PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat Général du Gouvernement
Direction des services administratifs et financiers

ACCORDS-CADRES INTERMINISTÉRIELS RELATIFS A LA FOURNITURE DE SERVICE RÉSEAU DANS LES TERRITOIRES D'OUTRE-MER FRANÇAIS AU PROFIT DU RIE

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)

Commun aux 7 lots

Numéro de consultation : 25_BAM_001

Table des matières

Table des matières 2

Chapitre 1 : Présentation des accords-cadres Interministériels 7

1.1 Objet de la consultation 7

1.1.1 Périmètre des accords-cadres 7

1.1.2 Allotissement 10

1.1.3 Présentation synthétique du projet d'achat 14

1.1.4 Documents de référence 15

1.1.5 Liste des annexes 16

1.1.6 Terminologie et glossaire 17

1.2 Présentation des précédents besoin et accords-cadres 21

1.3 Parties prenantes et organisation 22

1.3.1 Pouvoir Adjudicateur 22

1.3.2 Département Infrastructure et Services Opérés (ISO) 22

1.3.3 Interlocuteurs pour la cybersécurité (CSIRT) 24

1.3.4 Bénéficiaires 25

Chapitre 2 : Présentation du RIE 26

2.1 Présentation générale 26

2.2 Présentation de l'épine dorsale du RIE 27

2.3 Application aux territoires d'Outre-Mer 27

2.4 Quantité estimative du nombre de sites ultramarins 28

2.4.1 Liste des points d'interconnexion des transits transocéaniques à l'épine dorsale du RIE en Hexagone 28

2.4.2 Liste des Passerelles Outre-Mer (POM) 28

2.4.3 Nombre d'accès de collecte (hors POM) par territoire 29

Chapitre 3 : Définition du besoin 31

3.1 Infrastructures des titulaires des lots 1 à 5 et 7 31

3.1.1 Confidentialité des informations transportées 31

3.1.2 Conformité 31

3.1.3 Typologies de la sécurisation des infrastructures 31

3.1.4 Gestion des équipements d'extrémité 32

3.1.5 Définition des niveaux de service 40
3.1.6 Raccordement de la POM au réseau de collecte multi-VPN 43
3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés 46
3.2 Lot 1 et lot 2 : Prestations de Collecte 49
3.2.1 Principe d'architecture 49
3.2.2 Besoins de raccordement des sites ultramarins 49
3.2.3 Spécifications du réseau privé virtuel (VPN) 51
3.2.4 Plan d'adressage IP 51
3.2.5 AS BGP 52
3.2.6 Services IPv4 et IPv6 52
3.2.7 Etendue et capillarité du réseau du titulaire 52
3.2.8 Spécifications sur les accès mobiles et satellites 53
3.2.9 Qualité de services « QoS » 54
3.2.10 Voix et vidéo sur IP 56
3.2.11 Multicast 57
3.3 Lots 3, 4 et 5 : Transit sécurisé vers l'Hexagone et entre les territoires ultramarins 57
3.3.1 Liaisons transocéaniques « Entreprise » 59
3.3.2 Transit « Internet » 61
3.3.3 Services de chiffrement 62
3.3.4 MTU 64
3.3.5 Qualité de service 64
3.3.6 AS BGP 64
3.3.7 Transit non chiffré 65
3.4 Lot 7 : Transit sécurisé entre l'Hexagone et Saint Pierre et Miquelon 65
3.4.1 Transit internet sécurisé 66
3.4.2 Raccordement sur la double épine dorsale du RIE en métropole 67
3.4.3 MTU 68
3.4.4 Qualité de service 69
3.4.5 Protection des accès internet 69
3.5 Lot 6 : Management des services 71

Chapitre 4 : Mise en œuvre des accords-cadres 72

4.1 Passation des commandes d'achat 72

4.2 Plan d'assurance qualité de l'accord-cadre (PAQ) 73
4.3 Plan de gestion et d'amélioration continue (PGAC) 73
4.4 Politique de sécurité 73
4.4.1 Accès aux locaux et usage des ressources 73
4.4.2 Respect de la législation et de la règlementation en vigueur et SSI 75
4.4.3 Plan d'assurance sécurité (PAS) 75
4.5 Gouvernance de chaque accord-cadre 78
4.5.1 Comité de pilotage « COPIL » 78
4.5.2 Comité d'exploitation « COMEX » 79
4.5.3 Comité de sécurité « COSEC » 82
4.5.4 Comité de projet (de déploiement) « COPROJ » 84
4.5.5 Comité de suivi « COSUI » 85
4.6 Management des services (Lot 6) 86
4.6.1 Initialisation du Lot 6 86
4.6.2 Assistance à maîtrise d'ouvrage de la migration 88
4.6.3 Pilotage lors de la phase opérationnelle du service 98
4.7 Prestations d'entrée 105
4.7.1 Initialisation de l'accord-cadre 105
4.7.2 Cadrage du projet de migration des sites 106
4.7.3 Echanges automatisés des Lot 1 et 2 108
4.8 Migration des services 114
4.8.1 Phase 1 « Planification » 115
4.8.2 Phase 2 « Etude » 117
4.8.3 Phase 3 « Pilotes » 119
4.8.4 Phase 4 » Généralisation » 122
4.8.5 Modalités de déploiement 124
4.8.6 Instances de pilotage de la migration 125
4.9 Raccordement post-migration d'un accès 126
4.10 Gestion opérationnelle du service 126
4.10.1 Abonnements des accès et services associés inclus 126
4.10.2 Gestion des évolutions majeures 127
4.10.3 Gestion des évolutions mineures 128
4.10.4 Résiliation d'un accès 129

4.11 Gestion des incidents 129
4.11.1 Organisation générale du support 129
4.11.2 Prérequis et période de gel 131
4.11.3 Processus de déclaration d'un incident 132
4.11.4 Procédure d'escalade 133
4.11.5 Organisation du support du titulaire 134
4.11.6 Supervision réalisée par le titulaire 135
4.12 Gestion des problèmes 135
4.13 Gestion des opérations planifiées 136
4.14 Préparation du comité d'exploitation 137
4.14.1 Point quotidien sur les incidents nécessitant un suivi particulier 137
4.14.2 Point hebdomadaire sur les incidents en dépassement de GTR 137
4.14.3 Point bimensuel sur les productions en cours de traitement 138
4.14.4 Point mensuel 138
4.15 Opérations de vérification d'un accès 139
4.15.1 La Mise en ordre de marche (MOM) d'un accès 139
4.15.2 Livrables documentaires 140
4.15.3 Vérification d'aptitude (VA) d'un accès 140
4.15.4 Vérification de Service Régulier (VSR) d'un accès 142
4.16 Gestion des performances 143
4.17 Services et prestations complémentaires 143
4.17.1 Prestation d'expertise de la performance 143
4.17.2 Prestation de projet d'infrastructure 144
4.18 Réversibilité en fin de chaque accord-cadre 145

Chapitre 5 : Engagements de service 147

5.1 Engagements sur les prestations d'entrée 147
5.2 Engagements opérationnels des services des lots 1 à 5 et 7 148
5.2.1 Engagements d'exploitation (incident, planification, supervision) 149
5.2.2 Gestion des évolutions en vie de réseau post-migration 149
5.2.3 Engagements sur la relation client 150
5.2.4 Engagements sur la sécurité 151
5.2.5 Engagements sur la gouvernance de l'accord-cadre 151

5.2.6 Engagements sur les portails clients, interfaces et développements spécifiques 151
5.3 Qualité et performance des services des lots 1 à 5 et 7 153
5.3.1 Débit minimum garanti 153
5.3.2 Temps de transit et latence dans le réseau 153
5.3.3 Taux de perte des paquets IP ou des trames 154
5.3.4 Gigue des paquets IP ou des trames 154
5.3.5 Engagement sur le niveau de qualité et de performance 154
5.4 Engagements sur les prestations de sortie 157

Chapitre 6 : Annexes 158

6.1 Liste des Exigences 158
6.1.1 Lot 1 à 5 & 7 158
6.1.2 Lot 1 et 2 158
6.1.3 Lot 3 à 5 159
6.1.4 Lot 6 160
6.1.5 Lot 7 160
6.2 Liste des Points à préciser par le soumissionnaire dans son offre 160
6.2.1 Lot 1 à 7 160
6.2.2 Lot 1 à 5 & 7 162
6.2.3 Lot 1 et 2 163
6.2.1 Lot 3 à 5 166
6.2.2 Lot 6 166

Chapitre 1 : Présentation des accords-cadres Interministériels

1.1 Objet de la consultation

1.1.1 Périmètre des accords-cadres

Le présent document est le Cahier des Clauses Techniques Particulières (CCTP) relatif à la fourniture de service réseau de collecte dans les territoires d'Outre-Mer français ainsi que de transit sécurisé vers l'Hexagone et entre les territoires d'une même zone géographique.

La terminologie en matière de zone utilisée dans le présent CCTP est la suivante :

Zone géographique	Territoire ultramarin	Couverture « collecte »	Couverture « transit sécurisé »
Atlantique (zone Caraïbes) (points de concentration)	Guyane Martinique Guadeloupe Saint-Martin et Saint-Barthélemy	Lot 1	Lot 3
Océan Indien (points de concentration)	La Réunion Mayotte	Lot 2	Lot 4
Pacifique (points de concentration)	Polynésie Française Nouvelle-Calédonie Wallis-et-Futuna	Hors périmètre	Lot 5
Atlantique Nord	Saint-Pierre-et-Miquelon	Hors périmètre	Lot 7

Ce CCTP décrit les exigences et les attentes du pouvoir adjudicateur pour la mise en œuvre de services ayant vocation à assurer le transport de données, de voix et de vidéo entre les sites ultramarins de l'Administration d'une même zone géographique, d'une part, et entre les sites ultramarins et le réseau interministériel de l'Etat (RIE) dans l'Hexagone, d'autres part, ainsi que des services complémentaires d'accès à Internet.

{EX-L1 à 5 & 7/01}. 1.1.1 Périmètre des accords-cadres : Toute communication IP de l'État en dehors du territoire national fera l'objet d'une protection cryptographique « qualifiée » en confidentialité et en intégrité. Cette protection repose sur une des solutions listées dans le catalogue des produits et services qualifiés, agréés et certifiés par l'ANSSI. Elle est mise en œuvre soit par le titulaire du présent marché pour tous les tronçons à sa charge, soit par le pouvoir adjudicateur pour les autres tronçons.

Les interconnexions des flux chiffrés entre les territoires ultramarins et l'Hexagone, emprunteront soit des liaisons de transit de type entreprise, soit des liaisons de type Internet fournies par les lots 3, 4, 5 et 7

Le service de transit chiffré doit permettre aux différents sites clients raccordés aux VPN IP présents sur les réseaux de collecte de communiquer avec l'épine dorsale MPLS du RIE et les sites des autres territoires d'une même zone raccordés aux mêmes VPN IP communautaires de façon cloisonnée et résiliente.

La plateforme de livraison de service Outre-Mer (PLS OM) permet d'offrir des raccordements directs à la POM (Passerelle Outre-Mer) et la plateforme de service (PFS OM) permet des échanges entre les communautés présentes au sein du même territoire couvert par la POM considérée.

Les schémas ci-dessous illustrent les périmètres et la nature des prestations de services attendues pour un territoire ultra-marin sur la POM.

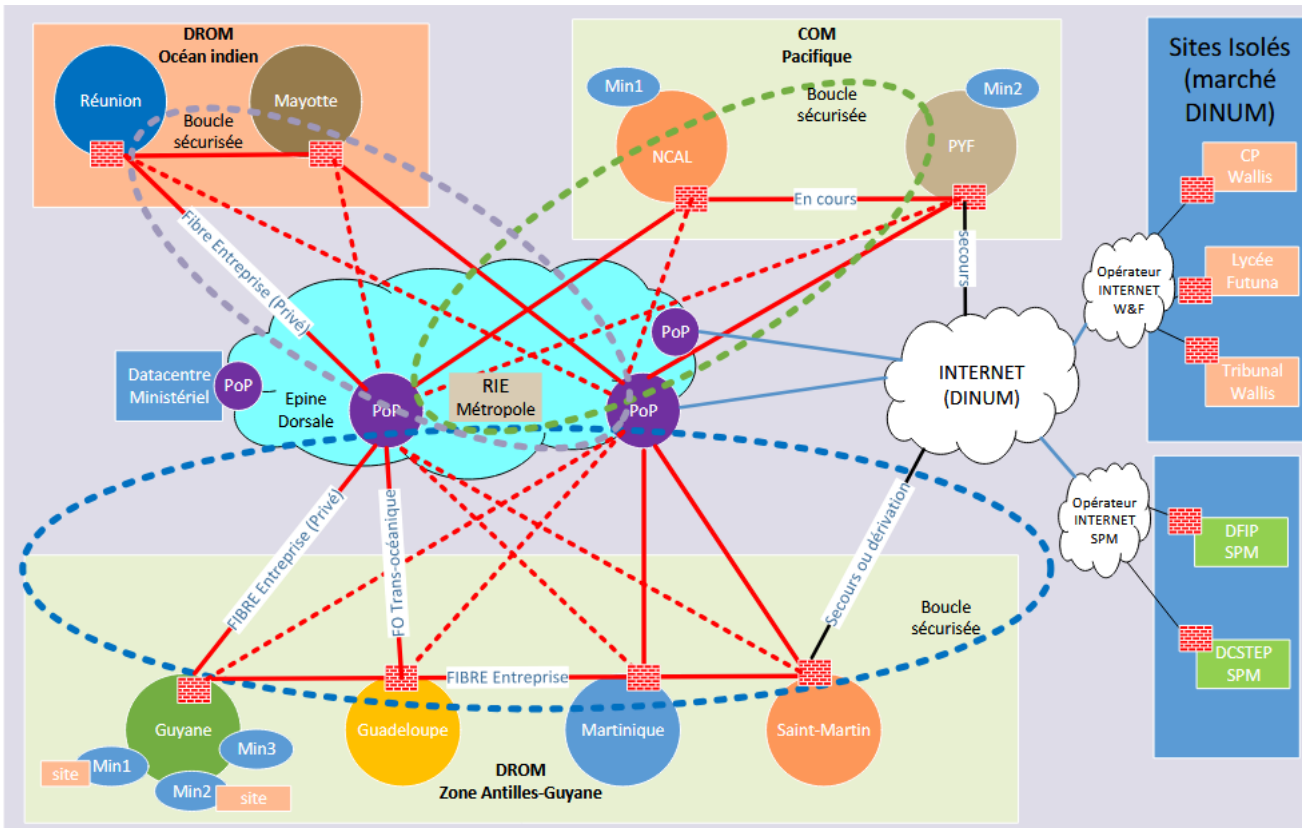


Figure 1 : Schéma transit sécurisé ultramarin

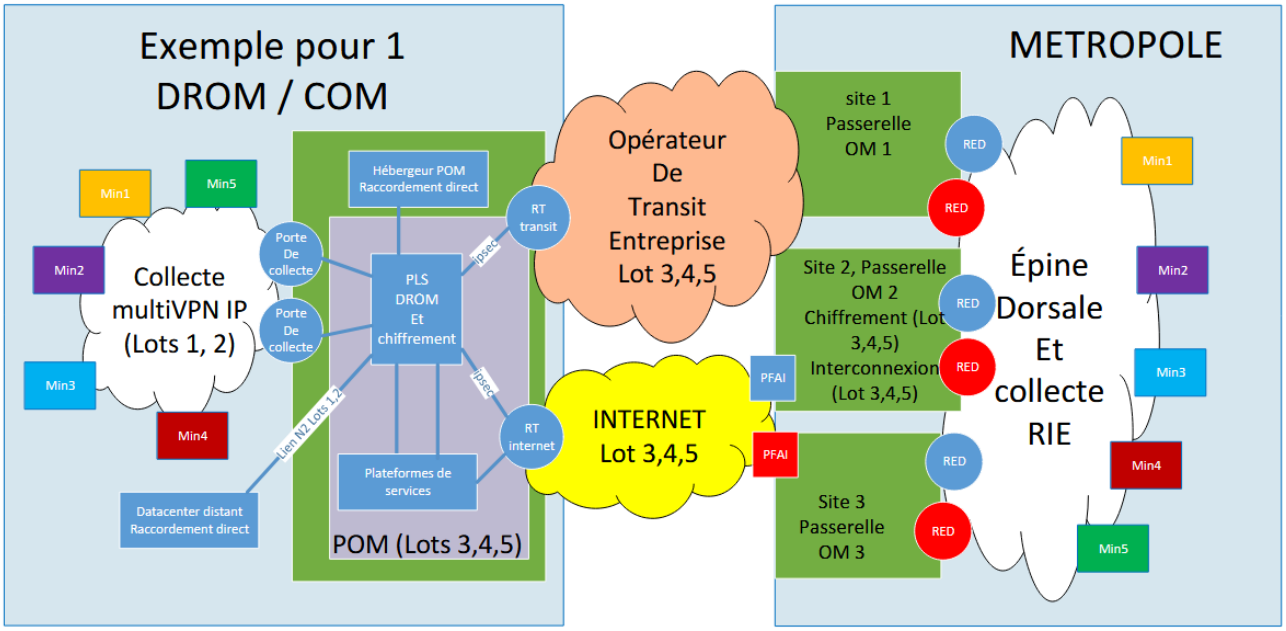


Figure 2 : Schéma détaillé pour un site DROM/COM

1.1.2 Allotissement

1.1.2.1 Lot 1 : Service de collecte VPN IP Atlantique

Ce lot concerne les territoires ultramarins des DROM des Antilles et de Guyane y compris Saint-Martin et Saint-Barthélemy. Il a pour objectif la mise en place d'un service de collecte VPN IP au sein des territoires concernés.

1.1.2.2 Lot 2 : Service de collecte VPN IP Océan Indien

Ce lot concerne les territoires ultramarins des DROM de Mayotte et de La Réunion. Il a pour objectif la mise en place d'un service de collecte VPN IP au sein de ces deux départements.

1.1.2.3 Lot 3 : Service de transit sécurisé « Atlantique »

Ce lot concerne les territoires de Guadeloupe, Martinique, Guyane française, Saint-Martin et Saint-Barthélemy.

Il a pour premier objectif la fourniture d'un service de transit chiffré résilient à haut débit entre les territoires ultramarins des Antilles et de Guyane eux-mêmes et entre ceux-ci et l'Hexagone. Le service offre la possibilité d'utiliser pour le transport des liaisons à haut débit garanti type entreprise et/ou des liaisons Internet à haut débit.

La topologie forme une boucle optique qui relie tous les sites de la zone et au moins 2 points de connexion à l'épine dorsale du RIE en Hexagone.

Il comprend également une solution satellite d'ultime secours pour raccorder les territoires concernés à l'Hexagone.

La prestation attendue sur ce lot comprend également la solution de Plateforme de Livraison de Service en territoire ultramarin (PLS OM) qui assure le raccordement au sein de la POM avec le réseau de collecte MultiVPN, les raccordements directs colocalisés ou distants et les plateformes de services associées. Cette PLS OM porte l'ensemble des VRF déployées sur le réseau de collecte ultramarin et assure l'interconnexion des L3VPN avec l'épine dorsale en Hexagone selon l'architecture définie et retenue en début de projet.

La solution d'échanges sécurisés entre les communautés de chaque territoire ultramarin constitue la première Plateforme de Service (PFS OM) attendue dans les prestations.

1.1.2.4 Lot 4 : Service de transit sécurisé « Océan Indien »

Ce lot concerne les territoires de La Réunion et Mayotte.

Il a pour objet la fourniture d'un service de transit chiffré résilient à haut débit entre ces deux territoires eux-mêmes et entre ceux-ci et l'Hexagone. Le service offre la

possibilité d'utiliser pour le transport des liaisons à haut débit garanti type Entreprise et/ou des liaisons Internet à haut débit.

La topologie forme une boucle optique qui relie les sites de la zone et au moins 2 points de connexion à l'épine dorsale du RIE en Hexagone.

Il comprend également une solution satellite d'ultime secours pour raccorder les territoires concernés à l'Hexagone.

Ce lot comprend également la fourniture de la solution de Plateforme de Livraison de Services en territoire ultramarin (PLS OM). Celle-ci assure le raccordement, au sein de la POM, au réseau de collecte MultiVPN, aux raccordements directs colocalisés ou distants, ainsi qu'aux plateformes de services associées. La PLS OM porte l'ensemble des VRF déployées sur le réseau de collecte ultramarin et assure l'interconnexion des L3VPN avec l'épine dorsale située en Hexagone, conformément à l'architecture définie et retenue en début de projet.

La solution d'échanges sécurisés entre les communautés de chaque territoire ultramarin constitue la première Plateforme de Service (PFS OM) attendue dans les prestations.

1.1.2.5 Lot 5 : Service de transit sécurisé « Pacifique »

Ce lot concerne les territoires de Polynésie Française et Nouvelle-Calédonie.

Il a pour objectif la fourniture d'un service de transit chiffré résilient à haut débit garanti et d'un service de transit chiffré Internet à haut débit entre ces deux territoires et l'Hexagone.

La topologie visée forme une boucle optique qui relie les sites de la zone et au moins 2 points de connexion à l'épine dorsale du RIE en Hexagone.

Il comprend également une solution satellite d'ultime secours pour raccorder les territoires concernés à l'Hexagone.

Ce lot fournit également la solution de Plateforme de Livraison de Service en territoire ultramarin (PLS OM) qui assure le raccordement au sein de la POM avec le réseau de collecte MultiVPN, les raccordements directs colocalisés ou distants et les plateformes de services associées. Cette PLS OM portera l'ensemble des VRF déployées sur le réseau de collecte ultramarin et assurera l'interconnexion des L3VPN avec l'épine dorsale en Hexagone selon l'architecture définie et retenue en début de projet.

La solution d'échanges sécurisés entre les communautés de chaque territoire ultramarin constitue la première Plateforme de Service (PFS OM) attendue dans les prestations.

1.1.2.6 Lot 6 : Management des services

Ce lot est relatif à une prestation de :

- Coordination et synchronisation des intervenants des titulaires des marchés ;
- Vérification de la cohérence et de la complémentarité des différents plans de l'accord-cadre : plans d'assurance qualité (PAQ), plans de gestion et d'amélioration continue (PGAC) et plans d'assurance sécurité (PAS) ;
- Préparation et animation des réunions des instances de gouvernance des marchés ;
- Consolidation des plannings, des plans de management des risques, des relevés de décisions, des plans d'actions… ;
- Suivi de l'exécution et *reporting* des plans d'actions ;
- Fourniture des tableaux de bord consolidés sur l'ensemble des lots.

Cette organisation signifie que les titulaires retenus sur les lots techniques concourent tous, à leur niveau, au bon fonctionnement de chaque accès de collecte en Outre-Mer :

- Les titulaires du lot 1 et du lot 2 « collecte » assurent non seulement les communications entre les sites distants d'une même communauté (VPN) au sein d'un même territoire et au sein de tous les territoires de la même zone géographique ; mais aussi sont responsables du raccordement de ces mêmes sites distants jusqu'aux Passerelles Outre-Mer (POM) du territoire concerné ;
- Les titulaires des lots 3, 4, 5 et 7 « transit sécurisé » sont responsables du chiffrement et de l'acheminement des flux chiffrés entre les territoires concernés d'une même zone géographique et entre ces mêmes territoires et l'Hexagone. Ce transport doit respecter le cloisonnement des flux entre les communautés imposés par les VPN mis en place par les titulaires des lots 1 et 2.

{PP-L6/01} 1.1.2.6 Lot 6 : Management des services : Une coordination rapprochée est donc nécessaire entre ces deux familles d'acteurs afin que les opérations se déroulent au mieux. La réponse au lot 6 de cette consultation doit apporter des explications détaillées sur la méthode et les moyens mis en œuvre par le titulaire pour répondre à cette demande du pouvoir adjudicateur.

1.1.2.7 Lot 7 : Service de transit sécurisé « Atlantique nord »

Ce lot concerne le territoire de Saint-Pierre-et-Miquelon.

Il a pour objectif la fourniture d'un service de transit chiffré à haut débit entre les sites des bénéficiaires du territoire de Saint-Pierre et Miquelon et l'Hexagone. La

collecte des flux chiffrés de chaque site souscrit est mutualisée sur des équipements dédiés en Hexagone.

Récapitulatif des lots :

Lot	Périmètre géographique	Objet du lot
Lot 1 – Service de collecte VPN IP Atlantique	Guadeloupe, Martinique, Guyane, Saint-Martin, Saint-Barthélemy	Mise en place d'un service de collecte VPN IP dans les territoires ultramarins de la zone Atlantique.
Lot 2 – Service de collecte VPN IP Océan Indien	Mayotte et La Réunion	Mise en place d'un service de collecte VPN IP dans les deux départements de la zone Océan Indien.
Lot 3 – Service de transit sécurisé Atlantique	Guadeloupe, Martinique, Guyane, Saint-Martin, Saint-Barthélemy	Fourniture d'un service de transit chiffré résilient à haut débit garanti et d'un service de transit chiffré Internet à haut débit entre les territoires de l'Atlantique et l'Hexagone.
Lot 4 – Service de transit sécurisé Océan Indien	La Réunion et Mayotte	Fourniture d'un service de transit chiffré résilient à haut débit garanti et d'un service de transit chiffré Internet à haut débit entre les territoires de l'Océan Indien et l'Hexagone.
Lot 5 – Service de transit sécurisé Pacifique	Polynésie française et Nouvelle-Calédonie	Fourniture d'un service de transit chiffré résilient à haut débit garanti et d'un service de transit chiffré Internet à haut débit entre les territoires du Pacifique et l'Hexagone.
Lot 6 – Management des services	Ensemble des lots et des zones ultramarines	Coordination, pilotage, consolidation et reporting des prestations de l'ensemble des lots.
Lot 7 Service de transit sécurisé Atlantique nord	Saint-Pierre et Miquelon	Fourniture d'un service de transit chiffré résilient à haut débit entre le territoire de Saint-Pierre et Miquelon et l'Hexagone.

1.1.3 Présentation synthétique du projet d'achat

1.1.3.1 Prestations d'entrée

Les prestations d'entrée sont les prestations qui sont commandées par l'Administration pour cadrer et lancer le projet de migration des accès des bénéficiaires pour chacun des 6 lots.

1.1.3.2 Prestations de transit sécurisé (lots 3, 4,5 et 7)

Les prestations dites de transit sécurisé sont les prestations commandées par l'Administration pour gérer les raccordements, leurs évolutions et leurs résiliations le cas échéant des infrastructures déployées par le titulaire au sein des Passerelle Outre-Mer (POM) et des points de raccordements à l'épine dorsale du RIE en Hexagone. Dans le cas du lot 7, chaque site client du territoire est collecté individuellement (absence de POM).

Ces prestations permettent d'interconnecter les réseaux L3VPN en DROM et en COM et les sites clients en raccordement direct sur la PLS OM à l'épine dorsale du RIE de manière cloisonnée. L'administration commandera le déploiement d'une plateforme de livraison de service au sein de la POM ainsi qu'une plateforme de service dédiée aux échanges entre les VPN des bénéficiaires des territoires ultramarins d'une même zone.

{PP-L3 & 5/01} 1.1.3.2 Prestations de transit sécurisé (lots 3, 4,5 et 7). Le titulaire répond au besoin de l'Administration en proposant des solutions techniques au niveaux de la POM et de l'interconnexion à l'épine dorsale. En fonction des choix technologiques retenus, le transit sécurisé est amené à transporter différentes natures de flux sans impact sur la qualité ressentie par les utilisateurs.

1.1.3.3 Migration des services (lot 1 et 2)

Ces prestations sont les prestations qui sont commandées par les bénéficiaires pour la migration de chacun de leurs accès de collecte distants, implantés sur leurs sites locaux, techniquement et administrativement, vers ce présent marché.

1.1.3.4 Gestion opérationnelle du service

En mode « vie de service » (VDS), à l'issue de la migration des services sur ce marché et à l'issue des installations de nouveaux services, leur gestion opérationnelle inclut :

- Les abonnements à un accès d'un site et tous les services associés ;
- La gestion des projets d'évolution ;
- La gestion des raccordements directs ;

- La gestion des changements mineurs et majeurs sur les configurations ;
- La résiliation d'un accès ;
- Les éventuelles prestations d'assistance et d'expertise supplémentaires.

1.1.3.5 Prestations de sortie

Les prestations de sortie sont les prestations qui sont commandées avant la fin de la durée de validité de chaque accord-cadre pour permettre à l'Administration la reprise à sa charge de la gestion de l'ensemble des services délégués inclus dans le présent marché.

1.1.4 Documents de référence

Réf.	Description	
[R1]	Bordereau des prix	Le bordereau des prix renseignés est annexé à chaque acte d'engagement (AE) du contrat.
[R2]	Bordereau des délais	Le bordereau des délais renseigné est annexé à chaque acte d'engagement (AE) du contrat.
[R3]	Liste des sites par zone géographique	La liste des sites par zone géographique renseignée est un appendice du cadre de réponse technique
[R4]	RFC1918	Address Allocation for Private Internets
[R5]	RFC6598	Réserve le bloc d'adresses 100.64.0.0/10 pour l'utilisation à l'intérieur du réseau de l'opérateur
[R6]	IGI 1300	Instruction générale interministérielle n° 1300 pourtant sur la protection du secret de la défense nationale du 15 novembre 2020 applicable au 1er juillet 2021.
[R7]	Code de la Sécurité Intérieure	Version en vigueur
[R8]	Instruction Interministérielle II 901	Instruction relative à la protection des systèmes d'information sensibles, notamment ceux traitant des informations portant la mention Diffusion Restreinte.
[R9]	Politique de sécurité des systèmes d'information de l'état (PSSIE)	Politique de sécurité qui fixe les règles de protection applicables aux systèmes d'information de l'État

Réf.	Description	
[R10]	Référentiel général de sécurité (RGS)	Référentiel qui est le cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens
[R11]	Référentiel général d'interopérabilité (RGI)	Référentiel qui est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration
[R12]	Règlement général sur la protection des données (RGPD)	Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

1.1.5 Liste des annexes

Annexe	Description	Emplacement
[A1]	Liste prévisionnelle des sites des bénéficiaires	CCTP annexe 01 - Liste prévisionnelle des sites des bénéficiaires
[A2]	Fichier de Commande RIE type	CCTP annexe 02 - Fichier de Commande RIE type
[A3]	PSSI RIE Version 2.0 – juin 2019	CCTP annexe 03 - NP-RI03-PSSI_RIE-v2.0
[A4]	Bonnes pratiques et les règles d'hygiène informatique édictées notamment par l'ANSSI du 23 janvier 2017	CCTP annexe 04 - Guide hygiène informatique ANSSI
[A5]	Glossaire des sigles et dictionnaire des termes Version 2.0 – juin 2019	CCTP annexe 05 - NP-RI015-Glossaire_Dictionnaire_v2.0.
[A6]	Corpus documentaires de textes de référence Version 2.1– septembre 2019	CCTP annexe 06 -NP-RI016-Corpus_Documentaire_Référence_v2.1
[A7]	Modèle de tableau de suivi complet	CCTP annexe 07 - Modèle Tableau de bord de suivi de production
[A8]	Format des PV de mise en service (en html)	CCTP annexe 08 - Modèle de PV de mise en service
[A9]	Nomenclature CIGREF des profils métiers du système d'information (version 2024)	CCTP annexe 09 - Nomenclature Cigref 2024

1.1.6 Terminologie et glossaire

Sigle ou Terme	Description
4G/5G	Quatrième ou cinquième génération des standards de la téléphonie mobile
ACIM	Accord Cadre Inter Ministériel
Accès RIE	Point de livraison du service de collecte. ▪ Un accès est caractérisé par : Sa technologie (cuivre ou fibre, xDSL, FTTx, 4G/5G, satellite…) ; ▪ Son débit ; ▪ Son niveau de sécurisation (simple, double, etc.) ; ▪ Sa redondance actif/actif ou partage de charge ; ▪ Ses niveaux d'engagements de service.
ACL	*Access Control List* est une liste d'adresses réseaux et de ports (TCP ou UDP) permettant de faire du contrôle. Elle peut être utilisée par différents système (filtrage, gestion de la QOS…)
Adduction	Cheminement de liens (fibres optiques ou câbles en cuivre) entre le point de concentration du réseau du titulaire et l'équipement réseau dans le site du bénéficiaire. Lorsque deux liens passent par le même chemin, il s'agit d'une adduction simple, lorsque deux liens passent par des chemins distincts, il s'agit d'une adduction double.
Administration	La DINUM et les bénéficiaires du marché
ADSL	*Asymmetric Digital Subscriber Line* : technologie de communication numérique de la famille xDSL. Elle permet d'utiliser une ligne téléphonique, une ligne spécialisée, ou encore une ligne RNIS pour transmettre et recevoir des données numériques de manière indépendante du service téléphonique conventionnel. Dans cette technologie le débit entrant et sortant ne sont pas forcément identiques.
API	*Application Programming Interface*, est un ensemble normalisé de classes, de méthodes, de fonctions et de constantes qui sert de façade par laquelle un logiciel offre des services à d'autres logiciels.
AS	*Autonomous System* : ensemble de réseaux dont la politique de routage interne est cohérente. Un *AS* est généralement sous le contrôle d'une entité ou organisation unique.
Bénéficiaires des accès	Entité de l'Administration qui commande et utilise les services en fonction et pour répondre à ses besoins

Sigle ou Terme	Description
CCAG	Cahier des clauses administratives générales applicable à l'accord-cadre
CCAP	Cahier des clauses administratives particulières de l'accord-cadre
CCTP	Cahier des clauses techniques particulières de l'accord-cadre
CE router	*Customer Edge Router* : Dans un réseau MPLS *(Multiprotocol Label Switching*) le routeur CE est l'équipement de routage IP raccordé à un routeur PE (*Provider Edge*),
CHORUS	Système d'information financier de l'État
Code RIE	Référence utilisée par le RIE pour identifier les accès RIE de façon unique
DAT	Dossier d'Architecture Technique
DDoS	*Distributed Denial of Service* (DDoS) = déni de service distribué
Epine dorsale du RIE	Cœur du réseau du RIE (*backbone* en anglais) sur lequel viennent se raccorder l'ensemble des services fournis à ses bénéficiaires (collecte, communication interministérielle, raccordement à leur centre de production, accès Internet).
Extranet RIE (NExt)	L'Extranet RIE est un portail accessible par les bénéficiaires pour instruire et suivre leurs commandes, leurs incidents et leur parc. Les titulaires n'ont pas accès à L'Extranet RIE.
FO ou FTTO	Fibre optique (*Fiber to the office*) : fibre dédiée, avec un débit symétrique et garanti
FTTH	*Fiber to the home :* offre grand public d'accès à Internet à très haut débit en fibre optique de « bout en bout » : ▪ Fibre optique depuis le cœur de réseau du titulaire jusqu'à la « Box » du bénéficiaire
FTTLA	*Fibre to the last active* : offre grand public d'accès à Internet à très haut débit en fibre optique jusqu'au dernier équipement actif : ▪ Fibre optique depuis le cœur de réseau du titulaire jusqu'à son dernier équipement actif ▪ Câble coaxial sur les derniers mètres entre l'équipement actif du titulaire et la « Box » du bénéficiaire
FFTx	Offre grand public d'accès à Internet à très haut débit en fibre optique équivalente à du FTTH ou FTTLA
Gbps	Giga (10^9) bits par seconde

Sigle ou Terme	Description
GTR	Garantie de Temps de Rétablissement du Service
HO	Heures ouvrées : du lundi au vendredi de 8 heure à 19 heure
HNO	Plages horaires en dehors des Heures ouvrées
HSPE	*High speed provider Edge*
IPv6	*Internet Protocol* version 6
IP	*Internet Protocol*
IPSEC	*Internet Protocol Security* : protocole permettant de sécuriser le transit des données.
L2VPN	Réseau privé virtuel dans lequel transite des trames appartenant à la couche 2 du modèle OSI. Il s'agit généralement de trames Ethernet.
L3VPN	Réseau privé virtuel dans lequel transite des datagrammes appartenant à la couche 3 du modèle OSI. Il s'agit généralement de datagrammes IP ou IPv6.
LAN	*Local Area Network* : réseau local
Mbps	Méga (10^6) bits par seconde
Migration	Ensemble des actions nécessaires pour la bascule et la reprise du réseau existant par les nouveaux titulaires dans le périmètre respectif de leur lot
MOM	Mise en Ordre de Marche
MTU	*Maximum transmission unit*
Point de concentration	Point de connexion à l'épine dorsale du RIE pour les services de collecte.
PE router	*Provider Edge router* : équipement d'entrée dans un réseau MPLS
PFAI	Plateforme d'accès à Internet
PFS	Plateforme de service
PLS	Plateforme de livraison de service

Sigle ou Terme	Description
POM	**Passerelle Outre-Mer** : ensemble d'équipements actifs et installés dans les locaux de l'État, permettant d'interconnecter un territoire à l'Hexagone et, le cas échéant, les territoires voisins entre eux au sein d'une même zone ; elle contient au minimum : ▪ Un accès à la collecte locale (dénommé « *porte de collecte opérateur local* ») issu des lots 1 et 2 de « collecte DROM » pour les zones Atlantique et Océan Indien et de marchés spécifiques (hors périmètre de ce CCTP) en zone Pacifique ; ▪ Un accès de transit vers l'Hexagone et au moins un des territoires ultramarins voisins de la même zone géographique (« *liaison transocéanique* ») et des équipements de *chiffrement interministériel* au titre des lots 3, 4 et 5 de « transit Outre-Mer ».
PoP	*Point of Presence* : point d'accès au cœur de réseau du titulaire
PSE	Prestations supplémentaires éventuelles
QoS	*Quality of Service* = Qualité de service
Porte de collecte d'opérateur	Equipement actif propriété du titulaire placé en frontal des routeurs de l'épine dorsale du RIE en Hexagone qui reçoit l'ensemble des flux de collecte du titulaire et qui assure l'interconnexion du réseau de collecte du titulaire avec le reste du RIE par l'intermédiaire de son raccordement au routeur RIE de l'épine dorsale (*backbone*) IP du RIE ou des équipements d'interconnexion de la POM en Outre-Mer.
SDSL	*Symmetric Digital Subscriber Line* : lien de technologie cuivre, la bande passante descendante (*download*) est égale à la bande passante montante ou en émission (*upload*).
Service de transit de type « Entreprise » résilient et à débit garanti	Service permettant la communication entre plusieurs équipements du pouvoir adjudicateur, à bande passante garantie en fonctionnement nominal, et apte à maintenir ou rétablir rapidement un niveau de service, éventuellement dégradé, en cas d'avarie(s) matérielle(s) ou logicielle(s).
Service de transit de type « Internet »	Service permettant la communication des sites du pouvoir adjudicateur vers Internet, à bande passante garantie en fonctionnement nominal, et apte à maintenir ou rétablir rapidement un niveau de service, éventuellement dégradé, en cas d'avarie(s) matérielle(s) ou logicielle(s).
Site RIE	Adresse géographique d'un ou plusieurs services de l'État qui est desservie par un ou plusieurs accès RIE. Un site accède alors au RIE au travers de la **collecte locale** puis de la **liaison avec l'Epine dorsale**.

Sigle ou Terme	Description
SPOF	*Single point of failure* : point de défaillance unique
Utilisateur final	Utilisateur d'un des bénéficiaires
VA	Vérification d'Aptitude
VRF	***Virtual routing and forwarding*** est une technologie qui permet à plusieurs instances d'une table de routage de coexister dans le même routeur en même temps.
VPN	*Virtual Private Network* : Permet d'avoir un réseau privé et sécurisé, partagé sur des infrastructures privées/publiques. Il existe actuellement près de 200 VPN distincts sur le RIE.
VDS	Vie de service
VDSL	*Very high-speed rate digital subscriber line* : lien de technologie cuivre, la bande passante descendante à haut débit (*download*) est asymétrique à la bande passante montante ou en émission (*upload*).
VSR	Vérification du Service Régulier

1.2 Présentation des précédents besoin et accords-cadres

Le besoin précédemment couvert était alloti en cinq lots, selon un découpage légèrement différent de celui retenu pour les présents accords-cadres. En particulier, le lot 1, qui regroupait les réseaux de collecte de l'ensemble des DROM, a été scindé en deux lots distincts, correspondant aux deux zones géographiques couvertes : la zone Atlantique, d'une part, et la zone Océan Indien, d'autre part.

La première différence importante entre le précédent dispositif et les présents accords-cadres concerne les prestations de chiffrement. Celles-ci étaient précédemment assurées par l'Administration dans le cadre d'un marché spécifique. Dans le cadre des présents accords-cadres, l'Administration demande que le chiffrement soit assuré par les opérateurs titulaires, pour l'ensemble des flux appelés à transiter hors du territoire national français, quel que soit le ou les lots dont ils sont titulaires.

La deuxième différence notable porte sur les modalités d'interconnexion entre, d'une part, les réseaux de collecte des lots 1 « Atlantique » et 2 « Océan Indien », ainsi que ceux de la zone Pacifique, et, d'autre part, les services de transit au sein de la POM, puis entre les services de transit des lots 3 « Atlantique », 4 « Océan Indien » et 5 « Pacifique » et l'épine dorsale située en Hexagone. Dans le cadre des présents accords-cadres, le titulaire d'un lot de transit interconnecte des réseaux L3VPN aux

deux extrémités de sa prestation : la POM locale du territoire ultramarin concerné et les points d'interconnexion retenus avec l'épine dorsale du RIE en Hexagone. Au sein de la POM, le titulaire déploie une Plateforme de Livraison de Services en territoire ultramarin (PLS OM), qui permet les nouveaux raccordements directs ainsi que le raccordement de la Plateforme de Services en territoire ultramarin (PFS OM).

La troisième différence notable concerne la fourniture de cette PFS OM. Cette plateforme est dédiée aux échanges entre les VPN des communautés présentes sur le périmètre de la POM concernée.

1.3 Parties prenantes et organisation

1.3.1 Pouvoir Adjudicateur

Le Pouvoir Adjudicateur des présents accords-cadres est représenté par la Direction des services administratifs et financiers (DSAF) du Premier Ministre.

1.3.2 Département Infrastructure et Services Opérés (ISO)

La DINUM est le maître d'ouvrage de l'exécution des accords-cadres.

A ce titre, la DINUM assure l'ensemble des tâches liées aux commandes, aux opérations de vérification, de recettes et de suivis des prestations des titulaires. Les quatre pôles décrits ci-après du département ISO de la DINUM sont directement impliqués dans ces processus.

1.3.2.1 Le Pôle Pilotage de la Qualité et des Partenariats (PQP)

Le pôle Pilotage de la Qualité des Partenariats assure non seulement les relations avec les partenaires contractuels mais aussi les relations avec les bénéficiaires du RIE. Il traite ainsi les besoins spécifiques « sur mesure » des bénéficiaires, nécessitant des études et le cas échéant, un devis de la part des titulaires des marchés. Une fois le besoin précisé et le devis élaboré, le processus reprend tel celui d'une commande « classique » notamment en termes de validation des mises en ordre de marche.

1.3.2.2 Le Pôle Production (ROC - Request Operations Center)

Le pôle Production gère l'ensemble des changements, mineurs et majeurs, à appliquer à la demande des bénéficiaires sur les accès du RIE utilisés par ces derniers.

Au titre de ses missions, il instruit, fait réaliser et s'assure de la bonne exécution des demandes de changements émises par les bénéficiaires des services du RIE entrés en « vie de service » (VDS). Dans ce but, le pôle Production conçoit et le pôle SI-RIE développe un système d'information permettant la gestion des demandes de changements formulées par les bénéficiaires du RIE et transmises aux titulaires des marchés via des interfaces de programmation d'application (API).

Le pôle ROC traite en outre tout ce qui relève d'un ensemble de commandes traitées en mode « projet » (chefferie de projet pour un suivi spécifique, massification en vue d'un traitement automatisé…).

Il a également la responsabilité de la bonne exécution de ces demandes, en particulier il procède à la validation des productions des titulaires.

Enfin, le ROC est chargé de rendre compte du traitement des commandes auprès des instances de pilotage et auprès des bénéficiaires.

1.3.2.3 Le Pôle Hypervision (NOC - Network Operations Center)

Le pôle Hypervision exerce les fonctions de supervision réseau du RIE et des services associés. Fonctionnant sans interruption tous les jours de l'année et 24 heures sur 24 (24/7), il assure la veille permanente du bon fonctionnement et de la sécurité du RIE et des services associés.

A ce titre, il est chargé :

- De contrôler en permanence l'état du RIE et des services associés ;
- De détecter et piloter la résolution des incidents réseau du RIE et des services associés ;
- D'alerter au plus tôt d'un dysfonctionnement pour engager sa résolution par les acteurs concernés ;
- De piloter le rétablissement du service en liaison avec les chaînes de soutien ministérielles, les industriels partenaires concernés ;
- D'assurer l'interface opérationnelle privilégiée des industriels partenaires de la DINUM et des chaines de soutien ministérielles (CSU), notamment en matière de communication ;
- D'alerter l'équipe sécurité de la DINUM (CSIRT-DINUM) en cas de soupçon d'incidents de sécurité ou de risque cyber ;
- D'apporter assistance aux utilisateurs du RIE et des services associés via leur chaine de soutien ministérielle ;
- De participer à l'élaboration, la qualité et la fiabilité des statistiques et des indicateurs composant le tableau de bord du département ISO de la DINUM.

1.3.2.4 Le Pôle Services Opérés d'Infrastructures (SOI)

Le pôle SOI est chargé de concevoir, de piloter la mise en œuvre et d'assurer le maintien en condition opérationnelle (MCO) et de sécurité (MCS) les architectures et services mutualisés déployés dans le cadre du réseau interministériel de l'Etat.

De façon synthétique, les équipes du pôle SOI sont composées d'experts, d'architectes et de chefs de projet en charge de la conception et du pilotage des projets d'évolution de :

- Ensemble des composants de l'épine dorsale (POP, PLS, RED, etc.) ;
- Architecture réseau MPLS du RIE comprenant épine dorsale et collecte ;
- Plateformes de services permettant les échanges interministériels (PFS) ;
- Plateforme de service permettant l'accès au réseau Internet (PFAI) ;
- Interconnexions avec les réseaux partenaires ;
- Architecture générale du raccordement des DROM et COM au RIE.

Par ailleurs, ces mêmes équipes assurent :

- L'expertise de haut niveau dans la vie courante et l'exploitation de l'ensemble de ces composants ;
- Le pilotage des infogérants en spécifiant précisément tout changement mis en œuvre pour répondre aux besoins des bénéficiaires.

1.3.2.5 Le Pôle Système d'information (SI RIE)

Le système d'information SI-RIE supporte les différentes activités du département ISO, Il est accessible à la fois des collaborateurs du département et des bénéficiaires via un portail « Extranet ».

Le pôle SI RIE assure :

- Le maintien en conditions opérationnelles (MCO) et de sécurité (MCS) du SI-RIE ;
- Le pilotage et la mise en œuvre des évolutions de ce SI.

Le pôle SI RIE pilote et met en œuvre la stratégie de mise en place d'API sous-tendant l'industrialisation des échanges avec les opérateurs et les bénéficiaires.

1.3.3 Interlocuteurs pour la cybersécurité (CSIRT)

Tous les événements de sécurité du périmètre de la DINUM sont gérés par son CSIRT (Computer Security Incident Response Team) qui contribue au système d'astreinte mis en œuvre à la DINUM. Celui-ci assure la coordination avec les autres structures spécialisée de l'État, principalement le CERT-FR de l'ANSSI.

A ce titre, il est chargé :

- D'assurer le suivi des Comités Sécurité (COSEC), notamment la revue régulière des vulnérabilités et du plan de remédiation associé ;
- De prendre en charge les incidents de sécurité après leur identification par le NOC RIE ;
- De coordonner les actions de réponse à incidents de sécurité au sein des ministères et avec les partenaires étatiques (notamment le CERT-FR) ;

- De contribuer au renforcement des capacités de cybersécurité du RIE, incluant des missions d'analyse avancée, de veille proactive et de recommandations stratégiques.

1.3.4 Bénéficiaires

Les bénéficiaires regroupent l'ensemble des ministères, directions et entités de l'Administration dont les sites sont raccordés au RIE listés à l'annexe 1 du CCAP.

Chapitre 2 : Présentation du RIE

2.1 Présentation générale

Le réseau interministériel de l'Etat (RIE) est un réseau unifié de communications numériques raccordant l'ensemble des administrations de l'État, conçu et exploité sous la responsabilité de la DINUM.

En qualité de support d'applications fédératrices interministérielles ainsi que d'applications métiers ministérielles, le RIE à vocation à être étendu afin d'intensifier les usages et ceci dans un cadre global d'amélioration de la sécurité, de la résilience, des débits et de fourniture de nouveaux services.

Les objectifs associés sont d'une part, de gagner en efficience en rationalisant son exploitation d'un point de vue économique et organisationnel et en mettant en place des services interministériels fédérateurs et d'autre part, d'augmenter sa résilience vis-à-vis d'attaques, de malveillance, de pannes.

La mise en place de ces évolutions du réseau interministériel de l'État s'inscrit dans le double contexte de la modernisation de l'Etat et de la montée générale et continue des menaces sur la sécurité des systèmes d'information, nécessitant une évolution en profondeur des infrastructures et de leur maîtrise.

Pour rappel, les principes qui dictent la réalisation du réseau interministériel de l'État et ses évolutions sont les suivants :

- Des choix technologiques pérennes :
  - Cœur du réseau à haut débit, IPv4 et IPv6 optimisant durablement le fonctionnement du réseau ;
- Une résilience forte :
  - Maillage fin pour résister aux pannes locales et aux dysfonctionnements ponctuels ;
  - Autonomie vis-à-vis de réseaux tiers et notamment d'Internet ;
  - Sécurisation en profondeur des flux pour détecter en amont les attaques ;
- Une souplesse dans les modes de raccordement :
  - Plusieurs types d'accès proposés pour répondre à la diversité des sites, des besoins en débit et en disponibilité ainsi que des contraintes géographiques ;
  - Progressivité des raccordements en fonction de la fin des contrats existant voire en anticipation ;
  - Accès sécurisé à Internet ;
- Un contrôle effectif des éléments clés :

- Forte maîtrise d'ouvrage par la DINUM pour assurer le pilotage et garantir la maîtrise des évolutions du réseau et de son exploitation.

2.2 Présentation de l'épine dorsale du RIE

L'épine dorsale du RIE est un réseau de transports de flux multi-protocoles. Il est constitué de plusieurs équipements actifs de réseaux raccordés entre eux à 100Gbit/s grâce à des liaisons optiques fournis par deux opérateurs nationaux. Ces équipements, propriétés de l'Etat, sont hébergés dans des centres de production informatiques gérés par les bénéficiaires (POP RIE).

Son rôle principal est de transporter les flux des bénéficiaires de manière cloisonnée entre le centre de production et l'utilisateur final. C'est sur cette épine dorsale que sont raccordées les collectes (Outre-Mer, international et Hexagone), les centres de productions informatiques des bénéficiaires et les services avancés fournis par la DINUM (communication interministérielle sécurisée, accès Internet sécurisé).

En 2025, trois de ces points de présence hébergent des équipements sur lesquels viennent s'interconnecter l'ensemble des réseaux de transit transocéanique des titulaires des lots 3, 4 et 5 du présent marché.

2.3 Application aux territoires d'Outre-Mer

Une « POM », Passerelle Outre-Mer, est un point de présence ultramarin qui regroupe les équipements actifs déployés dans le cadre des différents lots du présent marché et installés dans les locaux de l'État. Il faut noter qu'actuellement une seule et unique POM existe dans chaque département ou territoire d'Outre-Mer.

En 2025, les POM sont présentes :

- Pour la zone Atlantique : à Saint-Martin, en Guadeloupe, en Martinique et en Guyane ;
- Pour la zone Océan Indien : à la Réunion et à Mayotte ;
- Pour la zone Pacifique : en Nouvelle-Calédonie et en Polynésie Française.

Une POM permet d'interconnecter un territoire à l'Hexagone et, le cas échéant, les territoires voisins entre eux au sein d'une même zone. A cette fin, elle comprend au minimum :

- Un accès à la collecte locale (dénommé « porte de collecte opérateur local ») grâce au lot 1 et 2 ou à des marchés spécifiques dans les cas de la Polynésie Française et de la Nouvelle-Calédonie ;
- Un accès de transit chiffré vers l'Hexagone (« liaison transocéanique ») et entre les territoires voisins au sein d'une même zone grâce aux lots 3, 4 et 5 ;

- Une extension de l'épine dorsale dénommée « PLS OM » pour Plateforme de Livraison de Service Outre-Mer déployée entre collecte (lots 1 et 2) et transit sécurisé (lots 3, 4 et 5). Cette PLS OM permet les raccordements directs de bénéficiaires et les raccordements des plateformes de service incluses.

La POM est susceptible d'héberger d'autres briques fonctionnelles :

- Une plateforme de service (PFS OM) dédiée permettant aux différents bénéficiaires présents sur le territoire ultramarin considéré d'échanger entre leurs VPN respectifs sans avoir à remonter jusqu'au service équivalent de PFS situé en Hexagone ;

2.4 Quantité estimative du nombre de sites ultramarins

2.4.1 Liste des points d'interconnexion des transits transocéaniques à l'épine dorsale du RIE en Hexagone

Point d'interconnexion au RIE	Adresse
PA1 Mont Valérien Ministère des armées	Fort du Mont Valérien 92150 Suresnes
PA3 Rosny Ministère de l'intérieur	Fort de Rosny, 1 Bd Théophile Sueur 93100 Rosny-sous-Bois
Toulouse (pour accès Internet) Ministère de l'agriculture	2 route de Narbonne 31326 Castanet-Tolosan

2.4.2 Liste des Passerelles Outre-Mer (POM)

Zone géographique	Site d'implantation de la POM	Niveau de service minimal exigé
Atlantique	**Guadeloupe** Hôtel de police les Abymes ZAC Boissard Laffond 97139 Les Abymes	Lots 1 et 3 : Maximum
	Martinique Gendarmerie nationale Caserne Redoute 97200 Fort de France	Lots 1 et 3 : Maximum
	Saint-Martin Cité Administrative Concordia 97150 Saint-Martin	Lots 1 et 3 : Très élevé

Zone géographique	Site d'implantation de la POM	Niveau de service minimal exigé
	Guyane Ministère des armées DIRISI Cayenne Quartier de la Madeleine 97306 Cayenne Cedex	Lots 1 et 3 : Maximum
Océan indien	**Réunion** Préfecture 4, Place de la République 97400 Saint-Denis	Lots 2 et 4 : Maximum
	Mayotte Préfecture Avenue de la préfecture 97600 Mamoudzou	Lots 2 et 4 : Fort
Pacifique	**Polynésie française** Ministère des armées DIRISI Papeete Caserne Lieutenant-Colonel Broche 98701 Arue	Lot 5 : Très élevé
	Nouvelle-Calédonie Cour d'appel 1, rue de Metz 98800 Nouméa	Lot 5 : Très élevé

2.4.3 Nombre d'accès de collecte (hors POM) par territoire

2.4.3.1 Périmètre des lots 1 et 2

Zone géo-graphique	Code DROM	Territoire ultramarin	Nombre d'accès	dont FO/FTTH (lien principal)	dont xDSL (lien principal)	dont sécurisés (double lien)
Lot 1						
Atlantiq	971	Guadeloupe	121	64	57	14

ue	972	Martinique	103	62	41	19
	973	Guyane	115	75	40	23
	977 978	Saint-Martin Saint-Barthélemy	28	15	13	1
	Sous-total Atlantique (**Lot 1**)		0	367	216	151
Lot 2						
Océan indien	974	La Réunion	152	107	45	25
	976	Mayotte	72	35	37	9
	Sous-total Océan indien (**Lot 2**)		0	224	142	82
Total général			591	358	233	91

2.4.3.2 Hors périmètre des lots 1 et 2 (pour information)

Zone géographique	Code COM	Territoire ultramarin	Nombre d'accès
Atlantique	975	Saint-Pierre et Miquelon	9
Pacifique	986	Wallis et Futuna	6
	987	Polynésie française	53
	988	Nouvelle Calédonie	62

Chapitre 3 : Définition du besoin

3.1 Infrastructures des titulaires des lots 1 à 5 et 7

3.1.1 Confidentialité des informations transportées

Le service de connectivité des sites des bénéficiaires garantit le caractère privé des échanges sur son infrastructure. Les communications des différents clients sont bien cloisonnées même si elles partagent des supports physiques communs. Néanmoins, et en particulier pour le lot 1 et 2, il n'est pas demandé explicitement de prestation de chiffrement dans le cadre de ces marchés, sauf en cas, a priori exceptionnel et donc dûment documenté, de nécessité de transit des flux opérés en dehors de l'espace territorial français.

{PP-L1 à 5 & 7/01}. 3.1.1 Confidentialité des informations transportées : Description des moyens mis en œuvre pour garantir le caractère privé des échanges.

3.1.2 Conformité

Le titulaire est en conformité avec la réglementation nationale et internationale en vigueur concernant la fourniture de services de télécommunications (ITU-T, ISO, ETSI…).

En outre, les services proposés respectent les standards émis par les organismes de normalisation, ainsi que les guides de bonnes pratiques de l'ANSSI en termes d'architecture, d'administration et de sécurité des réseaux.

3.1.3 Typologies de la sécurisation des infrastructures

Le tableau ci-dessous décrit le référentiel de l'Administration en matière de typologie de la sécurisation des accès dans le cadre du RIE.

Niveaux	Boucle locale			Equipement d'extrémité site client	Garantie d'absence de point individuel de défaillance
	Rattachement	Adduction/ cheminement	Pénétration site client		
Type 1	1 POP	Simple	Simple	Simple	Non
Type 2	1 POP	Simple	Simple	Double	Non
Type 3a	1 POP	Double	Simple	Double	Non
Type 3b	1 POP	Double	Double	Double	Non
Type 4	2 POP	Simple	Simple	Double	Non
Type 5	2 POP	Double	Simple	Double	Non
Type 6	2 POP	Double	Double	Double	Bout en bout

3.1.4 Gestion des équipements d'extrémité

Les routeurs de site sont tous les équipements du titulaire installés sur les sites des bénéficiaires, y compris ceux installés sur les sites des POM.

Le titulaire fournit, installe, administre et maintient l'ensemble des équipements et des systèmes d'exploitation et les paramètres de configuration nécessaires au service.

Les équipements déployés sur la POM sont équipés de double alimentation pour garantir une résilience électrique alignée sur le niveau de résilience délivré par le centre hébergeur (objectif de 2 voies d'alimentation ondulées).

Les équipements d'extrémité recouvrent également les Équipements d'Accès au Service (EAS) à chaque extrémité des liens en protocole Ethernet (niveau 2) à haut débit pour le transport de données. Ces EAS doivent disposer d'une capacité de 1Gbps minimum à adapter au besoin.

L'opérateur aura en charge la fourniture des modules SFP correspondant au type de connexion commandé (type SR, LR, etc.).

3.1.4.1 Caractéristiques des équipements d'extrémité

Les caractéristiques minimales des routeurs de site sont :

- Fonctions de base des équipements :
  - IPv4 et IPv6 au même niveau ;
  - Fonction VRRP vers le LAN du bénéficiaire ;
  - Routage dynamique BGP vers un équipement du bénéficiaire ;
  - Relai DHCP ;
  - Typologies LAN souhaitées :
    - Mode 1 : Le routeur de site est la passerelle du LAN client ;
    - Mode 2 : Le routeur de site route le trafic vers un équipement géré par le bénéficiaire ;
    - Mode 3 : Mode 1 et Mode 2 suivant les besoins du site.
  - Capacité à gérer des ACL de filtrage étendues (locales) et des ACL de marquage ;
  - Une interface WAN ;
  - Interfaces LAN Ethernet 100 Mbps et 1Gbps (par défaut cuivre et optionnellement en fibre) selon le besoin du ministère (minimum 3 interfaces physiques LAN) ;

- Les interfaces LAN doivent pouvoir gérer plusieurs sous interfaces selon le protocole 802.1Q (VLAN) ;
- Supports de VPN multiples : Ces VPN sont portés par des interfaces physiques différentes ou par des sous-interfaces VLAN ;
- Possibilité de router vers des LAN cascadés (exemple : accès à une DMZ) ;
- Activation Netflow vers un serveur centralisé du client ;
- Gestion de profil QOS (ToS / DiffServ) en mode trust ou forcé vis-à-vis des paquets entrants côté LAN ;
- Gestion du marquage des Flux temps réels (classe voix et vidéo) ;
- Exploitation, supervision par différentes entités avec les protocoles déjà utilisés par la DINUM (SSH, SNMPv3, Syslog over TLS) ;
- Réglage automatique de l'horloge via le protocole NTP ;
- Taille maximale de 1U et maximum 1 ressource électrique aux normes locales ;
- Installation obligatoire dans une baie 19 pouces (un kit de pose en baie est fournie si l'équipement n'est pas nativement compatible).

- Fonctions additionnelles minimales (« à la carte ») des équipements sont :
  - Nombre de ports supplémentaires ;
  - Fonctions supplémentaires dans l'offre de service inscrites au catalogue du titulaire.

{EX-L1 & 2/01} 3.1.4.1 Caractéristiques des équipements d'extrémité : Les équipements disposent des caractéristiques minimales décrites dans le CCTP.

{PP-L1 à 5 & 7/02}. 3.1.4.1 Caractéristiques des équipements d'extrémité : Description des caractéristiques minimales.

{PP-L1 à 5 & 7/03}. 3.1.4.1 Caractéristiques des équipements d'extrémité : Description des fonctions additionnelles et de leurs caractéristiques.

{PP-L1 à 5 & 7/04}. 3.1.4.1 Caractéristiques des équipements d'extrémité : Description des équipements en fonction des niveaux d'engagement de service en précisant notamment le fournisseur, le modèle et les dimensions physiques, les configurations logicielles et versions installées.

{PP-L1 à 5 & 7/05}. 3.1.4.1 Caractéristiques des équipements d'extrémité : Précisions sur les limites techniques et fonctionnelles des équipements.

{PP-L1 à 5 & 7/06}. 3.1.4.1 Caractéristiques des équipements d'extrémité : Précisions sur l'évolutivité matérielle techniques et fonctionnelles des équipements.

En sus des routeurs pour les accès dits de niveau 3, le titulaire fournit des équipements d'extrémités (EAS) pour un service de réseau de type Ethernet (niveau 2) à 1 Giga Ethernet ou 10 Giga Ethernet ou équivalent qui :

- Supporte les VLAN (802.1q) ;
- Supporte les VLANs stacking (802.1ad) aussi appelé QinQ;
- Est transparent au «spanning tree» ;
- Gère la qualité de service (802.1p).

3.1.4.2 Qualité des configurations des équipements d'extrémité

Le titulaire déploie des configurations propres et optimisées, respectant les bonnes pratiques applicables (utilisant le moins de ressources possibles, code commenté dans les documents, industrialisation maximale…), en particulier en termes de sécurité si l'ANSSI a rédigé un guide sur le périmètre concerné.

Les configurations des équipements respectent les règles suivantes :

- Le nommage (identification) des équipements (éléments de configuration) est homogène et respecte une règle fournie par la DINUM ;
- Les configurations des équipements qui portent les mêmes services sont homogènes : les règles de paramétrage sont identiques et transposables ;
- Les équipements de même nature et affiliés à des mêmes niveaux de services possèdent des versions d'OS identiques.

Cette maîtrise des configurations est stable et pérenne.

Les composants mis en œuvre par le titulaire font l'objet d'une minimalisation et d'un durcissement en termes de sécurité :

- Limitation du nombre d'applications en écoute sur le réseau ;
- Désactivation des fonctionnalités inutiles ;
- Suppression des comptes et mots de passe constructeurs.

Tout écart des équipements, par rapport à l'état de l'art, fait l'objet d'une justification soumise à validation de la DINUM. Il s'agit notamment des écarts :

- Avec le référentiel général de sécurité (RGS) ;
- Avec le guide d'hygiène informatique ;
- Avec les guides de bonnes pratiques de l'ANSSI ;
- Avec des fonctionnalités non supportées par un équipement et nécessaires à la fourniture du service ;
- Avec les types d'équipements qualifiés par l'ANSSI, quand il en existe.

{PP-L1 à 5 & 7/07}. 3.1.4 Qualité des configurations des équipements d'extrémité : Description de la politique de gestion des configurations des équipements d'extrémité.

3.1.4.3 Procédure de validation des configurations des équipements d'extrémité

Quelle que soit l'origine du changement sur un équipement, le titulaire :

- Informe systématiquement la DINUM de toute création ou modification de configuration d'un équipement avant sa mise en œuvre ;
- Communique les configurations, objet de ces changements, sous un format et via un canal tous deux convenus avec la DINUM, pour leur validation.

Lors des opérations programmées, le titulaire fournit une procédure de validation des mises à jour et les éléments suivants :

- Les versions d'OS ;
- La configuration complète et commentée ;
  - Avec un obscurcissement possible des secrets de configuration ;
  - Avec la mise en évidence des modifications par rapport à une version antérieure (exemple : fichier au format diff) ;
- La liste des services ouverts et leur usage ;
- La liste des impacts potentiels sur le service.

Pour rappel, les configurations en vigueur sont mises à disposition de la DINUM de façon automatisée et sécurisée, a minima après chaque changement opéré.

3.1.4.4 Procédure de sauvegarde des configurations

Le titulaire met en œuvre une procédure de sauvegarde et de restauration (retour-arrière) de chaque version des configurations de ses équipements.

Les procédures de restauration sont régulièrement validées sur un environnement de test.

{PP-L1 à 5 & 7/08}. 3.1.4 Procédure de sauvegarde des configurations : Description de la procédure de sauvegarde et de restauration.

3.1.4.5 Gestion des correctifs de sécurité des équipements d'extrémité et des équipements déployés au sein des POM

Le titulaire met en œuvre des mécanismes de sécurité afin d'assurer une défense contre les attaques classiques contre les réseaux et les protocoles associés.

Au titre de la maintenance et du maintien en conditions de sécurité, le titulaire :

- Suit les évolutions logicielles des éditeurs de façon à être en mesure de se procurer les correctifs de sécurité mis à disposition régulièrement ;

- Surveille au moins les avis et les alertes d'un CERT ou du CERTFR ;
- Applique les correctifs de sécurité qui sont proposés par les éditeurs, dans les documents du CERTFR ou, le cas échéant, demandés explicitement par l'Administration.
- Partage son tableau de bord SSI avec la cellule Cyber de la DINUM et le présente lors des comités de sécurité

{EX-L1 à 5 & 7/02}. 3.1.4 Gestion des correctifs de sécurité des équipements d'extrémité : Le titulaire prohibe l'utilisation sur ses plates-formes des systèmes et logiciels obsolètes référencés par le CERTFR.

Si aucun correctif de sécurité n'est disponible auprès de l'éditeur, le titulaire suit les recommandations du CERTFR, dans le cadre d'un contournement provisoire.

Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le titulaire propose des mesures permettant d'éviter l'exploitation de la vulnérabilité.

Le titulaire maintient un état technique de parc, récapitulant les versions logicielles, vulnérabilités identifiées et mesures de contournement mises en œuvre.

L'état technique de parc est actualisé et mis à disposition :

- Au plus tard pour chacune des réunions du Comité sécurité « COSEC » ;
- Sur demande de la DINUM.

{PP-L1 à 5 & 7/09}. 3.1.4 Gestion des correctifs de sécurité des équipements d'extrémité : Description du maintien et du suivi de l'état technique de parc des équipements en précisant notamment sa fréquence d'actualisation, le moyen de mise à disposition.

3.1.4.6 Administration des équipements d'extrémité

Le titulaire utilise des modes d'accès sécurisés et notamment des mots de passe d'accès aux équipements d'extrémité différents de ceux utilisés pour ses autres clients.

Ces mots de passe sont systématiquement différents des mots de passe constructeur ou par défaut.

La gestion des configurations, matérielles et logicielles des équipements, des raccordements et des services réseaux associés, est effectuée exclusivement par les personnels du titulaire identifiés chargés de l'exploitation du réseau.

Des mécanismes techniques empêchent l'accès aux équipements par d'autres personnels du titulaire.

L'administration des équipements s'effectue avec les comptes nominatifs des personnels et la base des comptes est centralisée. Toute action des personnels en charge de l'administration des équipements doit être imputable et journalisée.

Les flux destinés à l'exploitation sont impérativement cloisonnés et inaccessibles depuis les réseaux utilisateurs et depuis Internet. Cela concerne notamment :

- Les flux destinés aux sauvegardes/restaurations des équipements ;
- Les flux de journalisation ;
- Les flux d'administration (SSHv2) ;
- Les flux de supervision (SNMPv3).

Le titulaire renouvelle périodiquement les secrets d'authentification des équipements d'extrémité vers les systèmes automatisés permettant leur administration (secrets SNMP, TACACS, clefs publiques d'authentification, etc.).

En particulier, la procédure de renouvellement des secrets d'authentification à destination des services de la DINUM doit garantir la continuité de son service de supervision.

Le titulaire met en œuvre une procédure de renouvellement et de transmission des secrets d'authentification, conformément aux règles d'hygiène et de bonnes pratiques. Plus généralement, le titulaire met en œuvre les recommandations relatives à l'administration sécurisée des systèmes d'information de l'ANSSI.

{PP-L1 à 5 & 7/10}. 3.1.4 Administration des équipements d'extrémité : Description de la politique d'administration des équipements.

3.1.4.7 Commandes des équipements d'extrémité mis à la disposition de l'Administration

Dans le cadre de l'administration des équipements, il est attendu du titulaire de :

- Mettre à disposition la totalité des commandes disponibles sur l'équipement en mode lecture seule, permettant notamment d'offrir des fonctions de *looking-glass* ;
- Fournir les moyens de pouvoir programmer un redémarrage des routeurs ;
- Permettre le changement des paramétrages des interfaces LAN des routeurs ;
- Mettre à disposition, à des fins de traitement des incidents, les commandes qu'il propose en écriture ;
- Permettre des accès en commande SSH sur la gestion des ACL des routeurs ;
- Activer *netflow* vers un serveur centralisé de la DINUM.

{PP-L1 à 5 & 7/11}. 3.1.4 Commandes des équipements d'extrémité mis à la disposition de l'Administration : Description de l'outil de restitution de la configuration de l'interface WAN côté PE en amont.

{PP-L1 à 5 & 7/12}. 3.1.4 Commandes des équipements d'extrémité mis à la disposition de l'Administration : Description des commandes proposées en écriture.

{PP-L1 à 5 & 7/13}. 3.1.4 Commandes des équipements d'extrémité mis à la disposition de l'Administration : Justification des éventuelles limitations.

{EX-L1 à 5 & 7/03}. 3.1.4 Commandes des équipements d'extrémité mis à la disposition de l'Administration : Le titulaire fournit de manière systématique, les configurations des équipements d'extrémité lors de chaque changement.

3.1.4.8 Gestion des journaux d'exploitation des équipements d'extrémité et de ceux déployés au sein de la POM

Le titulaire communique, en temps réel, dans le format protocole « *syslog* », les traces liées aux activités d'administration ou d'exploitation des équipements d'extrémité, notamment les évènements de type AAA/TACACS par exemple (échecs et réussites de connexion, commandes exécutées…) ou issues de la journalisation technique des équipements (journaux d'erreur…).

Ces évènements sont enregistrés et horodatés selon une source de temps fiable.

Le titulaire met en œuvre une architecture d'interconnexion sécurisée afin de permettre au système d'information de l'Administration de récupérer l'ensemble de ces journaux.

{PP-L1 à 5 & 7/14}. 3.1.4 Gestion des journaux d'exploitation des équipements d'extrémité : Description de l'architecture d'interconnexion sécurisée pour le recueil l'ensemble de ces journaux.

Les traces de sécurité issues de la journalisation technique des équipements sont analysées périodiquement par le titulaire afin d'identifier les anomalies éventuelles.

Le titulaire archive également l'ensemble des journaux bruts produits par les différents équipements, éventuellement mutualisés et autres que les équipements d'extrémité dédiés à l'usage de l'Administration, qui concourent à la mise en œuvre du service.

Ces journaux doivent, dans leur intégralité, pouvoir être communiqués à l'ANSSI en cas d'incident de sécurité, dans leur format brut natif.

Tout incident ou comportement anormal susceptible d'avoir un impact sur la sécurité du service fait l'objet d'une alerte. Un compte rendu peut être communiqué, sur demande de l'Administration.

3.1.4.9 Accès en lecture aux configurations par la DINUM

Le titulaire accorde un accès en lecture aux équipements d'extrémité et à ceux déployés au sein de la POM portant le service de l'Administration, afin de consulter et de modifier leur configuration (modification de paramètres…). La DINUM fournit les noms des personnes ayant les accès ou les services pour le cas de comptes génériques (utilisés par des automates internes). Cette liste peut être modifiée régulièrement.

{PP-L1 à 5 & 7/15}. 3.1.4 Accès en lecture aux configurations par la DINUM : Description des impacts sur les engagements de service d'un accès en écriture sur les équipements d'extrémité.

{PP-L1 à 5 & 7/16}. 3.1.4 Accès en lecture aux configurations par la DINUM : Justifications des éventuelles limitations d'un accès en écriture sur les équipements d'extrémité.

Tous les éléments de configuration permettant à la DINUM de réaliser ses propres opérations de validation des productions et de diagnostic de dysfonctionnement sont accessibles.

Le titulaire peut restreindre l'accès en lecture aux éléments secrets faisant partie de la configuration (par exemple, les clefs partagées TACACS, clefs privées SSH, ou encore les empreintes des mots de passe administrateur peuvent faire l'objet d'une anonymisation).

L'accès aux équipements d'extrémité est accordé à des comptes nominatifs ou génériques, associés à des profils d'autorisation.

Ces accès sont uniquement des accès en lecture seule : ils ne doivent en aucun cas permettre de modifier la configuration des équipements d'extrémité, sauf en cas d'autorisation spécifique et explicite pour la mise à jour des ACL des routeurs.

L'activation et l'autorisation de fonctions de diagnostic avancées (ex : capture de flux directement depuis l'équipement) peuvent être ponctuellement demandées pour certains profils.

L'ensemble de ces comptes sont gérés par un serveur d'authentification sécurisé (qui peut être le même que pour les utilisateurs du titulaire). Les utilisateurs de la DINUM sont en mesure de gérer eux même leur mot de passe ainsi que leur données personnelles (nom, prénom…). La continuité des accès aux équipements est assurée après un changement de mot de passe.

3.1.5 Définition des niveaux de service

Les niveaux de service sont fonction :

- De la Garantie du Taux de Disponibilité mensuelle d'un accès (GTD) ;
- De la Garantie du Temps de Rétablissement du service (GTR) ;
- De l'Indisponibilité Annuelle d'un Accès (IAA).

Niveau de service	Garantie du taux de disponibilité mensuelle d'un accès minimum (T_D)	Indisponibilité annuelle d'un accès (IAA) maximale	Niveau de GTR minimale par accès	Plage de garantie
Maximum	T_D > 99,995%	IAA < 1h	GTR Niv3	24/7/365
Très Fort	T_D > 99,99%	IAA < 2h	GTR Niv2	24/7/365
Fort	T_D > 99,98%	IAA < 3h	GTR Niv2	24/7/365
Très Elevé	T_D > 99,90%	IAA < 10h	GTR Niv2	24/7/365
Elevé	T_D > 99,86%	IAA < 8h	GTR Niv1	8-19h/ Jours Ouvrés
Best-effort	-	-	GTR Niv0	8-19h/ Jours Ouvrés

3.1.5.1 Garantie du taux de disponibilité mensuelle d'un accès (GTD)

La disponibilité d'un accès est la permanence des services permettant au bénéficiaire de l'accès d'émettre ou de recevoir en l'absence d'incident de sévérité 1 « Incident critique », quel que soit l'élément mis en cause fourni par le titulaire.

La disponibilité mensuelle d'un accès (T_D) se calcule selon la formule ci-après :

$$T_D = \frac{\text{Temps mensuel de disponibilité}}{\text{Durée de la plage mensuelle de garantie}}$$

En cas de non-respect du Taux de disponibilité mensuelle d'un accès définis par niveaux de service, les pénalités décrites au CCAP s'appliquent.

Dans le cas du service de transit sécurisé, la disponibilité du service s'entend de manière globale concernant le transport et le chiffrement.

3.1.5.2 Indisponibilité annuelle d'un accès (IAA)

Le constat d'indisponibilité concerne les services non fournis d'un accès à survenance d'un incident de sévérité 1 « Incident critique », quel que soit l'élément mis en cause fourni par le titulaire.

L'indisponibilité annuelle d'un accès (IAA) est la somme des temps d'indisponibilité constatée sur une année calendaire. Pour les années incomplètes, le constat d'indisponibilité est proratisé.

En cas de dépassement des temps d'indisponibilité annuelle d'un accès définis par niveaux de service, les pénalités décrites au CCAP s'appliquent.

Pour information, ci-après la correspondance entre les taux de disponibilités **annuelles** et les indisponibilités :

Niveau de service	Taux de disponibilité annuelle	Indisponibilité annuelle pour une plage de	
		24/7/365	Jours ouvrés (8 h - 19h)
Maximum	99,995%	26m 16 s	
Très Fort	99,99%	52m 33 s	
Fort	99,98%	1 h 45m 7 s	
Très Elevé	99,90%	8 h 45m 36 s	
Elevé	99,860%		3 h 50m 59 s

3.1.5.3 Rétablissement du service en cas d'incident

3.1.5.3.1 Définition des niveaux de sévérité des incidents

Les incidents sont des incidents de production / d'exploitation et/ou des incidents / des évènements de sécurité, en définitive tout fait constitutif d'un fonctionnement différent de celui attendu / prévu tel qu'il a été documenté ou reconnu publiquement comme faisant partie des « meilleures pratiques ».

Un incident est un événement qui diminue, dégrade ou interrompt le fonctionnement nominal du service ou qui ne respecte pas les engagements de qualité du service.

La classification de la sévérité des incidents dépend des impacts sur les services :

Niveau de sévérité	Type d'incident	Description
Sévérité 1	Incident critique	Un incident critique correspond à l'un des cas suivants : ▪ Interruption du service ; ▪ Utilisateurs isolés ; ▪ Dysfonctionnement total rendant le service inutilisable ; ▪ Fonctionnement fortement dégradé d'un service ; ▪ Incident qui impacte un nombre important d'utilisateurs.
Sévérité 2	Incident majeur	Un incident majeur correspond à l'un des cas suivants : ▪ Service dégradé comme notamment : - temps de réponse rallongé ; - débit diminué ; - indicateurs de performances altérés ; - qualité de services altérés ; ▪ Non-respect des engagements de qualité de service comme notamment : - taux de perte de paquet ou de trame ; - temps de transit ; - débit IP garanti ; - coupure de certains flux applicatifs ; - bagotements ; - basculement sur la solution de secours ; - mauvais fonctionnement d'un type de flux ; - etc. ▪ Pour un service sécurisé (lien principal / lien secouru) : incident sur l'un des liens même sans dégradation de service.
Sévérité 3	Incident mineur	Un incident mineur correspond à l'un des cas suivants : ▪ Dysfonctionnement transparent pour les utilisateurs ; ▪ Dégradation mineure du service sans impacter directement l'utilisation des services.
Sévérité 4	Demande d'information	Les demandes d'information auprès des titulaires sont intégrés à la gestion des incidents. Il ne s'agit pas d'incident à proprement parler cependant leur délai de réponse est défini au Bordereau des délais.

{PP-L1 à 5 & 7/17}. 3.1.5.3.1 Définition des niveaux de sévérité des incidents : Définition des niveaux de complexité « simple », « moyen » et « élevé » des « incidents » de niveau de sévérité 4 (Demande d'information).

3.1.5.3.2 Garantie du temps de rétablissement du service (GTR)

La GTR s'applique sur l'accès d'un site selon la sévérité des incidents :

GTR par accès d'un site	Incident critique	Incident majeur	Incident mineur	Plage de prise en compte de la garantie
GTR Niv0	10h	J+5 = 55h	J+7 = 77h	8-19h/Jours Ouvrés
GTR Niv1	4h	J+2= 22h	J+5= 55h	8-19h/Jours Ouvrés
GTR Niv2	4h	12h	96h	24/7/365
GTR Niv3	2h	6h	72h	24/7/365

Pour chaque incident, en cas de dépassement des temps de rétablissement du service d'un accès définis par niveaux de service, les pénalités décrites au CCAP s'appliquent.

3.1.6 Raccordement de la POM au réseau de collecte multi-VPN

La prestation de raccordement des infrastructures de la POM au réseau de collecte des lots 1 et 2 est commandée dès la notification de l'accord-cadre.

Dans le marché précédent, un seul site d'hébergement de la POM existait. Il héberge le service de concentration de la collecte dénommé porte de collecte, particulièrement sensible, et donc est équipé avec deux routeurs en redondance avec une double alimentation. Une possibilité de raccordement d'un nouveau ou d'un second site POM est demandée dans la présente consultation. Cette prestation est proposée et évaluée par le titulaire pour augmenter la résilience et le plan de reprise d'activité en cas de crise.

L'installation de ces équipements est réalisée par le titulaire.

Les principes de connexion des points de concentration de collecte sont les suivants :

- Tous les VPN présents sur chaque territoire (une vingtaine environ) sont portés jusqu'à ces points de concentration. On peut ajouter des VPN spécifiques à l'administration et à la supervision de la solution ;
- Comme tous les autres routeurs, le point de concentration respecte le cloisonnement entre les VPN ;
- Sur les portes de collecte, un seuil limite de bande passante est configuré pour chaque VPN existant afin de garantir une capacité réseau pour chaque bénéficiaire ;
- Dans chacun de ces VPN, les flux qui ne sont pas à destination d'un autre site du territoire sont transmis à la plateforme de livraison de service PLS OM donnant accès au service de transit sécurisé transocéanique du territoire ;

- Les flux en provenance des équipements de transit sont acheminés jusqu'au site de destination ;
- Les réseaux IP nécessaires à l'interconnexion d'équipements sont fournis par la DINUM en bonne entente avec le titulaire. Ces réseaux sont pris dans la plage réservée de la RFC 6598 (100.64.0.0/10). Néanmoins, en cas de problème, le titulaire peut utiliser des adresses IP publiques lui appartenant ;
- Les réseaux IPv6 nécessaires à l'interconnexion d'équipement sont de préférence pris parmi les adresses de lien local (fe80::/10) selon un plan fourni par la DINUM. En cas de d'impossibilité, un réseau fourni par la DINUM dans le réseau d'adresses publiques lui appartenant est attribué.

L'infrastructure de rattachement prévoit quand elle est unique :

- Deux liaisons via deux adductions vers le réseau de collecte du titulaire ;
- Deux liaisons vers les équipements constituant la plateforme de livraison de service Outre-Mer (PLS OM) qui interconnecte des plateformes de services optionnelles et les fonctions de transit transocéanique sécurisé (lots 3, 4 et 5) ;
- Un dispositif de routage des flux garantissant l'optimisation des chemins et la résilience du dispositif ;
- Une architecture logique permettant de ne pas décloisonner les VPN lors de la transmission à la couche adjacente (épine dorsale ou opérateur de transit sécurisé). Les modalités exactes de configuration sont fixées lors des réunions de lancement réunissant le pouvoir adjudicateur et les titulaires des lots concernés.

{PP-L1 & 2/01} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Précision des mécanismes de bascule des flux entre le point de concentration nominal et les points de concentration de secours.

{PP-L1 & 2/02} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Le cas échéant une description du mécanisme permettant le partage de charge entre les deux points de concentration.

{EX-L1 & 2/02} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Le niveau de service de raccordement à un point de concentration de collecte est le niveau « Maximum » avec la garantie d'absence de point individuel de défaillance.

{EX-L1 & 2/03} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : En se basant sur le référentiel des Typologies de la sécurisation des infrastructures, description de l'infrastructure pour garantir le niveau service « Maximum » avec la garantie d'absence de point individuel de défaillance.

{PP-L1 & 2/03} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Description de la politique de prise en compte des différentes hypothèses d'évolution des besoins, notamment en matière de débit.

{EX-L1 & 2/04} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : le candidat indique si Les interfaces d'interconnexion de la fibre optique sont compatibles monomode et/ou multimode.

Le choix du mode de raccordement est précisé par la DINUM au lancement de l'accord-cadre en fonction de l'implémentation des sites d'hébergement de la DINUM.

Les équipements du titulaire sont :

- Dans tous les cas, r*ackables* et installés dans les baies préexistantes fournies par l'hébergeur ;
- Munis d'une double alimentation électrique.

{PP-L1 & 2/04} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Description du modèle et des caractéristiques des équipements et notamment la taille des équipements et leur consommation électrique.

Pour la supervision et l'exploitation par la DINUM du réseau RIE, le titulaire :

- Fournit des indicateurs ou l'accès permettant au NOC RIE de la DINUM de superviser, de surveiller des indicateurs et de visualiser les flux des points de concentration en autonomie ;
- Met à disposition des mécanismes et outils de supervision, de monitorage et d'exploitation des flux des points de concentration (export Netflow compris) ;
- Met à disposition des dispositifs d'alertes lorsque les flux des VPN de collecte atteignent des seuils prédéfinis (anticipation d'actions de modification de « *shaping* » par l'Administration). Ces seuils sont réévalués par la DINUM régulièrement et transmis au titulaire lors de comités liés au pilotage ou à l'exploitation.

Ces informations sont préférentiellement fournies au travers d'API.

{PP-L1 & 2/05} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre de supervision et l'exploitation des flux des points de concentration et notamment au niveau :
- des indicateurs fournis,
- des mécanismes et des outils,
- des types d'alarmes remontées.

{EX-L1 & 2/05} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Les abonnements des connexions des points de concentration de collecte IP de l'épine dorsale du RIE au réseau de collecte IP du titulaire sont inclus dans le prix des forfaits mensuels de chaque abonnement.

3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés

La prestation de rattachement des points de concentration du transit sécurisé et services associés est commandée dès la notification de l'accord-cadre. Cela comprend tous les sites en Outre-Mer ainsi que des sites en Hexagone.

Les principes de rattachement des POM aux fournisseurs des lots de transit sont les suivants :

- Dans chacune des POM, sont déployées des briques fonctionnelles assurant les fonctions suivantes :
  - Transport réseau résilient vers l'Hexagone (via réseau entreprise et Internet) ;
  - Chiffrement des communications véhiculées sur les liens externes à la POM ;
  - Fonction de Plateforme de Livraison de Services PLS OM permettant de mettre en œuvre l'interconnexion des boitiers de chiffrement et différents types de raccordements locaux. Le service est résilient et permet au moins 24 raccordements (ports 1G/10G) ;
  - Interface de raccordement avec les 2 routeurs de porte de collecte (liens logiques pour chaque L3VPN) ;
  - Raccordements directs des bénéficiaires sur la POM en local ou distant via des liaisons Ethernet niveau 2 ;
  - Raccordement de la plateforme d'échanges sécurisés entre les L3VPN du territoire ultramarin de la POM ;

  ;

Dans le cas du doublement de la fonction POM dans un territoire ultramarin, l'architecture est adaptée pour offrir le niveau de résilience maximal.

- Sur les sites en Hexagone assurant des fonctions d'interconnexion vers les territoires d'Outre-Mer, les briques fonctionnelles suivantes sont déployées :
  - Transport réseau résilient vers chaque territoire (lots 3, 4 et 5) (via réseau entreprise et Internet). Le titulaire propose l'architecture résiliente la plus efficiente ;
  - Chiffrement des communications véhiculées sur les liens de transit sécurisé ;
  - Interface avec les routeurs d'épine dorsale RIE (boucle rouge et bleue) présents dans les POP RIE en Hexagone. Il y aura un lien vers un Cisco ASR9906 (boucle bleue) et un lien vers un Juniper MX480 (ou MX10003 selon le site) (boucle rouge). Le raccordement se fera grâce à des *transceivers* 10G LR ou des *transceivers* 100G LR4 (sous réserve d'évolution sur l'épine dorsale) ;
  - Le cloisonnement entre les VPN (L3VPN MPLS) doit être conservé jusqu'à l'interconnexion au RED ;
  - Les réseaux IP nécessaires à l'interconnexion d'équipements sont fournis par la DINUM en bonne entente avec le titulaire. Ces réseaux sont pris dans la plage réservée de la RFC 6598 (100.64.0.0/10). Néanmoins, en cas de problème, le titulaire peut utiliser des adresses IP publiques lui appartenant ;
  - Les réseaux IPv6 nécessaires à l'interconnexion d'équipement sont de préférence pris parmi les adresses de lien local (fe80::/10) selon un plan fourni par la DINUM. En cas d'impossibilité, un réseau fourni par la DINUM dans le réseau d'adresses publiques lui appartenant est attribué.

L'infrastructure de rattachement en POM et en Hexagone prévoit :

- Un dispositif de routage des flux garantissant l'optimisation des chemins et la résilience du dispositif ;
- Une architecture logique permettant de ne pas décloisonner les VPN lors de la transmission à l'équipement partenaire ;
- Une plateforme de livraison de service résiliente côté POM portant les raccordements logiques L3VPN avec les équipements d'interconnexion à l'épine dorsale côté Hexagone ;
- Des briques de chiffrement configurées pour faire transiter les flux transportant les différents L3VPN correspondants à l'architecture réseau retenue (la solution peut transporter des flux de différente nature en fonction de l'architecture proposée : tunnels GRE, MPLS, ISIS, VRF ?).

{PP-L3 & 5/02} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Description de la politique de prise en compte des différentes hypothèses d'évolution des besoins, notamment en matière de débit (sur la partie chiffrement et réseau de transport).

{EX-L3 à 5/01} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : le candidat met en œuvre des fibres et connecteurs compatibles avec les routeurs d'épine dorsale du RIE.

{PP-L3 & 5/03} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Le choix du mode de raccordement et des services déployés est arbitré par la DINUM au lancement de l'accord-cadre en fonction de l'implémentation des sites d'hébergement et de l'architecture globale proposée par le titulaire.

Les équipements du titulaire sont :

- Dans tous les cas, rackables et installés dans les baies préexistantes fournies par l'hébergeur ;
- Être muni d'une double alimentation électrique.

{EX-L3 à 5/02} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Les équipements du titulaire assurant les interconnexions à l'épine dorsale du RIE sont compatibles et interfaçables avec des équipements de la DINUM.

{PP-L3 & 5/04} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Description du modèle et des caractéristiques des équipements et notamment la taille des équipements et leur consommation électrique.

Pour la supervision et l'exploitation par la DINUM du réseau RIE, le titulaire :

- Fournit des indicateurs ou l'accès permettant au NOC RIE de la DINUM de superviser, de surveiller des indicateurs et de visualiser les flux véhiculés sur les liens de transit sécurisé en autonomie ;
- Met à disposition des mécanismes et outils de supervision, de monitorage et d'exploitation des flux en amont et aval des points de concentration. Le titulaire surveille le bon fonctionnement de l'ensemble des lignes de vie actives sur l'ensemble des couches du système d'interconnexion (routage, encapsulation, tunnels) ;
- Met à disposition des dispositifs d'alertes lorsque les flux chiffrés atteignent des seuils prédéfinis sur les liens de transit utilisés. Ces seuils sont réévalués en cas de nécessité par la DINUM et transmis au titulaire lors de comités lié au pilotage ou à l'exploitation. Le titulaire assure une surveillance des capacités de chiffrement afin d'éviter toute dégradation des performances liés à ces fonctions.

Ces informations sont fournies au travers de flux machine à machine ou au travers d'API.

{PP-L3 & 5/05} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre, de supervision et d'exploitation des flux des points de concentration et notamment au niveau :
- Des indicateurs fournis ;
- Des mécanismes et des outils ;
- Des types d'alarmes remontées.

3.2 Lot 1 et lot 2 : Prestations de Collecte

Le périmètre géographique de la collecte IP concerne les territoires suivants : la Guadeloupe, la Martinique, la Guyane française, la Réunion, Mayotte, Saint-Martin ainsi que Saint-Barthélemy, via la POM de Saint-Martin.

3.2.1 Principe d'architecture

Chacun des six territoires ultramarins, hormis Saint-Barthélemy qui est collecté avec Saint-Martin, concernés par la collecte IP comporte une Passerelle Outre-Mer (POM), point d'agrégation de la collecte locale à destination de l'épine dorsale du RIE en Hexagone et vers les autres territoires ultramarins via les lots de transit sécurisé.

Les bénéficiaires utilisent un ou plusieurs VPN pour faire transiter leur flux qui doivent être étanches les uns par rapport aux autres. Dans ces VPN, la communication entre deux sites se fait directement, la communication vers le site d'un autre territoire ultramarin ou vers l'Hexagone passe par la POM et le service de transit sécurisé. Il peut exister 2 sites POM hébergeant des portes de collecte pour des raisons de résilience.

3.2.2 Besoins de raccordement des sites ultramarins

Pour le raccordement à la collecte locale des sites ultramarins des bénéficiaires, le tableau ci-dessous illustre les caractéristiques souhaitées par type de support :

Support	Redondance	Gamme de débit (symétrique)
Fibre optique ou Radio		
Double fibre optique	Actif / Passif	10, 20, 50, 100, 200 et 500 Mbps
	Actif / Actif	
Simple fibre optique + secours FTTH ou 4/5G	Actif / Passif	
Simple fibre optique	-	
FTTH	-	Débit maximum à indiquer dans la réponse technique (asymétrique)
4/5G	-	

Support	Redondance	Gamme de débit (symétrique)
Satellite	-	Débit maximum à indiquer, types d'offre volumétrique et collecte technique identique à l'architecture 4/5G (chiffrement des flux)
Cuivre (uniquement maintien accès existant / non ouvert à la création)		
Simple fibre optique + secours *DSL (cuivre)	Actif / Passif	FO : 4, 6, 8, 10, 15 et 20 Mbps Secours SDSL : 4, 8 Mbps
Double SDSL	Actif / Passif	2x1 Mbps, 2x2 Mbps, 2x4 Mbps et 2x8 Mbps (débit ATM)
	Actif / Actif	
Simple SDSL	-	1, 2, 4 et 8 Mbps (débit ATM)
ADSL/VDSL	-	Débit maximum à indiquer dans la réponse technique (asymétrique)

Les prestations de collecte de type Ethernet niveau 2 supportent les caractéristiques suivantes pour une liaison point à point entre 2 sites d'un bénéficiaire ou 1 site bénéficiaire et un site POM :

Support	Redondance	Gamme de débit (symétrique)
Fibre optique		
Double fibre optique	Actif / Passif	500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps
	Actif / Actif	
Simple fibre optique	-	

En ce qui concerne le raccordement des POM à la collecte locale en lien multi VPN, les caractéristiques souhaitées sont les suivantes :

Support	Redondance	Gamme de débit (symétrique)
Double fibre optique	Actif / Passif	100, 200 et 500 Mbps 1, 2 et 5 Gbps

Les équipements fournis dans le cadre des lots 1 et 2, et installés dans la POM, la « porte de collecte opérateur local », doivent pouvoir s'interconnecter en cuivre et/ou en fibre aux équipements assurant le lien avec le transit transocéanique fournis dans le cadre des lots 3, 4 et 5. L'implémentation technique définitive fait l'objet de discussions entre les acteurs au démarrage du projet.

3.2.3 Spécifications du réseau privé virtuel (VPN)

L'infrastructure mise en œuvre supporte nativement un environnement multi-VPN.

Le réseau de collecte permet :

- De gérer l'ajout ou la suppression de VPN ;
- De permettre à un site d'accéder à un ou plusieurs VPN. Les VPN sont alors séparés dans le routeur du site par des interfaces physiques différentes ou des sous-interfaces VLAN (802.1Q) d'une même interface physique ;
- Les flux transportés par le réseau VPN du titulaire s'appuient sur des infrastructures dédiées aux entreprises.

{PP-L1 & 2/06} 3.2.3 : Spécifications du réseau privé virtuel (VPN) : Description des mécanismes mis en œuvre permettant d'ajouter ou de supprimer des VPN et précision des limitations éventuelles sur les performances techniques et économiques.

{PP-L1 & 2/07} 3.2.3 : Spécifications du réseau privé virtuel (VPN) : Description des mécanismes mis en œuvre de propagation des VPN sur le LAN et précision des limitations éventuelles sur les performances techniques et économiques.

3.2.4 Plan d'adressage IP

Le plan d'adressage RIE, isolé d'Internet, est essentiellement conforme aux normes RFC1918 et RFC6598 de l'IETF.

La RFC1918 est utilisée par tous les bénéficiaires et la RFC6598 est massivement utilisée au niveau RIE, pour de multiples besoins, comme notamment : l'adressage des *loopbacks* des équipements, l'adressage des applications interministérielles, etc.

Le titulaire ne peut en aucun cas utiliser des adresses décrites dans la RFC1918 dans les VPN du RIE pour le fonctionnement de son infrastructure. Le cas échéant, il peut utiliser des adresses décrites dans la RFC6598 après accord de la DINUM.

Les bénéficiaires font transiter dans leur VPN des adresses de la RFC1918 ou des adresses IPv4 et IPv6 leur appartenant.

{EX-L1 & 2/06} 3.2.4 Plan d'adressage IP : Les choix d'ingénierie du titulaire ne contraignent ou ne limitent en aucun cas l'Administration dans la gestion de son plan d'adressage IPv4 et IPv6, en particulier afin d'éviter tout risque de conflit entre les différents partenaires du RIE susceptibles d'avoir faits des choix qui leur sont propres.

{EX-L1 & 2/07} 3.2.4 Plan d'adressage IP : Le titulaire respecte strictement les principes de cloisonnement et d'indépendance du plan d'adressage du RIE.

{PP-L1 & 2/08} 3.2.4 Plan d'adressage IP : Description des principes de reprise du plan d'adressage permettant de respecter le cloisonnement et l'indépendance du plan d'adressage du RIE.

3.2.5 AS BGP

Les sites sont raccordés au réseau du titulaire du marché grâce au protocole BGP. Il faut que les numéros d'AS de chaque territoire soient différents.

Si le titulaire ne possède pas assez de numéro d'AS public différent, des numéros privés sont fournis par la DINUM en bon entente avec lui.

3.2.6 Services IPv4 et IPv6

Le titulaire fournit un service IPv4 et IPv6 entièrement fonctionnel sur la totalité de son offre, réseau opérateur et équipements d'extrémités compris.

{PP-L1 & 2/09} 3.2.6 Services IPv4 et IPv6 : Précisions sur la fourniture du service IPv4 et IPv6.

3.2.7 Etendue et capillarité du réseau du titulaire

Le service de collecte repose sur des infrastructures qui appartiennent en propre au titulaire ou qui sont louées à des opérateurs tiers.

La DINUM précise que les engagements du titulaire à son égard restent entiers en cas de recours éventuels à un opérateur ou des prestataires tiers.

L'infrastructure réseau du titulaire permet l'interconnexion des sites pour la fourniture de services réseaux IPv4 et IPv6 au travers d'accès permanents et doit permettre de fournir un service de type L3VPN « *any to any* ».

Le réseau de collecte est découpé en plusieurs VPN selon les besoins de cloisonnement définis par l'Administration (cas général : un VPN par bénéficiaire ministériel). Il se connecte au réseau de transit sécurisé ou à une brique fonctionnelle d'épine dorsale au sein de la POM. Le chiffrement concerne les flux transportés par les liens transocéaniques du lot de transit (entre la POM et l'Hexagone et également entre deux POM d'une même zone géographique).

La solution doit reposer sur une infrastructure réseau en mesure de supporter un environnement multi-VPN et la priorisation de flux (champs DSCP).

La solution du titulaire doit pouvoir gérer les sites de l'Administration ayant besoin que plusieurs VPN soient propagés sur le LAN (par des interfaces physiques distinctes du routeur ou des sous-interfaces VLAN).

Le service d'interconnexion offert peut reposer sur des infrastructures qui peuvent être soit privées, soit louées à des opérateurs tiers. Dans ce cas, le titulaire reste le seul porteur des engagements vis-à-vis du pouvoir adjudicateur.

La DINUM précise le fait qu'aucun filtrage ni modification des paquets IP ne doit être réalisé par le service réseau du titulaire sans demande explicite.

{EX-L1 & 2/08} 3.2.7 Etendue et capillarité du réseau du titulaire : Aucun filtrage ni modification des paquets IP n'est réalisé par le service réseau du titulaire sans demande explicite.

{EX-L1 & 2/09} 3.2.7 Etendue et capillarité du réseau du titulaire : Le titulaire décrit les mécanismes mis en œuvre pour répondre à cette architecture multi-VPN et les impacts des limitations éventuelles.

{PP-L1 & 2/10} 3.2.7 Etendue et capillarité du réseau du titulaire : Description de l'étendue et de la capillarité du service de collecte.

{PP-L1 & 2/11} 3.2.7 Etendue et capillarité du réseau du titulaire : Description du maillage des réseaux de collecte en précisant notamment sa redondance.

{PP-L1 & 2/12} 3.2.7 Etendue et capillarité du réseau du titulaire : Précisions des zones propriétaires des infrastructures.

{PP-L1 & 2/13} 3.2.7 Etendue et capillarité du réseau du titulaire : Précisions des zones non-propriétaires des infrastructures, le cas échant, description de maîtrise contractuelle des tiers propriétaires des infrastructures.

{PP-L1 & 2/14} 3.2.7 Etendue et capillarité du réseau du titulaire : Précisions du nombre de points de concentration sur les zones propriétaires et de leur capacité à être redondé.

3.2.8 Spécifications sur les accès mobiles et satellites

Les accès mobiles 4G/5G et les accès satellite font partie de la catégorie à débit non garanti pour lesquels le débit maximum est indiqué.

Les accès sans fil de type 4G/5G et satellite doivent implémenter un chiffrement des flux entre les équipements opérateur déployés sur les sites clients et le réseau du titulaire du lot de collecte ultramarin.

Les flux du site client raccordé au RIE sont réinjectés dans la VRF/VPN de la communauté d'appartenance du site.
Les échanges doivent être encapsulés dans un tunnel IPSEC entre le routeur CE et des routeurs PE aux caractéristiques minimales suivantes :

- Echange de clé IKEv2 ;
- Méthode d'authentification : secret partagé ;

- Protocole d'authentification : SHA 256 ;
- Chiffrement : AES-CBC-128 (évolutif en 256).

Les services disponibles sur les routeurs clients sont identiques à ceux de la 4G/5G :

- Multi-VRF ;
- Syslog ;
- SSH ;
- Netflow;
- SNMP ;
- IPsla.

L'opérateur déploie un routeur (ou autre équipement aux fonctions équivalentes) avec un kit 4G/5G ou un kit satellite composé d'un modem satellite, d'une tête émission/réception et d'une parabole selon la typologie de l'accès.

Le titulaire propose une prestation clé en main pour l'installation, comprenant la pré-visite, l'étude et les travaux d'installation des antennes. Cette prestation peut donner lieu à l'établissement d'un devis préalable. Le titulaire peut décliner plusieurs offres en fonction de critères de performance ou de complexité.

Un document de recette est remis à l'issue du déploiement de l'accès, attestant de son bon fonctionnement.

{PP-L1 & 2/15} 3.2.8 Spécifications sur les accès mobiles et satellites : La technologie satellite peut être en orbite basse ou géostationnaire. Le titulaire propose au moins une offre Française ou Européenne sous condition d'éligibilité du territoire.

3.2.9 Qualité de services « QoS »

L'infrastructure (hors lien niveau 2) mise en œuvre supporte la priorisation de flux (champs DSCP).

Le titulaire fournit un service à débit garanti sur tous les types de lien (à l'exception éventuelle des liens de type ADSL, FTTH, 4G ou 5G et satellite) permettant la mise en œuvre de plusieurs profils de QoS. Dans le cas d'un accès avec plusieurs VPN, un débit garanti est attribué à chacun des VPN présents (pour une somme totale égale à la valeur du lien commandé).

Les profils de QoS, des équipements d'accès (flux entrants sur le réseau), utilisent différentes classes de services, réparties de la façon suivante :

- Trois classes de données (DATA1, DATA2 et DATA3) plus une *best effort* (BE) ;
- Une classe vidéo (VISIO) ;
- Une classe voix (VOIX) ;
- Une classe réservée à la supervision / administration des équipements (MNGT) d'un maximum 2% de la bande passante, sur tous les profils de classe.

Champs DSCP	af31	af21	af11	ef	af41	cs6	
Profil / Usage	**DATA1**	**DATA2**	**DATA3**	**VOIX**	**VISIO**	**MNGT**	**BE**
Data	50%	35%	10%			2%	3%
Data + Voix + Visio	18%	7%	5%	30%	35%	2%	3%
Voix				95%		2%	3%
Visio					95%	2%	3%

En l'absence de profil de QoS appliqué, le service met en œuvre une unique classe de données appelée « *best effort* ».

Les flux sont classés selon des critères protocolaires ou des caractéristiques des utilisateurs du service (notamment les champs : adresses source / destination, ports TCP/UDP source / destination et DSCP du paquet IP).

Les flux marqués entrant sur le réseau du titulaire restent marqués et orientés vers la bonne classe de service. En particulier :

- L'interconnexion entre les VPN de collecte et les VPN de transit assure le maintien du marquage de flux. A ce titre, il est primordial que le marquage présenté en entrée du réseau du titulaire, quelles que soient les mutations, soit restitué en sortie de réseau à l'identique du marquage initial ;
- Les classes de service sont cohérentes de bout en bout.

Les flux Temps Réels (VOIX ou VIDEO) doivent pouvoir occuper la totalité de la bande passante de l'accès (cf. profils VOIX et VISIO ci-dessus). Il en est de même pour chacun des flux DATA.

Les politiques de marquage des flux pour chaque VPN client peuvent évoluer ou être enrichies en cours d'accord-cadre par la DINUM.

Les règles entre les classes de service permettent notamment de gérer les priorités entre les différentes classes de services définies et de leur associer des limites inférieures et/ou supérieures de bande passante consommée.

Le titulaire met en place un mécanisme (marquage en CS6 *network routing*) pour gérer la priorisation des flux des plans de contrôle et de gestion (BGP, SNMP, SSH, etc.) notamment pour garantir que des flux d'administration et de supervision (que

ce soit ceux du titulaire ou de la DINUM) restent prioritaires en cas de saturation des autres flux.

Le titulaire met en œuvre une fonctionnalité de « *looking-glass* » permettant d'interroger la configuration des *PE router* de collecte du titulaire (qu'ils soient mutualisés ou non) relative à la QoS, notamment au niveau des règles de marquage/classification et de réservation de bande passante (afin de valider la symétrie de cette configuration en vis-à-vis du reste du RIE).

{PP-L1 & 2/16} 3.2.9 Qualité de services « QoS » : Description de la mise en œuvre des classes de service en pourcentage des profils du tableau ci-avant, quel que soit la bande passante.

{PP-L1 & 2/17} 3.2.9 Qualité de services « QoS » : Description de la prise en compte de l'évolutivité ou de l'enrichissement des politiques, de marquage des flux pour chaque VPN client, de l'Administration, en cours d'accord-cadre.

3.2.10 Voix et vidéo sur IP

Les services de collecte ont la capacité de prendre en charge les flux voix et vidéo sur IP sur les accès disposant d'une classe de service voix et vidéo.

Le titulaire met en œuvre un dispositif permettant la souplesse et la visibilité des règles d'ingénierie et de dimensionnement des accès destinés à transporter de la voix et de la vidéo sur IP.

{PP-L1 & 2/18} 3.2.10 Voix et vidéo sur IP : Description des limitations notamment pour :
- les tailles de *payload* de la classe de service « voix »,
- la possibilité de faire cohabiter plusieurs codecs simultanément et le cas échéant des tailles de *payload* propres à chaque codec.

{PP-L1 & 2/19} 3.2.10 Voix et vidéo sur IP : Description des règles d'ingénierie des accès spécifiques voix sur IP en précisant notamment :
- les types d'accès éligibles à la VoIP (technologie en fonction de l'éligibilité, granularité des débits offerts…),
- le taux maximum d'utilisation du débit nominal de l'accès, en fonction des classes de services implémentées (CoS).

Sur demande de l'Administration, le débit de l'accès (ou d'un des VPN présents sur le site) est alloué en quasi-totalité (hors flux de management) au service voix ou vidéo. Par exemple, sur un accès de 4 Mbps, la configuration de l'allocation d'une classe vidéo 95% correspond à 3,8 Mbps.

{PP-L1 & 2/20} 3.2.10 Voix et vidéo sur IP : Précisions, le cas échéant, des limitations ou contraintes pour l'allocation de la quasi-totalité débit de l'accès (ou du VPN au sein d'un accès sub-VPN) au service voix ou vidéo.

3.2.11 Multicast

Sur demande de l'Administration le titulaire déploie du service « Multicast » par accès.

Ce déploiement est précédé d'une étude préalable du service.

Le déploiement par site éligible « Multicast » intègre les coûts de la modification de l'infrastructure et des équipements d'extrémités du titulaire.

Eventuellement un coût additionnel à l'abonnement du service de transport de flux est applicable.

{PP-L1 & 2/21} 3.2.11 Multicast : Description de la démarche de l'étude préalable du service « Multicast » par accès en précisant : les caractéristiques de l'offre, les types de protocole implémentés, le nombre maximum de routes par défaut, le type de route (statique, dynamique), le nombre maximum de routes par tunnel, les moyens qui sont mis en œuvre pour filtrer les routes afin de protéger les équipements d'extrémité (explosion des routes), les techniques mises en œuvre pour mettre en place la sélection d'un sous-ensemble de groupes de diffusion, les impacts à tout point de vue sur IPv4 et IPv6…

{PP-L1 & 2/22} 3.2.11 Multicast : Description des impacts éventuels sur les équipements d'extrémité.

{PP-L1 & 2/23} 3.2.11 Multicast : Justification des éventuels coûts additionnels à l'abonnement du service de transport de flux.

3.3 Lots 3, 4 et 5 : Transit sécurisé vers l'Hexagone et entre les territoires ultramarins

Ces 3 lots de transit sécurisé se composent d'une partie réseau de transport transocéanique, d'un service de chiffrement, d'une plateforme de livraison de service « PLS OM » et d'un service d'interconnexion à l'épine dorsale en métropole. S'y ajoutent des prestations supplémentaires pour répondre à des besoins spécifiques locaux en matière d'interactions entre bénéficiaires distincts.

La solution mise en œuvre doit répondre aux exigences de disponibilité, de sécurité et de qualité attendues par l'administration et être la plus efficiente possible.

Le pouvoir adjudicateur souhaite constituer trois réseaux d'interconnexion IP, un pour chacune des zones Atlantique, Océan Indien et Pacifique. Chaque zone forme ainsi une boucle qui relie 2 points d'interconnexion en Hexagone.

De cette façon, les différents territoires DROM et COM d'une même zone échangent entre eux sans passer par l'hexagone et chaque zone est raccordée par 2 chemins distincts à l'Hexagone.

Deux types de transit sont demandés :

- Le premier concerne un transit basé sur des liens de type Entreprise. Pour ce type de transit, des équipements sont installés sur chacune des « Passerelles Outre-Mer » (POM) dans le cadre de ce marché, et sur deux points d'interconnexion à l'épine dorsale du RIE en Hexagone ;
- Le second concerne un transit basé sur des liens de type Internet. Pour ce type de transit, des équipements sont installés sur chacune des « Passerelles Outre-Mer » (POM) et un ou plusieurs accès à Internet via la PFAI de la DINUM en Hexagone ;
- Des accès Internet de type satellite sont proposés par les titulaires sur les POM pour supporter les communications chiffrées. Ces accès sont destinés à être utilisés en ultime secours en fonction de leur capacité et des situations de crise
- Les 2 types de transit ont vocation à se compléter en termes de résilience pour minimiser les situations d'isolement d'un ou plusieurs territoires ultramarins de l'ensemble de la zone concernée par ce transit ;
- Le titulaire peut en sus proposer des scénarios permettant d'utiliser les 2 types de réseau de transit en même temps pour véhiculer les flux selon leur criticité et destination. La séparation du trafic vers les relais Internet en Hexagone est étudiée par exemple ;
- En Hexagone, la solution de chiffrement raccordée à Internet est séparée de la solution de chiffrement utilisée sur les liens de type Entreprise. Il est donc fourni des concentrateurs IPSEC distincts pour chaque type de réseau de transit Internet et Entreprise.

Le titulaire du lot 5 propose, via la fourniture d'accès internet à haut débit et au travers d'un service de chiffrement qualifié un scénario technique permettant le rattachement des sites des bénéficiaires du territoire de Wallis et Futuna ; actuels sites en architecture dite « Sites Isolés » et éventuels futurs sites.

Dans les deux modes de transit, l'opérateur de transit sécurisé fournit des services L3VPN entre collecte et épine dorsale du RIE. Ces services doivent être transportés en respectant un cloisonnement strict entre eux.

Ce lot de transit sécurisé introduit de nouvelles fonctions dans les POM permettant d'offrir de nouveaux services. Une fonction de Plateforme de Livraison de Service (PLS OM) qui gère :

- Le raccordement des portes de collecte des Lots 1 et 2 ainsi que des réseaux de collecte de la zone Pacifique ;

- Les raccordements directs colocalisés de l'hébergeur de la POM ou bien les raccordements distants via l'offre Ethernet du réseau de collecte ;
- Les raccordements des plateformes de service pour les échanges entre les communautés (PFS OM)

Le titulaire propose les différentes solutions de raccordement logique avec l'épine dorsale en fonction des choix techniques réalisés pour la solution de chiffrement. Dans le cas d'une extension de l'épine dorsale du RIE, le service de transit sécurisé doit pouvoir transporter des échanges MPLS et IS-IS entre routeurs d'épine dorsale en Hexagone et routeurs PLS OM (plateforme de livraison de service en Outre-Mer).

Une solution alternative peut consister en la mise en œuvre de VRF et de tunnels par VRF sur l'ensemble des briques entre la POM et l'épine dorsale du RIE. Le service de transit sécurisé délivrerait alors des interfaces logiques par VPN aux routeurs de porte de collecte côté POM et aux routeurs d'épine dorsale côté Hexagone. Dans le cas où les évolutions techniques ne seraient pas réalisables à l'initialisation du marché, l'architecture d'interconnexion existante est reproduite (tunnels GRE entre PLS OM et routeurs d'interconnexion à l'épine dorsale en métropole). Des routeurs sont fournis en métropole par le titulaire des lots de transit sécurisé pour gérer l'extrémité des tunnels GRE et le reversement dans les VRF présentes sur les routeurs d'épine dorsale.

{EX-L3 à 5/03} 3.3 Lots 3, 4 et 5 : Transit sécurisé vers l'Hexagone et entre les territoires ultramarins: Le titulaire prévoit que les solutions proposées soient compatibles avec l'installation et la mise en service, d'une seconde POM sur tous les territoires ultramarins déjà équipés d'une première POM.

L'implémentation technique définitive fait l'objet de discussion entre les acteurs au démarrage du projet. La DINUM se réserve le choix des différents types de réseau de transport et d'architecture mis en œuvre pour transporter les flux des bénéficiaires entre Outre-Mer et Hexagone.

3.3.1 Liaisons transocéaniques « Entreprise »

Le titulaire propose un service reposant sur un ensemble de liaisons transocéaniques pour raccorder les POM :

- A l'Hexagone sur deux points distincts d'interconnexion à l'épine dorsale du RIE tel que précisé ci-avant ;
- A, au minimum, une autre POM d'un territoire dans la même zone géographique :
  - Pour assurer la résilience du trafic vers l'Hexagone en cas de rupture du lien entre la POM considérée et son interconnexion avec l'épine dorsale du RIE ;
  - Pour permettre le trafic interne à la zone géographique au sein d'un même VPN sans avoir à remonter jusqu'en Hexagone.

Dans tous les cas, les parcours en Hexagone entre les points d'arrivée océaniques et les deux points d'interconnexion au RIE sont en niveau de service « maximum » : ils ne doivent présenter aucun point unique de défaillance (« SPOF »), ni matériel ni logiciel. Tout scénario présentant un SPOF de parcours sur le territoire hexagonal est rejeté.

Le besoin de transit est exprimé en débit utilisateur total mesuré entre la zone ultramarine prise dans son ensemble et l'Hexagone. Ce débit utilisateur total détermine la bande passante symétrique à garantir en service nominal entre un point de collecte en métropole et les POM de la zone ultramarine considérée. Le point de collecte en Hexagone de secours offre les mêmes caractéristiques de performances et débit. Ainsi, si l'administration commande 2Gbps selon le BPU pour la zone océan indien, la répartition des débits peut être la suivante :

- Site Hexagone 1 : 2,0 Gbps;
- Site Hexagone 2 : 2,0 Gbps;
- Site POM Réunion : 1,5 Gbps;
- Site POM Mayotte : 0,5 Gbps.

{PP-L3 & 5/06} 3.3.1 Liaisons transocéaniques « Entreprise » : Pour répondre à ce besoin, le titulaire propose la topologie de liaisons qui lui semble optimale pour l'ensemble de la durée d'exécution du marché.

Le service nominal est maintenu face à une défaillance unique, sauf limitation permise pour les cas de la Polynésie française et de la Nouvelle-Calédonie et explicitement décrite dans l'offre relative au Lot 5.

{EX-L3 à 5/04} 3.3.1 Liaisons transocéaniques « Entreprise » : La solution de transit sécurisé implémentée par le titulaire doit garantir la transmission de l'ensemble des paquets entrant dans les tunnels entre la zone ultramarine et la métropole à l'exception des paquets rejetés au niveau des accès télécom locaux (POM ou métropole) pour des raisons de saturation du débit souscrit. Dans ces cas de saturation, les mécanismes de QoS pour prioriser les flux en fonction de leur marquage s'appliquent sur les routeurs d'accès, en particulier pour préserver les paquets supportant les lignes de vie et les protocoles de routage.

Le titulaire démontre dans son offre :

- Le maintien du service nominal face aux cas de défaillance unique sous les réserves précédemment exprimées ;
- La capacité de son cœur de réseau mutualisé à fournir les débits souscrits par l'administration quel que soit la congestion du trafic global multi usages sur son cœur de réseau ;

- Les capacités de résilience, c'est-à-dire de service dégradé selon des cas de défaillance multiple, et leurs limites (exemple : perte de priorisation de flux, latence supérieure, délai de mise en œuvre et prérequis éventuels de déclenchement…).

{EX-L3 à 5/05} 3.3.1 Liaisons transocéaniques « Entreprise » : Le titulaire précise l'architecture réseau détaillée qu'il propose, avec un diagramme (redondance, vérification de l'absence de SPOF, mode dégradé, etc.). La qualité de l'offre est jugée sur la redondance (service nominal) et la résilience (service dégradé) des architectures face aux cas de panne.

Dans la mesure du possible, au moins un parcours nominal entre les POM et l'Hexagone doit n'utiliser que des infrastructures maîtrisées de type « entreprise », c'est-à-dire ne pas recourir à Internet. Des parcours de secours peuvent utiliser des tronçons Internet. Le cas échéant, l'articulation entre l'offre Entreprise et un transit secours via Internet est détaillée en termes de résilience. L'objectif à atteindre reste dans tous les cas l'absence de SPOF dans le raccordement entre l'Outre-Mer et l'Hexagone.

Les liaisons peuvent reposer sur des infrastructures qui peuvent être soit privées, soit louées à des opérateurs tiers. Dans ce cas, le titulaire reste le seul porteur des engagements vis-à-vis du pouvoir adjudicateur.

{EX-L3 à 5/06} 3.3.1 Liaisons transocéaniques « Entreprise » : Le titulaire décrit si les liaisons transocéaniques proposées sont dédiées à des clients « entreprise » ou s'ils transitent d'une manière ou d'une autre par Internet. Le cas échéant le titulaire détaille par « tronçon » les contraintes et limites des accès qu'il utilise. Le titulaire fait la distinction entre les zones dans lesquelles il est propriétaire des infrastructures et celles dans lesquelles il s'appuie sur des tiers.

La qualité de l'offre est jugée sur la maîtrise directe ou contractuelle des capacités de transport (une forte maîtrise est préférée, au travers de participations au capital des tiers ou d'accords commerciaux fortement engageants).

Les débits demandés pour les liaisons transocéaniques sont de 100, 200, 500 Mbps, 1, 2, 5 ou 10 Gbps.

3.3.2 Transit « Internet »

Le titulaire propose dans son offre de service des accès à Internet haut débit sur le territoire ultramarin considéré depuis un point d'accès colocalisé avec la POM dudit territoire.

Ce service a pour objet d'acheminer des flux chiffrés vers l'Hexagone. Dans ce cas de figure, les flux sont pris en charge en Hexagone via la plateforme d'accès à Internet du RIE (PFAI).

Le titulaire propose une configuration permettant de faire transiter les flux utilisateurs à destination d'Internet via la PFAI dans un tunnel dédié passant en priorité par Internet. Cette configuration permettra d'optimiser la gestion de la bande passante Entreprise en la réservant aux usages métiers internes.

Ces accès Internet peuvent aussi être mutualisés avec d'autres usages de manière sécurisée en fonction du besoin de l'Administration. Ils peuvent par exemple être employés au transport d'un flux sortant de navigation Internet

Les services attendus de la part du titulaire sont :

- Accès au réseau Internet (adresse IPv4 et IPv6 publique) ; Résilience ;
- Mécanismes de protection contre les attaques DDoS.

{EX-L3 à 5/07} 3.3.2 Transit « Internet : Le titulaire présente les fonctionnalités détaillées apportées par son service, les technologies mises en œuvre, les principes de redondance mis en œuvre. Le cas échéant, le titulaire détaille son service en fonction des zones géographiques et propose une gamme de débit/dimensionnement adapté.

La qualité de l'offre est jugée sur la simplicité d'utilisation et la conformité aux standards techniques.

Les débits demandés pour les liaisons transocéaniques basées sur une offre de transit « Internet » sont de 100, 200, 500 Mbps, 1, 2, 5 ou 10 Gbps, avec la possibilité de souscrire :

- Des doubles accès Internet sécurisés, constitués de deux routeurs via deux liens avec des parcours distincts vers deux points de présence opérateur (PoP) différents ;
- Mécanismes de protection contre les attaques DDoS.

L'Administration commande des accès Internet de manière unitaire pour chaque POM en DROM et COM. L'Administration utilise les accès Internet du RIE en Hexagone mais se réserve le droit de commander des accès Internet en Hexagone en cas de besoin.

La solution doit être compatible avec le déploiement d'une seconde POM sur le DROM/COM.

3.3.3 Services de chiffrement

Toute communication de l'État en dehors du territoire national fait l'objet d'une protection cryptographique en confidentialité et intégrité. En conséquence, les flux acheminés sur les liaisons transocéaniques de type Entreprise et Internet doivent impérativement être chiffrés avec des solutions qualifiées par l'ANSSI. Ce chiffrement est assuré dans le cadre de ce marché par les titulaires des lots 3, 4 et5.

Ceux-ci s'engagent à fournir un service de chiffrement qualifié au sens de l'Ordonnance 2005-1516 (protection en confidentialité et intégrité) des flux métiers et d'administration du RIE transitant hors du territoire national entre les territoires d'Outre-Mer français (DROM et COM) et l'Hexagone. Les flux du RIE sont :

- Des flux utilisateurs (de données, de voix et d'images) entre les sites ultramarins du pouvoir adjudicateur et vers des points de concentration en Hexagone ;
- Des flux d'administration et de supervision de la solution déployée dans le présent marché.

Le service de chiffrement traite les différents L3VPN du RIE en garantissant leur étanchéité. Aucun routage ne doit être permis entre ces L3VPN. En fonction des choix d'architecture réseau et des fonctionnalités activables sur les concentrateurs IPSEC, la configuration des boitiers de chiffrement est adaptée. Les tunnels chiffrés peuvent par exemple transporter des flux réseau natifs du type MPLS et ISIS (mode GRETAP) directement entre les routeurs de la PLS OM et les routeurs d'épine dorsale en Hexagone ou des flux IP par VRF (tunnels IPSEC par VRF) ou des tunnels GRE entre les PLS OM et les routeurs d'interconnexion à l'épine dorsale (transport des interconnexions de chaque VRF).

{PP-L3 & 5/07} 3.3.3 Services de chiffrement : Le titulaire propose des solutions techniques en argumentant les avantages et inconvénients de chaque scénario.

Par ailleurs, le marquage des flux en termes de qualité de service (QoS) doit être maintenu lors du chiffrement et du déchiffrement.

Ce marché couvre les prestations d'étude et de mise en place initiale du service de chiffrement, de déploiement de la solution technique, et de gestion opérationnelle et vie du service de chiffrement, en particulier :

- Le titulaire met en œuvre les configurations permettant de garantir le maintien des différentes lignes de vie liées aux protocoles de chiffrement, aux protocoles de routage et au cloisonnement des VPN ;
- Le titulaire supervise l'état des tunnels chiffrés et supervise les changements de circuits empruntés entre les POM ultramarines et les points d'interconnexion à l'épine dorsale en Hexagone. Il met ces informations à disposition du pouvoir adjudicateur ;
- Le titulaire supervise les performances des chiffreurs et l'ensemble des taux de pertes de paquets sur son périmètre de responsabilité et met à disposition de l'administration un tableau de bord synthétique.

{EX-L3 à 5/08} 3.3.3 Services de chiffrement : Le chiffrement des informations transitant sur le réseau de transport doit être réalisé par des chiffreurs qualifiés au niveau standard par l'ANSSI.

{EX-L3 à 5/09} 3.3.3 Services de chiffrement : Le titulaire précise la conformité de l'organisation qu'il met en place avec les dispositions de l'annexe I de l'Instruction Interministérielle n°901.

3.3.4 MTU

La MTU doit pouvoir être configurée au-delà de 1500 (« jumbo frame ») au minimum en IPv4 et IPv6 de bout en bout. Le chemin MTU (« Path MTU Discovery ») doit être fonctionnel tout le long de la liaison.

{EX-L3 à 5/10} 3.3.4 MTU : Le titulaire détaille la MTU standard et la MTU maximale qu'il peut proposer sur ses accès en standard. Le cas échéant il précise s'il est possible d'aller au-delà et en précise les coûts (UO complémentaire par exemple). Il décrit les possibilités de paramétrages et les impacts inhérents. Il précise l'applicabilité du « Path MTU Discovery » dans son offre.

3.3.5 Qualité de service

L'Administration peut marquer ses flux IP selon le protocole DSCP. Il est nécessaire que le service de transit sur le périmètre entreprise, en cas de congestion ou de dégradation de la bande passante disponible suite à une avarie, honore les mécanismes de priorisation de flux prévus par le protocole DSCP.

Le service de transit ne doit en aucune façon modifier les champs DSCP des paquets IP, sauf accord ou demande expresse de l'Administration.

Le titulaire du lot de transit sécurisé est responsable du marquage et du traitement priorisé des flux de type ligne de vie transitant sur le réseau entreprise (DPD (dead Peer Detection IPSEC), tunnels GRE le cas échéant, protocoles BGP et BFD, etc…).

{EX-L3 à 5/11} 3.3.5 Qualité de service : Le titulaire détaille le cas échéant la mise en œuvre des mécanismes de priorisation de flux (QoS) basés sur les champs DSCP appliqués en entrée sur les liaisons.

3.3.6 AS BGP

Le raccordement entre les titulaires des lots 1 et 2, d'une part, et les titulaires des lot 3, 4 et 5, d'autre part, se fera de manière dynamique avec le protocole BGP. Il en est de même pour le raccordement avec l'épine dorsale du RIE.

Ces raccordements utilisent un numéro d'AS différent des autres raccordements.

Si les titulaires ne disposent pas d'un nombre suffisant de numéros d'AS publics distincts, des numéros d'AS privés sont fournis par la DINUM, en concertation avec eux.

3.3.7 Transit non chiffré

L'architecture actuelle de transport transocéanique repose sur deux briques fonctionnelles distinctes, couvertes par deux supports contractuels différents :

- un service de transit de type « Entreprise » et/ou « Internet »
- un service de chiffrement.

L'architecture cible mise en œuvre dans le cadre des présents accords-cadres vise à réunir ces deux composantes au sein d'un service unique de transit sécurisé, intégrant nativement le chiffrement des flux.

Toutefois, afin d'assurer la continuité des services pendant la période transitoire nécessaire à la migration de l'architecture existante vers l'architecture cible, l'Administration se réserve la possibilité de commander aux titulaires des prestations de transit sans chiffrement intégré.

3.4 Lot 7 : Transit sécurisé entre l'Hexagone et Saint Pierre et Miquelon

Ce lot de transit sécurisé se compose d'une partie accès réseau internet (niveau de service : best effort) pour au moins 6 sites concernés sur le territoire de Saint-Pierre et Miquelon, d'un service de chiffrement et d'un service d'interconnexion à l'épine dorsale en métropole. Les sites clients sont raccordés en direct vers le réseau RIE en métropole via un lien VPN IPSEC et un tunnel GRE. La mise en œuvre de tunnels GRE entre le LAN et le réseau d'épine dorsale en métropole permet de cloisonner les réseaux clients dans leur communauté ministérielle sur le raccordement à l'épine dorsale en métropole. Les terminaisons des tunnels GRE en métropole sont portées par des équipements gérés dans le cadre d'un autre marché.

L'administration commande des raccordements pour les sites éligibles et en particulier les sites de la catégorie « sites isolés » du précédent marché DROM/COM.

3.4.1 Transit internet sécurisé

Le titulaire propose dans son offre de service des accès à Internet haut débit et un service de chiffrement qualifié sur le territoire ultramarin considéré depuis les emprises de l'administration à raccorder sur le réseau RIE de la métropole.

Ce service a pour objet d'acheminer des flux chiffrés vers l'Hexagone entre un concentrateur IPSEC dédié à l'emprise, fourni et administré par le titulaire du lot 7 et des concentrateurs centraux mutualisés en métropole. Dans ce cas de figure, l'accès internet côté métropole est pris en charge via la plateforme d'accès à Internet du RIE (PFAI) sur deux localisations géographiques. Le titulaire est responsable de la livraison et de l'administration des passerelles outremer nominale et secours dédiés à Saint-Pierre et Miquelon en métropole.

La solution mise en œuvre doit répondre aux exigences de disponibilité, de sécurité et de qualité attendues par l'administration et être la plus efficiente possible.

{EX-L7/01} 3.4.1 Transit internet sécurisé : Le titulaire présente les fonctionnalités détaillées apportées par son service, les technologies mises en œuvre, les principes de redondance mis en œuvre. Le cas échéant, le titulaire détaille son service en fonction des zones géographiques de S-P&M et propose une gamme de débit/dimensionnement adapté.

Le type de transit sécurisé demandé a les caractéristiques suivantes :

- un transit basé sur des liens de type Internet. Pour ce type de transit, des équipements de routage et chiffrement sont installés sur chaque site à raccorder de Saint-Pierre et Miquelon et sur au moins 2 sites d'hébergement du service PFAI de la DINUM en Hexagone
- Les accès internet proposés peuvent être en simple attachement avec un routeur ou bien en double attachement avec deux équipements d'extrémités distincts
- Des accès Internet de type satellite sont proposés sur les sites pour supporter les communications chiffrées. Ces accès sont utilisés en ultime secours en fonction de leur capacité et des situations de crise

Les débits demandés pour les liaisons internet sont de 50, 100, 200, 500 Mbps, 1 Gbps sur les sites de SPM. La capacité de chiffrement sur les concentrateurs centraux en métropole est de 1, 2 ou 5 Gbits de trafic chiffré.

Les équipements de sécurité assurant le chiffrement et le cloisonnement des flux vis-à-vis d'internet répondent aux exigences du chapitre 3.3.3 du présent CCTP. Le titulaire s'engage à fournir un service de chiffrement qualifié au sens de l'Ordonnance 2005-1516 (protection en confidentialité et intégrité) des flux métiers

et d'administration du RIE transitant hors du territoire national entre les territoires d'Outre-Mer français (DROM et COM) et l'Hexagone

{EX-L7/02} 3.4.1 Transit internet sécurisé : Le chiffrement des informations transitant sur le réseau de transport doit être réalisé par des chiffreurs qualifiés au niveau standard par l'ANSSI.

{EX-L7/03} 3.4.1 Transit internet sécurisé : Le titulaire précise la conformité de l'organisation qu'il met en place avec les dispositions de l'annexe I de l'Instruction Interministérielle n°901.

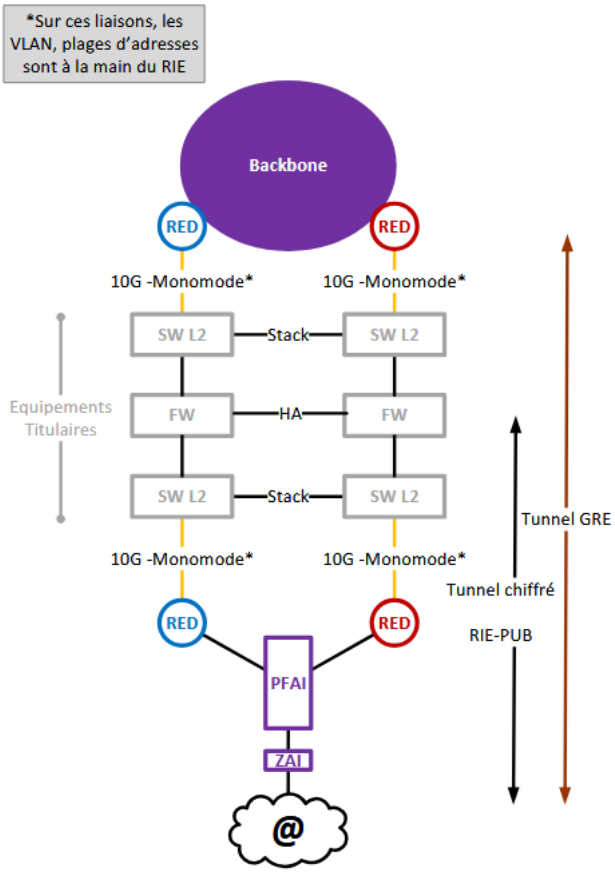
3.4.2 Raccordement sur la double épine dorsale du RIE en métropole

Côté métropole, le service de passerelle internet du RIE est utilisé pour raccorder les concentrateurs IPSEC. Les concentrateurs IPSEC sont raccordés entre la PFAI et les routeurs de la double épine dorsale.

Le schéma ci-dessous illustre l'architecture visée. Le titulaire fournit les équipements de chiffrement et les 4 commutateurs de raccordement sur les routeurs d'épine dorsale (RED) bleu et rouge.

Les flux véhiculés par les tunnels IPSEC chiffrés sont des tunnels GRE dont la terminaison est portée par les RED.

Les raccordements entre les commutateurs et les RED (routeurs d'épine dorsale) sont réalisés via des modules 10Gigabits monomode.



3.4.3 MTU

La MTU doit pouvoir être configurée au-delà de 1500 (« jumbo frame ») au minimum en IPv4 et IPv6 de bout en bout. Le chemin MTU (« Path MTU Discovery ») doit être fonctionnel tout le long de la liaison.

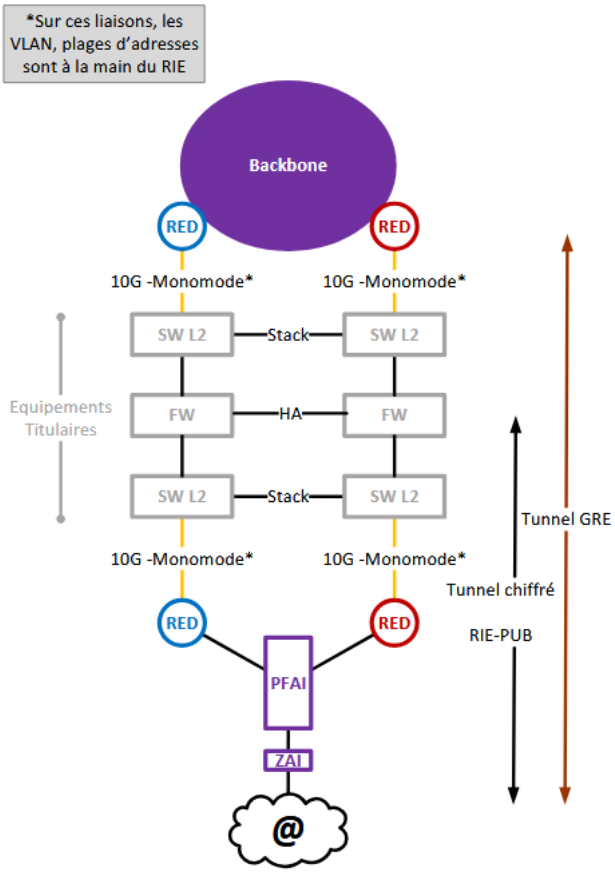
{EX-L7/04} 3.4.2 Raccordement sur la double épine dorsale du RIE en métropole

Côté métropole, le service de passerelle internet du RIE est utilisé pour raccorder les concentrateurs IPSEC. Les concentrateurs IPSEC sont raccordés entre la PFAI et les routeurs de la double épine dorsale.

Le schéma ci-dessous illustre l'architecture visée. Le titulaire fournit les équipements de chiffrement et les 4 commutateurs de raccordement sur les routeurs d'épine dorsale (RED) bleu et rouge.

Les flux véhiculés par les tunnels IPSEC chiffrés sont des tunnels GRE dont la terminaison est portée par les RED.

Les raccordements entre les commutateurs et les RED (routeurs d'épine dorsale) sont réalisés via des modules 10Gigabits monomode.



{EX-L7/05} MTU : Le titulaire détaille la MTU standard et la MTU maximale qu'il peut proposer sur ses accès en standard. Le cas échéant il précise s'il est possible d'aller au-delà et en précise les coûts (UO complémentaire par exemple). Il décrit les possibilités de paramétrages et les impacts inhérents. Il précise l'applicabilité du « Path MTU Discovery » dans son offre.

3.4.4 Qualité de service

L'Administration peut marquer ses flux IP selon le protocole DSCP.

Le service de transit ne doit pas modifier les champs DSCP des paquets IP, sauf accord ou demande expresse de l'Administration.

3.4.5 Protection des accès internet

Le fournisseur d'accès internet met en œuvre un dispositif anti-DDoS qui permet de protéger l'ensemble des sites clients déployés.

{EX-L7/06} 3.4.4 Protection des accès internet : le titulaire détaille le dispositif anti-DDoS mis en œuvre et les capacités de protection des sites de l'administration couverts par l'offre.

3.5 Lot 6 : Management des services

La DINUM envisage de déléguer à un tiers des prestations de service sur un périmètre comprenant :

- En phase de déploiement et migration, la coordination et le suivi des intervenants des accès de collecte et des POM (opérateur de collecte, opérateur de transit transocéanique, hébergeur de la plateforme, maîtrise d'ouvrage DINUM et bénéficiaires) avec l'organisation et l'animation des comités de suivi opérationnel et des groupes de travail nécessaires ;
- Pour toutes les phases, y compris en phase d'exploitation, la fourniture des tableaux de bord d'indicateurs consolidés, synthétiques et pertinents auprès des instances du pouvoir adjudicateur.

En sa qualité d'assistant à la maitrise d'ouvrage, le titulaire de ce lot a la responsabilité de la gestion de projet de déploiement des équipements (CE et POM) dans les sites et de migration des services (câblage, mise en baie, mise en service, VA, VSR et recette) en coordonnant les travaux et interventions de l'ensemble des différentes parties-prenantes.

Il assure la coordination de tous les titulaires des lots du présent marché en particulier sur les aspects suivants :

- Mise en place et le suivi d'un planning global des opérations à réaliser ;
- Déclinaison par accès d'un planning détaillé d'intervention avec mise en exergue des étapes critiques et des prérequis exigés ;
- Suivi et maitrise des risques ;
- Assistance à la recette ;
- Organisation et animation de réunions de suivi des opérations ;
- Mobilisation de l'ensemble des parties prenantes ;
- Gestion des alertes auprès du pouvoir adjudicateur afin d'arbitrage.

{EX-L6/01} 3.5 Lot 6 : Management des services : Le titulaire indique l'organisation qu'il compte mettre en place pour la gestion opérationnelle et sous quel délai une équipe projet peut être activée sur demande du pouvoir adjudicateur.

Chapitre 4 : Mise en œuvre des accords-cadres

4.1 Passation des commandes d'achat

La passation des commandes d'achat concerne toute demande d'achat ou d'acquisition d'équipements, de services, de prestations, de déploiement de liens ou des accès du présent accord-cadre.

Chaque passation d'une commande d'achat est formalisée par un bon de commande envoyé au titulaire dont la réception vaut date de notification et ordre d'exécution.

Le bon de commande est structuré en deux parties :

- Un volet administratif et financier :

  Le volet administratif et financier correspond à la commande budgétaire « CHORUS » émise directement par le service achat des bénéficiaires auprès du titulaire.

- Un volet technique :

  Le volet technique d'une commande d'achat est :

  - Soit saisi par les bénéficiaires dans l'Extranet RIE de la DINUM ;
  - Soit décrit dans un fichier par le service bénéficiaire et transmis auprès du département ISO de la DINUM.

L'émission des commandes d'achat se fait :

- Pour une commande des bénéficiaires d'achat d'un accès ou d'un lien, le volet technique de la commande saisie dans l'Extranet RIE est aiguillé de manière automatisée vers le titulaire du lot 1 ou 2 concerné ;
- Pour une commande liée à la mise en place d'outil ou liée à l'organisation de l'accord-cadre, la commande est passée par la DINUM quel que soit le lot concerné ;
- Pour une commande de prestation pour les titulaires des lots 3, 4 et 5, la commande est passée par la DINUM ;
- Pour une commande des bénéficiaires de prestations ponctuelles (formations, expertises…), les bénéficiaires passent directement leur commande auprès des titulaires ; ces commandes ayant pu faire l'objet de demande et d'établissement d'un devis.

Les modalités de passation et de formalisation des bons de commandes sont exposées à l'article 4 du CCAP.

4.2 Plan d'assurance qualité de l'accord-cadre (PAQ)

Le plan d'assurance qualité (PAQ) de l'accord-cadre est établi lors :

- De l'initialisation de l'accord-cadre des lots 1 à 5 et 7 ;
- De l'initialisation de l'accord-cadre du lot 6.

Le PAQ de l'accord-cadre est mis à jour régulièrement pour refléter l'état réel de l'accord-cadre en cas d'évolutions et/ou changements des éléments constitutifs au PAQ de l'accord-cadre.

Les évolutions du PAQ de l'accord-cadre sont validées par le titulaire et l'Administration, généralement lors d'un Comité de pilotage de l'accord-cadre « COPIL ».

{PP-L1 à 7/01}. 4.2 Plan d'assurance qualité de l'accord-cadre (PAQ) : Proposition d'un plan type d'assurance qualité de l'accord-cadre.

4.3 Plan de gestion et d'amélioration continue (PGAC)

Les prestations font l'objet d'un plan de gestion et d'amélioration continue.

L'objet de ce plan est d'identifier des axes d'amélioration et définir les plans d'actions associés visant au renfort de l'efficacité des intervenants du titulaire et des ressources de l'Administration.

{PP-L1 à 7/02}. 4.3 Plan de gestion et d'amélioration continue (PGAC) : Proposition d'un plan de gestion et d'amélioration continue en détaillant notamment les principaux axes, la démarche et la mise en œuvre de l'amélioration continue.

4.4 Politique de sécurité

4.4.1 Accès aux locaux et usage des ressources

Les modalités d'accès aux sites (qu'ils soient de collecte ou de concentration à l'épine dorsale du RIE) sont susceptibles pour certains sites de collectes et pour tous les sites de concentration de faire l'objet de conditions d'accès particulières, notamment en cas de contrôle élémentaire préalable obligatoire, et d'entrainer à ce titre des délais d'obtention des autorisations dont les titulaires doivent tenir compte dans le déroulement de leurs actions.

Les personnels du titulaire qui ont accès aux locaux et/ou aux informations de l'Administration sont nommément désignés. Ils respectent les règles de sécurité générale de la DINUM et en particulier la PSSI du RIE ainsi que, en tant que de

besoin, les règles de sécurité particulières en vigueur au sein des établissements auxquels il doit accéder pour ses interventions.

Les accès aux locaux de l'Administration sont sécurisés et réglementés. Les modalités d'accès sont précisées par l'Administration lors de la réunion de lancement. Ces modalités peuvent varier en fonction des locaux concernés. Certains sites peuvent en outre nécessiter la réalisation préalable d'une mesure de contrôle élémentaire des personnels du titulaire intervenant sur site, mesure prévue à l'article 32 de l'**Erreur ! Source du renvoi introuvable.** (cf. référence [R6]) et à l'article L114-1 du Code de la Sécurité Intérieure (cf. référence [R7]).

Le titulaire se soumet sans réserve à cette mesure ainsi qu'aux décisions d'autorisation ou de refus d'admission qui en découlent.

Lors d'un accès par le titulaire au site d'un centre d'exploitation de l'Administration, par exemple pour une intervention technique, le titulaire respecte, pour le site considéré :

- La date et la plage horaire de la visite qui ont été préalablement définies conjointement entre le titulaire et l'Administration ;
- Les modalités d'accès, notamment en matière d'identification et de contrôle de sûreté, ainsi que les règles de sécurité définies par le responsable du site concerné ;
- Les procédures et règles de fonctionnement définies par le responsable du site concerné.

La gestion des prises de rendez-vous est définie par les procédures de l'Administration en fonction de la sensibilité, d'un point de vue sécuritaire, du site concerné par la visite.

Le titulaire informe l'Administration **au moins sept jours calendaires à l'avance** de toute visite de site ou intervention technique au sein d'un site de l'Administration.

Ce délai peut être prolongé lorsqu'une mesure de contrôle élémentaire doit être réalisée.

Ce délai peut être raccourci en cas d'urgence opérationnelle avérée et avec l'accord préalable de l'Administration et du responsable du site concerné.

Les visites et interventions techniques du titulaire au sein d'un site se font :

- Pendant les jours et heures d'ouverture du site concerné ;
- En présence d'un représentant local du site ;
- En respectant les procédures d'accréditation requises et les préavis définis par les règles spécifiques d'accès au site concerné.

4.4.2 Respect de la législation et de la règlementation en vigueur et SSI

Le titulaire s'engage à respecter les lois, règlements et les normes en vigueur, notamment celles liées à la sécurité des systèmes d'information ainsi qu'à la réglementation des communications électroniques.

Il s'engage par ailleurs à prendre connaissance, respecter et faire respecter :

- La PSSI RIE Version 2.0 – juin 2019 (cf. annexe [A3]) ;
- L'**Erreur ! Source du renvoi introuvable.** (cf. référence [R8]) ;
- La Politique de sécurité des systèmes d'information de l'état (PSSIE) (cf. référence [R9]) ;
- Les Bonnes pratiques et les règles d'hygiène informatique édictées notamment par l'ANSSI (cf. annexe [A4]) ;
- Le **Erreur ! Source du renvoi introuvable.** (cf. référence [R10]) ;
- Le **Erreur ! Source du renvoi introuvable.** (cf. référence [R11]) ;
- Le Règlement général sur la protection des données (RGPD) (cf. référence [R12]) ;
- Les autres normes et standards applicables émis par les organismes de normalisation.

{PP-L1 à 7/03}. 4.4.2 Respect de la législation et de la règlementation en vigueur et SSI : Présentation sous la forme d'une matrice de la conformité, de l'organisation mise en place en vue de respecter les dispositions de l'annexe 1, intitulée « Règles pour les entités situées hors du champ d'application de la PSSIE », de l'**Erreur ! Source du renvoi introuvable.** (cf. référence [R8]).Plan d 'assurance sécurité (PAS)

4.4.3 Plan d'assurance sécurité (PAS)

De façon générale, le titulaire applique et fait appliquer à ses éventuels sous-traitants la politique de sécurité du RIE et respecte les exigences de sécurité du présent marché décrites au chapitre « Respect de la législation et de la règlementation en vigueur et SSI ».

Le titulaire définit en particulier :

- L'organisation mise en place ;
- La méthodologie à suivre pour gérer la sécurité ;
- Les mesures techniques, organisationnelles et procédurales mises en œuvre.

4.4.3.1 Contenu du Plan d'assurance sécurité (PAS)

Le titulaire élabore un plan d'assurance sécurité (PAS) décrivant l'ensemble des dispositions spécifiques à mettre en œuvre pour garantir le respect des exigences de sécurité.

Outre les éléments définis dans les différentes prestations de service attendues, le PAS comprend a minima les thèmes suivants :

- L'organisation de la sécurité du titulaire, incluant :
  - L'ensemble des contraintes légales, réglementaires ou émises par l'Administration ;
  - Les modalités d'application de la politique de sécurité interne.
- La gestion des ressources humaines, incluant :
  - La politique de gestion des ressources humaines dans l'optique de la sécurité dont :
    - La sensibilisation des personnels à la SSI ;
    - La formation des personnels à la SSI ;
  - La gestion des habilitations délivrées dans le cadre de l'application de la réglementation visant la protection du secret.
- Le rôle du correspondant de sécurité, incluant ;
  - Le profil type du correspondant valable pour toute la durée de l'accord-cadre ;
  - Les modalités de suppléance pour pallier une éventuelle indisponibilité
  - Les modalités de notification de son remplacement ;
  - Les modalités pour traiter les questions relatives notamment :
    - Au suivi des incidents de sécurité opérationnels ;
    - Au maintien et de la mise en application du PAS ;
    - A tout autre sujet ayant attrait à la sécurité de l'accord-cadre
- L'évaluation de la sensibilité et protection des informations :
  - Description de la politique d'évaluation de la sensibilité des informations et du processus de traitement adapté aux obligations réglementaires.
- La gestion des risques :
  - Description de la gestion des risques et du suivi permanent de son niveau de maitrise de risques ainsi que du respect des politiques et règles de sécurité applicables, y compris auprès de ses propres sous-traitants.
- L'architecture et exploitation des SI :

- Description des réseaux et les systèmes mis en place en précisant les éventuelles interconnexions avec d'autres réseaux et les moyens mis en œuvre pour tenir à jour la cartographie des SI.

- La sécurité des postes de travail et des supports informatiques :
  - Description des mesures mises en place pour assurer et garantir la sécurité des postes de travail et des supports informatiques.
- La gestion des autorisations d'accès physiques :
  - Description de la procédure de gestion des accès physiques aux bâtiments du titulaire avec notamment les modalités de gestion des demandes et de suppressions d'accès.
- La gestion des autorisations et contrôle d'accès logiques aux ressources :
  - Description de la procédure de gestion des accès logiques aux ressources avec notamment les modalités de gestion des demandes et de suppressions d'accès ainsi que les modalités de contrôle.
- La gestion de la continuité d'activité du titulaire :
  - Description des mesures mises en place afin d'assurer la continuité d'activité.
- La gestion de crise sécurité :
  - Description, sur son domaine de responsabilité SI, du processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'évènements remettant en cause de façon inacceptable le respect des engagements de service et de sécurité SI contractualises. Ce volet précise au minimum :
    - Les principes d'escalades (critères de déclenchement, synoptique d'escalade) ;
    - La composition de la cellule de crise : fonctions et responsabilités des membres. La liste nominative des membres et de leurs suppléants est référencée dans un annuaire tenu à jour par le correspondant sécurité ;
    - Les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).
- Le Maintien en condition de sécurité, conformité et démarche de contrôle interne :
  - Description des procédures et les fréquences des contrôles internes mises en place pour garantir la conformité et le niveau de sécurité au démarrage de l'accord-cadre ainsi que son maintien tout au long de l'accord-cadre.

{PP-L1 à 7/04}. 4.4.3.1 Contenu du Plan d'assurance sécurité (PAS) : Proposition d'un Plan type d'Assurance Sécurité.

4.4.3.2 Modalité d'exécution du Plan d'assurance sécurité (PAS)

{PP-L1 à 7/05}. 4.4.3.2 Modalité d'exécution du Plan d'assurance sécurité (PAS) : Proposition d'une organisation en précisant les fonctions de sécurité générale, de sécurité des systèmes d'information et de sûreté déjà existantes.

Conformément aux procédures et fréquences des contrôles internes, le correspondant sécurité communique sans délai les résultats de ces contrôles.

En cas d'écart ou de non-conformité au niveau d'exigence requis, un plan de remédiation est formalisé et communiqué après la constatation des écarts mentionnés.

La régularisation de ces écarts et non-conformités peut donner lieu à la mise en place d'un plan dont l'application peut se faire dans un délai convenu entre l'Administration et le titulaire.

4.5 Gouvernance de chaque accord-cadre

4.5.1 Comité de pilotage « COPIL »

Caractéristiques	Description
Objet	Le comité de pilotage pour l'ensemble des lots, tenu lot par lot, est l'instance décisionnelle qui assure le pilotage de l'accord-cadre et les éléments de la gouvernance qualité (PAQ) et sécurité (PAS) communs à tous les lots de 1 à 5 et 7. Cette instance met en place et suit les dispositions et les opérations communes à tous les titulaires.
Périodicité	▪ Mensuelle lors de la migration ; ▪ Trimestrielle post-migration.
Membres permanents	▪ Le Chef du département ISO de la DINUM ; ▪ Les responsables des pôles production (ROC), pilotage de la qualité et des partenariats (PQP), hypervision (NOC) ; ▪ Le représentant légal du titulaire.
Membres occasionnels	Autres invités sur décision de la DINUM.
Lieu	Dans les locaux de l'Administration et/ou en visioconférence.
Préparation	La préparation de cette instance est à la charge de la DINUM assistée du titulaire du lot 6 le cas échéant.
Rôle	Les participants ont autorité pour décider des actions et acter des décisions relatives au fonctionnement et au déroulement des prestations de l'accord-cadre. Ce comité a pour objectif d'examiner et d'étudier toutes les questions contractuelles et liées au déroulement des prestations, d'arbitrer et d'assurer la gestion des risques liés.

Caractéristiques	Description
	Il permet la remontée d'informations auprès de l'assistant à maîtrise d'ouvrage sur le déroulement des prestations.
Ordre du jour type	L'ordre du jour de ce comité se base sur les éléments suivants : ▪ La validation du compte rendu de la précédente réunion ; ▪ Les indicateurs de pilotage ; ▪ Le bilan de l'avancement de la prestation de migration puis de raccordement, la synthèse des travaux et le résultat des actions particulières effectuées ; ▪ L'examen du portefeuille de risques ; ▪ La mise à jour des plannings si nécessaire ; ▪ Les décisions en suspens, pouvant impliquer d'autres intervenants ; ▪ Les indicateurs de qualité ; ▪ Les aspects financiers ; ▪ La synthèse des actions prévues pour la période à venir et le calendrier des réunions suivantes ; ▪ Le bilan des validations de livrables et de recettes.
Restitution	Chaque comité fait l'objet d'un compte rendu réalisé par le titulaire du lot 6 le cas échéant et à défaut par le titulaire du lot considéré.

4.5.2 Comité d'exploitation « COMEX »

Caractéristiques	Description
Objet	Le comité exploitation, pour l'ensemble des lots, tenu lot par lot, a pour périmètre l'exploitation du RIE. Il permet aux différents acteurs d'assurer une qualité de service et une qualité de prestation de gestion par les titulaires.
Périodicité	Mensuelle
Membres permanents	▪ Les responsables des pôles production ROC), pilotage de la qualité et des partenariats (PQP), hypervision (NOC) ; ▪ Le responsable technique du titulaire
Membres occasionnels	Autres invités sur décision de la DINUM ou du département ISO
Lieu	Dans les locaux de l'Administration et/ou en visioconférence
Préparation	La préparation de cette instance est à la charge de la DINUM assistée du titulaire du lot 6 le cas échéant, sur la base des *reportings* extraits des indicateurs remontés des titulaires des lots 1 à 5 et 7 (cf. chapitre « Préparation du comité d'exploitation »).
Rôle	Le comité d'exploitation a pour but l'analyse des indicateurs de suivi de la qualité de service et de la qualité de la prestation de gestion opérationnelle des titulaires des lots 1 à 5 et 7. Le comité d'exploitation repose a minima sur les deux livrables suivants :

Caractéristiques	Description
	▪ Une présentation synthétique des indicateurs de qualité de service ; ▪ Un tableau de bord d'exploitation.
Indicateurs de qualité de service sur le trimestre écoulé	Une synthèse trimestrielle des principaux indicateurs suivants doit être au moins présentée pour chaque trimestre écoulé : ▪ Taux d'incident sur parc ; ▪ Nombre d'incidents en dépassement de GTR et taux d'incidents résolus dans la GTR ; ▪ Indisponibilité mensuelle par site, en durée, par famille de niveau de sécurisation ; ▪ Indisponibilité annuelle par site, avec le nombre de sites en dessous de la valeur d'engagement, par famille de niveau de sécurisation ; ▪ Taux d'incidents ouverts de façon proactive ; ▪ Nombre d'incidents multi-bénéficiaires ; ▪ Nombre et typologie des demandes de modification (créations, changements, résiliations) en dépassement de délai ; ▪ Nombre et typologie des demandes de modification (créations, changements) ayant fait l'objet d'une invalidation de production par la DINUM (pôle-Production).
Indicateurs de qualité de service mensuels, avec évolution par rapport au mois précédent	Une synthèse mensuelle des indicateurs et informations suivants doivent être au moins présentés, sur une base mensuelle avec évolution par rapport au mois précédent : ▪ Nombre d'incidents, ventilés par responsabilité opérateur / client ; ▪ Nombre d'incidents multi-clients ; ▪ Nombre d'incidents en dépassement de GTR et taux d'incidents résolus dans la GTR ; ▪ Nombre d'escalades ; ▪ Taux de tickets proactifs de sévérité 1 et 2 ; ▪ Nombre et typologie des demandes de modification (créations, changements, résiliations) : reçues, traitées, en cours de production, etc. ▪ Nombre et typologie des demandes ayant été produites au-delà du délai contractuel et taux de respect des délais de production ; ▪ Délais moyen, médian, maximum et minimum de production des demandes réalisées de la période par type de demande ; ▪ Délai de prise en compte des demandes (mesuré entre la transmission de la demande par l'Administration au titulaire et son apparition dans les outils de suivi et de *reporting* de production du titulaire).
Analyses des indicateurs de qualité de service	Les informations suivantes doivent être a minima présentées, sur une base mensuelle : ▪ Analyse du nombre de productions en dépassement de délais, précisant : - Le nombre de production en dépassement de délai, le taux de

Caractéristiques	Description
	respect des délais de production sur 13 mois glissants ; - Les causes de dépassement de délais de production ; - Les délais de production, ventilés par plages en nombre de semaines de dépassement. ▪ Analyse du nombre de tickets en dépassement de GTR, précisant : - Le nombre de tickets en dépassement de GTR, le taux de respect de la GTR, en distinguant les incidents unitaires des incidents génériques ou multi-bénéficiaires, sur 13 mois glissants, - Les causes des incidents en dépassement de GTR (CPE, backbone opérateur…) ; - Les délais de rétablissement des tickets d'incident de sévérité 1, ventilés par plage horaire 0-4H, 4-6H, 6-8H, 8-10H, 10-12H et 12H et plus. ▪ Analyse du taux global de disponibilité, sur 13 mois glissants ; ▪ Analyse du taux global de respect des délais de production, sur 13 mois glissants ; ▪ Analyse du taux d'incident sur parc, précisant sur 13 mois glissants : - Le nombre d'incidents de responsabilité opérateur ; - Le nombre de liens déployés ; - Le taux d'incident déduit des précédents indicateurs. ▪ Analyse du nombre d'incidents majeurs, sur 13 mois glissants : - Nombre d'incidents majeurs de responsabilité opérateur ou administration, - Nombre d'incidents majeurs d'origine multi-clients ; ▪ Analyse du nombre d'escalades, ventilé par niveau d'escalade, sur 13 mois glissants ; ▪ Analyse du nombre d'escalades de production, ventilées par niveau d'escalade, sur 13 mois glissants ; ▪ Analyse des incidents récurrents, précisant le code RIE de l'accès concerné, le nombre total d'occurrences, l'évolution du nombre d'occurrences par rapport au mois antérieur (évolution du total sur 13 mois glissants), la cause de la dernière occurrence, et la dernière action engagée ainsi que le plan de résolution identifié.
Tableau de bord d'exploitation	Le tableau de bord d'exploitation est relatif au suivi de la qualité de service : pour une période d'observation mensuelle, ce tableau de bord consolide : ▪ L'ensemble des tickets d'incident fermés sur la période d'observation ; ▪ L'ensemble des raccordements fermés sur la période d'observation. Le tableau de bord recense également les indicateurs de disponibilité du réseau et de délai de production, avec l'historique nécessaire à l'appréciation de leur évolution et à la vérification du respect des exigences contractuelles. Ce tableau de bord est livré au moins sous un format conforme à l'un des

Caractéristiques	Description
	formats recommandés par le référentiel général d'interopérabilité. Il doit impérativement pouvoir faire l'objet d'un traitement informatisé automatique. Les formats riches et / ou propriétaires ne peuvent donc pas être les formats exclusivement communiqués. Le titulaire est en mesure de décrire la méthodologie de calcul, d'extraction et de traitement automatique (typage, nomenclature ou standard respecté, par exemple le format ISO8601/RFC3339 pour les dates) des données d'indicateurs enregistrées dans le tableau de bord. Le titulaire doit communiquer l'intégralité des données brutes qui permettent le re-calcul des indicateurs présentés
Restitution	Chaque comité fait l'objet d'un compte rendu réalisé par le titulaire du lot 6 le cas échéant et à défaut par le titulaire du lot considéré.

4.5.3 Comité de sécurité « COSEC »

Caractéristiques	Description
Objet	Le comité de sécurité, pour l'ensemble des lots, tenu lot par lot, est l'instance qui garantit la mise en œuvre et le maintien en condition de sécurité. Les participants ont autorité pour décider des actions et acter des décisions relatives au fonctionnement et au déroulement de la prestation, sous couvert du comité de pilotage marché, pour toutes questions en matière de Sécurité des Systèmes d'Information (SSI).
Périodicité	Au moins trimestrielle ou d'une durée inférieure et ponctuellement en cas d'événement ou autre nécessité, sur demande de l'un des participants, validée par le RSSI du RIE (DINUM ISO).
Membres permanents	▪ Le RSSI du département ISO de la DINUM qui préside le comité ; ▪ Le responsable du CSIRT DINUM ; ▪ Les responsables des pôles production (ROC), pilotage de la qualité et des partenariats (PQP), hypervision (NOC) ; ▪ Le responsable sécurité du titulaire ; ▪ Le titulaire du lot 6 le cas échéant.
Membres occasionnels	Autres invités sur décision de la DINUM ou du département ISO
Lieu	Dans les locaux de l'Administration et/ou en visioconférence
Ordre du jour type	L'ordre du jour des réunions « ordinaires » du comité de sécurité comprend au minimum : ▪ La validation du compte rendu de la précédente réunion ; ▪ L'analyse des indicateurs de performances liées à la sécurité et des écarts par rapport aux objectifs fixés ; ▪ Le point des actions non soldées et le bilan des actions terminées ; ▪ La mesure de l'efficacité des processus ;

Caractéristiques	Description
	▪ Le point des non-conformités règlementaires ayant un impact sur la sécurité ; ▪ Annuellement, le bilan des actions de l'année écoulée et la définition des objectifs de sécurité pour l'année suivante.
Préparation	La préparation de cette instance est à la charge de la DINUM assistée du titulaire du lot 6 le cas échéant, sur la base des *reportings* extraits des outils des titulaires des lots 1 à 5 et 7.
Rôle	Le comité de sécurité est une des instances de pilotage des prestations tout particulièrement chargée de garantir la mise en œuvre et le maintien en conditions de sécurité. Pour ce faire, il doit notamment : ▪ Proposer la politique de sécurité, en conformité avec les règles et « bonnes pratiques » en vigueur ; ▪ Définir et adopter les processus transcrivant les niveaux de sécurité attendus dans les activités opérationnelles ; ▪ Prendre acte des résultats des activités de gestion des risques : identification des risques (événements redoutés, scénarios de menace), évaluation des risques (gravité et vraisemblance), traitement préventif ou correctif des risques (mesures de sécurité préconisées, plans d'action), analyse et retour d'expérience (cartographie, détermination d'événements déclencheurs…) ; ▪ Valider les mesures organisationnelles et techniques proposées dans le cadre du processus de gestion des risques et en mesurer les effets ; ▪ Décider des mesures à mettre en œuvre à la suite de l'évaluation initiale d'un risque nouveau ou à la réévaluation d'un risque déjà identifié ; ▪ Assurer une surveillance continue : - Du niveau de performance en matière de sécurité des activités opérationnelles, au regard de la politique de sécurité et des objectifs définis ; - De la mise en œuvre de plan d'actions lorsque ce niveau de performance est dégradé ; - De la mise en œuvre effective et dans les délais appropriés de chaque action de sécurité lié à un évènement ou un risque identifié, - De l'efficacité des processus relatifs au maintien en conditions de sécurité ; ▪ Veiller, le cas échéant, au respect des procédures relatives au Règlement général sur la protection des données (RGPD) en relation avec les référents habilités des titulaires concernés et de la DINUM ; ▪ Veiller à ce que les ressources suffisantes soient allouées en termes de fonctionnement et de réalisation des objectifs de sécurité ; ▪ Valider les méthodes de promotion de la sécurité ; ▪ Proposer les orientations, techniques et organisationnelles, s'agissant de sécurité, à soumettre au comité de pilotage pour validation.
Tableau de bord sécurité	Le tableau de bord sécurité est relatif au suivi du niveau de sécurité global et des éventuels incidents de sécurité. Pour une période d'observation

Caractéristiques	Description
	mensuelle, ce tableau de bord consolide *au moins* : ▪ La revue des comptes et des droits permettant les accès aux différents systèmes (Portail d'exploitation, agrégats d'événements, TACACS, etc.) et leurs usages ; ▪ Le suivi du parc, de l'état du support et du MCO/MCS ; ▪ Le suivi des vulnérabilités affectant le parc, l'analyse de leur applicabilité et de leur impact ; ▪ Le suivi des incidents de sécurité signalés, de leur qualification et de leur traitement ; ▪ Le suivi du plan d'assurance sécurité des plans de mise à jour MCO/MCS, le suivi des éventuels plans de remédiation aux vulnérabilités, les retours d'expérience sur incident et les propositions d'amélioration. Le tableau de bord sécurité est transmis au plus tard 48 heures ouvrées avant chaque réunion planifiée du COSEC. Il fait l'objet de mesures de protection adéquates lors de sa transmission.
Restitution	Chaque comité fait l'objet d'un compte rendu réalisé par le titulaire du lot 6 le cas échéant et à défaut par le titulaire du lot considéré.

4.5.4 Comité de projet (de déploiement) « COPROJ »

Caractéristiques	Description
Objet	Le comité projet assure la mise en place et le suivi global des opérations dans le cadre : ▪ Des migrations des sites ; ▪ Des raccordements multisites et/ou multi-liens (plus de 20 liens) post-migration.
Périodicité	▪ Hebdomadaire, la périodicité peut néanmoins être variable en fonction du nombre de raccordements en cours de production
Membres permanents	▪ Les responsables des pôles production (ROC), pilotage de la qualité et des partenariats (PQP), hypervision (NOC) ; ▪ Les personnes en charge des sites des bénéficiaires ou leurs représentants ; ▪ Le directeur de projet du titulaire. ▪ Le titulaire du lot 6 le cas échéant.
Membres occasionnels	Autres invités sur décision de la DINUM ou du département ISO
Lieu	Dans les locaux de l'Administration et/ou en visioconférence
Préparation	La préparation de cette instance est à la charge de la DINUM assistée du titulaire du lot 6 le cas échéant, sur la base des *reportings* extraits des outils des titulaires des lots 1 à 5 et 7.

Caractéristiques	Description
Rôle	Le comité de de projet de déploiement suit à un niveau hiérarchique supérieur, l'avancement des travaux de la migration des sites et/ou de raccordements multisites et/ou multi liens (plus de 20 liens) post-migration. Le COPROJ remonte à l'instance COPIL l'ensemble des éléments nécessitant arbitrage, et présentant un impact direct sur la qualité des prestations et la sécurité des sites. Il émet également des recommandations sous forme de note(s), à l'attention du COPIL dans le but de faciliter la prise de décision.
Ordre du jour type	L'ordre du jour type : ▪ Parcours des tableaux de bords des migration et/ou des raccordements ; ▪ Suivi des macro-planning des jalons clés sur les différents sites ; ▪ Analyse des risques et des problèmes ayant un impact sur le projet ; ▪ Validation des actions proposées par le COSUI ; ▪ Date du ou des prochains comités.
Restitution	Chaque comité fait l'objet d'un compte rendu réalisé par le titulaire du lot 6 le cas échéant et à défaut par le titulaire du lot considéré.

4.5.5 Comité de suivi « COSUI »

Caractéristiques	Description
Objet	Le comité de suivi assure le suivi opérationnel des actions de raccordements post-migration.
Périodicité	Hebdomadaire, la périodicité peut néanmoins être variable en fonction du nombre de raccordements en cours de production
Membres permanents	▪ Les responsables des pôles production (ROC), pilotage de la qualité et des partenariats (PQP), hypervision (NOC) ; ▪ Les personnes en charge des sites des bénéficiaires ou leurs représentants ; ▪ Le chef de projet du titulaire ; ▪ Le titulaire du lot 6 le cas échéant.
Membres occasionnels	Autres invités sur décision de la DINUM ou du département ISO
Lieu	Dans les locaux de l'Administration et/ou en visioconférence
Préparation	La préparation de cette instance est à la charge de la DINUM assistée du titulaire du lot 6 le cas échéant, sur la base des *reportings* extraits des outils des titulaires des lots 1 à 5 et 7.
Rôle	Ce comité a pour objectif d'assurer le suivi de l'avancement des raccordements des sites post-migration, le suivi des plannings, suivi des risques et dérives.

Caractéristiques	Description
	Il permet d'étudier les problématiques techniques et/ou de sécurité. Le comité de suivi remonte au comité de pilotage tout élément décisionnel nécessaire au bon avancement du projet.
Ordre du jour type	L'ordre du jour type est le suivant : ▪ Présentation du journal horodaté des incidents à corriger en cours de projets ou des problèmes rencontrés ; ▪ Parcours des tableaux de bords des raccordements ; ▪ Suivi du planning détaillé et des jalons ; ▪ Analyse des risques et des problèmes ; ▪ Identification des actions nécessaires ; ▪ Suivi des actions liées projet ; ▪ Date du ou des prochains comités.
Restitution	Chaque comité fait l'objet d'un compte rendu réalisé par le titulaire du lot 6 le cas échéant et à défaut par le titulaire du lot considéré.

4.6 Management des services (Lot 6)

Le Lot 6 relatif au management des services traite des prestations d'assistance à maîtrise d'ouvrage pour coordonner et assister la DINUM au pilotage de l'ensemble des prestations des titulaires des autres lots du présent accord cadre et également des prestations des titulaires des marchés spécifiques de services de collecte dans les territoires de la Polynésie Française et de la Nouvelle-Calédonie.

4.6.1 Initialisation du Lot 6

Définition globale de l'activité		
L'initialisation du Lot 6 a pour objectif : ▪ De mettre en place et d'initialiser ses outils de pilotage et de suivi, en particulier le plan d'assurance qualité de l'accord-cadre (PAQ accord-cadre) ; ▪ De mettre en œuvre la gouvernance de l'accord-cadre ; ▪ De mettre en œuvre le *reporting* des activités liées aux services.		
Description générale de l'activité		
Phase	**Tâches**	**Livrables**
1	**Préparer l'Initialisation** Le titulaire : ▪ Organise une réunion de lancement avec l'Administration ; ▪ Participe aux réunions de lancement organisées avec les titulaires des lots 1 à 5 et 7 ; ▪ Définit le plan d'actions précis de cette prestation d'initialisation avec le planning associé.	▪ Plan d'actions ; ▪ Planning ; ▪ Compte rendu des réunions.

2	**Mettre en œuvre le cadre organisationnel** Dans le respect des modalités de la gouvernance de l'accord-cadre, le titulaire définit conjointement avec les titulaires des lots 1 à 5 et 7 et met en œuvre les modalités d'échanges harmonisées avec les titulaires des lots 1 à 5 et 7 : ▪ Pour la préparation des comités de la gouvernance de l'accord-cadre ; ▪ Pour le *reporting* des activités liées aux services. En cas de désaccord, l'Administration définit les modalités de gouvernance et de *reporting* de l'accord-cadre.	▪ Modalité des échanges mises en œuvre.
3	**Rédiger les différents plans de l'accord-cadre : PAQ, PGAC et PAS** Le titulaire : ▪ Rédige le Plan d'assurance sécurité (PAS) de son périmètre ; ▪ Elabore le Plan d'assurance qualité de l'accord cadre (PAQ) de son périmètre ; ▪ Elabore le Plan de gestion et d'amélioration continue (PGAC) de son périmètre.	▪ PAQ Accord-cadre ; ▪ PGAC Accord-cadre ; ▪ Plan d'Assurance Sécurité.

Engagement de service

Les engagements sur la fourniture des livrables sont :

- Le délai maximum de la mise œuvre **des modalités des échanges** avec les titulaires des lots 1 à 5 et 7 est de **15 jours ouvrés** à compter de la notification de l'accord-cadre ;
- Le délai maximum de l'actualisation du plan d'assurance sécurité de l'accord-cadre (**PAS**) est de **20 jours ouvrés** à compter de la notification de l'accord-cadre ;
- Le délai maximum de l'actualisation du plan d'assurance qualité de l'accord-cadre (**PAQ Accord-cadre**) est de **20 jours ouvrés** à compter de la notification de l'accord-cadre ;
- Le délai maximum de l'actualisation du Plan de gestion et d'amélioration continue de l'accord-cadre (**PGAC Accord-cadre**) est de **20 jours ouvrés** à compter de la notification de l'accord-cadre.

Outils du titulaire

Les éventuels outils informatiques du titulaire respectent la politique de sécurité et notamment les engagements relatifs aux portails clients, interfaces et développements spécifiques.

Unité d'œuvre associée

L'unité d'œuvre de cette prestation est un forfait.

{PP-L6/02} 4.6.1 Initialisation du Lot : Exemple de planning d'initialisation en précisant le nombre et la nature des ateliers à réaliser avec l'Administration et/ou son assistant à maîtrise d'ouvrage.

{PP-L6/03} 4.6.1 Initialisation du Lot : Description des moyens humains et organisationnels mis en œuvre en précisant notamment, les profils pressentis, les expériences dans ce type de projet de migration et les CV types.

{PP-L6/04} 4.6.1 Initialisation du Lot : Proposition de modalités d'échanges avec les titulaires des lots 1 à 5 et 7, à soumettre à l'approbation de l'Administration pour la préparation des comités de la gouvernance de l'accord-cadre et le *reporting* des activités liées aux services.

4.6.2 Assistance à maîtrise d'ouvrage de la migration

Le titulaire assiste la DINUM dans le pilotage global de la migration. Cette assistance couvre le suivi et la coordination de l'ensemble des activités de migration, jusqu'à la fin de la vérification en service régulier (VSR) réalisée pour chaque nouveau déploiement.

La prestation d'accompagnement de la migration comprend :

- Une phase de Cadrage du projet de migration des sites du titulaire du lot 6 en vue de la préparation des migrations au cours de laquelle, le titulaire élabore notamment un plan de migration détaillé pour chacun des lots 1 à 5 et 7 du présent accord-cadre et chaque marché de l'accord-cadre à renouveler ;
- L'assistance au pilotage des migrations des marchés de l'accord-cadre à renouveler jusqu'à la bascule de responsabilité vers les titulaires des lots 1 à 5 et 7.

4.6.2.1 Cadrage du projet de migration des sites

Définition globale de l'activité
Le cadrage du projet de migration débute dès la notification de l'accord-cadre, ce cadrage a pour objectif : ▪ La préparation du projet de migration au cours de laquelle, le titulaire élabore notamment un plan de migration détaillé pour chacun des lots 1 à 5 et 7 du présent accord-cadre et chaque marché de l'accord-cadre à renouveler ; ▪ La mise au point le dispositif d'assistance au pilotage des migrations jusqu'à la fin de la migration.

Description générale de l'activité		
Phase	**Tâches**	**Livrables**
1	**Préparation des différents projets de migration** L'objet de cette phase est de mettre en place les conditions préalables nécessaires à la réalisation effective des migrations par les titulaires des lots 1 à 5 et 7, en coordination avec les différents bénéficiaires de l'Administration. A cet effet, le titulaire du lot 6 : ▪ Prend connaissance du périmètre de l'accord-cadre à migrer et des acteurs concernés ; ▪ Initialise la démarche du projet de migration et met en place l'ensemble des outils et *reporting* associés ; ▪ Eventuellement, sollicite les titulaires des lots 1 à 5 et 7, pour vérifier les éligibilités de certains sites des bénéficiaires (à noter que certains types d'accès de l'accord-cadre à renouveler ont été supprimés) ; ▪ Elabore un plan de migration pour chacun des titulaires des lots 1 à 5 et 7, à l'appui duquel il repositionne les phases de la démarche de déploiement ; ▪ Initie une matrice de gestion des risques ; ▪ Adapte et met à jour la gouvernance du projet selon les titulaires des lots 1 à 5 et 7 retenus (fréquences des réunions, regroupements potentiels…) ; ▪ Prépositionne dans un calendrier prévisionnel, au sein des phases, en accord avec les bénéficiaires et les titulaires des lots 1 à 5 et 7, les différentes étapes de chaque sous-projet de migration (visite de sites, raccordement, desserte interne, prise de rendez-vous, transfert de compétences, référencement des sites, référencement des services) ; ▪ Rédige un plan d'assurance qualité spécifique au projet de migration.	▪ Démarche projet et outils de *reporting* en place ; ▪ Plan de migration pour chaque lot ; ▪ Calendrier prévisionnel de migration ; ▪ Matrice de gestion des risques initiée ; ▪ Adaptation de la gouvernance du projet de migration ; ▪ PAQ du projet de migration.

2	**Préparation de la phase d'Assistance au pilotage des migrations** Le titulaire propose un dispositif, soumis à la validation de l'Administration, pour réaliser la phase d'assistance au pilotage des migrations. Ce dispositif s'adapte à la démarche de migration retenue, dont les données dépendent des points particuliers suivants : ▪ La migration de l'accord-cadre à renouveler vers le présent accord-cadre implique une multiplicité de partenaires : trois (3) titulaires sortants qui doivent potentiellement transférer leurs activités vers un nombre pouvant aller jusqu'à cinq (5) titulaires entrants durant la période de tuilage ; ▪ Les titulaires sortants restent pleinement responsables de leur exécution jusqu'à la fin de la période de tuilage de chaque marché à renouveler, évoluant vers un allotissement différent, à tout le moins concernant les services de chiffrement ; ▪ Compte tenu de la multiplicité des intervenants et du nombre des bénéficiaires, les titulaires centralisent leurs échanges avec la DINUM.	▪ Proposition du dispositif de la phase d'Assistance au pilotage des migrations

Eléments d'entrée
L'Administration n'identifie pas d'élément d'entrée particulier.
Engagement de service
Le cadrage est effectué dans un délai maximum de 20 jours ouvrés, avec la fourniture : ▪ De la démarche projet et de la mise en place des outils de *reporting* sous 10 jours ouvrés ; ▪ Du plan d'assurance qualité spécifique au projet de migration sous 10 jours ouvrés.
Outils du titulaire
Les éventuels outils informatiques du titulaire respectent la politique de sécurité et notamment les engagements relatifs aux portails clients, interfaces et développements spécifiques.
Unité d'œuvre associée
L'unité d'œuvre de cette prestation est un forfait.

{PP-L6/05} 4.6.2.1 Cadrage du projet de migration des sites : Description des moyens humains et organisationnels mis en œuvre en précisant notamment, les profils pressentis, les expériences dans ce type de projet de migration et les CV types.

{PP-L6/06} 4.6.2.1 Cadrage du projet de migration des sites : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre.

{PP-L6/07} 4.6.2.1 Cadrage du projet de migration des sites : Description d'un plan type du plan d'assurance qualité spécifique au projet de migration.

{PP-L6/08} 4.6.2.1 Cadrage du projet de migration des sites : Propositions pour compléter la démarche proposée.

4.6.2.2 Assistance au pilotage des migrations

<table>
<tr><th colspan="3">Définition globale de l'activité</th></tr>
<tr><td colspan="3">Le titulaire accompagne la DINUM dans le pilotage global de toutes les opérations de migration.
À ce titre, il assiste au pilotage la DINUM dans la coordination des différents titulaires concernés, le suivi et la maitrise des risques, le suivi des calendriers, la bonne mobilisation des parties prenantes, l'émission de toute alerte, etc.
Cette assistance couvre toute la période de migration, jusqu'à la fin de la vérification en service régulier (VSR) du dernier site déployé.</td></tr>
<tr><th colspan="3">Description générale de l'activité</th></tr>
<tr><th>Phases</th><th>Tâches</th><th>Livrables</th></tr>
<tr><td rowspan="2">1</td><td>Préparation, animation de la gouvernance spécifique à la migration</td><td rowspan="2">▪ Support des comités ;
▪ Comptes-rendus des comités</td></tr>
<tr><td>L'organisation de la gouvernance spécifique au projet de migration est définie lors du cadrage du projet de migration des sites.
Les comités spécifiques dédiés au projet de migration sont :
▪ Le Comité de pilotage de l'accord-cadre « COPIL » ;
▪ Le Comité de projet de déploiement « COPROJ ».
Le titulaire :
▪ Prépare les comités :
- Consolide les éléments fournis par les titulaires sortants et entrants relatifs à l'avancement des opérations de migration ;
- Présente l'état d'avancement par rapport au calendrier ;
- Ressence les difficultés rencontrées et les risques identifiés ainsi que les actions correctives proposées ;
- Elabore un tableau de bord par bénéficiaire ;
▪ Participe aux comités ;
▪ Rédige les comptes rendus des comités ;
▪ Coordonne le suivi des actions décidées lors des comités ;
▪ Propose à la DINUM l'organisation de toute réunion complémentaire, avec ou sans les titulaires concernés, qu'il estime nécessaire afin de garantir le bon déroulement des opérations de migration.</td></tr>
<tr><td>2</td><td>Suivi et coordination des projets de migration</td><td>▪ Tableau de suivi des</td></tr>
</table>

	En sa qualité d'assistant au pilotage du projet de migration, le titulaire : ▪ Est à l'interface entre : - Les titulaires des lots 1 à 5 et 7 ; - Le département ISO de la DINUM ; - Les bénéficiaires ; - Les titulaires sortants. ▪ Assiste la DINUM dans le suivi et la traçabilité de l'ensemble des actions des titulaires des lots 1 à 5, liées aux opérations de migration en temps réel et à la mise en place des points de concentration et de raccordement à l'épine dorsale RIE des passerelles Outre-Mer (POM) ; ▪ Coordonne la bonne réalisation des actions liées aux opérations de migration ; ▪ Fournit un tableau de bord de la phase de migration retraçant l'état d'avancement de tous les chantiers liés aux opérations de migration ; ▪ Fournit un *reporting* périodique et coordonne l'avancement des projets de migration bénéficiaire par bénéficiaire sur leur parc respectif ; ▪ Identifie et communique à la DINUM sans délai tout écart entre les actions réalisées au titre des opérations de migration et le plan de suivi et de maîtrise de la migration.	actions de la phase de migration ; ▪ Tableau d'avancement des opérations de migration ; ▪ Tableau de bord de la migration ; ▪ Fiche d'écart entre les actions réalisées et le plan de suivi et de maîtrise de la migration ; ▪ *Reporting* périodique aux bénéficiaires
3	**Focus sur l'assistance de la Phase 1 « Planification »** Le titulaire : ▪ Collecte les contraintes de planning des autres intervenants ; ▪ Propose une démarche et un plan d'action du projet de migration ; ▪ Elabore un planning global de migration consolidé ; ▪ Prépare, organise et participe aux réunions ; ▪ Rédige les comptes-rendus de réunion et suit leur validation ; ▪ Assure le suivi des actions identifiées lors des réunions.	▪ Planning global de migration consolidé ; ▪ Comptes-rendus préparés, rédigés et validés.

4	**Focus sur l'assistance de la Phase 2 « Etude »** Le titulaire : ▪ Prépare, organise et participe aux réunions ; ▪ Réalise des préconisations et cadre les cahiers de tests ; ▪ Assure le suivi d'exécution de la phase et le *reporting* ; ▪ Le cas échéant, assiste l'Administration pour expertiser/analyser les spécifications techniques des titulaires des lots 1 à 5 et 7 ; ▪ Rédige les comptes-rendus de réunion et suit leur validation ; ▪ Assure le suivi des actions identifiées lors des réunions.	▪ Préconisation sur les cahiers de tests ; ▪ Le cas échéant, rapport d'expertise ou d'analyse ; ▪ Comptes-rendus préparés, rédigés et validés.
5	**Focus sur l'assistance de la Phase 3 « Pilotes »** Le titulaire : ▪ Prépare, organise et participe aux réunions ; ▪ Assiste l'Administration à la réalisation des vérifications (recette) des sites pilotes dont le détail est décrit dans les activités du « Département ISO de la DINUM » de la Phase 3 « Pilotes » ; ▪ Assiste l'Administration pour consolider les remontées des résultats des vérifications d'aptitude et des vérifications de service régulier pour chaque bénéficiaire ; ▪ Informe les bénéficiaires de la date du début des abonnements des accès (les bénéficiaires se chargeant de résilier les abonnements de l'accord-cadre sortant) ; ▪ Calcule les éventuelles pénalités à appliquer aux titulaires des lots 1 à 5 et 7 et les transmet au service achat concerné ; ▪ Assure le suivi d'exécution de la phase et le *reporting* ; ▪ Le cas échéant, assiste l'Administration pour le transfert de compétences des outils mis à disposition par les titulaires des lots 1 à 5 et 7 ; ▪ Le cas échéant, assiste l'Administration pour expertiser/analyser les solutions mise en œuvre par les titulaires des lots 1 à 5 et 7 ; ▪ Rédige les comptes-rendus de réunion et suit leur validation ; ▪ Assure le suivi des actions identifiées lors des réunions.	▪ Documents préparatoires aux vérifications ; ▪ Cahiers de tests vérifiés des sites pilotes ; ▪ Cahiers de tests vérifiés de l'interopérabilité ; ▪ *Reporting* des activités ; ▪ Le cas échéant, rapport d'expertise ou d'analyse ; ▪ Comptes-rendus préparés, rédigés et validés.

6	**Focus sur l'assistance de la Phase 4 « Généralisation »** Le titulaire : ▪ Prépare, organise et participe aux réunions ; ▪ Assiste l'Administration à la réalisation des vérifications (recette) des sites bénéficiaires dont le détail est décrit dans les activités du « Département ISO de la DINUM » de la Phase 4 « Généralisation » ; ▪ Assiste l'Administration pour consolider les remontées des résultats des vérifications d'aptitude et des vérifications de service régulier pour chaque bénéficiaire ; ▪ Informe les bénéficiaires de la date du début des abonnements des accès (les bénéficiaires se chargeant de résilier les abonnements de l'accord-cadre sortant) ; ▪ Calcule les éventuelles pénalités à appliquer aux titulaires des lots 1 à 5 et 7 et les transmet au service achat concerné ; ▪ Assure le suivi d'exécution de la phase et le *reporting* ; ▪ Assiste l'Administration à la vérification des livrables documentaires des titulaires des lots 1 à 5 et 7, notamment : - Du Plan d'Assurance Qualité (PAQ) mis à jour ; - Du Plan d'Assurance Sécurité (PAS) mis à jour ; - Du Plan de Gestion et d'Amélioration continue (PGAC) mis à jour ; ▪ Le cas échéant, assiste l'Administration pour expertiser/analyser les solutions mise en œuvre par les titulaires des lots 1 à 5 et 7 ; ▪ Rédige les comptes-rendus de réunion et suit leur validation ; ▪ Assure le suivi des actions identifiées lors des réunions.	▪ Documents préparatoires aux vérifications ; ▪ Cahiers de tests vérifiés des sites des bénéficiaires ; ▪ Cahiers de tests vérifiés de l'interopérabilité ; ▪ *Reporting* des activités ; ▪ Le cas échéant, rapport d'expertise ou d'analyse ; ▪ Comptes-rendus préparés, rédigés et validés.

7	**Suivi des commandes** Pendant toute la phase de mise au point des échanges automatisés par API du lot 1 et 2, le titulaire, met à jour l'état d'avancement d'exécution du volet technique des commandes d'achat dans l'Extranet RIE ou autre portail de l'Administration. Par ailleurs, le titulaire suit la réalisation du processus de commande et formalise dans un tableau de bord : ▪ L'état d'avancement de chaque commande ; ▪ Les écarts constatés avec le calendrier et les délais fixés ; ▪ Les risques associés. Le titulaire remonte toute alerte au cas où une dérive est constatée sur le bon déroulement d'une commande. Le titulaire élabore un *reporting* à destination de chacun des bénéficiaires.	▪ Bilan des saisies dans l'Extranet RIE ou autre portail de l'Administration ; ▪ Tableau de bord du suivi de commandes.

Eléments d'entrée

L'Administration n'identifie pas d'élément d'entrée particulier.

Engagement de service

Les engagements de service sont les suivants :

- Pour la phase 1 « Préparation, animation de la gouvernance spécifique à la migration » :
  - Le délai de la fourniture du support de réunion des comités est au minimum 2 jours ouvrés avant la tenue de chaque réunion du comité ;
  - Le délai de la rédaction des **comptes-rendus des comités** est au **maximum de 2 jours ouvrés** après la tenue de chaque comité.
- Tout au long de la phase 2 « Suivi et coordination des projets de migration », la fourniture :
  - Hebdomadaire du tableau d'avancement des opérations de migration ;
  - Hebdomadaire du tableau de bord de la migration ;
  - Du *reporting* aux bénéficiaires selon une fréquence convenue avec les bénéficiaires.
- Tout au long de la phase 3 « Suivi des commandes », la fourniture :
  - Hebdomadaire du tableau de bord du suivi commandes ;
- Tout au long de la phase 4 « Finalisation de la migration d'un regroupement de sites », la fourniture :
  - Au fil de l'eau des prononcés des vérifications d'aptitude et des vérifications de service régulier ;
  - Dans un délai de 5 jours ouvrés, le bilan de fin de migration d'un regroupement de sites par bénéficiaire.

Outils du titulaire

Les éventuels outils informatiques du titulaire respectent la politique de sécurité et notamment les engagements relatifs aux portails clients, interfaces et développements spécifiques.

Unité d'œuvre associée

L'assistance au pilotage est un prix forfaitaire basé sur la décomposition des profils des intervenants du poste « II) Profils des prestations d'assistance au pilotage » du bordereau des prix unitaires.

Les profils concernés sont les profils de la norme CIGREF de l'annexe [A9] : « Nomenclature CIGREF des métiers du système d'information » associés à un niveau de qualification dans le poste. Ces profils sont :

- Directeur de projets ;
- Chef de projet maitrise d'ouvrage ;
- Chargé de pilotage SI (PMO) ;
- Architecte technique.

{PP-L6/09} 4.6.2.2 Assistance au pilotage des migrations : Propositions de l'organisation à mettre en œuvre, pour chacune des phases (Phase 1 « Planification », Phase 2 « Etude », Phase 3 « Pilotes » et Phase 4 « Généralisation ») en précisant les profils selon l'annexe [A9] « Nomenclature CIGREF des métiers du système d'information ».

Les propositions prennent en compte
- les quantités estimatives du nombre de sites à migrer,
- d'un calendrier de déploiement sur 18 mois,
- de ratio globaux selon les types de migration des sites, qui sont soit

* techniques en cas de changement de technologie et/ou de titulaire,
* administratives en cas de reconduction du titulaire sortant.

Les propositions d'organisation sont à réalisées pour les ratios suivants
- la migration des sites est une migration à 100% technique,
- la migration des sites est une migration à 75% technique et à 25% administrative,
- la migration des sites est une migration à 50% technique et à 50% administrative,
- la migration des sites est une migration à 25% technique et à 75% administrative.

{PP-L6/10} 4.6.2.2 Assistance au pilotage des migrations : Précisions sur les délais de mobilisation des profils mentionnés dans la réponse du point à préciser {PP-L6/09} en vue de respecter les délais de chacune des phases.

{PP-L6/11} 4.6.2.2 Assistance au pilotage des migrations : Focus sur les profils pressentis, pour assister l'Administration à l'expertise et/ ou l'analyser des spécifications techniques et des solutions mise en œuvre par les titulaires des lots 1 à 5, avec notamment leur niveau de qualification dans le poste et leurs expériences dans les projets de migration réseau.

{PP-L6/12} 4.6.2.2 Assistance au pilotage des migrations : Focus sur les profils pressentis, pour assister l'Administration à la préparation et la réalisation des vérifications (recette) des sites, avec notamment leur niveau de qualification dans le poste et leurs expériences dans les projets de migration réseau.

{PP-L6/13} 4.6.2.2 Assistance au pilotage des migrations : Proposition pour chaque autre type de profils pressentis, d'un échantillonnage des profils, avec notamment leur niveau de qualification dans le poste, leurs expériences dans l'assistance au pilotage des projets de migration réseau.

{PP-L6/14} 4.6.2.2 Assistance au pilotage des migrations : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre.

{PP-L6/15} 4.6.2.2 Assistance au pilotage des migrations : Propositions pour compléter la démarche proposée.

{PP-L6/16} 4.6.2.2 Assistance au pilotage des migrations : Exemples de tableaux de bord avec des explications sur les éléments complémentaires.

{PP-L6/17} 4.6.2.2 Assistance au pilotage des migrations : Précisions sur la fourniture d'outils de restitution des tableaux de bord et du suivi du projet de migration.

{PP-L6/18} 4.6.2.2 Assistance au pilotage des migrations : Proposition d'outils de collecte des indicateurs de gouvernance pour les titulaires des lots 1 à 5.

4.6.3 Pilotage lors de la phase opérationnelle du service

Définition globale de l'activité		
Le pilotage opérationnel du service débute dès la fin de migration du premier site. Le titulaire accompagne la DINUM dans le pilotage global pour la gestion lors de la phase d'exploitation du réseau post-migration et pendant toute la durée de l'accord-cadre. À ce titre, il assiste la DINUM au pilotage tout particulièrement dans la gouvernance de l'accord-cadre et la coordination des grands chantiers.		
Description générale de l'activité		
Phases	**Tâches**	**Livrables**
1	**Préparation, animation de la gouvernance de l'accord-cadre**	▪ Support des réunions

	Le titulaire organise et participe à l'ensemble des comités liés à la gouvernance de l'accord-cadre. Pour chacun de ces comités, le titulaire : ▪ Prépare les réunions de comités : - Consolide les éléments fournis par les titulaires des lots 1 à 5 et 7 dont le détail est précisé dans la description des comités ; - Ressence les difficultés rencontrées et les risques identifiés ainsi que les actions correctives proposées ; ▪ Participe aux comités ; ▪ Rédige les comptes rendus des réunions de comités ; ▪ Coordonne le suivi des actions décidées par les comités ; ▪ Propose à la DINUM l'organisation de toute réunion complémentaire, avec ou sans les titulaires concernés, qu'il estime nécessaire afin de garantir le bon déroulement des opérations de migration.	de comités ; ▪ Comptes-rendus des réunions de comités
2	**Fourniture des tableaux de bord** Le titulaire fournit des rapports opérationnels mensuels sous forme de tableaux de bord (au format PDF et XLS) pour les inventaires, incluant, au moins, les éléments ci-dessous : ▪ La synthèse des éléments marquants du mois précédent ; ▪ L'inventaire des services activés pour chaque accès, comprenant : - La référence de l'accès, son adresse et le numéro de désignation d'installation (NDI) le cas échéant ; - Le titulaire et le lot concerné ; - Le type de lien (niveau de service, bande passante et éventuellement l'infrastructure de sécurisation et le profil de CoS) ; - Le modèle d'équipement d'extrémité. ▪ Les modifications, de configuration et d'architecture, réalisées sur le réseau ; ▪ La liste des équipements d'extrémités dont le taux de charge CPU moyen devient critique ; ▪ La liste des liens dont le taux de charge moyen dépasse les 75% durant les heures ouvrées (mesure au 95e centile) ; ▪ LA liste des liens dont le taux de charge moyen est en dessous de 30% durant les heures ouvrées, ▪ Une analyse des taux de charges CPU et débits,	▪ Tableau de bord

	accompagnée de recommandations ; ▪ Les débits consommés à travers le service du titulaire Le titulaire organise et participe à l'ensemble des comités liés à la gouvernance de l'accord-cadre. Pour chacun de ces comités, le titulaire fournit : ▪ Les éléments de métrologie sur l'utilisation des services ; ▪ Le tableau de suivi des engagements contractuels et un graphique reprenant l'historique sur 6 mois glissants : - Indicateurs de qualité de service sur le réseau ; - Taux de disponibilité mensuel ; - Respect des temps de rétablissement ; - Temps de transit, gigue et taux de perte de paquet, ▪ Le calcul des pénalités ; ▪ Le rapport des incidents survenus et des problèmes en cours d'investigations ; ▪ Un graphique reprenant l'historique du volume mensuel d'incidents ouverts durant le mois, fermés durant le mois et le nombre total d'incidents restants ouverts au dernier jour du mois sur 6 mois glissants ; ▪ Les informations sur les opérations planifiées du mois à venir ; ▪ Les informations sur les commandes, évolutions et demandes en cours ; ▪ L'évolution du parc sur la période concernée (ajout d'accès…), ▪ L'évolution de l'état d'éligibilité des sites aux nouveaux supports (xDSL, FO…).	
3	**Suivi et coordination des projets de raccordements de sites post-migration**	▪ Tableau de bord du

	En sa qualité d'assistant au pilotage, le titulaire : ▪ Est à l'interface entre : - Les titulaires des lots 1 à 5 et 7 ; - Le département ISO de la DINUM ; - Les bénéficiaires ; - Les titulaires sortants. ▪ Assiste la DINUM dans le suivi et la traçabilité de l'ensemble des actions liées aux opérations du projet de raccordement des sites post-migration en temps réel ; ▪ Coordonne la bonne réalisation des actions liées aux opérations de raccordement ; ▪ Fournit un tableau de bord du projet de raccordement des sites post-migration ; ▪ Fournit un *reporting* périodique et la coordination de l'avancement du projet de raccordement des sites post-migration. ▪ Assiste l'Administration pour consolider les remontés des résultats des vérifications d'aptitude et des vérifications de service régulier pour chaque bénéficiaire ; ▪ Calcule les éventuelles pénalités à appliquer aux titulaires des lots 1 à 5 et 7 et les transmet au service achat concerné.	projet de raccordement des sites post-migration ; ▪ *Reporting* périodique aux bénéficiaires ; ▪ Bilan de fin du projet de raccordement des sites post-migration par bénéficiaire.
4	**Assistance aux vérifications du déploiement des sites post-migration** Le titulaire : ▪ Assiste techniquement l'Administration pour la préparation, la définition et l'exécution des opérations de vérification ; ▪ Assiste l'Administration pour consolider les remontés des résultats des vérifications d'aptitude et des vérifications de service régulier pour chaque bénéficiaire ; ▪ Informe les bénéficiaires de la date du début des abonnements des accès ; ▪ Calcule les éventuelles pénalités à appliquer aux titulaires des lots 1 à 5 et 7 et les transmet au service achat concerné.	▪ Documents préparatoires aux vérifications ; ▪ Bilan de fin de déploiement par bénéficiaire.

5	**Assistance à l'analyse ou l'expertise technique** Le titulaire : ▪ Le cas échéant, assiste l'Administration pour expertiser/analyser les spécifications techniques des titulaires des lots 1 à 5 et 7 ; ▪ Le cas échéant, assiste l'Administration pour expertiser/analyser les solutions proposées par les titulaires des lots 1 à 5 et 7 ; ▪ Le cas échéant, participe à des réunions techniques et rédige les comptes-rendus de réunion et suit leur validation ; ▪ Assure le suivi des actions identifiées lors des réunions.	▪ Le cas échéant, rapport d'expertise ou d'analyse ; ▪ Le cas échéant, compte rendu de réunion.

Eléments d'entrée

L'Administration n'identifie pas d'élément d'entrée particulier.

Engagement de service

Les engagements de service sont les suivants :

- Pour la phase 1 « Préparation, animation de la gouvernance spécifique à la migration » :
  - Le délai de la fourniture du support de réunion des comités est au minimum 2 jours ouvrés avant la tenue de chaque comité ;
  - Le délai de la rédaction des comptes-rendus de réunions des comités est au maximum de 2 jours ouvrés après la tenue de chaque comité.
- Pour la phase 2 « Fourniture des tableaux de bord » :
  - Les tableaux de bord consolidés le 10 de chaque mois ;
- Tout au long de la phase 3 « Suivi et coordination des projets de raccordements de sites post-migration », la fourniture :
  - Hebdomadaire du tableau de bord des projets de raccordement des sites post-migration ;
  - Du *reporting* aux bénéficiaires selon une fréquence convenue avec les bénéficiaires.
  - Au fil de l'eau des prononcés des vérifications d'aptitude et des vérifications de service régulier.

Outils du titulaire

Les éventuels outils informatiques du titulaire respectent la politique de sécurité et notamment les engagements relatifs aux portails clients, interfaces et développements spécifiques.

Unité d'œuvre associée
L'assistance au pilotage est un prix forfaitaire basé sur la décomposition des profils des intervenants du poste « II) Profils des prestations d'assistance au pilotage » du bordereau des prix unitaires. Les profils concernés sont les profils de la norme CIGREF de l'annexe [A9] : « Nomenclature CIGREF des métiers du système d'information » associés à un niveau de qualification dans le poste. Ces profils sont : ▪ Directeur de projets ; ▪ Chef de projet maitrise d'ouvrage ; ▪ Chargé de pilotage SI (PMO) ; ▪ Architecte technique.

{PP-L6/19} 4.6.3 Pilotage lors de la phase opérationnelle du service : Présentation des hypothèses de dimensionnement des moyens humains et organisationnels à mettre en œuvre pour l'assistance au pilotage des quantités estimatives de sites du chapitre 2.2.

{PP-L6/20} 4.6.3 Pilotage lors de la phase opérationnelle du service : Précisions sur les délais de mobilisation des profils mentionnés dans la réponse du point à préciser {PP-L6/19}.

{PP-L6/21} 4.6.3 Pilotage lors de la phase opérationnelle du service : Focus sur les profils pressentis, pour assister l'Administration à l'expertise et/ou l'analyser des spécifications techniques et des solutions proposées par les titulaires des lots 1 à 5 et 7, avec notamment leur niveau de qualification dans le poste et leurs expériences dans les projets d'infrastructure réseau.

{PP-L6/22} 4.6.3 Pilotage lors de la phase opérationnelle du service : Précisions sur les délais de mobilisation des profils mentionnés dans la réponse du point à préciser {PP-L6/21}.

{PP-L6/23} 4.6.3 Pilotage lors de la phase opérationnelle du service : Focus sur les profils pressentis, pour assister l'Administration à la préparation et la réalisation des vérifications (recette) des sites, avec notamment leur niveau de qualification dans le poste et leurs expériences dans les projets d'infrastructure réseau.

{PP-L6/24} 4.6.3 Pilotage lors de la phase opérationnelle du service : Précisions sur les délais de mobilisation des profils mentionnés dans la réponse du point à préciser {PP-L6/23}.

{PP-L6/25} 4.6.3 Pilotage lors de la phase opérationnelle du service : Proposition pour chaque autre type de profils pressentis, d'un échantillonnage des profils, avec notamment leur niveau de qualification dans le poste, leurs expériences dans l'assistance au pilotage opérationnel des réseaux.

{PP-L6/26} 4.6.3 Pilotage lors de la phase opérationnelle du service : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre.

{PP-L6/27} 4.6.3 Pilotage lors de la phase opérationnelle du service : Propositions pour compléter la démarche proposée.

{PP-L6/28} 4.6.3 Pilotage lors de la phase opérationnelle du service : Propositions pour compléter le tableau de bord avec un exemple pour illustrer le tableau de bord et des explications sur les éléments complémentaires.

{PP-L6/29} 4.6.3 Pilotage lors de la phase opérationnelle du service : Précisions sur la fourniture d'outils de restitution des tableaux de bord et du suivi du pilotage.

{PP-L6/30} 4.6.3 Pilotage lors de la phase opérationnelle du service : Proposition d'outils de collecte des indicateurs de gouvernance pour les titulaires des lots 1 à 5 et 7.

4.7 Prestations d'entrée

4.7.1 Initialisation de l'accord-cadre

<table>
<tr><th colspan="3">Définition globale de l'activité</th></tr>
<tr><td colspan="3">L'initialisation de l'accord-cadre a pour objectif :
De mettre en place et d'initialiser les outils de pilotage et de suivi, en particulier le plan d'assurance qualité de l'accord-cadre (PAQ accord-cadre) ;
De mettre en œuvre la gouvernance de l'accord-cadre ;
De mettre en œuvre le reporting des activités liées aux services.</td></tr>
<tr><th colspan="3">Description générale de l'activité</th></tr>
<tr><th>Phase</th><th>Tâches</th><th>Livrables</th></tr>
<tr><td rowspan="2">1</td><td>Préparer l'Initialisation</td><td rowspan="2">Plan d'actions ;
Planning ;
Compte rendu des réunions.</td></tr>
<tr><td>Pour chacun des 6 lots, le titulaire :
Organise la réunion de lancement avec l'Administration et, le cas échéant, fait participer le titulaire du Lot 6 ;
Définit le plan d'actions précis de cette prestation d'initialisation avec le planning associé.</td></tr>
<tr><td rowspan="2">2</td><td>Mettre en œuvre le portail client</td><td rowspan="2">Portail client opérationnel.</td></tr>
<tr><td>Dans l'attente de la mise au point des échanges automatisés par API du lot 1,2 et pour les lots 3, 4, 5 et 7, le titulaire met en œuvre son portail client de :
Gestion de parc ;
Gestion des incidents ;
Gestion du volet technique des commandes.</td></tr>
<tr><td>3</td><td>Mettre en œuvre le cadre organisationnel</td><td>Modalités des échanges</td></tr>
</table>

	Dans le respect des modalités de la gouvernance de l'accord-cadre, le titulaire de chacun des 6 lots, et le cas échéant pour les lots 1 à 5 et 7 conjointement avec le titulaire du lot 6, définit et met en œuvre les modalités d'échanges : ▪ Pour la préparation des réunions des comités de la gouvernance de l'accord-cadre ; ▪ Pour le *reporting* des activités liées aux services. En cas de désaccord entre différents titulaires, l'Administration définit les modalités de gouvernance et de *reporting* de l'accord-cadre.	mises en œuvre.
4	**Rédiger les différents plans de l'accord-cadre : PAQ, PGAC et PAS** Chaque titulaire : ▪ Rédige le Plan d'assurance sécurité (PAS) de son périmètre ; ▪ Elabore le Plan d'assurance qualité de l'accord-cadre (PAQ) de son périmètre ; ▪ Elabore le Plan de gestion et d'amélioration continue (PGAC) de son périmètre ; ▪ Propose le modèle de tableau de bord de suivi des services de son périmètre et en accord avec des indicateurs de services définis.	▪ PAQ Accord-cadre ; ▪ PGAC Accord-cadre ; ▪ Modèle de tableau de bord et indicateurs de services ; ▪ Plan d'Assurance Sécurité.

Engagement de service
Les engagements sur la fourniture des livrables sont mentionnés au chapitre » Engagements sur les prestations d'entrée ».
Outils du titulaire
Les éventuels outils informatiques du titulaire respectent la politique de sécurité et notamment les engagements relatifs aux portails clients, interfaces et développements spécifiques.
Unité d'œuvre associée
L'unité d'œuvre de cette prestation est un forfait.

{PP-L1 à 7/06}. 4.7.1 Initialisation de l'accord-cadre : Exemple de planning d'initialisation en précisant le nombre et la nature des ateliers à réaliser avec l'Administration et/ou son assistant à maîtrise d'ouvrage.

{PP-L1 à 7/07}. 4.7.1 Initialisation de l'accord-cadre : Description des moyens humains et organisationnels mis en œuvre en précisant notamment, les profils pressentis, les expériences dans ce type de projet de migration et les CV types.

4.7.2 Cadrage du projet de migration des sites

Définition globale de l'activité

Le cadrage du projet de migration débute dès la notification de l'accord-cadre. Ce cadrage a pour objectif :

- De préparer le projet de migration au cours duquel, le titulaire de chacun des lots 1 à 5 et 7 élabore notamment un plan de migration détaillé en collaboration avec l'Administration et le cas échéant son assistant à maîtrise d'ouvrage, titulaire du Lot 6 ;
- De répondre aux sollicitations de l'Administration et le cas échéant son assistant à maîtrise d'ouvrage pour vérifier l'éligibilité des sites des bénéficiaires ;
- De concevoir les spécifications techniques.

Description générale de l'activité

Phase	Tâches	Livrables
1	**Préparation des différents projets de migration** L'objet de cette phase est de mettre en place les conditions préalables nécessaires à la réalisation effective des migrations des différents accès de l'Administration. A cet effet, le titulaire, y compris celui du Lot 6 : ▪ Répond aux sollicitations de l'Administration ou de son assistant à maîtrise d'ouvrage, pour vérifier les éligibilités de certains sites des bénéficiaires (à noter que certains types d'accès de l'accord-cadre à renouveler ont été supprimés) ; ▪ De manière générale, apporte toute l'assistance pour la préparation des commandes des bénéficiaires ; ▪ Participe à l'élaboration du plan de migration de son périmètre avec l'Administration ou de son assistant à maîtrise d'ouvrage ; ▪ Remonte les risques identifiés ; ▪ Participe à l'élaboration d'un calendrier prévisionnel, en accord avec les bénéficiaires et l'Administration ou de son assistant à maîtrise d'ouvrage ; ▪ Rédige un plan d'assurance qualité spécifique au projet de migration de son périmètre.	▪ Plan de migration pour chaque site existant ; ▪ Calendrier prévisionnel de migration ; ▪ Matrice de gestion des risques initiée ; ▪ Adaptation de la gouvernance du projet de migration ; ▪ PAQ du projet de migration.
2	**Elaboration des spécifications techniques** Le titulaire produit un Document d'Architecture Technique (DAT) qu'il met à jour tout au long de la vie de l'accord-cadre. En particulier, le titulaire du Lot 6 s'assure de la cohérence et de la complétude de l'ensemble des DAT établis par les titulaires des autres lots et produit la version intégrée d'un DAT global.	▪ DAT.

Engagement de service

Le cadrage est effectué dans un délai maximum de 20 jours ouvrés avec la fourniture du plan d'assurance qualité spécifique au projet de migration sous 10 jours ouvrés.

Outils du titulaire
Les éventuels outils informatiques du titulaire respectent la politique de sécurité et notamment les engagements relatifs aux portails clients, interfaces et développements spécifiques.
Unité d'œuvre associée
L'unité d'œuvre de cette prestation est un forfait.

{PP-L1 à 7/08}. 4.7.2 Cadrage du projet de migration des sites : Description des moyens humains et organisationnels mis en œuvre en précisant notamment, les profils pressentis, les expériences dans ce type de projet de migration et les CV types.

{PP-L1 à 7/09}. 4.7.2 Cadrage du projet de migration des sites : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre.

{PP-L1 à 7/10}. 4.7.2 Cadrage du projet de migration des sites : Description d'un plan type du plan d'assurance qualité spécifique au projet de migration.

{PP-L1 à 7/11}. 4.7.2 Cadrage du projet de migration des sites : Propositions pour compléter la démarche proposée.

4.7.3 Echanges automatisés des Lot 1 et 2

L'Administration souhaite automatiser autant que possible les échanges entre son Système d'Information (SI RIE) et celui du titulaire afin de pouvoir industrialiser l'ensemble des processus mis en œuvre, et notamment en matière de gestion des changements et de gestion des incidents.

Dans tous les cas d'échanges automatisés entre le SI de l'Administration et celui du titulaire, les clés utilisées doivent être celles du référentiel de l'Administration (numéro de commande RIE, code d'accès RIE, nom de l'équipement…) ;

Dans cette optique, deux principales solutions sont retenues :

- Echange par interfaces de programmation applicative (API) ;
- Echange par flux sécurisés Machine à Machine (M2M)

4.7.3.1 Echange par API

4.7.3.1.1 Couverture fonctionnelle des API

Le premier format d'échange retenu est celui des API (interfaces de programmation applicative) qui doit permettre de couvrir la plupart des échanges avec les titulaires liés à l'exploitation courante du réseau. Ces échanges par API automatisés concernent notamment :

- La gestion des commandes d'achat (volet technique)[1] : création d'accès et de liens, évolutions majeures[2] et mineures[3], résiliations et suivi des projets en cours de production par le titulaire ;
- La gestion des configurations techniques des équipements du réseau (consultation, modification) à l'initiative de l'Administration ;
- La gestion des Travaux Programmés (création / modification / suppression) envoyés ou reçus par API ;
- La gestion des incidents[4] (création de ticket d'incident, modification, suivi et clôture).

Ces APIs doivent être documentées en respectant le format d'OpenAPI et doivent être accompagnées d'une documentation permettant leur usage dans le contexte du RIE.

Les fonctionnalités automatisées par API (ou saisie en mode dégradé sur le Portail client type « web ») sont commandées, à la survenance du besoin, **une seule fois**, à l'aide des unités d'œuvre du poste « I-c) Echanges automatisés par API » suivantes :

- « Echanges automatisés par API des fonctions minimales » pour les fonctionnalités minimales ;
- « Echanges automatisés par API des fonctions complémentaires » pour les fonctionnalités complémentaires décrites dans l'offre du titulaire.

Durant l'accord-cadre, des fonctionnalités supplémentaires aux fonctionnalités minimales et complémentaires dont l'objectif est de fluidifier les échanges au profit commun de l'ensemble des parties prenantes, sont susceptibles d'être ajoutées.

L'Administration ne prévoit pas, pour la mise en œuvre de ces fonctionnalités supplémentaires, de rétribution particulière.

4.7.3.1.2 Modalités de mise en œuvre des API

L'objectif de l'Administration est d'automatiser progressivement ces échanges selon un délai maximum mentionné au chapitre relatif aux engagements sur les prestations d'entrée.

Dans l'attente de l'automatisation des échanges par API, le titulaire met en œuvre un Portail client type « Web » permettant de réaliser la saisie des échanges « manuellement ».

---

[1] *Cf. chapitre 4.1 : « Passation des commandes d'achat »*
[2] *Cf. chapitre 4.10.2 : « Gestion des évolutions majeures »*
[3] *Cf. chapitre 4.10.3 : « Gestion des évolutions mineures »*
[4] *Cf. chapitre 4.11 : « Gestion des incidents »*

Ce Portail client du titulaire peut être également utilisé dans un mode « secours » en cas d'indisponibilité du système d'échange automatisé par API :

- Dans le cadre d'une maintenance programmée conjointement avec l'Administration ;
- D'un dysfonctionnement et en attendant son rétablissement.

{PP-L1 & 2/24} 4.7.3.1.2 Modalités de mise en œuvre des API : Description du macro-planning de déploiement de la mise en œuvre progressive des échanges automatisés des fonctionnalités minimales et complémentaires.

{PP-L1 & 2/25} 4.7.3.1.2 Modalités de mise en œuvre des API : Description du macro-planning de déploiement de la mise en œuvre « immédiate » du portail client type « Web » des fonctionnalités minimales et complémentaires.

4.7.3.2 Echange par flux sécurisés Machine à Machine

Dans le cas où une API ne n'est pas disponible ou pas opportune, il peut être envisagé de récupérer un flux d'information grâce à un transfert machine à machine (type *sftp*).

Dans ce cas la fréquence des transferts et les spécifications détaillées contenant les règles de nommage et la structure du format d'échange sont réalisées conjointement entre le titulaire et l'Administration.

4.7.3.3 Sécurisation des échanges automatisés inter-SI

L'interconnexion des systèmes se fait par la mise en place par le titulaire de deux liens sécurisés fonctionnant en mode normal/secours pour véhiculer les flux d'échange à travers un VPN dédié aboutissant à deux des points de concentration de l'épine dorsale RIE.

{PP-L1 & 2/26} 4.7.3.3 Sécurisation des échanges automatisés : Description de l'interconnexion sécurisée entre le SI-RIE de l'Administration et le système d'information du titulaire.

4.7.3.4 Echanges automatisés du volet technique des commandes d'achat

La liste minimale des fonctionnalités du volet technique des commandes d'achat, à mettre en œuvre via des API automatisées ou saisie en mode dégradé sur le Portail client type « web » du titulaire est :

- Une demande d'éligibilité en vue de la passation d'une commande d'achat d'accès ;
- Une demande de l'état du parc (commandé et en service) ;

- Une création, modification, consultation et annulation d'une commande d'achat d'accès ;
- Une résiliation d'un accès ;
- Le suivi de l'état d'une commande d'achat ;
- La fourniture de liste de commandes d'achat par statut.

{PP-L1 & 2/27} 4.7.3.4 Echanges automatisés du volet technique des commandes d'achat : Présentation des fonctionnalités automatisées par API minimales attendues.

{PP-L1 & 2/28} 4.7.3.4 Echanges automatisés du volet technique des commandes d'achat : Présentation des fonctionnalités automatisées par API complémentaires.

{PP-L1 & 2/29} 4.7.3.4 Echanges automatisés du volet technique des commandes d'achat : Présentation des fonctionnalités minimales attendues du Portail client type « web ».

{PP-L1 & 2/30} 4.7.3.4 Echanges automatisés du volet technique des commandes d'achat : Présentation des fonctionnalités complémentaires du Portail client type « web ».

Les informations et notifications remontées du titulaire vers l'Administration, se font par messagerie électronique automatique aux adresses indiquées par l'Administration.

En complément du code RIE, les informations à remonter sont décrites dans l'annexe [A2] : « Fichier de Commande RIE type ».

Les informations et notifications remontées concernent :

- L'accusé de réception d'une nouvelle commande d'achat ou de sa mise à jour en indiquant :
  - La bonne prise en compte de la commande d'achat ;
  - La référence et l'horodatage du ticket de la commande d'achat ;
- Les notifications de création ou de mise à jour des commandes d'achat ;
- La notification immédiate au département ISO de la DINUM du gel de la production d'une commande d'achat en précisant sa raison et sa motivation ;
- L'envoi systématique des avis d'ouverture et de fermeture des commandes d'achat sous un format brut et respectueux des standards d'échange définis par l'Administration.
- A la mise en service de l'accès, le titulaire transmet un Procès-Verbal au format électronique, PV dont les éléments permettront à l'Administration de vérifier de manière industrielle la conformité entre la commande et le service mis en œuvre par le titulaire.

4.7.3.5 Echanges automatisés de la gestion des incidents et de travaux programmés

La liste minimale des fonctionnalités de la gestion des incidents, à mettre en œuvre via des API automatisées ou saisies en mode dégradé sur le Portail client type « web » du titulaire, permet :

- De déclarer de nouveaux incidents ;
- De déclarer des travaux ou des opérations planifiées ;
- De mettre à jour et consulter le suivi des incidents ouverts : commentaires, changements de statut, niveau d'escalade, temps de gel, temps de résolution… ;
- De consulter la traçabilité des contacts effectués et des interventions sur site ou à distance pour la résolution des incidents ;
- De fermer un incident ;
- De consulter un incident ou des travaux ou opérations planifiées des trois derniers mois ;
- De consulter l'état du parc ;
- De lister les incidents en pouvant filtrer sur n'importe quel attribut d'un incident (statut, durée de gel, durée de résolution…)

Les informations et notifications remontées du titulaire vers l'Administration, se font par messagerie électronique automatique aux adresses indiquées par l'Administration. Cela concerne :

- L'accusé de réception d'un nouvel incident ou de sa mise à jour en indiquant :
  - La bonne prise en compte de l'incident ; pour les incidents déclarés par téléphone ou par messagerie, le délai d'accusé réception maximum est de 15 minutes ;
  - La référence et l'horodatage du ticket de la commande ;
- Les notifications de création ou de sa mise à jour des incidents ;
- Les notifications de création ou de sa mise à jour des travaux ou opérations planifiées ;
- La notification immédiate au département ISO du gel d'un incident en précisant sa raison et sa motivation ;
- L'envoi systématique des avis d'ouverture et de fermeture des incidents sous un format brut et respectueux des standards d'échange définis par l'Administration.

{PP-L1 & 2/31} 4.7.3.5 Echanges automatisés de la gestion des incidents : Présentation des fonctionnalités automatisées par API minimales attendues.

{PP-L1 & 2/32} 4.7.3.5 Echanges automatisés de la gestion des incidents : Présentation des fonctionnalités automatisées par API complémentaires.

{PP-L1 & 2/33} 4.7.3.5 Echanges automatisés de la gestion des incidents : Focus sur les fonctionnalités liées à la remonté de manière automatisée par API des informations et alertes de supervision.

{PP-L1 & 2/34} 4.7.3.5 Echanges automatisés de la gestion des incidents : Focus sur les fonctionnalités liées à la remonté de manière automatisée par API des indicateurs quotidiens, hebdomadaires, bimensuels et mensuels.

{PP-L1 & 2/35} 4.7.3.5 Echanges automatisés de la gestion des incidents : Présentation des fonctionnalités minimales attendues du Portail client type « web ».

{PP-L1 & 2/36} 4.7.3.5 Echanges automatisés de la gestion des incidents : Présentation des fonctionnalités complémentaires du Portail client type « web ».

{PP-L1 & 2/37} 4.7.3.5 Echanges automatisés de la gestion des incidents : Focus sur les fonctionnalités liées à la remonté de manière automatisée par API de la supervision et de l'exploitation des flux des points de concentration des portes de collecte opérateur.

4.7.3.6 Echanges automatisés de la gestion des configurations des équipements d'extrémité

Dès la création d'un accès et quel que soit l'origine des changements intervenants sur un équipement du réseau, le titulaire met à disposition de l'Administration la configuration des équipements d'extrémité.

La mise en œuvre de cet échange pour l'obtention des configurations complètes et commentées sous un format texte brut (avec un obscurcissement possible des secrets de configuration dont la liste est préalablement convenue entre le titulaire et l'Administration) permet :

- De consulter à tout instant les configurations des équipements d'extrémité mis à disposition de l'Administration et reflétant l'état effectif des équipements d'extrémité du réseau ;
- De consulter l'état du parc des équipements d'extrémité.

{PP-L1 & 2/38} 4.7.3.6 Echanges automatisés de la gestion des configurations des équipements d'extrémité : Présentation des fonctionnalités minimales attendues automatisées par API avec leur calendrier de mise en œuvre.

{PP-L1 & 2/39} 4.7.3.6 Echanges automatisés de la gestion des configurations des équipements d'extrémité : Présentation des fonctionnalités complémentaires automatisées par API avec leur calendrier de mise en œuvre.

4.8 Migration des services

La migration ou déploiement initial constitue un projet à part entière, et nécessite la mise en place d'une démarche projet spécifique avec la mobilisation des mêmes comités que ceux déployés dans le cadre du déploiement de liens à grande échelle.

Pour information, la liste prévisionnelle des sites à migrer est donnée dans l'annexe [A1] : « Liste prévisionnelle des sites des bénéficiaires ».

Les délais de la migration sont mentionnés au chapitre relatif aux engagements sur les prestations d'entrée.

La chronologie, du lancement des actions et des commandes associées, est la suivante :

- Dès la notification des accords-cadres (lot 1 à 5 et 7), la DINUM, passe les commandes suivantes :
  - Initialisation des accords-cadres ;
  - Cadrage du projet de migration des sites ;
  - Rattachement aux points de concentration de collecte, porte de collecte opérateur, déploiement du la plateforme de livraison de service du transit sécurisé transocéanique, y compris pour les lots 3, 4 et 5, l'interconnexion à l'épine dorsale du RIE en Hexagone ;
  - Installation des nouveaux accès du Lot 7 (S-P&M)
  - Réalisation des échanges automatisés par API du lot 1 et 2 ;
- Dès que les commandes de migration des sites des bénéficiaires sont prêtes :
  - Le cas échéant, la DINUM commande au titulaire du Lot 6 l'assistance au pilotage des migrations permettant de suivre la migration des sites des bénéficiaires ;
  - Les bénéficiaires émettent leurs commandes respectives auprès de la DINUM qui transmet aux titulaires des Lots 1 et 2 après enregistrement dans le SI-RIE.
- La notification des commandes concrétise le lancement de la migration des sites dont les phases sont :

Phase	Objectif
Phase 1 « Planification »	Aboutir à une démarche de migration balisée par lot avec un plan d'actions de migration assorti d'un calendrier global de réalisation
Phase 2 « Etude »	▪ Réaliser le maquettage des infrastructures ; ▪ Concevoir l'ensemble des études techniques
Phase 3 « Pilotes »	▪ Tester et vérifier par l'Administration, sur un nombre restreint d'accès désignés dont en particulier, pour les lots 1 à 5 et 7, l'interconnexion à l'épine dorsale du RIE, l'architecture, le dimensionnement, les processus de déploiement. ▪ Réaliser les ajustements techniques et organisationnels nécessaires à la Phase 4 » Généralisation » ▪ Mettre en place l'exploitation du service dès le début de la phase de généralisation pour les accès migrés
Phase 4 « Généralisation »	▪ Construire l'ensemble des accès de façon regroupé. ▪ Tester et vérifier le déploiement de l'ensemble des sites par l'Administration.

{EX-L1 à 5 & 7/04}. 4.8 Migration des services : L'impact de la migration doit être maîtrisé sur les services réseaux fournis à l'utilisateur final, avec l'objectif d'éviter, à défaut de minimiser, les interruptions de service.

4.8.1 Phase 1 « Planification »

Phase 1 « Planification »	
Objectifs	
Les objectifs de cette phase sont d'aboutir à une démarche de migration balisée par lot avec un plan d'actions de migration assorti d'un calendrier global de réalisation.	
Prérequis	
Les prérequis de la phase sont la réalisation préalable : ▪ Accord-cadre initialisé ; ▪ Projet de migration des sites cadré ; ▪ Commandes émises par les bénéficiaires désignant la liste des sites à migrer.	
Activités à réaliser	
Acteur	**Activité**
Bénéficiaires demandeurs	▪ Emettent leur bon de commande en précisant la liste des sites à migrer ; ▪ Indiquent les contacts à mobiliser par bénéficiaires ; ▪ Précisent leurs contraintes calendaires ; ▪ Valident le plan d'action et le planning général pour leur périmètre respectif ; ▪ Décrivent les spécifications techniques des accès des sites à migrer.
Départemen	▪ Pilote le projet ;

Phase 1 « Planification »	
t ISO de la DINUM	▪ Valide le plan d'action et le planning général ; ▪ Communique les prérequis nécessaires à la migration ; ▪ Dresse la démarche et le plan d'action du projet de migration ;
Pour chaque titulaire des lots 1 à 5	Les activités à réaliser sont : ▪ Vérifie les prérequis nécessaires à la migration ; ▪ Définit son organisation du projet de migration en lien avec les autres intervenants ; ▪ Identifie les différentes actions à réaliser dans le cadre de la migration ; ▪ Met en œuvre la démarche et le plan d'action de migration ; ▪ Elabore un planning de migration en prenant en compte les contraintes des autres intervenants ; ▪ Réalise l'analyse des risques critérisés et avec les mitigations associées. Les livrables sont : ▪ Plan d'actions de migration décliné par regroupement de sites à migrer ; ▪ Calendrier global de réalisation organisé par regroupement de sites à migrer ; ▪ Tableau de gestion des risques ; ▪ Plan d'Assurance Qualité (PAQ) mis à jour ; ▪ Plan d'Assurance Sécurité (PAS) mis à jour.
Modalités d'exécution	
Les modalités d'exécution sont : ▪ Des réunions de travail avec l'ensemble des parties prenantes ; ▪ Le cadrage logistique et la planification des réunions par l'Administration ou, le cas échéant le titulaire du lot 6.	
Engagement de service	
Le délai de réalisation de cette phase est mentionné au chapitre relatif aux engagements sur les prestations d'entrée. Les engagements sur la fourniture des éléments et des comptes rendus sont mentionnés au chapitre relatif aux engagements sur la gouvernance de l'accord cadre.	

{PP-L1 à 7/12}. 4.8.1 Phase 1 « Planification » : Proposition d'une démarche de migration complémentaire et du plan d'action associé en indiquant les principaux jalons associés.

{PP-L1 à 7/13}. 4.8.1 Phase 1 « Planification » : Description des moyens humains et organisationnels mise en œuvre pour garantir la tenue des délais de cette phase.

{PP-L1 à 7/14}. 4.8.1 Phase 1 « Planification » : Précision et justification d'éventuelles prérequis nécessaires à la phase.

4.8.2 Phase 2 « Etude »

<table>
<tr><th colspan="4">Phase 2 « Etude »</th></tr>
<tr><th colspan="4">Objectifs</th></tr>
<tr><td colspan="4">Les objectifs de cette phase sont :
▪ De réaliser les études techniques associées aux différents chantiers (spécifications techniques…) ;
▪ De mettre à jour le Dossier d'architecture Technique (DAT) ;
▪ De rédiger l'ensemble des spécifications techniques liées à l'architecture, à l'administration et à l'exploitation des infrastructures et du service d'interconnexion ;
▪ D'ajuster le cas échéant le plan de migration élaboré en Phase 1 « Planification » ;
▪ De former l'Administration aux outils de gestion et de suivi opérationnel du titulaire.</td></tr>
<tr><th colspan="4">Prérequis</th></tr>
<tr><td colspan="4">Les prérequis de la phase sont la réalisation préalable :
▪ Les sortants de la Phase 1 « Planification » validés ;
▪ La description technique des accès des sites à migrer de la part des bénéficiaires ;
▪ Les éventuelles évolutions de la part de l'Administration.</td></tr>
<tr><th colspan="4">Activités à réaliser</th></tr>
<tr><th>Acteur</th><th colspan="3">Activité</th></tr>
<tr><td>Département ISO de la DINUM</td><td colspan="3">▪ Pilote le projet et représente les bénéficiaires ;
▪ Participe aux réunions techniques si nécessaire ;
▪ Valide les spécifications techniques.</td></tr>
<tr><td rowspan="5">Pour chaque titulaire des lots 1 à 5</td><td>Etape</td><td>Activités</td><td>Livrables</td></tr>
<tr><td>1</td><td>Adapter et finaliser l'architecture technique du service proposé en fonction des mises à jour et évolutions fournies au titulaire au démarrage de cette phase</td><td>▪ Spécifications d'architectures détaillées du service d'interconnexion</td></tr>
<tr><td>2</td><td>Concevoir le dossier d'architecture détaillée et d'exploitation des sites pilotes</td><td>▪ Dossier d'architecture détaillée et d'exploitation des sites pilotes</td></tr>
<tr><td>3</td><td>Pour les lots 1 à 5 et 7, réaliser la maquette d'interopérabilité entre :
▪ La solution du titulaire et l'épine dorsale du RIE ;
▪ La solution du titulaire et le LAN de l'Administration.</td><td>▪ Cahier de test rempli</td></tr>
<tr><td>4</td><td>Rédiger l'ensemble des spécifications techniques liées à l'architecture, à l'administration et</td><td>▪ Spécifications d'architectures détaillées de l'administration et de l'exploitation de la solution</td></tr>
</table>

Phase 2 « Etude »			
		à l'exploitation du service d'interconnexion	▪ Dossier d'ingénierie ▪ Dossier de configuration des équipements d'extrémité ▪ Configurations par type d'accès et d'équipement ▪ Liste des services ouverts et leur usage ▪ Versions d'OS des équipements déployés ▪ Dossiers de transfert de compétence
	5	Décrire précisément le processus du déploiement	▪ Mise à jour du Plan d'Assurance Qualité (PAQ) et du Plan d'Assurance Sécurité (PAS) ▪ Spécifications organisationnelles du processus de transition Build-Run
	6	Rédaction du dossier de recette	▪ Cahier de recette
	7	Former l'Administration aux outils gestion et de suivi opérationnel du titulaire	▪ PV de formation

Modalités d'exécution
Les modalités d'exécution sont : ▪ Des réunions de travail avec l'ensemble des parties prenantes ; ▪ Le cadrage logistique et la planification des réunions par l'Administration ou, le cas échéant le titulaire du lot 6.

Engagement de service
Le délai de réalisation de cette phase est mentionné au chapitre relatif aux engagements sur les prestations d'entrée. Les engagements sur la fourniture des éléments et des comptes rendus sont mentionnés au chapitre relatif aux engagements sur la gouvernance de l'accord cadre.

{PP-L1 à 7/15}. 4.8.2 Phase 2 « Etude » : Proposition d'une démarche complémentaire et du plan d'action associé en indiquant les principaux jalons associés.

{PP-L1 à 7/16}. 4.8.2 Phase 2 « Etude » : Description des moyens humains et organisationnels mise en œuvre pour garantir la tenue des délais de cette phase.

{PP-L1 à 7/17}. 4.8.2 Phase 2 « Etude » : Précision et justification d'éventuelles prérequis nécessaires à la phase.

4.8.3 Phase 3 « Pilotes »

<table>
<tr><th colspan="2">Phase 3 « Pilotes »</th></tr>
<tr><th colspan="2">Objectifs</th></tr>
<tr><td colspan="2">La phase pilote pour avoir un sens doit être réalisée en environnement de production et donc sur des sites réels des bénéficiaires selon les niveaux de sécurité du lot du titulaire.
Pour les Lots 1 et 2, la phase pilote comprend le raccordement du réseau de collecte du titulaire à la POM du territoire concerné, elle-même raccordée, par les titulaires des Lots 3, 4 ou 5 ou 7, sur au moins deux des points de concentration choisis et tels que définis dans le dossier d'architecture.
Les étapes de cette phase sont :
▪ Mettre en œuvre les sites pilotes sur la nouvelle infrastructure et migrer les accès ;
▪ Déclarer la Mise en Ordre de Marche (MOM) ;
▪ Réaliser la Vérification d'Aptitude (VA) et la Vérification du Service Régulier (VSR) du site pilote ;
▪ Transférer les compétences à l'Administration sur les outils mis à disposition par chaque titulaire.</td></tr>
<tr><th colspan="2">Prérequis</th></tr>
<tr><td colspan="2">Les prérequis de la phase sont la réalisation préalable :
▪ Les sortants de la Phase 2 « Etude » validés ;
▪ Les éventuelles évolutions de la part de l'Administration ;
▪ La validation de la démarche de migration ajustée ;
▪ Les spécifications techniques validées ;
▪ La liste des contacts des sites du bénéficiaire concerné et des personnels habilités à accompagner les personnels du titulaire si nécessaire ;
▪ La fourniture et la réalisation des travaux à la charge des bénéficiaires :
- De desserte interne ;
- De baies rackables disponibles avec le nombre d'emplacements suffisant ;
- Fluides ;
- Cheminement de fibre optique ou câbles des sites
- Etc.</td></tr>
<tr><th colspan="2">Activités à réaliser</th></tr>
<tr><th>Acteur</th><th>Activité</th></tr>
<tr><td>Bénéficiaires demandeurs</td><td>▪ Identifient les sites pilotes de son périmètre ;
▪ Mobilisent les personnels sur les sites pilotes ;
▪ Assistent la DINUM aux opérations de vérification des sites pilotes.</td></tr>
<tr><td>Département ISO de la DINUM</td><td>▪ Pilote le projet et représente les bénéficiaires ;
▪ Participe aux réunions techniques si nécessaire ;
▪ Réalise la recette du site pilote (test des processus de migration qui comprend une recette fonctionnelle applicative) :
- Vérification des procédures de déploiement des sites de</td></tr>
</table>

<table>
<tr><th colspan="4">Phase 3 « Pilotes »</th></tr>
<tr><td></td><td colspan="3">l'Administration ;
- Vérification des procédures de retour arrière ;
- Vérification de l'architecture, des règles de dimensionnement, des classes de services et de toutes les fonctionnalités ;
- Vérification des engagements du titulaire d'un point de vue performance ;
- Vérification des engagements du titulaire en termes de délai de déploiement de la solution ;
- Vérification de la mise en œuvre des systèmes d'administration et d'exploitation du titulaire ;
- Vérification de la mise en œuvre des systèmes de suivi et de supervision mis à disposition pour le compte de l'Administration. ;
- Vérification pour les lots 1 à 5 et 7 de l'interopérabilité entre :
▪ La solution du titulaire et l'épine dorsale du RIE ;
▪ La solution du titulaire et le LAN de l'Administration
▪ Suite aux vérifications effectuées, prononce positive ou non de la Vérification d'Aptitude du site pilote ;
▪ Peut demander au titulaire d'appliquer les procédures de retour arrière définies de façon à revenir à l'état initial.</td></tr>
<tr><td rowspan="4">Pour chaque titulaire des lots 1 à 5 et 7</td><td>Etape</td><td>Activités</td><td>Livrables</td></tr>
<tr><td>1</td><td>▪ Met en œuvre les outils d'exploitation et de supervision ;
▪ Met en œuvre les moyens de communication entres la DINUM/ISO et le titulaire</td><td>▪ PV de constat de bon fonctionnement</td></tr>
<tr><td>2</td><td>▪ Réalise le transfert de compétences des outils mis à disposition par le titulaire auprès de l'Administration pour la gestion et le suivi opérationnel</td><td>▪ Support pédagogique
▪ Guides utilisateur</td></tr>
<tr><td>3</td><td>▪ Met en place un inventaire exhaustif des configurations de chaque raccordement, équipement d'extrémité et classe de services mis en œuvre (dossier de site) ;
▪ Contrôle au préalable le bon fonctionnement ;
▪ Met en ordre de marche les accès</td><td>▪ PV de conformité de l'installation
▪ Dossiers de sites</td></tr>
</table>

<table>
<tr><th colspan="4">Phase 3 « Pilotes »</th></tr>
<tr><td></td><td></td><td>▪ Maintient en conditions opérationnelles et de sécurité les accès à l'issue de la Mise en Ordre de Marche</td><td></td></tr>
<tr><td></td><td>4</td><td>▪ Transmet les paramétrage et configuration des équipements d'extrémités à l'Administration ;
▪ Assiste l'Administration qui procède à ses vérifications
▪ Réalise les ajustements suite aux observations de l'Administration</td><td rowspan="2">▪ Mise à jour du Plan d'Assurance Qualité (PAQ) et du Plan d'Assurance Sécurité (PAS)
▪ Mise à jour des spécifications techniques et organisationnelles du processus de migration</td></tr>
<tr><td></td><td>5</td><td>▪ Assiste, notamment le titulaire du Lot 6, l'Administration qui procède à ses vérifications d'interopérabilité entre :
- La solution de chaque titulaire et l'épine dorsale du RIE ;
- La solution de chaque titulaire et le LAN de l'Administration ;
▪ Réalise les ajustements suite aux observations de l'Administration</td></tr>
<tr><th colspan="4">Modalités d'exécution</th></tr>
<tr><td colspan="4">Les modalités d'exécution sont :
▪ Des réunions de travail avec l'ensemble des parties prenantes ;
▪ Le cadrage logistique et la planification des réunions par l'Administration ou, le cas échéant le titulaire du lot 6.</td></tr>
<tr><th colspan="4">Engagement de service</th></tr>
<tr><td colspan="4">Le délai de réalisation de cette phase est mentionné au chapitre relatif aux engagements sur les prestations d'entrée.
Les engagements sur la fourniture des éléments et des comptes rendus sont mentionnés au chapitre relatif aux engagements sur la gouvernance de l'accord cadre.</td></tr>
</table>

{PP-L1 à 7/18}. 4.8.3 Phase 3 « Pilotes » : Proposition d'une démarche complémentaire et du plan d'action associé en indiquant les principaux jalons associés.

{PP-L1 à 7/19}. 4.8.3 Phase 3 « Pilotes » : Description des moyens humains et organisationnels mise en œuvre pour garantir la tenue des délais de cette phase.

{PP-L1 à 7/20}. 4.8.3 Phase 3 « Pilotes » : Précision et justification d'éventuelles prérequis nécessaires à la phase.

4.8.4 Phase 4 » Généralisation »

Phase 4 » Généralisation »	
Objectifs	
L'objectif de la phase 4 « Généralisation » est de généraliser les déploiements de l'ensemble de sites selon les modalités définies lors de la Phase 3 « Pilotes » et la planification définie lors de la Phase 1 « Planification ». Les étapes de cette phase sont : ▪ Mettre en œuvre et migrer les accès en plusieurs regroupements de sites sur la nouvelle infrastructure ; ▪ Déclarer la Mise en Ordre de Marche ; ▪ Réaliser la Vérification d'Aptitude (VA) et la Vérification du Service Régulier (VSR) des sites migrés ; ▪ Transférer les compétences à l'Administration sur les outils mis à disposition par chaque titulaire.	
Prérequis	
Les prérequis de la phase sont la réalisation préalable : ▪ Les sortants de la Phase 3 « Pilotes » validés ; ▪ Pour les lots 1 à 5 et 7, l'interconnexion avec l'épine dorsale du RIE fonctionnelle ; ▪ La liste des contacts des sites du bénéficiaire concerné et des personnels habilités à accompagner les personnels du titulaire si nécessaire.	
Activités à réaliser	
Acteur	**Activité**
Bénéficiaires demandeurs	▪ Mobilisent les personnels (contacts locaux) sur les sites ; ▪ Si nécessaire, réalisent les travaux préalables à l'installation du titulaire : - Desserte interne ; - Baies *rackables* disponibles avec le nombre d'emplacements suffisant ; - Fluides ; - Cheminement de fibre optique ou câbles des sites ; ▪ Assistent la DINUM aux opérations de vérification des sites migrés.
Département ISO de la DINUM	▪ Pilote le projet et représente les bénéficiaires ; ▪ Participe aux réunions techniques si nécessaire ; ▪ Réalise la recette des sites bénéficiaires en procédant aux mêmes vérifications que celles définies dans la Phase 3 « Pilotes » ; ▪ Suite aux vérifications effectuées, prononce ou pas la Vérification d'Aptitude du site ; ▪ Peut demander au titulaire d'appliquer les procédures de retour arrière définies de façon à revenir à l'état initial.

<table>
<tr><th colspan="4">Phase 4 » Généralisation »</th></tr>
<tr><td rowspan="4">Pour chaque titulaire des lots 1 à 5 et 7</td><th>Etape</th><th>Activités</th><th>Livrables</th></tr>
<tr><td>1</td><td>▪ Déploie les accès aux sites par regroupement selon le plan de migration défini ;
▪ Contrôle au préalable le bon fonctionnement des sites déployés ;
▪ Met en ordre de marche les accès des sites déployés ;
▪ Ouvre le service de l'ensemble des sites concernés ;
▪ Déclare la mise en ordre de marche de l'ensemble des sites concernés.</td><td>▪ PV de conformité de l'installation
▪ Déclaration de MOM</td></tr>
<tr><td>2</td><td>▪ Maintient en conditions opérationnelles et de sécurité les accès migrés ;
▪ Met en place un inventaire exhaustif des configurations de chaque raccordement, équipement d'extrémité et classe de services mis en œuvre.</td><td>▪ Dossiers de sites</td></tr>
<tr><td>3</td><td>▪ Transmet les paramétrages et configurations des équipements d'extrémités à l'Administration ;
▪ Assiste l'Administration qui procède à ses vérifications ;
▪ Réalise les ajustements suite aux observations de l'Administration.</td><td rowspan="2">▪ Mise à jour du Plan d'Assurance Qualité (PAQ) et du Plan d'Assurance Sécurité (PAS)
▪ Mise à jour des spécifications techniques et organisationnelles du processus de migration</td></tr>
<tr><td>4</td><td>▪ Assiste, notamment le titulaire du Lot 6, l'Administration qui procède à ses vérifications d'interopérabilité entre :
- La solution du titulaire et l'épine dorsale du RIE ;
- La solution du titulaire et le LAN de l'Administration ;
▪ Réalise les ajustements suite aux observations de l'Administration.</td></tr>
<tr><th colspan="4">Modalités d'exécution</th></tr>
<tr><td colspan="4">Les modalités d'exécution sont :
▪ Les visites et déplacements sur site pour réaliser les actions énoncées ;
▪ L'ouverture progressive des services selon le plan de déploiement défini lors Phase 1</td></tr>
</table>

Phase 4 » Généralisation »
« Planification » avec ses éventuels ajustements ; ▪ Le suivi de l'exécution et la remontée d'éventuelles alertes par le titulaire du Lot 6, le cas échéant.
Engagement de service
Le délai de réalisation de cette phase est mentionné au chapitre relatif aux engagements sur les prestations d'entrée. Les engagements sur la fourniture des éléments et des comptes rendus sont mentionnés au chapitre relatif aux engagements sur la gouvernance de l'accord-cadre.

{PP-L1 à 7/21}. 4.8.4 Phase 4 » Généralisation » : Proposition d'une démarche complémentaire et du plan d'action associé en indiquant les principaux jalons associés.

{PP-L1 à 7/22}. 4.8.4 Phase 4 » Généralisation » : Description des moyens humains et organisationnels mise en œuvre pour garantir la tenue des délais de cette phase.

{PP-L1 à 7/23}. 4.8.4 Phase 4 » Généralisation » : Précision et justification d'éventuelles prérequis nécessaires à la phase.

{PP-L1 à 7/24}. 4.8.4 Phase 4 » Généralisation » : Précisions des moyens mis en œuvre de l'assistance sur site les personnels de l'Administration aux opérations de recette d'aptitude (VA).

{PP-L1 à 7/25}. 4.8.4 Phase 4 » Généralisation » : Description des indicateurs du cahier de recette de référence des services.

4.8.5 Modalités de déploiement

Dans le cadre de la migration des services ou du raccordement post-migration d'un accès, le titulaire a sous sa responsabilité l'exécution des prestations décrites ci-après.

4.8.5.1 Visite de sites

Le titulaire réalise des visites préalables sur les sites définis par l'Administration. Cette tâche est réalisée au plus tôt par le titulaire afin d'identifier tout problème qui peut impacter la création des liens sur ces sites.

Le titulaire est plus particulièrement vigilant aux aspects relatifs à la double pénétration dans ces bâtiments quand elle est prévue, ainsi qu'aux problématiques de dessertes internes.

La visite de site fait l'objet d'un compte rendu de la part du titulaire mentionnant les points contrôlés et indiquant si l'accès sur le site peut être déployé et migré en l'état

ou, à défaut, quels travaux sont nécessaires pour que ce soit le cas en indiquant explicitement ceux qui sont à la charge du bénéficiaire.

4.8.5.2 Raccordement

Le titulaire réalise la création des accès avec l'installation des équipements d'extrémités et leur raccordement.

Le titulaire fournit l'ensemble des accessoires de montage pour les équipements à installer dans les baies de l'Administration (écrous prisonniers, plateaux porteurs…).

Dans le cadre de ses prestations d'installation des équipements sur les sites de l'Administration, le titulaire assure :

- Le rangement régulier de tous les outillages dans les locaux mis à disposition ;
- L'enlèvement régulier des emballages ;
- La remise en état et le nettoyage régulier des locaux après intervention pour les désordres de son fait.

4.8.5.3 Desserte Interne

La desserte interne est à la charge des bénéficiaires, cependant, la fourniture de la desserte interne peut être proposée et entrée dans le cadre des prestations supplémentaires éventuelles (PSE).

Dans ce cadre la desserte interne concerne le câblage à réaliser entre le point de livraison de l'accès et l'emplacement pour l'installation de l'équipement de service du titulaire.

La desserte interne consiste à prolonger la livraison du lien d'accès du répartiteur général jusqu'au local technique (et emplacement) où se situera l'équipement du titulaire qui est raccordée au lien d'accès.

L'intervention pour les travaux de desserte interne s'effectue aux heures ouvrées.

4.8.6 Instances de pilotage de la migration

Pendant toute la migration des sites, les instances de gouvernance et l'ensemble des dispositifs prévus dans le chapitre « Gouvernance de l'accord-cadre » s'appliquent.

Cependant, les fréquences de deux d'entre-elles sont plus élevées :

- Le Comité de pilotage de l'accord-cadre « COPIL » dont la fréquence est au minimum mensuel ;
- Le Comité de projet de déploiement « COPROJ » dont la fréquence est au minimum bimensuel.

4.9 Raccordement post-migration d'un accès

Dès la validation par l'Administration du Procès-verbal (PV) de la Mise en ordre de marche (MOM) du premier (1er) site du périmètre convenu de migration, la gestion opérationnelle du service (« VDS » pour Vie de service) couvre l'exploitation des services migrés ainsi que toutes nouvelles opérations de production des accès au réseau (création, modification et résiliation d'accès).

Ces nouvelles opérations peuvent être – ou non – regroupées, selon la demande de l'Administration :

- Soit sous forme de projet de déploiement : elles suivent dans ce cas le même processus de gestion globale que pour la migration des services, avec la production d'un certain nombre d'opérations, pour un ou plusieurs bénéficiaires, dans un calendrier donné, pour un périmètre donné ;
- Soit en tant qu'opération isolée, sans notion de regroupement. Une telle opération suit dans ce cas la logique standard de commande / livraison décrite au chapitre relatif à la passation des commandes d'achat.

4.10 Gestion opérationnelle du service

4.10.1 Abonnements des accès et services associés inclus

Les services associés qui sont inclus dans le coût de chaque abonnement sont :

- Abonnement au service de transport des flux ;
- Gestion des incidents ;
- Supervision réalisée par le titulaire ;
- Gestion des problèmes ;
- Préparation du comité d'exploitation ;
- Fourniture d'éléments entrant dans l'exploitation ou la supervision courante du service ;
- Passation des commandes ;
- Fourniture, l'installation, l'administration et la maintenance des équipements d'extrémités du titulaire ;
- Services de partage de charge (actif/passif ou actif/actif) lorsque l'infrastructure le permet ;
- Administration et maintenance applicative (incluant la maintenance évolutive) des API ;
- Pilotage de l'accord-cadre (partie commerciale et opérationnelle) ;

- Participation aux réunions des comités de gouvernance de l'accord-cadre dans lesquels la présence du titulaire est précisée ;
- De manière générale les prestations, les services, les documents et éléments à fournir ou à mettre à jour, pour lesquels des unités d'œuvre spécifiques ne sont pas mentionnés dans le bordereau des prix unitaires et décrits ou listés dans le présent document.

4.10.2 Gestion des évolutions majeures

Les évolutions majeures sont des changements demandés par l'Administration qui modifient l'abonnement au(x) service(s).

Le traitement des évolutions majeures :

- Soit ne génère pas de coût, notamment pour :
  - Les demandes portant sur des services associés déjà inclus dans le coût de l'abonnement de l'accès ;
  - Les demandes d'augmentations de la bande passante d'un accès ou d'un lien sans impact sur l'infrastructure du titulaire ;
- Soit est financé par une unité d'œuvre définie dans le bordereau des prix unitaires.

La liste des évolutions majeures pour lesquels les unités d'œuvre du poste « Mise en service » sont utilisables sont notamment :

- La création d'un nouvel accès ;
- L'augmentation de la bande passante nécessitant une modification de l'infrastructure du titulaire ;
- L'augmentation d'un niveau de service nécessitant une modification de l'infrastructure du titulaire ;
- La sécurisation géographique sur des points d'accès différents ;
- L'ajout d'un service d'échange et de filtrage entre les communautés d'un DROM
- L'ajout d'un service d'accès Internet pour un usage donné
- Tout autre évolution justifiée et soumise à l'Administration pour acceptation.
-

{EX-L1 à 5 & 7/05}. Gestion des évolutions majeures4.10.2 Gestion des évolutions majeures : Les modifications de l'infrastructure du titulaire non consécutives à une demande d'évolution majeure de la part de l'Administration sont à la charge du titulaire.

-

{PP-L1 à 5 & 7/18}. Gestion des évolutions majeures4.10.2 Gestion des évolutions majeures : Exemples de propositions des évolutions majeures pouvant être soumis à l'acceptation de l'Administration.

Les impacts sur l'infrastructure du titulaire sont notamment :

- Le changement des équipements d'extrémités du titulaire ;
- Le changement de la boucle locale :
  - Modification du rattachement consécutive à une demande explicite de l'Administration ;
  - Doublement de l'adduction (cheminement des fibres optiques ou supports autres) ;
  - Doublement de la pénétration du site de l'Administration ;
- Tout autre impact justifié et soumis à l'Administration pour acceptation.

{PP-L1 à 5 & 7/19}. 4.10.2 Gestion des évolutions majeures : Exemples de propositions de type d'impact sur l'infrastructure du titulaire pouvant être soumis à l'acceptation de l'Administration.

Les délais de mise en œuvre du poste « Mise en service » sont mentionnés dans le Bordereau des délais (cf. référence [R2]).

4.10.3 Gestion des évolutions mineures

Les évolutions mineures sont des changements demandés par l'Administration qui ne modifient pas l'abonnement au(x) service(s).

Le traitement des évolutions mineures :

- Soit ne génère pas de coût, notamment pour les demandes portant sur des services associés déjà inclus dans le coût de l'abonnement de l'accès ;
- Soit est financé par une unité d'œuvre définie dans le bordereau des prix unitaires ;
- Soit est financé par les unités d'œuvre du poste « Evolutions mineures sans impact sur l'infrastructure » du bordereau de prix unitaires.

La liste des évolutions mineures pour lesquelles les unités d'œuvre du poste « Evolutions mineures sans impact sur l'infrastructure » sont utilisables, comprend notamment :

- La configuration ou le paramétrage (notamment les routes statiques et les ACL) d'un équipement du titulaire demandé par l'Administration ;
- Le paramétrage d'un réseau logique VPN ;
- L'application d'une configuration d'une QOS ;

- L'ajout des règles de flux sur les pares-feux de la plateforme de service PFS DROM
- L'ajout de filtrage liste blanche et noire sur une solution d'accès Internet
- Tout autre évolution sans impact sur l'infrastructure du titulaire justifiée et soumise à l'Administration pour acceptation.

{EX-L1 à 5 & 7/06}. 4.10.3 Gestion des évolutions mineures : Exemples de propositions des évolutions mineures pouvant être soumis à l'acceptation de l'Administration.

La mise en œuvre du poste « Evolutions mineures sans impact sur l'infrastructure » est la suivante :

- L'Administration commande une quantité de ticket ;
- Chaque évolution mineure consomme un et un seul ticket ;
- Les tickets non utilisés en fin d'accord-cadre ne sont pas dus.

Le titulaire dresse le bilan par bénéficiaire des tickets consommés par chacun d'eux lors de chaque réunion régulière du Comité d'exploitation « COMEX ».

4.10.4 Résiliation d'un accès

Lors de la résiliation d'un accès en-cours d'accord-cadre, le titulaire :

- Transmet la configuration des équipements qui concernent l'Administration ;
- Décommissionne l'ensemble de ses équipements d'extrémité ;
- Décommissionne l'ensemble de la desserte interne (fibres optiques, coaxiaux…), si le titulaire l'a installée, sur demande du responsable du site de l'Administration.

4.11 Gestion des incidents

4.11.1 Organisation générale du support

4.11.1.1 Support niveau 1 : CSU (chaine de soutien aux utilisateurs)

La chaîne de support utilisateurs (CSU) est une structure interne et spécifique, notamment en matière d'organisation, à chaque bénéficiaire, rattachée à sa direction ou service du numérique. La CSU est sollicitée en première intention par les utilisateurs du bénéficiaire pour signaler un incident.

Les intervenants des CSU ont la charge de consigner les incidents dans l'outil central de l'Administration. Ils réalisent ou/et pilotent les actions nécessaires en prérequis dans le cadre de la qualification des incidents. Ils valident la bonne résolution de l'incident par le retour au fonctionnement nominal du service entrainant alors la fermeture du ticket d'incident par le pôle Hypervision.

Les CSU sont les cellules opérationnelles au sein de l'organisation des bénéficiaires, intervenant dans le cadre d'un incident. Chaque CSU :

- Assure l'interface avec d'une part les utilisateurs des bénéficiaires et d'autre part le pôle Hypervision ;
- Enregistre dans le système de gestion des incidents de l'Administration les incidents décelés par les utilisateurs des bénéficiaires ;
- Procède à une première vérification, le cas échéant identifie des réponses à apporter au vu de leur connaissance (problématique déjà connue) ;
- Exécute les actions requises ou préconisées par le pôle Hypervision ou les opérateurs sur la vérification des équipements (validation des prérequis), en s'appuyant sur les services techniques des sites concernés.

Les CSU sont les interlocuteurs privilégiés des bénéficiaires pour la gestion des incidents affectant leur réseau.

Si un incident n'est pas résolu par la CSU compétente, il est alors pris en charge par le pôle Hypervision (niveau 2).

4.11.1.2 Support niveau 2 : Pôle Hypervision

Le NOC RIE du pôle Hypervision, en tant que support de niveau 2 :

- Qualifie l'incident et le cas échéant détermine son niveau de sévérité ;
- Réalise des opérations de vérification plus poussées ;
- S'il s'agit de problème de sécurité, le NOC fait un signalement au CSIRT de la DINUM qui prend en charge les opérations spécifiques en matière de SSI (mitigation dans le cadre d'une attaque DDoS par exemple) en lien avec le RSSI du RIE et en s'appuyant sur la filière SSI des bénéficiaires ;
- Dispose d'une vue sur la supervision des équipements et est capable de déterminer si un équipement est toujours actif ou non.

Le cas échéant, si les actions correctives menées ne permettent toujours pas la résolution de l'incident, le support niveau 2 saisit le titulaire concerné par l'incident.

4.11.1.3 Support niveau 3 : Titulaire des lots 1 à 5 et 7

Sur la base des éléments communiqués par le NOC RIE, le support niveau 3 :

- Assure une qualification supplémentaire de l'incident ;
- Fait intervenir un niveau d'expertise plus poussée ;
- Propose une solution de contournement et/ou résout l'incident ;
- Met tout en œuvre pour corriger l'incident dans les engagements de GTR et d'IAA correspondant au niveau de service de l'accès.

4.11.2 Prérequis et période de gel

Les « prérequis » sont des actions à réaliser ou des éléments à fournir par l'Administration et nécessaires au titulaire pour réaliser son diagnostic d'un dysfonctionnement ou pour analyser toute demande de l'Administration.

Que ce soit pour le traitement des incidents ou l'exécution des commandes de changement ou de création de liens d'accès, les « temps de gel » pris en compte sont :

- Le temps de la communication par l'Administration des « prérequis » ;
- Le temps de la non disponibilité du contact sur le site de l'Administration incluant :
  - La période pendant laquelle le contact site est injoignable ;
  - Le temps d'attente de l'arrivée du contact site à condition que :
    - Le titulaire ait au préalable pris un rendez-vous confirmé par l'Administration ;
    - Le titulaire dispose du numéro de téléphone fixe ou mobile du contact pour l'aviser de son arrivée sur site.

Le titulaire suit et trace toutes les actions justifiant le « temps de gel » (début, fin, cause…) dans le ticket d'incident ou le suivi de la production d'un accès (création et évolution).

Les « temps de gel » non pris en compte sont tous les temps où la responsabilité de l'Administration n'est pas formellement démontrée par le titulaire, notamment :

- Tous les temps qui n'ont pas été justifiés par le titulaire même si la responsabilité de l'Administration est supposée ;
- Tous les temps qui n'ont pas été tracés par le titulaire ;
- Le temps de déplacement d'intervention du titulaire sur le site de l'Administration.

Dans les cas particuliers des incidents génériques ou multi-sites ou multi-clients :

- La GTR s'applique individuellement pour chacun des accès concernés par l'incident générique ;
- Le temps d'indisponibilité n'est pas gelé, notamment du fait des délais de fourniture des prérequis qui n'ont pas lieu d'être.

4.11.3 Processus de déclaration d'un incident

4.11.3.1 Processus 1 « Signalement par les CSU »

A la suite du constat d'un dysfonctionnement du réseau, la CSU du bénéficiaire affecté par celui-ci crée un signalement sous la forme d'un « ticket » auprès du pôle Hypervision soit via l'Extranet du RIE, sur l'espace dédié au signalement d'incident, soit par mail ou encore par téléphone.

Le processus de gestion des incidents dans le cadre d'un signalement fait par les CSU est le suivant :

- La vérification de la présence effective d'un dysfonctionnement :
  - Le NOC réalise une vérification de prérequis avant la confirmation d'ouverture du ticket d'incident ;
  - La vérification des prérequis s'accompagne d'un gel du ticket saisi pour le décompte du temps de rétablissement du service (GTR) ;
  - Si les prérequis ne sont pas concluants, le ticket saisi est fermé avec l'indication « hors périmètre ».
- Si les prérequis sont validés et le dysfonctionnement confirmé, le NOC réalise l'ouverture du ticket d'incident directement auprès du titulaire si ce dernier n'a pas déjà identifié l'incident ;
- Après résolution de l'incident par le titulaire, le NOC procède à une vérification du rétablissement en mode nominal du service.
- Le NOC :
  - Ferme le ticket de l'incident en accord avec le titulaire si l'incident est isolé et résolu ;
  - Maintient le ticket ouvert pour cause de récurrence de l'incident ;
  - Informe par mail (envoyé via l'Extranet RIE) et/ou par téléphone la CSU de la résolution de l'incident.

4.11.3.2 Processus 2 « Alarme de la supervision de l'Administration »

Dans le cas où le pôle Hypervision, détecte lui-même un incident, le pôle Hypervision :

- Crée un ticket d'incident dans son outil de suivi ;
- Réalise des demandes de prérequis auprès de la CSU du bénéficiaire.

La suite du processus est identique au Processus 1 « Signalement par les CSU ».

4.11.3.3 Processus 3 « Détection proactive par le titulaire »

Dans le cas où le titulaire détecte un incident, le titulaire :

- Emet un message de début d'incident par mail au pôle Hypervision ;
- Notifie l'incident sur son Portail client ou via API ;
- Demande les prérequis au NOC qui la relaye vers les CSU.

La suite du processus est identique au Processus 1 « Signalement par les.

{PP-L1 à 5 & 7/20}. 4.11.3.3 Processus 3 « Détection proactive par le titulaire » : Description des mécanismes de détection proactive des incidents.

4.11.4 Procédure d'escalade

Une procédure d'escalade, technique et managériale, est définie entre l'Administration et le titulaire. Elle a pour vocation de mettre en relation, de mobiliser et d'impliquer les compétences techniques ou managériales requises à la résolution d'incidents complexes ou présentant un retard significatif par rapport aux délais contractuels de rétablissement du service.

Cette procédure d'escalade au sein de l'Administration se caractérise par 4 niveaux hiérarchiques qui se mobilisent selon les degrés de criticité voire des dérives constatées sur le traitement des incidents :

Niveau d'escalade	Niveau hiérarchique concerné DINUM / ISO	Niveau hiérarchique concerné Titulaire
N1	Les « hyperviseurs » du pôle Hypervision	Les ressources techniques du titulaire ou équivalent
N2	Les référents du pôle Hypervision	Le chef de projet opérationnel du titulaire ou équivalent
N3	Les responsables du pôle Hypervision	Le directeur opérationnel du titulaire ou un niveau équivalent
N4	Les responsables du département DINUM / ISO	La direction générale du titulaire ou un niveau équivalent

{PP-L1 à 5 & 7/21}. 4.11.4 Procédure d'escalade : Précision du niveau hiérarchique des interlocuteurs et leur entité d'appartenance pour chaque niveau hiérarchique (N1 à N4).

Condition de déclenchement	Niveau d'escalade concerné
Dès le dépassement des délais de la GTR	N1
Dépassement des délais de la GTR +50%	N2
Dépassement des délais de la GTR +100%	N3
Dépassement des délais de la GTR +150%	N4

{PP-L1 à 7/26}. 4.11.4 Procédure d'escalade : Propositions pour compléter la démarche proposée.

4.11.5 Organisation du support du titulaire

Dans le cadre de ses prestations de service, le titulaire met en œuvre une organisation de support permettant notamment :

- La supervision proactive de ses infrastructures et des services de transport fournis, avec un enregistrement et un signalement automatique des incidents ;
- Le recueil, la qualification ainsi que le traitement de l'ensemble des signalisations (incidents, demandes, travaux programmés, gel de production…) de l'Administration ;
- La coordination des équipes opérationnelles du titulaire en cas d'intervention à distance ou sur site ;
- L'information des différents acteurs du traitement d'un incident, ainsi que la traçabilité opérationnelle intégrale des tickets d'incident ;
- A la demande de l'Administration ou de manière proactive en cas d'incident significatif, tant par ses impacts métier que par ses caractéristiques techniques, l'analyse *post-mortem* d'un incident (RetEx) :
  - Historique détaillé du traitement ayant permis sa résolution ;
  - Proposition d'amélioration du processus de traitement ;
  - Identification des causes racines ;
  - Plan d'actions pour supprimer l'avènement de nouvelles occurrences ou mitiger leurs impacts en matière de qualité de service ;
- La mise en œuvre des procédures d'escalade.

{PP-L1 à 5 & 7/22}. 4.11.5 Organisation du support du titulaire : Description des moyens humains et organisationnels mise en œuvre du support du titulaire.

{PP-L1 à 5 & 7/23}. 4.11.5 Organisation du support du titulaire : Précision du profil pressenti du référent technique et opérationnel mis à disposition.

Cette organisation :

- Est joignable à travers un numéro de téléphone unique, dédié et non surtaxé ;
- Supporte les échanges dématérialisés, sur le Portail du titulaire ou via API et également via une adresse de messagerie électronique générique et dédiée.

Les échanges réalisés avec le titulaire (support client, services techniques, etc.) le sont exclusivement en langue française.

Des mécanismes de protection des échanges sont mis en œuvre, si leur niveau de sensibilité le justifie.

4.11.6 Supervision réalisée par le titulaire

Le titulaire assure la supervision complète et permanente de son infrastructure réseau, des accès nominaux, des accès de secours et des équipements d'extrémités en temps réel 24 heures sur 24 et sept jours sur sept, tous les jours de l'année.

Les données attendues sont les informations d'état des services rendus et le statut des équipements, dédiés ou non, constitutifs des services afin d'assurer l'ouverture proactive de tickets d'incident et / ou l'aide au diagnostic lors de la procédure de gestion des incidents.

Le titulaire fournit un outil en accès web (portail client) et via API permettant d'accéder à des informations unitaires (par incident, accès, etc.) et de visualiser les informations de supervision sur l'ensemble du périmètre de façon agrégée par bénéficiaire.

Le titulaire met en œuvre les mécanismes de notification définis au chapitre relatif aux échanges automatisés de la gestion des incidents.

{PP-L1 à 5 & 7/24}. 4.11.6 Supervision réalisée par le titulaire : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre et notamment au niveau des équipements et indicateurs supervisés, des types d'alarmes remontées, des mesures de performance du réseau et des seuils de remontée d'alarmes, des niveaux de sévérité des incidents en fonction des alarmes remontées, de la profondeur de l'historique des informations…

{PP-L1 à 5 & 7/25}. 4.11.6 Supervision réalisée par le titulaire : Description de l'organisation et des moyens mise en œuvre pour réaliser la supervision.

4.12 Gestion des problèmes

Chaque titulaire assure la gestion des problèmes intervenant sur l'ensemble des services.

La gestion des problèmes correspond à la recherche des causes racines sous-jacentes d'incidents afin d'éviter la récurrence d'incidents de même nature ainsi qu'à la recherche des causes racines sous-jacentes des dégradations de service notamment en matière de performance.

Les procédures de gestion des problèmes sont soit initiées de manière proactive par le titulaire soit demandées par l'Administration.

{PP-L1 à 7/27}. 4.12 Gestion des problèmes : Description des moyens humains et organisationnels mise en œuvre pour la gestion des problèmes.

{PP-L1 à 7/28}. 4.12 Gestion des problèmes : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre pour la gestion des problèmes.

{PP-L1 à 7/29}. 4.12 Gestion des problèmes : Proposition d'une démarche pour la gestion des problèmes.

4.13 Gestion des opérations planifiées

Avant toute opération planifiée sur son réseau, comme par exemple des travaux de maintenance, pouvant impacter les services délivrés et leurs performances, le titulaire notifie à l'Administration :

- Via l'API d'exploitation prévue à cette fin ;
- Par messagerie électronique, sous un format impérativement adapté à un traitement informatisé automatique ;
- Par diffusion sur le portail web client du titulaire.

{PP-L1 à 5 & 7/26}. 4.13 Gestion des opérations planifiées : Description des procédures et moyens de diffusion des notifications des opérations planifiées.

Le titulaire prend connaissance de l'organisation mise en place par l'administration pour gérer les opérations programmées et adaptent ses délais de prévenance et le contenu des informations nécessaires à l'analyse des opérations.

L'Administration peut refuser le lancement d'une opération jusqu'à 2 jours ouvrés avant la date de lancement prévue. Dans ce cas, l'Administration propose une date de report de l'opération ne dépassant pas, si possible, 10 jours ouvrés.

La notification d'avis de travaux programmés contient entre autres :

- La description de l'opération et son objectif ;
- Le planning prévisionnel de l'intervention, en termes de planification (date, heure, durée) et de plages d'impact (heures, durées prévisionnelles) ;
- L'étude de risque et les impacts éventuels sur les services de l'Administration ;
- Les procédures de tests, recette et de retour arrière prévues.

Les opérations présentant un risque d'impact direct sur les services de l'Administration, sont réalisées en heures non ouvrées (HNO) sur une plage horaire qui est définie d'un commun accord entre l'Administration et le titulaire.

Toute opération planifiée, ayant un impact sur le service, fait l'objet d'une phase de tests y compris en cas de retour arrière, suivie en cas de succès d'une notification confirmant le rétablissement en mode nominal du service.

L'administration se réserve le droit d'annuler une opération sans délai en cas de crise ou de force majeure évaluée par les services de l'Etat.

{PP-L1 à 5 & 7/27}. 4.13 Gestion des opérations planifiées : Précision sur les procédures utilisées pour sécuriser les opérations planifiées telles que les procédures, les tests des secours ainsi que leur fréquence et les procédures de retour arrière.

4.14 Préparation du comité d'exploitation

4.14.1 Point quotidien sur les incidents nécessitant un suivi particulier

Un point quotidien sur les incidents en cours nécessitant un suivi particulier est organisé entre les référents du titulaire et ceux de l'Administration ou de son assistant à maîtrise d'ouvrage.

Ce point prend place en jours ouvrés exclusivement. Il permet de partager les informations suivantes sur les incidents en cours :

- Incidents de sévérité 1 (incident critique) ;
- Incidents de sévérité 2 (incident majeur) ;
- Incidents récurrents ;
- Incidents en attente de retour client / prérequis ;
- Incidents en observation ;
- Incidents clos.

4.14.2 Point hebdomadaire sur les incidents en dépassement de GTR

Lors du point hebdomadaire sur les incidents de responsabilité du titulaire en dépassement de garantie de temps de rétablissement, le titulaire justifie des temps de gel enregistrés afin de valider ou ajuster la durée de dépassement calculée par l'Administration, sur la base des informations suivantes :

- Numéro de ticket d'incident sous ses deux (2) références opérateur et Administration ;
- Code RIE de l'accès concerné ;
- Date d'ouverture du ticket opérateur ;
- Sévérité de l'incident ;
- Date de relève de l'incident ;
- Date de résolution de l'incident ;
- Date de fermeture de l'incident ;
- Niveau d'escalade ;

- Garantie contractuelle du taux de rétablissement.

4.14.3 Point bimensuel sur les productions en cours de traitement

Lors du point bimensuel sur les évolutions majeures en cours de production, le titulaire justifie ses délais de traitement, le calcul des temps de gel de production enregistrés afin de valider ou ajuster la durée de dépassement calculée par l'Administration, sur la base des informations suivantes :

- Numéro de commande dans le référentiel de l'Administration ;
- Code RIE de l'accès concerné ;
- Type de l'accès ;
- Date de la commande ;
- Délai contractuel de production et date contractuelle limite de mise en service de la production ;
- Elément susceptible d'entraîner un dépassement du délai contractuel ;
- Dates d'ouverture et de fin des périodes de gel de production ;
- Elément déclencheur des périodes de gel de production ;
- Date de mise en service : cible, prévue, réelle ;
- Date d'émission du Procès-verbal (PV) de Mise en ordre de marche (MOM) de l'accès ;
- Date de validation du PV de recette par l'Administration.

4.14.4 Point mensuel

Le point mensuel porte principalement sur :

- Les divers décomptes, permettant une analyse quantitative, et tout indicateurs clés de performance de tous les faits techniques constatés sur la période ;
- L'ajustement ou la correction, le cas échéant, d'un commun accord par le titulaire et l'Administration des informations relatives :
  - Aux tickets d'incident fermés de la période écoulée (responsabilité, cause racine, durée de dépassement de GTR, etc.) ;
  - Aux évolutions, majeures et mineures, produites et validées sur la période écoulée (durée de dépassement d'exécution par le titulaire, analyse et vérification des demandes de report de livraison, etc.) ;
- La confrontation des arriérés (*backlog*) côté titulaire et Administration des incidents encore ouverts ;

- Les incidents ainsi que les évolutions, ayant fait l'objet d'une escalade auprès du titulaire, afin de valider les niveaux d'escalades et d'en garantir la traçabilité ;
- Les analyses qualitatives détaillées des incidents marquants, avec pour chaque cas, une fiche synthétique individuelle, qui récapitule en complément des éléments intrinsèques de l'incident :
  - Le résumé des actions de résolution de l'incident ;
  - Une analyse des causes du dépassement de la GTR ;
  - Un plan d'amélioration.
- La vérification de la bonne exécution des travaux programmés annoncés, ainsi que de la bonne transmission des avis de travaux programmés correspondants ;

4.15 Opérations de vérification d'un accès

4.15.1 La Mise en ordre de marche (MOM) d'un accès

La Mise en ordre de marche (MOM) comprend :

- L'installation des équipements sur site client ;
- La mise en service, c'est-à-dire le raccordement aux réseaux WAN et LAN, des accès au service de collecte des lots 1 à 5 et 7 ;
- Éventuellement, la migration ou le raccordement post-migration, du site client de son ancien accès vers le nouvel accès.

Durant la phase de migration ou de raccordement post-migration, le titulaire se coordonne avec l'Administration ou son assistant à maîtrise d'ouvrage (titulaire du Lot 6) afin d'éviter, à tout le moins limiter, au maximum la rupture du service d'accès au RIE pour l'utilisateur final du bénéficiaire.

Toutes les opérations de construction d'infrastructures qui nécessitent un accès physique aux sites ne peuvent se faire que pendant les jours et heures d'ouverture de ces sites, en présence d'un contact local, après prise de rendez-vous préalable et formellement validé par les deux (2) parties.

Sur un site donné, disposant d'un lien nominal et d'un lien de secours, le déploiement de ce site est considéré comme effectif uniquement lorsque les deux liens sont construits, mis en ordre de marche et migrés en production.

En cas de problèmes lors des opérations de déploiement, l'Administration attend du titulaire une forte implication, réactivité et capacité à résoudre les différents problèmes rencontrés. Lors des migrations, dans le cas où la résolution des problèmes ne peut s'effectuer dans un délai maximum d'une heure, le titulaire effectue un retour-arrière et rétablit le service du précédent état stable.

Suite à la construction des accès, la fiche d'intervention rédigée par le titulaire détaille les travaux effectués et est contresignée par un agent habilité de l'Administration ou un de ses représentants présents sur site. Cette fiche est un des éléments de la Vérification d'Aptitude de la phase de migration ou de raccordement post-migration.

Après la migration ou le raccordement post-migration du site client sur l'accès produit, le titulaire prononce la Mise en Ordre de Marche pour l'accès concerné.

Certains bénéficiaires optent pour une stratégie de migration groupée ou de raccordement post-migration groupés (par exemple l'ensemble des accès du bénéficiaire sur une zone géographique donnée migrent au cours de la même semaine) : dans ce cas, la Mise en Ordre de Marche peut être prononcée globalement pour l'ensemble des accès faisant l'objet de cette migration ou ces raccordements post-migration groupés.

L'exploitation du service est effective dès la notification de la Mise en Ordre de Marche pour les accès migrés.

4.15.2 Livrables documentaires

Les livrables des différentes phases du projet sont rédigés par le titulaire et soumis pour validation à l'Administration. Tous les livrables sont fournis sous un format de suite bureautique modifiable.

L'Administration dispose d'un délai maximum en jours ouvrés, défini dans le PAQ et ne pouvant pas être inférieur à 5 jours ouvrés afin de valider un livrable à compter de sa livraison.

Les échanges éventuels sur les livrables s'effectuent sous forme de fiches de relecture.

Pour gérer les livrables, le titulaire utilise l'outil de travail collaboratif mis à disposition par l'Administration, permettant de stocker, échanger et structurer l'ensemble des livrables pour les deux parties. Cet outil est accessible au travers d'un accès à Internet et d'une authentification nominative.

4.15.3 Vérification d'aptitude (VA) d'un accès

En prérequis de la Vérification d'aptitude (VA), le titulaire fournit à l'Administration un cahier de recette pour les équipements, les liens et les fonctionnalités de chaque accès concerné, décrivant notamment :

- Les procédures de recette ;
- Le planning des recettes et l'ensemble des tests unitaires ;
- Les procédures de retour-arrière ;

- Un dossier de suivi en exploitation de chaque accès, décrivant notamment :
  - Les caractéristiques techniques du raccordement ;
  - Les procédures à appliquer en cas de défaillance de l'accès.

Les procédures de recette sont adaptées aux différents types d'accès en fonction du niveau de sécurisation et des services complémentaires souscrits.

Pour chaque test unitaire, les cahiers de recette doivent préciser :

- L'identifiant et l'objet du test (notamment son code RIE) ;
- L'environnement technique de test (moyens mis en œuvre) ;
- La mise en œuvre du test (description pas à pas des opérations de test) ;
- Les résultats attendus à chaque étape ;
- Les résultats obtenus.

L'Administration peut éventuellement compléter les cahiers de test. Les procédures de tests validées par l'Administration s'appliquent à chaque phase de migration ou de raccordement post-migration.

A l'issue de la déclaration de la Mise en ordre de marche (MOM) du titulaire, l'Administration peut réaliser les tests de Vérification d'aptitude pendant une durée maximale de 5 jours ouvrés.

L'Administration réalise les tests les plus critiques dès la migration ou le raccordement post-migration effectués pour constater le bon fonctionnement de l'accès. L'Administration peut ensuite procéder à des tests complémentaires.

Les tests de Vérification d'aptitude sont réalisés par l'Administration avec l'assistance du titulaire du lot concerné qui réalise les actions nécessaires au bon déroulement des tests.

Le titulaire est disponible pendant toute la durée de la période de Vérification d'aptitude pour résoudre les problèmes, et le cas échéant activer une procédure de retour arrière sur les liens opérationnels précédant la migration ou le raccordement post-migration.

A l'issue des tests de Vérification d'aptitude, le cahier de test est complété par l'Administration, au niveau de chaque test, par les résultats obtenus avec l'historique de déroulement du test. L'Administration transmet alors au titulaire une copie du cahier de recette complété.

Durant cette étape, des réserves peuvent être émises provoquant de facto un ajournement de la réception des prestations :

- Toute anomalie entrant dans le cadre de la définition des incidents de niveau 1 (critique), de niveau 2 (majeur) ou de niveau 3 (mineur) non résolue ;
- La non-fourniture ou non-conformité des documentations.

En cas d'ajournement, une nouvelle Mise en ordre de marche est exécutée par le titulaire dans les plus brefs délais et au maximum dans les 5 jours ouvrés.

Si le résultat de la Vérification d'aptitude est positif, l'Administration notifie au titulaire sa décision de réception des prestations.

Si l'Administration ne notifie pas sa décision dans le délai convenu, le résultat de la Vérification d'aptitude est considéré comme positif et la période de Vérification de service régulier (VSR) débute.

4.15.4 Vérification de Service Régulier (VSR) d'un accès

La période de Vérification de service régulier (VSR) d'un accès débute à la suite de la validation de la Vérification d'Aptitude. Sa durée est fixée en fonction du type d'accès :

- Six (6) semaines pour les accès de niveau de service « Maximum », « Très Fort » et « Fort » ;
- Quatre (4) semaines pour les accès de niveau de service « Très Elevé », « Elevé » ;
- Deux (2) semaines pour les accès de niveau de service « Best-effort ».

L'objectif de la Vérification de Service Régulier est de contrôler :

- La conformité aux engagements de qualité de service :
  - Lors de la montée en charge ;
  - En conditions opérationnelles d'exploitation ;
- La qualité du support technique.

Durant cette étape, les critères d'ajournement sont au minimum les suivants :

- Toute anomalie entrant dans le cadre de la définition des incidents de niveau 1 (critique), de niveau 2 (majeur) ou de niveau 3 (mineur) non résolue ;
- La non-fourniture ou non-conformité des documentations.

Si l'Administration ne notifie pas sa décision dans le délai convenu, le résultat de la Vérification de service régulier est considéré comme positif et les prestations sont réputées reçues.

4.16 Gestion des performances

En cas de doute sur les performances des services, l'Administration ou un tiers mandaté par celle-ci peut auditer la qualité et les performances des services fournis.

Cet audit porte notamment sur :

- La qualité des flux transportés « éléments du trafic » (volume, pics, taux de perte de paquets, temps de transit et latence, gigue…) ;
- La répartition du trafic par type de flux (répartition de charge, gestion de la QoS…).

Le titulaire met à la disposition de l'Administration ou du tiers mandaté les éléments techniques nécessaires à l'audit de l'Administration dans un délai maximum de 5 jours ouvrés.

{PP-L1 à 5 & 7/28}. 4.16 Gestion des performances : Précisions des éléments techniques nécessaire à l'audit, mis à disposition de l'Administration ou du tiers mandaté et des délais associés.

Si les résultats d'un audit mettent en évidence que la perte de performance :

- Est entièrement imputable au titulaire, un incident de sévérité 2 (« incident majeur ») est déclenché et sa résolution respecte les engagements de service associés ;
- N'est pas entièrement imputable au titulaire, l'Administration peut commander une prestation d'expertise de la performance.

4.17 Services et prestations complémentaires

4.17.1 Prestation d'expertise de la performance

Cette prestation, réalisée en mode projet, porte sur les aspects techniques de l'architecture du réseau. Elle peut être commandée :

- Lorsqu'une dégradation de la performance est constatée et que tout ou partie de la dégradation de performance est imputable à l'Administration ;
- Pour étudier les impacts d'un projet de l'Administration sur l'infrastructure réseau ;
- Pour étudier les impacts de la mise en œuvre d'un service global du titulaire sur l'environnement technique de l'Administration.

Les livrables attendus de la part du titulaire sont au moins :

- Les comptes-rendus de réunion ;

- Une analyse d'impacts ;
- Un plan d'actions et ou des recommandations.

{PP-L1 à 7/30}. 4.17.1 Prestation d'expertise de la performance : Description de la méthode, des principales activités et des livrables associées.

{PP-L1 à 7/31}. 4.17.1 Prestation d'expertise de la performance : Proposition des profils types, avec notamment leur niveau de qualification, leurs expériences.

{PP-L1 à 7/32}. 4.17.1 Prestation d'expertise de la performance : Exemples d'expertises types avec des propositions de métriques pour évaluer la charge de réalisation en jour-homme.

4.17.2 Prestation de projet d'infrastructure

La prestation consiste en des tâches rentrant dans le cadre normal de l'évolution du réseau, non forcément connues précisément au moment de la rédaction du présent CCTP, non susceptibles d'être par avance forfaitisées ou évaluées sans une étude précise et approfondie du travail à réaliser par le titulaire.

Cette prestation est prise en charge par l'Administration, si elle n'entre pas dans le cadre de la gestion des évolutions majeures et si elle réclame une étude de faisabilité, parfois étendue à l'ensemble de l'infrastructure.

Cette prestation peut correspondre, par exemple, à des changements importants des normes en vigueur, à la révision de certains choix techniques de réalisation pour optimiser les performances ou améliorer l'exploitation.

Dans ce cas, l'Administration peut solliciter le titulaire pour une étude technique, pouvant notamment comporter :

- Une étude de faisabilité, évaluant les gains et les risques ;
- Une étude d'impact sur l'exploitation ;
- La proposition de scénarios alternatifs ;
- La quantification de la charge de travail nécessaire.

La réalisation de documents techniques approfondis, sortant du cadre habituel de la gestion opérationnelle des services fait également partie de cette prestation et peut être expressément demandée par l'Administration.

La prestation est un prix forfaitaire basé sur la décomposition des profils des intervenants tels que définis au bordereau des prix unitaires.

Les profils concernés sont les profils de la norme CIGREF de l'annexe [A9] : « Nomenclature CIGREF des profils métiers du système d'information (version 2024) » associés à un niveau de qualification dans le poste. Ces profils sont :

- Directeur de projets ;
- Chef de projet maitrise d'œuvre ;
- Technicien réseaux-télécoms ;
- Administrateur d'outils / de systèmes / de réseaux-télécoms ;
- Intégrateur d'exploitation ;
- Expert systèmes d'exploitation / réseau télécom ;
- Architecte technique.

{PP-L1 à 7/33}. 4.17.2 Prestation de projet d'infrastructure : Description de la méthode, des principales activités et des livrables associées.

{PP-L1 à 7/34}. 4.17.2 Prestation de projet d'infrastructure : Proposition d'un échantillonnage des profils pressentis, avec notamment leur niveau de qualification dans le poste, leurs expériences dans les projets d'infrastructure.

{PP-L1 à 7/35}. 4.17.2 Prestation de projet d'infrastructure : Exemples de projets d'infrastructure types avec des propositions de métriques pour évaluer la charge de réalisation basée sur les unités d'œuvre du bordereau des prix.

4.18 Réversibilité en fin de chaque accord-cadre

La réversibilité consiste en fin de chaque lot à réaliser un basculement progressif du réseau du titulaire sortant vers le réseau du titulaire entrant.

Dans ce cadre, le titulaire met en œuvre les moyens humains et matériels afin de permettre à l'Administration ou à tout tiers mandaté par l'Administration de reprendre dans les meilleures conditions l'exécution des services concernés.

Une phase de réversibilité débute sur demande de l'Administration en fin d'exécution de l'accord-cadre ou en cas de résiliation anticipée de celui-ci. La notification de la réversibilité est émise par l'Administration au minimum un mois avant le début de cette phase.

Pendant toute cette phase de réversibilité, le titulaire :

- Respecte l'ensemble de ses obligations contractuelles et assure une continuité dans la fourniture des services, sous réserve des éventuelles perturbations rencontrées dans la fourniture ou le niveau de qualité des services qui est dues à la mise en œuvre des opérations de migration. Le titulaire est responsable de la qualité des interventions qui sont nécessaires de sa part pendant cette phase ;
- Fournit à l'Administration et au tiers désigné par l'Administration les informations nécessaires, (incluant notamment les paramètres nécessaires et l'adressage des

équipements d'extrémité) pour leur permettre de préparer la réversibilité, à l'exception des informations ayant un caractère confidentiel ou relevant du savoir-faire ou des méthodes du titulaire, de ses fournisseurs ou sous-traitants ;

- Reprend éventuellement des équipements du titulaire s'ils ont été mis à disposition par le titulaire.

Les différentes étapes identifiées sont les suivantes :

- La définition du Plan de Réversibilité ;
- L'initialisation de la phase de réversibilité ;
- La préparation du transfert ;
- Le transfert ;
- La recette.

Les livrables attendus sont :

- Phase d'initialisation : plan de réversibilité, planning associé… ;
- Phase de préparation : inventaire détaillé des moyens humains, services, matériels, logiciels, documents… ;
- Transfert : fourniture des documentations et spécifications relatives aux services… ;
- Réception : PV de recette…

{PP-L1 à 5 & 7/29}. 4.18 Réversibilité en fin de chaque accord-cadre : Description des différentes étapes identifiées de la démarche de réversibilité pour un basculement progressif du réseau du titulaire sortant avec les livrables associés.

{PP-L1 à 5 & 7/30}. 4.18 Réversibilité en fin de chaque accord-cadre : Description des moyens humains et organisationnels pour assurer le bon déroulement de la phase de réversibilité.

{PP-L1 à 5 & 7/31}. 4.18 Réversibilité en fin de chaque accord-cadre : Description des principes de la continuité des services pendant la phase de réversibilité et des procédures de retour en arrières.

Chapitre 5 : Engagements de service

Le respect des engagements de service s'entend en dehors des opérations planifiées convenues en commun avec l'Administration.

5.1 Engagements sur les prestations d'entrée

Description	Fréquence de contrôle
Le délai maximum de la mise en œuvre du **portail client du titulaire** de gestion des **incidents** est de **35 jours ouvrés** à compter de la notification de l'accord-cadre	Fin d'initialisation de chaque lot
Le délai maximum de la mise en œuvre du **portail client du titulaire** de gestion du **volet technique des commandes d'achat** est **35 jours ouvrés** à compter de la notification de l'accord-cadre	
Le délai maximum de la mise œuvre des **modalités des échanges avec le titulaire du** lot 6 est de **15 jours ouvrés** à compter de la notification de l'accord-cadre	
Le délai maximum de la fourniture de la version initiale du plan d'assurance sécurité de l'accord-cadre (**PAS**) est de **20 jours ouvrés** à compter de la notification de l'accord-cadre	
Le délai maximum de la fourniture de la version initiale du plan d'assurance qualité de l'accord-cadre (**PAQ Accord-cadre**) est de **20 jours ouvrés** à compter de la notification de l'accord-cadre	
Le délai maximum de la fourniture de la version initiale du Plan de gestion et d'amélioration continue de l'accord-cadre (**PGAC Accord-cadre**) est de **20 jours ouvrés** à compter de la notification de l'accord-cadre	
Le délai maximum du cadrage du projet de migration des sites des lots 1 à 5 est de **20 jours ouvrés** à compter de la notification de l'accord-cadre	Fin du cadrage
Le délai maximum de l'actualisation du plan d'assurance qualité spécifique au projet de migration (**PAQ Migration**) est de **10 jours ouvrés** à compter de la notification de l'accord-cadre	
Le délai maximum de la **Phase 1 « Planification »** est de **5 jours ouvrés** à compter de la notification du bon de commande de chaque bénéficiaire dans lesquels sont mentionnés la liste des sites à migrer	Fin de phase 1
Le délai maximum de la **Phase 2 « Etude » des Lots 1 et 2** est de **15 jours ouvrés** à compter de la notification du bon de commande de chaque bénéficiaire dans lesquels sont mentionnés la liste des sites à migrer. Ce délai est ajustable selon les conclusions de la Phase 1	Fin de phase 2

Description	Fréquence de contrôle
« Planification »	
Le délai maximum de la **Phase 2 « Etude » des lots 3 à 5 et 7** est de **30 jours ouvrés** à compter de la notification du bon de commande du pouvoir adjudicateur dans lequel est mentionné la liste des sites à migrer.	Fin de phase 2
Le délai maximum de la **Phase 3 « Pilotes »** est **35 jours ouvrés** à compter de la notification du bon de commande de chaque bénéficiaire dont le pouvoir adjudicateur (Lots 3 à 5 et 7) dans lesquels sont mentionnés la liste des sites à migrer. Ce délai est ajustable selon les conclusions de la Phase 1 « Planification »	Fin de phase 3
Les délais maximums **de rattachement aux points de concentration de collecte** des titulaires **des lots 1 à 5 et 7** sont mentionnés sur le Bordereau des délais (cf. référence [R2]).	En cours de phase 3
Le délai maximum de **migration des sites** qui est le délai de la fin de la Phase 4 « Généralisation » est mentionné sur le Bordereau des délais (cf. référence [R2]). Ce délai ne peut excéder **18 mois calendaires** à compter de la notification du bon de commande de chaque bénéficiaire pour les Lots 1 et 2 dans lesquels sont mentionnés la liste des sites à migrer	Fin de la migration
Le délai maximum de **migration des sites POM sur le nouveau service de transit sécurisé** qui est le délai de la fin de la Phase 4 « Généralisation » est mentionné sur le Bordereau des délais (cf. référence [R2]). Ce délai ne peut excéder **6 mois calendaires** à compter de la notification du bon de commande pour les Lots 3, 4, 5 et 7 dans lesquels sont mentionnés la liste des sites POM	Fin de migration
Le délai maximum de mise en place des **échanges automatisés des fonctions minimales attendues** sont mentionnés sur le Bordereau des délais (cf. référence [R2]). Ce délai ne peut excéder **6 mois calendaires** à compter de la notification de l'accord-cadre pour les fonctions minimales attendues	Fin de la migration
Le délai maximum de mise en place des **échanges automatisés des fonctions complémentaires** sont mentionnés sur le Bordereau des délais (cf. référence [R2]). Ce délai ne peut excéder **19 mois calendaires** à compter de la notification de l'accord-cadre pour les fonctions minimales attendues	Fin de la migration

5.2 Engagements opérationnels des services des lots 1 à 5 et 7

5.2.1 Engagements d'exploitation (incident, planification, supervision)

Description	Fréquence de contrôle
Le support technique du titulaire est joignable (contact d'un intervenant au support) sur la plage de service, soit 24/7	Mensuel
Le taux de détection proactive des incidents (supervision) par les titulaires est d'au-moins 85%	Mensuelle
Le délai de prévenance des opérations planifiées est de **10 jours ouvrés** avant le début des opérations.	Mensuelle
Le titulaire communique en temps réel, sur demande de l'Administration : ▪ Les traces liées aux activités d'administration ou d'exploitation des équipements d'extrémité, notamment les évènements de type AAA/TACACS (échecs et réussites de connexion, commandes exécutées…) ▪ Les traces issues de la journalisation technique des équipements (journaux d'erreur …) ▪ 100% des journaux des activités d'administration et d'exploitation.	Fin de la période demandée

5.2.2 Gestion des évolutions en vie de réseau post-migration

Description	Fréquence de contrôle
Le délai maximum pour réaliser une demande d'**évolution mineure** est de **2 jours ouvrés** à compter de l'envoi de la demande au titulaire.	Mensuelle
Le délai maximum pour réaliser une demande d'**évolution majeure**, entrant dans le cadre de l'unités d'œuvre du poste **« III-a) Mise en service »,** est le délai de **« Mise en service »** mentionné dans le Bordereau des délais (cf. référence [R2]) de chaque titulaire.	Bilan mensuel de chaque demande
Le délai maximum de **réponse/confirmation des demandes de programmation** des opérations sur site en heures non ouvrées est de **2 jours ouvrés**	Bilan mensuel de chaque demande
Le délai maximum d'intervention/**réalisation des demandes de programmation** des **opérations** sur site est de **20 jours ouvrés** à compter de la date de la demande	
Le taux d'échec (service non opérationnel pour une cause imputable au titulaire) sur la mise en service d'un point d'accès est inférieur à 15%	Annuelle
Le taux de respect des délais de livraison d'un point d'accès est au minimum de 80%	Annuelle

Description	Fréquence de contrôle
Au maximum 2% des livraisons ont un retard de plus de 10 jours ouvrés par rapport aux délais attendus	Annuelle
Le délai maximum pour réaliser une **étude préalable du service Multicast par accès** est de **15 jours ouvrés** à compter de la notification du bon de commande	Fin étude
Le délai de déploiement **du service Multicast par accès** est mentionné sur le bon de commande suite à l'étude préalable et en accord avec l'Administration	Fin déploiement
Le délai maximum pour réaliser une étude d'ajout de plateforme de service est de **30 jours ouvrés**	Fin étude
Le délai de déploiement d'une plateforme de service sur un DROM est de **60 jours ouvrés**	Fin déploiement

5.2.3 Engagements sur la relation client

Description	Fréquence de contrôle
Le portail de gestion client du titulaire ainsi que les échanges par API (service Web) sont disponibles 24h/24, 7J/7 à 100% (hors maintenance programmée).	Mensuelle
Le délai d'ouverture d'un ticket est au maximum de 15 minutes sur les plages du support. Ce délai est calculé entre la déclaration d'un incident (Client, supervision…) et l'ouverture d'un ticket.	Mensuelle
Le délai d'accusé réception d'une commande d'achat à partir de son envoi (par mail ou par API d'exploitation) est au maximum de **15 minutes** sur les plages du support.	Mensuelle
Le délai maximum de réponse aux demandes de devis préalable à la passation d'une commande d'achat est de **10 jours ouvrés.**	Mensuelle
Le nombre de **devis rejetés** maximum **par semestre**, en cas d'erreur imputable au titulaire dans son contenu est de **3.**	Semestriel
Le délai maximum **d'enregistrement** de la **commande d'achat** dans le système du titulaire et de l'accessibilité de son suivi est au maximum de **5 jours ouvrés** après l'émission de la commande par l'Administration.	Mensuelle
Toute demande de **rendez-vous** pour réaliser une **visite** de site est réalisée par le titulaire **au moins 5 jours ouvrés** suivant l'enregistrement de la commande dans le système du titulaire.	Mensuelle
Le délai maximum pour **confirmer une date de visite** est de **24 h** à compter de la proposition du bénéficiaire du site.	Mensuelle
Le délai maximum de transmission d'un compte rendu au bénéficiaire et à la DINUM d'une visite sur site est de **2 jours ouvrés**	Mensuelle

Description	Fréquence de contrôle
à compter de la fin de la visite	

5.2.4 Engagements sur la sécurité

Description	Fréquence de contrôle
Le délai maximum de l'actualisation du plan d'assurance sécurité (**PAS**) est de **15 jours ouvrés** à compter de la notification de l'accord-cadre	Fin d'initialisation de l'accord-cadre
Le délai maximum de mise en œuvre du plan d'assurance sécurité (**PAS**) est de **3 mois calendaires** à compter de la notification de l'accord-cadre	Trimestrielle
Le délai maximum de mise en œuvre **du plan de remédiation** est de **10 jours ouvrés** après la constatation des écarts	Trimestrielle

5.2.5 Engagements sur la gouvernance de l'accord-cadre

Description	Fréquence de contrôle
Le titulaire communique l'ensemble des indicateurs nécessaires aux comités au moins **2 jours ouvrés avant** la tenue des comités	Mensuel
Le taux de présence du titulaire aux réunions des comités ou ateliers auxquels le titulaire est convié à participer est d'**au moins 90%**	Mensuel

5.2.6 Engagements sur les portails clients, interfaces et développements spécifiques

Le tableau ci-après décrit les engagements :

- Des interfaces applicatives des échanges automatisés par API ou via le portail client du titulaire ;
- Des éventuels développements spécifiques réalisés en cours d'accord-cadre.

Description	Point de mesure
Les temps de réponse maximum de chaque API est d'une seconde	Écarts constatés à l'usage ou par audit spécifique
Le nombre de requêtes en erreur ou en indisponibilité du service distant est inférieur à 2%	Écarts constatés à l'usage sur une période mensuelle

Description	Point de mesure
Les développements spécifiques font l'objet de mesures de protections particulières en matière de disponibilité, d'intégrité, de confidentialité et de traçabilité : ▪ Absence de faille de cross site *scripting* : Les failles XSS se produisent à chaque fois qu'une application prend des données écrites par l'utilisateur et les envoie à un browser web sans avoir au préalable validé ou codé ce contenu. ▪ Absence de faille d'injection SQL : L'injection se produit quand des données écrites par l'utilisateur sont envoyées à un interpréteur en tant qu'élément faisant partie d'une commande ou d'une requête, sans en contrôler les impacts. ▪ Absence de faille dite « PATH TRAVERSAL » : Les attaques dites « de traversement de répertoires » (en anglais *directory traversal ou path traversal*) consistent à modifier le chemin de l'arborescence dans l'URL afin de forcer le serveur à accéder à des sections du site non autorisées. ▪ Absence d'informations sensibles et/ou modifiables dans le dispositif de gestion des sessions utilisateurs (i.e. – cookies) : Les droits d'accès aux comptes et les jetons de session peuvent être insuffisamment protégés. Un tiers non habilité peut ainsi compromettre les mots de passe, les clefs, ou les jetons d'authentification identités pour s'approprier les identités d'autres utilisateurs. ▪ Absence de bombe logique : Les bombes logiques sont des dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système. Elles sont généralement utilisées dans le but de créer un déni de service. ▪ Absence de données d'authentification qui transitent ou sont stockées en clair (i.e. – identifiant, authentifiant) ou chiffrées avec un algorithme faible : L'obtention de mots de passe en clair et/ou inscrit dans le code est un moyen très simple pour contourner tous les mécanismes de sécurité. ▪ Absence de faille d'inclusion de fichiers : Un code vulnérable à l'inclusion de fichier à distance (RFI - *Remote File Inclusion*) permet à des tiers non habilités d'inclure du code et des données pouvant corrompre l'application et son socle technique. ▪ Absence de référence directe non sécurisée à un objet : Une référence directe à un objet se produit quand l'application expose une référence à un objet d'exécution interne, tel qu'un fichier, un dossier, un enregistrement de base de données, ou	Audit spécifique

Description	Point de mesure
une clef, comme paramètre d'URL ou de formulaire. Les attaquants peuvent manipuler ces références pour avoir accès à d'autres objets sans autorisation. ▪ Absence de faille de *Cross Site Request Forgery* (CSRF) : Une attaque CSRF (*Cross Site Request Forgery*) force le navigateur d'une victime authentifiée à envoyer une demande pré-authentifiée à une application web vulnérable et ainsi d'exécuter sur cette dernière des opérations non souhaitée par l'utilisateur. ▪ Absence de message d'erreur avec des « informations techniques » à destination des utilisateurs : Les applications peuvent involontairement divulguer des informations sur leur configuration, fonctionnement interne, voire des données personnelles. Les attaquants utilisent cette faiblesse pour acquérir des données sensibles ou exploitables pour réaliser des intrusions. ▪ Absence de faille de débordement de tampon : Les attaques par « débordement de tampon » (en anglais « *Buffer overflow* », parfois également appelées dépassement de tampon) ont pour principe l'exécution de code arbitraire par un programme en lui envoyant plus de données qu'il n'est censé en recevoir.	

5.3 Qualité et performance des services des lots 1 à 5 et 7

5.3.1 Débit minimum garanti

Le débit minimum garanti est le débit minimum correspondant à la bande passante commandée de chaque accès.

{PP-L1 à 5 & 7/32}. 5.3.1 : Débit minimum garanti : Description des moyens techniques pour mesurer le débit minimum garantie.

5.3.2 Temps de transit et latence dans le réseau

Le temps de transit de bout en bout, inclut les délais dans les liens d'accès et dans les équipements d'extrémités, quels que soient les débits de raccordements et pour un trajet entre n'importe quels sites de l'Administration.

Etant précisé que le temps de transit de bout en bout s'entend entre deux sites déduction faite des temps de transit hors du périmètre de la responsabilité du titulaire. Pour information les temps de transit des flux transitant par l'épine dorsale

en mode nominal sont de 3 ms maximum et entre 20 et 40 ms sur le réseau de collecte métropole.

La latence est le délai ou temps de réponse (en anglais *delay*) qui caractérise le retard entre l'émission et la réception d'un paquet IP ou d'une trame.

{PP-L1 à 5 & 7/33}. 5.3.2 Temps de transit et latence dans le réseau : Description des moyens techniques pour mesurer le temps de transit de bout en bout.

5.3.3 Taux de perte des paquets IP ou des trames

Le taux de perte des paquets IP ou des trames est la proportion de paquets (ou trames) non reçus ou erronés entre deux accès sur l'ensemble des paquets (ou trames) émis.

L'indicateur de taux de perte de paquets IP ou des trames est mesuré par rapport aux taux de perte sur un itinéraire critique entre deux accès.

Le taux de perte sur un itinéraire est mesuré indépendamment de la charge des accès à condition toutefois que le débit moyen généré entre deux mesures ne soit pas supérieur au plus petit des débits d'extrémité de l'itinéraire.

{PP-L1 à 5 & 7/34}. 5.3.3 Taux de perte des paquets IP ou des trames : Description des moyens techniques pour mesurer le taux de perte des paquets IP ou des trames.

5.3.4 Gigue des paquets IP ou des trames

La gigue est l'écart type des valeurs de temps de transit observés au cours de la mesure entre les deux équipements d'extrémité concernés.

{PP-L1 à 5 & 7/35}. 5.3.4 Gigue des paquets IP ou des trames : Description des moyens techniques pour mesurer la gigue des paquets IP ou des trames.

5.3.5 Engagement sur le niveau de qualité et de performance

En cas de dépassement de l'un des seuils autorisés, les engagements de résolution d'un incident de sévérité 2 (incident majeur) de la Garantie du temps de rétablissement du service (GTR) s'appliquent.

5.3.5.1 Lot 1 et 2 – Collecte

Thème	Description	Fréquence de contrôle
Temps de transit	Les délais de transit aller-retour, respectent à 85%, les temps suivants : ▪ < 90 ms sur la classe DATA	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès

	▪ < 80 ms sur la classe VIDEO ▪ < 50 ms sur la classe VOIX	filaires uniquement)
Taux de perte de paquets IP	Les taux de perte de paquets, respectés à 100%, sont de : ▪ < 0,1 % pour la classe DATA ▪ < 0,05 % pour la classe VIDEO ▪ < 0,03 % pour la classe VOIX	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès filaires uniquement)
Gigue	<10 ms sur 90e percentile	Basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès filaires uniquement)
Débit minimum garanti	Le débit minimum garanti est d'au minimum à 97% de la bande passante de l'accès hors interruption de service (en dehors des liaisons pour lesquelles le débit n'est, par nature, pas garanti, notamment les liaisons FTTH, 4/5G et satellite)	Écarts constatés par sondage basé sur des campagnes de mesure à la demande sur 5 jours ouvrés

5.3.5.2 Lot 3 – Transit Océan Atlantique

Thème	Description	Fréquence de contrôle
Temps de transit	Les délais de transit aller-retour, respectent à 85%, les temps suivants : ▪ < 200 ms sur la classe DATA ▪ < 180 ms sur la classe VIDEO ▪ < 150 ms sur la classe VOIX	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès filaires uniquement)
Taux de perte de paquets IP	Les taux de perte de paquets, respectés à 100%, sont de : ▪ < 0,1 % pour la classe DATA ▪ < 0,05 % pour la classe VIDEO ▪ < 0,03 % pour la classe VOIX	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès filaires uniquement)
Gigue	<10 ms sur 90e percentile	Basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès filaires uniquement)
Débit minimum garanti	Le débit minimum garanti est d'au minimum à 97% de la bande passante de l'accès hors interruption de service	Écarts constatés par sondage basé sur des campagnes de mesure à la demande sur 5 jours ouvrés

5.3.5.3 Lot 4 – Transit Océan Indien

Thème	Description	Fréquence de contrôle
Temps de transit	Les délais de transit aller-retour, respectent à 85%, les temps suivants : ▪ < 200 ms sur la classe DATA ▪ < 180 ms sur la classe VIDEO ▪ < 150 ms sur la classe VOIX	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès filaires uniquement)
Taux de perte de paquets IP	Les taux de perte de paquets, respectés à 100%, sont de : ▪ < 0,1 % pour la classe DATA ▪ < 0,05 % pour la classe VIDEO ▪ < 0,03 % pour la classe VOIX	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès filaires uniquement)
Gigue	<10 ms sur 90e percentile	Basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès filaires uniquement)
Débit minimum garanti	Le débit minimum garanti est d'au minimum à 97% de la bande passante de l'accès hors interruption de service	Écarts constatés par sondage basé sur des campagnes de mesure à la demande sur 5 jours ouvrés

5.3.5.4 Lot 5 – Transit Océan Pacifique

Thème	Description	Fréquence de contrôle
Temps de transit	Les délais de transit aller-retour, respectent à 85%, les temps suivants : ▪ < 300 ms sur la classe DATA ▪ < 280 ms sur la classe VIDEO ▪ < 250 ms sur la classe VOIX	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès fibre optique Entreprise uniquement)
Taux de perte de paquets IP	Les taux de perte de paquets, respectés à 100%, sont de : ▪ < 0,1 % pour la classe DATA ▪ < 0,05 % pour la classe VIDEO ▪ < 0,03 % pour la classe VOIX	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès fibre optique Entreprise uniquement)
Gigue	<10 ms sur 90e percentile	Basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès fibre optique Entreprise uniquement)
Débit minimum garanti	Le débit minimum garanti est d'au minimum à 97% de la bande passante de l'accès hors interruption de service	Écarts constatés par sondage basé sur des campagnes de mesure à la demande sur 5 jours

Thème	Description	Fréquence de contrôle
		ouvrés

5.3.5.5 Lot 7 – Transit sécurisé entre l'Hexagone et Saint Pierre et Miquelon

Thème	Description	Fréquence de contrôle
Temps de transit	Le délai de transit aller-retour est strictement inférieur à 200 ms dans au moins à 85% des cas	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès fibre optique Entreprise uniquement)
Taux de perte de paquets IP	Les taux de perte de paquet sont strictement inférieurs à 0,1%, respectés à 100%	Écarts constatés par sondage basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès fibre optique Entreprise uniquement)
Gigue	<10 ms sur 90e percentile	Basé sur l'envoi d'un paquet de 128 octets entre 2 points d'accès d'un même VPN (accès fibre optique Entreprise uniquement)
Débit minimum garanti	Le débit minimum garanti est d'au minimum à 97% de la bande passante de l'accès hors interruption de service	Écarts constatés par sondage basé sur des campagnes de mesure à la demande sur 5 jours ouvrés

5.4 Engagements sur les prestations de sortie

Description	Fréquence de contrôle
Le délai maximum de la **réversibilité globale en fin d'accord-cadre des lots 1 à 5** mentionné dans le Bordereau des délais (cf. référence [R2]) de chaque titulaire.	Fin de migration de l'accord-cadre
Le délai maximum de r**ésiliation d'un accès** est d'**un mois calendaire** à compter de la date de demande de résiliation.	Bilan mensuel de chaque demande
Le délai maximum de **décommissionnement des équipements** et du câblage d'**un mois calendaire**	

Chapitre 6 : Annexes

6.1 Liste des Exigences

6.1.1 Lot 1 à 5 & 7

{EX-L1 à 5 & 7/01} 1.1.1 Périmètre de l'accord-cadre : Toute communication IP de l'État en dehors du territoire national fera l'objet d'une protection cryptographique « qualifiée » en confidentialité et en intégrité. Cette protection repose sur une des solutions listées dans le catalogue des produits et services qualifiés, agréés et certifiés par l'ANSSI. Elle est mise en œuvre soit par le titulaire du présent marché pour tous les tronçons à sa charge, soit par le pouvoir adjudicateur pour les autres tronçons. 9

{EX-L1 à 5 & 7/02} 3.1.4 Gestion des correctifs de sécurité des équipements d'extrémité : Le titulaire prohibe l'utilisation sur ses plates-formes des systèmes et logiciels obsolètes référencés par le CERTFR. 37

{EX-L1 à 5 & 7/03} 3.1.4 Commandes des équipements d'extrémité mis à la disposition de l'Administration : Le titulaire fournit de manière systématique, les configurations des équipements d'extrémité lors de chaque changement. 39

{EX-L1 à 5 & 7/04} 4.8 Migration des services : L'impact de la migration doit être maîtrisé sur les services réseaux fournis à l'utilisateur final, avec l'objectif d'éviter, à défaut de minimiser, les interruptions de service. 111

{EX-L1 à 5 & 7/05} Gestion des évolutions majeures4.10.2 Gestion des évolutions majeures : Les modifications de l'infrastructure du titulaire non consécutives à une demande d'évolution majeure de la part de l'Administration sont à la charge du titulaire. 124

{EX-L1 à 5 & 7/06} 4.10.3 Gestion des évolutions mineures : Exemples de propositions des évolutions mineures pouvant être soumis à l'acceptation de l'Administration. 126

6.1.2 Lot 1 et 2

{EX-L1 & 2/01} 3.1.4.1 Caractéristiques des équipements d'extrémité : Les équipements disposent des caractéristiques minimales décrites dans le CCTP. 34

{EX-L1 & 2/02} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Le niveau de service de raccordement à un point de concentration de collecte est le niveau « Maximum » avec la garantie d'absence de point individuel de défaillance. 45

{EX-L1 & 2/03} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : En se basant sur le référentiel des Typologies de la sécurisation des infrastructures, description de l'infrastructure pour garantir le niveau service « Maximum » avec la garantie d'absence de point individuel de défaillance. 45

{EX-L1 & 2/04} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : le candidat indique si Les interfaces d'interconnexion de la fibre optique sont compatibles monomode et/ou multimode. 46

{EX-L1 & 2/05} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Les abonnements des connexions des points de concentration de collecte IP de l'épine dorsale du RIE au réseau de collecte IP du titulaire sont inclus dans le prix des forfaits mensuels de chaque abonnement. 47

{EX-L1 & 2/06} 3.2.4 Plan d'adressage IP : Les choix d'ingénierie du titulaire ne contraignent ou ne limitent en aucun cas l'Administration dans la gestion de son plan d'adressage IPv4 et IPv6, en particulier afin d'éviter tout risque de conflit entre les différents partenaires du RIE susceptibles d'avoir faits des choix qui leur sont propres. 52

{EX-L1 & 2/07} 3.2.4 Plan d'adressage IP : Le titulaire respecte strictement les principes de cloisonnement et d'indépendance du plan d'adressage du RIE. 53

{EX-L1 & 2/08} 3.2.7 Etendue et capillarité du réseau du titulaire : Aucun filtrage ni modification des paquets IP n'est réalisé par le service réseau du titulaire sans demande explicite. 54

{EX-L1 & 2/09} 3.2.7 Etendue et capillarité du réseau du titulaire : Le soumissionnaire décrit les mécanismes mis en œuvre pour répondre à cette architecture multi-VPN et les impacts des limitations éventuelles. 54

6.1.3 Lot 3 à 5

{EX-L3 à 5/01} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : le candidat met en œuvre des fibres et connecteurs compatibles avec les routeurs d'épine dorsale du RIE. 48

{EX-L3 à 5/02} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Les équipements du titulaire assurant les interconnexions à l'épine dorsale du RIE sont compatibles et interfaçables avec des équipements de la DINUM. 48

{EX-L3 à 5/03} 3.3 Lots 3, 4 et 5 : Transit sécurisé vers l'Hexagone et entre les territoires ultramarins : Le titulaire prévoit que les solutions proposées soient compatibles avec l'installation et l595959 60

{EX-L3 à 5/04} 3.3.1 Liaisons transocéaniques « Entreprise » : La solution de transit sécurisé implémentée par le titulaire doit garantir la transmission de l'ensemble des paquets entrant dans les tunnels entre la zone ultramarine et la métropole à l'exception des paquets rejetés au niveau des accès télécom locaux (POM ou métropole) pour des raisons de saturation du débit souscrit. Dans ces cas de saturation, les mécanismes de QoS pour prioriser les flux en fonction de leur marquage s'appliquent sur les routeurs d'accès, en particulier pour préserver les paquets supportant les lignes de vie et les protocoles de routage. 60

{EX-L3 à 5/05} 3.3.1 Liaisons transocéaniques « Entreprise » : Le titulaire précise l'architecture réseau détaillée qu'il propose, avec un diagramme (redondance, vérification de l'absence de SPOF, mode dégradé, etc.). La qualité de l'offre est jugée sur la redondance (service nominal) et la résilience (service dégradé) des architectures face aux cas de panne. 61

{EX-L3 à 5/06} 3.3.1 Liaisons transocéaniques « Entreprise » : Le titulaire décrit si les liaisons transocéaniques proposées sont dédiées à des clients « entreprise » ou s'ils transitent d'une manière ou d'une autre par 61. Le cas échéant le titulaire détaille par « tronçon » les contraintes et limites des accès qu'il utilise. Le titulaire fait la distinction entre les zones dans lesquelles il est propriétaire des infrastructures et celles dans lesquelles il s'appuie sur des tiers. 63

{EX-L3 à 5/07} : Le titulaire présente les fonctionnalités détaillées apportées par son service, les technologies mises en œuvre, les principes de redondance mis en œuvre. Le cas échéant, le titulaire détaille son service en fonction des zones géographiques et propose une gamme de débit/dimensionnement adapté. 62

{EX-L3 à 5/08} 3.3.3 Services de chiffrement : Le chiffrement des informations transitant sur le réseau de transport doit être réalisé par des chiffreurs qualifiés au niveau standard par l'ANSSI. 64

{EX-L3 à 5/09} 3.3.3 Services de chiffrement : Le titulaire précise la conformité de l'organisation qu'il met en place avec les dispositions de l'annexe I de l'Instruction Interministérielle n°901. 64

{EX-L3 à 5/10} 3.3.4 MTU : Le titulaire détaille la MTU standard et la MTU maximale qu'il peut proposer sur ses accès en standard. Le cas échéant il précise s'il est possible d'aller au-delà et en précise les coûts (UO complémentaire par exemple). Il décrit les possibilités de paramétrages et les impacts inhérents. Il précise l'applicabilité du « Path MTU Discovery » dans son offre. 64

{EX-L3 à 5/11} 3.3.5 Qualité de service : Le titulaire détaille le cas échéant la mise en œuvre des mécanismes de priorisation de flux (QoS) basés sur les champs DSCP appliqués en entrée sur les liaisons. 64

6.1.4 Lot 6

{EX-L6/01} 3.4 Lot 6 : Management des services : Le soumissionnaire indique l'organisation qu'il compte mettre en place pour la gestion opérationnelle et sous quel délai une équipe projet peut être activée sur demande du pouvoir adjudicateur. 67

6.1.5 Lot 7

{EX-L7/01} 3.4.1 Transit internet : Le titulaire présente les fonctionnalités détaillées apportées par son service, les technologies mises en œuvre, les principes de redondance mis en œuvre. Le cas échéant, le titulaire détaille son service en fonction des zones géographiques de S-P&M et propose une gamme de débit/dimensionnement adapté. 61

{EX-L7/02} 3.4.1 Transit internet : Le chiffrement des informations transitant sur le réseau de transport doit être réalisé par des chiffreurs qualifiés au niveau standard par l'ANSSI. 62

{EX-L7/03} 3.4.1 Transit internet : Le titulaire précise la conformité de l'organisation qu'il met en place avec les dispositions de l'annexe I de l'Instruction Interministérielle n°901. 62

{EX-L7/04} 3.4.2 MTU : Le titulaire détaille la MTU standard et la MTU maximale qu'il peut proposer sur ses accès en standard. Le cas échéant il précise s'il est possible d'aller au-delà et en précise les coûts (UO complémentaire par exemple). Il décrit les possibilités de paramétrages et les impacts inhérents. Il précise l'applicabilité du « Path MTU Discovery » dans son offre. 62

{EX-L7/05} 3.4.4 Protection des accès internet : le titulaire détaille le dispositif anti-DDoS mis en œuvre et les capacités de protection des sites de l'administration couverts par l'offre. 62

6.2 Liste des Points à préciser par le soumissionnaire dans son offre

6.2.1 Lot 1 à 7

{PP-L1 à 7/01} 4.2 Plan d'assurance qualité de l'accord-cadre (PAQ) : Proposition d'un plan type d'assurance qualité de l'accord-cadre. 69

{PP-L1 à 7/02} 4.3 Plan de gestion et d'amélioration continue (PGAC) : Proposition d'un plan de gestion et d'amélioration continue en détaillant notamment les principaux axes, la démarche et la mise en œuvre de l'amélioration continue. 69

{PP-L1 à 7/03} 4.4.2 Respect de la législation et de la règlementation en vigueur et SSI : Présentation sous la forme d'une matrice de la conformité, de l'organisation mise en place en vue de respecter les dispositions de l'annexe 1, intitulée « Règles pour les entités situées hors du champ d'application de la PSSIE », de l'Instruction Interministérielle II 901 (cf. référence [R8]). 71

{PP-L1 à 7/04} 4.4.3.1 Contenu du Plan d'assurance sécurité (PAS) : Proposition d'un Plan type d'Assurance Sécurité. 74

{PP-L1 à 7/05} 4.4.3.2 Modalité d'exécution du Plan d'assurance sécurité (PAS) : Proposition d'une organisation en précisant les fonctions de sécurité générale, de sécurité des systèmes d'information et de sûreté déjà existantes. 74

{PP-L1 à 7/06} 4.7.1 Initialisation de l'accord-cadre : Exemple de planning d'initialisation en précisant le nombre et la nature des ateliers à réaliser avec l'Administration et/ou son assistant à maîtrise d'ouvrage. 102

{PP-L1 à 7/07} 4.7.1 Initialisation de l'accord-cadre : Description des moyens humains et organisationnels mis en œuvre en précisant notamment, les profils pressentis, les expériences dans ce type de projet de migration et les CV types. 102

{PP-L1 à 7/08} 4.7.2 Cadrage du projet de migration des sites : Description des moyens humains et organisationnels mis en œuvre en précisant notamment, les profils pressentis, les expériences dans ce type de projet de migration et les CV types. 104

{PP-L1 à 7/09} 4.7.2 Cadrage du projet de migration des sites : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre. 104

{PP-L1 à 7/10} 4.7.2 Cadrage du projet de migration des sites : Description d'un plan type du plan d'assurance qualité spécifique au projet de migration. 104

{PP-L1 à 7/11} 4.7.2 Cadrage du projet de migration des sites : Propositions pour compléter la démarche proposée. 104

{PP-L1 à 7/12} 4.8.1 Phase 1 « Planification » : Proposition d'une démarche de migration complémentaire et du plan d'action associé en indiquant les principaux jalons associés. 112

{PP-L1 à 7/13} 4.8.1 Phase 1 « Planification » : Description des moyens humains et organisationnels mise en œuvre pour garantir la tenue des délais de cette phase. 112

{PP-L1 à 7/14} 4.8.1 Phase 1 « Planification » : Précision et justification d'éventuelles prérequis nécessaires à la phase. 113

{PP-L1 à 7/15} 4.8.2 Phase 2 « Etude » : Proposition d'une démarche complémentaire et du plan d'action associé en indiquant les principaux jalons associés. 115

{PP-L1 à 7/16} 4.8.2 Phase 2 « Etude » : Description des moyens humains et organisationnels mise en œuvre pour garantir la tenue des délais de cette phase. 115

{PP-L1 à 7/17} 4.8.2 Phase 2 « Etude » : Précision et justification d'éventuelles prérequis nécessaires à la phase. 115

{PP-L1 à 7/18} 4.8.3 Phase 3 « Pilotes » : Proposition d'une démarche complémentaire et du plan d'action associé en indiquant les principaux jalons associés. 118

{PP-L1 à 7/19} 4.8.3 Phase 3 « Pilotes » : Description des moyens humains et organisationnels mise en œuvre pour garantir la tenue des délais de cette phase. 118

{PP-L1 à 7/20} 4.8.3 Phase 3 « Pilotes » : Précision et justification d'éventuelles prérequis nécessaires à la phase. 118

{PP-L1 à 7/21} 4.8.4 Phase 4 » Généralisation » : Proposition d'une démarche complémentaire et du plan d'action associé en indiquant les principaux jalons associés. 121

{PP-L1 à 7/22} 4.8.4 Phase 4 » Généralisation » : Description des moyens humains et organisationnels mise en œuvre pour garantir la tenue des délais de cette phase. 121

{PP-L1 à 7/23} 4.8.4 Phase 4 » Généralisation » : Précision et justification d'éventuelles prérequis nécessaires à la phase. 121

{PP-L1 à 7/24} 4.8.4 Phase 4 » Généralisation » : Précisions des moyens mis en œuvre de l'assistance sur site les personnels de l'Administration aux opérations de recette d'aptitude (VA). 121

{PP-L1 à 7/25} 4.8.4 Phase 4 » Généralisation » : Description des indicateurs du cahier de recette de référence des services. 121

{PP-L1 à 7/26} 4.11.4 Procédure d'escalade : Propositions pour compléter la démarche proposée. 131

{PP-L1 à 7/27} 4.12 Gestion des problèmes : Description des moyens humains et organisationnels mise en œuvre pour la gestion des problèmes. 133

{PP-L1 à 7/28} 4.12 Gestion des problèmes : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre pour la gestion des problèmes. 133

{PP-L1 à 7/29} 4.12 Gestion des problèmes : Proposition d'une démarche pour la gestion des problèmes. 133

{PP-L1 à 7/30} 4.17.1 Prestation d'expertise de la performance : Description de la méthode, des principales activités et des livrables associées. 141

{PP-L1 à 7/31} 4.17.1 Prestation d'expertise de la performance : Proposition des profils types, avec notamment leur niveau de qualification, leurs expériences. 141

{PP-L1 à 7/32} 4.17.1 Prestation d'expertise de la performance : Exemples d'expertises types avec des propositions de métriques pour évaluer la charge de réalisation en jour-homme. 141

{PP-L1 à 7/33} 4.17.2 Prestation de projet d'infrastructure : Description de la méthode, des principales activités et des livrables associées. 142

{PP-L1 à 7/34} 4.17.2 Prestation de projet d'infrastructure : Proposition d'un échantillonnage des profils pressentis, avec notamment leur niveau de qualification dans le poste, leurs expériences dans les projets d'infrastructure. 142

{PP-L1 à 7/35} 4.17.2 Prestation de projet d'infrastructure : Exemples de projets d'infrastructure types avec des propositions de métriques pour évaluer la charge de réalisation basée sur les unités d'œuvre du bordereau des prix 142

6.2.2 Lot 1 à 5 & 7

{PP-L1 à 5 & 7/01} 3.1.1 Confidentialité des informations transportées : Description les moyens mis en œuvre pour garantir le caractère privé des échanges. 32

{PP-L1 à 5 & 7/02} 3.1.4.1 Caractéristiques des équipements d'extrémité : Description des caractéristiques minimales. 34

{PP-L1 à 5 & 7/03} 3.1.4.1 Caractéristiques des équipements d'extrémité : Description des fonctions additionnelles et de leurs caractéristiques. 34

{PP-L1 à 5 & 7/04} 3.1.4.1 Caractéristiques des équipements d'extrémité : Description des équipements en fonction des niveaux d'engagement de service en précisant notamment le fournisseur, le modèle et les dimensions physiques, les configurations logicielles et versions installées. 34

{PP-L1 à 5 & 7/05} 3.1.4.1 Caractéristiques des équipements d'extrémité : Précisions sur les limites techniques et fonctionnelles des équipements. 34

{PP-L1 à 5 & 7/06} 3.1.4.1 Caractéristiques des équipements d'extrémité : Précisions sur l'évolutivité matérielle techniques et fonctionnelles des équipements. 34

{PP-L1 à 5 & 7/07} 3.1.4 Qualité des configurations des équipements d'extrémité : Description de la politique de gestion des configurations des équipements d'extrémité. 36

{PP-L1 à 5 & 7/08} 3.1.4 Procédure de sauvegarde des configurations : Description de la procédure de sauvegarde et de restauration. 36

{PP-L1 à 5 & 7/09} 3.1.4 Gestion des correctifs de sécurité des équipements d'extrémité : Description du maintien et du suivi de l'état technique de parc des équipements en précisant notamment sa fréquence d'actualisation, le moyen de mise à disposition. 37

{PP-L1 à 5 & 7/10} 3.1.4 Administration des équipements d'extrémité : Description de la politique d'administration des équipements. 38

{PP-L1 à 5 & 7/11} 3.1.4 Commandes des équipements d'extrémité mis à la disposition de l'Administration : Description de l'outil de restitution de la configuration de l'interface WAN côté PE en amont 39

{PP-L1 à 5 & 7/12} 3.1.4 Commandes des équipements d'extrémité mis à la disposition de l'Administration : Description des commandes proposées en écriture. 39

{PP-L1 à 5 & 7/13} 3.1.4 Commandes des équipements d'extrémité mis à la disposition de l'Administration : Justification des éventuelles limitations. 39

{PP-L1 à 5 & 7/14} 3.1.4 Gestion des journaux d'exploitation des équipements d'extrémité : Description de l'architecture d'interconnexion sécurisée pour le recueil l'ensemble de ces journaux. 39

{PP-L1 à 5 & 7/15} 3.1.4 Accès en lecture aux configurations par la DINUM : Description des impacts sur les engagements de service d'un accès en écriture sur les équipements d'extrémité. 40

{PP-L1 à 5 & 7/16} 3.1.4 Accès en lecture aux configurations par la DINUM : Justifications des éventuelles limitations d'un accès en écriture sur les équipements d'extrémité. 40

{PP-L1 à 5 & 7/17} 3.1.5.1 Définition des niveaux de sévérité des incidents : Définition des niveaux de complexité « simple », « moyen » et « élevé » des « incidents » de niveau de sévérité 4 (Demande d'information) 44

{PP-L1 à 5 & 7/18} Gestion des évolutions majeures4.10.2 Gestion des évolutions majeures : Exemples de propositions des évolutions majeures pouvant être soumis à l'acceptation de l'Administration. 124

{PP-L1 à 5 & 7/19} 4.10.2 Gestion des évolutions majeures : Exemples de propositions de type d'impact sur l'infrastructure du titulaire pouvant être soumis à l'acceptation de l'Administration. 125

{PP-L1 à 5 & 7/20} 4.11.3.3 Processus 3 « Détection proactive par le titulaire » : Description des mécanismes de détection proactive des incidents. 130

{PP-L1 à 5 & 7/21} 4.11.4 Procédure d'escalade : Précision du niveau hiérarchique des interlocuteurs et leur entité d'appartenance pour chaque niveau hiérarchique (N1 à N4). 130

{PP-L1 à 5 & 7/22} 4.11.5 Organisation du support du titulaire : Description des moyens humains et organisationnels mise en œuvre du support du titulaire. 131

{PP-L1 à 5 & 7/23} 4.11.5 Organisation du support du titulaire : Précision du profil pressenti du référent technique et opérationnel mis à disposition. 131

{PP-L1 à 5 & 7/24} 4.11.6 Supervision réalisée par le titulaire : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre et notamment au niveau des équipements et indicateurs supervisés, des types d'alarmes remontées, des mesures de performance du réseau et des seuils de remontée d'alarmes, des niveaux de sévérité des incidents en fonction des alarmes remontées, de la profondeur de l'historique des informations… 132

{PP-L1 à 5 & 7/25} 4.11.6 Supervision réalisée par le titulaire : Description de l'organisation et des moyens mise en œuvre pour réaliser la supervision. 132

{PP-L1 à 5 & 7/26} 4.13 Gestion des opérations planifiées : Description des procédures et moyens de diffusion des notifications des opérations planifiées. 133

{PP-L1 à 5 & 7/27} 4.13 Gestion des opérations planifiées : Précision sur les procédures utilisées pour sécuriser les opérations planifiées telles que les procédures, les tests des secours ainsi que leur fréquence et les procédures de retour arrière. 134

{PP-L1 à 5 & 7/28} 4.16 Gestion des performances : Précisions des éléments techniques nécessaire à l'audit, mis à disposition de l'Administration ou du tiers mandaté et des délais associés. 140

{PP-L1 à 5 & 7/29} 4.18 Réversibilité globale en fin d'accord-cadre : Description des différentes étapes identifiées de la démarche de réversibilité pour un basculement progressif du réseau du titulaire sortant avec les livrables associés. 145

{PP-L1 à 5 & 7/30} 4.18 Réversibilité globale en fin d'accord-cadre : Description des moyens humains et organisationnels pour assurer le bon déroulement de la phase de réversibilité. 145

{PP-L1 à 5 & 7/31} 4.18 Réversibilité globale en fin d'accord-cadre : Description des principes de la continuité des services pendant la phase de réversibilité et des procédures de retour en arrières. 145

{PP-L1 à 5 & 7/32} 5.3.1 : Débit minimum garanti : Description des moyens techniques pour mesurer le débit minimum garantie. 152

{PP-L1 à 5 & 7/33} 5.3.2 Temps de transit et latence dans le réseau : Description des moyens techniques pour mesurer le temps de transit de bout en bout. 153

{PP-L1 à 5 & 7/34} 5.3.3 Taux de perte des paquets IP ou des trames : Description des moyens techniques pour mesurer le taux de perte des paquets IP ou des trames. 153

{PP-L1 à 5 & 7/35} 5.3.4 Gigue des paquets IP ou des trames : Description des moyens techniques pour mesurer la gigue des paquets IP ou des trames. 153

6.2.3 Lot 1 et 2

{PP-L1 & 2/01} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Précision des mécanismes de bascule des flux entre le point de concentration nominal et les points de concentration de secours. 45

{PP-L1 & 2/02} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Le cas échéant une description du mécanisme permettant le partage de charge entre les deux points de concentration. 45

{PP-L1 & 2/03} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Description de la politique de prise en compte des différentes hypothèses d'évolution des besoins, notamment en matière de débit. 46

{PP-L1 & 2/04} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Description du modèle et des caractéristiques des équipements et notamment la taille des équipements et leur consommation électrique. 46

{PP-L1 & 2/05} 3.1.6 Raccordement de la POM au réseau de collecte multi-VPN : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre de supervision et l'exploitation des flux des points de concentration et notamment au niveau : - des indicateurs fournis, - des mécanismes et des outils, - des types d'alarmes remontées. 47

{PP-L1 & 2/06} 3.2.3 : Spécifications du réseau privé virtuel (VPN) : Description des mécanismes mis en œuvre permettant d'ajouter ou de supprimer des VPN et précision des limitations éventuelles sur les performances techniques et économiques. 52

{PP-L1 & 2/07} 3.2.3 : Spécifications du réseau privé virtuel (VPN) : Description des mécanismes mis en œuvre de propagation des VPN sur le LAN et précision des limitations éventuelles sur les performances techniques et économiques. 52

{PP-L1 & 2/08} 3.2.4 Plan d'adressage IP : Description des principes de reprise du plan d'adressage permettant de respecter le cloisonnement et l'indépendance du plan d'adressage du RIE. 53

{PP-L1 & 2/09} 3.2.6 Services IPv4 et IPv6 : Précisions sur la fourniture du service IPv4 et IPv6. 53

{PP-L1 & 2/10} 3.2.7 Etendue et capillarité du réseau du titulaire : Description de l'étendue et de la capillarité du service de collecte. 54

{PP-L1 & 2/11} 3.2.7 Etendue et capillarité du réseau du titulaire : Description du maillage des réseaux de collecte en précisant notamment sa redondance. 54

{PP-L1 & 2/12} 3.2.7 Etendue et capillarité du réseau du titulaire : Précisions des zones propriétaires des infrastructures. 54

{PP-L1 & 2/13} 3.2.7 Etendue et capillarité du réseau du titulaire : Précisions des zones non-propriétaires des infrastructures, le cas échant, description de maîtrise contractuelle des tiers propriétaires des infrastructures. 54

{PP-L1 & 2/14} 3.2.7 Etendue et capillarité du réseau du titulaire : Précisions du nombre de points de concentration sur les zones propriétaires et de leur capacité à être redondé. 54

{PP-L1 & 2/15} 3.2.8 Spécifications sur les accès mobiles et satellites : La technologie satellite peut être en orbite basse ou géostationnaire. Le titulaire propoest au moins une offre Française ou Européenne sous condition d'éligibilité du territoire. 55

{PP-L1 & 2/16} 3.2.9 Qualité de services « QoS » : Description de la mise en œuvre des classes de service en pourcentage des profils du tableau ci-avant, quel que soit la bande passante. 57

{PP-L1 & 2/17} 3.2.9 Qualité de services « QoS » : Description de la prise en compte de l'évolutivité ou de l'enrichissement des politiques, de marquage des flux pour chaque VPN client, de l'Administration, en cours d'accord-cadre. 57

{PP-L1 & 2/18} 3.2.10 Voix et vidéo sur IP : Description des limitations notamment pour : - les tailles de *payload* de la classe de service « voix », - la possibilité de faire cohabiter plusieurs codecs simultanément et le cas échéant des tailles de *payload* propres à chaque codec. 57

{PP-L1 & 2/19} 3.2.10 Voix et vidéo sur IP : Description des règles d'ingénierie des accès spécifiques voix sur IP en précisant notamment : - les types d'accès éligibles à la VoIP (technologie en fonction de l'éligibilité, granularité des débits offerts…), - le taux maximum d'utilisation du débit nominal de l'accès, en fonction des classes de services implémentées (CoS). 57

{PP-L1 & 2/20} 3.2.10 Voix et vidéo sur IP : Précisions, le cas échéant, des limitations ou contraintes pour l'allocation de la quasi-totalité débit de l'accès (ou du VPN au sein d'un accès sub-VPN) au service voix ou vidéo. 58

{PP-L1 & 2/21} 3.2.11 Multicast : Description de la démarche de l'étude préalable du service « Multicast » par accès en précisant : les caractéristiques de l'offre, les types de protocole implémentés, le nombre maximum de routes par défaut, le type de route (statique, dynamique), le nombre maximum de routes par tunnel, les moyens qui sont mis en œuvre pour filtrer les routes afin de protéger les équipements d'extrémité (explosion des routes), les techniques mises en œuvre pour mettre en place la sélection d'un sous-ensemble de groupes de diffusion, les impacts à tout point de vue sur IPv4 et IPv6... 58

{PP-L1 & 2/22} 3.2.11 Multicast : Description des impacts éventuels sur les équipements d'extrémité. 58

{PP-L1 & 2/23} 3.2.11 Multicast : Justification des éventuels coûts additionnels à l'abonnement du service de transport de flux. 58

{PP-L1 & 2/24} 4.7.3.1.2 Modalités de mise en œuvre des API : Description du macro-planning de déploiement de la mise en œuvre progressive des échanges automatisés des fonctionnalités minimales et complémentaires. 106

{PP-L1 & 2/25} 4.7.3.1.2 Modalités de mise en œuvre des API : Description du macro-planning de déploiement de la mise en œuvre « immédiate » du portail client type « Web » des fonctionnalités minimales et complémentaires. 106

{PP-L1 & 2/26} 4.7.3.3 Sécurisation des échanges automatisés : Description de l'interconnexion sécurisée entre le SI-RIE de l'Administration et le système d'information du titulaire. 106

{PP-L1 & 2/27} 4.7.3.4 Echanges automatisés du volet technique des commandes d'achat : Présentation des fonctionnalités automatisées par API minimales attendues. 107

{PP-L1 & 2/28} 4.7.3.4 Echanges automatisés du volet technique des commandes d'achat : Présentation des fonctionnalités automatisées par API complémentaires. 107

{PP-L1 & 2/29} 4.7.3.4 Echanges automatisés du volet technique des commandes d'achat : Présentation des fonctionnalités minimales attendues du Portail client type « web ». 107

{PP-L1 & 2/30} 4.7.3.4 Echanges automatisés du volet technique des commandes d'achat : Présentation des fonctionnalités complémentaires du Portail client type « web ». 107

{PP-L1 & 2/31} 4.7.3.5 Echanges automatisés de la gestion des incidents : Présentation des fonctionnalités automatisées par API minimales attendues. 109

{PP-L1 & 2/32} 4.7.3.5 Echanges automatisés de la gestion des incidents : Présentation des fonctionnalités automatisées par API complémentaires. 109

{PP-L1 & 2/33} 4.7.3.5 Echanges automatisés de la gestion des incidents : Focus sur les fonctionnalités liées à la remonté de manière automatisée par API des informations et alertes de supervision. 109

{PP-L1 & 2/34} 4.7.3.5 Echanges automatisés de la gestion des incidents : Focus sur les fonctionnalités liées à la remonté de manière automatisée par API des indicateurs quotidiens, hebdomadaires, bimensuels et mensuels. 109

{PP-L1 & 2/35} 4.7.3.5 Echanges automatisés de la gestion des incidents : Présentation des fonctionnalités minimales attendues du Portail client type « web ». 109

{PP-L1 & 2/36} 4.7.3.5 Echanges automatisés de la gestion des incidents : Présentation des fonctionnalités complémentaires du Portail client type « web ». 109

{PP-L1 & 2/37} 4.7.3.5 Echanges automatisés de la gestion des incidents : Focus sur les fonctionnalités liées à la remonté de manière automatisée par API de la supervision et de l'exploitation des flux des points de concentration des portes de collecte opérateur. 109

{PP-L1 & 2/38} 4.7.3.6 Echanges automatisés de la gestion des configurations des équipements d'extrémité : Présentation des fonctionnalités minimales attendues automatisées par API avec leur calendrier de mise en œuvre. 110

{PP-L1 & 2/39} 4.7.3.6 Echanges automatisés de la gestion des configurations des équipements d'extrémité : Présentation des fonctionnalités complémentaires automatisées par API avec leur calendrier de mise en œuvre. 110

6.2.1 Lot 3 à 5

{PP-L3 & 5/01} 1.1.3.2 Prestations de transit sécurisé (lots 3, 4 et 5) : Le soumissionnaire répond au besoin de l'Administration en proposant des solutions techniques au niveaux de la POM et de l'interconnexion à l'épine dorsale. En fonction des choix technologiques retenus, le transit sécurisé est amené à transporter différentes natures de flux sans impact sur la qualité ressentie par les utilisateurs. 15

{PP-L3 & 5/02} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Description de la politique de prise en compte des différentes hypothèses d'évolution des besoins, notamment en matière de débit (sur la partie chiffrement et réseau de transport). 48

{PP-L3 & 5/03} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Le choix du mode de raccordement et des services déployés est arbitré par la DINUM au lancement de l'accord-cadre en fonction de l'implémentation des sites d'hébergement et de l'architecture globale proposée par le titulaire. 49

{PP-L3 & 5/04} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Description du modèle et des caractéristiques des équipements et notamment la taille des équipements et leur consommation électrique. 49

{PP-L3 & 5/05} 3.1.7 Rattachement des POM aux fournisseurs de transits sécurisés : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre, de supervision et d'exploitation des flux des points de concentration et notamment au niveau : - Des indicateurs fournis ; - Des mécanismes et des outils ; - Des types d'alarmes remontées. 50

{PP-L3 & 5/06} 3.3.1 Liaisons transocéaniques « Entreprise » : Pour répondre à ce besoin, le soumissionnaire propoest la topologie de liaisons qui lui semble optimale pour l'ensemble de la durée d'exécution du marché. 61

{PP-L3 & 5/07} 3.3.3 Services de chiffrement : Le soumissionnaire propose des solutions techniques en argumentant les avantages et inconvénients de chaque scénario. 65

6.2.2 Lot 6

{PP-L6/01} 1.1.2.6 Lot 6 : Management des services : Une coordination rapprochée est donc nécessaire entre ces deux familles d'acteurs afin que les opérations se déroulent au mieux. La réponse au lot 6 de cet appel d'offre doit apporter des explications détaillées sur la méthode et les moyens mis en œuvre par le titulaire pour répondre à cette demande du pouvoir adjudicateur. 14

{PP-L6/02} 4.6.1 Initialisation du Lot : Exemple de planning d'initialisation en précisant le nombre et la nature des ateliers à réaliser avec l'Administration et/ou son assistant à maîtrise d'ouvrage. 87

{PP-L6/03} 4.6.1 Initialisation du Lot : Description des moyens humains et organisationnels mis en œuvre en précisant notamment, les profils pressentis, les expériences dans ce type de projet de migration et les CV types. 88

{PP-L6/04} 4.6.1 Initialisation du Lot : Proposition de modalités d'échanges avec les titulaires des lots 1 à 5, à soumettre à l'approbation de l'Administration pour la préparation des comités de la gouvernance de l'accord-cadre et le *reporting* des activités liées aux services. 88

{PP-L6/05} 4.6.2.1 Cadrage du projet de migration des sites : Description des moyens humains et organisationnels mis en œuvre en précisant notamment, les profils pressentis, les expériences dans ce type de projet de migration et les CV types. 90

{PP-L6/06} 4.6.2.1 Cadrage du projet de migration des sites : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre. 90

{PP-L6/07} 4.6.2.1 Cadrage du projet de migration des sites : Description d'un plan type du plan d'assurance qualité spécifique au projet de migration. 91

{PP-L6/08} 4.6.2.1 Cadrage du projet de migration des sites : Propositions pour compléter la démarche proposée. 91

{PP-L6/09} 4.6.2.2 Assistance au pilotage des migrations : Propositions de l'organisation à mettre en œuvre, pour chacune des phases (Phase 1 « Planification », Phase 2 « Etude », Phase 3 « Pilotes » et Phase 4 « Généralisation ») en précisant les profils selon l'annexe [A9] « Nomenclature CIGREF des métiers du système d'information ». Les propositions prennent en compte - les quantités estimatives du nombre de sites à migrer, - d'un calendrier de déploiement sur 18 mois, - de ratio globaux selon les types de migration des sites, qui sont soit * techniques en cas de changement de technologie et/ou de titulaire, * administratives en cas de reconduction du titulaire sortant. Les propositions d'organisation sont à réalisées pour les ratios suivants - la migration des sites est une migration à 100% technique, - la migration des sites est une migration à 75% technique et à 25% administrative, - la migration des sites est une migration à 50% technique et à 50% administrative, - la migration des sites est une migration à 25% technique et à 75% administrative.97

{PP-L6/10} 4.6.2.2 Assistance au pilotage des migrations : Précisions sur les délais de mobilisation des profils mentionnés dans la réponse du point à préciser {PP-L6/09} en vue de respecter les délais de chacune des phases.97

{PP-L6/11} 4.6.2.2 Assistance au pilotage des migrations : Focus sur les profils pressentis, pour assister l'Administration à l'expertise et/ ou l'analyser des spécifications techniques et des solutions mise en œuvre par les titulaires des lots 1 à 5, avec notamment leur niveau de qualification dans le poste et leurs expériences dans les projets de migration réseau.97

{PP-L6/12} 4.6.2.2 Assistance au pilotage des migrations : Focus sur les profils pressentis, pour assister l'Administration à la préparation et la réalisation des vérifications (recette) des sites, avec notamment leur niveau de qualification dans le poste et leurs expériences dans les projets de migration réseau.97

{PP-L6/13} 4.6.2.2 Assistance au pilotage des migrations : Proposition pour chaque autre type de profils pressentis, d'un échantillonnage des profils, avec notamment leur niveau de qualification dans le poste, leurs expériences dans l'assistance au pilotage des projets de migration réseau.98

{PP-L6/14} 4.6.2.2 Assistance au pilotage des migrations : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre.98

{PP-L6/15} 4.6.2.2 Assistance au pilotage des migrations : Propositions pour compléter la démarche proposée.98

{PP-L6/16} 4.6.2.2 Assistance au pilotage des migrations : Exemples de tableaux de bord avec des explications sur les éléments complémentaires.98

{PP-L6/17} 4.6.2.2 Assistance au pilotage des migrations : Précisions sur la fourniture d'outils de restitution des tableaux de bord et du suivi du projet de migration.98

{PP-L6/18} 4.6.2.2 Assistance au pilotage des migrations : Proposition d'outils de collecte des indicateurs de gouvernance pour les titulaires des lots 1 à 5.98

{PP-L6/19} 4.6.3 Pilotage lors de la phase opérationnelle du service : Présentation des hypothèses de dimensionnement des moyens humains et organisationnels à mettre en œuvre pour l'assitance au pilotage des quantités estimatives de sites du chapitre 2.2.104

{PP-L6/20} 4.6.3 Pilotage lors de la phase opérationnelle du service : Précisions sur les délais de mobilisation des profils mentionnés dans la réponse du point à préciser {PP-L6/19}.104

{PP-L6/21} 4.6.3 Pilotage lors de la phase opérationnelle du service : Focus sur les profils pressentis, pour assister l'Administration à l'expertise et/ ou l'analyser des spécifications techniques et des solutions proposées par les titulaires des lots 1 à 5, avec notamment leur niveau de qualification dans le poste et leurs expériences dans les projets d'infrastructure réseau.104

{PP-L6/22} 4.6.3 Pilotage lors de la phase opérationnelle du service : Précisions sur les délais de mobilisation des profils mentionnés dans la réponse du point à préciser {PP-L6/21}.104

{PP-L6/23} 4.6.3 Pilotage lors de la phase opérationnelle du service : Focus sur les profils pressentis, pour assister l'Administration à la préparation et la réalisation des vérifications (recette) des sites, avec notamment leur niveau de qualification dans le poste et leurs expériences dans les projets d'infrastructure réseau.104

{PP-L6/24} 4.6.3 Pilotage lors de la phase opérationnelle du service : Précisions sur les délais de mobilisation des profils mentionnés dans la réponse du point à préciser {PP-L6/23}.104

{PP-L6/25} 4.6.3 Pilotage lors de la phase opérationnelle du service : Proposition pour chaque autre type de profils pressentis, d'un échantillonnage des profils, avec notamment leur niveau de qualification dans le poste, leurs expériences dans l'assistance au pilotage opérationnel des réseaux.104

{PP-L6/26} 4.6.3 Pilotage lors de la phase opérationnelle du service : Description des moyens techniques (outils informatiques et/ou méthodologiques) mis en œuvre.104

{PP-L6/27} 4.6.3 Pilotage lors de la phase opérationnelle du service : Propositions pour compléter la démarche proposée.104

{PP-L6/28} 4.6.3 Pilotage lors de la phase opérationnelle du service : Propositions pour compléter le tableau de bord avec un exemple pour illustrer le tableau de bord et des explications sur les éléments complémentaires.104

{PP-L6/29} 4.6.3 Pilotage lors de la phase opérationnelle du service : Précisions sur la fourniture d'outils de restitution des tableaux de bord et du suivi du pilotage.104

{PP-L6/30} 4.6.3 Pilotage lors de la phase opérationnelle du service : Proposition d'outils de collecte des indicateurs de gouvernance pour les titulaires des lots 1 à 5.105