CROUS AIX-MARSEILLE AVIGNON

Direction des Systèmes d'Information

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

Marché de maintien en condition opérationnelle

WAN — SD-WAN — UCaaS

Accord-cadre — Appel d'offres ouvert européen

Marché de continuité — Référence : **260667**

Version 1.0 — 2026

Préambule

Au sein de ce Cahier des Clauses Techniques Particulières (CCTP), certaines parties sont présentées de manière particulière afin d'attirer l'attention du candidat sur des points nécessitant une réponse spécifique dans le dossier de réponse.

Rx.x	*Remarque X.X : Il s'agit d'une remarque ou d'un point particulier nécessitant une réponse spécifique dans le dossier de réponse,*

1. Objet du marché

Le présent Cahier des Clauses Techniques Particulières a pour objet de définir les prestations attendues dans le cadre d'un marché de maintien en condition opérationnelle, d'exploitation, de support et d'évolution du réseau WAN, de l'infrastructure SD-WAN et des services de téléphonie d'entreprise en mode UCaaS du **Crous Aix-Marseille Avignon**.

Le présent marché s'inscrit dans la continuité du marché précédent relatif à l'interconnexion de sites, à l'accès Internet, au projet SD-WAN et aux services UCaaS associés, dont le déploiement a été conduit de 2023 à 2025. Il ne constitue pas un nouveau projet de refonte globale mais vise prioritairement :

- le maintien en condition opérationnelle de l'architecture déployée ;
- la prise en charge des incidents, des demandes de service et des évolutions courantes ;
- la continuité des services de téléphonie hébergée ;

Le titulaire devra assurer une parfaite continuité de service vis-à-vis de l'architecture actuellement en production, sans remise à plat, sans migration non justifiée et avec un niveau élevé de reprise de l'existant tant sur la partie réseau WAN que sur la partie téléphonie.

2. Contexte et périmètre général

2.1 Contexte du marché

Le **Crous Aix-Marseille Avignon** dispose d'une infrastructure de réseau WAN et de téléphonie unifiée gérée par un prestataire unique. Le marché précédent a porté sur l'évolution du réseau historique MPLS vers une architecture SD-WAN Fortinet et sur la mise en place de services de téléphonie UCaaS. Depuis 2023, les sites ont été progressivement migrés vers cette architecture SD-WAN, dont le déploiement est désormais achevé.

L'architecture actuellement en production repose sur les composants suivants :

- des boîtiers FortiGate déployés sur les sites distants, selon leur profil de criticité (FortiGate 40F pour les sites simples, FortiGate 60F en cluster pour les sites sensibles) ;
- un cluster FortiGate 200G au siège, maintenu dans le cadre d'un contrat séparé hors périmètre du présent marché — ces équipements sont mentionnés ici pour la

compréhension de l'architecture globale mais ne font l'objet d'aucune prestation de MCO dans le présent marché ;
- FortiManager et FortiAnalyzer, déployés sous forme de machines virtuelles dans l'infrastructure de virtualisation interne du **Crous Aix-Marseille Avignon** ;
- une solution de téléphonie UCaaS fondée sur Alcatel OmniPCX Enterprise, hébergée par le prestataire, avec des profils utilisateurs déployés, des terminaux en production et des services fonctionnels en place ;
- des liens d'interconnexion de sites sur le réseau RAIMU (réseau de l'Université d'Aix-Marseille) coexistant avec les accès WAN du périmètre du présent marché.

2.2 Périmètre géographique

Le périmètre initial du marché couvre, à la date de notification, un ensemble estimé entre 32 et 35 sites répartis sur le territoire de responsabilité du **Crous Aix-Marseille Avignon**.

Ce nombre sera confirmé à la date de notification et constitue le périmètre fixe du marché, tel que détaillé dans l'annexe inventaire des sites.

3. Principes directeurs du marché

3.1 Marché de continuité et de stabilité

Le titulaire devra assurer une parfaite continuité de service vis-à-vis de l'architecture actuellement exploitée. Il est attendu que les prestations proposées limitent au maximum toute rupture d'architecture, toute remise à plat ou toute opération de migration qui ne serait pas strictement nécessaire à la continuité de service, au maintien de la sécurité ou au maintien du support éditeur. Le présent marché est un marché de MCO stricte de l'existant.

Le titulaire devra démontrer dans son mémoire technique sa maîtrise des technologies Fortinet (SD-WAN, FortiGate, FortiManager, FortiAnalyzer) et Alcatel-Lucent Enterprise (OmniPCX Enterprise, écosystème UCaaS) et justifier de son aptitude à reprendre l'exploitation de l'architecture existante à compter du premier jour du marché.

R3.1	*Remarque 3.1 : Le titulaire précisera dans son mémoire technique la méthodologie de prise en charge du périmètre à la notification, les délais de montée en charge de son équipe, les outils et accès qu'il nécessite pour reprendre l'exploitation, et les risques identifiés lors de la transition.*

3.2 Maîtrise financière et cadre tarifaire

Le marché repose sur un bordereau des prix unitaires (BPU) contractuel, détaillé et exploitable pendant toute la durée d'exécution. Les prix pourront être exprimés selon deux mécanismes complémentaires :

- des prix unitaires fermes pour les prestations récurrentes et les services définis à l'avance ;
- des taux de remise garantis par famille de produits sur les tarifs catalogue constructeur, pour les équipements, licences et prestations commandés à la demande.

Le mécanisme de remise catalogue devra couvrir non seulement les références présentes au catalogue au moment de la notification du marché, mais également les gammes futures amenées à remplacer des références existantes, afin de permettre le remplacement ou l'extension du parc même si un modèle n'est plus disponible à la commande.

R3.2	*Remarque 3.2 : Le titulaire précisera dans son offre le mode d'application des remises par famille de produits Fortinet et Alcatel-Lucent Enterprise, le mécanisme de révision des tarifs catalogue de référence, et sa capacité à maintenir les taux de remise contractuels sur les gammes successeurs.*

R3.3	*Remarque 3.3 : Le titulaire précisera dans son offre son aptitude à mettre en place un système de facturation lissé permettant une péréquation des remises sur l'ensemble de l'année civile, avec une hiérarchisation de la facturation en trois niveaux minimum (service, site, entité).*

3.3 Développement durable et RSE

Le titulaire précisera les dispositions prises en matière de responsabilité sociétale des entreprises, de limitation des déplacements, de reconditionnement ou de reprise des matériels en fin de vie, de réduction des emballages, de maîtrise énergétique des solutions proposées et de politique d'insertion professionnelle, conformément à l'article 14 du Décret n°2016-360 du 25 mars 2016.

R3.4	*Remarque 3.4 : Le titulaire présentera dans son offre une synthèse d'une page de sa démarche RSE en lien avec l'objet du marché.*

3.4 Clause de réversibilité

Le titulaire devra prévoir les modalités de réversibilité permettant, en fin de marché ou en cas de changement de titulaire, d'assurer la continuité de service, la restitution des données, la remise de la documentation à jour, la transmission des configurations et la coopération nécessaire avec le pouvoir adjudicateur et, le cas échéant, avec le titulaire entrant.

Trois mois avant l'échéance du marché, le titulaire devra fournir l'ensemble des informations et documentations techniques utiles, notamment : l'état de parc complet, le plan d'adressage, le paramétrage explicite documenté de l'ensemble des systèmes WAN, SD-WAN et UCaaS, ainsi que les fichiers de configuration de chaque équipement et système.

À l'issue du marché, la solution UCaaS hébergée devra être dans une version logicielle encore maintenue et commercialisée par l'éditeur pour au moins 12 mois, afin de permettre la continuité de service sans contrainte immédiate de mise à jour pour le titulaire entrant.

R3.5	*Remarque 3.5 : Le titulaire précisera dans son offre les conditions de réversibilité, les délais d'assistance au titulaire entrant (au moins 2 mois), les modalités pratiques de transfert documentaire et les limites de son engagement. Il accepte l'application de pénalités fortes en cas de non-respect des engagements de réversibilité, telles que définies au CCAP.*

4. Pilotage du marché

4.1 Gouvernance et interlocuteurs

Le titulaire mettra en place une gouvernance adaptée comprenant a minima : un interlocuteur contractuel, un responsable technique, un point d'entrée support identifié et des modalités d'escalade adaptées aux niveaux de sévérité des incidents.

Le titulaire organisera a minima une réunion de lancement après notification, des comités de suivi opérationnel hebdomadaires ou bimensuels pendant les phases de projet, des comités de pilotage trimestriels pendant la phase d'exploitation courante, et toute réunion exceptionnelle requise en cas d'incident majeur ou d'évolution structurante.

R4.1	*Remarque 4.1 : Le titulaire présentera dans son offre l'organisation de son équipe projet et support, les modalités d'escalade, la fréquence et les thèmes des réunions proposées, et les outils de visioconférence mis à disposition.*

4.2 Base documentaire

Le titulaire tiendra à jour une base documentaire complète comprenant : le Plan Qualité Service (PQS), le Dossier d'Architecture Technique (DAT), le Dossier d'Exploitation (DOE), les inventaires d'équipements et de licences, les plans d'adressage, les matrices de flux, les procédures de sauvegarde et de restauration, les comptes rendus d'intervention et tout document nécessaire à l'exploitation du service.

Les documents devront être mis à jour au fil de l'eau et consolidés a minima mensuellement ou à chaque modification significative de l'architecture, du paramétrage ou du parc. L'évolution mensuelle du parc (équipements SD-WAN, accès WAN, licences UCaaS) fera l'objet d'un fichier au format exploitable (XLSX, CSV ou équivalent) transmis au **Crous Aix-Marseille Avignon**.

R4.2	*Remarque 4.2 : Le titulaire présentera dans son offre la liste complète des livrables documentaires prévus, leur fréquence de mise à jour et les modalités d'accès par le Crous Aix-Marseille Avignon.*

4.3 Outils de suivi

Le titulaire mettra à disposition un portail extranet ou un outil équivalent permettant le suivi des incidents, des demandes de service, des changements, des interventions, de la facturation, des actifs et des indicateurs de qualité de service. Cet outil devra permettre l'export des données dans un format exploitable (XLSX, CSV ou équivalent).

R4.3	*Remarque 4.3 : Le titulaire présentera dans son offre les fonctionnalités de son portail extranet, les droits d'accès proposés et les indicateurs de qualité de service mis à disposition du Crous Aix-Marseille Avignon.*

5. Infrastructure WAN et accès opérateurs

5.1 Description de l'existant WAN

Le titulaire prendra en charge l'exploitation de l'ensemble des accès WAN et Internet nécessaires au fonctionnement des sites du périmètre. L'existant comprend différentes typologies de liens selon le profil et la criticité de chaque site :

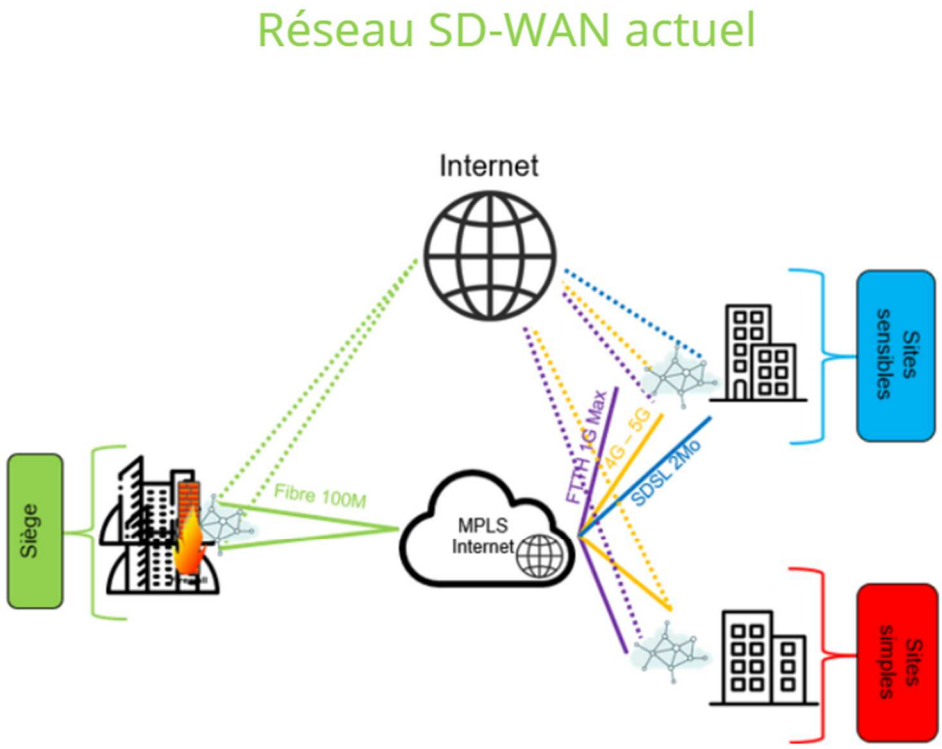
- accès FTTH (fibre mutualisée) pour les sites simples et sensibles ;
- accès xDSL (ADSL/VDSL) dans le cas où le site n'est pas éligible à la FTTH ;
- accès FTTO (fibre dédiée) pour les sites à haute criticité ou à forts débits ;
- accès SDSL sur support cuivre pour certains non éligible la FTTO ;
- accès 4G/5G en solution de secours ou en lien principal provisoire pour certains sites.

L'inventaire détaillé des accès en place à la date de notification fait l'objet de l'annexe « État de parc » jointe au marché. Cet état de parc constitue la base contractuelle de prise en charge des accès existants.

A noter également que le **Crous Aix-Marseille Avignon** dispose aujourd'hui également d'une 20aine de liens d'interconnexion de sites sur le réseau RAIMU (https://dirnum.univ-amu.fr/fr/reseau). Ces liens sont hors périmètre du présent marché mais le titulaire devra en avoir connaissance pour comprendre la topologie complète et s'y adapter le cas échéant.

5.2 Prestations attendues sur les accès WAN

Le **Crous Aix-Marseille Avignon** dispose aujourd'hui d'un **réseau SD-WAN,** basé sur la solution Fortinet, interconnectant l'ensemble de ses sites propres (et hébergeurs) et disposant d'une sortie Internet centralisée sur le site principal ainsi qu'une évasion locale pour les sites distants.



Le titulaire prendra en charge l'exploitation de l'ensemble des accès WAN et Internet nécessaires au fonctionnement des sites. L'existant comprend différentes typologies de liens, notamment FTTH, FTTO, SDSL, xDSL ainsi que des accès mobiles 4G et 5G selon les usages et les niveaux de résilience recherchés.

Le titulaire prendra en charge le maintien en condition opérationnelle de l'architecture SD-WAN Fortinet déployée sur le périmètre du **Crous Aix-Marseille Avignon**. Cette architecture comprend un cluster FortiGate 200G au siège, ainsi que des équipements Fortinet implantés sur les sites distants en fonction des besoins locaux et du niveau de criticité de chaque site :

- 2x FortiGate 60F pour les sites sensibles
- 1x FortiGate 40F pour les sites simples

Les fonctions de gestion centralisée et de journalisation reposent sur FortiManager et FortiAnalyzer, déployés sous forme de machines virtuelles dans l'environnement d'hébergement du **Crous Aix-Marseille Avignon**. L'accès du titulaire à ces composants est réalisé via un accès VPN sécurisé encadré par le **Crous Aix-Marseille Avignon**, dans le respect du principe de moindre privilège et des règles de sécurité définies par l'établissement.

Le titulaire assurera la supervision, la maintenance, le traitement des incidents, le suivi des tickets opérateurs, la gestion des escalades, le suivi des délais de mise en service, la gestion des modifications et des suppressions d'accès, ainsi que l'assistance au pilotage du parc de liens.

Le titulaire portera, pour le compte du **Crous Aix-Marseille Avignon**, la relation opérationnelle avec les opérateurs de boucle locale, de collecte ou d'accès, selon le modèle contractuel retenu, afin de limiter la charge d'exploitation pour les équipes internes du **Crous Aix-Marseille Avignon**.

R5.1	*Remarque 5.1 : Le titulaire précisera dans son offre ses engagements contractuels avec les opérateurs sous-jacents, les mécanismes de garantie de temps de rétablissement end-to-end et les niveaux de service garantis par type d'accès.*

5.3 Évolutivité du parc WAN

Le titulaire devra être en mesure de modifier, résilier, migrer ou faire évoluer tout accès pendant la durée du marché. Les délais indicatifs de référence sont présentés dans le tableau ci-après. Ces délais constituent des engagements contractuels fermes et non de simples délais moyens constatés.

Type d'accès	Modification	Résiliation
ADSL / VDSL (cuivre)	5 jours ouvrés	48 heures
FTTH	5 jours ouvrés	48 heures
SDSL (cuivre)	5 jours ouvrés	48 heures
FTTO / Fibre dédiée	5 jours ouvrés	48 heures
4G/5G (activation)	48 heures	48 heures

R5.2	*Remarque 5.2 : Le titulaire précisera dans son offre son engagement du respect de ces délais ou des délais plus favorables qu'il peut proposer, item par item. Il précisera également les conditions de résiliation anticipée, les engagements minimaux par type d'accès et les pénalités associées en cas de dépassement.*

5.4 Niveaux de service WAN

Le titulaire précisera pour chaque type de lien les garanties de temps de rétablissement (GTR), les plages horaires de couverture (a minima GTR 4H HNO 24h/24 7j/7 pour les liens critiques), les conditions de supervision et les mécanismes de pénalités associés.

La solution proposée devra permettre la mise en œuvre d'une politique de qualité de service (QoS) permettant le transport de la voix, de la vidéo et de la data, avec une capacité de segmentation par type de flux et par classe de service.

R5.3	*Remarque 5.3 : Le titulaire précisera son offre de service pour le transport des flux voix, vidéo et data, notamment le taux de disponibilité de son réseau, les délais de transit, la gigue mesurée, et les classes de service disponibles. Aujourd'hui 3 classes de service sont en place.*

6. Infrastructure SD-WAN Fortinet

6.1 Description de l'architecture SD-WAN en place

Le titulaire prendra en charge le maintien en condition opérationnelle de l'architecture SD-WAN Fortinet déployée sur l'ensemble du périmètre. Cette architecture comprend les composants suivants :

6.1.1 Équipements sur les sites distants

Les boîtiers FortiGate sont déployés selon le profil de chaque site :

- Sites simples : un équipement FortiGate 40F, raccordé à un lien FTTH/xDSL principal et un secours 4G ;
- Sites sensibles : un cluster de deux équipements FortiGate 60F, raccordés à un lien FTTH/xDSL principal, un lien FTTO/SDSL et un secours 4G.

6.1.2 Équipements du siège

Un cluster FortiGate 200G est en place au siège, raccordé à deux liens FTTO, 1 lien FTTH et 1 lien de l'opérateur RAIMU qui ne fait pas parti du périmètre du titulaire. Ces équipements font l'objet d'un contrat de maintenance séparé et sont exclus du périmètre de MCO du présent marché. Le titulaire en aura néanmoins connaissance pour assurer la cohérence globale de l'architecture SD-WAN.

6.1.3 Outils de gestion centralisés

FortiManager (FMG) et FortiAnalyzer (FAZ) sont déployés sous forme de machines virtuelles dans l'infrastructure de virtualisation interne du **Crous Aix-Marseille Avignon**. Le titulaire accède à ces composants via un accès VPN sécurisé, encadré par le **Crous Aix-Marseille Avignon**, dans le respect du principe de moindre privilège et des règles de sécurité définies par l'établissement.

6.1.4 Architecture de tunnels SD-WAN en place

L'architecture SD-WAN repose sur une topologie de tunnels IPsec montés entre chaque lien disponible sur les sites distants et les liens du siège. Le titulaire assure le maintien, la supervision et la restauration de l'ensemble de ces tunnels dans le cadre de la MCO. Le détail des paramètres (interfaces, adressage, politiques IKE/IPsec) figure dans le Dossier d'Architecture Technique (DAT) joint en annexe. La matrice contractuelle de tunnels par profil de site est la suivante :

- ✓ **Site simple (FG40F) — 4 tunnels maintenus :** lien FTTH site ↔ FTTH siège — lien FTTH site ↔ RAIMU siège — lien 4G site ↔ FTTH siège — lien 4G site ↔ RAIMU siège.
- ✓ **Site sensible (FG60F cluster) — 5 tunnels maintenus :** lien FTTH site ↔ FTTH siège — lien FTTH site ↔ RAIMU siège — lien 4G site ↔ FTTH siège — lien 4G site ↔ RAIMU siège — lien MPLS site ↔ MPLS siège.

Le lien RAIMU du siège est utilisé comme extrémité de tunnel SD-WAN uniquement. La sortie Internet principale du **Crous Aix-Marseille Avignon** via RAIMU est hors périmètre du présent marché.

R6.1	*Remarque 6.1 : Le titulaire précisera dans son offre sa maîtrise des technologies FortiGate, FortiManager et FortiAnalyzer, et les certifications Fortinet détenues par ses équipes (niveau NSE minimum requis et niveaux supérieurs détenus).*

6.2 Prestations de MCO sur les équipements SD-WAN des sites

Le titulaire assurera la maintenance corrective, préventive et évolutive des équipements FortiGate 40F et 60F exploités dans le cadre du marché. Les prestations comprennent notamment :

- le diagnostic des incidents et la résolution des pannes ;
- l'assistance à distance et les interventions sur site lorsque nécessaire ;
- la gestion des configurations et la cohérence des politiques SD-WAN ;
- la gestion des règles de sécurité liées au service SD-WAN ;
- la vérification régulière du bon fonctionnement des mécanismes de résilience (basculement de liens, cluster HA) ;
- le maintien de la cohérence des versions logicielles FortiOS entre les boîtiers et les outils de gestion ;
- la préparation et l'application des mises à jour de sécurité et des montées de version FortiOS, en cohérence avec la matrice de compatibilité Fortinet ;
- la gestion des licences FortiGuard (bundles UTP ou équivalent) et leur renouvellement annuel ;
- la coordination des opérations de remplacement en cas de défaillance matérielle ou d'obsolescence.

R6.2	*Remarque 6.2 : Le titulaire précisera dans son offre sa méthodologie d'intervention sur site, les délais d'intervention par niveau de sévérité, et ses engagements en matière de remplacement matériel (délais de fourniture d'un équipement de substitution).*

6.3 Prestations de MCO sur FortiManager et FortiAnalyzer

6.3.1 Périmètre du titulaire

Le périmètre du titulaire comprend l'administration fonctionnelle et logicielle de FortiManager et de FortiAnalyzer. Les prestations incluent notamment :

- les mises à jour logicielles de FMG et FAZ, en cohérence avec les versions FortiOS des boîtiers gérés ;
- la vérification de la compatibilité de version avant toute opération de mise à jour (respect de la matrice de compatibilité Fortinet) ;
- la sauvegarde régulière des configurations FortiManager ;
- le contrôle du bon fonctionnement des outils (synchronisation des politiques, réception des logs, alertes) ;
- la gestion des licences FortiCare associées aux VMs (renouvellement annuel valorisé au BPU) ;
- l'analyse des alertes et des journaux, et l'assistance à l'exploitation quotidienne.

6.3.2 Périmètre du Crous Aix-Marseille Avignon

Le périmètre du **Crous Aix-Marseille Avignon** couvre l'infrastructure d'hébergement des machines virtuelles, à savoir l'hyperviseur, le stockage, les ressources d'infrastructure, les sauvegardes d'infrastructure, les snapshots et les éléments d'exploitation relevant strictement de la plateforme de virtualisation interne. Toute indisponibilité liée à l'infrastructure de virtualisation est exclue du périmètre de responsabilité du titulaire.

6.3.3 Modalités d'accès à distance

Le titulaire accède à FortiManager et FortiAnalyzer via un accès VPN dédié, encadré et mis à disposition par le **Crous Aix-Marseille Avignon**. Cet accès est soumis à un principe de moindre privilège, à une traçabilité complète des connexions et au respect des règles de sécurité définies par le **Crous Aix-Marseille Avignon**. Le titulaire s'engage à n'utiliser cet accès qu'à des fins strictement nécessaires à l'exécution du marché.

R6.3	*Remarque 6.3 : Le titulaire détaillera dans son offre les modalités précises d'intervention à distance via le VPN mis à disposition, les prérequis éventuels, les mesures de traçabilité mises en œuvre et les contraintes de sécurité respectées.*

6.4 Supervision et métrologie

Le titulaire assurera une supervision continue de l'infrastructure SD-WAN et fournira des éléments de métrologie permettant le suivi de la disponibilité des liens, des performances, des basculements de liens, de la consommation des accès, des événements de sécurité et des incidents récurrents.

Le titulaire pourra s'appuyer sur les outils déjà déployés (DigitalView ou équivalent) ou proposer tout outil équivalent, sous réserve de compatibilité avec l'environnement existant et de validation par le **Crous Aix-Marseille Avignon**. Les données de supervision devront être exportables au format CSV ou XLSX.

R6.4	*Remarque 6.4 : Le titulaire précisera dans son offre l'outil de supervision proposé, les indicateurs disponibles, la fréquence de collecte, les modalités d'accès du Crous Aix-Marseille Avignon aux tableaux de bord et les capacités d'export des données.*

6.5 Commandes de matériel Fortinet à la demande

Le présent marché n'a pas pour objet l'acquisition initiale d'un parc Fortinet, le **Crous Aix-Marseille Avignon** ayant déjà investi dans les équipements nécessaires au déploiement du SD-WAN. En revanche, le marché doit permettre la commande ponctuelle, à la demande, d'équipements Fortinet, de licences, de bundles FortiGuard, de services de support éditeur et de matériels de remplacement ou d'extension.

Le titulaire proposera un mécanisme contractuel fondé sur l'application de taux de remise contractuels par famille de produits sur le tarif catalogue Fortinet. Ce mécanisme devra couvrir non seulement les références disponibles au catalogue au moment de la notification, mais

également les gammes futures amenées à remplacer les références existantes, selon le principe de continuité de gamme défini ci-après.

Principe de continuité de gamme : si un équipement à remplacer n'est plus disponible au catalogue Fortinet au moment du besoin, le titulaire proposera l'équipement successeur de gamme équivalente et appliquera les taux de remise contractuels correspondant à la famille du successeur. Ce mécanisme est opposable pendant toute la durée d'exécution du marché.

R6.5	*Remarque 6.5 : Le titulaire précisera dans son offre les taux de remise applicables par famille de produits Fortinet (équipements low-end, high-end, accessoires, licences et souscriptions), le tarif catalogue de référence retenu et la méthode de mise à jour de ce catalogue en cours de marché.*

7. Services de téléphonie UCaaS

7.1 Description de l'existant

La solution de téléphonie en place repose sur Alcatel OmniPCX Enterprise (OXE), couplé à la plateforme de communications unifiées Rainbow Entreprise (Alcatel-Lucent Enterprise), hébergée par le titulaire dans un modèle UCaaS par abonnement mensuel par profil utilisateur. Elle couvre l'ensemble des sites du **Crous Aix-Marseille Avignon**.

Le dimensionnement actuel de la solution comprend notamment (les chiffres sont donnés à titre indicatif et peuvent évoluer) :

- 441 numéros SDA ;
- environ 300 licences utilisateurs réparties comme suit : des licences simples (dont environ 58 mobiles DECT et des hard phones avec ou sans option messagerie vocale), 124 licences communication unifiée Rainbow Entreprise, environ 10 licences agent ACD, et 1 licence poste opérateur ;
- une console d'administration téléphonie et communication unifiée ;
- environ 250 terminaux hard phone (types Alcatel IPTouch 8008/8018, 8028s/8038/8068s, ALE-300, ALE-20) ;
- 58 mobiles DECT (types Alcatel 8232s et 8234) ;
- 40 bornes IP-DECT type Alcatel 8378.

Les communications sortantes sont facturées à l'usage selon un coût à la minute par destination, inclus dans le forfait illimité métropole fixe et mobile.

L'état de parc détaillé de la solution UCaaS fait l'objet de l'annexe « État de parc UCaaS » jointe au marché.

7.2 Prestations de MCO sur la solution OXE hébergée

Le titulaire assurera la supervision, la maintenance, le support, la gestion des incidents, les mises à jour applicatives, les correctifs de sécurité, la sauvegarde et les opérations de restauration nécessaires au maintien du service de téléphonie hébergée. Les prestations comprennent notamment :

- la surveillance continue de la disponibilité de la solution et de la qualité d'acheminement des appels ;
- la gestion corrective et curative des incidents, selon les niveaux de sévérité définis au chapitre 8 ;
- la maintenance préventive annuelle (analyse des logs, alertes systèmes, mesures de performance, vérification des sauvegardes) ;
- les mises à jour applicatives de l'OXE et des composants associés, dans une version maintenue par l'éditeur ;
- la sauvegarde régulière des configurations et des bases de données de la solution, et les procédures de restauration ;
- l'administration fonctionnelle courante (gestion des profils, des groupements, des règles d'accueil, des plages horaires) ;
- le maintien à jour de la documentation technique de la solution (DAT, DOE, collecte des données).

La solution devra être maintenue dans une version applicative commercialisée et supportée par l'éditeur Alcatel-Lucent Enterprise pendant toute la durée du marché.

R7.1	*Remarque 7.1 : Le titulaire précisera dans son offre les certifications Alcatel-Lucent Enterprise détenues par ses équipes, sa maîtrise de la solution OXE hébergée ainsi que de Rainbow Entreprise, et la roadmap éditeur applicable aux composants de la solution en place.*

7.3 Maintien des services fonctionnels existants

Le titulaire assurera le maintien de l'ensemble des services fonctionnels en production à la date de notification du marché, sans modification ni régression fonctionnelle. Ces services comprennent notamment :

- la téléphonie IP sur postes fixes (hard phones) et softphones ;
- la téléphonie mobile indoor (DECT) sur certains sites ;
- les services de communication unifiée (profil C) ;
- le service d'accueil ACD (file d'attente, scripts vocaux DTMF, supervision) ;
- les scripts d'accueil SVI par entité (plages horaires, messages d'accueil de jour et de nuit, messages d'attente) ;
- les groupements de postes par entité (modes séquentiel, cyclique, parallèle) ;
- le couplage annuaire Active Directory ;
- les services de téléphonie d'urgence pour les sites d'hébergement étudiants ;
- les usages de bureau partagé (fonction desk sharing sur les postes fixes).

R7.2	*Remarque 7.2 : Le titulaire confirmera dans son offre la continuité de chacun de ces services fonctionnels et précisera les éventuelles limites ou prérequis associés.*

7.4 Profils utilisateurs et gestion des licences

Le titulaire maintiendra les profils utilisateurs en place tels que décrits dans l'état de parc UCaaS. Il devra être en capacité de faire évoluer le parc d'utilisateurs pendant la durée du marché, sans remise en cause de l'architecture globale. Les profils de référence sont :

- Profil A : licence utilisateur simple avec poste téléphonique IP, incluant la possibilité de click-to-call via l'application Rainbow Essential (gratuite) depuis un terminal mobile, l'appel étant établi via le poste physique ;
- Profil B : licence utilisateur simple avec softphone ;
- Profil C : licence utilisateur communication unifiée Rainbow Entreprise (profil multidevice, softphone autonome, messagerie vocale unifiée, mobilité) ;
- Profil D : licence utilisateur accueil opérateur (poste standard avec console de supervision) ;
- Profil E : licence utilisateur agent ACD ;
- Profils spécifiques : fax, SIP, DECT.

Le modèle de flexibilité des licences devra permettre un ajout unitaire ou par tranche (modulo 1, 5 ou 10) sans coût autre que l'abonnement mensuel correspondant au BPU. La capacité d'évolution de la solution s'étend de 400 à plus de 600 licences utilisateurs.

R7.3	*Remarque 7.3 : Le titulaire précisera dans son offre les modalités d'ajout ou de suppression de licences en cours de marché, les délais de mise en œuvre, et sa politique de flexibilité. Il précisera également sa capacité à proposer des licences temporaires pour les besoins ponctuels (période de rentrée universitaire, par exemple).*

7.5 Terminaux, accessoires et périphériques

Le titulaire permettra la commande à la demande de terminaux, accessoires, passerelles, matériels DECT et équipements analogiques compatibles avec la solution OXE en place. Le BPU couvrira a minima :

- les terminaux de type 1 (équivalent Alcatel 8008/8018), de type 2 (équivalent Alcatel 8028/8038) et de type 3 (équivalent Alcatel 8068/ALE 300) ;
- les postes DECT de type 1 et de type 2 ;
- les softphones ;
- les casques filaires et sans fil, les combinés sans fil, les conférenciers SIP ;
- les bornes IP-DECT ;
- les passerelles SIP/analogique.

R7.4	*Remarque 7.4 : Le titulaire proposera dans son offre un catalogue de terminaux et d'accessoires avec les prix publics catalogue et les taux de remise consentis dans le cadre du marché. Chaque terminal proposé intègre un cordon de raccordement RJ45 d'au moins 1,50 mètre.*

7.6 Usages nomades et travail hybride

Le titulaire assurera la continuité de service pour les usages nomades déjà en production : télétravail (hard phone ou softphone sur réseau public avec chiffrement natif), bureau partagé (log/délog sur poste non affecté), et fixe-mobile convergence (softphone sur smartphone via WiFi ou 4G).

R7.5	*Remarque 7.5 : Le titulaire précisera dans son offre les conditions de continuité de chaque usage nomade, les profils de licence associés et les éventuels prérequis réseau ou applicatifs.*

7.7 Carnet multiservice

Un carnet multiservice prépayé de 20 à 50 unités d'œuvre permettra de réaliser, à la demande, des opérations de change non comprises dans le forfait MCO. Ce carnet sera rechargeable par tranches de 20 ou 50 unités d'œuvre en cours d'exécution. À l'issue du marché, les unités d'œuvre non consommées seront converties en prestation au prorata du budget restant non utilisé.

R7.6	*Remarque 7.6 : Le titulaire précisera dans son offre les modalités d'utilisation du carnet multiservice, les opérations éligibles et les règles de décompte des unités d'œuvre.*

7.8 Formation, accompagnement et prestations complémentaires

Le titulaire proposera au BPU des prestations de formation, d'accompagnement et des services complémentaires valorisés en unités d'œuvre, selon les profils :

Formation et accompagnement :

- formations utilisateurs par profil (sessions de 1h30 sur site, de 8 à 14 personnes) ;
- formation administrateur/gestionnaire pour 2 personnes, couvrant la création d'utilisateurs, la gestion des entités, la gestion des règles d'accueil et l'exploitation des tableaux de bord ;
- notices simplifiées contextualisées par profil d'usage ;
- assistance post-déploiement sur site (demi-journée) lors de l'intégration d'un nouveau site ou d'une entité.

Production de guides vocaux :

- enregistrement studio de messages d'accueil, d'attente et de nuit (voix off professionnelle) ;
- intégration et déploiement des guides vocaux dans la solution OXE, par entité et plage horaire.

R7.7	*Remarque 7.7 : Le titulaire présentera dans son offre le catalogue des prestations proposées, les programmes de formation associés, les modalités de commande des guides vocaux (délais, formats livrables, nombre de prises en charge par unité d'œuvre) et leur valorisation au BPU.*

8. Exigences transverses de MCO

8.1 Horaires de service et astreinte

La plage nominale de couverture est du lundi au vendredi de 8h à 18h. En dehors de ces plages, une astreinte téléphonique devra être disponible pour les incidents de niveau Majeur/Bloquant. Une couverture élargie le samedi de 8h à 18h pourra être activée ponctuellement, notamment en période de rentrée universitaire, selon les modalités définies au BPU.

R8.1	*Remarque 8.1 : Le titulaire précisera dans son offre les modalités de prise en charge des incidents en dehors des heures ouvrées, les conditions d'activation de la couverture élargie le samedi et le coût associé au BPU.*

8.2 Gestion des incidents — niveaux de sévérité et GTR

Le titulaire définira une classification claire des incidents selon leur sévérité et s'engagera sur les délais de prise en charge et de rétablissement suivants :

Niveau	Rappel	Prise en charge	Délai rétablissement	Plage
Majeur / Bloquant	30 min	1h	4h (ligne ou site)	24h/24 7j/7
Mineur / Défaut — critique	1h	2h	8h ouvrées	Lun–Ven 8h–18h
Mineur — non critique	4h	8h	5 jours ouvrés	Lun–Ven 8h–18h

Tout incident de niveau Majeur/Bloquant déclenchera automatiquement une procédure d'escalade et une notification immédiate au **Crous Aix-Marseille Avignon**. L'intervention est considérée comme terminée lorsque le **Crous Aix-Marseille Avignon** a constaté que le service est rétabli et a validé la clôture de l'incident.

Deux incidents présentant le même symptôme dans le même mois, même résolus, déclenchent une démarche de gestion de problème (au sens ITIL) visant à identifier les causes profondes et à mettre en place une correction globale.

R8.2	*Remarque 8.2 : Le titulaire précisera dans son offre les modalités opérationnelles de maintien de ces engagements, les circuits d'escalade, les outils de suivi et les modèles de compte rendu d'intervention.*

8.3 Gestion de la sécurité et des failles

Le titulaire assurera une veille de sécurité permanente relative aux composants exploités (équipements Fortinet, solution OXE, outils de gestion) et informera sans délai le **Crous Aix-Marseille Avignon** de toute vulnérabilité critique identifiée. Les délais d'intervention suivants s'appliquent :

- 1 jour ouvré pour aviser le **Crous Aix-Marseille Avignon** d'une faille de type zéro-day dès sa connaissance et évaluer son impact sur l'architecture ;

- 1 jour ouvré pour la mise en place du patch correctif dès publication par l'éditeur (faille zéro-day) ;
- 3 jours ouvrés pour toute autre faille dès connaissance par l'éditeur ou un organisme d'État (CERT-FR, ANSSI).

R8.3	*Remarque 8.3 : Le titulaire précisera dans son offre l'organisation mise en place pour la veille et la gestion des failles, et fournira un exemple de communication utilisée pour les vulnérabilités de type zéro-day.*

8.4 Sauvegardes et restauration

Le titulaire précisera les modalités de sauvegarde des configurations (boîtiers FortiGate, FortiManager, solution OXE), les fréquences de sauvegarde, les procédures de restauration, les responsabilités respectives entre le titulaire et le **Crous Aix-Marseille Avignon**, et les délais de restauration garantis en cas d'incident.

Les processus de sauvegarde et de restauration seront présentés à l'équipe d'exploitation du **Crous Aix-Marseille Avignon** lors de la réunion de lancement, puis documentés dans le DOE.

R8.4	*Remarque 8.4 : Le titulaire précisera dans son offre les politiques de sauvegarde applicables à chaque composant du périmètre, les fréquences, les durées de rétention et les délais de restauration garantis.*

8.5 Maintenance préventive annuelle

Dans le cadre de la maintenance préventive, les actions suivantes devront être réalisées au minimum annuellement :

- analyse des logs et des traces d'événements ;
- analyse des alertes systèmes ;
- vérification des mécanismes de secours électrique et fonctionnel ;
- mesures de performance et de dimensionnement ;
- mesures de charges réseaux ;
- validation des bases documentaires et des sauvegardes ;
- présentation du plan produit des éditeurs et fabricants concernés.

R8.5	*Remarque 8.5 : Le titulaire présentera dans son offre les modalités, le périmètre et les livrables associés aux actions de maintenance préventive annuelle.*

8.6 Certifications et compétences requises

Le titulaire devra disposer des plus hauts niveaux de certification obtenus auprès des éditeurs et constructeurs concernés. Ces certifications devront notamment couvrir :

- Fortinet : certifications NSE de niveau avancé (NSE 7 minimum) pour les équipements FortiGate, FortiManager et FortiAnalyzer ;
- Alcatel-Lucent Enterprise : certifications de niveau avancé sur OmniPCX Enterprise et l'écosystème UCaaS.

Les certifications devront être valables pour toute la durée d'exécution du marché.

R8.6	*Remarque 8.6 : Le titulaire fournira dans son offre les certifications détenues par les personnes amenées à intervenir dans le cadre du marché (noms, niveaux, dates de validité).*

9. Bordereau des prix unitaires

Le BPU constituera un document contractuel majeur du marché. Il devra permettre de couvrir de manière lisible l'ensemble des prestations récurrentes et unitaires susceptibles d'être commandées pendant la durée d'exécution. Le BPU devra distinguer clairement :

- les frais de mise en service (FAS) ;
- les coûts récurrents mensuels (abonnements, liens, licences) ;
- les coûts unitaires ponctuels (prestations, équipements, déplacements) ;
- les taux de remise appliqués par famille de produits ;
- les éventuelles conditions d'engagement et règles de facturation en cas de création, de modification, de suppression ou de résiliation de service.

Le BPU devra notamment couvrir les rubriques suivantes :

- Accès WAN : FTTH, FTTO, SDSL, ADSL/VDSL, 4G/5G — par débit et par option de GTR ;
- SD-WAN : licences FortiGuard (renouvellement annuel par type d'équipement), licences FortiCare VMs FMG/FAZ, équipements Fortinet à la demande (par famille avec taux de remise catalogue), prestations de configuration et d'intégration ;
- Ajout de site : prestation complète par profil de site (simple, sensible) ;
- UCaaS : abonnements mensuels par profil utilisateur (A, B, C, D, E, spécifiques), numéros SDA, options (ACD, SVI, messagerie) ;
- Terminaux et accessoires UCaaS : par modèle, avec prix catalogue et taux de remise ;
- Services et formations : unités d'œuvre (UO Projet, UO Technicien, UO Formation, UO Câbleur, carnet multiservice) ;
- Couverture élargie samedi : forfait mensuel ou ponctuel.

R9.1	*Remarque 9.1 : Le titulaire précisera dans son offre les règles de facturation au prorata en cas de résiliation en cours de mois, les conditions de portabilité de numéros, et les délais de facturation pour chaque type de prestation.*

10. Mise en œuvre et réversibilité

À la notification du marché, une réunion de lancement sera organisée afin de valider le périmètre initial, les interlocuteurs, les outils, les modalités d'accès (notamment l'accès VPN aux VMs FMG/FAZ), les procédures d'escalade, les documents de référence, les circuits de validation et les premières actions de prise en charge.

À cette occasion seront également présentés par le titulaire : les processus de sauvegarde et de restauration, les modalités d'administration à distance des composants centraux, et le planning d'établissement de la base documentaire initiale.

En fin de marché, le titulaire assurera, sans rupture de service, les opérations nécessaires à la réversibilité, notamment la restitution de la documentation, des historiques, des sauvegardes, des éléments de paramétrage et des informations utiles à la poursuite de l'exploitation. Un bilan de réversibilité sera remis sous deux semaines à l'issue de la période de transfert.

11. Annexes techniques attendues

Les annexes du marché comprendront notamment :

- l'inventaire détaillé des sites couverts à la notification, avec le type d'accès et le profil de site ;
- l'inventaire du parc d'équipements Fortinet (modèles, numéros de série, versions FortiOS, licences FortiGuard en place et dates d'expiration) ;
- la description des VMs FortiManager et FortiAnalyzer (versions, ressources allouées) et les modalités d'accès VPN mis à disposition du titulaire ;
- l'état de parc UCaaS détaillé (licences, profils, terminaux, bornes DECT, SDA) ;
- le bordereau des prix unitaires ;
- les niveaux de service et les grilles de pénalités associées ;
- les modèles de comptes rendus, tableaux de bord et ordres du jour des comités de suivi.

12. Éléments attendus dans le mémoire technique du candidat

Le candidat présentera dans son mémoire technique a minima les éléments suivants :

- son organisation de support et d'exploitation (équipe projet, équipe support, interlocuteurs, niveaux d'escalade) ;
- sa méthodologie de prise en charge du périmètre à la notification et les premières actions dans les 30 jours ;
- ses engagements de service détaillés (GTR, disponibilité, sécurité) ;
- les modalités d'administration à distance des VMs FortiManager et FortiAnalyzer via le VPN encadré fourni par le **Crous Aix-Marseille Avignon** ;
- sa capacité à maintenir l'architecture Fortinet existante et à intégrer des équipements de gammes futures selon le principe de continuité de gamme ;
- sa capacité à maintenir la solution OXE hébergée et l'ensemble des services UCaaS en place ;
- les certifications détenues sur les technologies Fortinet et Alcatel-Lucent Enterprise ;
- les taux de remise proposés par famille de produits, logiciels, services et catalogues constructeurs ;
- les modalités de sécurité, de traçabilité des accès distants et de réversibilité en fin de marché ;
- la roadmap des éditeurs et constructeurs pour les composants du périmètre.

— Fin du CCTP —