



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)

**Accord-cadre interministériel relatif au transit
internet zone nord en métropole pour le
réseau interministériel de l'État (RIE)**

Table des matières

Préambule

1	Introduction	7
1.1	Présentation de la DINUM.....	7
2	Le réseau interministériel de l'état	8
2.1	La genèse du RIE	8
2.2	La stratégie du RIE	9
2.3	Les briques de services du RIE	10
2.4	L'épine dorsale et le transit internet.....	11
2.5	Les services internet	12
3	Expression des besoins fonctionnels et techniques	13
3.1	Objet du document	13
3.2	L'environnement technique de l'accord-cadre	13
3.3	Périmètre de l'accord-cadre	13
3.4	Le mémoire technique détaillé	16
3.5	Infrastructures du titulaire	16
3.5.1	Architecture du Backbone Internet.....	16
3.5.2	Conformité	17
3.6	Service de transit Internet.....	17
3.7	Service anti-DDoS	18
3.7.1	Généralités	18
3.7.2	Utilisateurs et connexions	18
3.7.3	Spécifications du dispositif attendu	18
3.7.4	Contre-mesures.....	19

3.7.5	CTI.....	19
3.7.6	Flowspec.....	19
3.7.7	Alerting	19
3.7.8	Maintenance et sauvegardes	20
3.7.9	Interface Machine to Machine (API)	20
3.7.10	Exploitation	20
3.8	Accès extranet	21
4	Déploiement du service	22
4.1	Organisation et pilotage du projet	22
4.1.1	Organisation du pouvoir adjudicateur	22
4.1.2	Organisation du titulaire	22
4.1.3	Instances de pilotage.....	23
4.2	Définitions et méthodes.....	27
4.2.1	Format des livrables	27
4.2.2	Déploiement.....	28
4.2.3	Vérification d’aptitude (VA)	28
4.2.4	Vérification de service régulier (VSR).....	30
4.3	Etapes du projet	30
4.3.1	Étape 1 : Lancement du projet	30
4.3.2	Étape 2 : Etude et spécifications	31
4.3.3	Étape 3 : Livraison	32
4.4	Planning de déploiement	34
5	Gestion opérationnelle	35
5.1	Organisation	35
5.1.1	Organisation du pouvoir adjudicateur	35

5.1.2	Organisation attendue du titulaire	35
5.2	Instance de pilotage	35
5.3	Support client	35
5.4	Supervision	37
5.5	Gestion des incidents	37
5.5.1	Classification des incidents et moyens mis en œuvre	37
5.5.2	Procédures et outils	38
5.6	Gestion des évolutions	38
5.7	Gestion des problèmes.....	39
5.8	Gestion des configurations des équipements d'extrémité	39
5.8.1	Qualité des configurations	39
5.8.2	Validation des configurations.....	39
5.8.3	Administration des équipements par le titulaire	40
5.8.4	Procédure de sauvegarde des configurations.....	40
5.8.5	Information sur les configurations	40
5.9	Suivi de la qualité de service	41
5.10	Suivi des mitigations anti-DDoS.....	41
5.11	Reporting	41
5.12	Reporting des mitigations anti-DDoS	42
6	Engagements	43
6.1	Garantie de délai de mise en service d'un lien	43
6.2	Garantie de délai de mise en œuvre des évolutions.....	44
6.3	Garantie de mise en œuvre des tâches d'exploitation	44
6.4	Disponibilité du service	44
6.5	Garantie de temps de rétablissement.....	45

6.6	Bande passante garantie	45
6.7	Garantie de protection Anti-DDoS	45
7	Expertise technique et accompagnement à la mitigation (UO type 4) 47	
7.1	Formation et transfert de compétences à l’outil de mitigation. (UO 4.0)	47
7.2	Expertise technique et diagnostic de flux (UO 4.1).....	47
8	Description des prestations	48
8.1	UOs de type 1	48
8.2	UO de type 2.....	48
8.3	UO de type 3.....	49
8.4	UO de type 4.....	49
9	Glossaire	50
10	Annexes	52
10.1	Adresse des POP du RIE v2	52
10.2	Historique - Caractérisation des configurations, alertes et attaques	52
10.3	Tiers Transit IP : de niveau Tier 1 au niveau Tier 3.....	52
10.4	Configuration des peering des titulaires actuels.....	53

PREAMBULE

Dans la suite du document, sont mentionnés des marqueurs EX et PP.

Les marqueurs « EX » désignent les exigences obligatoires qui doivent être satisfaites par le soumissionnaire. À défaut, son offre sera déclarée irrégulière.

Les marqueurs « PP » correspondent aux points devant être précisés par le soumissionnaire. Ils ne présentent pas de caractère obligatoire, mais sont pris en compte dans l'évaluation et la notation de l'offre.

1 INTRODUCTION

Présentation de la DINUM

La direction interministérielle du numérique (DINUM), rattachée aux Services du Premier Ministre, a été créée par [le décret du 25 octobre 2019](#).

Elle a pour mission d'élaborer la stratégie numérique de l'État et de piloter sa mise en œuvre. Elle exerce aussi les missions de « chief data officer » et de DRH du numérique de l'État.

En tant que cheffe de file du numérique de l'État, elle a pour objectif de rendre l'État plus efficace, plus simple et plus souverain grâce au numérique et collabore à cet effet avec l'ensemble des directions numériques des ministères et ses partenaires.

Elle est placée sous l'autorité conjointe du Premier ministre et du ministre de l'action publique, de la simplification et de la transformation de l'action publique.

Elle est également à la disposition du ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique dans le cadre de l'exercice de ses attributions relatives au numérique (<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047478124>)

La DINUM accompagne les ministères dans leur transformation numérique, conseille le gouvernement et développe des services et ressources partagées comme le réseau interministériel de l'État, FranceConnect, data.gouv.fr ou api.gouv.fr.

Elle pilote, avec l'appui des ministères, le programme d'accélération de la transformation numérique du service public.

La DINUM comprend un département en charge des « Infrastructures et Services Opérés » (DINUM/ISO) qui conçoit, pilote et opère des services d'infrastructures à valeur ajoutée mutualisés entre les administrations, dont le Réseau Interministériel de l'Etat (RIE).

2 LE RESEAU INTERMINISTERIEL DE L'ETAT

La genèse du RIE

Le conseil des ministres du 25 mai 2011 a décidé de la mise en place d'un réseau interministériel sécurisé regroupant l'ensemble des réseaux des ministères et permettant la continuité de l'action gouvernementale en cas de dysfonctionnement grave d'Internet.

Le réseau interministériel de l'Etat intégrera à la cible les différents besoins ministériels en offrant une connectivité inter-sites à haut débit et à haute disponibilité. Ce réseau sera le support d'applications fédératrices interministérielles ainsi que d'applications métiers ministérielles. Il vise à terme à remplacer l'ensemble des réseaux ministériels.

Les objectifs associés sont d'une part, de gagner en efficience par rapport aux réseaux ministériels en « silo », en rationalisant leur exploitation d'un point de vue économique et organisationnel et en mettant en place des services interministériels fédérateurs, et d'autre part d'augmenter la résilience vis-à-vis d'attaques, de malveillance, de pannes.

La mise en place du réseau interministériel de l'Etat s'inscrit dans le double contexte de la réforme 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.

Le réseau interministériel de l'Etat se repose sur les principes suivants :

- des choix technologiques pérennes : cœur du réseau à haut débit, protocoles de réseau évolutif IPv4 & 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 existants voire en anticipation ;
- des services associés construits progressivement : accès à Internet et services de mobilité et de nomadisme présents dès la construction du réseau interministériel ; mise en œuvre concomitante d'autres services applicatifs tels que messagerie, annuaire, partage de fichiers, etc. ;
- un contrôle effectif des éléments clés : maîtrise d'ouvrage forte par la DINUM pour assurer le pilotage et garantir la maîtrise du réseau ; exploitation étatique des éléments de sécurité permettant la défense en profondeur ; externalisation de

l'administration des équipements du cœur en étape de mise en place (qui pourra ensuite être confiée à un opérateur ministériel ou interministériel).

Le RIE transporte des « flux critiques » et la tendance devrait se renforcer.

Le backbone RIE est doté d'une double boucle optique d'une capacité nominale de 100GE.

La gestion de ce réseau et ses évolutions sont confiées à la DINUM/ISO.

Aujourd'hui l'ensemble des ministères dispose d'un ou plusieurs réseaux propres ; certains regroupements ont par ailleurs été faits dans le cadre de marchés communs.

Ces réseaux sont nationaux et peuvent regrouper différentes communautés souvent séparées en plusieurs VPN avec, selon les cas, la mise en œuvre de droits d'accès stricts.

Les réseaux ministériels sont interconnectés au travers du réseau d'interconnexion AdER. Les plans d'adressage ne sont, dans la majorité des cas, pas compatibles, ce qui nécessite des opérations de réécriture d'adresses de réseau dans un référentiel global permettant les échanges entre sites ne dépendant pas d'un même ministère.

La stratégie du RIE

Le réseau interministériel de l'Etat constitue le réseau de transport unifié pour l'ensemble des ministères.

Le cœur du RIE est un réseau haut débit de transport multiservices sur le territoire français, à très haut niveau de résilience et de sécurité, indépendant vis-à-vis d'Internet.

Il doit faciliter les échanges interministériels tout en garantissant la disponibilité, l'intégrité, la traçabilité et la confidentialité des informations et des échanges.

L'architecture du RIE découle de ses objectifs en termes d'efficience pour les échanges inter ministériels, de sécurité, de résilience, de souplesse et d'évolutivité.

Ainsi le cœur du RIE est composé d'un backbone, IPv4 et prêt pour IPv6, maillant les grandes villes de France métropolitaine en Fibre Optique Noire (FON).

Les points de présence de ce backbone, appelés les routeurs d'épine dorsale ou RED, interconnectent l'ensemble des réseaux de collecte permettant le raccordement de l'ensemble des sites ministériels, ainsi que les réseaux externes.

Les réseaux de collecte IP et Ethernet sont gérés par deux opérateurs nationaux dont les réseaux sont multi-raccordés à l'épine dorsale du RIE.

L'accès Internet est réalisé à travers des points de transit internet rattachés à des routeurs d'épine dorsale et permettant d'assurer une résilience complète. Le pouvoir adjudicateur

dispose de son propre numéro de système autonome internet et dispose de larges plages d'adresses IPv4 et IPv6 publiques protégées des attaques par des mécanismes Anti-DDoS.

Les plates-formes Internet et plates-formes d'accès externes, assurant des fonctionnalités de sécurité et de filtrage, sont réparties physiquement sur les POP.

Les briques de services du RIE

Le RIE est composé de plusieurs briques fonctionnelles qui font, pour la plupart, l'objet de procédures et de marchés indépendants.

Pour donner une vision globale au titulaire, le RIE est composé :

- d'une brique de service « Transport Optique » interconnectant les RED du RIE à une infrastructure à haut débit, fournissant des longueurs d'onde sur tout le territoire de France métropolitaine ;
- d'une brique de service « Epine Dorsale » qui correspond aux équipements de niveau Ethernet et IP et aux prestations nécessaires au déploiement et à l'exploitation de ces équipements ;
- d'une brique de service de « Transit Internet » qui permet de connecter le RIE à Internet à travers deux opérateurs de transit internet sur plusieurs points distincts ;
- d'une brique de service « Plates-formes Internet et plates-formes d'accès externes » qui correspond aux équipements de sécurité et de filtrage et aux prestations nécessaires au déploiement et à l'exploitation des plates-formes Internet et plates-formes d'accès externes ;
- d'une brique de service « Réseaux de collecte IP et Ethernet en métropole » qui assure les services de réseaux IP pour les sites du pouvoir adjudicateur en métropole et les services de réseaux Ethernet pour les sites du pouvoir adjudicateur en métropole;
- d'une brique de service « Réseaux de collecte IP en Outre-Mer » qui assure les services de réseaux IP pour les sites du pouvoir adjudicateur dans les DROM-COM ;

Les services et outils pour l'hypervision sont assurés par les équipes NOC RIE/CSIRT-SOC RIE, /SI RIE. Ils permettent d'assister le pouvoir adjudicateur dans les opérations de vérification des déploiements des réseaux de collecte, d'avoir une vision globale de l'ensemble des briques de services du RIE en termes de supervision et d'assurer un service de support centralisé constituant l'interface entre les supports de toutes ces briques de services et le pouvoir adjudicateur.

L'épine dorsale et le transit internet

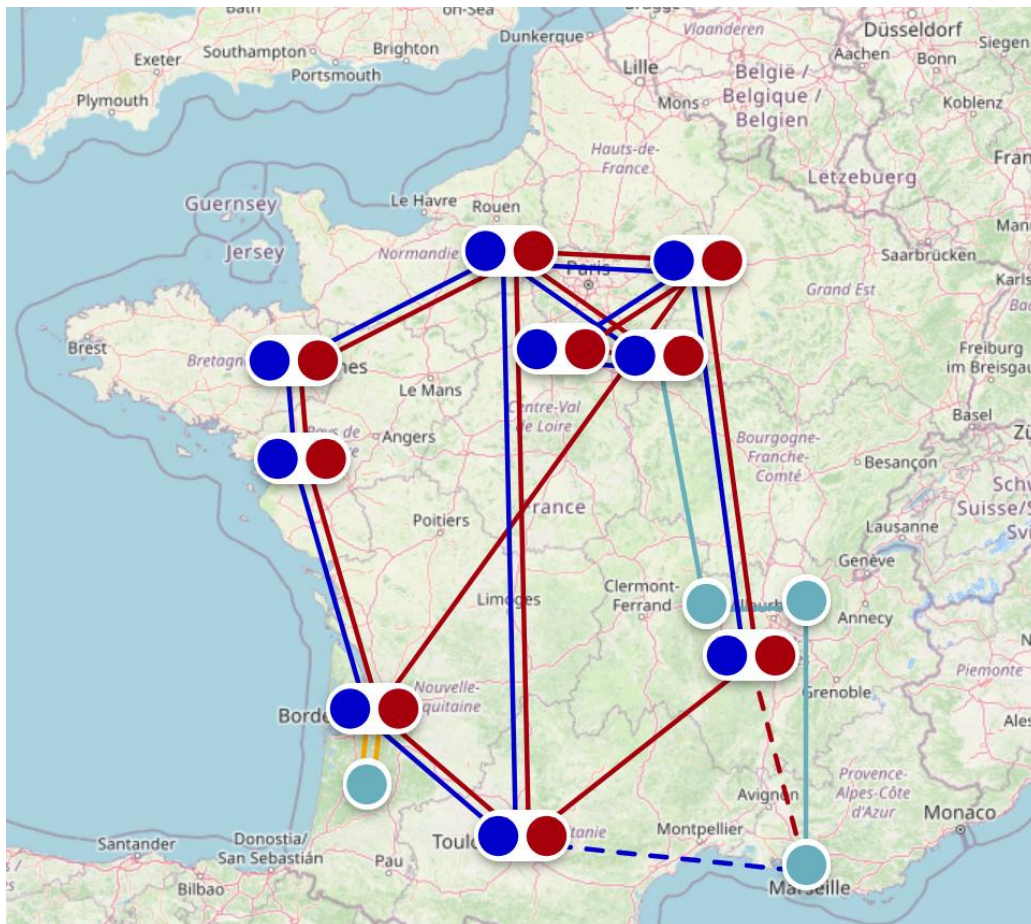
L'épine dorsale complète a été mise en service le 1er semestre 2013, ouvrant la voie au raccordement de 4 liens de transit internet et de 4 plateformes d'accès à internet.

Le cœur du réseau optique (RIE v2.0) est composé de 9 POP interconnectés : Rennes (RNS), Nantes (NTE), Bordeaux (BD2), Toulouse (TLS), Lyon (LY3), Paris (PA1, PA2, PA3, PA4).

Chaque POP est équipé de 2 routeurs RED :

- un RED « bleu » raccordé à la boucle optique « bleu » de Renater,
- un RED « rouge » raccordé à la boucle optique « rouge » de Terralpa.

Les routeurs RED « bleu » sont connectés entre eux à 100GE, les RED « rouge » sont connectés entre eux à 100GE, et sur un même POP, les routeurs RED « bleu » et « rouge » sont raccordés entre eux à 2x100GE.



Actuellement, l'accès à internet pour la métropole se fait par deux zones de transit, Nord et Sud. Le transit internet Nord se fait via les liens de Paris PA3 et de Paris PA4, le transit Sud se fait via les liens de Toulouse TLS et Bordeaux BD2. Chaque lien de transit internet est raccordé à un routeur de transit du RIE.

Les liens de transit Nord et Sud sont gérés par deux opérateurs distincts pour des raisons de résistance aux attaques et aux défaillances de mode commun.

Les services internet

Les plates-formes d'accès à internet (PFAI) sont au nombre de quatre :

- elles sont colocalisées chacune sur leur POP,
- elles sont raccordées d'un côté au routeur de transit internet,
- elles sont raccordées côté épine dorsale aux 2 routeurs RED « bleu » et « rouge ».

Ces plates-formes sont redondées et dimensionnées pour accueillir jusqu'à 600 000 agents utilisateurs répartis sur les 4 infrastructures. Elles sont partagées entre plusieurs ministères.

Elles couvrent les besoins de service internet pour l'ensemble des utilisateurs du RIE et sont amenées à évoluer en fonctionnalités, en quantité et en qualité de service.

A ce jour les plates-formes offrent un accès au web sécurisé pour 300 000 agents.

Ces plates-formes portent l'infrastructure matérielle et logicielle pour l'accès sécurisé aux services internet (dns, messagerie, proxy web, filtrage, antivirus, firewall, etc.).

L'expérience de la crise sanitaire COVID-19 amène le pouvoir adjudicateur à renforcer ses attentes pour l'accès distant de ses agents en télétravail et en moyens de visioconférence.

Au fil des dernières années, l'Internet fixe et mobile s'est imposé comme un moyen de communication indispensable pour la gestion de crise. Le pouvoir adjudicateur compte s'appuyer sur le RIE et ses services internet pour ses besoins critiques.

type Transit Internet zone nord en métropole et du service de protection anti-DDoS pour le RIE 2.0.

Le RIE dispose actuellement de quatre points d'accès de transit internet Paris PA3, Paris PA4, Toulouse TLS, Bordeaux BD2 via ses deux transitaires sur les zones Nord et Sud.

Ces quatre points de transit PA3/PA4/TLS/BD2 forment la zone d'accès à internet (ZAI) qui porte le système autonome public BGP du RIE (AS60855) enregistré auprès du RIPE NCC.

<https://apps.db.ripe.net/db-web-ui/query?from=www&searchtext=AS60855>

Les marchés ne prévoient pas de changer cette répartition de liens.

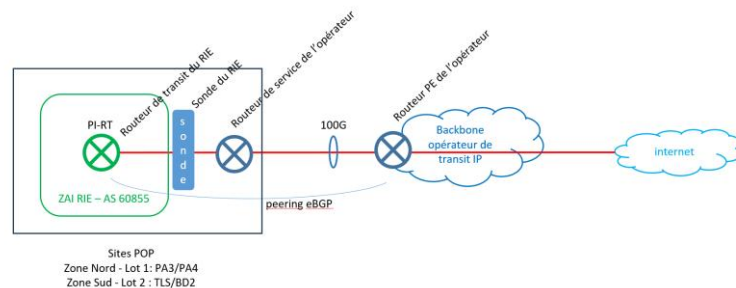
Déploiement Ex 1 : Un lien est porté par une interface physique 100G

Déploiement Ex 2 : La capacité de trafic s'entend symétrique montant et descendant

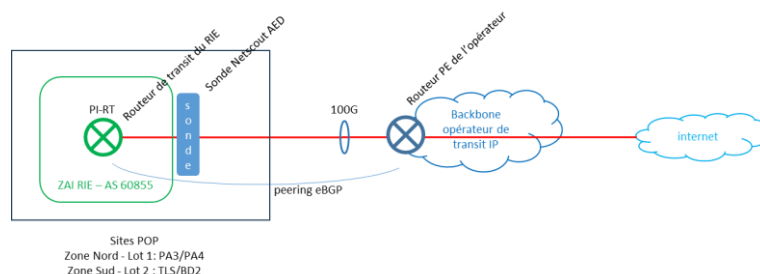
Les marchés ne prévoient pas de changer de mode de raccordement aux sondes et aux routeurs de la ZAI, néanmoins un raccordement direct en fibre nue (sur les AED) est entendable.

Le peering se fait depuis les routeurs de transit

Le transitaire annonce soit la full-table internet soit une route par défaut.



Ci-dessus le mode de raccordement avec routeur multi-service opérateur



Ci-dessous le raccordement en fibre nue.

Les routeurs de transit sont de type :

- Juniper 10003 pour les sites de PA3 et PA4, (routeurs PI-RT2).
- Cisco NCS 57B1 5DSE pour les sites de TLS et BD2, (routeurs PI-RT3).

Les routeurs de transit portent les annonces de l'AS BGP du RIE.

La DINUM est enregistrée comme LIR (Local Internet Registry) auprès du RIPE NCC.

A ce titre, des ministères lui ont délégué la gestion de leurs IPv4 PI allant du /16 au /24 :

- 143.126.0.0/16 Ministère de la Culture
- 143.196.0.0/16 Direction Générale de l'Aviation Civile (annonces partagées)
- 164.131.0.0/16 Ministère de la Santé et des Affaires Sociales
- 185.24.184.0/22 Direction Interministérielle du Numérique
- 193.17.19.0/24 Ministère des Finances
- 194.5.170.0/23 Ministère de la Transition Ecologique
194.5.172.0/23
194.5.174.0/24
- 195.42.231.0/24 Services du Premier Ministre

Les annonces BGP des adresses IPv4 et IPv6 sont portées par les quatre routeurs de transit de la ZAI. Elles sont distribuées sur la « full-table » internet via les deux transitaires.

Le RIE et la ZAI assurent le routage dynamique des flux internet entrants et sortants.

Les flux montants sont routés par défaut vers la ZAI puis vers les routeurs transitaires.

Les flux descendants sont routés via les deux transitaires sur la base des annonces de la ZAI, puis routés via le backbone RIE jusqu'aux plates-formes PFAI.

Pour les besoins opérationnels du RIE, la DINUM dispose notamment :

- d'un préfixe /22 « mutualisé » 185.24.184.0/22 qui est attribué à 99% et utilisé pour l'infrastructure des PFAI ou par les différentes communautés ministérielles,
- d'un préfixe /22 « mutualisé » 143.126.248.0/22 qui est attribué à 25% et utilisé pour les mêmes usages que son précédent historique ci-dessus.

Déploiement Ex 3 : Il est demandé au titulaire de proposer une solution Anti-DDoS permettant de protéger l'ensemble des adresses des préfixes annoncés par la ZAI.

Le pouvoir adjudicateur souhaite disposer d'une interface web lui permettant d'assurer le nettoyage de ses flux durant les attaques de type DDoS sur les adresses de son AS 60855.

Plusieurs agents habilités de l'administration, notamment les équipes DINUM/ISO, NOC RIE et CSIRT/SOC RIE, doivent pouvoir travailler simultanément sur cette interface web, selon les droits qui leur sont attribués de l'administration

Déploiement Ex 4 : Le pouvoir adjudicateur a mis en œuvre une infrastructure réseau très résiliente et souhaite que son infrastructure d'accès à internet, et le service d'anti-DDoS, soient assurés par un réseau de transit internet de type Tier 1 ou Tier 2.

Déploiement Ex 5 : Enfin, le titulaire s'engage à respecter les lois, règlements et normes liés à la sécurité des systèmes d'information et les textes en vigueur associés aux lois et décrets d'application sur la réglementation des télécommunications, ainsi qu'à la loi « Informatique et Libertés ».

Le présent accord-cadre couvre la zone Nord et les POP suivants :PA3 Rosny & PA4 Osny.

Les adresses précises de ces 2 POP sont indiquées en annexe.

Chaque plateforme de service d'accès à internet du RIE (PFAI) sont irriguées par un lien de transit colocalisé sur le site POP, pour un routage optimal avec internet.

Un autre marché couvre déjà la zone Sud pour des raisons de « résilience opérateur ».

Le titulaire indique toute information utile au raccordement des différents POP (contraintes, différences de coûts, etc...)

La mise en œuvre de la totalité du périmètre et son évolution pendant la période d'exploitation sont assurées par le titulaire dans le cadre du marché.

Le mémoire technique détaillé

*Déploiement Ex 6 : Les différentes prestations attendues par l'administration sont présentées dans ce cahier des charges en termes de **besoins** et de **résultats attendus**, et non de moyens à mettre en œuvre par le titulaire.*

Dans le cadre de l'exécution du présent accord-cadre, le titulaire se conforme aux moyens (y compris ingénierie détaillée) et aux résultats (y compris engagements de qualité de service) décrits dans le mémoire technique détaillé.

Infrastructures du titulaire

3.5.1 Architecture du Backbone Internet

Le titulaire fournit au pouvoir adjudicateur le détail de l'architecture sur laquelle s'appuient le service de transit Internet ainsi que le service anti-DDoS.

Déploiement Ex 7 : Le titulaire doit être opérateur de sa propre infrastructure anti-DDoS, sur son propre backbone.

3.5.2 Conformité

Le titulaire engage sa responsabilité quant à la conformité de son offre avec la réglementation nationale et internationale en vigueur concernant la fourniture de services de télécommunications (ITU-T, ISO, ETSI, ...).

En outre, les services proposés doivent être respectueux des standards tels qu'émis par les organismes de normalisation.

Service de transit Internet

Le service demandé dans le présent CCTP correspond à la fourniture d'un service de transit Internet via les deux liens actifs de PA3 et PA4.

Déploiement Ex 8 : Les liens sont fournis sur deux POP différents et ils aboutissent sur deux POP opérateurs différents.

Le trafic Internet transite en actif/actif suivant les annonces dynamiques faites aux routeurs transitaires par les routeurs de transit du RIE.

Ce service de transit Internet doit permettre l'annonce des plages d'adresses IPv4 et IPv6 publiques via le protocole (external) BGP par les routeurs de transit de la ZAI du réseau RIE.

Le pouvoir adjudicateur réalise lui-même le routage dynamique vers les liens de transit internet du titulaire dans le cadre du marché.

Pour chaque POP, le titulaire déploie un lien fibre d'interface 100 GE, indique le type de connecteurs utilisés en interface avec son équipement d'extrémité.

Déploiement Ex 9 : Le titulaire fournit les adresses publiques d'interco /31 avec le routeur de transit.

La volumétrie cible est de 1 million d'utilisateurs au total pour les flux sortants. Les équipements mis en place par le titulaire doivent être capables de gérer une charge correspondant à ce nombre d'utilisateurs, ainsi que la charge liée aux services applicatifs accessibles depuis l'extérieur (serveur web, messagerie, vpn, etc...)

Service anti-DDoS

3.7.1 Généralités

Pour ce service, l'interlocuteur privilégié du titulaire est le **CSIRT DINUM** qui s'appuie sur le NOC RIE pour de l'intervention en HNO sur la base d'astreintes.

Le service demandé correspond à la fourniture d'un service anti-DDoS pour l'ensemble des IP publiques annoncées depuis le système autonome BGP du RIE.

*Déploiement Ex 10 : Le titulaire doit être **souverain** sur son infrastructure anti-DDoS.*

Déploiement Ex 11 : L'infrastructure peut être mutualisée avec d'autres clients mais doit pouvoir supporter des DDoS de 100 Gbps.

Le titulaire partage avec le pouvoir adjudicateur, sous 15 jours après la réunion de lancement du marché et après chaque évolution, sous la forme d'un document word structuré qu'il pourra annexer au Plan d'Assurance Sécurité PAS :

- {PP 01} son plan de remédiation en cas de saturation de son système anti-DDoS
- {PP 02} la capacité de ses peering upstream
- {PP 03} la volumétrie à partir de laquelle il blackhole le trafic du pouvoir adjudicateur

3.7.2 Utilisateurs et connexions

Le pouvoir adjudicateur a besoin de 2 niveaux de comptes :

- Lecture seule
- Lecture écriture : possibilité de modifier les éléments de configuration concernant les assets/objets de la DINUM dans la solution

{PP 04} Décrire les moyens d'authentification multi facteurs de la solution

3.7.3 Spécifications du dispositif attendu

{PP 05} Préciser les mécanismes qui permettent l'apprentissage des préfixes IP à protéger

Déploiement Ex 12 : Le pouvoir adjudicateur doit pouvoir bénéficier de 10 groupes d'adresses IP à protéger

{PP 06} Il sera précisé les possibilités d'administration des 10 groupes d'adresses IP par le pouvoir adjudicateur

{PP 07} Il sera précisé les possibilités d'administration par le pouvoir adjudicateur (Définir/modifier/supprimer) des seuils de trafic par protocole appliqués aux groupes d'ips afin de déclencher des actions automatiques de nettoyage de flux et l'envoi

d'alertes

{PP 08} Il sera précisé les possibilités d'administration par le pouvoir adjudicateur (Créer/modifier/supprimer) des modèles de protection applicables sur les groupes d'IP (liste des types de protection attendus en annexe)

{PP 09} Il sera précisé comment le pouvoir adjudicateur pourra appliquer les modèles de protection automatiquement sur les groupes d'adresses IP sur un dépassement de seuil de trafic

Déploiement Ex 13 : Le pouvoir adjudicateur doit disposer d'une interface web lui permettant de :

- Appliquer les modèles de protection automatiquement sur les groupes d'adresses IP sur un dépassement de seuil de trafic
- Appliquer les modèles de protection manuellement sur les groupes d'adresses IP ou un préfixe
- Créer/modifier/supprimer une règle de type blackhole sur un ou plusieurs préfixes IP
- Consulter les flux transitant sur son AS ainsi que les protections en cours et alertes en cours

3.7.4 Contre-mesures

{PP 10} Préciser la liste des contremesures défensives applicables sur les flux de transit

3.7.5 CTI

{PP 11} Décrire les moyens et formats d'import et de mise en traitement des marqueurs de compromission du pouvoir adjudicateur (import externe à la solution)

3.7.6 Flowspec

Déploiement Ex 14 :

le titulaire doit être en mesure de mettre en place, à la demande du pouvoir adjudicateur et en 24/7, des règles de filtrage de niveau 3 et 4 de type Flowspec sur ses routeurs périphériques. Le titulaire applique son devoir de conseil sur cette demande. Il peut le cas échéant refuser sa mise en œuvre lorsqu'elle apparaît manifestement inadaptée ou susceptible de dégrader le service ou le service de l'opérateur.

{PP 12} Préciser les moyens mis à disposition du pouvoir adjudicateur permettant de suivre les effets en temps réel des règles de type Flowspec appliquées à son périmètre

3.7.7 Alerting

Déploiement Ex 15 : Le pouvoir adjudicateur doit avoir la possibilité de :

- Créer/modifier/supprimer les notifications externes (envoi des alertes)

{PP 13} Préciser les protocoles sécurisés à disposition pour l'alerting

Déploiement Ex 16 :

Le pouvoir adjudicateur doit recevoir automatiquement une notification en cas de dépassement de seuil, déclenchement d'alerte et retour à la normale

3.7.8 Maintenance et sauvegardes

{PP 14} Préciser les moyens mis à disposition du pouvoir adjudicateur permettant de sauvegarder tout ou partie de sa configuration métier déployée dans la solution anti-DDoS

Déploiement Ex 17 : Il est attendu le partage des roadmaps de mise à jour de la solution ainsi que les change logs avant mise à jour

3.7.9 Interface Machine to Machine (API)

Dans le cas où la solution anti DDoS proposée serait en mesure de fournir une API.

{PP 15} Préciser si le soumissionnaire prévoit de mettre à disposition une API pour accéder à certaines fonctions de paramétrage et de configuration de la solution anti-DDoS

{PP 16} Préciser les modalités d'accès et les possibilités de l'API de la solution technique retenue

3.7.10 Exploitation

L'instance anti-DDoS dédiée au périmètre du pouvoir adjudicateur est administrable à la fois par le titulaire et par les agents habilités du pouvoir adjudicateur, selon des profils de droits distincts et tracés.

{PP 17} Préciser combien de comptes nominatifs seront disponibles pour l'exploitation de la solution d'anti-DDoS

{PP 18} Préciser combien de personnes pourront être connectés en même temps à l'interface de mitigation ainsi qu'à l'interface extranet, en lecture

{PP 19} Préciser combien de personnes pourront être connectés en même temps à l'interface de mitigation ainsi qu'à l'interface extranet, en écriture

Déploiement Ex 18 : Exposer une méthodologie de travail permettant la mise en place d'un versioning de la configuration appliquée sur le système anti-DDoS.

Le système anti-DDoS permet au pouvoir adjudicateur d'identifier en permanence la version de configuration appliquée en production. Le titulaire expose la méthodologie de versioning associée, incluant a minima l'identification de la version en production, l'historique des modifications, la date d'application et les modalités de retour arrière le cas échéant.

Déploiement Ex 19 : En 24/7 le pouvoir adjudicateur doit pouvoir solliciter le soumissionnaire pour la mise en place d'une protection de type « flowspec » ou pour une expertise concernant une protection dont l'efficacité est douteuse.

Déploiement Ex 20 : Dans le cas où le soumissionnaire serait amené à insérer une règle de filtrage de type flowspec dans ses routeurs périphériques avec un impact potentiel sur un ou plusieurs préfixes IP du pouvoir adjudicateur, il est attendu une notification du NOC RIE en 24/7

Déploiement Ex 21 : Le partage réciproque de matrices d'escalades est attendu.

Accès extranet

Le titulaire fournit au pouvoir adjudicateur une interface web authentifiée par 2 facteurs (2FA), accessible en liste blanche, pour environ 25 comptes nominatifs ou fonctionnels.

L'interface permet de gérer les comptes, de présenter les éléments contractuels relatifs aux deux liens de transit de la zone (adresses d'interconnexion, paramètres MD5, BGP, BFD, etc.), ainsi que la documentation technique (DAT, etc.) et contractuelle, incluant les éléments financiers, les échéances contractuelles, les tickets de support, les maintenances programmées, la matrice d'escalade et les tableaux de bord techniques....

Cet extranet pourra intégrer des outils : ping, traceroute, looking glass BGP ...

4 DEPLOIEMENT DU SERVICE

Le déploiement débute à la date de notification du marché ainsi qu'à chaque reconduction et s'achève par la décision d'admission des prestations prononcée à la mise en service des accès Internet.

A compter de l'admission des accès Internet, le titulaire assure l'exploitation du service d'accès Internet, du service anti-DDoS et extranet pendant la durée du marché et à fournir, durant cette période, les prestations de service demandées.

Organisation et pilotage du projet

4.1.1 Organisation du pouvoir adjudicateur

L'organisation du pouvoir adjudicateur est précisée au lancement du marché.

4.1.2 Organisation du titulaire

Le titulaire est le maître d'œuvre et, à ce titre, assure l'ensemble des tâches nécessaires à la mise en œuvre des accès Internet souhaités par le pouvoir adjudicateur. Il constitue son équipe projet et en fournit la composition définitive lors de la réunion de lancement du marché.

L'organisation projet du titulaire prend en charge les domaines technique et commercial.

Le titulaire désigne un interlocuteur unique et pérenne en charge du pilotage du projet, a minima jusqu'à constatation du service régulier.

La liste des intervenants du titulaire pour le projet est soumise à validation du représentant du pouvoir adjudicateur qui se réserve le droit de récuser à tout moment, et sous 15 jours calendaires, un ou plusieurs intervenants y compris, sur décision motivée, un chef de projet du titulaire.

Le titulaire :

- anime et gère l'ensemble de la mise en œuvre des accès Internet et l'anti-DDoS ;
- définit et fait approuver les procédures de fonctionnement, traduites dans un Plan d'Assurance Qualité (PAQ) et un Plan d'Assurance Sécurité (PAS) régulièrement mis à jour ;
- adapte les moyens et les ressources en fonction de l'évolution de la charge et des besoins ;

- rend compte régulièrement au représentant du pouvoir adjudicateur de l'avancée de la mise en œuvre des services qui lui ont été confiés ;
- adapte le contenu organisationnel et technique de chaque étape de la prestation ;
- remet les livrables demandés et apporte, à la demande du pouvoir adjudicateur, les corrections nécessaires dans un délai maximal de trois jours ouvrés, afin de ne pas compromettre la durée respective de chacune des phases de mise en œuvre ;
- élabore le planning détaillé de la mise en œuvre dans le respect impératif des délais fixés par le CCTP et répondre de son bon suivi ;
- propose et met en œuvre les processus de recette, sous la supervision du pouvoir adjudicateur ;
- prépare, anime les réunions périodiques avec le pouvoir adjudicateur et en rédiger les comptes rendus.

En outre, le titulaire garantit :

- la maîtrise des délais et des coûts ;
- la définition, la réalisation, le test et la cohérence technique des prestations techniques fournies ;
- la définition et la gestion de la qualité des prestations et des résultats intermédiaires et finaux ;
- la coordination des différents intervenants dont il est responsable directement ou indirectement (personnel du prestataire, fournisseurs, sous-traitants ou cotraitants) ;
- le rapport auprès du pouvoir adjudicateur du suivi de la prestation, notamment par sa participation aux différentes instances de pilotage définies au titre de l'assurance qualité.

4.1.3 Instances de pilotage

Le pouvoir adjudicateur organise le pilotage du marché autour de 4 comités :

- Le comité de pilotage COPIL
- Le comité de projet COPROJ
- Le comité d'exploitation COEX

Ci-après le contenu de chaque comité.

4.1.3.1 Comité de pilotage

Le comité de pilotage (COPI) associe des représentants du pouvoir adjudicateur, notamment la DSAF pour les sujets contractuels, des représentants de la DINUM pour le suivi opérationnel et technique, ainsi que les représentants du titulaire. Les décisions contractuelles relèvent du pouvoir adjudicateur ; le suivi technique et opérationnel est assuré par la DINUM dans son rôle de service bénéficiaire et prescripteur technique.

Ce comité a pour objectif d'examiner et d'étudier toutes les questions contractuelles et stratégiques liées au déroulement de la prestation et d'assurer la gestion des risques.

Il permet la remontée d'informations, via un canal officiel, auprès du représentant du pouvoir adjudicateur sur le déroulement de la prestation.

L'ordre du jour de ce comité se base sur la liste, non exhaustive, des éléments suivants :

- les indicateurs de pilotage ;
- l'état d'avancement de la prestation, la synthèse des activités et le résultat des actions particulières effectuées ;
- la réestimation des délais des travaux en cours et la mise à jour des plannings si nécessaire ;
- les décisions en suspens, pouvant impliquer d'autres intervenants ;
- les indicateurs de qualité et les tendances en matière de volumétrie ;
- la revue des incidents critiques et des incidents de sécurité éventuels ainsi que le suivi des plans d'actions décidés suite à ces incidents ;
- les aspects financiers ;
- les pénalités applicables éventuelles ;
- la synthèse des actions prévues pour la période à venir et le calendrier des réunions suivantes ;
- le bilan des validations de livrables et des opérations de vérification.

En phase de déploiement, le comité de pilotage se réunit de façon mensuelle si nécessaire. Il fait l'objet d'une proposition d'ordre du jour par le titulaire, diffusée au minimum 5 jours ouvrés avant sa tenue, complétée si besoin et validée par le pouvoir adjudicateur, et d'un compte rendu réalisé par le titulaire, envoyé au maximum 2 jours ouvrés après la réunion pour validation par le pouvoir adjudicateur. Après validation du pouvoir adjudicateur, la diffusion du compte rendu aux intervenants concernés est assurée par le titulaire.

En fonction de la criticité des événements abordés et des niveaux d'arbitrage et de décisions requis, la réunion peut donner lieu à un comité de pilotage exceptionnel auquel participent le personnel du titulaire et le personnel du pouvoir adjudicateur figurant dans le tableau des escalades du Plan d'Assurance Qualité.

Le comité de pilotage comporte deux parties distinctes, le service des accès à internet et le service anti-DDoS.

4.1.3.2 Comité de projet

Un comité de projet (COPROJ), composé de représentants du pouvoir adjudicateur et du titulaire est constitué. Il se réunit toutes les semaines pendant la phase de travaux et une fois la VSR finalisée.

Il se réunit à la demande du pouvoir adjudicateur une fois les travaux terminés sur les 2 liens de transit.

Les participants ont pour objectif de suivre l'avancement des travaux de déploiement des liens, jusqu'à la réalisation des tests de VA et de VSR.

Il fait autorité pour décider des actions et acter des décisions relatives au fonctionnement et au déroulement de la prestation.

L'ordre du jour de ce comité se base sur la liste, non exhaustive, des éléments suivants :

- le suivi de livraison des documents livrables (Qualité, Sécurité, Recette, CR ...)
- l'établissement du planning détaillé des chantiers,
- le suivi d'avancement du déploiement des liens de transit IP,
- le suivi d'avancement des configurations anti-DDoS,
- la résolution des points techniques et organisationnels pouvant avoir un impact sur l'avancement des chantiers,
- le suivi d'exécution des tests techniques de validation d'aptitude.

Le cas échéant, le comité de projet rapporte au comité de pilotage toutes les informations d'ordre stratégique nécessitant la tenue d'un COPIL exceptionnel.

Le comité de projet comporte deux parties distinctes : transit internet et anti-DDoS.

4.1.3.3 Comité de suivi opérationnel

Un comité de suivi opérationnel (COEX), composé de représentants du pouvoir adjudicateur et du titulaire, est constitué dès lors qu'un lien est raccordé et en Validation d'Aptitude.

Ce comité a pour objectif d'assurer un suivi d'exploitation des liens et d'étudier les problématiques techniques intervenues durant la dernière période.

C'est durant ce comité que le titulaire transmet au pouvoir adjudicateur le suivi des indicateurs et les engagements contractuels. Le détail de ces indicateurs et des engagements est précisé dans la suite du document, l'indicateur principal étant la disponibilité des liens.

Le titulaire propose une trame de présentation (MS Powerpoint, PDF ou équivalent web) au pouvoir adjudicateur qui pourra en demander des adaptations.

Dans l'éventualité de non-respect des engagements de qualité constaté en comité, le pouvoir adjudicateur se réserve le droit d'engager une prestation d'ingénierie (réalisée en propre ou via un tiers qui n'est pas nécessairement le titulaire) ayant pour but de réaliser des audits de qualité et de performance sur les services fournis.

Ce comité se réunit deux fois par mois durant la période de VA et de VSR. Une fois les 2 liens en service régulier, le comité se réunit une fois tous les 3 mois. Il peut être convoqué suite à l'occurrence d'un incident majeur (une rupture de lien ou une attaque DDoS), à la demande de l'une des parties sur convocation.

Le comité fait l'objet d'une proposition d'ordre du jour par le titulaire, diffusée au minimum 5 jours ouvrés avant sa tenue, complétée si besoin et validée par le pouvoir adjudicateur. Un compte rendu de comité, réalisé par le titulaire, est envoyé au maximum 2 jours ouvrés après la réunion et pour validation par le pouvoir adjudicateur. Après validation du pouvoir adjudicateur, la diffusion du compte rendu aux intervenants concernés est assurée par le titulaire, dans un délai de deux jours ouvrés.

Partie COSEC intégré

Au besoin un volet sécurité pourra être proposé par le titulaire ou le pouvoir adjudicateur.

Côté titulaire il est attendu un retour sur les attaques par déni de service majeures ayant transité par son backbone. Également les événements de sécurité concernant les équipements directement reliés aux routeurs Internet du RIE devront être partagés pendant le comité.

Côté pouvoir adjudicateur en cas d'attaques majeures un retour d'expérience sera fait pendant le comité.

Synthèse

Comité	Objet principal	Périodicité	Indicateurs / sujets suivis
COPIL – Comité de pilotage	Pilotage stratégique et contractuel du marché, suivi des risques et arbitrages.	Mensuel en phase de déploiement, si nécessaire. Possibilité de COPIL exceptionnel selon la criticité	Indicateurs de pilotage, avancement de la prestation, plannings, décisions en suspens, qualité de service, volumétrie, incidents critiques et incidents de

		des événements.	sécurité, plans d’actions, aspects financiers, pénalités, validations de livrables et opérations de vérification.
COPROJ – Comité de projet	Suivi opérationnel du déploiement des liens de transit Internet et des configurations anti-DDoS jusqu’aux tests de VA et de VSR.	Hebdomadaire pendant la phase de travaux et jusqu’à la finalisation de la VSR. Ensuite, à la demande du pouvoir adjudicateur.	Livraison des documents, planning détaillé des chantiers, avancement du déploiement des liens de transit IP, avancement des configurations anti-DDoS, résolution des points techniques et organisationnels, suivi des tests techniques de validation d’aptitude.
COEX – Comité de suivi opérationnel	Suivi d’exploitation des liens, analyse des problématiques techniques et suivi des engagements contractuels.	Deux fois par mois pendant les périodes de VA et de VSR. Une fois les deux liens en service régulier : tous les 3 mois. Peut être convoqué en cas d’incident majeur.	Disponibilité des liens, indicateurs d’exploitation, engagements contractuels, incidents majeurs, rupture de lien, attaques DDoS, qualité et performance des services fournis.
Volet sécurité intégré au COEX / COSEC	Suivi spécifique des événements de sécurité et retours d’expérience liés aux attaques majeures.	Au besoin, dans le cadre du COEX.	Attaques par déni de service majeures, événements de sécurité concernant les équipements reliés aux routeurs Internet du RIE, retours d’expérience en cas d’attaques majeures.

Définitions et méthodes

4.2.1 Format des livrables

Les livrables des différentes étapes du projet sont rédigés par le titulaire et soumis pour validation au pouvoir adjudicateur.

Tous les livrables du titulaire sont fournis sous un format lisible par les versions courantes d’OpenOffice, LibreOffice et MS Office et dans un format ouvert pour les schémas et configurations.

Dans le cas où les schémas et configurations ne peuvent être fournis que dans un format propriétaire, le titulaire fournit également le logiciel et la licence associée au pouvoir adjudicateur.

Pour gérer les livrables, le titulaire peut proposer, durant l’étape de mise en œuvre et pendant toute la durée de l’accord-cadre, un outil de travail collaboratif souverain, asynchrone et de gestion documentaire, permettant de stocker et d’échanger l’ensemble des livrables entre les parties.

L’utilisation de l’outil proposé par le titulaire est soumise à l’accord préalable du pouvoir adjudicateur. À défaut d’accord, ou si l’outil proposé ne répond pas aux exigences de l’Administration, le pouvoir adjudicateur peut imposer l’utilisation de son propre outil collaboratif.

L’absence de proposition d’un tel outil par le soumissionnaire ne constitue pas, en elle-même, un motif de rejet de l’offre ni un élément défavorable dans l’appréciation de celle-ci.

4.2.2 Déploiement

Le déploiement comprend l'installation et la mise en œuvre des accès Internet sur les POP du lot concerné ainsi que la mise en place de la solution anti-DDoS sur ces accès.

4.2.3 Vérification d'aptitude (VA)

Type d'anomalie	Définition	Délai de contournement attendu	Délai de correction / solution définitive
Anomalie bloquante	Toute anomalie empêchant la mise en service, la continuité du service, la sécurité du service ou la réalisation d'un test essentiel prévu au cahier de recette.	Le titulaire met en œuvre sans délai les actions nécessaires et propose, lorsque cela est techniquement possible, une solution de contournement dans un délai maximal de 5 jours à compter de la constatation de l'anomalie.	La correction définitive doit intervenir dans les meilleurs délais et, en tout état de cause, avant toute décision positive de vérification d'aptitude ou de service régulier, sauf acceptation expresse du pouvoir adjudicateur.
Anomalie non bloquante	Toute anomalie n'empêchant pas la poursuite des vérifications ni l'usage du service, sous réserve qu'elle ne compromette ni la sécurité, ni la continuité, ni les performances essentielles du service.	Si un contournement est nécessaire, le titulaire propose une mesure temporaire dans un délai maximal de 5 jours à compter de la constatation de l'anomalie.	Le titulaire transmet un plan de correction précisant les actions prévues, les responsables et les délais de résolution. Ce plan est soumis à validation du pouvoir adjudicateur. La correction intervient dans le délai validé par celui-ci, et au plus tard avant la fin de la période de VSR, sauf accord exprès du pouvoir adjudicateur ;

En prérequis de la VA, le titulaire fournit au pouvoir adjudicateur un cahier de recette pour les liens, les équipements et les fonctionnalités de chaque POP concerné, décrivant notamment :

- les procédures de tests ;
- le planning des tests et l'ensemble des tests unitaires (*);
- les procédures de retour arrière ;
- un dossier de suivi en exploitation de chaque site, décrivant notamment :
 - Les caractéristiques techniques du raccordement ;
 - Les procédures à appliquer en cas de défaillance du site.

Pour chaque test unitaire, les cahiers de recette doivent préciser :

- l'identifiant du test ;
- l'objet du test ;
- l'environnement technique de test (moyens mis en œuvre) ;
- la mise en œuvre du test (description pas à pas du test) ;
- les résultats attendus et les résultats obtenus.

Le pouvoir adjudicateur peut compléter les cahiers de test en tant que de besoin. Les procédures de tests validées par le pouvoir adjudicateur doivent être appliquées à chaque étape du déploiement.

Le titulaire effectue préalablement à la livraison les tests et remplit le cahier de tests qu'il fournit au pouvoir adjudicateur dès lors que le titulaire a validé tous les tests. Il est présent pendant les opérations de vérification et réalise les actions nécessaires au bon déroulement des tests.

Le titulaire est disponible pendant toute la durée des opérations de vérification pour résoudre les problèmes éventuels survenant.

Durant cette étape, les critères d'ajournement sont notamment les suivants :

- une anomalie bloquante non résolue ;
- non respect des engagements de qualité de service ;
- non fourniture des documentations ou documentation incomplète.

La Validation d’Aptitude des liens de transit requiert que la solution d’anti-DDoS soit bien opérationnelle et apte à faire face à des attaques sur un préfixe annoncé sur ces liens.

La phase de Validation d’Aptitude peut être ajournée en cas de risque identifié à ce niveau par le pouvoir adjudicateur et faire l’objet d’un retour-arrière, c’est-à-dire de retrait du lien.

4.2.4 Vérification de service régulier (VSR)

La période de VSR d’un site débute suite à la validation de la VA le concernant.

L’objectif de la VSR est de contrôler la conformité globale du service fourni :

- conformité aux engagements de qualité de service lors de la montée en charge ;
- conformité pour la mise en place de mitigations sur le lien du site ;
- qualité du support technique.

Durant cette étape, les critères d’ajournement sont au minimum les suivants :

- une anomalie bloquante non résolue ;
- une anomalie non bloquante, détectée lors de la VA, non résolue ;
- non respect des engagements de qualité de service ;
- non-conformité avec les procédures et les engagements d’exploitation et de maintenance.

Au terme de cette période, le service est réputé régulier si l’ensemble des engagements de qualité de service, d’exploitation, de maintenance et de sécurité sont respectés.

Etapes du projet

4.3.1 Étape 1 : Lancement du projet

Le délai maximum pour la réalisation de cette étape est fixé à deux semaines à compter de la date de réception du bon de commande.

Cette étape comprend notamment la finalisation et la validation des équipes projet intervenantes, la préparation et la tenue de la réunion de lancement, ainsi que la remise des premiers livrables attendus au titre de cette étape.

La réunion de lancement est organisée par le titulaire en présentiel, dans un délai maximum de sept jours à compter de la notification du bon de commande. À cette occasion, le titulaire présente un support de type PowerPoint proposant un ordre du jour permettant d’aborder

l'ensemble des points contractuels, organisationnels et techniques du projet. L'ordre du jour et les éventuels documents préparatoires sont transmis au pouvoir adjudicateur préalablement à la tenue de la réunion.

À l'issue de cette étape, le titulaire fournit, au titre des livrables, un PAQ (Plan d'Assurance Qualité), un PAS (Plan d'Assurance Sécurité) ainsi qu'un planning projet détaillé, compatible avec les délais d'exécution prévus dans le CCTP et dans son offre technique.

4.3.2 Étape 2 : Etude et spécifications

Cette étape débute à l'issue de l'étape de lancement et le délai maximum pour sa réalisation est fixé dans le chapitre engagements.

Le titulaire rédige l'ensemble des spécifications techniques liées à l'architecture, à l'administration, à l'exploitation, à la sécurisation et la supervision des accès Internet.

Les livrables associés à cette étape sont les suivants :

- la documentation de la solution anti-DDoS et les identifiants pour y accéder.
- les spécifications d'architecture détaillées des accès ;
- le plan d'adressage pour chaque accès ;
- les règles d'interfaçage entre les équipements du pouvoir adjudicateur et ceux du titulaire ;
- les spécifications détaillées de l'administration, de l'exploitation, de la sécurisation et de la supervision des accès ;
- le dossier de configuration des équipements d'extrémité incluant les configurations logicielles et matérielles par accès ;
- le Plan Qualité Service Client (PQSC) ;
- le Planning de déploiement. Ce planning du déploiement est établi conformément aux indications données par le pouvoir adjudicateur et demeure sous la validation de ce dernier ;
- le Cahier de tests pour les opérations de vérification. Les cahiers de tests sont constitués par le titulaire, complétés et modifiés si besoin avant validation par le pouvoir adjudicateur.

4.3.3 Étape 3 : Livraison

Le démarrage de cette étape est conditionné par l'acceptation des prestations du titulaire des deux étapes précédentes par le pouvoir adjudicateur.

4.3.3.1 Vérification d'aptitude

Différentes vérifications techniques valident le bon déroulement du déploiement des accès et des interconnexions avec le backbone RIE (intercos, flux, debits, paramétrages ...).

Les livrables associés à cette étape sont :

- le cahier de tests complété par les résultats des contrôles nécessaires à la validation des fonctions principales telles qu'elles sont définies ;
- les configurations mises à jour pour l'ensemble des équipements installés.

La vérification d'aptitude a pour objectifs :

- la validation des procédures de déploiement ;
- la validation des procédures de retour arrière ;
- la validation de l'architecture, des règles de dimensionnement, et de toutes les fonctionnalités notamment le bon fonctionnement de bascule des flux d'un accès à l'autre en cas de dysfonctionnement et conformément aux annonces BGP ;
- la validation des engagements du titulaire d'un point de vue performances ;
- la validation de l'interconnexion du nouvel accès avec le RIE,
- la validation des moyens de sécurisation des accès ;
- la validation des moyens de mitigation via le service anti-DDoS ;
- la mise en œuvre des systèmes d'administration et d'exploitation du titulaire ;
- la mise en œuvre des systèmes de suivi et de supervision mis à disposition du pouvoir adjudicateur ainsi qu'un accès en lecture aux configurations des équipements ;
- la vérification des procédures d'exploitation et des plans de reprise d'activité et de continuité d'activité.

Sur la base du cahier de tests complété par le titulaire, le pouvoir adjudicateur contrôle que les configurations et les tests effectués sont conformes aux prescriptions fixées dans le CCTP et au mémoire technique du titulaire annexé à l'acte d'engagement.

La durée de la vérification d'aptitude est fixée à 5 jours ouvrés.

Les opérations de vérification d'aptitude comprennent à minima :

- la vérification du débit demandé ;
- la vérification de l'interconnexion de l'accès avec le RIE, pour tous les accès ;
- la vérification de la continuité de service en cas de dysfonctionnement de l'accès nominal ;
- la validation des procédures de déploiement technique et organisationnel des accès Internet ;
- les tests de sécurisation (accès limité au réseau d'administration, tests des liens de secours, etc...) et de mitigation en cas d'attaque DDoS.

La vérification d'aptitude par le pouvoir adjudicateur, sans réserve majeure, est un prérequis au démarrage de la vérification de service régulier.

4.3.3.2 Vérification de service régulier

En cas de décision positive de vérification d'aptitude par le pouvoir adjudicateur, l'étape de vérification de service régulier est lancée. Cette étape de vérification est suivie, si elle est validée par le pouvoir adjudicateur, de l'exploitation de ce même périmètre.

La période de VSR des accès Internet et du service anti-DDoS est fixée à **deux mois**.

Cette étape cruciale doit permettre de tester et de valider le fonctionnement des accès et des services associés. Le cas échéant, elle doit également permettre de réaliser les ajustements techniques et organisationnels nécessaires à l'exploitation de l'accès Internet.

Le titulaire réalise l'ensemble des tests qui ont pour objectif de finaliser la validation de l'accès et des services anti-DDoS associés.

Les tests de cette vérification de service régulier doivent permettre :

- la validation des procédures de shut/no shut des liens et des transferts de charge ;
- la validation de l'architecture, des règles de dimensionnement ;
- la validation des engagements du titulaire d'un point de vue performance ;
- la validation des moyens de sécurisation des accès et des flux (typ. Anti-DDoS);
- la validation des engagements du titulaire en termes de délai de déploiement de la solution ;

- la validation des systèmes d'administration, d'exploitation, de maintenance et de supervision du titulaire ;
- les mises à jour éventuelles de la documentation fournie.

Un audit de sécurité des accès peut par ailleurs être réalisé par le pouvoir adjudicateur lors de la période de vérification de service régulier.

Le pouvoir adjudicateur réalise également une validation du fonctionnement de ses propres applications. Il sollicite le cas échéant le titulaire sur des problématiques de fonctionnement de ses applications liées à un paramétrage bloquant de l'accès.

Au terme de cette période, le service des accès est réputé régulier si l'ensemble des engagements de qualité de service, d'exploitation et de maintenance est respecté. Dans ce cas, la phase d'exploitation opérationnelle des accès correspondants est déclenchée.

Les opérations de vérification ont pour objectif de valider, d'une part, la réception de l'ensemble des produits et services mis en œuvre et, d'autre part, le respect de l'architecture définie ainsi que des spécifications techniques détaillées.

Planning de déploiement

Pour chaque lot, le titulaire respecte un délai maximal de fourniture du service d'accès Internet à compter de la notification du marché, incluant la validation des opérations de vérification prononcée par le pouvoir adjudicateur. À défaut, il s'expose aux pénalités prévues au CCAP.

Pour le déploiement des liens, le délai maximum est de 16 semaines.

Pour le déploiement de l'anti-DDoS, le délai maximum est de 1 mois après déploiement des liens.

5 GESTION OPERATIONNELLE

Organisation

5.1.1 Organisation du pouvoir adjudicateur

L'organisation du pouvoir adjudicateur est définie lors de l'étape 1.

5.1.2 Organisation attendue du titulaire

Le titulaire présente un unique responsable de l'équipe projet en charge de la gestion opérationnelle des services souscrits.

En cas de remplacement ou de récusation du responsable de la prestation ou d'un membre clé de l'équipe opérationnelle, le titulaire assure la continuité du service et propose un remplaçant présentant un niveau de compétence équivalent dans un délai maximal de 7 jours ouvrés. En cas d'urgence opérationnelle, une solution transitoire est mise en place sans délai.

Instance de pilotage

Le titulaire analyse conjointement avec la DINUM, les indicateurs de suivi de la qualité de service ainsi que la qualité de sa prestation de gestion opérationnelle. Il propose, le cas échéant, des axes d'amélioration de ces indicateurs, puis les met en œuvre après accord du pouvoir adjudicateur.

En phase de gestion opérationnelle, le comité de pilotage se réunit semestriellement. Chaque comité fait l'objet d'une proposition d'ordre du jour établie par le titulaire, diffusée au minimum cinq jours ouvrés avant sa tenue, puis complétée si nécessaire et validée par le pouvoir adjudicateur. Un compte rendu est rédigé par le titulaire et transmis au pouvoir adjudicateur au plus tard quatre jours ouvrés après la réunion, pour validation. Après validation, le titulaire assure la diffusion du compte rendu aux intervenants concernés.

En fonction de la criticité des événements abordés et des niveaux d'arbitrage ou de décision requis, la réunion peut donner lieu à un comité de pilotage spécifique, auquel participent les représentants du titulaire et du pouvoir adjudicateur mentionnés dans le tableau des escalades du Plan d'Assurance Qualité.

Support client

Le titulaire assure un service de **support client 24h/24, 7j/7** permettant de signaler tout dérangement du service par téléphone, avec un numéro unique, ou à travers un portail client (typ. extranet opérateur), le tout en langue française.

Le support client est préférentiellement effectué à proximité des équipes d'administration et d'exploitation, ainsi que du représentant du pouvoir adjudicateur, afin de garantir la bonne interaction entre l'ensemble des équipes en charge de la gestion du réseau.

Le support client assure :

- l'enregistrement de tout dérangement de façon réactive ou proactive;
- l'ouverture de tickets d'incidents ;
- le suivi des tickets d'incidents ;
- la communication vers le pouvoir adjudicateur des changements d'état des tickets d'incidents.

Le titulaire propose un point d'entrée opérationnel unique, **disponible 24/7** pour toute remontée d'incidents ou d'anomalies sur les services associés, au pouvoir adjudicateur et à ses représentants, ainsi qu'aux différents titulaires du marché connexe de réalisation du RIE auxquels le pouvoir adjudicateur délègue sa responsabilité.

Le rôle du guichet unique est de :

- superviser l'ensemble des services et d'assurer la continuité des services lors des opérations liées au changement et à la production du réseau et des raccordements ;
- enregistrer tout dérangement, assurer le suivi et la gestion des incidents en cours ;
- coordonner les équipes d'exploitation opérationnelles en cas d'intervention à distance ou sur site ;
- produire pour les comités d'exploitation un rapport de suivi d'activité du support client indiquant notamment le nombre d'appels reçus, le nombre d'appels en absence, le délai de prise en compte d'un incident (temps écoulé entre le signalement d'un incident et l'envoi de l'accusé de réception).

Le pouvoir adjudicateur exige de la part du titulaire une détection et une gestion des incidents **pro-active**. Le titulaire doit donc être en mesure d'assurer un service de détection et de correction des incidents en temps réel et en continu sur les services proposés. Il informe le pouvoir adjudicateur en cas de détection de problème ou d'incident.

Cette équipe doit être en mesure d'assurer le diagnostic et la résolution des incidents ou dysfonctionnements, tout en minimisant les impacts éventuels sur les services du pouvoir adjudicateur.

Dans le cas d'une attaque en déni de service, sur détection de ses sondes, le titulaire doit remonter une alarme au NOC / CSIRT (SOC RIE) du pouvoir adjudicateur qui lui permet d'ouvrir un ticket et solliciter sa chaîne d'alerte interne.

En fonction des informations qui lui sont accessibles à son niveau sur la provenance des flux (adresse IP, domaine ou pays ...), le titulaire met en place les filtres et limitations permettant d'endiguer l'attaque. Le cas échéant, le pouvoir adjudicateur peut donner des directives sur la stratégie de mitigation ou la mitigation à mettre en œuvre.

Le titulaire assure le suivi de mitigation via son outil de gestion de ticket.

Le titulaire résout les problèmes et incidents récurrents, au sens ITIL.

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

Supervision

Le titulaire assure la supervision complète de son infrastructure réseau, des accès nominaux et de secours et des équipements d'extrémité en temps réel 24h/24, 7J/7.

Le titulaire supervise les alarmes d'attaques et en informe le CSIRT.

Les données attendues sont les informations d'état 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.

Il est recommandé au titulaire de disposer d'outils d'aide à l'exploitation de type looking-glass : ping traceroute, commande BGP ...

Gestion des incidents

Un incident débute à minima à partir de la remontée d'une alerte sur les plates-formes de supervision du titulaire ou à la signalisation, par l'interface web mise à disposition par le titulaire, par téléphone ou par mail, telle que décrite au paragraphe 5.3. La clôture d'un ticket d'incident nécessite l'accord préalable du pouvoir adjudicateur.

Le fonctionnement est dit dégradé lorsque l'état du service est distinct de l'état nominal (par exemple par non-respect des engagements de qualité de service).

5.5.1 Classification des incidents et moyens mis en œuvre

Le titulaire classe les incidents en fonction des impacts qu'ils ont sur l'utilisation des services selon les définitions suivantes :

- **Incident de sévérité 1** : incident générant une interruption totale du service.
- **Incident de sévérité 2** : incident générant une interruption totale ou partielle d'un des liens, les annonces du RIE et les flux correspondants sont basculés sur un autre lien sans dégradation de service (impact sur le trafic, non-respect des engagements de qualité de service, perte de routes...), excepté en cas de non-respect du débit contractuel sur le lien de secours.
- **Incident de sévérité 3** : le dysfonctionnement est transparent pour les utilisateurs et n'impacte pas directement l'utilisation des services.

Le titulaire met en œuvre les moyens adaptés à chaque niveau de sévérité.

Tout incident est pris en charge par le titulaire dans un délai inférieur à cinq minutes à compter du déclenchement de l'alarme.

5.5.2 Procédures et outils

Le titulaire assure la gestion des incidents affectant l'ensemble des services fournis selon les modalités suivantes : les incidents sont ouverts sous un numéro unique par le support client, à la suite de la déclaration d'un dérangement auprès de celui-ci, ou de manière proactive à la suite de la remontée d'une alerte sur les plateformes de supervision. Chaque incident doit faire l'objet d'un accusé de réception par courriel.

Les règles de nommage des références des tickets d'incidents sont définies par le pouvoir adjudicateur et doivent être respectées par le titulaire.

Le titulaire fournit une procédure ainsi qu'une grille d'escalade mentionnant les interlocuteurs et les entités impliqués. Ces documents sont régulièrement mis à jour.

Le titulaire assure la gestion des incidents au moyen d'un outil dédié. La transmission des informations doit être réalisée dans des conditions garantissant leur confidentialité, notamment lors de leur transmission, ainsi que l'authentification des utilisateurs.

Cet outil de ticketing doit être accessible via Internet de manière sécurisée, idéalement au moyen d'un accès restreint par liste blanche.

Gestion des évolutions

Le pouvoir adjudicateur souhaite disposer d'un service souple et évolutif. Ces attentes portent notamment sur la possibilité de faire évoluer la bande passante des accès Internet, à la hausse comme à la baisse, ainsi que sur l'ajout de nouveaux accès ou le retrait d'accès existants.

Le titulaire met à jour l'ensemble des livrables impactés par les évolutions mises en œuvre.

Les opérations de vérification menées dans le cadre des évolutions des accès reprennent à minima la vérification de la mise à disposition du débit demandé sur les accès et la continuité de service en cas de dysfonctionnement. La durée de la validation d'aptitude en cas d'évolution de la bande passante est fixée à 1 journée.

La durée de validation d'aptitude d'un nouvel accès, déjà indiquée dans le paragraphe relatif au déploiement des services, est de 5 jours ouvrés.

Gestion des problèmes

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

La gestion des problèmes correspond à la recherche des causes sous-jacentes d'incidents afin d'éviter la récurrence d'incidents de même nature ainsi qu'à la recherche des causes sous-jacentes des dégradations de service (perte de paquet, temps de transit, ...).

Les procédures de gestion des problèmes sont soit initiées pro-activement par le titulaire soit demandées par le pouvoir adjudicateur.

Gestion des configurations des équipements d'extrémité

5.8.1 Qualité des configurations

Le titulaire déploie des configurations propres (utilisant le moins de ressources possibles, code commenté dans les documents, industrialisation maximale, ...) et restrictives, sans services inutiles.

Les configurations des équipements respectent les règles suivantes :

- 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 logicielles identiques.

Cela s'applique à la configuration des routeurs de l'opérateur présents sur les POP.

5.8.2 Validation des configurations

Le titulaire soumet à validation par le pouvoir adjudicateur toutes les configurations avant déploiement initial et avant toute modification. A cet effet, les configurations ont fait préalablement l'objet d'opérations de vérifications.

Le titulaire fournit une procédure de validation des mises à jour et les éléments suivants pour validation :

- les versions logicielles,
- la configuration complète et commentée,
- la liste des services et leur usage.

5.8.3 Administration des équipements par le titulaire

Le titulaire utilise des modes d'accès sécurisés et notamment à utiliser des mots de passe d'accès aux outils et équipements différents de ceux utilisés pour les autres clients. Ces mots de passe seront systématiquement différents des mots de passe constructeur ou par défaut. Cela s'applique aux mots de passe de protection des peerings.

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 à d'autres personnels du titulaire.

Les IP d'interco étant publiques, le titulaire doit avoir un mode d'accès et de paramétrage sécurisé.

5.8.4 Procédure de sauvegarde des configurations

Le titulaire met en œuvre une procédure de sauvegarde de chaque version des configurations.

L'historique de l'ensemble des configurations doit être conservé. Celles-ci sont clairement identifiées et indexées pour pouvoir être exploitées rapidement en cas de besoin. Le titulaire met à jour pendant toute la durée du marché les versions logicielles des différents équipements qu'il a fournis et dont il a la gestion.

Des tests réguliers de sauvegarde et de restauration sont effectués par le titulaire.

L'ensemble des modifications est tracé et imputable au personnel du titulaire chargé de l'exploitation.

5.8.5 Information sur les configurations

En cas de nécessaire mise à jour du système/firmware des routeurs d'extrémité et de la modification d'équipements réseau permettant de délivrer le service d'accès à internet sur chacun des 2 liens, le titulaire en informe le pouvoir adjudicateur au préalable.

Suivi de la qualité de service

Le titulaire fournit tous les éléments permettant au pouvoir adjudicateur de valider les engagements contractuels souscrits. Cela signifie que le titulaire est en mesure de communiquer des indicateurs de suivi de qualité de service en comparaison au niveau d'engagement et notamment (liste non exhaustive à compléter le cas échéant par le titulaire):

- charge des accès,
- taux de disponibilité,
- respect des temps de rétablissement du service,
- respect des délais de mise en œuvre des évolutions.

Le titulaire met à disposition du pouvoir adjudicateur ces indicateurs de suivi de qualité :

- dans les tableaux de bord mensuels et le suivi d'indicateurs,
- ou dans un outil, en accès Web, permettant de visualiser des statistiques sur l'évolution des indicateurs de suivi de la qualité de service.

Le pouvoir adjudicateur se réserve le droit d'engager une prestation d'ingénierie, réalisée en interne ou confiée à un tiers, lequel ne sera pas nécessairement le titulaire, afin de mener des audits de qualité et de performance sur les services fournis..

Suivi des mitigations anti-DDoS

Le titulaire assure un rapport de suivi et de clôture de chaque mitigation sous la forme d'un compte rendu au format PDF dans un formalisme simple et lisible défini avec le pouvoir adjudicateur en début de contrat. Ce rapport lui sera communiqué au plus vite, idéalement sous 24h, par le moyen le plus efficace.

Les mitigations automatiques et/ou de petite taille et les faux positifs pourront être exclus de ces rapports.

Reporting

Le titulaire transmet avant le 10 de chaque mois, des rapports opérationnels mensuels sous forme de tableaux de bord, de statistiques, au format OpenOffice, LibreOffice ou MS Office, incluant, a minima, les éléments ci-dessous :

- tous les incidents faisant l'objet d'engagements ;
- le niveau des débits clients constatés sur les équipements et nombre d'alertes sur seuil de dépassement associées ;

- le nombre de sessions simultanées sur les équipements et nombre d’alertes sur seuil de dépassement associées ;
- la répartition de l’utilisation de la bande passante par accès qui devra être cohérente avec le fonctionnement attendu ;
- le rapport des incidents survenus et des problèmes en cours d’investigation ;
- le cas échéant, les résultats sur les tests de fonctionnement des moyens de secours ;
- les dernières modifications réalisées ;
- les demandes et évolutions en cours de traitement ;
- les propositions de modifications et d’évolutions.

Reporting des mitigations anti-DDoS

Le titulaire transmet chaque mois un rapport d’attaques et de mitigations sous une forme à convenir avec le pouvoir adjudicateur, sous forme de tableaux de bord, au format OpenOffice, LibreOffice ou MS Office.

Le titulaire pourra intégrer son rapport de mitigations dans le rapport vu précédemment.

Le rapport fait référence à l’ensemble des compte-rendu de chaque attaque et mitigation du mois et présente une synthèse sous différents angles et d’anticiper les tendances.

Les mitigations automatiques et/ou de petite taille et les faux positifs pourront être exclus de ces rapports ou mentionnés de façon minimale.

6 ENGAGEMENTS

Les engagements de qualité de service et des pénalités associées (voir CCAP) permettent de répondre aux exigences du pouvoir adjudicateur.

Les engagements présentent les caractéristiques générales suivantes :

- l'engagement sur une garantie de temps de rétablissement du service débute à partir du signalement ou la remontée d'un incident occasionnant une interruption ou une dégradation du service ;
- les engagements s'entendent pour un incident signalé ou détecté dans les plages de maintenance définies. Pour un incident signalé ou détecté en dehors de la plage de maintenance, la GTRS s'applique dès le début de la plage de maintenance suivante. Pour un incident signalé ou détecté dans la plage de maintenance, la fin de la plage de maintenance n'entraîne pas le gel du ticket ni le décompte de la durée comptabilisée pour l'incident ;
- il appartient au titulaire de prouver la non disponibilité du contact site pour décompter le « temps de gel ». Le temps de gel ne peut en aucun cas inclure le temps de déplacement du technicien du titulaire, il ne peut inclure que les temps sous responsabilité du pouvoir adjudicateur ;
- dans le cas d'un incident générique qui impacte plusieurs accès les pénalités doivent être appliquées à chaque accès impacté, les GTRS sont liées à chaque accès ;
- les délais maximum de mise en œuvre des demandes d'exploitation courent à compter du dépôt de la demande par le pouvoir adjudicateur auprès des services du titulaire dans les plages d'exploitation définies.

Garantie de délai de mise en service d'un lien

Intitulé de l'engagement	Garantie de délai du déploiement d'un accès de transit Internet
Définition	Ce sont les délais de chaque étape telle que décrite dans le § « 4.3 – Etapes du projet ».
Méthode de mesure	Tel que décrit à l'article « 4.3 – Etapes du projet ».
Valeurs d'engagement	• Lancement : indicateur : 2 semaines • Etudes et spécifications : indicateur : < 4 semaines • Déploiement : < 16 semaines validation d'aptitude comprise

Garantie de délai de mise en œuvre des évolutions

Les engagements de mise en œuvre des évolutions attendus par le pouvoir adjudicateur sont les suivants :

Intitulé de l'engagement	Garantie de délai de mise en œuvre des évolutions
Définition	Délais d'exécution des évolutions à la hausse ou à la baisse du débit hors modification physique de l'interface
Méthode de mesure	Les délais d'exécution des évolutions courent à compter du dépôt de la demande par le pouvoir adjudicateur auprès des services du titulaire
Valeurs d'engagement	• Changement – délai nominal: inférieur à 1 semaine • Changement – délai d'urgence: à préciser dans le mémoire technique

Garantie de mise en œuvre des tâches d'exploitation

Les engagements de mise en œuvre des tâches d'exploitation attendus par le pouvoir adjudicateur sont les suivants :

Intitulé de l'engagement	Garantie de délai de mise en œuvre des tâches d'exploitation
Définition	Délais d'exécution des tâches d'exploitation
Méthode de mesure	Les délais d'exécution des tâches d'exploitation courent à compter du dépôt de la demande par le pouvoir adjudicateur auprès des services du titulaire dans les plages d'exploitation définies.
Valeurs d'engagement	• Changement – délai nominal : à préciser dans le mémoire technique • Changement – délai d'urgence: à préciser dans le mémoire technique

Disponibilité du service

L'engagement de disponibilité porte sur le service d'accès à Internet depuis un POP.

Les engagements de disponibilité attendus par le pouvoir adjudicateur sont les suivants :

Intitulé de l'engagement	Disponibilité mensuelle du service
Définition	Le service est partiellement ou totalement indisponible lorsqu'un incident de sévérité de niveau 1 ou 2 est déclaré
Méthode de mesure	L'indisponibilité mensuelle est calculée par POP avec le cumul des durées d'indisponibilité sur un mois, à partir des informations figurant dans les tickets d'incidents.
Valeurs d'engagement	• Disponibilité minimale du service de 99,9%

Garantie de temps de rétablissement

Intitulé de l'engagement	Garantie de temps de rétablissement des services de transit Internet
Définition	Temps maximum de rétablissement du service
Méthode de mesure	Le temps de rétablissement débute lors de l'ouverture d'un dossier d'incident de niveau 1 ou 2 auprès de support et finit lors du rétablissement du service (ou du remplacement du composant défectueux) permettant le rétablissement du fonctionnement nominal. Toute période pendant laquelle le contact site est injoignable (temps de gel) est décomptée
Valeurs d'engagement	GTR 4 heures 24h/24 7j/7

Bande passante garantie

Intitulé de l'engagement	Disponibilité mensuelle du débit garanti des services de transit Internet
Définition	Durée de disponibilité du débit garanti sur la période concernée (hors interruption de service pris en compte dans la disponibilité du service)
Méthode de mesure	La disponibilité au débit garanti vient de la supervision du pouvoir adjudicateur
Valeurs d'engagement	Bande passante garantie 100% du temps

Garantie de protection Anti-DDoS

Intitulé de l'engagement	Garantie de disponibilité de l'interface de mitigation
Définition	Disponibilité de l'interface de mitigation
Méthode de mesure	L'interface de mitigation est l'outil permettant à la DINUM de se protéger contre des attaques DDoS. Elle doit être disponible et offrir un fort niveau de réactivité. Cette mesure s'applique à tout instant
Valeurs d'engagement	- Login en moins de 2 minutes incluant le second facteur 2FA - Temps de réaction des commandes < 5s

Intitulé de l'engagement	Garantie d'accès concurrent à l'interface
Définition	Disponibilité d'accès simultané de 5 personnes à l'interface
Méthode de mesure	L'interface de mitigation est l'outil permettant à la DINUM de se protéger contre des attaques DDoS. Plusieurs experts et intervenants doivent pouvoir accéder en même temps à l'interface en lecture ou en lecture/écriture à des fins d'analyse et de protection. Cette mesure s'applique à tout instant
Valeurs d'engagement	Au moins 5 accès simultanés

Intitulé de l'engagement	Garantie de réception des alertes
Définition	Réception des messages d'alerte après leur envoi
Méthode de mesure	L'alerting du CSIRT est primordial pour garantir un bon temps de réaction lors d'une attaque. En situation normale, les alertes doivent être reçues au plus tard

	5 minutes après leur envoi par la plateforme du titulaire. Le titulaire doit donc disposer d'une infrastructure d'envoi d'alertes permettant de le garantir
Valeurs d'engagement	• Alerte reçue en moins de 5 minutes après envoi par la plateforme

7 EXPERTISE TECHNIQUE ET ACCOMPAGNEMENT A LA MITIGATION (UO TYPE 4)

Préalablement à la passation de chaque bon de commande et en raison de la complexité des prestations relevant de l'UO type 4, un devis de dimensionnement pourra être demandé au titulaire en fonction du besoin détaillé exprimé par le pouvoir adjudicateur.

Le titulaire transmet dans un délai maximum d'un mois, un devis sur la base des prix indiqués au BPU. Ces devis permettent de vérifier le caractère adéquat des modalités techniques et financières de la satisfaction des besoins du pouvoir adjudicateur.

Après validation par le pouvoir adjudicateur, le bon de commande afférent est émis. Le titulaire réalise les prestations conformément aux besoins exprimés et à son offre technique et financière.

Formation et transfert de compétences à l'outil de mitigation. (UO 4.0)

La solution déployée par le titulaire est soit dédiée soit mutualisée pour plusieurs clients. Le titulaire forme le personnel CSIRT DINUM et DINUM/ISO (NOC RIE et SOI) à l'utilisation de ces outils en tant que client, avant la mise en production de la solution.

Le CSIRT est l'utilisateur principal de cette solution en cas d'attaque pour engager toutes les mitigations nécessaires au bon rétablissement du service nominal. Il est prévu que le NOC RIE puisse lancer des mitigations selon un protocole de fiches réflexes rédigées avec le CSIRT.

L'équipe SOI est formée à l'utilisation de cet outil à des fins d'analyse mais il n'est pas prévu qu'elle puisse mettre en œuvre des mitigations.

La formation couvre à la fois les aspects théoriques et pratiques liés à la surveillance du trafic, à la détection des attaques et à leur mitigation. Le programme comprend la présentation de l'architecture globale, la configuration des politiques de mitigation, la gestion des alertes et des rapports.

A l'issue de la formation les participants seront en mesure d'interpréter les tableaux de bord, d'optimiser les stratégies de protection et de gérer efficacement les incidents de sécurité de type DDoS.

Expertise technique et diagnostic de flux (UO 4.1)

Le titulaire assure sur demande du pouvoir adjudicateur, une prestation d'expertise technique.

Le titulaire assure, sur demande du pouvoir adjudicateur, une prestation d'expertise de flux, sur les accès spécifiés par le pouvoir adjudicateur, et notamment sur :

- des tests de débit d'un lien de transit vers le réseau du titulaire (optique ...) ;
- des éléments de trafic (volume, pics, IP accounting, ...).

Cette prestation est formalisée par un document transmis au pouvoir adjudicateur. Ce livrable fait l'objet d'une vérification documentaire simple.

8 DESCRIPTION DES PRESTATIONS

Les prestations attendues par le pouvoir adjudicateur s'exécutent par émission de bons de commandes sur la base d'unités d'œuvre (à l'exception des UO type 4, qui font l'objet d'un devis de dimensionnement préalable au regard de leur complexité, voir article 7 du CCTP).

Une unité d'œuvre répond à un besoin précis et couvre un ensemble d'actions réalisées par le titulaire permettant de produire les livrables identifiés dans les délais convenus. Les livrables sont décrits au niveau de chaque prestation.

Pour chaque lot, le bordereau des prix unitaires présente les unités d'œuvre correspondant aux prestations attendues par le pouvoir adjudicateur sur chacun des POP, nominal et secours.

UOs de type 1

La série d'UO numérotées de 1.x concerne la mise en place du service et la gestion des accès pour le transit internet :

- UO 1.0 : gestion opérationnelle d'un lien FO 100GE ;
- UO 1.10 : raccordement initial FO 100GE du PIB PA3 ;
- UO 1.20 : raccordement initial FO 100GE du PIB PA4.

Livrables :

- Plan d'Assurance Qualité PAQ et Plan d'Assurance sécurité PAS
- Planning projet détaillé pour la phase de déploiement
- Spécifications d'architecture détaillées DATD des accès
- Plans d'adressage par accès
- Règles d'interfaçage entre les équipements du pouvoir adjudicateur et ceux du titulaire
- Spécifications détaillées de l'administration, de l'exploitation, de la sécurisation et de la supervision des accès DEX
- Dossier de configuration des équipements d'extrémité incluant les configurations logicielles et matérielles par type d'accès et les versions d'Os des équipements déployés
- Plan Qualité Service Client (PQSC)
- Planning de déploiement des sites
- Cahier de tests pour les opérations de vérification

Validation :

- Vérifications documentaires simples
- Vérification d'aptitude
- Vérification de service régulier

UO de type 2

La série d'UO concerne la bande passante du lien transit internet :

UO 2.0 : gestion opérationnelle d'un service d'accès Internet de 11Gbps à 100Gbps. Prix par lien au Gbps.

Livrables :

- Compte-rendu de réunion
- Bilan et rapports opérationnels depuis le comité de pilotage précédent

Validation :

- Vérifications documentaires simples

UO de type 3

La série d'UO concerne la gestion du service anti-DDoS :

- UO 3.0 : déploiement du service anti-DDoS opérateur ;
- UO 3.1 : gestion opérationnelle du service anti-DDoS opérateur ;
- UO 3.2 : licences pour 4 AED 8200 Netscout ;
- UO 3.3 : maintenance pour 4 AED 8200 Netscout ;
- UO 3.4 : licence pour 1 AEM pour 4 AED 8200 Netscout ;
- UO 3.5 : abonnement AIF pour 4 AED 8200 Netscout.

UO de type 4

La série d'UO est relative à l'expertise technique et l'accompagnement à la mitigation.

- UO 4.0 : expertise technique et diagnostic de flux ;
- UO 4.1 : formation et transfert de compétences à l'outil de mitigation.

Livrables :

- Support de formation
- Rapport d'analyse

Validation :

Vérification documentaire simple du livrable écrit, complétée le cas échéant par une restitution orale accompagnée d'un support ou d'un compte rendu.

9 GLOSSAIRE

ACL	Access Control List
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
AS	Autonomous System
BGP	Border Gateway Protocol
CCTP	Cahier des Clauses techniques Particulières
COSSI	Centre Opérationnel de la Sécurité des Systèmes d'Information
DC	Datacenter ministériel
DGAFP	Direction Générale de l'Administration et de la Fonction Publique
DINUM	Direction Interministérielle du Numérique
DISIC	Direction Interministérielle des Systèmes d'Information et de Communication
DQE	Devis Quantitatif Estimatif
DWDM	Dense Wavelength Division Multiplexing
FON	Fibre Optique Noire
GTR	Garantie de Temps de Rétablissement
IdF	Ile de France
IRU	Indefeasible Right of Use
Incident	« Tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service. »
LAN	Local Area Network
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NOC	Network Operation Center
NR	Nœud de raccordement
OSI	Open Systems Interconnection
PIB	Voir renommage POP (site) ou RED (routeur)
PMD	Polarisation Mode Dispersion
Problème	« Cause inconnue d'un incident significatif ou de plusieurs incidents présentant les mêmes symptômes affectant le bon fonctionnement du système d'information »
PLS	Point de Livraison de Service
PV	Procès Verbal
RGAA	Référentiel Général d'Accessibilité
RGI	Référentiel Général d'Interopérabilité
RGS	Référentiel Général de Sécurité
RED	Routeur d'Epine Dorsale
RIE	Réseau Interministériel de l'Etat
SAE	Services Achats de l'Etat

Shelter	Lieu d'hébergement de l'opérateur FON, permettant d'accueillir des équipements optiques intermédiaires du backbone RIE nécessaires à l'amplification et parfois à la régénération du signal optique.
SIC	Systèmes d'Information et de Communication
SOC	Security Operation Center
SIDISIC	Services Interministériels Départementaux des Systèmes d'Information et de Communication
Span	Un span est un segment de FON entre deux shelters, ou entre un POP et un shelter
Tronçon	Le tronçon est une liaison FON de bout en bout, constituée d'un ensemble de span, raccordant deux sites appartenant au pouvoir adjudicateur ou à un hébergeur tiers pour le compte du pouvoir adjudicateur.
VLAN	Virtual LAN
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

10 ANNEXES

Adresse des POP du RIE v2

- PA3 Ministère de l'Intérieur, 1 boulevard Théophile Sueur, 93 110 Rosny-sous-Bois
- PA4 Centre Informatique des Douanes, 27, rue des beaux soleils, 95 520 Osny

Historique - Caractérisation des configurations, alertes et attaques

En 2017, lors de la mise en place de l'anti-DDoS sur nos accès, nous avons noté des attaques par paquets bogons (avec pour IP source des IP privées RFC1918). Ces attaques sont maintenant filtrées par nos transitaires par ACL sur leurs routeurs.

En 2017 durant une attaque une annonce de route a été « hijackée » très furtivement.

En 2019, lors d'une attaque sur un accès, une mauvaise configuration des tunnels GRE d'un de nos deux transitaires nous a fait perdre des routes et a fait qu'il s'est mis à nous annoncer nos propres routes. Depuis ce jour, nous avons bloqué ce type d'annonces sur nos routeurs de transit par sécurité.

En 2020, de nouvelles attaques consistaient à spoofer (source) des IP de nos propres préfixes. Ces attaques sont maintenant bloquées sur nos routeurs de transit.

Les attaques sont variées et adaptatives au fil des mitigations. Le plus souvent il s'agit d'attaques sur des serveurs d'infrastructure (DNS...) ou web, et en ICMP, UDP ou TCP.

La volumétrie et la durée des attaques est variable de 10Mbps à plusieurs 320 Gbps (36h).

Tiers Transit IP : de niveau Tier 1 au niveau Tier 3

La hiérarchie d'Internet est souvent classée en trois niveaux distincts, avec le niveau Tier 1 le plus haut. Comprendre les différences entre ces niveaux est essentiel pour apprécier la valeur des opérateurs de Transit IP.

NB : le niveau de « Tier » d'un réseau de Transit IP n'est pas comparable au niveau de « Tier » d'un centre de données, la gradation étant même inversée.

Tier 1: Ce sont des opérateurs mondiaux qui ont accès à l'ensemble de l'Internet. Ils s'échangent gracieusement (settlement-free peering) des flux IP entre opérateurs Tier 1.

Tier 2: les opérateurs achètent souvent du transit à des réseaux de niveau Tier 1. Ils peuvent établir des peering payants avec d'autres réseaux pour réduire leurs coûts de transit et améliorer les performances. Ils n'ont pas la présence mondiale d'un fournisseur de niveau 1.

Tier 3: Ce sont généralement des FAI régionaux qui dépendent entièrement de l'achat de transit IP auprès d'opérateurs majeurs de niveau Tier 1 ou Tier 2. Ils ont une portée de réseau limitée et dépendent de leurs opérateurs pour router des paquets à destinations mondiales.

Configuration des peering des titulaires actuels

<i>Peering AS174</i>	<i>Cogent (USA)</i>	<i>Tier 1</i>
<i>Peering AS1273</i>	<i>Vodafone (UK)</i>	<i>Tier 2</i>
<i>Peering AS1299</i>	<i>Arelion (Telia, Suède)</i>	<i>Tier 1</i>
<i>Peering AS2914</i>	<i>NTT USA</i>	<i>Tier 1</i>
<i>Peering AS3320</i>	<i>Deutsche Telekom (GER)</i>	<i>Tier 1</i>
<i>Peering AS6762</i>	<i>Telecom Italia (IT)</i>	<i>Tier 1</i>