

**CCTP 2025-016**

*DELIVRANCE DE SERVICES INTERNET LOISIRS AU PROFIT DU PERSONNEL DES FORCES ARMEES EN NOUVELLE CALEDONIE (FANC)*



**MINISTÈRE DES ARMEES**

**DIRECTION DU COMMISSARIAT D'OUTRE-MER**

**GROUPEMENT DE SOUTIEN COMMISSARIAT NOUVELLE-CALEDONIE**

**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)**

**Marché N° 2025-016**

**DELIVRANCE DE SERVICES INTERNET LOISIRS AU PROFIT DU PERSONNEL DES FORCES ARMEES EN  
NOUVELLE CALEDONIE (FANC)**

## SOMMAIRE

<b>ARTICLE 1. OBJET DU MARCHÉ .....</b>	<b>4</b>
1.1 Objet du marché.....	4
1.2 Définition des prestations .....	5
1.3 Acronymes et Terminologie.....	6
1.3.1 Acronymes .....	6
1.3.2 Terminologie .....	7
<b>ARTICLE 2. GENERALITES.....</b>	<b>7</b>
2.1 Prévention .....	7
2.2 Ressources .....	7
<b>ARTICLE 3. CARACTERISTIQUES DU MATERIEL DEPLOYE .....</b>	<b>7</b>
3.1 Qualité et origine du matériel .....	7
3.2 Contraintes environnementales .....	8
3.3 Architecture générale du réseau .....	8
<b>ARTICLE 4. CARACTERISTIQUE DE LA CONNEXION DEPLOYEE .....</b>	<b>9</b>
4.1 Objectifs de la connexion.....	9
4.2 Caractéristique générale.....	9
4.2.1 Compte utilisateur .....	9
4.2.2 Connexion et déconnexion .....	10
4.2.3 Profil utilisateur .....	10
4.2.4 Portail web utilisateur .....	10
4.2.5 Lutte contre la cyber-délinquance et journalisation .....	11
4.2.6 Dispositif de la « bulle silence ».....	11
4.3 Caractéristique technique de la connexion WIFI .....	11
4.3.1 Exigence spécifique au réseau WIFI .....	11
4.3.2 Débit minimum garanti par utilisateur .....	12
4.3.3 Exigence de sécurité des échanges .....	13
4.3.4 Le SSID .....	13
<b>ARTICLE 5. INSTALLATION DU MATERIEL .....</b>	<b>14</b>
5.1 Spécification relatives aux infrastructures physiques.....	14
5.2 Normalisation.....	15
5.3 Délai d'installation du matériel .....	15
5.4 Suivi du déploiement sur l'ensemble des sites : .....	15
5.5 Réception des travaux.....	16
5.6 Engagement du titulaire .....	16

<b>ARTICLE 6.</b>	<b>SOUTIEN LOGISTIQUE ET MAINTIEN EN CONDITION OPERATIONNELLE</b>	
<b>(MCO)</b>	<b>17</b>	
6.1	Généralités.....	17
6.2	Assistance.....	17
6.3	Garantie de temps de rétablissement (GTR).....	17
6.4	Maintenance préventive et curative.....	18

## ARTICLE 1. OBJET DU MARCHÉ

### 1.1 Objet du marché

Le présent marché a pour objet la mise en œuvre et la délivrance de services de télécommunications (internet) de loisir au profit du personnel des forces armées en Nouvelle Calédonie (FANC).

Prestations principales demandées :

- la fourniture, l'installation, le paramétrage et le déploiement des infrastructures et matériels sur l'ensemble des bâtiments décrits ci-après et conformément aux spécificités techniques prévues au marché,
- la mise à disposition de services Internet de loisir pour le personnel des FANC dans les différents bâtiments,
- la mise à disposition d'outils d'authentification d'accès aux services (portail web),
- La fourniture de prestation d'exploitation, de maintenance des infrastructures de réseaux et des services associés installés dans les différents sites prévus au marché,
- La fourniture de prestations d'aide au pilotage, la mise à disposition d'outils de pilotage et de *reporting* en ligne comme des indicateurs de performance, des tableaux de bord, des suivis des incidents, des suivis des engagements de qualité de service, des facturations ou des inscriptions (liste non exhaustive),
- La fourniture d'un service client et soutien logistique au profit des utilisateurs et des gestionnaires tel que défini à l'article 6 du présent CCTP,
- Le démontage, démantèlement, dépollution et remise en conformité des bâtiments en cas de fin de marché,
- La dépose et repose des équipements passifs et actifs en cas de réhabilitation de bâtiment.

En cas de fourniture d'un service complémentaire payant tel que défini à l'article 4.1 du présent CCTP, celle-ci doit prendre en charge les paiements par Carte Bancaire (CB) ou tout autre moyen de paiement sécurisé (VISA, AMEX, *Paypal*, etc...)

## 1.2 Définition des prestations

Le présent marché est défini comme il suit :

**POSTE A-** La fourniture, l'installation, le paramétrage et le déploiement des infrastructures et matériels sur les bâtiments des FANC qui se trouvent principalement sur les emprises suivantes :

- **Nouméa**
  - Quartier Bataillon Mixte du Pacifique
  - Base Navale de Chaleix
  - Station de Ouen Toro
  - Pointe de l'Artillerie
  - Quartier de l'Artillerie
  - Caserne Gally-Passebosc
- **Plum**
  - Quartier Broche (RIMAP NC)
  - Résidence HIBISCUS
- **BA186 La Tontouta**
  - Quartier Lieutenant Paul Klein
- **Nandaï**
  - Quartier Lieutenant Paul Klein

Pour des raisons de renouvellement d'infrastructure, cette liste est susceptible d'évoluer pendant la durée d'exécution du marché.

Les prestations feront l'objet d'une demande de devis sur la base des éléments de base d'ordre technique définis en annexe 1 de l'acte d'engagement.

**POSTE B-** La mise à disposition de services Internet de loisir pour le personnel des FANC dans les différents bâtiments déjà équipés.

<b>Emprises militaires Nouméa</b>	<b>Bâtiments</b>	<b>Effectif sur site (estimatif)</b>
Quartier Bataillon Mixte du Pacifique Rue Louis Flize Pointe de l'Artillerie NOUMEA	13 (espace de convivialité) – 15 – 19 – 30 – 31 – 32 – 33 – 41 Bâtiment DIASS	Environ 200 personnes
Base navale Chaleix Rue du Capitaine Desmier NOUMEA	14 (espace de convivialité) – 17 – 18 – 19 – 20 – 61 – 68 (espace convivialité)	Environ 125 personnes
Station du OUN TORO	04	Environ 20 personnes
<b>Emprise militaire PLUM</b>	<b>Bâtiments</b>	<b>Effectif sur site (estimatif)</b>
Quartier Broche (Rimap NC) RP1 PLUM	097 (espace de convivialité) – 002 – 003 – 004 – 059 – 084 – 088 – 089 – 090 – 166 -167 – 168 – 169 – 170 – centre de restauration unique - Bar	Environ 550 personnes.

<b>Emprise militaire NANDAI</b>	<b>Bâtiments</b>	<b>Effectif sur site (estimatif)</b>
Camp de Nandaï RT1 NANDAÏ	051 (espace de convivialité) – 002 – 003 – 005 – 017– 022 – 027 – 029 Bâtiment infirmerie (pièces 08-09-10-11-14-15-18)	Environ 160 personnes.
<b>Emprise militaire BA186 LA TONTOUTA</b>	<b>Bâtiments</b>	<b>Effectif sur site (estimatif)</b>
Quartier Lieutenant Paul Klein (BA 186) LA TONTOUTA	Zone hébergement et restauration limité au périmètre représenté par les bâtiments 003 / 004 / 005 / 023 / 024 / 025 / Faré loisir	Environ 120 personnes

**Pour des raisons de renouvellement d'infrastructure, cette liste est susceptible d'évoluer.**

## **1.3 Acronymes et Terminologie**

### **1.3.1 Acronymes**

<b>ACRONYME</b>	<b>Développement de l'acronyme</b>
CCAP	Cahier des Clauses Administratives Particulières
CCTP	Cahier des Clauses Techniques Particulières
GTR	Garantie du Temps de Rétablissement
HTTPS	HyperText Transfer Protocole Secure
IP	Internet Protocol
LAN	Local Area Network
OSPF	Open Shortest Path First
POC	Point de Contact (coordinateur local sur chaque emprises)
POE	Power Over Ethernet
QOS	Quality of Service (Qualité de Service)
RGPD	Règlement Général sur la Protection des Données
RIP	Routing Information Protocol
SLA	Services Level Agreement
SMS	Short Message Service (service d'envoi de messages courts entre mobiles)
SNMP	Simple Network Management Protocol
VoIP	Voice Over IP
SSID	Service Set Identifier

### 1.3.2 Terminologie

Les termes employés dans le présent document sont définis comme suit :

- **Site** : un site est une emprise militaire ou non. Les sites peuvent être de tailles variables et peuvent accueillir un nombre variable d'utilisateurs sur différentes zones.

Un site comprend un ou plusieurs ouvrages bâtis éligibles au service de wifi s'ils se rattachent aux destinations suivantes :

- **Lieux d'hébergement** : hébergement troupe, hébergement cadre, hébergement troupes de passage, chambres d'hôtellerie;
- **Zones de convivialité** : foyers, bars, espaces de détente,
- **Zones d'attente et d'information (Périmètre des directions des ressources humaines des armées)**. Une zone d'attente peut être située en emprise ou hors emprise militaire et comprend également les espaces Atlas (\*).
- **Utilisateurs finaux** : tout personnel, civil ou militaire, éligible au service, présent sur site.
- **Bénéficiaire** : Entité publique ou privée (pour les prestations payantes hors périmètre du présent marché) souscrivant, auprès du titulaire, aux prestations de wifi résultant du présent marché,
- **Point de Contact** : Gestionnaire identifié par l'entité bénéficiaire pour chaque site en charge de la remontée d'incidents ainsi que la communication vers le titulaire et les utilisateurs.

(\*) Les zones ATLAS sont des espaces physiques concentrant un nombre varié de moyens d'information et de services (courrier, conciergerie, réservation de chambre, etc.) adaptés aux besoins et capacités du site au profit des militaires.

## ARTICLE 2. GENERALITES

### 2.1 Prévention

Un plan de prévention sera établi en liaison avec les chargés de prévention désignés par l'Administration. Il sera obligatoirement signé le jour de l'ouverture des chantiers.

### 2.2 Ressources

Le titulaire doit disposer des moyens humains et matériels adaptés à l'exécution des travaux à réaliser. Il supporte les conséquences résultant de moyens insuffisants, inutilisables ou inappropriés. L'Administration ne fournira ni l'outillage, ni les appareils de mesures nécessaires à la réalisation des travaux.

Le titulaire doit acquérir et entretenir parmi son personnel la compétence suffisante pour la réalisation des travaux et l'exploitation du réseau. Il doit également employer du personnel qualifié pour créer les plans des installations réalisées et les mettre à jour par tous moyens.

## ARTICLE 3. CARACTERISTIQUES DU MATERIEL DEPLOYE

### 3.1 Qualité et origine du matériel

Les fournitures préconisées par le titulaire/fournisseur respectent impérativement les normes en vigueur particulièrement dans le domaine des télécommunications et des installations électriques.

Tous les éléments de l'installation doivent être neufs, en parfait état de fonctionnement et conformes aux normes en vigueur et au présent descriptif.

Les composants des installations doivent disposer d'un label (ou équivalent) ou d'un certificat de qualité délivré par un organisme officiel chaque fois qu'il est possible. En cas d'équivalence, le titulaire en apporte la preuve par tous moyens.

Les matériels doivent être garantis par leur constructeur pour l'utilisation envisagée.

Le titulaire doit permettre la mise en œuvre d'une architecture réseau Ethernet suffisamment robuste pour a minima connecter les équipements informatiques (ordinateur, tablette, smartphone, etc.) des utilisateurs au réseau Internet. L'infrastructure réseau Ethernet doit être basée sur des infrastructures câbles et/ou sans fil reposant sur la technologie Wi-Fi.

### 3.2 Contraintes environnementales

Les marques et modèles de matériels fournis au titre du présent marché doivent présenter des caractéristiques conformes aux normes édictées par la Commission Européenne en la matière de limitation des substances dangereuses dans la conception des appareils électroniques (*directive 2011/65/UE du 8 juin 2011 et décret n°2013-988 du 6 novembre 2013*), respect dans les processus de fabrication, emballage et livraison d'un éco label (ou équivalent) qui engage le fabricant au-delà du strict respect de cette directive.

Le titulaire s'engage sur le respect de la collecte et du recyclage des déchets électroniques (conformément à la *directive 2012/19/UE du 4 juillet 2012 et du décret 2014-928 du 19 août 2014*).

En fin de marché si celui-ci n'est pas reconduit, lors d'un changement de prestataire, lors de la fermeture d'un site ou d'un bâtiment ou lorsque dans le cadre de l'exécution du marché il est nécessaire de changer tout ou partie du matériel mis en place, le titulaire doit assurer les prestations de démontage, de dépollution, de collecte, de transport, de destruction et/ou de recyclage des infrastructures actives déployées lui appartenant sur ledit site ou bâtiment et éventuellement des infrastructures physiques.

Cette dépollution sera demandée par ordre de service et devra intervenir dans les 3 mois suivants la fin du marché.

En cas de non-respect de cette obligation des pénalités pourront être établies conformément à l'article 8 du CCAP.

### 3.3 Architecture générale du réseau

De manière générale, l'architecture réseau du titulaire doit permettre de véhiculer sur l'Internet l'ensemble des flux voix, vidéo et données en appliquant une qualité de service et un niveau de sécurité adaptés, tous matériels et logiciels nécessaires à la délivrance des services et notamment :

- Infrastructures passives :
  - câbles en catégorie 6 minimum pour le raccordement des bornes et des différentes infrastructures actives ;
  - coffrets réseau sécurisés permettant la mise en rack des différentes infrastructures actives ;
- Infrastructures actives :
  - point d'accès sans fil PoE (et antennes) en nombre suffisant pour assurer la couverture totale des étages et bâtiments composant les formations (sites) ;
  - équipements devant être hors d'atteinte physique des utilisateurs ;
  - commutateurs réseaux disposant de l'auto-alimentation des ports IEEE 802.3af (Power Over Ethernet) ;
  - équipement intégré assurant les fonctionnalités de filtrage, de priorisation de flux et d'équité entre les utilisateurs ainsi que l'équilibrage de charge ;
  - matériels synchronisables à une source de temps ;
- Câblage et prises :
  - prises étiquetées ;
  - passage des câbles à l'extérieur et intérieur selon des directives du responsable de la sécurité informatique militaire local, la mise en place des poteaux, les raccordements d'énergie (tableaux électrique et prises) ;
  - fourniture et pose des câbles réseaux (cuivre, optique, etc.), prises informatiques, etc. avec étiquetage et repérage et les chemins de câbles associés ;



- fourniture et le montage de coffrets et baies.

Les infrastructures réseau Ethernet du titulaire sur les sites doivent être basées sur des infrastructures câbles et/ou sans fil reposant sur la technologie Wi-Fi pour la distribution, satisfaisant en particulier la norme 802.11ac, pour répondre aux besoins de transport des données informatiques, de la voix et de la vidéo en appliquant une qualité de service et un niveau de sécurité adaptés.

Le titulaire prend à sa charge l'installation des infrastructures réseaux sur l'intégralité du site à desservir notamment :

- commutateurs réseaux disposant de l'auto-alimentation des ports IEEE 802.3af, voire 802.3at,
- points d'accès sans fil (et antennes) en nombre suffisant pour assurer la couverture totale des étages et bâtiments composant les sites,
- équipements intégrés assurant les fonctionnalités de filtrage, de priorisation de flux, de marquage des flux et d'équité entre les utilisateurs ainsi que l'équilibrage de charge,
- matériels qui peuvent être synchronisés à une source de temps.

Les équipements actifs du titulaire ne peuvent pas être installés à moins de deux mètres d'un équipement actif du réseau Défense. Seuls les équipements actifs de réseau sont présents sur les sites à l'exception des serveurs d'accès au réseau.

## **ARTICLE 4. CARACTERISTIQUE DE LA CONNEXION DEPLOYEE**

### **4.1 Objectifs de la connexion**

Le service délivré par le titulaire doit permettre aux utilisateurs :

- d'accéder aux services de l'Internet via des terminaux personnels (ordinateurs, smartphone, tablette mobile, etc.) ;
- de permettre pour un utilisateur de se connecter à au moins trois équipements simultanément.

L'offre devra également être déclinée comme il suit :

- Offre principale : permettant à chaque utilisateur final de disposer gratuitement d'un accès internet à hauteur de deux (2) Gbits par jour.
- Offre complémentaire : faculté laissée à chaque utilisateur final de souscrire, moyennant finance, à une offre complémentaire préférentielle d'accès internet d'a minima 30 Gbits par jour.

La connexion WIFI proposée dans le présent marché doit être délivrée par une installation fibre ou cuivre (technologie qui répond le mieux aux exigences de résultat définies).

Le titulaire a la possibilité de proposer des services additionnels (*VoD, Streaming TV, VoIP, etc.*), non inclus dans les prix proposés, faisant l'objet d'une tarification distincte.

### **4.2 Caractéristique générale**

#### **4.2.1 Compte utilisateur**

Le titulaire a en charge le mécanisme de gestion des comptes de manière dématérialisée via son portail Web (achat, report de soldes, incidents de fonctionnement, remboursements, litiges, etc.).

La création du compte doit être confirmée conformément à la législation en vigueur (réception d'un SMS et/ou d'un mail sur un numéro de téléphone ou local ou étranger).

Le titulaire peut soumettre une solution alternative mais qui ne doit en aucun cas remplacer la solution de validation par réception d'un code de vérification via SMS et/ou mail.

Pour les zones d'attente, il sera demandé simplement une authentification par mail sans demander à l'utilisateur des informations personnelles à part son mail.

La procédure d'identification/authentification de l'utilisateur doit être sécurisée en HTTPS du fait que des informations personnelles sensibles sont échangées via Internet.

L'authentification sur le portail web du titulaire doit être opérée à minima par couple (login/password). La politique de gestion des mots de passe à respecter :

- longueur minimum prédéfinie (supérieur à 8 caractères : N = 8),
- impossibilité de réutiliser les n derniers mots de passe (N = 5),
- nombre de tentatives possibles (N = 3).

Le portail web doit bien évidemment permettre la modification, la suppression, la mise en veille (verrouillage des comptes non utilisés), etc. de comptes utilisateurs par l'administration.

Le titulaire doit se conformer aux exigences du *Règlement Général de sur Protection des données* (RGPD).

#### **4.2.2 Connexion et déconnexion**

Lors de la première connexion, l'utilisateur doit être redirigé vers le site extranet du titulaire afin de valider les droits et devoirs de l'utilisateur, chartre d'utilisation, conditions générales de vente, etc.

Les mécanismes mis en œuvre doivent sécuriser la déconnexion effective de l'utilisateur même en cas de non-respect de la procédure adéquate (exemple mécanisme d'arrêt automatique ou déconnexion à la fermeture du navigateur).

#### **4.2.3 Profil utilisateur**

A minima, deux types de profils doivent être configurables sur le portail web du titulaire :

- Gestionnaire (POC), à disposition de l'administration :
  - Vision totale des consommations et des performances sur l'ensemble des sites.
  - Permet de mettre en œuvre la « bulle silence » mentionnée au point 4.2.6 du CCTP.
- Utilisateurs :
  - Vision limitée à sa consommation et à la performance de la connexion.

Les profils utilisateurs auront accès au portail web utilisateur.

#### **4.2.4 Portail web utilisateur**

Le titulaire doit mettre à la disposition des utilisateurs un portail web (intranet), accessible gratuitement à partir des principaux navigateurs (Internet Explorer, Firefox, Chrome, etc.) et permettant :

- L'accès aux droits et devoirs de l'utilisateur, chartre d'utilisation, conditions générales d'utilisation, politique d'utilisation des données personnelles etc.,
- L'authentification via login/mot de passe,
- La gestion du compte et des consommations,
- L'émission et le suivi, par les utilisateurs, de tickets d'incident,
- L'accès au service de support client et de FAQ,
- La connexion se fait par la saisie des seules informations requises par le respect de la législation en vigueur (création de compte et/ou identifiants).

Le portail web du titulaire doit être au minimum bilingue (français/anglais).

Les données personnelles stockées au titre du portail devront être en conformité avec le RGPD et être stockées sur le territoire national ou, à défaut, au sein de l'espace Schengen frontalier au territoire français.

Dans le cas du SSID – zone de convivialité, dès que l'utilisateur est connecté sur le réseau (SSID) le portail web doit s'ouvrir par défaut (fonction de portail captif).

Lors de leur première connexion, le portail web du titulaire doit rappeler de manière non équivoque les droits et devoirs de l'utilisateur et l'informer sur les mesures de cyber surveillance mises en œuvre ainsi que ses droits d'accès aux informations le concernant.

Les utilisateurs doivent être amenés, par l'interface proposée, à prendre connaissance et valider les conditions générales et d'utilisation des services d'accès Internet et de Téléphonie.

#### 4.2.5 Lutte contre la cyber-délinquance et journalisation

Le respect de la législation concernant la conservation des données nécessite que le système garde en mémoire les éléments permettant de satisfaire les exigences des textes législatifs et réglementaires en vigueur et notamment :

- loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne ;
- loi n°2033-239 du 18 mars 2003 pour la sécurité intérieure ;
- loi n°2004-575 du 21 juin 2004 sur la confiance dans l'économie numérique ;
- loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme ;
- décret n°2006-358 du 24 mars 2006 relatif à la conservation des données de communication électronique.

**Journalisation** : Les mécanismes mis en œuvre doivent permettre d'établir la traçabilité des actions (qui a accédé à tel site ? à quelle date ? depuis quelle station ?) au profit des autorités judiciaires compétentes tout en interdisant cette corrélation par le personnel d'administration.

La mise en œuvre du protocole SNMP doit l'être au minimum dans sa version 3.

La journalisation est centralisée et réalisée à la charge du titulaire pour l'ensemble des équipements actifs et des serveurs. Les connexions sont également journalisées.

Les journaux doivent être conservés un an par le titulaire, conformément à la législation.

Par défaut, le filtrage des services Internet ne sera pas activé.

#### 4.2.6 Dispositif de la « bulle silence »

L'administration peut demander à tout moment au titulaire de suspendre tous les services de télécommunications pendant une période définie ou non définie sur un ou plusieurs sites donnés. Elle a pour but de ne pas permettre la fuite d'informations pendant cette période de coupure des communications.

La bulle de silence doit pouvoir être mise en œuvre en 24/7 de manière instantanée.

Cette fonctionnalité doit pouvoir être contrôlée par le profil gestionnaire.

Cette dernière n'impacte pas la facturation.

Les utilisateurs sont informés de l'activation de la bulle de silence par le biais d'un message immédiat diffusé sur le portail web sous forme de bandeau.

##### Moyens de déclenchement de la bulle de silence :

4 cas de figure peuvent se présenter :

- Cas N°1 - Activation de la bulle silence par le pilote opérationnel (Bénéficiaire).
- Cas N°2 - Activation de la bulle silence par le prestataire (Titulaire).

#### 4.3 Caractéristique technique de la connexion WIFI

##### 4.3.1 Exigence spécifique au réseau WIFI

L'architecture réseau Ethernet proposée par le titulaire doit disposer au minimum des fonctionnalités suivantes :

- native 802.11a/b/g/n/ac avec prise en charge de plusieurs SSID (au minimum 3),
- support du protocole IPv4 (évolutive vers IPv6 par simple évolution du firmware),
- support des fonctions de routage IP (protocoles RIP, OSPF, etc.), de segmentation (VLAN) et des protocoles de redondance de niveau 2 et 3 (VRRP, HSRP, etc.),
- gestion de la Qualité de service (QoS) avec gestion de la bande passante au niveau du trafic IP et des services,
- support des principaux protocoles d'authentification (Radius, 802.1X, filtrage MAC/IP, etc.) et de chiffrement (WEP, WPA, WPA2, etc.).

Les parties d'authentification, d'hébergement des pages web, d'informations relatives aux logs et aux incidents doivent être hébergées à distance, sous la responsabilité du titulaire et doivent être sécurisées (piratage, redondance ...).

La connexion aux services Internet du titulaire doit être la plus simple et automatisée possible pour l'utilisateur, dans le respect des exigences de sécurité et de traçabilité.

Le titulaire doit se conformer aux directives ci-dessous : la conformité au rapport technique relatif aux recommandations pour la mise en œuvre de réseaux Wi-Fi (n°2011/116576/DGA MI/SSI/IPS/AI/17S870162/NC du 16 avril 2011) nécessitant d'être en conformité avec les actions suivantes :

- interdire le Wi-Fi non sécurisé (émission omnidirectionnelle, utilisation de clés de chiffrement partagées à très longue période de vie quel qu'en soit le type, WEP, WPA, identification faible, authentification inexistante, services Internet sans chiffrement, ...). La mise en place de solution Wi-Fi et son accès sécurisé sont étudiés et précisés dans le présent marché ;
- assurer le cloisonnement entre les flux lorsque plusieurs applications correspondant à des besoins distincts sont mises en œuvre sur un réseau Wi-Fi ;
- ne pas permettre aux terminaux utilisateurs de communiquer entre eux en local ;
- opter pour le mode « infrastructure » (pas de mode ad hoc) ;
- assurer une cohérence dans l'utilisation des canaux et des bandes de fréquences utilisés localement ;
- utiliser l'authentification et les flux du type WPA2 ;
- renforcer la sécurisation des points d'accès, en particulier les accès permettant la supervision (interdire la supervision à partir de l'interface Wi-Fi) et l'administration des points d'accès ;
- privilégier une solution permettant la centralisation des configurations et des politiques de sécurité des points d'accès afin de s'assurer de leur homogénéité ;
- désactiver les modes IEEE 802.11 non utilisés ;
- définir un identifiant de réseau (SSID) personnalisé (nom du service communiqué par l'administration) ;
- réaliser et maintenir un dossier d'ouvrage exécuté en relation avec la gestion du site.

Pour le contrôle d'accès au réseau sans-fil Wi-Fi, l'infrastructure du titulaire doit supporter la norme **802.1x** couplée au protocole de type **EAP** (*Extensible Authentication Protocol*) et **PEAP** (*Protected Extensible Authentication Protocol*) pour le transport des informations d'identification en mode client/serveur vers la plateforme de contrôle d'accès. La solution doit supporter, à minima, les mécanismes d'identification EAP suivant :

- EAP-TLS ;
- EAP-TTLS ;
- PEAP de type PEAPv0/EAP-MS-CHAPv2.

D'autre part, la solution proposée doit fournir des mécanismes de détection de bornes dites « pirates » par le réseau radio afin de permettre à l'administrateur réseau de désassocier tout utilisateur qui tenterait de s'attacher au rogue AP.

#### **4.3.2 Débit minimum garanti par utilisateur**

Le titulaire propose, un débit conforme aux exigences contractuelles. Ce débit garanti figure dans son offre et fera l'objet d'une pondération de la note attribuée conformément au RC.

Par ailleurs, la solution du titulaire doit permettre de contrôler l'utilisation du débit de l'accès Internet suivant les règles suivantes :

- Répartition équitable du débit entre les utilisateurs actifs à un instant t,
- Classification et priorisation des flux et applications pour maîtriser la qualité du service « ressenti » suivant les types de flux (flux temps réel voix et vidéo, navigation internet et mail priorités sur les téléchargements).

Des pénalités pourront, le cas échéant, être appliquées conformément à l'article 8 du CCAP.

### **4.3.3 Exigence de sécurité des échanges**

Le titulaire doit respecter les conditions suivantes :

- contrôler, protéger et tracer l'accès physique aux éléments actifs du réseau ;
- utiliser du HTTPS dès que des informations personnelles sensibles sont susceptibles d'être échangées via une interface web ;
- être en conformité vis-à-vis de la CNIL et des prescriptions de l'ANSSI.

### **4.3.4 Le SSID**

Le titulaire doit configurer plusieurs SSID sur son réseau Wi-Fi pour la connexion aux services du titulaire, avec a minima :

- SSID « à définir » :
  - Ce SSID est destiné aux connexions des équipements informatiques des utilisateurs au réseau local.
  - Ce SSID doit être sécurisé par un mot de passe ADMIN accessible par l'administration ;
  - L'accès aux services Internet doit être le plus simple et le plus automatisé possible pour l'utilisateur, dans le respect des exigences de sécurité et de traçabilité.
- SSID zone de convivialité :
  - Ce SSID est destiné aux connexions des équipements informatiques en libre accès au réseau local.
  - Ce SSID pourra être sécurisé par un mot de passe partagé.
  - Les demandes d'accès aux services Internet doivent être redirigées automatiquement vers le portail web du titulaire dans un rôle de portail captif avec demande de login/mot de passe.
- SSID admin local – Gestionnaire :
  - Ce SSID est destiné aux connexions des équipements informatiques du gestionnaire au réseau local.
  - Ce SSID doit être sécurisé par un mot de passe partagé.
  - L'accès aux services proposés au gestionnaire de site doit être le plus simple et le plus automatisé possible pour le gestionnaire de site, dans le respect des exigences de sécurité et de traçabilité.

Les utilisateurs disposant d'un compte utilisateur valide doivent pouvoir se connecter aux services internet au travers du SSID « à définir ». L'utilisateur doit pouvoir ainsi se reconnecter de façon automatique (après une mise en veille de leur appareil par exemple) sans que cela nécessite une nouvelle authentification.

L'utilisateur doit pouvoir se connecter aux services depuis son compte utilisateur au travers de plusieurs équipements informatiques (ordinateur portable, smartphones, tablettes, etc.), avec un maximum de 3 terminaux distincts.

Par ailleurs, le compte utilisateur doit être reconnu sur l'ensemble des sites. A ce titre, il pourra se connecter simplement aux services Internet sur les autres sites.

## ARTICLE 5. INSTALLATION DU MATERIEL

### 5.1 Spécification relatives aux infrastructures physiques

Le titulaire fournit et met en place l'ensemble des installations utiles, permettant de répondre aux exigences de connectivité précitées, se trouvant entre la borne de raccordement extérieure à l'emprise militaire et le système déployé permettant de garantir l'accès à internet (borne WIFI). Cela comprend notamment :

- l'ensemble des câbles réseaux (de catégorie 6a au minimum) et fibre optique déployés afin de relier les boîtiers internet ;
- les fourreaux, poteaux, mâts et autre support au déploiement des installations ;
- la fourniture et montage de baies et coffrets muraux 19" sécurisés permettant la mise en clayette des différentes infrastructures ;
- la fourniture, le montage et le repérage de platines d'arrivées et de départs de fibres optiques et de panneaux passes-fils ;
- le montage de tous les équipements fournis (actifs et passifs), dans les baies et coffrets 19" des locaux techniques. Tous les équipements doivent être montés dans les baies ;
- la fourniture, le montage et le repérage de jarretières optiques entre les platines de fibres optiques et les équipements actifs ;
- la fourniture, le montage et le repérage de bandeaux de brassage équipés de prises RJ-45, câblé catégorie 6 minimum, et de panneaux passes-fils ;
- la fourniture, le montage et le repérage des câbles d'interconnexion entre les équipements actifs dans un même local ;
- la fourniture, le montage et le repérage de cordons de brassage cuivre catégorie 6 et plus entre les équipements actifs et les panneaux de brassage ;
- la fixation des bornes et la fourniture du câble réseau catégorie 6 minimum entre la prise RJ-45 et la borne Wi-Fi ;
- l'étiquetage et nommage du matériel selon la nomenclature OGIT transmise par la DIRISI.

**Le matériel déployé sur les sites reste à la fin de l'exécution du marché la propriété de l'administration toutefois pendant l'exécution le titulaire en assure la maintenance pour limiter toute interruption de service. Des pénalités, le cas échéant, pourront s'appliquer conformément à l'article 8 du CCAP.**

Il est à noter que les bornes Wi-Fi doivent être hors d'atteinte physique des utilisateurs. Par ailleurs, aucun matériel ne devra être installé dans les locaux de la DIRISI. Une distance minimale de deux (2) mètres devra être respectée avec tout équipement informatique ou électronique du MINARM et avec tout équipement traitant d'information classifiée.

D'une manière générale, le déploiement d'infrastructures réseaux filaires ou sans-fil doit s'adapter aux directives militaires du responsable de la sécurité informatique militaire local (DIRISI/CIRISI) suivant la classification des zones du site.

Le titulaire ne peut pas, sous prétexte d'ignorance, déployer des équipements non adaptés aux conditions environnementales locales.

Les étiquettes de marquage doivent être :

- Lisibles,
- Indécollables et ineffaçables,
- Visibles sans manipulation de l'objet repéré,
- Durables dans le temps.

Tous les câbles sont repérés aux deux extrémités par une étiquette visible sous manchon translucide thermo-rétractable. L'étiquetage et le nommage du matériel doit répondre à la nomenclature OGIT transmise par la DIRISI.

Par ailleurs, dans le cadre du Dossier d'Ouvrages Exécutés du site, le titulaire doit fournir pour chaque câble réseau, un tableau reprenant les valeurs d'atténuation linéique et d'insertion, relevées dans les deux sens sur chaque fibre optique, la moyenne pour chacune des longueurs d'onde mesurées ainsi que les courbes de réflectométrie des liaisons optiques.

## 5.2 Normalisation

Les infrastructures de câblage à prévoir par le titulaire sur les sites doivent être conformes, au minimum, aux normes des systèmes génériques de câblage structurés en vigueur :

- ISO/CEI 11801 (Amend 1 & 2) : Norme internationale.
- EN 50173-1 (C 90-485-1) : Norme européenne.
- EIA/TIA-568A (Addendum 5) : Norme américaine.

La conformité du système de câblage doit respecter les dispositions complémentaires suivantes et notamment concernant les normes des installations électriques basse tension, de compatibilité électromagnétique et de protection contre l'incendie :

- HD 608 : Spécifications génériques des câbles à paires symétriques ;
- EN 187000 : Spécifications génériques des câbles à fibres optiques ;
- NF C 15-100 : Installation électrique basse tension ;
- UTE 89336 : Directive compatibilité électromagnétique ;
- EN 50081-1 : Compatibilité électromagnétique (émission) ;
- EN 50082-1 : Compatibilité électromagnétique (immunité) ;
- IEC 60332, HD 405 : Propagation du feu ;
- IEC 1034, HD 606 : Emission de fumée ;
- IEC 754, HD 602 : Acidité et corrosivité.

L'ensemble des prestations sont exécutées conformément aux normes EN 60793, EN 60794, NFC 15.100 portant sur les liaisons et câbles optiques.

Le fait de ne pas énumérer la totalité des normes et règlements ne peut être pris pour argument d'ignorance par le titulaire, celui-ci étant réputé les connaître, du seul fait de soumissionner.

## 5.3 Délai d'installation du matériel

Le titulaire s'engage à respecter la durée définie sur le devis pour réaliser les travaux d'installation nécessaire pour la mise en service effective et opérationnelle de l'accessibilité au réseau internet.

En cas de retard, des pénalités pourront être appliquées conformément à l'article 8 du CCAP.

## 5.4 Suivi du déploiement sur l'ensemble des sites :

Le titulaire se charge des études relevant de sa compétence.

Les prestations sont réalisées dans les règles de l'art. La pose et l'installation complète du matériel font parties de la prestation. Le titulaire doit préciser dans son offre les raccordements électriques et la place nécessaires à l'implantation de ses matériels.

Le titulaire :

- Assure une prestation de déploiement de la solution en collaboration avec le personnel de l'administration ;
- Désigne un responsable unique qui sera en charge de la conduite et de la coordination de l'ensemble des actions et intervenants sur les deux sites durant le déploiement. Il devra veiller à entretenir une bonne et étroite collaboration avec les correspondants de la DIRISI et de la DID ;
- Respecte les étapes du déploiement qui sont précisées dans son offre ;
- S'assure de la faisabilité de l'installation de ses matériels sur chaque site ;
- S'engage à livrer une fourniture conforme aux lois, règlements ainsi qu'aux normes françaises et européennes en vigueur pendant la durée du marché, notamment en matière d'hygiène et sécurité des conditions de travail.

Le titulaire prend en charge l'organisation de réunions de point de situation durant les phases de déploiement et la rédaction des comptes rendus avec l'ensemble des services de l'Administration.

## **5.5 Réception des travaux**

Avant d'initier la réception définitive, le titulaire s'assure des points suivants :

- Les travaux sont effectivement terminés ;
- Les mesures des supports sont réalisées et disponibles ;
- Les matières, outils sont dégagés, le chantier est propre ;
- Le dossier d'ouvrage exécuté est réalisé et disponible.

Le titulaire doit mettre à disposition de l'Administration, le personnel nécessaire pour l'assister et participer à cette réception. La réception doit apporter la preuve que les opérations d'installation ont été réalisées de bout en bout et sont pleinement fonctionnelles.

Toutes les non-conformités ou dysfonctionnements au cours de la réception doivent être corrigés dans les délais spécifiés et être inscrits sur le procès-verbal de réception.

Le dossier d'ouvrage exécuté des installations livrées remis par le titulaire à l'Administration contient a minima :

- Le nom du site ;
- Un dossier technique de l'installation réalisée (comprenant des photos de l'installation, les synoptiques et schémas de fonctionnement) ;
- Un tableau récapitulatif, pour chaque site, le type de prestation, le matériel déployé (avec sur demande notice technique et configuration), l'implantation des équipements etc. ;
- La documentation en français de la console d'administration et de supervision si existante ;
- Les cahiers de tests et de recettes ;
- L'identification de l'ensemble des paramètres réseau ;
- La maintenance préventive des équipements ;
- La garantie de temps de rétablissement et les coordonnées du service après-vente ;
- La valeur mesurée de la bande passante dans les deux sens ;
- La valeur de la latence.
- Un plan de l'implantation du réseau

L'ensemble des livrables est à fournir au format électronique sur support type clé USB. Un tirage papier est également fourni à l'Administration.

Une fois les connexions livrées et fonctionnelles et le dossier d'ouvrage exécuté transmis, l'Administration réalisera une phase de vérification d'aptitude et une phase de vérification de services régulier :

- la vérification d'aptitude aura pour but de constater que les prestations livrées présentent les caractéristiques techniques qui les rendent aptes à remplir les fonctions demandées dans le présent CCTP ;
- la vérification de service régulier aura pour objet de constater que les prestations fournies sont capables d'assurer un service régulier dans les conditions normales d'exploitation prévues dans le présent CCTP.

La décision de réception définitive des travaux est prise à l'issue de ces deux phases de tests.

## **5.6 Engagement du titulaire**

Le titulaire est réputé avoir pris connaissance des contraintes de tous ordres imposées par l'environnement des sites indiqués au marché, ainsi que des conditions de réalisation des prestations. L'administration fournira au titulaire les éléments, en sa possession, nécessaires à la bonne appréhension de la prestation attendue.

Toutes les prestations sont exécutées conformément aux normes et décrets en vigueur portant sur les installations et plus généralement sur la délivrance des prestations décrites dans le présent CCTP.

La qualité et la continuité du service constituent une prescription impérative du présent marché. Les engagements de qualité de service (SLA- service level agreement) du Titulaire en termes de performances



techniques et fonctionnelles, de disponibilité, de garantie de temps de rétablissement (GTR) doivent en tous points correspondre aux exigences du présent CCTP.

Le non-respect des engagements de qualité de service est sanctionné par les pénalités prévues à l'article 8 du CCAP.

## **ARTICLE 6. SOUTIEN LOGISTIQUE ET MAINTIEN EN CONDITION OPERATIONNELLE (MCO)**

### **6.1 Généralités**

Le MCO fait partie des obligations du titulaire et doit permettre de pallier tous les dysfonctionnements constatés et d'assurer la continuité et la disponibilité du service.

Le MCO prend en compte les éléments suivants :

- La gestion de configuration ;
- L'assistance et le support technique pour l'exploitation et les opérations de maintenance ;
- La fourniture de la documentation d'utilisation et un accompagnement téléphonique en cas de difficultés d'utilisation ;
- Le soutien de l'ensemble des matériels déployés (y compris support fibre/cuivre) et notamment ceux constituant le lien de bout en bout (vérification, intervention, réparation, remplacement) ;
- Les interventions sur site à la demande de la Division de Conduite du Soutien (DCS) ;
- Le soutien des logiciels ;
- La veille technologique et la gestion de l'obsolescence du système déployé.

Le titulaire s'engage à intervenir, sur site si nécessaire, dans les 4 heures après avoir été informé d'une problématique d'accès à internet conformément aux exigences du présent marché. Ce délai commence à courir à partir du moment où l'information du titulaire (via un appel au service client ou une utilisation de l'outil de ticketing) est intervenue dans les heures d'ouverture du service d'assistance téléphonique comme décrit ci-dessous.

La date et l'heure d'émission de l'appel ou du ticket fait foi.

### **6.2 Assistance**

Le titulaire met à disposition auprès de l'utilisateur final, a minima 10 heures sur 24 et 7 jours sur 7, un service d'assistance téléphonique exclusivement en langue française parfaitement maîtrisée, avec un délai garanti de réponse du front office ne pouvant excéder 10 minutes. Ce service doit être en mesure de fournir une assistance de premier niveau (type gestion des incidents) et de fournir en instantanée l'état du lien (supervision).

L'ouverture de ce service d'assistance téléphonique sur une amplitude horaire plus conséquente sera valorisée au RC.

Le titulaire met également à disposition 24 heures sur 24 et 7 jours sur 7 un service de déclaration et de suivi d'incident (outil de ticketing) disponible via internet.

### **6.3 Garantie de temps de rétablissement (GTR)**

Le temps de rétablissement correspond au délai écoulé entre l'heure de signalement de l'incident par l'Administration au service d'assistance téléphonique ou sur l'outil de ticketing et l'heure de fin de l'incident.

Ce temps de rétablissement ne peut excéder 24h00. La réduction de ce temps de rétablissement sera valorisée au RC.

#### **6.4 Maintenance préventive et curative**

Les prestations de maintenance doivent prévoir notamment l'échange standard d'un composant hors service ou défectueux. Les matériels en panne seront remplacés dans un délai compatible avec les exigences de rétablissement prévu précédemment.

Le titulaire doit fournir les mises à jour logicielles et matérielles nécessaires au maintien en condition opérationnelle et de sécurité des solutions déployées, en particulier, si une faille de sécurité est découverte dans le logiciel d'un équipement. Les matériels qui ne pourraient être mis à jour du fait de leur obsolescence doivent être remplacés dans les trois mois suivant la déclaration du constructeur.

-----  
**A titre d'information les caractéristiques techniques du matériel existant sur les sites se décomposent comme suit :**

- bornes WIFI de marque RUCKUS R320