lancement du RRF a été décidé par le cabinet de la Première Ministre en réunion interministérielle le 29 juillet 2022. Le projet d'orientation et de programmation du ministère de l'intérieur (LOPMI) publié le 24 janvier 2023 introduit la notion de réseau de communication électronique des services de secours et de sécurité et définit les spécificités de l'opérateur RRF.

L'ACMOSS a été officiellement créée début avril, le décret au journal officiel ayant été publié le 31 mars 2023.

Le réseau RRF opéré par l'ACMOSS est constitué d'un cœur de réseau LTE en full MVNO interconnecté aux réseaux d'accès radio de des opérateurs commerciaux.

En conséquence, le Ministère de l'Intérieur ne prévoit pas de déployer de réseau sur l'ensemble du territoire national avec les fréquences 700MHz PPDR mais s'appuie sur les réseaux opérateurs commerciaux raccordés au RRF. Ces fréquences 700MHz PPDR ont vocation à être utilisées dans le cadre de déploiement de bulles tactiques mobiles dont les relais véhiculaires et de couverture de zones spécifiques.

Ces fréquences peuvent être assignées à certains exploitants de réseaux mobiles privés qui concourent au secours, à la sécurité ou à l'ordre public et, de manière plus élargie à contribuent à l'intérêt général. Cette autorisation est réalisée sous conditions d'un intérêt commun entre le Ministère de l'Intérieur et le Réseau Partenaire.

Elles sont déployées dans des infrastructures critiques, telles que les réseaux de transports en commun, les réseaux autoroutiers, les gares ou aéroports ou encore les infrastructures de production et de transport d'énergie. Ces assignations de fréquences sont accordées par le ministère de l'Intérieur et des Outre-mer assure en échange d'accueil des usages régaliens.

1.3 OBJECTIF DU DOCUMENT

Ce document « Référentiel d'interconnexion RRF-réseau partenaire » a pour objectif de :

- Cadrer l'engagement que la ressource 700 PPDR n'est pas pour un usage propre du réseau mobile privé mais pour les missions de secours et de sécurité auxquelles contribuent les réseaux mobiles privés et dans le cas d'intervention des forces de sécurité et de secours, permettre à leur service d'entrer en communication avec les forces de sécurité et de secours ;
- Décrire les architectures permettant d'exploiter au mieux la ressource rare que constitue le spectre avec la meilleure efficacité opérationnelle dans ce contexte d'ouverture vers des partenaires privés avec pour certains, le souhait d'une gestion en propre de leur réseau radio reposant sur ce spectre dédié à ces besoins ;
- Elaborer une phase d'étude & une phase de mise en œuvre débouchant sur la production de plusieurs livrables à l'initiative des réseaux mobile privé : Rédaction de livrables techniques (architecture, spécifications d'interfaces, sécurité, cahiers de tests) ;

Ce document décrit aussi les relations et l'organisation à mettre en œuvre entre le RRF et les réseaux partenaires et permet

- D'élaborer le PMP (cartographie des participants, quand et comment solliciter les participants, RACI, Jalons clé)

Enfin, le corpus documentaire associé au document porte les éléments suivants :

- L'accord de confidentialité entre le réseau mobile privé et ses partenaires et l'ACMOSS en **Annexe 5.3**
- Les spécifications fonctionnelles (besoin propre aux abonnées du RRF en terme de géolocalisation, QoS, débit...) **Livrable 2**
- Le PMP (cartographie des participants, quand et comment solliciter les participants, RACI, Jalons clé) **Livrable 1**
- Les livrables de la conception HLD, LLD et de l'intégration (cahier de tests)
- La convention d'exploitation **Annexe 5.5 qui permet le basculement en opération après la VSR et permet l'utilisation du réseau partenaire pour les utilisateurs du RRF relatif à l'interconnexion ;**

Le RRF comme le réseau partenaire est le seul responsable de la définition de l'architecture de son réseau radio. **Les exigences spécifiques liées à l'interfaçage entre les réseaux et à l'accueil des forces régaliennes sur le réseau partenaire sont décrites dans ce document**. Les architectures du réseau RRF et des réseaux partenaires respectent les standards du 3GPP et en particulier ceux de la technologie LTE (Long Term Evolution) et leurs évolutions.

Tout au long de la vie des réseaux radio, chaque acteur (RRF et réseau partenaire) reste responsable des équipements et systèmes qu'il a mis en place.

Ce document ne décrit pas la totalité des fonctionnalités attendues ni les choix d'exploitation qui sont de la responsabilité de chacun des gestionnaires de réseaux. **Le document décrit des objectifs de performances attendues de chacun des réseaux pour assurer leur interfaçage et l'itinérance des forces régaliennes sur le réseau partenaire.**

1.4 APPLICABILITE ET GESTION DES EVOLUTIONS

Les architectures retenues et agréées par les partenaires sont déclinées au sein de ce document qui présente les obligations technico-fonctionnelles imposées à chaque partenaire pour pouvoir construire son réseau radio sur la base des fréquences dédiées PPDR tout en garantissant l'accueil des usages régaliens conformément au mandat exprimé.

Sur la base de ces exigences, chaque demandeur doit construire un dossier de demande étoffé pour permettre aux services du ministère de l'intérieur, affectataire exclusif des fréquences, de procéder à une analyse approfondie de la demande. En cas d'avis favorable, un accord est conclu entre le Ministère de l'Intérieur et ce demandeur. **Les détails de la démarche sont décrits dans le document en section §2.**

Ce document est amené à évoluer pour prendre en compte notamment, les avancées de la normalisation du 3GPP. Le tableau auquel il se réfère figure en annexe.

Dans l'annexe 1, un tableau décrit les principales normes applicables.

1 ARCHITECTURE

1.1 PREREQUIS

Le RRF est un réseau mobile très haut débit de type full MVNO permettant de délivrer des services de communications critiques (MCX), de téléphonie, d'internet et d'accès aux intranets des métiers des communautés. Il possède une infrastructure cœur LTE complète en propre incluant les équipements suivant MME, HSS, SGW, PGW, PCRF. Le réseau d'accès radio repose sur deux opérateurs publics en architecture S8 Home Routing.

Le réseau RRF est un réseau 4G/5G NSA évolutif vers la 5G SA.

En préambule, il est rappelé que les fréquences dédiées PPDR ont vocation en premier lieu à servir le réseau radio national Étatique. L'ouverture en usage dérogatoire à des partenaires extérieurs doit répondre aux besoins PPDR, mais avec une gestion d'infrastructure exercée par les gestionnaires des réseaux partenaires. En contrepartie, cet usage dérogatoire impose de garantir l'accueil, la priorité et la préemption de la ressource au profit des forces régaliennes lors de leurs interventions sur site d'un réseau partenaire.

Un réseau partenaire devra donc être en capacité de fournir un service radio au profit :

- Des forces régaliennes régulières, permanentes ou événementielles présentes dans sa zone de couverture ;
- De ses propres services en particulier ceux concourant au secours, à la sécurité ou à l'ordre publics.

Il se doit de garantir la capacité à transmettre des flux des utilisateurs RRF vers le cœur de réseau RRF. Le détail des flux et les besoins de qualité de services sont décrits dans le paragraphe §1.3 « Paramétrages ».
Le réseau partenaire doit répondre aux normes 3GPP en vigueur pour s'interconnecter au RRF, celles-ci sont listées en annexe dans un souci de lisibilité et de simplification de mise à jour. Ce niveau n'exclut pas l'adjonction de niveaux de sécurisation supérieurs par tunnelisation ou de type applicatif.
Les équipements RRF susceptibles de se connecter au réseau partenaire sont de différents sortes (téléphones mobiles, tablettes, passerelles bas débit, relais véhiculaires…). Ils doivent tous être autorisés sur le réseau partenaire, à condition d'être homologués sur le réseau partenaire (des équipements ne respectant pas les standards pourraient ne pas être homologués). La liste des modèles utilisés pourra être fournie à l'opérateur partenaire dans le cadre du partenariat.

1.2 ARCHITECTURE DE RACCORDEMENT

1.2.1 ARCHITECTURE D'ACCES RADIO

Pour permettre l'utilisation de la couverture des réseaux des opérateurs partenaires aux abonnées RRF, il est possible de raccorder les réseaux partenaires au RRF de deux façons :

- Roaming S8 home routing
- RAN sharing MOCN

Ces architectures sont standardisées par la 3GPP afin de garantir l'interopérabilité entre réseaux et faciliter les mobilités entre ceux-ci.

Le RRF dispose de trois environnements : deux environnement de production et d'un environnement de préproduction dédié aux réseaux mobile privés.

Ces environnements devront être pris en considération pour le raccordement.

1.2.1.1 Roaming S8 Home Routing

Le « roaming » ou « itinérance » consiste à autoriser les abonnés d'un réseau A (Home PLMN (Public Land Mobile Network)) à bénéficier d'un ensemble de services du réseau visité B (Visited PLMN).

Le « Home Routing » signifie que les serveurs applicatifs (MCPTT, VoLTE, Intranet, …) sont hébergés au cœur du réseau A (Home PLMN) et que le réseau B ne fait que transporter les plans de trafic de l'abonné.

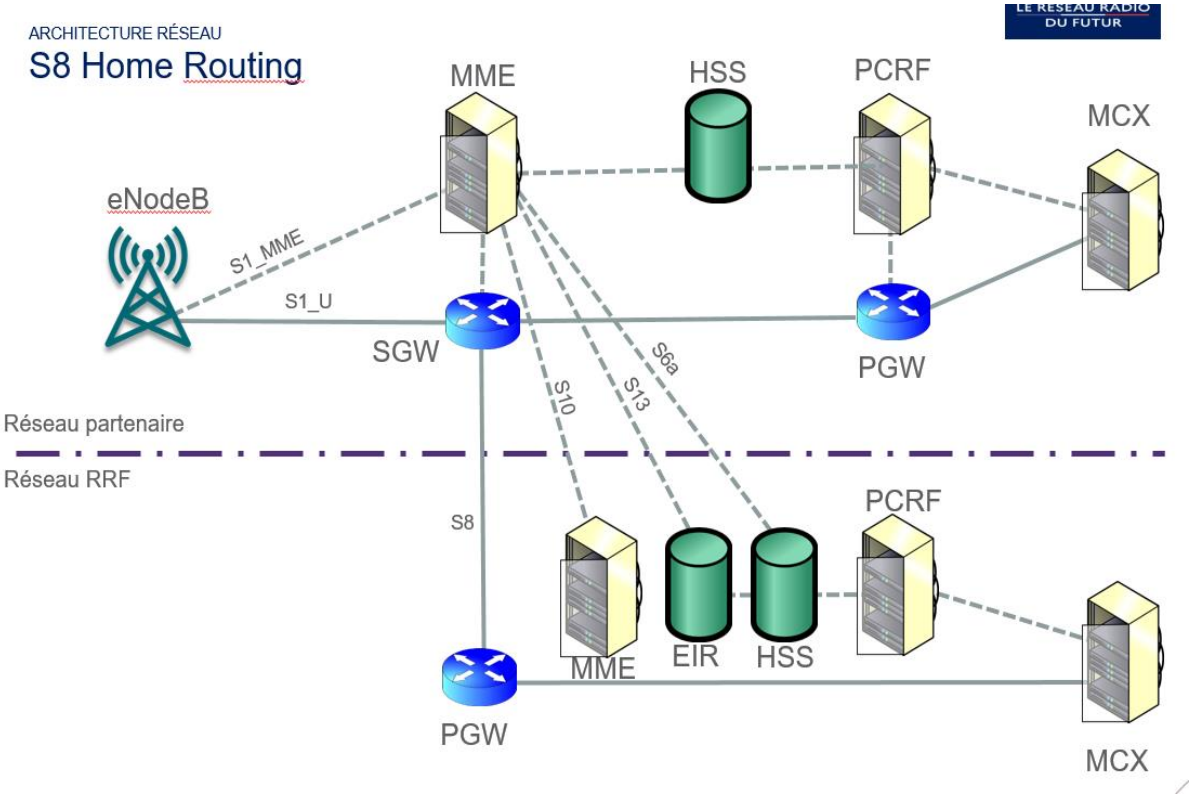

Figure 1 : Schéma d'architecture de raccordement en S8HR

Les interfaces 3GPP mises en œuvre dans ce type d'architecture sont :

- Interface S6a : Interface entre MME du réseau partenaire et le HSS du RRF. S6a est une Interface Diameter et utilise SCTP comme transport.
- Interface S8 : Interface entre la SGW du réseau partenaire et de la PGW du RRF. L'interface est basée sur le protocole GTPv2-C pour le plan contrôle et GTPv1-U pour le plan usager, ces protocoles sont transportés par de l'UDP/IP.
- Interface S13 Interface entre les MME du réseau partenaire et l'EIR du RRF. Il est prévu d'avoir une interface S13 entre le MME des opérateurs et l'EIR du RRF pour implémenter une logique de filtrage par IMEI suivante:
    - Liste blanche: accès autorisé
    - Liste grise: autorisé mais avec traçage
    - Liste noire: non autorisé
    - IMEI non listés : non autorisés.
- Interface DNS : Les serveurs DNS du réseau partenaire seront utilisés pour résoudre les APN et APN RRF. La protection des adressages associés aux noms de domaines dans le cadre du service DNS est garantie par un partitionnement des données afin de les rendre accessibles uniquement aux équipements nécessitant d'en disposer.

1.2.1.2 RAN Sharing MOCN (Multi Operator Core Network)

Le « RAN Sharing » correspond à la capacité d'un réseau à partager ses ressources radio avec un autre réseau. Le partage de ressources et la séparation des flux entre réseaux se font ici au niveau de chaque eNodeB (Station radio en LTE).

Dans sa version Multi Cœur de Réseau (MOCN), chaque eNodeB partagé se raccorde aux cœurs de chaque réseau. L'eNodeB peut être paramétré pour réserver statiquement une partie des

ressources radio à chaque réseau de rattachement ou l'allouer dynamiquement en partage au bénéfice des abonnés de chacun des réseaux.

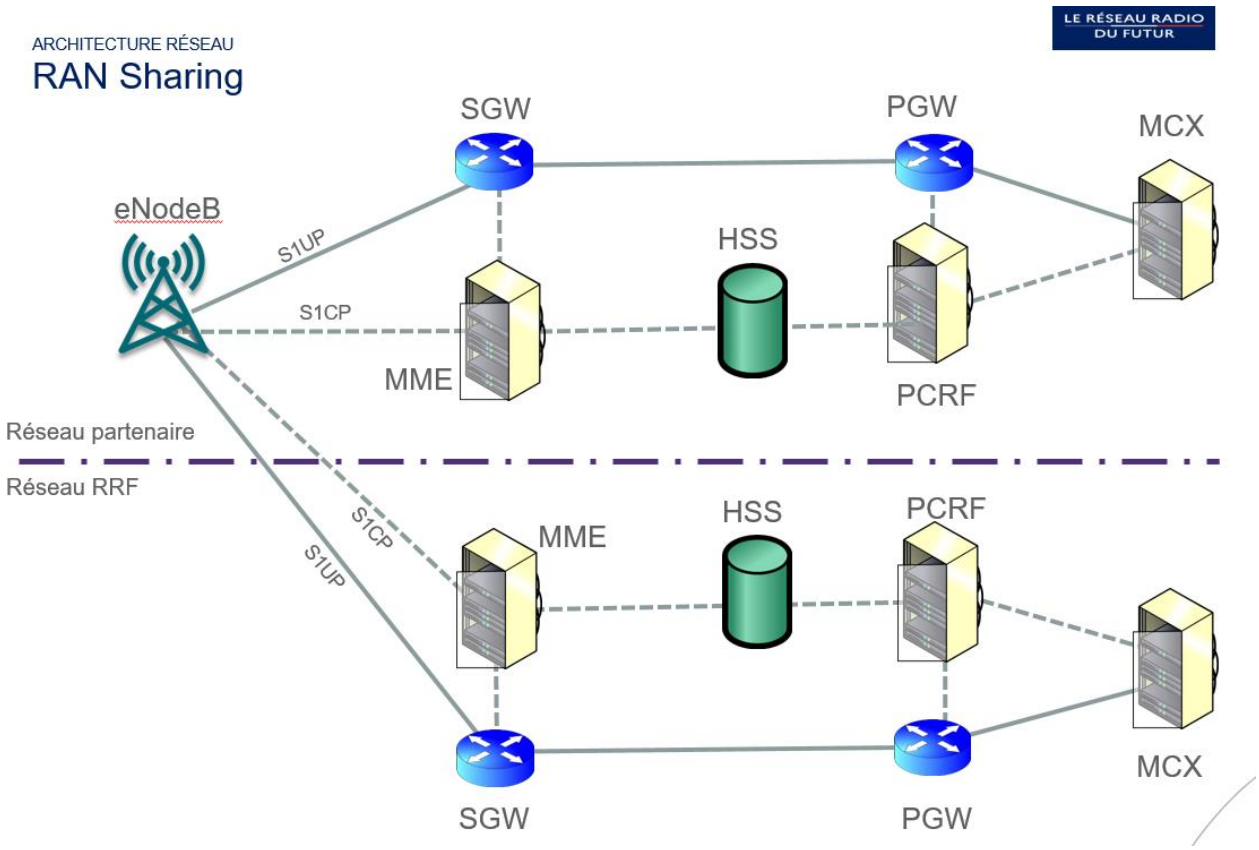

Figure 2 : Schéma d'architecture en RAN Sharing MOCN

Les interfaces 3GPP misent en œuvre sont:

- S1_MME : interface entre la NodeB du réseau partenaire et le MME du RRF, elle transporte toute la signalisation liée à l'abonné RRF vers le cœur de réseau RRF
- S1_U : interface entre la NodeB du réseau partenaire et la SGW du RRF, elle transporte tout le trafic user plan de l'abonné RRF vers le cœur de réseau RRF.

Le mode MOCN mis en œuvre respectera la norme 3GPP « TS 23.251 v15.1.0 ».

Le choix de la configuration pour un réseau partenaire s'établira de manière concertée avec le gestionnaire du réseau régalien.

Les réseaux partenaires devront se conformer à toutes les obligations et options technico-fonctionnelles d'interfaçage au RRF retenues lors du choix d'interconnexion. Ces obligations incluent naturellement toutes les contraintes de sécurité imposées par le gestionnaire de réseau régalien en liaison avec l'ANSSI.

1.2.2 AUTRES INTERCONNEXIONS

En supplément des interfaces permettant l'usage de couverture des opérateurs partenaires, d'autres interfaces pourraient être mises en place suivant les besoins métiers. Celles-ci feront l'objet de discussion pour entériner les besoins et donc les mises en place.

1.2.2.1 Interfaces inter-MCX

Le serveur d'application MCX du RRF est chargée de gérer les communications critiques des différents métiers de la police et du secours.

Si le réseau opérateur dispose d'un serveur MCX et suivant les besoins des métiers de disposer de groupes de conférence communs, il pourra être décidé (d'un commun accord) de mettre en place des interfaces Inter serveur MCX.

Pour ce faire, les serveurs d'applications MCX doivent présenter les interfaces 3GPP inter-MCX suivantes :

- MCX-1, CSC-16, CSC-17
- MCData-3
- MCPTT-3
- MCVideo-3

Ces mécanismes d'interopérabilité par service MCX ainsi que les gestions de groupes inter-MCX seront définis au cas par cas en fonction de leur intérêt et de leur nécessité.

1.2.2.2 Interfaces géolocalisation

Des systèmes de géolocalisation peuvent être mis en place pour répondre à la problématique de milieu contraint (indoor, souterrain…) par les réseaux partenaires.

Après accord entre les parties, ces systèmes peuvent être mis à disposition pour les clients RRF. Les interfaces nécessaires seront discutées entre les parties.

Il n'y a pas d'échange de localisation des clients RRF vers l'opérateur partenaire et inversement sans autorisation explicite et temporaire liée à un besoin sur une zone d'intervention. Les modalités de ce partage seront cadrées par des procédures à définir entre les parties.

1.2.2.3 Interfaces taxation, supervision

Des interfaces supplémentaires peuvent être mise en place entre le réseau RRF et le réseau partenaire pour répondre aux besoins d'administration et de supervision suivant les besoins remontés des deux parties.

Il pourra s'agir notamment :

- D'échanger des informations d'usages des réseau (CDR – Compte Rendu D'Appel) pour la taxation ;
- De remonter des informations de supervision permettant d'informer sur l'état de son réseau ;
- De communiquer des opérations planifiées ;
- D'ouvrir des incidents si des dysfonctionnements sont constatés.

Ces échanges d'informations permettent de répondre aux besoins d'exploitabilité et de maintenance listés en section §3 – Modalités d'exploitation.

1.2.3 INTERFACES ET NORMES 3GPP

Le RRF et les réseaux partenaires doivent respecter les normes 3GPP des interfaces télécom entre réseaux dans un souci d'interconnexion.

En annexe 1 sont rassemblées les normes 3GPP nécessaires aux interfaces listées précédemment. Cette liste aura vocation à être mise à jour dans le temps suivant l'avancement de la normalisation.

1.2.4 ARCHITECTURE PHYSIQUE

Des liens d'interconnexion en fibre optique doivent être mis en place pour raccorder le réseau de l'opérateur partenaire et le réseau RRF. Ils seront dimensionnés pour écouler le trafic des utilisateurs RRF (cf. §1.4 « Dimensionnement »).

Le raccordement se fait de préférence avec le la FO noire sans héberger des équipements actifs (switchs, FW, routeur).

La liaison vers le Datacenter du RRF est sous la responsabilité du réseau mobile privé.

Les réseaux partenaires devront se montrer en capacité d'acheminer les flux au point de raccordement défini en concertation avec l'ACMOSS.

Le raccordement entre l'infrastructure RRF et le réseau partenaire se fait par raccordement sécurisé de niveau 3 (double pénétration, double adduction, double rattachement). Toutefois, en concertation avec l'ACMOSS et sous couvert de faisabilité et de facilités techniques offertes, il pourra être toléré exceptionnellement des raccordements présentant une sécurité moindre après accord de l'ACMOSS.

La responsabilité des gestionnaires de réseaux s'arrête aux points de raccordement définis entre le réseau régalien et les réseaux partenaires.

La mise en œuvre de la sécurité sur ces accès d'interconnexion obéit aux prescriptions de l'ANSSI.

1.3 PARAMETRAGES

1.3.1 LES TYPES DE TRAFIC PORTES PAR LE RESEAU

Le réseau partenaire doit transporter les différents types de flux émis par les clients RRF jusqu'au cœur de réseau RRF :

- Les appels Voix sur LTE : portés par l'APN IMS, ce trafic est traité par le cœur de réseau RRF ;
- Les usages MCX avec les services MCPTT, MCVidéo, MCData portés par l'APN MCX. Ces flux transiteront jusqu'au MCX Serveur RRF ;
- L'envoi et la réception de SMS et de MMS, les SMSoverIP passent par l'APN ims vers la IP-SM-GW et le SMS-C, Les MMS passent via l'APN mms
- L'usage data, porté par l'APN data.
- Services IP sécurisés (accès aux intranet métiers et à internet)
- Une catégorie spécifique de mobiles (STORM) utilise l'APN mi pour les flux MCX et data

1.3.2 LES MÉCANISMES DE QOS

L'accès au réseau radioélectrique des opérateurs partenaires doit supporter la fonctionnalité ACB, et la gestion de la QOS : ARP et QCI permettant la mise en place des mécanismes de priorité et de préemption définis à partir de la Release 12 du 3GPP et permettant ainsi aux services de secours et de sécurité de bénéficier d'un service d'accès radio prioritaire dans certaines circonstances.

Les mécanismes dont bénéficient les utilisateurs du RRF doivent être l'ACB, l'ARP et les QCI

1.3.2.1 L'Access Class Barring, ou ACB

L'ACB est un mécanisme défini par le 3GPP qui permet, en cas de congestion de l'eNodeB, de prioriser la connexion à celle-ci aux terminaux de classes prioritaires (portant un ACB de 11 à 15).

Le réseau partenaire doit mettre en œuvre le mécanisme d'ACB sur son réseau pour les utilisateurs du RRF.

1.3.2.2 L'Allocation Retention Priority, ou ARP

L'ARP est un mécanisme de contrôle d'admission défini par le 3GPP qui permet en cas d'indisponibilité de ressources sur le réseau pour transporter de nouveaux paquets de données, de préempter la session de l'utilisateur avec l'ARP le plus élevé par un utilisateur avec un ARP inférieur. De la sorte, la session de l'utilisateur avec l'ARP le plus élevé se retrouve coupée.

Le réseau partenaire doit prendre en compte les valeurs de ARP priority level (PL), de vulnérabilité (PVI) et de préemption (PCI) demandées par les sessions établies par les utilisateurs RRF et s'assurer qu'elles sont bien prioritaires par rapport aux utilisateurs du réseau partenaire.

Les valeurs seront déterminées conjointement entre l'ACMOSS et le réseau partenaire.

1.3.2.3 Les Quality of Service Class Identifiers, ou QCI

Les QCI sont des valeurs indiquant le niveau de qualité de service associé à certains trafics LTE (exemples : QCI 3 pour les jeux vidéo, QCI 70 pour le MCData, etc.). A chaque QCI est associé une priorité de traitement, un temps de latence et un taux de déformation du paquet de données transmis.

Voici les QCI utilisés par flux de services par les utilisateurs du RRF :

- QCI 1 et 5 pour le service VoLTE ;
- QCI 6 pour les services IP sécurisés ;
- QCI 65 pour le service voix MCPTT en GBR ;
- QCI 69 pour le service MCPTT en non GBR, QCI de signalisation MCX, incluant MCData SDS ;
- QCI 70 pour le service MCData FD, pour le service vidéo en V1 et V2 ;
- QCI 67 pour le service MCVidéo en GBR en VS ;

Ces QCI doivent être supportés et implémentés par le réseau partenaire et la QoS associée mise en œuvre.

Ci-dessous le tableau de QCI et de paramètres de qualité de services normé par le 3GPP

QCI	Re-source Type	Prio-rité	Délai	Taux d'erreurs	Exemple de flux
1	GBR	2	100 ms	10^{-2}	Conversational Voice
2		4	150 ms	10^{-3}	Conversational Video (Live Streaming)
3		3	50 ms	10^{-3}	Real Time Gaming
4		5	300 ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
65		0.7	75 ms	10^{-2}	Mission Critical user plane Push To Talk voice (e.g. MCPTT)
66		2	100 ms	10^{-2}	Non-Mission-Critical user plane Push To Talk voice
5		1	100 ms	10^{-6}	IMS Signalling
6		6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file)

7	Non-GBR	7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8		8	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc…)
9		9	300 ms	10^{-6}	sharing, progressive video, etc…
67		1.5	100 ms	10^{-3}	Mission Critical video user plane
69		0.5	60 ms	10^{-6}	Mission Critical delay sensi-tive signalling (e.g. MC-PTT signalling)
70		5.5	200 ms	10^{-6}	Mission Critical Data (e.g. ex-ample services are the same as QCI 6/8/9)

Tableau 1 : QCI et paramètres de qualité du 3GPP

1.3.2.4 Indicateurs de performance (KPI) MCX

Les indicateurs de performances de bout-en-bout sont définis par le 3GPP pour les services MCPTT dans la spécification 3GPP « TS 22.179 ». Ci-dessous le tableau résumant la liste des KPIs, leur signification et les valeurs maximales recommandées :

Variable	Indicateur	Définition	Valeur
KPI 1	Temps d'accès sur conférence ouverte (MCPTT Access time)	Cas le plus usité, temps maximal entre l'appui sur le bouton de prise de canal et le retour de signalisation du droit de parler.	< 300 ms pour 95% des appels
KPI 2	Temps de d'accès bout en bout incluant ouverture de conférence (End-to-end MCPTT Access time)	Typiquement cas des appels direct, temps maximal entre l'appui sur le bouton et le retour de l'ouverture de la conférence, de l'alerte et de l'ouverture du flux audio/vidéo avec le(s) appelé(s).	< 1000 ms
KPI 3	Délai de latence de la voix bouche à oreille (Mouth-to-ear latency)	Délai de propagation de la voix du micro de l'émetteur aux haut-parleurs de(s) l'écoutant(s).	< 300 ms
KPI 4	Délai de réception voix sur entrée sur Conférence établi (Maximum Late call entry time)	Délai entre sélection de la conférence par l'utilisateur et réception de la première trame voix de la conférence	<350 ms pour les systèmes cryptés.

Tableau 2 : Indicateurs de performance (KPI) du 3GPP

1.3.2.5 Priorités contextuelles des flux MCX

Le serveur d'application MCX permet, de manière dynamique, d'associer des AVP et des valeurs de préemption différentes pour des flux en fonction d'un contexte opérationnel d'emploi exceptionnel. Ce processus permet d'accentuer momentanément la criticité de certains flux par rapport à d'autres.
Par exemple, il peut privilégier temporairement l'envoi de données de mises à jour d'une cartographie essentielle à des unités devant progresser dans des environnements inconnus et en situation de criticité forte.
Le détail de ce besoin doit être étudié entre les parties pour être mis en œuvre de manière concertée.

1.3.2.6 Continuité de gestion de QoS sur les réseaux de transport

Les réseaux de transport IP ont leur propre gestion de QoS. Afin d'en tirer le meilleur profit pour le LTE, le 3GPP permet de traduire les marquages QCI en marquages DSCP sous la forme de tables interprétables par les réseaux IP.

La déclinaison des tables n'est pas imposée par la norme et obéit à des spécificités propres à chaque réseau de transport IP. La déclinaison des tables de marquages QCI-DSCP relève de la responsabilité des gestionnaires de réseau. Le gestionnaire de réseau RRF doit indiquer comment sont marqués ses flux à l'interface de son réseau. Il est de la responsabilité du réseau partenaire de re-marquer ces flux. Le réseau partenaire doit garantir la gestion de la qualité de service par flux, libre à lui de mettre en place la solution technique (par exemple, intégration du marquage dans son encapsulation des messages) tant qu'elle permet de garantir au RRF que la gestion de la qualité de service est assurée de manière adéquate pour chaque flux. Quel que soit le marquage effectué sur un réseau partenaire, les flux doivent satisfaire aux critères de performance imposés par l'ACMOSS. Le gestionnaire de réseau partenaire reste libre des moyens à mettre en œuvre pour les satisfaire.

1.3.3 CONFIGURATION RADIO

1.3.3.1 Usage de spectre : gestion des fréquences

Les fréquences 700MHz PPDR affectées au Ministère de l'Intérieur sont composées de :

- (Obligatoire)La bande 28 constituée de 2 x 3 MHz ;
- (Optionnelle)La bande 68 constituée de 2 x 5 MHz.

Les deux configurations autorisées sont les suivantes :

- Utilisation du 2x3 MHz ;
- Utilisation du 2x3 MHz en bande maitresse (bande 28) et du 2x5 MHz comme bande capacitaire (bande 68)

1.4 DIMENSIONNEMENT

1.4.1 PERFORMANCE RADIO DE REFERENCE ET COUVERTURE

Le Ministère de l'Intérieur souhaite s'assurer que la couverture offerte par les réseaux réponde au niveau de service requis. Les capacités du réseau à fournir du débit varient suivant l'atténuation entre l'eNodeB et les terminaux.

On entend par :

- « **Périmètre nominal** », l'usage dans le périmètre courant d'une cellule. Le Ministère de l'Intérieur considère la limite du « périmètre nominal » au seuil de service de la vidéo sens montant :
    - Si 2*3 MHz bande 28 seule : 2 Mbit/s
    - Si 2*3 MHz bande 28 + 2*5 MHz bande 68 : 5 Mbit/s

  Le Ministère de l'Intérieur requiert que ce seuil soit atteint sur l'ensemble de la zone de travail quotidien de son personnel dans l'emprise du réseau partenaire.

- « **Périmètre étendu** », l'usage jusqu'en bordure de couverture d'une cellule et cela dans tous les cadres géographiques d'emploi (extérieur, bâtiments, parkings, sous-sols, souterrains, masques physiques…). Le Ministère de l'Intérieur considère la limite du « périmètre étendu » au seuil de service de la voix sens montant (128kbit/s). Cette limite correspond à la zone où l'utilisateur régalien est sous la protection de l'appel de détresse vers le réseau.

La définition des périmètres par le partenaire tient compte des spécifications radio des terminaux homologués par le Ministère d'Intérieur.

Le gestionnaire de réseau partenaire fournit, avec son projet, les zones de couverture sur son emprise mettant en évidence les périmètres nominaux et étendus, en extérieur et en intérieur sur lesquelles il est prêt à s'engager en utilisant les fréquences du Ministère de l'Intérieur.

1.4.2 USAGES ET FLUX ASSOCIES

Les réseaux partenaires prennent en compte les usages des utilisateurs RRF dans leur conception.

En dehors de problèmes de capacité et en usage normal, un terminal doit pouvoir sur le périmètre nominal :

- Echanger de la voix (MCPTT, VoLTE,.) selon tout mode de fonctionnement opérationnel ;
- Accéder à toutes ses applications métier et plus globalement à son intranet ;
- Accéder à internet dans la limite des règles de sécurité autorisées par son gestionnaire de flotte ;
- Lire une vidéo en temps réel et en streaming ;
- Envoyer une vidéo visant une lecture en temps réel et en streaming ;
- Bénéficier des usages bureautiques courants ;
- Recevoir/envoyer une photo de 100 Ko à plusieurs Mo.

En termes d'acheminement, il est primordial que la technique ne contraigne pas les usages fonctionnels justifiant des temps d'attente compatibles avec les usages opérationnels les plus courants.

Pour caractériser les flux associés aux usages du Ministère de l'Intérieur, nous définissons trois situations de fonctionnement :

1/ Usage normal : correspond à un trafic prévisionnel statistique d'usage « quotidien » (missions quotidiennes essentielles) dit « à l'heure chargée ». Les réseaux partenaires et RRF sont conçus et dimensionnés pour écouler ce trafic. En usage normal, il est nécessaire de se rapprocher le plus possible d'une garantie minimale de trafic prioritaire pour desservir les utilisateurs et les flux les plus prioritaires de chaque organisation présente sur site (tant utilisateurs RFF que partenaires). Chaque entité peut disposer d'un minimum garanti (mais non réservé) de bande passante.

2/ Usage de crise : répond à un trafic imprévu et disproportionné correspondant à la gestion d'un évènement exceptionnel par son ampleur, sa durée, son impact (par exemple panne du réseau, incendie, accident, attentat). Des mécanismes doivent être mis en place pour s'assurer qu'en dehors des activations des plans de crise, aucun des acteurs ne puisse se retrouver momentanément sans aucune garantie d'un minimum de communications par cellules.

En situation de crise, il faut s'assurer conformément au plan de crise :

- Les contextes sont partagés, à savoir que la crise est connue de tous ;
- Les usages non prioritaires sont identifiés et stoppés soit par consignes aux personnels, soit par l'exploitation, soit par le(s) gestionnaire(s) de communications (MCx) ;
- Une part de la ressource reste disponible pour les usages du réseau partenaire.

Les paramètres techniques permettant ce partage de ressource et de bande passante doivent être discutés et revus entre les parties.

1.4.3 DIMENSIONNEMENT DES CAPACITES

1.4.3.1 Principes généraux de dimensionnement

Les capacités du réseau partenaire doivent répondre à un trafic prévisionnel statistique d'usage normal. Ces capacités minimales doivent être définies avec l'ACMOSS à la conception du réseau partenaire. Les éléments nécessaires à l'élaboration de ce dimensionnement sont :

- Le nombre et la répartition géographique des utilisateurs (terminaux portatifs ou modems) ;
- Le modèle de trafic de chacun des groupes d'utilisateurs (terminaux portatifs ou modems) ;
- Les éléments techniques de performances des solutions sur la bande 700 MHz visée.

Il est rappelé que la situation de crise n'est pas à dimensionner dans le design et la conception du réseau. En revanche, une réponse de type « best effort » doit être fournie par les mécanismes de préemption mis en œuvre localement au profit des forces de sécurité.

En période de crise, il convient de permettre aux équipes et aux équipements impliqués dans la crise de bénéficier du maximum des ressources disponibles sur les réseaux via les mécanismes de priorités vu en section §1.3 « Paramétrages ».

La bande passante est garantie par conception en tout point de l'emprise.

1.4.3.2 Evolution des flux

On entend par utilisateur actif tout terminal opérant au moment de la mesure de charge.

En cas de croissance d'un flux non anticipée lors du dimensionnement initial (validé en début de projet : (**Livrable 2**) émanant des utilisateurs RRF visiteur sur un réseau partenaire, des analyses doivent être faites par les parties pour en mesurer les impacts notamment en termes de bande passante. Ce surcoût de bande passante est défini par utilisateur actif (ex : + x kbps/utilisateur actif). Les mesures d'impacts effectuées seront échangées et validées par les parties.

Si le supplément de flux par utilisateur actif est dans la limite de 5% d'augmentation par rapport au dimensionnement initial global*, alors ce surcoût de bande passante est totalement pris en charge par le réseau partenaire et ce, de manière transparente pour le visiteur. Le « dimensionnement initial » courant prévu pour est le besoin en bande passante défini à l'initiation du projet et réévalué à chaque renouvellement régulier d'autorisation d'usage des fréquences (en général, tous les dix ans).

Si le supplément de flux par utilisateur actif va au-delà des 5% d'augmentation par rapport au dimensionnement initial*, alors la prise en compte de ce surcoût sera convenue entre les parties. Dans l'attente ou en l'absence d'accord, le réseau partenaire n'est pas tenu d'écouler tous les flux critiques supplémentaires.

L'ACMOSS précisera le dimensionnement initial* pour les besoins en usage normal du RRF, car le réseau partenaire peut prévoir dès le départ les % de capacité supplémentaire. En effet, il risque d'être très difficile d'augmenter après déploiement la capacité du réseau sans refaire complètement l'ingénierie de déploiement radio (avec des coûts très conséquents)

1.4.3.3 Evolution des effectifs actifs

En cas d'évolution à la hausse d'un périmètre régalien visiteur (i.e. afflux d'usagers régaliens) de manière régulière ou permanente sur un site d'un réseau partenaire, le redimensionnement du réseau lié à cet afflux doit être :

- Totalement pris en charge par le réseau partenaire et ce, de manière transparente pour les utilisateurs actuels si le surplus d'utilisateurs actifs est dans la limite de 5% d'augmentation de l'effectif actif initialement prévu ;
- Convenu entre les parties si le surplus d'utilisateurs actifs va au-delà des 5% d'augmentation de l'effectif actif initialement prévu.

« L'effectif actif » initialement prévu est l'effectif actif pris en compte à l'initiation du projet et réévalué à chaque renouvellement régulier d'autorisation d'usage des fréquences (en général, tous les 10 ans).

Si le réseau partenaire recouvre plusieurs zones d'emprises alors la mesure d'effectif actif est faite par rapport aux zones d'emprises concernées par tout nouvel afflux supplémentaire d'usagers régaliens réguliers ou permanents.

Si le renouvellement d'autorisation d'usage des fréquences n'obéit pas à la régularité habituelle de 10 ans de durée, cette mise à jour de l'effectif actif doit être (re)vue entre les parties.

1.5 SECURITE

L'ACMOSS et le partenaire sont respectivement responsables de la sécurisation de leur propre réseau. Les deux réseaux doivent être cloisonnés de manière étanche afin d'éviter toute propagation d'attaque informatique.

Les partenaires s'accordent pour mettre en œuvre les bonnes pratiques de sécurisation de leur réseau radio. La mise en œuvre de la sécurisation couvre tous les éléments participant à ce réseau, y compris les terminaux.

Chaque partenaire doit mettre en œuvre les règles de sécurité issues des bonnes pratiques définies par l'ANSSI et le 3GPP. Chaque partenaire est responsable de la mise en œuvre des règles de sécurité pouvant lui être imposées par la législation ou l'ANSSI. Si certaines règles ont un impact sur le partenaire en interface, les partenaires conviennent de se réunir pour échanger sur les éléments à mettre en œuvre pour garantir la tenue des exigences et identifier les moyens nécessaires à l'atteinte de l'objectif de sécurisation.

Les partenaires doivent s'accorder sur la mise en œuvre des infrastructures de gestion des clefs et certificats.

Les exigences techniques spécifiques liées à la sécurité informatique sont décrites dans l'annexe 2.

2 ORGANISATION DE DEMANDE ET DE MISE EN PLACE D'INTERCONNEXION DE RESEAUX

2.1 DEMANDE AUPRES DU MINISTERE DE L'INTERIEUR

Les représentants du réseau partenaire doivent faire parvenir au Ministère de l'Intérieur et à l'ACMOSS une demande préliminaire de délégation de spectre.

Cette demande est réalisée auprès des interlocuteurs suivant :

Ministère de l'intérieur :

Mr Lionel FRION

N° de Téléphone : (+33) 7 85 02 33 42 / Tél : (+33) 1 80 15 50 18

Courriel : lionel.frion@interieur.gouv.fr

ACMOSS :

Mme Claire RAYNAL

Courriel : operateur-acmoss@interieur.gouv.fr

La demande doit intégrer les éléments suivants :

- La zone de couverture spécifiée (Surface/Souterrain) sous forme d'image et de fichier .shp ;
- L'architecture préliminaire de la solution (cœur de réseaux, nombre de points d'émission radio…) ;
- L'usage prévu (nombre d'utilisateurs, type de flux, cible d'utilisation, liste des métiers des utilisateurs du réseau (interne et externe à l'entreprise)….) ;
- Le calendrier de déploiement ;
- La durée d'affectation visée (5, 10 ou 15 années) ;
- Le mode d'interconnexion souhaité avec le RRF :
  - Roaming S8 Home Routing ;
  - Ran Sharing MOCN.
- Le corpus documentaire suivant signé, comprenant :
  - Le document « Référentiel d'interconnexion RRF-réseau partenaire » signé par les parties : ACMOSS, le réseau mobile privé, sous couvert de l'AGURRE
  - L'accord de confidentialité entre le réseau mobile privé et ses partenaires et l'ACMOSS
  - La convention d'exploitation signée

Les intervenants du Ministère de l'Intérieur (DTNUM) fournissent une réponse sous forme de courrier dans un délai de deux mois donnant un accord de principe concernant l'autorisation d'usage du spectre, le cas échant, les intervenants demandent des informations complémentaires au demandeur.

Ce document « Référentiel d'interconnexion RRF-réseau partenaire » signé entre les parties ACMOSS et le réseau mobile privé sous couvert de l'AGURRE sera transmis à la DGE et à l'ARCEP afin de démarrer le processus d'autorisation d'utiliser des fréquences (AUF) 700 PPDR.

La DGE établit le cadre juridique pour les redevances. L'ARCEP établit l'autorisation d'usage de Fréquence.

La demande d'autorisation à l'ARCEP sera précisée ultérieurement.

2.2 PHASE D'ETUDE

Le début du projet est précédé de la signature d'un accord de confidentialité (voir annexe 5.3) entre l'ACMOSS, l'entité exploitant le réseau partenaire, le réseau mobile privé, les sous-traitants de chaque entité.
Par la suite une réunion de lancement est initiée entre les représentants respectivement désignés du côté de l'ACMOSS et du réseau partenaire. Cette réunion vise à définir le contenu du plan de management du projet de raccordement (PMP). Ce PMP décrit :

- L'organisation projet mise en œuvre au sein des deux entités ;
- La cartographie des participants ;
- Quand et Comment solliciter les participants ;
- Les jalons clés ;
- Le dispositif de pilotage projet (réunion d'avancement et pilotage, processus d'escalade…) ;
- Le planning de mise en œuvre ;
- La liste des livrables prévue ;

Le PMP est produit par l'équipe technique du réseau partenaire. Il constitue le premier livrable du projet (**Livrable 1**).

L'équipe de l'ACMOSS est ensuite chargée de réaliser une étude visant à estimer le trafic qui sera généré par ses utilisateurs au sein du réseau partenaire en situation d'exploitation normale et en charge (heures de pointe ou évènements d'ampleurs réguliers), (mais hors situation de crise ?). Cette étude précise ainsi :

- Le nombre d'utilisateurs de l'ACMOSS susceptibles d'intervenir sur le réseau partenaire découpé par zone ;
- Le profil d'abonné moyen de chaque utilisateur ;
- La localisation projetée des utilisateurs sur le réseau visité.

L'étude de trafic de l'ACMOSS constitue le deuxième livrable de l'étude (**Livrable 2**).

L'équipe projet (constituée d'intervenants de l'ACMOSS et du réseau partenaire) doit ensuite produire la spécification d'interface. Celle-ci doit préciser :

- Les points de raccordement physiques et logiques entre le RRF et le réseau partenaire ;
- La liste des paramètres spécifiques à l'interfaçage entre le RRF et le réseau partenaire ;
- La nature des mécanismes de sécurisation des liens ;
- La spécification des interfaces destinées à la supervision des réseaux ;
- La matrice de responsabilité des différentes interfaces (mise en œuvre, exploitation) ;
- Le bordereau de raccordement ;

Cette spécification d'interface constitue le troisième livrable de l'étude (**Livrable 3**).

Le réseau mobile privé et l'ACMOSS définissent une convention d'exploitation qui fixera les responsabilités et les limites d'intervention de chacun sur les réseaux et les interfaces ainsi que les modalités d'exploitations en accord avec les principes qui sont définis dans la section §3 « Modalités d'exploitation ».

Ce document définit en particulier :

- La durée de la convention ;
- Les prestations de maintenance préventives et correctives ;
- La supervision et l'administration des interfaces ;
- La gestion des incidents ;
- La gestion des évolutions.

Cette convention d'exploitation constitue le **Livrable 4** « Exploitation ».

Pour tenir compte des exigences de sécurité informatique, le partenaire doit disposer d'un plan

d'assurance cybersécurité ainsi qu'un plan de tests et de recette de la cybersécurité (contrôle, vérification, évaluation). Ces documents doivent tenir compte de l'interface avec le RRF.
Le partenaire détaille pour chaque interface avec le RRF une matrice d'exigences cybersécurité, avec pour chacune une méthode de validation et les procédures d'essai adéquates. Les essais porteront sur la vérification de la mise en place de mesures techniques sur le périmètre de chaque interface :

- Mesures de durcissement (désactivation des composants, des comptes, des ports inutiles, des fonctions non utilisées, etc…) ;
- Mise en place de mesures de renforcement des protections suivant les recommandations des constructeurs et de l'ANSSI ;
- Mesures de sécurisation réseau : authentification, filtrage, cloisonnement, chiffrement, etc…

Le partenaire décrit dans son plan d'assurance cybersécurité les processus organisationnels liés à la gestion de la cybersécurité, notamment les modalités de sollicitation du SOC (security operational center) du partenaire.

Les essais peuvent être réalisés sur plateforme de tests et complétés sur les systèmes installés.
Le livrable « Sécurité » constitue le **Livrable 5**.

Pour finir l'équipe projet établit le cahier de recette visant à valider le fonctionnement des interfaces. Ce cahier de recette constitue le **Livrable 6** et décrit :

- Les configurations de tests à mettre en œuvre ;
- Les moyens humains et matériels à mobiliser ;
- Les protocoles de tests à suivre ;
- Les résultats attendus ;
- Le formalisme de restitution des tests (fiches, fichiers de suivi…).

Les objectifs des tests reflètent les spécifications. On identifie les types d'anomalies pouvant être rencontrées durant la phase de tests :

- Critique : Désigne toute anomalie empêchant l'accomplissement d'une exigence fonctionnelle ou technique indispensable pour l'exploitation sans aucune possibilité de contournement ;
- Majeure : Désigne toute anomalie empêchant l'accomplissement d'un exigence fonctionnelle ou technique majeur, mais dont il existe un contournement (La solution de contournement doit être acceptable pour les utilisateurs, mainteneurs et administrateurs …) ;
- Mineure : Désigne toute anomalie qui n'est ni critique, ni majeure ;

Le partenaire et l'ACMOSS s'accordent sur la réalisation de tests en usine ou sur une plateforme de test reproduisant les conditions de raccordement pour s'assurer du fonctionnement de ses solutions, sans que cela ne le dédouane de la validation des interfaces en conditions réelles.

Lors de la réalisation de tests de bout en bout, de tests de couverture et de performances, il est demandé au partenaire d'utiliser des terminaux du même type que ceux utilisés par l'ACMOSS, ou prêtés par l'ACMOSS le cas échéant (avec les cartes SIM adéquates et configurés pour fonctionner avec le cœur de réseau du RRF).
Le cahier de recette précise le séquencement des différentes phases de tests, des différents tests unitaires aux tests d'intégration.
Le cahier de recette constitue le sixième et dernier livrable de l'étude (**Livrable 6**).

2.3 PHASE DE MISE EN ŒUVRE

La phase de mise en œuvre peut commencer après la réunion de lancement avec le Ministère de l'Intérieur. Les exploitants respectifs du réseau partenaire et du RRF ont la responsabilité de déployer puis de valider les interfaces qui ont été définies dans le **Livrable 3**.
Dans un premier temps, le Partenaire doit réaliser le raccordement physique et logique des deux

réseaux selon les spécifications et le type d'architecture choisi :

- Création de liens de connexion (fibres optiques) entre les points d'interfaçage ;
- Création de circuits permettant de joindre les points d'interfaçage sur des réseaux de communication existants (fibres noires) ;
- Raccordement d'équipements (switches, routeurs, serveurs…).

Le Ministère de l'Intérieur de son côté a la responsabilité de fournir les points d'interfaçage à son réseau, et de permettre l'accès physique des personnels du Partenaire aux équipements désignés pour réaliser les raccordements et les configurations. Le Ministère de l'Intérieur réalise l'installation des équipements sous sa responsabilité et leurs paramétrages.
Les liens physiques ainsi créés sont ensuite configurés pour répondre aux besoins du type particulier d'interface, avec les paramètres qui ont été définis en collaboration avec le Ministère de l'Intérieur dans le **Livrable 3**.

Pour les paramétrages et les configurations, le Ministère de l'Intérieur et le Partenaire se concerteront pour effectuer ces actions, chacun sur son propre réseau. Pour assurer un bon déroulement du déploiement, les deux parties désignent chacune un responsable chargé de s'assurer de la bonne implémentation des équipements et de recueillir les besoins de l'autre partie.

Le partenaire peut dans un premier temps réaliser les tests sur sa propre plateforme ou sur une plateforme constructrice s'il en a la possibilité, avant de les reproduire en conditions réelles. La plateforme de tests doit reproduire les réseaux et interfaces avec les mêmes équipements et configurations, et permettre les vérifications nécessaires sans impacter le fonctionnement des réseaux réels.
Lorsque cette étape est terminée, et après une première vérification en interne de la conformité des installations et des configurations, le Partenaire avertit le Ministère de l'Intérieur et demande à commencer les tests de recette des interfaces, tel que définis dans le **Livrable 6**.

Le Ministère de l'Intérieur ainsi que le Partenaire fournissent les moyens humains et techniques nécessaires à cette opération en fonction des besoins de chaque côté des interfaces :

- Responsables des recettes, ingénieurs, techniciens ;
- Moyens généraux tels que véhicules, PC, téléphones, suites logicielles standards, etc… ;
- Moyens particuliers : équipements de tests spécialisés (réflectomètres, analyseurs de protocoles, autres) ;

Les interfaces sont testées en suivant les procédures définies dans le cahier de recettes. Les résultats sont consignés sur des fiches pour chaque test, avec les défauts constatés le cas échéant.
Le partenaire informe le Ministère de l'Intérieur de l'avancement des essais, et de la résolution des anomalies si nécessaire. A la fin du déroulement du cahier de tests, un rapport de tous les essais réalisés est rédigé. Il intègre la liste des réserves avec les informations concernant leur gravité (Mineure/Majeure/Bloquante) et un planning estimatif de leur résolution.
Le rapport liste et précise la nature des réserves :

- Réserves non bloquantes : Exprimées lorsque des anomalies mineures ont été relevées. La réception du système ne peut être prononcée mais les acteurs s'engagent à corriger ces anomalies dans des délais précisés lors de l'expression de ces réserves
- Réserves bloquantes : Exprimées lorsque des anomalies critiques ou majeures ont été constatées. La levée de ces réserves conditionne la réception du système Les acteurs doivent résoudre au plus tôt les dysfonctionnements détectés afin que la qualité du système soit garantie

L'acceptation de la recette des interfaces est réalisée de concert par le Ministère de l'Intérieur et le partenaire selon les conditions fixées dans le **Livrable 6**.

Lorsque la recette d'interface montre des résultats concluants selon les conditions fixées dans le **Livrable 6**, le Partenaire demande le lancement de la recette de bout en bout, qui inclut les

interfaces et les deux systèmes radio. Cette recette a pour but de vérifier, notamment, les fonctionnalités du réseau partenaire et ses performances lorsqu'un ou plusieurs terminaux du Ministère de l'Intérieur font du roaming sur ce réseau.

Les résultats sont consignés sur des fiches pour chaque test afin de valider le fonctionnement de l'ensemble du système impliquant le réseau Ministère de l'Intérieur et le réseau partenaire.
L'ensemble des anomalies qui peuvent être constatées sont notées en fonction de la nature et de la gravité de l'anomalie, et aussi en fonction du réseau responsable de cette dernière.

Lorsque le Ministère de l'Intérieur ainsi que son partenaire estiment que la recette bout en bout est concluante selon les conditions fixées dans le document de recette globale, la mise en service opérationnelle peut être effectué.

Celle-ci s'accompagne d'une mise à jour des livrables « Sécurité » (**Livrable 5**) et « Exploitation » (**Livrable 4**) avec la liste des cyber-risques résiduels, et les remarques et commentaires sur les procédures d'exploitation qui seraient apparus lors des phases d'installation et de recette des interfaces.

Un **PV de basculement** en opération doit être rédigé indiquant le lancement en opération du réseau partenaire. Une période de Vérification de Service Régulier (VSR) peut être requise par le Ministère de l'Intérieur, d'une durée à déterminer par les parties et avec des conditions de sortie à définir.
Au terme de cette période, le réseau partenaire est considéré comme apte au service, dans cette configuration.

Lorsque le réseau est considéré comme apte au service, ce dernier doit être en mesure d'offrir des garanties au niveau de la continuité de service. C'est pour ça qu'il est important de garantir la sécurité du réseau et son exploitation.
Le partenaire et le RRF doivent être en mesure de garantir la sécurité du réseau tant sur le plan des menaces physiques (vandalisme, catastrophes naturelles…) que sur le plan des menaces informatiques (surveiller les accès non autorisés, l'utilisation abusive, la modification ou le refus des ressources accessibles sur le réseau…).
En plus de la cyber sécurité, le partenaire propose un système de maintenance et d'exploitation avec pour but d'optimiser le fonctionnement du réseau et d'apporter si cela est nécessaire des actions correctives ou préventives.
L'exploitation du réseau implique pour le partenaire la prise en compte de différents points importants :

- La fourniture du personnel ainsi que des outils dédiés ;
- La maîtrise complète des équipements qui constituent le réseau ;
- La mise en place de protocoles d'interventions à suivre ;
- Les résultats attendus en fonction des cas.

A l'issu de la période de VSR, le Partenaire rassemble dans un référentiel d'exploitation :

- Les résultats de couverture (surface totale de couverture outdoor/indoor, pourcentage de couverture…) ;
- Les performances des différents indicateurs de performances (puissance du signal reçu, qualité du signal reçu, handover…) ;
- Les configurations des équipements et des interfaces.

Ce référentiel d'exploitation doit être utilisé par le partenaire pour garantir le fonctionnement optimal du réseau pendant toute la durée de la convention avec le Ministère de l'Intérieur.

3 MODALITES D'EXPLOITATION

Les prestations attendues par l'ACMOSS sur les réseaux partenaires sont toutes les actions permettant le maintien en condition opérationnelle des systèmes et infrastructures qui contribuent au bon fonctionnement du réseau.
Ces prestations sont définies en détail lors de la signature de la convention d'exploitation, permettant de spécifier les conditions et modalités du service de maintenance, le SLA.
A minima, la convention aborde les points suivants :

- Les rôles et les responsabilités de l'ACMOSS et du partenaire (plan de management de maintenance avec matrice RACI si besoin) ;
- La durée de la convention et les conditions, modalités de résiliations ;
- Le périmètre et les référentiels techniques (architectures, interfaces, configurations, performance, disponibilité, couverture) de référence d'exploitation ;
- Les prestations attendues et plus particulièrement les engagements de maintenance en termes de Garantie du Temps de Résolution (GTR) ;
- Les processus autour de la gestion des évolutions et des qualifications associées ;
- Les outils, procédures et indicateurs permettant le pilotage de la maintenance ;
- Les limites de la prestation (par exemple mise à disposition des terminaux pour les utilisateurs RRF).

3.1 DUREE DE LA CONVENTION

Sauf mention contraire, la durée de la convention est calée sur la durée d'affectation de la délégation de fréquence.

3.2 PRESTATIONS DE MAINTENANCE

Les responsabilités du RRF et des réseaux partenaires sur l'administration, la supervision, le paramétrage, la maintenance et la qualification des réseaux sont les suivantes:

- Chaque partie est responsable de la supervision, de l'administration et de la maintenance de son réseau ;
- Chaque partie s'engage à maintenir son réseau en état de fonctionnement selon le niveau de service attendu ;
- Chaque réseau doit supporter le bon fonctionnement du transport des flux de données des utilisateurs RRF :
    - Par le respect des configurations de référence des réseaux et des terminaux ;
    - Par une résolution partagée des problèmes ;
    - Par une information réciproque des états courants et planifiés des réseaux ;
    - Par une vision partagée et planifiée des évolutions ;
    - Par une qualification des évolutions des réseaux et des terminaux ;

Les principales prestations attendues par l'ACMOSS des exploitants des réseaux partenaires sont :

- La gestion des incidents - en jours et heures ouvrés et non ouvrés – y compris les incidents de cyber sécurité ;
- La gestion des évolutions ;
- Le pilotage et le suivi de la convention d'exploitation.

3.3 GESTION DES INCIDENTS

La convention d'exploitation doit spécifier l'organisation et le processus autour de la gestion des incidents.

Un incident est tout événement qui sort du cadre d'exploitation normal du service principal et qui entraîne une interruption ou une dégradation du service. L'objectif principal du processus de gestion des incidents est de restituer le service dans les délais les plus courts en minimisant l'impact sur les utilisateurs.
En cas d'incident cyber sécurité, l'objectif est d'évaluer les risques de propagation et de limiter l'extension de l'incident au RRF (ou inversement, au réseau partenaire).

L'appréciation du niveau de criticité d'un incident est déterminée en fonction du niveau d'impact et d'urgence.

- Le niveau d'impact est déterminé en fonction du volume et de l'ampleur de l'incident et de son effet sur les utilisateurs.
- Le niveau d'urgence est déterminé en fonction de l'intensité de l'incident par rapport à l'activité de l'utilisateur. Il traduit l'intensité opérationnelle, géographique ou temporelle (élévation du niveau d'intensité lié à un événement particulier : grande manifestation…) du dysfonctionnement.

La convention définit à minima pour chacune des parties :

- Les engagements de résolution d'incidents et plages horaires associées (GTR, Heures ouvrés, Heures non ouvrées) ;
- Les différents cas de pannes et leurs criticités associées ;
- Les modalités de signalement d'incidents entre le RRF et les réseaux partenaires (Outillage de suivi des incidents, organisation) ;
- Les modalités d'isolement des réseaux en cas d'incident cyber sécurité à risque de propagation ;
- La matrice d'escalade.

Le RRF et les réseaux partenaires communiquent sur les incidents ou opérations planifiées ayant lieu sur leur réseau et ayant un impact sur le réseau partenaire (perte de lien, coupure des équipements interconnectés…).

Dans certains cas, des dispositifs d'interconnexion, permettant le partage d'alarmes, le partage d'outils de suivi d'incident, de visualisation d'alarmes peuvent être étudiés et mis en place suivant la faisabilité technique.

3.4 INTERRUPTIONS PROGRAMMEES

Des opérations de maintenance préventive ou de mise en production sont nécessaires pour garantir le bon fonctionnement du service. Ces opérations peuvent nécessiter des interruptions de service.

La convention d'exploitation doit décrire à minima :

- Les modalités d'organisation et de communication entre les parties dans le cadre d'opérations planifiées ayant une incidence sur le service ou sur le risque d'incidence (moyens de communication, préavis, délais de confirmation de prise en compte, …) ;
- L'analyse des impacts à fournir lors de la notification des interruptions programmées.

Dans certains cas exceptionnels, il est possible qu'une des deux parties soit contrainte de procéder à une interruption urgente du service dans le cadre d'une opération de maintenance pour laquelle il n'est pas possible de respecter un préavis. Dans ce cas, les responsables du réseau (RRF ou réseau partenaire) sont informés de l'impact de l'opération sur le service.

3.5 VIE DU RESEAU

Chaque réseau est responsable de son administration et de sa configuration et veille à respecter le cadrage validé en phase projet consolidé dans le référentiel d'exploitation (Livrable 4, et annexé à la convention).

La définition du référentiel d'exploitation se réalise en phase projet et est validée à l'issue de la Vérification de Service Régulier (VSR).
Le référentiel d'exploitation définit a minima :

- Les architectures des réseaux (RRF et réseau partenaire) et si besoin de leurs plateformes ;

- La configuration de référence des réseaux de production ;
- Les interfaces entre les deux réseaux ;
- Les indicateurs de performance et de disponibilité (KPI attendus, méthodologies de calcul et seuils) ;
- Le référentiel de couverture ;
- Le référentiel du dimensionnement de flux critiques demandés par l'ACMOSS et l'effectif actif ;
- Le référentiel des terminaux (matériel et logiciel) utilisés par RRF sur le réseau partenaire.

La convention d'exploitation doit définir les modalités de mise à jour de ce référentiel. Cette mise à jour peut être due à :
- Une évolution du RRF ou du réseau partenaire ;
- Un incident dans le cadre de la gestion des incidents. Dans ce cas, les responsables du réseau (RRF ou réseau partenaire) sont informés de l'impact de l'opération sur le service.

3.6 GESTION DES EVOLUTIONS

Les architectures du RRF et des réseaux partenaires respectent les standards du 3GPP.

Ainsi, durant leur cycle de vie, les réseaux partenaires ainsi que le RRF vont subir de nombreuses modifications et peuvent rencontrer aussi des anomalies, incidents ou des non-conformités justifiant une évolution. Le périmètre des évolutions inclut également la qualification préalable des terminaux.

La proposition d'évolution peut venir du RRF et/ou du réseau partenaire.

Chaque processus d'évolution passe par les étapes suivantes :
- Description et justification de l'évolution ;
- Evaluation des impacts de l'évolution (stratégie de tests, critères de succès…) ;
- Approbation ou refus de l'évolution ;
- Qualification de l'évolution (tests, levées de réserves…) ;
- Mise en œuvre de l'évolution et suivi de son application (généralisation).

Chaque partie cherche à valider au maximum au sein de son réseau les évolutions afin de minimiser les démarches impliquant les deux parties.

La convention d'exploitation décrit a minima :
- L'organisation (acteurs, rôles, outillage et moyens humains et matériels mis à disposition) ;
- Les procédures : définition de l'évolution (mineure ou majeure), évaluation des impacts, processus de mise en œuvre (conception, tests, mise en production…) ;
- Le suivi des évolutions et le partage des prévisions d'évolutions (roadmap) à court et moyen terme en cohérence avec les stratégies techniques respectives du RRF et du réseau partenaire ;
- Le partage réciproque des revues de gestion de l'obsolescence et des schémas directeurs d'évolutions des matériels et logiciels déployés sur les réseaux.

Les dispositions croisées suivantes sont imposées entre les partenaires :
- Le gestionnaire du RRF peut s'opposer à la généralisation d'une évolution du réseau partenaire qui apporterait une régression des services à ses utilisateurs ou un risque majeur (par exemple sur la sécurité) ;
- Les gestionnaires de réseaux partenaires peuvent s'opposer à la généralisation d'une évolution du RFF qui apporterait une régression sur les services à ses utilisateurs ou un risque majeur (par exemple sur la sécurité) ;
- Les gestionnaires des réseaux partenaires comme le gestionnaire du RRF ne sauraient faire évoluer leur réseau sans une procédure de qualification croisée préalable effectuée en coopération ;
- Les gestionnaires des réseaux partenaires doivent apporter les ressources nécessaires à la qualification et au déploiement des évolutions de réseaux, des applications, des interfaces et des terminaux du RRF ;

- Le gestionnaire du RRF doit apporter les ressources nécessaires à la qualification et au déploiement des évolutions de réseaux, des applications, des interfaces et des terminaux des réseaux partenaires.

3.7 PILOTAGE ET SUIVI DE L'EXPLOITATION

Deux instances de coordination ci-après sont à prévoir pour réaliser le suivi de la convention d'exploitation :

- Le comité technique est organisé semestriellement a minima et traite des aspects suivants :
  - Suivi des incidents (ouverts, clôturés, identification des retours d'expériences, escalades) et de la conformité des engagements définis dans la convention ;
  - Partage des interruptions programmées ;
  - Partage réciproque des évolutions prévues et organisation de la gestion des évolutions à prévoir ;
  - Demandes spécifiques vis-à-vis d'événements exceptionnels.
- Le comité de pilotage a un rôle de suivi général et d'arbitrage lié au fonctionnement des réseaux. Organisé annuellement, ce comité de pilotage traite des aspects suivants :
  - Suivi des engagements réciproques ;
  - Suivi des KPI du réseau partenaire définis dans le référentiel (évolution des flux critiques, évolution de l'effectif actif, couverture) ;
  - Partage réciproque des revues de gestion de l'obsolescence et des schémas directeurs d'évolutions des matériels et logiciels déployés sur les réseaux (facultatif) ;
  - Examen des demandes qui sortent du domaine de la convention.

4 OBLIGATIONS – SYNTHESE DES EXIGENCES

Liste des exigences	
Exigence 1	Les architectures du réseau régalien et des réseaux partenaires respectent les standards du 3GPP et en particulier ceux de la technologie LTE (Long Term Evolution) et leurs évolutions.
Exigence 2	Au fur et à mesure des progrès, des évolutions normatives et du développement du RRF, l'ACMOSS se réserve le droit de réclamer des implémentations au cas par cas. Ce processus sera négocié à l'issue d'une étude d'impact menée conjointement entre les parties.
Exigence 3	Afin de prendre en compte les évolutions de la norme LTE, le référentiel technique d'exigences sera mis à jour régulièrement. Toute révision fera l'objet de partage au sein du groupe de travail comprenant l'AGURRE, l'ACMOSS, l'ARCEP.
Exigence 4	Les membres du groupe de travail en charge des modifications du référentiel technique d'exigences devront être représentatifs de la totalité des parties tant côté RRF que côté réseaux partenaires. Cette représentation continuera d'être assurée quelles que soient les évolutions futures de la structure de gouvernance en charge du RRF.
Exigence 5	L'ouverture en usage dérogatoire des fréquences PPDR vers des partenaires extérieurs impose d'en garantir l'usage aux forces régaliennes déployées sur site d'un réseau partenaire.
Exigence 6	Le ministère de l'intérieur conditionne la mise à disposition des fréquences PPDR à des exploitants dont tout ou partie des usages concoure directement et indirectement à la sécurité des biens et des personnes.
Exigence 7	Un réseau partenaire est un réseau contingenté et cloisonné sur certaines portions du territoire. Un réseau partenaire pourra se limiter à une ou plusieurs bulles circonscrites, ou bénéficier d'une ou plusieurs distributions linéiques (emprises extérieures ou souterraines) sur le territoire ou bien les deux.
Exigence 8	Le réseau partenaire doit garantir la capacité de son réseau à transmettre les flux des utilisateurs de tout type : • Les appels Voix sur LTE • Les usages MCX avec les services MCPTT, MCVidéo, MCData • L'envoi et la réception de SMS et de MMS, • L'usage data, porté par l'APN data. Ce flux sera encapsulé par des VPN.
Exigence 9	Les terminaux en usage par les abonnés du RRF doivent être homologués sur le réseau partenaire. Des protocoles de validation des terminaux sont définis entre les parties.
Exigence 10	Le réseau partenaire doit garantir un niveau de sécurisation adéquat au niveau de la couche LTE basé sur la norme 3GPP. Ce niveau n'exclut pas l'adjonction de niveaux de sécurisation supérieurs par tunnelisation ou de type applicatif
Exigence 11	Le réseau partenaire doit s'assurer que les adjonctions de niveaux de sécurisation ne compromettent pas le service pour les usagers
Exigence 12	Aucune des parties ne saurait s'octroyer de manière unilatérale l'exclusivité d'une des sous-bandes allouées (2x3 et 2x5 MHz). A cet effet, un partenaire reste libre de déployer les sous-bandes selon les besoins à satisfaire mais ne pourra pas refuser l'accès d'une sous-bande déployée à un visiteur.

Liste des exigences	
Exigence 13	Les réseaux partenaires et RRF doivent étudier et dans la mesure du possible mettre en place les mécanismes permettant de maintenir la continuité d'une communication établie par un utilisateur RRF entre leurs réseaux dans le cas où ils se recouvriraient radio-électriquement (par exemple, par handover) : • en mode veille ; • en mode connecté avec maintien des sessions, sans rupture des flux temps réels (ex : parole, vidéo…)
Exigence 14	Tous les sites radios émettant sur les fréquences PPDR du MI en 700 MHz doivent pouvoir accueillir les usagers du RRF afin de remplir leur mission de sécurité et de secours en liaison avec les forces de sécurité et le commandement environnants. L'usage du spectre doit respecter strictement le canevas de qualité de service défini entre et avec les partenaires et en aucun cas, les usagers RRF ne sauraient être exclus des services offerts sur tout ou partie des réseaux partenaires
Exigence 15	Les gestionnaires de réseaux doivent garantir la priorisation et la capacité de préemption des flux liés aux missions d'assistance et de sécurité des personnes sur les autres flux, tel que spécifié dans l'étude de dimensionnement, dans la limite du maintien de la ressource suffisante au réseau d'accueil pour pouvoir répondre à ses besoins critiques.
Exigence 16	Les gestionnaires de réseaux doivent garantir les échanges protocolaires entre les réseaux (partenaire et RRF) permettant aux réseaux partenaires d'enclencher leurs propres mécanismes de priorisation des usages en cas de congestion
Exigence 17	Le réseau partenaire doit présenter les mécanismes de résilience face à des dégradations de leur environnement (énergie, transmissions, rupture aérienne …) et garantir un niveau de fonctionnement minimal en cas de défaillance des composants du réseau.
Exigence 18	Chaque gestionnaire de réseaux a la responsabilité et le contrôle de sa sécurité, de la gestion de ses utilisateurs et de leurs droits sur son réseau
Exigence 19	Dans certains types d'environnement très spécifiques notamment en raison d'une sensibilité nucléaire, radiologique, bactériologique, chimique, explosif, électrique ou autre liées à certains environnements d'emploi, le ministère de l'intérieur peut envisager de déroger à ses dispositions courantes afin de s'adapter aux contraintes spécifiques d'environnement
Exigence 20	Le réseau partenaire doit interdire l'usage de la bande 700 MHz « PPDR » aux terminaux du public et mettre en place des mécanismes permettant de prévenir les trafics pouvant provenir de tous terminaux non autorisés en bande 700 MHz « PPDR »
Exigence 21	Le réseau partenaire souhaitant déployer un réseau peut déployer son réseau suivant l'un des deux types d'interfaçages avec le RRF : une architecture de « Roaming home routed S8 » ou une architecture de « Ran sharing MOCN ».
Exigence 22	Les processus permettant d'assurer la disponibilité du réseau partenaire sont définis de manière concertée en phase d'études.
Exigence 23	Les réseaux partenaires doivent respecter les QCI définis par l'ACMOSS pour répondre aux KPI de bout en bout définis par la norme.
Exigence 24	Les réseaux partenaires se conforment aux conditions d'interconnexions avec le MCX RRF et ses différentes options mises en œuvre par l'ACMOSS. En tout état de cause, le MCX RRF respecte la norme.
Exigence 25	La mise en œuvre des réseaux partenaires et du RRF obéit à une action de planification radio partagée entre les différents gestionnaires d'infrastructure. Cette règle de planification sera maintenue tout au long de la vie du réseau.

Liste des exigences	
Exigence 27	Toute interférence doit être diagnostiquée en commun et son correctif s'impose aux réseaux concernés.
Exigence 28	Le plan de voisinage élaboré en collaboration par chaque réseau partenaire et le réseau régalien est revu régulièrement à la lecture des performances du réseau et des évolutions de l'infrastructure radio de chacune des parties.
Exigence 29	Toute évolution de paramétrage ou de configuration impactant les flux RRF doit respecter la norme. Elle est mise en œuvre de manière concertée après validation entre le réseau partenaire et le RRF.
Exigence 30	Les règles d'emploi des ARP définies par la norme sont strictement respectées.
Exigence 31	Les flux LTE doivent être marqués conformément aux attentes de chacun des réseaux interconnectés en entrée de chaque réseau. Le gestionnaire du RRF indiquera comment sont marqués ses flux à l'interface de son réseau. Le réseau partenaire reste libre des moyens à mettre en œuvre pour satisfaire le service attendu.
Exigence 32	En l'absence de partage de contexte opérationnel et donc d'affectation dynamique des priorités, ces priorités sont implémentées en statique et chaque partie s'engage à en respecter les termes en s'assurant des règles d'interfaçage suivantes : • le réseau visité affecte bien les niveaux de priorités requis par les flux visiteurs ; • le marquage paquet DCSP est conforme à la requête PGW ; • le marquage DSCP sur le réseau de transport est conforme aux tables de marquage IP.
Exigence 33	Le MININT demande de se référer à la normalisation en ouvrant les classes 11 à 15 selon les besoins tant sur le RRF que sur les réseaux partenaires : • 15 et 11 : respectivement PLMN Staff (Personnel opérant le réseau) et PLMN use (usages propres au réseau) • 14 : Emergency Services (Services de secours) : • 13 : Public Utilities (Opérateur d'infrastructures) : • 12 : Security Services (Forces de l'ordre) • les autres utilisateurs amenés à bénéficier du réseau régalien bénéficieront d'une classe d'accès 12 ou 14 pour les utilisateurs régaliens et 13 pour les utilisateurs non-régaliens • les utilisateurs du secours ou de la sécurité dont la gestion est déléguée aux réseaux partenaires bénéficieront d'une classe d'accès en cohérence avec leur emploi, de type 12 ou 14.
Exigence 34	Le réseau partenaire doit avoir une attention particulière sur le strict respect des obligations liées à la sécurité des réseaux et de leurs interconnexions. Ces obligations sont imposées par le gestionnaire du RRF en liaison avec l'ANSSI.
Exigence 35	Une fonctionnalité à usage commun ne peut être mise en œuvre que lorsqu'elle est totalement stabilisée par la norme. Des solutions propriétaires peuvent être momentanément admises mais revêtiront un caractère transitoire dans l'attente de la finalisation de la norme. En tout état de cause, sa mise en œuvre s'établit de manière concertée entre les parties.
Exigence 36	Le réseau partenaire fournit, avec son projet, les zones de couverture sur son emprise et à l'extérieur mettant en évidence les zones de services nominal et étendu, en extérieur et en intérieur.
Exigence 37	Le réseau partenaire s'engage à implémenter l'architecture en réponse au dimensionnement défini en phase études pour les usagers RRF. En cas de constat de dépassement du trafic défini au-delà de cinq pourcents, le réseau partenaire et RFF conviennent d'ajout de ressources après concertation.

Liste des exigences	
Exigence 38	Chaque réseau partenaire doit prendre en compte dans son dimensionnement les besoins de trafic référencés pour un utilisateur RRF. Ce tableau est fourni dans le livrable technique. Il peut être mis à jour de manière concertée entre les parties.
Exigence 39	En usage normal, les réseaux partenaires se doivent de répondre aux débits montants et descendants des utilisateurs régaliens présents sur leur infrastructure et dans la limite des besoins définis. Les débits indiqués dans le tableau référençant les besoins de trafic pour un utilisateur régalien incluent l'encryptage du MI.
Exigence 40	En cas de crise, le gestionnaire de réseau partenaire devra être en mesure de garantir à l'Etat une capacité minimale de communication respectivement dans les zones nominales et étendues
Exigence 41	Les réseaux partenaires devront se montrer en capacité de pouvoir acheminer les flux au point de raccordement défini en concertation avec l'ACMOSS.
Exigence 42	La responsabilité des gestionnaires de réseaux s'arrête aux points de raccordement définis entre le réseau régalien et les réseaux partenaires.
Exigence 43	Au préalable de la mise en service du réseau partenaire, la convention d'exploitation doit être signée avec l'ACMOSS.
Exigence 44	L'ACMOSS se réserve le droit de demander des améliorations à l'exploitant du réseau partenaire s'il observe des écarts dans la conception et/ou l'exploitation du réseau partenaire par rapport aux dossiers d'études et aux dispositifs prévus dans la convention d'exploitation.
Exigence 45	En cas de crise, le gestionnaire du RRF devra pouvoir facilement contacter un administrateur du réseau partenaire selon un processus défini conjointement.
Exigence 46	L'exploitant du réseau partenaire est responsable de mettre en œuvre et exploiter son réseau de manière à respecter les critères de performances définis entre les parties.
Exigence 47	En cas d'altération avérée des performances, l'exploitant est chargé de mener les actions correctives permettant le retour aux performances nominales du réseau.
Exigence 48	Le réseau devra être sécurisé conformément aux préconisations de la norme 3GPP en particulier.
Exigence 49	Le référentiel d'exploitation doit être maintenu à jour.

5 ANNEXES

5.1 LISTE DES NORMES APPLICABLES

Les réseaux RRF et partenaires se doivent de respecter les normes 3GPP associées sur les interfaces exposées entre les réseaux.

Cette annexe rassemble les normes 3GPP supportées par les interfaces du RRF. Cette liste sera mise à jour dans le temps suivant l'avancement de la normalisation.

Interfaces	**Référence 3GPP**
S6a	29.272 v15.9.0
S8	29.274 v15.4.0
S13	29.272 v15.9.0
S10	29.274 v15.4.0
Interface de taxation (CDR, TAP, NRTRDE)	32.299 v15.7.0
S1-U	36.410 v15.0.0 36.411 v15.0.0 36.412 v15.0.0 36.413 v15.7.1 36.414 v15.0.0
S1-C	36.410 v15.0.0 36.411 v15.0.0 36.412 v15.0.0 36.413 v15.7.1 36.414 v15.0.0
MCX-1, CSC-16, CSC-17	TS 23.280 v15.6.0
MCData-3	TS 23.282 v15.4.0
MCPTT-3	TS 23.379 v15.5.0 et TS 23.379
MCVideo-3	TS 23.281 v15.6.0
indicateurs de performances de bout-en-bout pour les services MCPTT	TS 22.179

Tableau 3 : Liste des normes applicables

5.2 LISTE DES EXIGENCES DE SECURITE

Recommandations ANSSI		
R1	Les usagers souscrivant au service LTE doivent être authentifiés sur le réseau au moyen d'une carte USIM supportant l'algorithme d'authentification 3G AKA et l'usage du bit 0 du champ AMF, précisant qu'il s'agit d'une authentification EPS-AKA.	Primordiale
R2	Le réseau partenaire doit configurer une politique d'authentification régulière des usagers (plusieurs fois par jour).	Primordiale
R3	Le réseau partenaire doit vérifier le support systématique des deux algorithmes cryptographiques SNOW 3G et AES par les équipements et terminaux LTE. Par ailleurs une même configuration de priorité de sélection de ces algorithmes doit être appliquée à l'ensemble des eNodeB et MME au sein du réseau mobile LTE.	Primordiale
R5	Le réseau partenaire et l'ACMOSS doivent veiller au strict respect de la norme 3GPP au sein des terminaux, et plus largement des eNodeB et MME, en ce qui concerne la mise en œuvre des mécanismes de contrôle d'intégrité et de chiffrement de la signalisation (RRC et NAS). Par ailleurs les eNodeB et MME doivent être configurés afin d'activer systématiquement le chiffrement des messages de signalisation. Le réseau partenaire veillera à ce que les terminaux LTE soient conformes aux recommandations précédentes. Enfin Le réseau partenaire veillera à désactiver le support des algorithmes EIA0 et EEA0 dans ses eNodeB et MME	Primordiale
R6	Le réseau partenaire doit configurer les eNodeB de son réseau afin d'activer systématiquement le chiffrement du trafic utilisateur sur la voie radio.	Primordiale
R7	Le réseau partenaire doit configurer les MME afin que les M-TMSI attribués aux terminaux soient renouvelés très fréquemment (plusieurs fois par heure) et lorsque le terminal mobile est en situation de mobilité.	Primordiale
R9	Le réseau partenaire doit mettre en place des passerelles VPN IPsec à la bordure du cœur de réseau afin de protéger le trafic IP des interfaces S1, X2 et O&M. Les interfaces O&M pourront être protégées par le protocole TLS dans un premier temps si leur encapsulation dans un tunnel IPsec n'est pas possible. La configuration devra être conforme au guide de déploiement publié sur le site de l'ANSSI [Ref 1 et Ref 2].	Primordiale
R10	Le réseau partenaire doit mettre en place une infrastructure de gestion des clés indépendante du fournisseur d'équipements du réseau mobile LTE.	Primordiale
R11	Le réseau partenaire doit veiller au strict respect des normes 3GPP concernant les eNodeB (normes TS 33.401, 33.210 et 33.310), et mettre en place une authentification mutuelle des eNodeB et passerelles VPN grâce au protocole IKEv2 et à l'usage de certificats X.509. Les certificats devront être conformes au RGS [Ref 3].	Primordiale
R12	Le réseau partenaire doit mettre en place un mécanisme d'enrôlement des eNodeB fondé sur le protocole CMPv2 conformément à la norme 3GPP TS 33.210.	Primordiale
R13	Le réseau partenaire doit mettre en place, dans les équipements d'accès radio eUTRAN et le réseau de transport, une ségrégation des réseaux séparant les trois principaux types de flux (O&M, signalisation, données utilisateurs). Il doit également	Primordiale

Recommandations ANSSI		
	configurer des restrictions d'accès (routes IP, ACL, ou de préférence des règles de filtrage à état) afin de minimiser l'exposition du cœur de réseau et des réseaux de maintenance vis-à-vis du réseau de transport sur lequel sont installés les eNodeB.	
R14	Le réseau partenaire doit mettre en place, dans le cœur de réseau EPC, une ségrégation des réseaux séparant les principaux types de flux (O&M, signalisation accès et cœur de réseau, données utilisateurs, interceptions légales, applications, etc.). Il doit également configurer des restrictions d'accès (routes IP, ACL, règles de filtrage à état) afin de minimiser l'exposition du cœur de réseau et des réseaux de maintenance vis-à-vis du réseau de transport sur lequel sont installés les équipements	Primordiale
R15	P, T2 - Pour sécuriser le service DNS mis en œuvre dans la résolution des noms au sein de l'infrastructure du réseau 2G et 3G, l'opérateur veillera à répartir les données accessibles aux équipements internes du réseau, les données accessibles à des équipements externes (par exemple via les interfaces de roaming), et les données accessibles aux abonnés du service mobile d'autre part, sur des équipements distincts et cloisonnés	
R16	Il est de la responsabilité du réseau partenaire de déployer une infrastructure d'administration sécurisée qui permette la protection et la traçabilité des accès des différentes personnes effectuant les opérations de maintenance et d'exploitation. Cette traçabilité doit être faite en conformité avec la législation française.	Primordiale
R17	Le réseau partenaire doit mettre en place sur le HSS et sur l'interface S6a un mécanisme d'identification fiable de la provenance des requêtes d'authentification issues des MME, permettant de personnaliser correctement les vecteurs d'authentification des usagers en situation d'itinérance	Souhaitable
R18	Il est primordiale de déployer une ou des passerelles d'interconnexion avec les partenaires nationaux ou de roaming international sur les interfaces mettant en œuvre le protocole Diameter. Cette passerelle devra implémenter les fonctions de Diameter Edge Agent (DEA), Diameter Routing Agent (DRA) et Diameter proxy. En particulier, Le réseau partenaire mettra en place sur ces passerelles les règles de filtrage et les outils de surveillance lui permettant de s'assurer de la conformité des requêtes transitant sur son réseau avec les spécifications d'interface de ses équipements de cœur de réseau EPC .	Primordiale
R19	Le réseau partenaire doit protéger les interfaces de son réseau avec des réseaux externes et ou partenaires en mettant en œuvre IPsec sur les interfaces sur lesquelles transitent des informations sensibles. En particulier il doit sécuriser les interfaces vers ses HSS. Le déploiement d'IPsec devra respecter le guide de configuration publié sur le site de l'ANSSI [Ref 1].	Primordiale
R20	Pour sécuriser le service DNS mis en œuvre dans la résolution des noms au sein du l'infrastructure LTE, Le réseau partenaire veillera à répartir les données accessibles aux équipements internes au réseau, les données accessibles pour des équipements externes (par exemple via les interfaces de roaming), et les données accessibles aux usagers au service LTE, sur des équipements distincts et cloisonnés.	Primordiale
R21	Le réseau partenaire veillera à ce que les eNodeB qu'il déploie répondent aux exigences minimales de sécurité telles qu'énoncées dans la norme 3GPP. Le réseau partenaire doit s'assurer	Primordiale

Recommandations ANSSI		
	qu'ils n'exposent aucune interface physique ou logique qui faciliterait la compromission du système.	
R22	Les équipements de cœur de réseau EPC doivent être déployés dans une configuration implémentant une redondance interne à l'équipement de type N+1 ou 1+1, interne au site de déploiement (double adduction et éventuellement acheminement différentié) et géographique. Les dispositifs concernés par cette recommandation sont choisis en fonction du nombre de leur sensibilité au regard de la continuité de l'action des services essentiels du réseau partenaire et de l'État.	Primordiale
R23	Les équipements du réseau d'accès eUTRAN doivent être déployés dans une configuration implémentant une redondance interne à l'équipement de type N+1 ou 1+1, interne au site de déploiement (double adduction et éventuellement acheminement différentié) des fonctions supportées. Les dispositifs concernés par cette recommandation sont choisis en fonction de leur sensibilité au regard de la continuité de l'action des services essentiels du réseau partenaire et de l'État.	Primordiale
R24	Les interconnexions entre les équipements du réseau LTE doivent être redondées par deux liaisons distinctes empruntant des chemins géographiques distincts dans le cas de liaisons entre sites de cœur de réseau. Le réseau partenaire déploiera en particulier ses interfaces entre eNodeB et MME dans un mode S1-flex afin d'assurer la continuité du service en cas de défaillance du MME ou d'opérations de maintenance sur celui-ci.	Primordiale
R25	Le réseau partenaire mettra en place une procédure de sauvegarde régulière (hebdomadaire ou journalière selon les équipements) et sécurisée (intégrité et conservation hors ligne) des bases de données et des configurations, de ses équipements.	Primordiale
R26	Le réseau partenaire mettra en place une procédure de sauvegarde régulière (hebdomadaire ou journalière) et sécurisée des journaux d'exploitation et des journaux d'administration de ses équipements.	Primordiale

5.3 ACCORD DE CONFIDENTIALITE

ACCORD DE CONFIDENTIALITE

ENTRE LES SOUSSIGNEES

xxxxxx
Société enregistrée xxxx et dont le siège social est situé xxxx, représentée par xxxxx, agissant en qualité de xxxxx, dûment habilité aux fins des présentes

Ci-après dénommée « l'opérateur partenaire »

D'autre part,

ET

L'ACMOSS
Située au 17 Pl. des Reflets, 92400 Courbevoie, représentée par M. Guillaume Lambert, en sa qualité de directeur de l'ACMOSS, dûment habilité à l'effet des présentes

Ci-après dénommée « ACMOSS»

D'autre part,

Ci-après collectivement dénommées les "Parties",

ou individuellement "Partie Divulgatrice" et "Partie Réceptrice",

Préambule

La mise en œuvre du Réseau Radio du Futur (RRF) qui vise à construire une solution de communication critique à très haut débit, résiliente, sécurisée, pour les services de sécurité, de secours, de gestion des crises et des catastrophes est un enjeu majeur pour la capacité de communication opérationnelle de l'Etat.

Dans l'objectif de répondre aux besoins de couverture des opérations des forces de sécurité et de secours des conventions sont mises en place pour raccorder le RRF et le réseau d'opérateur partenaire. Ce partenariat donnera lieu à des échanges d'informations pour mettre en œuvre ce service et ces interconnexions.

Les Parties se sont rapprochées pour définir les conditions et modalités gouvernant la remise et l'utilisation de ces Informations Confidentielles auxquelles les Parties déclarent se soumettre irrévocablement.

Il a été arrêté et convenu ce qui suit

1. Définitions

1.1. « Information(s) Confidentielle(s) » désigne :

(a) Toutes les informations, de quelque nature qu'elles soient (notamment d'ordre technique, économique, stratégique, commercial, financier, comptable, juridique et administratif), ayant trait à la Partie Divulgatrice et/ou son activité et qui auront été communiquées, par écrit, ou oralement, ou par tout autre moyen, à la Partie Réceptrice et/ou à ses Représentants, par ladite Partie Divulgatrice et/ou Représentants ;

(b) Toutes les analyses, compilations, études et autres documents que les Parties ou ses représentants auront préparés ou fait préparer et qui incorporeront, feront référence ou simplement résulteront des informations visées au paragraphe (a) ci-dessus ;

1.2. « Représentants » désigne : les dirigeants, mandataires sociaux, salariés, conseils, prestataires, sous-traitants et employés d´une Partie ou d´une Société Affiliée à XXXXX. Par « Société Affiliée », on entend toute société qui, au jour de la signature du présent Accord de Confidentialité ou pendant la durée du présent Accord de Confidentialité, est contrôlée directement ou indirectement par XXXX. ou contrôle directement ou indirectement XXXX., ou avec laquelle XXXX est sous contrôle commun (direct ou indirect), selon la définition de contrôle à l´article L233-3 du Code de Commerce.

2. Engagements

2.1. Au vu de ce qui est exposé ci-dessus, les Parties s'engagent et se portent fort du respect de cet engagement par ses Représentants, par la signature de la présente, sans condition, limitation ou restriction aucune, à :

(a) N'utiliser les Informations Confidentielles reçues de l'autre Partie qu'à seule fin d'étude de l'Objectif, à l'exclusion de toute autre utilisation, notamment l'utilisation de ces informations, directement ou indirectement, seule ou via une tierce personne, aux fins de fournir des prestations de services pour son propre compte ou pour des tiers ;

(b) Ne pas copier les Informations Confidentielles reçues de la Partie Divulgatrice, ni les reproduire, ni les dupliquer totalement ou partiellement, sans l'accord préalable et écrit

de ladite Partie Divulgatrice ;

(c) Ne pas divulguer, en tout ou partie, de quelque manière que ce soit, à tous tiers, les Informations Confidentielles reçues de la Partie Divulgatrice. Dans l'hypothèse où la Partie Réceptrice ou l'un de ses Représentants serait dans l'obligation légale de divulguer tout ou partie de ces Informations Confidentielles, la Partie Réceptrice fournira sans délai à la Partie Divulgatrice la notification préalable et écrite d'une telle obligation afin que cette dernière puisse, le cas échéant, prendre toute mesure ou action de protection et qu'en toutes circonstances soit possible une consultation préalable avec la Partie Divulgatrice et ses Représentants sur l'étendue et le calendrier de la divulgation envisagée ;

(d) Limiter, par tous moyens appropriés, la diffusion totale ou partielle ou l'utilisation des Informations Confidentielles à ceux de ses Représentants dont l'intervention pour l'exécution du Contrat s'avérerait nécessaire; la Partie Réceptrice s'engage à informer préalablement ces Représentants de la nature confidentielle des Informations Confidentielles, à leur imposer des obligations similaires de confidentialité que celles que la Partie Réceptrice a souscrit par la présente, et à prendre toute disposition nécessaire pour leur faire respecter le présent Accord de Confidentialité ;

(e) Informer la Partie Divulgatrice de toute violation ou non-respect des obligations imposées par le présent Accord de Confidentialité dont la Partie Réceptrice aurait connaissance et fournir toute l'assistance possible pour minimiser les effets d'une telle violation ou d'un tel non-respect.

2.2. Il est convenu que les obligations visées au présent Accord de Confidentialité ne s'appliqueront pas aux informations qui, au sens des présentes, devraient être considérées comme des Informations Confidentielles mais dont la Partie Réceptrice apportera la preuve que :

(a) Elles étaient déjà dans le domaine public au jour de leur divulgation à la Partie Réceptrice ou à ses Représentants ;

(b) Elles ont été communiquées à la Partie Réceptrice ou à ses Représentants, à titre non confidentiel, par une source autre que la Partie Divulgatrice, ou ses Représentants, qui ne fait pas l'objet d'une interdiction légale ou contractuelle de révéler cette information.

2.4. Chaque Partie s'engage à indemniser l'autre Partie de tout dommage, préjudice ou perte de quelque nature que ce soit, résultant du non-respect de l'une quelconque des obligations mises à sa charge et à celles de ses Représentants par le présent Accord de Confidentialité.

3. Divers

3.1 Le présent Accord de Confidentialité engage les successeurs ayants-droit ou ayants-cause éventuels des Parties.

3.2 Le fait pour une Partie de ne pas se prévaloir d'une disposition du présent Accord de Confidentialité n'emporte en aucun cas renonciation au bénéfice d'une quelconque des clauses du présent Accord de Confidentialité.

3.3 Le présent Accord de Confidentialité ne peut être cédé ou transféré, en tout ou partie, par une Partie à un tiers, sans le consentement écrit et préalable de l'autre Partie.

3.4 Le présent Accord de Confidentialité prend effet à compter de sa signature par les Parties, étant entendu que les échanges d'informations déjà intervenus entre les Parties dans le cadre du même objet y seront soumis, et restera en vigueur pour la durée de la convention additionnée de deux (2) années étant entendu que l'obligation de confidentialité contenue à l'article 2 du présent Accord de confidentialité perdurera au-delà du terme de l'Accord de Confidentialité et ce pour une durée de dix (10) ans à compter de son expiration.

3.5 Le présent Accord de Confidentialité est régi par le droit français.

Tout différend, quel qu'en soit l'objet et le fondement, se rattachant au présent Accord de Confidentialité ou qui en serait la suite ou la conséquence sera soumis à la compétence exclusive du Tribunal administratif de Paris.

Paris, le XXXX.

Société :
Nom :
Titre :
Signature :

Entité : La Direction de l'ACMOSS
Nom : Guillaume Lambert
Titre : Directeur
Signature :

FIN DU DOCUMENT