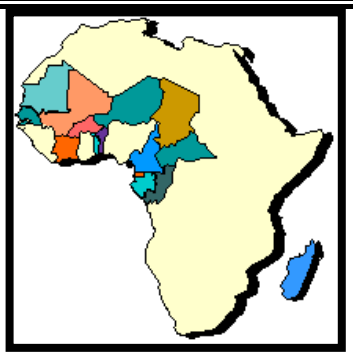
ASECNA

AGENCE POUR LA SECURITE DE LA NAVIGATION AERIENNE EN AFRIQUE ET A MADAGASCAR

☐BENIN ☐BURKINA FASO ☐CAMEROUN ☐ CENTRAFRIQUE ☐ COMORES ☐ CONGO ☐ COTE D'IVOIRE ☐ FRANCE ☐ GABON ☒SIEGE		☐ GUINEE BISSAU ☐ GUINEE EQUATORIALE ☐MADAGASCAR ☐MALI ☐ MAURITANIE ☐ NIGER ☐ RWANDA ☐ SENEGAL ☐ TCHAD ☐TOGO

Mise en place d'un système de contrôle d'accès au réseau informatique de l'ASECNA

PSE 2023-2027

OP: 2919, CB: 2490, NPE: 926 080

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

CERTIFIEE ISO 9001 v. 2008

DIRECTION GENERALE

Direction des Moyens Techniques et Informatiques

✉ : 3144 DAKAR-YOFF SENEGAL ☎ : (221) 33 849 66 00 Fax : (221) 33 823 46 54

HISTORIQUE DU DOCUMENT

VERSION	DATE	DESCRIPTION DE L'EVOLUTION	OBSERVATIONS
V1	04/10/2023	Définition des spécifications techniques	
V2	06/05/2024	Mise à jour des spécifications techniques	

NOTE IMPORTANTE : Toute nouvelle version annule et remplace la version précédente qui doit être détruite ou portée clairement sur la page de garde la mention manuscrite *VERSION PERIMEE.*

MAITRISE DU DOCUMENT

MAITRISE DU DOCUMENT				
	Nom	**Fonction**	**Visa**	**Date**
Rédacteur	SOGBOSSI Aurlus	DTIDR		10-06-24
Vérificateur	SOILIH Rashid	DTIDR		11-06-24
Approbateur	TSHIMANGA née ZOUNGARANI Flora Mathilde	DTIDR		12-06-24

LISTE DE DISTRIBUTION	
DESTINATAIRES:	DGDS
AMPLIATAIRES:	

1. Introduction

1.1 Objet du Projet

Dans le cadre du renforcement de la sécurité de son réseau informatique, l'ASECNA se propose à travers son Plan de Services et d'Equipements (PSE) 2023-2027, de mettre en place un système de contrôle d'accès à son réseau informatique.

1.2 Objet du document

Le présent document constitue le Cahier des Prescriptions Techniques Particulières du projet de mise en place d'un système de contrôle d'accès au réseau informatique de l'ASECNA. L'objet du document est de définir les exigences et fonctionnalités minimales de la solution de sécurité à acquérir.

2. Contexte du projet

2.1 Présentation de l'ASECNA

L'Agence pour la Sécurité de la Navigation Aérienne en Afrique et à Madagascar (ASECNA) est un établissement public à caractère multinational. Elle est dotée de la personnalité juridique et jouit d'une autonomie financière. Elle regroupe 19 Etats qui sont : Bénin, Burkina Faso, Cameroun, Centrafrique, Congo, Côte d'Ivoire, France, Gabon, Guinée Equatoriale, Guinée Bissau, Madagascar, Mali, Mauritanie, Niger, Rwanda, Sénégal, Tchad, Togo et Union des Comores.

L'ASECNA est implantée sur vingt-huit (28) sites principaux :

- Une Direction Générale, à Dakar au Sénégal, repartie sur quatre (04) sites : Jean Jaurès en ville (DGVille), Yoff (DGYoff), SAN MARCO à Yoff et Almadies.
- Dix-huit (18) Représentations : Bénin, Burkina Faso, Cameroun, République Centrafricaine, Congo, Côte d'Ivoire, Gabon, Guinée Equatoriale, Guinée Bissau, Madagascar, Mali, Mauritanie, Niger, Rwanda, Sénégal, Tchad, Togo, l'Union des Comores ;
- Trois (03) écoles : ERNAM (Dakar/Sénégal), ERSI (Douala/Cameroun) et EAMAC (Niamey/Niger);
- Trois (03) Délégations respectivement en Europe (Paris), auprès de l'Organisation de l'Aviation Civile Internationale (OACI à Montréal) et à l'Union Africaine (Addis-Abeba).

L'ASECNA assure une mission de service public de sécurité de la navigation aérienne et de la météorologie aéronautique.

2.2 Description de l'existant

L'Agence dispose pour ses besoins de fonctionnement, d'un panel de plus d'une centaine de serveurs et près de 5000 Devices (PCs, smartphones, imprimantes, Cameras, APs et autres types IOT etc.) interconnectés via un réseau WAN et plusieurs réseaux LANs.

Le site de DGYoff est le site principal de l'infrastructure réseau de l'Agence. Il agrège tous les accès en provenance des autres sites de l'Agence et à destination des applications et services localisés au siège.

Le site de DGVille héberge certaines applications et constitue le site de backup de l'organisme pour les applications et serveurs existants.

Plusieurs centaines d'utilisateurs sont physiquement localisés sur les différents sites du Siège. Et ces utilisateurs accèdent aux applications au travers du réseau local LAN ou élargi (pour les utilisateurs de Dakar Ville) à travers la liaison fibre de 200 Mo reliant les deux sites (DGYoff et DGVille) avec un backup VPN de 40Mbs.

Le site de DGYoff est relié aux sites de l'ERNAM, de SAN MARCO et des Almadies par fibre optique.

Toutes les Représentations (à l'exception de la Représentation du Sénégal reliée par fibre optique) sont connectées au site de Yoff via des liaisons satellitaires et des liaisons VPN.

L'ASECNA dispose d'une infrastructure de sécurité composée :

- Des pares-feux
- Des IPS/ IDS
- MFA & SSO
- ZTNA
- WAF
- Des zones démilitarisées et d'isolation
- D'un domaine Active Directory avec l'activation de plusieurs stratégies
- Des proxy et proxy inverses ;
- Des autorités de Certificat interne ;
- Des documents et procédure décrivant des scénarii d'attaque.

2.3 Description de l'architecture cible

L'architecture cible repose sur quarante-huit (48) sites dont deux (02) sites de type Siège (sites de DGYoff et DGVille) et 46 de type succursale. Le schéma ci-dessous présente la description de l'architecture cible souhaitée.

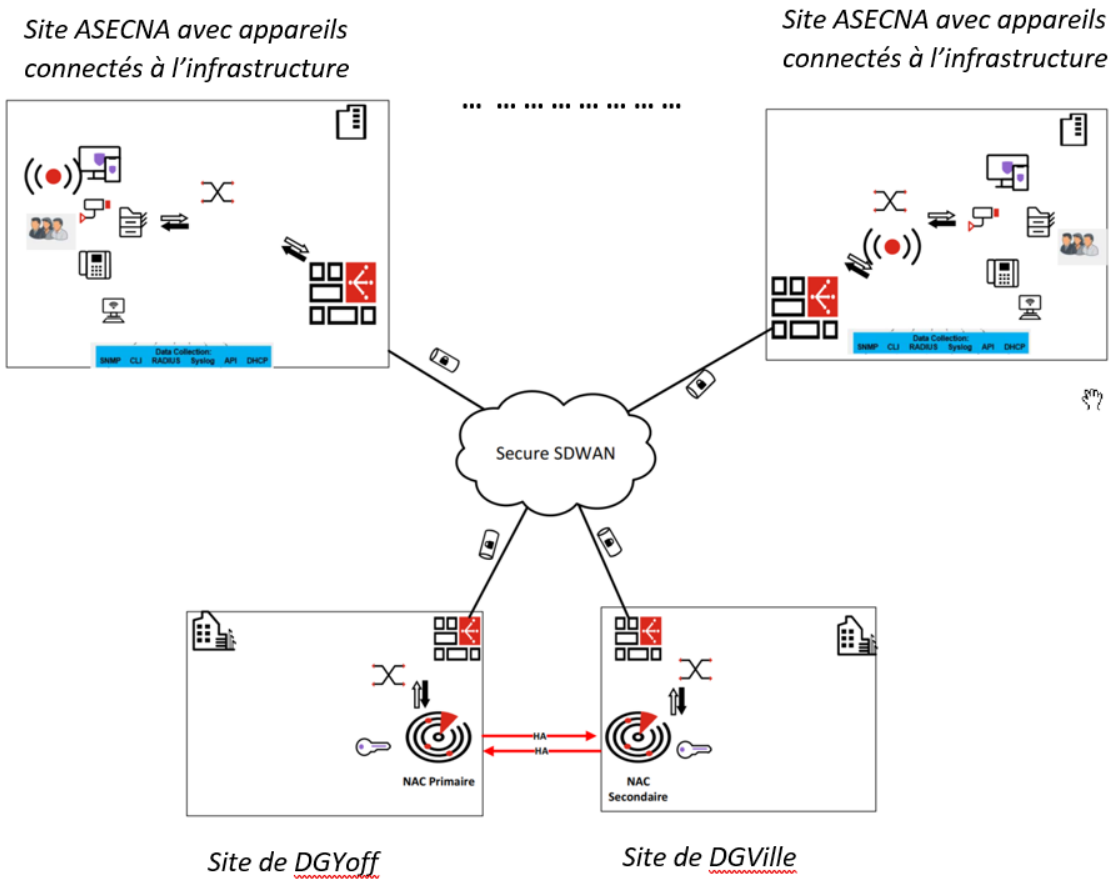
La solution NAC sera déployée en primaire sur le site de DGYoff et en secondaire sur le site de DGVille avec replication des appliances physiques entre les deux sites.

La solution NAC sera déployée en haute disponibilité sur les sites principal et secondaire en tant qu'équipements physiques.

La solution NAC communique avec les périphériques d'infrastructures, tels que les contrôleurs sans fil, les points d'accès, les commutateurs, les Firewalls, le MFA & SSO et autres installés sur l'ensemble des quarante-huit (48) sites de l'ASECNA.

Tous les appareils connectés à l'infrastructure sur tous les sites de l'ASECNA seront détectés et visibles depuis la console centrale et les politiques de contrôles d'accès seront appliquées à partir de cette même console.

Ci-dessous l'architecture cible de la solution NAC à deployer.



Architecture cible

3. Spécifications des offres

3.1 Prestations attendues

Cette section prescrit la consistance des travaux à réaliser dans le respect des spécifications techniques minimales associées.

Lors de la visite obligatoire des sites de Dakar avant la proposition de son offre, le Soumissionnaire vérifiera les informations fournies dans ce document.

A travers les visites de sites qui seront organisés à cet effet, il devra les compléter afin de tenir compte de tous les aspects pour proposer une offre la plus complète possible.

Il ne pourra en aucun cas se prévaloir ni des omissions, ni des oublis.

Le Soumissionnaire doit fournir des prestations suivantes :

- Fournir, installer et configurer la solution NAC dans l'environnement de production. La configuration de la solution se fera suivant les meilleures pratiques de sécurité recommandées et conforment aux exigences de la norme ISO 27001. Toutes les offres doivent se conformer à cette norme dans sa version la plus récente ;
- Tester et valider la plateforme en production ;
- Surveiller la plateforme en production ;
- Faire la recette site de la solution (**la recette sera précédée d'un test intrusif**) ;

- Transfert de compétences aux Ingénieurs et Techniciens de l'Agence ;
- Former les ingénieurs et techniciens de l'ASECNA ;
- Fournir l'ensemble des livrables du projet : dossiers d'architecture, d'ingénierie, d'installation et de configuration, d'exploitation, de gestion projet et les procédures de gestion d'incidents associées ;
- Fournir la datasheet des composantes de la solution NAC ;
- Fournir la garantie sur l'ensemble des composantes de la solution ;
- Réaliser les maintenances préventives et curatives lors de la période de garantie ;
- Proposer une procédure de backup en conformité avec la politique de sécurité de l'ASECNA ;
- Proposer une procédure de HA en conformité avec la politique de sécurité de l'ASECNA.

3.2 Spécifications techniques des équipements

Le soumissionnaire doit proposer une solution NAC qui répond aux spécifications techniques minimales suivantes :

Spécifications minimales exigées	**Spécifications proposées (préciser les références sur la datasheet fourni)**
Description	
Être capable de s'intégrer avec les équipements réseau et sécurité existant	
Etre capable de s'interfacer avec multiples solutions mêmes hétérogènes	
Eliminer ***'les angles morts'*** et offrir des données riches sur les hosts connectés (IoT Devices)	
Offrir la visibilité réseau, le Profiling de Devices, Conformité des Endpoints, et le Provisioning réseau automatique	
Le système ne doit pas se baser sur une intégration avec Port SPAN	
Permettre d'authentifier et autoriser les utilisateurs et les Endpoints via connexion par câble, sans fil ou VPN avec des politiques de sécurité spécifiques	
Fonctionner sur les endpoints avec Agent ou sans Agent (Agentless)	
Offrir la possibilité d'avoir un Agent dissolvable pour quelques profils	
Etre capable de faire des inventaires de tous type de devices connectes au réseau mêmes non-PC comme les imprimantes, IP-Phones, Smart Phones, IoT.	
Autoriser l'accès via affectation de VLAN ou application d'une Access Control List (ACL)	
Obligatoirement s'intégrer avec l'infrastructure existante en utilisant les protocoles SNMP v1/v2c/v3, CLI (SSH v1 et v2, Telnet), Syslog, API, LDAP, DHCP, MDM et Radius	

Ne doit pas dépendre que de l'intégration 802.1x et Radius	
Etre évolutive et offrir la possibilité de commencer avec un petit scoop au départ et s'élargir par la suite	
La solution NAC ne doit pas être en coupure (Out of Band)	
En cas d'indisponibilité du NAC, les terminaux authentifiés fonctionnent et aucun nouvel équipement ne doit pouvoir se connecter au réseau	
La solution doit offrir un management des GUEST simple et rapide pour créer des comptes guest par des agents operateurs normaux sans demander au Staff IT	
La solution NAC doit être basée sur un model licencing perpétuel	
La solution NAC doit être au format Hardware	
Supporter au minimum 100 terminaux et extensibles à 50 000	
Permettre la visibilité, le contrôle et la réponse (remédiation)	
Le nombre total de terminaux/Endpoints/IOT/OT/ que doit supporter la solution est 6000	
La garantie constructeur doit être de 3 ans	
La solution NAC doit être en mode HA	
Exigences de profiling des Endpoints	
La fonctionnalité de profiling doit être fournie sans licence additionnelle	
Supporter, pour les Devices sans agents, le profiling basé sur le DHCP fingerprinting, scan NMAP, Vendor OUI, Emplacement,Ports Ouverts, connexion SSH ou Telnet et aussi l'existence de l'agent persistent.	
Supporter le Profiling pour iPhone, iPad, Android, les imprimantes réseau, les cameras de surveillance IP, et tout autre appareils IoT	
Supporter le Profiling via les caractéristiques SNMP, NMAP, TCP & UDP	
Supporter le Profiling via WMI	
Possibilité de créer des règles de Profiling personnalisées	
Exigences d'authentification	
Supporter nativement le Radius MAC-adresse Withelisting et Blacklisting	
Supporter l'Authentification Multi-Facteur (MFA)	
Supporter des options d'authentification flexibles comme le 802.1X, Web Authentication et MAC authentification ;	
Supporter l'intégration avec LDAP, RADIUS et Microsoft AD	
Supporter l'authentification des utilisateurs et des machines sans besoin de configuration additionnelle ;	
Permettre d'authentifier un Endpoint utilisant un scanning Agentless (sans agent installé) ;	
Permettre uniquement aux devices managés ou authentifiés à se connecter au réseau de l'organisation et	

appliquer les politiques de sécurité en bloquant, isolant et remédiant les postes non conformes dans le réseau, et la mise en quarantaine sans intervention de l'administrateur.	
S'integrer avec les solutions MDM comme AirWatch, Maas360 et Mobilelron, etc	
Exigences pour la conformité et la remédiation des Endpoints	
Pouvoir vérifier plusieurs règles de conformité à travers un agent lourd installé pour contrôler si : • un antivirus a été installé ; • sa version est mise à jour ; • certains services ou applications fonctionnent correctement sur le poste de travail ; Selon l'état de conformité du poste de travail, il lui sera : • garanti un niveau d'accès spécifique ; ou éventuellement, • assigner un VLAN de quarantaine pour le temps nécessaire à la remédiation Apres ces étapes, l'agent vérifie automatiquement de nouveau la conformité. Si le poste de travail s'avère conforme, la solution pourra appliquer une nouvelle politique. Ce contrôle de conformité peut être répété périodiquement pour vérifier par exemple qu'un antivirus ne s'est pas désactivé après la première vérification.	
Les agents devront être téléchargeables depuis la solution au moment du premier contrôle de conformité	
Supporter les Agents (Agent Persistant et Agent Dissolvable) et doit aussi permettre de scanner les Endpoints sans Agent (Agentless)	
Fournir un Rôle Quarantaine lié aux solutions de patch management intégrées : Dans le cadre de ce rôle de quarantaine. la solution doit fournir un portail web captif d'auto- correction" Les périphériques non conformes doivent être mis en quarantaine de manière dynamique et accompagnés d'instructions de correction automatique tels que biofix et patchlink	
Fournir des mises à jour planifiées pour AV et Antispyware (version du fichier .dat et du moteur) et des exceptions à créer si nécessaire	
Gestion des invités	
La gestion des invités doit supporter les notifications par SMS et Email	
La gestion des invites doit être configurable pour répondre à diverses exigences telles que les invites à court ou long terme, le mode conférence ou les invités auto-enregistrés	
La solution doit offrir un accès administratif limité et contrôlé pour la gestion des invités uniquement	
La gestion des invites doit permettre d'offrir des accès parrainés par les employés	

Exigences de gestion et de reporting	
Offrir une console intégrée de Monitoring, de création de rapports et de dépannage pour faciliter la tâche des opérateurs et des administrateurs du helpdesk	
Comporter un modèle de création de stratégie avec des Templates prédéfinis et un assistant de création de stratégies facilitant le déploiement de stratégies à l'échelle de l'entreprise	
Possibilité d'avoir des solutions de Management et de Reporting dédiées	
Inclure un module de Monitoring, Reporting et Diagnostique intégré accessible via la GUI	
Automatisation des réponses	
Offrir l'automatisation des actions suites a des détections de brèches ou attaques en s'intégrant avec d'autres solutions de sécurité	
Licence et support	
Les licences et support doivent couvrir l'ensemble des fonctionnalités de la solution.	
Les licences fournies doivent être perpétuelles	

Spécifications techniques de l'Appliance physique de la solution NAC (Quantité 02)

Spécifications minimales exigées et quantités		Spécifications proposes et quantités
Système		
CPU	2,1 G, 8C/16T, 9,6 GT/s, 11 Mo de cache, Turbo (quantité 2)	
Mémoire	8 Go (quantité 4)	
Disque dur	Disque dur SATA 6 Gbit/s enfichable à chaud (quantité 2)	
Lecteur optique	Pas nécessaire	
BMC	iDRAC9 Express, intégré (Qté 1)	
Interface réseau	Broadcom 5720 QuadPort 4x 1 Go Ethernet, RJ45	
Carte RAID	Contrôleur RAID intégré PERC H330 (Qté 1)	
Configuration RAID	RAID1	
Accès aux consoles	Aucun	
Facteur de forme	Montable en rack 1U	
Environnement		
Source de courant	Double alimentation enfichable à chaud	
Affichage du panneau	Pas d'écran LCD	
Attestation		

Sécurité	Certifié comme applicable par les autorités de sécurité des produits du monde entier, notamment aux États-Unis (NRTL), au Canada (SCC) et dans l'Union européenne (CE).	
Électromagnétique (CEM)	Certifié comme applicable par les autorités EMC du monde entier, notamment aux États-Unis (FCC), au Canada (ICES) et dans l'Union européenne (CE).	
Matériaux	Certifié comme applicable par les autorités des matériaux du monde entier, y compris l'Union européenne (ROHS) et la Chine (ROHS).	

3.3 Livrables du projet

I. Formations

Les formations sont destinées au Personnel IT en charge de la sécurité informatique de l'ASECNA. Elles doivent correspondre aux formations officielles de l'éditeur de la solution.

L'objectif est de disposer de personnel IT qualifié et capable de configurer, d'exploiter et d'administrer le système NAC selon les règles de sécurité défini par l'ASECNA.

Toutes les formations doivent se dérouler dans un **centre agréé** par l'éditeur de la solution NAC.

Le Soumissionnaire est tenu de prendre en charge totalement les frais de formation de l'ensemble des participants y compris les vouchers des examens de certifications.

Le Soumissionnaire est invité à proposer, aux équipes techniques de l'ASECNA, des formations officielles certifiantes ci-après :

- Formation certifiante sur la solution NAC dans un centre agréé pour onze (11) personnes.
- Formation certifiante CEH (Certified Ethical Hacker) pour une (01) personne

II. Planning et méthodologies des différentes prestations

Les prestations de fourniture, d'installation et de configuration (incluses d'ailleurs dans les prix) de la solution NAC doivent respecter la démarche suivante :

- Des réunions de cadrage et de suivi du projet ;
- Une phase d'implémentation et de configuration ;
- Une phase de déploiement ;
- Une phase de tests et de validation ;
- Une phase de surveillance des équipements en production ;
- Une phase de formation et de transfert de compétences.

a) Réunions de cadrage et de suivi

Une première réunion de cadrage du projet doit être prévue pour concerter les objectifs ainsi que le planning du projet. Cette réunion doit être tenue, dans les 05 jours, au maximum, qui suivent l'ordre de service de commencement des prestations. Un point d'avancement et de cadrage se fera de manière hebdomadaire pour le bon déroulement du projet

b) Phase d'implémentation et de configuration

Lors de cette phase, le Soumissionnaire fera les implémentations et configuration nécessaire sur les équipements fournis dans un environnement hors de production.

Tous les travaux de configuration, d'installation et de déploiement des équipements objets de cet appel d'offres doivent être réalisés sans interruption ou dégradation des services opérationnels au niveau de l'ASECNA.

La mise en production se fera conformément aux plans de déploiement, de test et prérequis qui seront préalablement validés par l'ASECNA.

Le Soumissionnaire doit procéder à :

- La mise en rack des équipements ;
- L'interconnexion avec l'infrastructure réseau et sécurité existants ;
- Test des installations.

En termes de livrables, le Soumissionnaire doit fournir la liste non exhaustive des livrables précisés dans les prestations.

La phase de mise en production ne débutera qu'après validation par le maître d'ouvrage des différents livrables de la présente phase.

c) Phase de déploiement

Le Soumissionnaire sera amené à élaborer une procédure de déploiement qui doit être validée par l'équipe de l'ASECNA. Elle doit être complète et englobera toutes les étapes de l'installation au déploiement des équipements sur les sites (mise en production) de la Direction Générale à Dakar. Une fois validé, le Soumissionnaire procédera au déploiement des équipements dans la plateforme en production.

La phase de test et de validation ne débutera qu'après déploiement de tous les équipements vers la plate-forme de production.

d) Phase de test et de validation

Le Soumissionnaire est amené à élaborer dans un premier temps un plan de test et un cahier de test (fonctionnement et performance) qui doit être validé par l'équipe de l'ASECNA. Sur base de ce plan, des tests vont être réalisés par le Soumissionnaire en présence de l'équipe de l'ASECNA, pour vérifier le bon fonctionnement et les performances des différents équipements et logiciels installés et leur conformité aux besoins exprimés dans le présent cahier de prescriptions spéciales et lors de la phase préliminaire.

En termes de livrables, le Soumissionnaire doit fournir :

- Plan de test et cahier de test ;
- Résultats des tests.

e) Phase de formation et de transfert de compétences

Cette phase sera consacrée à la formation du personnel de l'ASECNA, ainsi que le transfert de toute compétence nécessaire pour gérer la nouvelle plateforme. A la suite des transferts de compétences et des formations, les livrables de supports de formations et documents d'exploitation devront être fournis.

A partir de cette date, la phase de support après-vente devra couvrir les mises à jour et demandes d'assistances/modifications ou d'améliorations de l'ASECNA.

f) Dispositions générales

- Les interventions techniques devront tenir compte des contraintes en termes d'horaires (7h30 – 15H30) ;
- Les travaux nécessitant l'arrêt d'un service se feront hors des heures de travail et devront faire l'objet d'une planification rigoureuse.

III. Responsabilité et engagement du Prestataire pendant la période de garantie

a) Nature des prestations durant la période de garantie

- **Maintenance Hardware**

- Maintenance préventive des équipements en production ;
- Maintenance curative pour :
    - Le dépannage des équipements et matériels défectueux sur appel du maître d'ouvrage ;
    - La résolution des problèmes de paramétrage (tuning) des équipements sur appel du maître d'ouvrage.
- Mise à jour des firmwares planifiée en commun accord entre le maître d'ouvrage et le titulaire ;
- Un accès à un service de support client (Hot Line) pour pouvoir soumettre des questions relatives au paramétrage et de configuration des équipements fournis.

b) Centre d'appel

Pendant la période de garantie, le Soumissionnaire s'engage à mettre en place un centre d'appel (numéro de téléphone unique) à la disposition du maître d'ouvrage. Ce centre d'appels devra être aux standards internationaux devra assurer la prise en charge des appels des représentants du maître d'ouvrage et d'attribuer un numéro à chaque appel.

Ce centre d'appel doit être disponible chaque jour du lundi au vendredi de 07H30 à 15h30.

c) Enregistrement des appels par le maître d'ouvrage auprès des prestataires

Toutes les pannes ou anomalies constatées par le Maître d'Ouvrage, pourront être signalé au Soumissionnaire par l'un des moyens suivants :

- un appel téléphonique ;
- une demande d'intervention écrite communiquée au technicien relevant du Prestataire s'il se trouve sur place ;
- une correspondance.

Ainsi le Soumissionnaire remettra au maître d'ouvrage

- un numéro de téléphone unique ;
- une adresse mail.

d) Remise en état de l'équipement en panne sur site

Par remise en état, il est entendu la remise en service du matériel via :

- Pour les incidents hardwares :
    - Soit un procédé de réparation sur site ;
    - Soit un remplacement provisoire de l'équipement défectueux par un équipement équivalent dont les performances seront validées par le maître d'ouvrage.
- Pour les incidents logiciels :
    - Soit via un procédé de rectification sur site ;
    - Soit un procédé de correction temporaire ou de solutions d'urgence de contournement si la rectification définitive nécessite un délai plus long.

e) Réparation en atelier

- Pour les incidents hardwares : Quand la réparation nécessite le retour en atelier du Soumissionnaire, le matériel défectueux devra être récupéré pour réparation et retourné au lieu de son exploitation par les services du Soumissionnaire et à sa charge. Les frais de transport éventuels d'un équipement pour réparation, dans les ateliers du Soumissionnaire, sont à la charge de ce dernier.
- Pour les incidents logiciels : Lorsque la rectification définitive exige un délai long de mise en œuvre qui risquent de gêner l'exploitation, le Soumissionnaire est tenu d'apporter une solution dans les délai impartis en collaboration avec l'éditeur pour assurer le bon fonctionnement du logiciel.

f) Remplacement définitif des équipements

Lorsque l'équipement en panne ne peut pas être réparé dans le délai de 10 jours, le Soumissionnaire doit procéder à son remplacement définitif par un équipement de même marque

et performances au moins égales à celles de l'ancien. Un PV de remplacement définitif sera établi entre le maître d'ouvrage et le Soumissionnaire.

g) Fiche d'intervention

A la fin de chaque intervention, le Soumissionnaire doit établir une fiche d'intervention qui porte sur les tâches effectuées. Cette fiche, datée et signée par les représentants du Maître d'ouvrage et du Soumissionnaire, doit indiquer la date et l'heure exacte d'achèvement des travaux réalisés par le Soumissionnaire et doit être communiquée au Maître d'ouvrage.

La date de fermeture des appels (date de résolution de l'incident) sera la date d'achèvement mentionnée sur la fiche d'intervention. Si la fiche d'intervention est non datée, la date de fermeture sera la date à laquelle le maître d'ouvrage a fermé l'appel au niveau de son système de gestion des incidents.

h) Délais

Le Soumissionnaire s'engagera à respecter les délais suivants :

Délai d'intervention	Délai de remise en état	Délai de réparation en atelier
02 Heures	24 Heures	15 jours pour les incidents hardwares 07 jours pour les incidents logiciels

NB : les délais ci-dessus sont comptés à partir de l'heure de l'enregistrement d'appel auprès du Soumissionnaire.

IV. Qualification du Prestataire

NB : L'ASECNA se réserve le droit de vérifier par des moyens qui lui seront propres l'exactitude de toutes les informations transmises par le soumissionnaire.

i. Le Soumissionnaire doit apporter la preuve écrite :

- qu'il satisfait aux exigences de capacité technique c'est-à-dire :
  - qu'il disposera des moyens logistiques de service après-vente ;
  - qu'il disposera des moyens humains nécessaires (disponibilité d'un personnel qualifié);
- que les fournitures ou ressources techniques qu'il propose fonctionnent normalement dans les conditions de travail des pays tropicaux.

ii. Le Soumissionnaire doit prouver, documentation à l'appui, qu'il satisfait aux exigences d'expérience ci-après :

- Expérience du Soumissionnaire/Fabricant en matière de déploiement de solution NAC. Nombre minimum de marchés : au moins deux (2) exécutés de manière satisfaisante en tant que principal fournisseur de solution NAC.

N.B. : *Les critères de capacité technique et d'expérience serviront uniquement à établir si le Soumissionnaire/Fabricant possède une capacité technique lui permettant d'exécuter le Marché de manière satisfaisante. Ils ne serviront pas de coefficient de pondération pour déterminer le Soumissionnaire le moins disant.*

iii. Le Soumissionnaire doit prouver, documentation à l'appui, s'il n'est pas fabricant, qu'il est partenaire Authorized.

iv. Le Soumissionnaire doit prouver, documentation à l'appui, qu'il dispose pour le projet d'au moins un ingénieur sécurité ayant une certification de niveau expert sur la solution NAC de l'éditeur. La certification doit être en cours de validité.

4. Autres dispositions générales

Les dispositions suivantes s'appliquent aux solutions à acquérir.

a. Evolution technologique

Les configurations proposées au fur et à mesure de l'exécution du marché devront tenir compte des dernières évolutions technologiques et proposer à la date de la commande le nouveau produit dont les performances seront supérieures à celles définies dans le CPTP initial et à coût équivalent.

b. Inspections et essais

Les inspections et tests suivants seront réalisées : vérification et un test de bon fonctionnement des tous les matériels fournis pour tous les lots lors de la réception provisoire.

c. Lieu de livraison

DIRECTION GENERALE DE L'ASECNA
DIRECTION DES MOYENS TECHNIQUES ET INFORMATIQUES
ASECNA – BP 8163 Aéroport Léopold Sédar SENGHOR, Dakar-Yoff (Sénégal), Téléphone: +221 33 869 51 24/25 – Télécopie: +221 33 820 00 15

FIN DE DOCUMENT