

بسم الله الرحمن الرحيم

République Islamique de
Mauritanie
Honneur – Fraternité – Justice

**Ministère de la fonction publique et
de la modernisation de
l'administration**



الجمهورية الإسلامية الموريتانية
شرف / أخاء / عدل

وزارة الوظيفة العمومية وعصرنة الإدارة

APPEL D'OFFRES INTERNATIONAL

ACQUISITION D'UNE SOLUTION D'OPTIMISATION ET DE SECURISATION DU RESEAU EN DEUX LOTS SEPARES

Financement : Budget de l'Etat

Août 2007

SECTION I

1 AVIS D'APPEL D'OFFRES (AAO)

AVIS D'APPEL D'OFFRES

Le Ministère de la Fonction Publique et de la Modernisation de l'Administration de la République Islamique de Mauritanie, sur financement du Budget de l'Etat, invite, par le présent Appel d'Offres, les sociétés informatiques admises à concourir à présenter leurs offres sous pli fermé, pour la fourniture d'une solution d'optimisation et de sécurisation du réseau de l'administration en vue d'assurer une meilleure qualité de service dans le cadre de sa mission de modernisation de l'administration en **deux lots (2) indépendants** portants sur :

- **Lot1 : Protection résidente, stratégie de sécurité et optimisation de la configuration**
- **Lot 2 : Filtrage du contenu et optimisation de la navigation**

Les soumissionnaires intéressés à concourir peuvent obtenir des informations supplémentaires et examiner les Dossiers d'Appel d'Offres dans les locaux du Ministère de la Fonction Publique et de la Modernisation de l'Administration, (Direction Générale de l'Informatique de l'Administration) Immeuble du Gouvernement BP : 184 – République Islamique de Mauritanie ; Téléphone ; (222) 5255430 ; Fax : (222) 529 79 07 ; E-mail : medkaber@modernisation.gov.mr Ou sur le site internet du département à l'adresse web suivante : <http://www.modernisation.gov.mr>.

Le Dossier d'Appel d'Offres pourra être acheté par les candidats, sur demande écrite au service mentionné ci-dessus et moyennant paiement au Trésor Public d'un montant forfaitaire non **remboursable de 10.000 Ouguiyas**.

Toutes les offres doivent être déposées à l'adresse indiquée ci-dessous au plus tard le **mercredi 19 septembre 2007 à 10H** et être accompagnées d'une garantie d'offre d'un montant au moins égal à 1% du montant de la soumission.

Dossiers adressés à :

**Monsieur le Président de la Commission Centrale des Marchés,
Immeuble du Gouvernement,
BP: 184 Nouakchott - Mauritanie**

Les plis seront ouverts en présence des représentants des soumissionnaires qui souhaitent être présents à l'ouverture, **mercredi 19 septembre 2007 à 10H**, à l'adresse ci-dessus de la commission centrale des marchés

Le Secrétaire Général du MFPMA

Mohameden Ould Bah Ould Hamed

SECTION II

2 DONNEES PARTICULIERES DE L'APPEL D'OFFRES

TABLE DES MATIERES

1. OBJET	6
2. CONSISTANCE DE LA PRESTATION	6
3. DELAI DE LIVRAISON :	6
4. GARANTIE	6
5. CALCUL DES COUTS ET MONNAIE DE SOUMISSION	6
6. PIECES CONSTITUTIVES DU DOSSIER D'APPEL D'OFFRES :	6
7. CAUTIONNEMENT PROVISOIRE	7
8. COMPOSITION DES OFFRES :	7
9. PRESENTATION DES OFFRES :	8
10. LIEU ET DATE DE DEPOT DES OFFRES :	8
11. SUITE A DONNER A L'APPEL D'OFFRE :	9
12. OUVERTURE DES PLIS :	9
13. FORME DES SOUMISSIONS :	9
14. REGIME FISCAL ET DOUANIER :	9
15. RENSEIGNEMENT :	9
16. EVALUATION ET COMPARAISON DES OFFRES :	9
17. ACQUISITION DU DOSSIER D'APPEL D'OFFRES :	10

1. Objet

Le présent document a pour objet de définir les données particulières de l'appel d'offres relatif à l'acquisition d'une solution d'optimisation et de sécurisation destinée à optimiser le réseau administratif et à renforcer la sécurité du système d'information de l'Administration publique mauritanienne.

2. Consistance de la prestation

La prestation objet du présent appel d'offres porte sur la fourniture et la mise en œuvre d'une solution d'optimisation et de sécurisation globale en deux lots indépendants portant sur :

- **LOT 1 : Protection résidente, stratégie de sécurité et optimisation de la configuration**
- **LOT 2 : Filtrage du contenu et optimisation de la navigation**

Les prestations en objet concernent la fourniture et l'installation conformément aux règles de l'art des solutions ci-dessus et tels que définis dans les prescriptions techniques du présent dossier d'appel d'offres.

3. Délai de livraison :

Les délais d'exécution seront proposés par les soumissionnaires, qui soumettront avec leurs offres un planning détaillé d'exécution des différentes prestations. Toutefois, les délais proposés ne devront pas excéder 1 mois.

4. Garantie

La garantie des prestations est obligatoire pour une période de 12 (douze) mois à compter de la date de la réception provisoire.

5. Calcul des coûts et monnaie de soumission

Les coûts des prestations seront exprimés en toutes taxes. La monnaie de soumission est l'Ouguiya (**UM**), conformément au modèle de soumission.

6. Pièces constitutives du Dossier d'Appel d'Offres :

Les pièces constitutives du dossier d'appel d'offres sont les suivantes :

- Pièce n° 1 : Avis d'appel d'offres ;
- Pièce n° 2 : Données particulières de l'appel d'offres ;
- Pièce n° 3 : Le Modèle de soumission ;
- Pièce n° 4 : Le Cahier des Prescriptions Spéciales de l'appel d'offres ;
- Pièce n° 5 : Le Modèle de contrat ;
- Pièce n° 6 : Devis estimatif et Quantitatif et bordereau des prix unitaires ;
- Pièce n° 7 : Les Prescriptions Techniques des fournitures ;
- Pièce n° 8 : Modèle de curriculum vitae
- Pièce n° 9 : Modèle de cautionnement provisoire ;
- Pièce n° 10 : Modèle de cautionnement définitif ;
- Pièce n° 11 : Modèle de cautionnement de restitution d'avance.

7. Cautionnement provisoire

Le soumissionnaire devra constituer, auprès d'une banque agréée ou installée en Mauritanie, un cautionnement provisoire égal au moins à **1%** du montant de sa soumission. Ce cautionnement sera libéré à la désignation du candidat retenu. Le cautionnement du soumissionnaire retenu ne sera libéré qu'après la mise en place du cautionnement définitif.

8. Composition des offres :

L'offre présentée par le soumissionnaire comprendra les documents suivants dûment remplis:

1. la soumission, le bordereau des prix, l'engagement sur la qualité du service;
2. une garantie d'offre dûment établie et signée ;
3. les chiffres d'affaires certifiés des trois dernières années (2004, 2005 et 2006), sauf cas de société(s) nouvellement créée(s);
4. la liste des Marchés similaires exécutés au cours des cinq dernières années, sauf cas de société(s) nouvellement créée(s);
5. un document délivré par une banque acceptable pour l'Administration attestant que le candidat dispose de fonds propres suffisants ou qu'il bénéficiera d'un crédit pour l'exécution du Marché, s'il en est l'attributaire;
6. présenter et s'engager sur un calendrier de livraison;
7. fournir obligatoirement les prospectus et catalogues indiquant les spécifications techniques de la solution proposée. Les dits prospectus doivent confirmer obligatoirement les spécifications demandées dans le cahier des charges.
8. présenter une autorisation de (des) éditeur(s), dans le cas où le fournisseur n'est pas éditeur de la solution à livrer, incluant le certificat d'origine de la solution et les coordonnées de la personne signataire.
9. présenter le service après vente.
10. présenter les attestations suivantes, originales et en cours de validité à la date limite du dépôt des offres (uniquement pour les entreprises installées en Mauritanie ou y ayant travaillé) :
 - attestation des Impôts ;
 - attestation du Trésor Public ;
 - attestation de la Direction du Travail ;
 - attestation de la CNSS ;
 - attestation de la Direction du Contrôle des Banques
 - attestation d'inscription au registre du commerce
11. certificat de non faillite et de non liquidation judiciaire (pour les sociétés étrangères).
12. Attestation de pouvoir du mandataire.

9. Présentation des offres :

L'ensemble des pièces énumérées dans le paragraphe 8 sera, sous peine de nullité, remis en quatre exemplaires (un original et trois copies) comme suit :

9.1 Offre financière :

Une première enveloppe appelée «**Proposition financière**» fournira tous les détails des coûts, elle doit contenir les pièces suivantes :

- La soumission ;
- Devis estimatif et Quantitatif et bordereau des prix unitaires dûment remplis.

9.2 Offre technique :

Les pièces restantes seront contenues dans une deuxième enveloppe qui portera la mention «**Proposition technique**» et qui contiendra également les éléments suivants :

- Une description détaillée de la (des) société(s) soumissionnaire(s) et une présentation générale des références et expériences acquises dans le cadre des projets similaires;
- Des commentaires ou suggestions sur la solution technique demandée;
- Le cautionnement provisoire ;
- Les pièces du DAO paraphées et signées ;
- Les attestations ;
- L'offre de maintenance.

Les deux enveloppes seront placées dans une grande enveloppe. Cette dernière doit porter uniquement la mention suivante :

**ACQUISITION D'UNE SOLUTION D'OPTIMISATION ET DE SECURISATION DU
RESEAU, LOT
« A n'ouvrir qu'en séance publique de la CCM »**

10. Lieu et date de dépôt des offres :

Les offres seront remises à l'adresse suivante :

**SECRETARIAT GENERAL DU GOUVERNEMENT
COMMISSION CENTRALE DES MARCHES
BP : 184 - Nouakchott**

Au plus tard, le : MERCREDI 19 SEPTEMBRE 2007 à 10 H.

Les Offres doivent porter les indications suivantes :

- **Au centre :**
« **Monsieur le Président de la Commission Centrale des Marchés, Secrétariat Général du Gouvernement, BP. : 184 - Nouakchott** »

- **En haut et à gauche :**
« Appel d'Offres MFPMA pour l'Acquisition d'une Solution d'Optimisation et de Sécurisation du Réseau, lot ...».
- **En bas de page :**
« A n'ouvrir qu'en séance publique d'ouverture des plis ».

11. Suite à donner à l'appel d'offre :

L'Administration se réserve le droit de ne donner aucune suite ou ne donner qu'une suite partielle au présent appel d'offres, dans les conditions prévues par l'article 53 du décret 08-2002 du 28 Février 2002 portant Code des marchés publics.

12. Ouverture des plis :

L'ouverture des plis aura lieu en séance publique au siège de la Commission Centrale des Marchés à la date et l'heure indiquées dans l'avis d'appel d'offres. Elle s'effectuera en un seul temps pour les offres techniques et les offres financières.

13. Forme des soumissions :

Les soumissions devront être conformes sous peine de nullité au modèle de soumission (pièce n° 3) du présent dossier d'appel d'offres.

14. Régime fiscal et douanier :

Le marché qui découlera du présent appel d'offres s'exécutera en toutes taxes, droits de douanes compris.

15. Renseignement :

Tous les renseignements complémentaires pourront être obtenus auprès de l'adresse suivante :

Ministère de la Fonction Publique et de la Modernisation de l'Administration – (Direction Générale de l'Informatique de l'Administration) immeuble du Gouvernement BP : 184 – Nouakchott ; Téléphone ; (222) 525 54 30 ; Fax : (222) 529 79 07 ; E-mail : medkaber@modernisation.gov.mr.

16. Evaluation et comparaison des offres :

L'évaluation et comparaison des offres techniques des soumissionnaires déclarés recevables se feront sur la base des critères suivants :

1. Conformité de la solution proposée aux prescriptions techniques du DAO ;
2. Références techniques du (des) soumissionnaire(s) (expériences similaires) ;
3. Délai de livraison proposé ;
4. Proposition financière ;
5. Transfert de compétences.

L'Administration se réserve le droit de vérifier l'authenticité des pièces fournies, ou de procéder à des visites de lieu le cas échéant. Le marché sera attribué au soumissionnaire techniquement éligible et dont l'offre financière est la moins disante. Toutefois, les prix proposés doivent être raisonnables.

17. Acquisition du dossier d'appel d'offres :

Le Dossier d'Appel d'Offres pourra être acheté par les candidats, sur demande écrite au service mentionné ci-dessus et moyennant paiement d'un montant non remboursable de **10.000 Ouguiya**.

**Direction du Trésor et de la Comptabilité Publique,
Téléphone ; (222) 525 81 50**

SECTION III

3 CAHIERS DES PRESCRIPTIONS SPECIALES (CPS)

TABLE DES MATIERES

I. INDICATIONS GENERALES	13
1. OBJET DU CAHIER DES PRESCRIPTIONS SPECIALES.....	13
2. PRESCRIPTION DE L'APPEL D'OFFRES	13
3. MODE D'EXECUTION DES PRESTATIONS	13
4. RESPONSABILITES DE L'INTERVENANT	13
5. ADMINISTRATION CONTRACTANTE	13
6. CADRE D'EXECUTION DES PRESTATIONS.....	14
7. MONTANT DU MARCHE	14
8. LANGUE DU MARCHE.....	14
9. BASE DE REGLEMENT DU MARCHE	14
II. CLAUSES FINANCIERES.....	14
10. CAUTIONNEMENT DEFINITIF	14
11. NANTISSEMENT.....	15
12. AVANCES	15
13. PROCEDURES DE REGLEMENT	15
14. DOMICILIATION DES PAIEMENTS	15
15. PENALITES DE RETARD	16
16. DROIT D'ENREGISTREMENT	16
17. REMUNERATION POUR PRESTATIONS SUPPLEMENTAIRES.....	16
III. CLAUSES DIVERSES	16
18. DELAI DE LIVRAISON	16
19. LIEUX DE LIVRAISON	16
20. CONTESTATION ET LITIGES.....	17
21. RESILIATION DU MARCHE	17
22. TAXES ET DROITS DE DOUANES.....	17
23. RESPONSABILITE DU SOUMISSIONNAIRE.....	17
24. REPRESENTATION DU SOUMISSIONNAIRE	17
25. REFERENCE AUX TEXTES GENERAUX.....	18
26. PIECES CONTRACTUELLES DU MARCHE.....	18
27. APPROBATION DU MARCHE.....	18

I. INDICATIONS GENERALES

1. Objet du Cahier des Prescriptions Spéciales

Le présent cahier des prescriptions spéciales fixe les conditions particulières administratives et financières selon lesquelles seront exécutées les prestations liées à l'acquisition et la mise œuvre d'une solution d'optimisation et de sécurisation du réseau administratif.

2. Prescription de l'appel d'Offres

Les prestations objet du présent appel d'offres portent sur la fourniture, en deux (2) lots indépendants, et la mise en œuvre d'une solution d'optimisation et de sécurisation du réseau administratif.

- **Lot1 : Protection résidente, stratégie de sécurité et optimisation de la configuration (antivirus et pare feu physique).**
- **Lot 2 : Filtrage du contenu et optimisation de la navigation (antispams, antivirus, proxy et proxy cache)**

Les prestations seront réalisées selon les prescriptions des documents suivants :

- Devis estimatif et Quantitatif et bordereau des prix unitaires ; et
- Les spécifications techniques de la solution.

3. Mode d'exécution des prestations

Les prestations constituant l'appel d'offres seront réalisées en deux lots séparés par un ou plusieurs soumissionnaires ou groupements. Dans ce cas, le groupement désignera un mandataire commun qui sera reconnu par l'Administration comme étant le seul et unique représentant du groupement.

Le soumissionnaire aura la faculté de sous-traiter (une partie ou la totalité) des prestations nécessitant une spécialisation ne relevant pas du domaine de ses actions.

Il est stipulé que le (les) sous-traitant(s) agréé(s) ne pourront obtenir directement de l'administration contractante le règlement des services dont ils auront assuré l'exécution; ils seront rémunérés obligatoirement par le titulaire du marché.

4. Responsabilités de l'intervenant

Le soumissionnaire supportera seul et entièrement les conséquences directes (financières ou pénales lors de l'exécution du marché) qui pourraient résulter de l'inobservation des règlements et usages généraux et particuliers en la matière par les sous-traitants.

5. Administration Contractante

Le(s) marché(s) sera (ont) conclu(s) par le Ministère de la Fonction Publique et de la Modernisation de l'Administration, agissant au nom et pour le compte de l'Etat mauritanien.

La Direction Général de l'Informatique de l'administration est chargée de la gestion du (des) marché(s).

6. Cadre d'exécution des prestations

La description détaillée des prestations du soumissionnaire dans le cadre du présent marché est définie dans les sections « **Devis estimatif et Quantitatif et bordereau des prix unitaires** » et « **Spécifications Techniques** » qui tiennent lieu de termes de référence du soumissionnaire.

7. Montant du Marché

Le montant du marché découlera de la proposition financière, en toutes taxes, établie par le soumissionnaire telle qu'elle résulte de sa soumission en référence au cadre du devis quantitatif et estimatif et en application des prix du bordereau des prix unitaires, après vérifications et réajustements éventuels de ces prix.

Le marché sera à prix global et forfaitaire non révisable et non actualisable.

8. Langue du Marché

Toutes les correspondances concernant l'administration et les documents de soumission, relatifs au(x) marché(s) qui découlera (ont) du présent appel d'offres seront rédigés en langue française.

9. Base de règlement du Marché

Le marché qui aura lieu suite au présent appel d'offres sera passé dans les conditions suivantes :

1. Il est précisé que les prix remis par le soumissionnaire couvrent toutes les charges et dépenses de toutes sortes, qu'il aura à effectuer pour la réalisation des prestations demandées (fourniture, installation sur les sites de destination, essai et mise en marche de la solution et le transfert des compétences).
2. Les prix tiennent compte également des aléas et sujétions des prestations envisagées, dont le soumissionnaire est censé connaître parfaitement la nature et les difficultés afférentes à leur mise en œuvre.
3. Les prix du marché sont fermes, non actualisables et non révisables pendant toute la durée de l'exécution des prestations.

II. CLAUSES FINANCIERES

10. Cautionnement définitif

Le soumissionnaire retenu devra fournir, dans un délai de 5 jours après la notification du marché et avant la première demande de paiement, un cautionnement définitif égal à 5% (cinq pour cent) du montant du marché. Il peut être remplacé par une caution personnelle et solidaire, inconditionnelle et irrévocable fournie par un établissement bancaire agréé et établi en Mauritanie au profit et pour le compte du Ministère de la Fonction Publique et de la Modernisation

de l'Administration et payable à la première demande. Le cautionnement sera libéré ou la caution bancaire sera restituée dans un délai de 60 jours suivant la réception définitive des prestations.

11. Nantissement

En vue du nantissement éventuel du marché, dans les conditions fixées par l'article 97 du décret N° 08-2002 du 12 février 2002, portant Code des marchés publics, qui stipule que :

- § L'administration chargée de la certification des sommes dues en application des termes du marché et d'établir les ordres de paiement, sera le Ministère de la fonction publique et de la Modernisation de l'Administration.;
- § Le fonctionnaire chargé de fournir au titulaire du marché toutes les informations et données nécessaires à l'exécution des prestations est le Secrétaire Général du Ministère de la fonction publique et de la Modernisation de l'Administration.

12. Avances

Le titulaire du marché pourra bénéficier d'une avance de démarrage de 30% (trente pour cent) du montant du marché, conformément aux dispositions de l'article 84 du décret N° 08-2002 du 12 février 2002. Cette avance doit être cautionnée à 100% par un établissement bancaire établi et agréé en Mauritanie (article 87 du décret N° 08-02 du 12 février 2002). Ce cautionnement doit être inconditionnel, irrévocable et payable à la première demande. Il doit être établi au nom et pour le compte du Ministère de la Fonction Publique et de la Modernisation de l'Administration.

13. Procédures de règlement

Le soumissionnaire sera payé de la manière suivante :

- Une avance de 30% acompte, dès la notification du marché, conformément aux dispositions du paragraphe 12 ci-dessus.
- 70% à la réception provisoire des fournitures, sanctionnée par un procès-verbal de réception.

Les demandes de paiement doivent être libellées en UM (ouguiya) et l'exécution effectuée conformément à la répartition des montants définis dans le marché.

14. Domiciliation des paiements

Les paiements seront effectués par virement bancaire dans un compte ouvert au nom du soumissionnaire dans un établissement bancaire domicilié en Mauritanie.

15. Pénalités de retard

En cas de retard par rapport au délai fixé à la soumission, le soumissionnaire sera passible de pénalités. Le nombre de jours de retard sera le nombre de jours francs, samedi, dimanche et jours fériés compris.

Le montant des pénalités est fixé à 1/2.000ème du montant du marché par jour calendaire de retard (samedi, dimanche et jours fériés compris).

Les pénalités courent de plein droit par la seule échéance du terme et sans qu'il soit besoin de mise en demeure ni préavis. L'application des pénalités ne saurait en aucun cas faire obstacle à l'application des mesures coercitives prévues par la réglementation en vigueur, en particulier en cas de résiliation du marché.

L'administration pourra revendiquer à la fois le paiement des pénalités pour retard et la confiscation du cautionnement définitif à titre de dommage et intérêt sans préjudice pour tout autre recours.

Le montant global des pénalités de retard est plafonné à 7% du montant global du marché.

16. Droit d'enregistrement

Les frais d'enregistrement et timbres du présent Marché, seront à la charge de l'adjudicataire et effectués par ses soins.

17. Rémunération pour prestations supplémentaires

Les opérations supplémentaires demandées par ordre de service de l'Administration seront réglées sur la base du bordereau des prix unitaires établi par le soumissionnaire dans sa soumission, dans les limites prévues par la réglementation (décret 08-02 du 12/2/2002) ou à défaut par entente préalable entre le soumissionnaire et l'Administration.

III. CLAUSES DIVERSES

18. Délai de livraison

Les délais seront appliqués conformément aux dispositions du paragraphe 3 du Cahier des Conditions Générales du dossier d'appel d'offres et prendront effet dès la notification de l'ordre de service invitant le soumissionnaire retenu à démarrer les prestations.

19. Lieux de livraison

Les fournitures seront livrées, installées, essayées et mises en marche à Nouakchott, dans les sites qui seront spécifiés à cet effet par le Ministère de la fonction publique et de la Modernisation de l'Administration.

20. Contestation et litiges

Si, au cours de l'exécution du marché, des contestations ou des litiges surgissent entre l'administration et le soumissionnaire et à défaut d'un règlement à l'amiable, il en sera référé aux juridictions mauritaniennes compétentes en la matière.

21. Résiliation du marché

A défaut par le soumissionnaire de remplir ses obligations contractuelles, il sera procédé à l'application des dispositions du décret N° 08-2002 du 12 février 2002, portant Code des Marchés publics.

22. Taxes et droits de douanes

Ce marché sera exécuté en toutes taxes, droits de douanes compris.

23. Responsabilité du soumissionnaire

Le soumissionnaire est réputé connaître les conditions et les difficultés liées à l'exécution des prestations objet du présent appel, les risques et sujétions qu'il pourra entraîner. A ce titre, il ne pourra se prévaloir d'aucune omission, erreur ou imprécision du dossier d'appel d'offres.

Le soumissionnaire sera seul et pleinement responsable des accidents et dommages de toutes natures qui surviendraient aux tiers, à son personnel et à son matériel.

Il veillera, le cas échéant, à mettre à la disposition de ses agents tous les moyens nécessaires à la bonne exécution de leurs tâches.

Le prestataire devra être compétent sur l'ensemble des solutions qu'il propose. Il doit disposer obligatoirement d'un personnel formé sur les technologies proposées parce qu'il ne sera pas toléré aucune interruption de service sur le réseau.

Le prestataire devra être donc certifié sur la technologie qu'il compte proposer et fournir au moins deux personnes formées et certifiées sur la solution. Les documents prouvant les certifications devront être fournies obligatoirement dans la réponse.

Le soumissionnaire fournira les garanties nécessaires et le support nécessaire après installation pour une continuité totale du service.

Le soumissionnaire indiquera les procédures de mises à jour des équipements et des logiciels.

Le soumissionnaire indiquera les délais de garantie du matériel et des logiciels. S'il nécessite des extensions de garantie ou de support technique, il devra clairement l'indiquer dans son offre.

24. Représentation du soumissionnaire

Dès la notification du marché, le soumissionnaire indiquera à l'administration le nom de la personne désignée comme étant son représentant et qui sera autorisée à recevoir les instructions relatives au marché. Il devra faire connaître le lieu d'élection de son domicile à Nouakchott en vue de recevoir toutes les notifications se rapportant au marché.

25. Référence aux textes généraux

Le soumissionnaire restera soumis aux dispositions du décret portant Code des marchés publics passés au nom et pour le compte de l'Etat, à savoir le décret N° 08-2002 du 12 février 2002.

26. Pièces contractuelles du marché

Les pièces contractuelles qui constitueront le marché et qui découlent du présent appel d'offres sont dans l'ordre :

1. les offres technique et financière qui comprennent :
 - la soumission ;
 - le devis estimatif et Quantitatif et bordereau des prix unitaires ;
 - les Spécifications techniques;
 - les éventuels PV de mise au point ;
 - la proposition financière ;
 - la proposition technique.
2. le Cahier des Prescriptions Spéciales (CPS) ;
3. le Cahier des Clauses Administratives Générales (CCAG) ;
4. le Cahier des Prescriptions Techniques (CPT) ;
5. Le cautionnement.

27. Approbation du marché

Le marché ne deviendra exécutoire qu'après son approbation par Monsieur le Ministre de la Fonction Publique et de la Modernisation de l'Administration.

SECTION IV

4 MODELE DE SOUMISSION (MS)

MODELE DE SOUMISSION
(à établir sur papier libre)

Je (nous), soussigné (nom, prénom), domicilié à (adresse complète), BP, Tél. :, Fax :, inscrit au registre de commerce de la chambre de commerce sous le numéro et titulaire de la carte Import/Export n° du

Après avoir pris connaissance des pièces contenues dans le dossier d'appel d'offres relatif à «**l'acquisition d'une solution d'optimisation et de sécurisation du réseau, lot ...** », me soumet et m'engage (nous engageons) à livrer les prestations conformément aux prescriptions des différentes pièces du dossier d'appel d'offres, moyennant le montant et le délai de livraison qui suivent :

- Montant (en TT) : -----
(en chiffres et en lettres)
- Délai: -----
(en mois)

Je déclare (nous déclarons) avoir apprécié sous ma (notre) responsabilité la nature et la difficulté des travaux à réaliser.

L'exécution des parties suivantes des prestations sera confiée à des sous-traitants, sous réserve de l'autorisation de l'administration :

En cas d'agrément de la présente soumission, la constitution du cautionnement définitif prescrit ou l'engagement de la caution solidaire en tenant lieu, sera effectué(e) dans les délais et conditions prévus au dossier d'appel d'offres.

Je me considère (nous nous considérons) engagé(s) par la présente soumission pour une période de 90 jours à compter de la date limite de dépôt des offres.

Je demande (nous demandons) à ce que les sommes dues par l'administration me (nous) soient payées au compte : ----- (numéro et Agence).

Fait à (lieu et date)

Le(s) soumissionnaire(s)

Cachet(s) et Signature(s).

SECTION V

5 MODELE DE MARCHE (MM)

TABLE DES MATIERES

1. OBJET DU MARCHE	24
2. PIECES CONSTITUTIVES DU MARCHE	24
3. PRESTATIONS A REALISER PAR LE FOURNISSEUR	24
4. TEXTES REGLEMENTAIRES	24
5. MONTANT DU MARCHE	25
6. DELAI DE LIVRAISON :	25
7. LIEUX DE LIVRAISON :	25
8. PENALITES DE RETARD ET MISE EN DEMEURE	25
9. AVANCE DE DEMARRAGE.....	25
10. CAUTIONNEMENT DEFINITIF	26
11. MODE DE REGLEMENT DES TRAVAUX.....	26
12. MODALITES DE PAIEMENT.....	26
13. PRESCRIPTIONS FISCALES ET DOUANIERES	26
14. DOMICILE DE L'ATTRIBUTAIRE DU MARCHE	26
15. NANTISSEMENT.....	26
16. ACTUALISATION ET REVISION DES PRIX	27
17. RESILIATION ET LITIGES	27
18. RECEPTION PROVISoire	27
19. RECEPTION DEFINITIVE	27
20. ENREGISTREMENT ET TIMBRES	27
21. APPROBATION DU MARCHE	27



République Islamique de Mauritanie

Honneur – Fraternité - Justice

Ministère de la fonction publique et de la modernisation de l'administration

Marché N° : ----- /CCM/MFPMA/DGIA/07

Objet : FOURNITURE ET INSTALLATION D'UNE SOLUTION
D'OPTIMISATION ET DE SECURISATION DU RESEAU ,LOT

Adjudicataire :

Montant :

Délai d'Exécution :

Financement : BUDGET ETAT - 2007

Adjugé le :

Approuvé le :

Notifié le :

VISAS du Président de la CCM

ENTRE:

Le Ministère de la Fonction Publique et de la Modernisation de l'Administration, agissant au nom et pour le compte de l'Etat mauritanien, désigné dans le présent Marché par le terme «Administration»

ET:

Le Directeur général de....., agissant au nom et pour le compte de, désigné dans le présent Marché par le terme «Fournisseur»

IL A ETE CONVENU CE QUI SUIT**1. Objet du Marché**

Le présent Marché a pour objet la fourniture et l'installation d'une solution d'optimisation et de sécurisation du réseau administratif.

2. Pièces constitutives du Marché

Le Marché est constitué des pièces suivantes dans l'ordre de priorité :

- 1- Le présent contrat ;
- 2- La soumission du fournisseur et ses annexes ;
- 3- Le cahier des prescriptions techniques CPT du DAO ;
- 4- Les Données particulières de l'appel d'offres ;
- 5- Le cahier des Clauses Administratives Spéciales du DAO ;
- 6- Le cautionnement définitif.

3. Droits de propriétés

Les solutions et licences livrées seront la propriété de l'Etat Mauritanien

4. Prestations à réaliser par le fournisseur

La description des prestations à réaliser par le fournisseur est donnée dans les Spécifications techniques (CPT du DAO) qui fait partie intégrante du présent marché. Toute fois, le titulaire du marché exécutera ces prestations selon les meilleures pratiques professionnelles en matière de fourniture des solutions de sécurité et d'optimisation des réseaux informatiques.

5. Assurances

Le titulaire du marché contractera une assurance de responsabilité civile couvrant les dommages corporels et matériels qui pourraient être consécutifs à son intervention dans le cadre de la réalisation des prestations.

6. Textes réglementaires

Le présent Marché est passé en vertu des dispositions du décret N° 08-2002 du 12 février 2002, portant Code des marchés publics.

7. Montant du Marché

Le montant du Marché tel qu'il résulte de la soumission du fournisseur, en toutes taxes s'élève à : UM.

8. Garantie

Le soumissionnaire garantit la conformité de la solution aux spécifications techniques décrites dans son offre, son installation convenable et conforme au code des conditions minima d'exécution et aux règles de l'art ainsi que le bon état de leur fonctionnement.

Le titulaire du marché exécutera à sa charge toutes les mises au point, toutes les réparations et tous les remplacements de logiciels nécessaires au maintien en bon état de fonctionnement et dans le respect des qualités de service demandés durant la période de garantie.

Durant la période de garantie, le titulaire interviendra sur les lieux où seront installés les logiciels livrés ; en particulier, il assurera, sous peine de pénalités et à ses frais, une maintenance préventive (mensuelle, trimestrielle) pendant cette période.

La durée de garantie prend effet à partir de la date de la signature de la réception provisoire.

9. Délai de livraison

Le délai de livraison ne doit pas excéder 30 jours sous peine de nullité. Ce délai commence à courir dès la notification de l'ordre de service de démarrage des prestations

10. Lieux de livraison :

Les logiciels seront livrés et installés à Nouakchott, dans les sites qui seront indiqués à cet effet par le Ministère de la Fonction Publique et de la Modernisation de l'Administration.

11. Pénalités de retard et mise en demeure

A défaut d'avoir terminé les présents travaux dans le délai contractuel, une pénalité égale à **UN DEUX MILLIEME (1/2000ème) du montant du Marché par jour calendaire de retard** sera appliquée au fournisseur, sans préjuger des mesures coercitives prévues par la réglementation en vigueur en Mauritanie qui pourraient être prises par l'Administration (Articles 118 du code des marchés publics).

Le montant sera retenu sur les sommes dues au fournisseur. Le montant de ces pénalités est plafonné à 7% du montant du Marché.

Il est précisé qu'aucune prime ne serait accordée au fournisseur, dans le cas où les travaux seraient terminés avant l'échéance fixée dans le présent contrat.

12. Avance de démarrage

Le fournisseur pourra solliciter, conformément aux articles 84, 86 et 87 du décret N° 08-02 du 12 février 2002, l'octroi d'avance de démarrage. Le montant de cette avance est fixé à **(30 %)** du montant du Marché.

Le versement de l'avance sera effectué sur présentation d'une demande expresse du fournisseur, accompagnée d'un cautionnement bancaire garantissant à 100% le remboursement de cette avance.

La caution doit être délivrée par un établissement bancaire établi ou agréé en Mauritanie. Elle doit être inconditionnelle, irrévocable et payable à la première demande.

13. Cautionnement définitif

Le cautionnement définitif, ou la caution bancaire qui le remplace doit être égal à **5%** (cinq pour cent) du Marché. Il devra être constitué et présenté avant la première demande de paiement.

Ce cautionnement doit être délivré par un établissement bancaire établi ou agréé en Mauritanie. Il doit être inconditionnel, irrévocable et payable à la première demande.

Ce cautionnement sera restitué ou la caution bancaire libérée à la suite d'une mainlevée délivrée dans un délai maximum de 60 jours suivant la réception définitive des fournitures.

14. Mode de règlement des prestations

Le fournisseur sera payé de la manière suivante :

- 30 % avance de démarrage ;
- 70 % à la présentation du PV de réception provisoire des fournitures.

15. Modalités de paiement

L'Administration se libérera des sommes dues par elle par crédit du compte N° : ..., ouvert au nom du fournisseur à

16. Prescriptions fiscales et douanières

Le Marché s'exécutera en toutes taxes, droits de douanes compris.

17. Domicile de l'attributaire du Marché

Le fournisseur est tenu de faire connaître le lieu de son domicile pendant la durée d'exécution des prestations à l'Administration. Faute par lui d'avoir satisfait à cette obligation dans un délai de 30 (trente) jours à dater de la notification du Marché, toutes les notifications qui se rapportent au fournisseur seront valables lorsqu'elles ont été faites à son siège.

18. Nantissement

En vue du nantissement éventuel du marché, dans les conditions fixées par le décret N° 08-02 du 12 février 2002, article 97, il est stipulé que :

- § L'administration chargée de la certification des sommes dues en application des termes du marché et d'établir les ordres de paiement, sera le Ministère de la fonction publique et de la modernisation de l'administration;

- § Le fonctionnaire chargé de fournir au titulaire du marché toutes les informations et données nécessaires à l'exécution des prestations est le Secrétaire Général du Ministère de la fonction publique et de la modernisation de l'administration.

19. Actualisation et révision des prix

Les prix de ce Marché sont fermes, non actualisables et non révisables.

20. Résiliation et litiges

La résiliation du Marché aura lieu dans les cas visés dans les articles 128 à 131 du décret 08-02 du 12 février 2002.

Faute de règlement à l'amiable, les litiges seront tranchés par la juridiction mauritanienne compétente.

21. Réception provisoire

La réception provisoire sera prononcée à l'issue des essais ou contrôles nécessaires pour constater la conformité des fournitures aux spécifications décrites dans les différents composants du DAO. Elle sera effectuée, en présence du Fournisseur, par une commission composée des représentants :

- De la Commission Centrale des Marchés ;
- Du Ministère de la Fonction Publique et de la Modernisation de l'Administration;
- De la Direction générale du budget ;
- Du Représentant de la Société exécutant le projet ou marché.

22. Réception définitive

La réception définitive sera prononcée par la même commission que celle désignée à l'article 21 à l'expiration d'un délai de garantie d'un an et selon les critères exigés par la réception provisoire.

23. Enregistrement et timbres

Les formalités et les coûts d'enregistrement et timbres sont à la charge du fournisseur.

24. Approbation du Marché

Le Marché ne sera exécutoire qu'après son approbation par Monsieur le ministre de la fonction publique et de la modernisation de l'administration.

Fait à Nouakchott, le

Le Fournisseur

**Le Ministre de la Fonction Publique et de
La Modernisation de l'Administration**

SECTION VI

6 DEVIS ESTIMATIF ET QUANTITATIF ET BORDEREAU DES PRIX UNITAIRES

Devis estimatif et Quantitatif				
Numéro	Désignation	Quantité	Prix Unitaire	Prix Total
1	Antivirus pour postes du travail	1500		
2	Antivirus pour serveurs	100		
3	Firewall physique	2		
4	Service mise en place Stratégie de sécurité	1		
5	Service Optimisation de la configuration Existante	1		
6	Service filtrage Virus/Spam pour les emails en amont	1		
7	Service de Filtrage du contenu en amont	1		
8	Service (Appliance) filtrage du contenu et optimisation de la navigation	1		

Bordereau des prix unitaires			
Numéro	Désignation	Prix Unitaire en Chiffres	Prix Unitaire en Lettres
1	Antivirus pour postes du travail		
2	Antivirus pour serveurs		
3	Firewall physique		
4	Service mise en place Stratégie de sécurité		
5	Service Optimisation de la configuration Existante		
6	Service filtrage Virus/Spam pour les emails en amont		
7	Service de Filtrage du contenu en amont		
8	Service (Appliance) filtrage du contenu et optimisation de la navigation		

SECTION VII

7 SPECIFICATIONS TECHNIQUES

7.1 Contexte

Dans le cadre de son plan d'action de 2007, le Ministère de la Fonction Publique et de la Modernisation de l'Administration, à travers la Direction Générale de l'Informatique de l'Administration envisage d'acquérir une solution permettant de renforcer l'efficacité de l'Intranet du Gouvernement sur les deux plans suivants :

- Sécurité contre les contenus et courriers indésirables. Il s'agit de protéger le réseau contre les risques liés à l'utilisation des ressources externes, notamment l'Internet et les supports externes.
- Performance pour l'optimisation de la bande passante afin de rationaliser l'utilisation de cette ressource rare, coûteuse et critique.

A cet effet, le Ministère lance la présente consultation pour le choix d'un fournisseur en mesure d'offrir une solution répondant aux besoins ci-dessus.

Le présent cahier des charges décrit l'objectif visé et les caractéristiques techniques des solutions.

7.2 L'Objectif visé :

Il s'agit d'une solution de deux lots :

LOT 1 : Protection résidente, stratégie de sécurité et optimisation de la configuration

- ☞ Une solution antivirale pour les serveurs et les postes de travail du parc informatique de l'administration qui incorpore un module pour le filtrage de la messagerie ; ce module est destiné principalement au filtrage des messages échangés en interne.
- ☞ Une solution de pare feu physique permettant de protéger l'Intranet contre les accès externes non autorisés : détection d'intrusion, service d'accès à distance sécurisé et protection des services publiés.
- ☞ Optimisation et sécurisation des configurations des équipements réseaux existants avec la mise en place des outils d'audit et de monitoring.
- ☞ Mise en place d'une politique de sécurité spécifique

LOT 2 : Filtrage du contenu et optimisation de la navigation

- ☞ Un service hébergé/managé pour le filtrage de la messagerie et du trafic Web entrant et sortant contre tout contenu nuisible (courriers indésirables, virus et autre contenu/codes malveillants). Le prestataire doit disposer de centres de traitement hautement disponibles pour le filtrage de tous les flux échangés entre les utilisateurs de l'Intranet et le monde extérieur.
- ☞ Une solution intégrée (appliance) d'optimisation de la bande passante offrant au moins les fonctionnalités de Proxy pour le contrôle d'accès Web et de Proxy cache.

7.3 Descriptions techniques

7.3.1 La solution antivirale

Le logiciel d'antivirus devra disposer des fonctionnalités suivantes:

- ☞ Administration centralisée
- ☞ Logiciel évolutif (possibilité de rajouter de licences supplémentaires)
- ☞ verrouillage des paramètres des clients
- ☞ Possibilité d'installer l'antivirus client en « standalone » (sans utiliser la console d'administration)
- ☞ Analyse aussi bien les messages entrants que sortants en temps réel à partir du serveur
- ☞ Mises à jour automatiques des définitions de virus au moins une fois par jour
- ☞ Compatibilité Windows 2000/XP pour la version cliente et Windows 2000/2003 Serveur pour la version serveur
- ☞ Permet une sélection des fichiers/dossier à scanner
- ☞ Permet de scanner les emails à l'arrivée (cas de PC/Portable isolé)
- ☞ Permet de scanner les supports amovibles
- ☞ Permet de scanner les archives
- ☞ Permet de planifier l'analyse
- ☞ Permet une protection en temps réel
- ☞ Permet de mettre les fichiers infectés en quarantaine et de les détruire ou de les désinfecter
- ☞ Permet le choix manuel (détruire, mettre en quarantaine ou désinfecter les fichiers)
- ☞ Possède la fonctionnalité de récupération après panne (disaster recovery)

Ces données doivent être vérifiées dans les tests de sécurité des laboratoires et organisations (par exemple SC Magazine)

7.3.2 Pare feu physique

Le Ministère de la Fonction Publique et de la Modernisation souhaite mettre à niveau les équipements de la sécurité d'accès avec la mise en place des dernières générations de pare-feu matériel redondant. Les équipements seront mis en fail-over et devront intégrer :

- Les technologies les plus récentes des serveurs de sécurité
- Fonctionnalité de VPN et de accès à distance SSL
- Traitement et politique de services
- Débit du pare-feu supérieur ou égal à 450 Mbits/s
- Débit de protection simultanée contre les menaces (pare-feu + services IPS) supérieur ou égal à 300Mbits/s
- Débit du VPN supérieur ou égal à 200 Mbits/s
- Connexions supérieures à 200 000
- Homologues VPN IPSec 750
- Niveaux de licence des homologues VPN SSL jusqu'à 750
- Contextes de sécurité jusqu'à 20

- Interfaces: 4 ports Gigabit Ethernet et 1 port Fast Ethernet
- Interfaces virtuelles (VLAN) : 100
- Évolutivité Équilibrage: de charge et mise en grappe des VPN
- Haute disponibilité: Actif/actif, actif/veille

7.3.3 Optimisation de la configuration

Le MFPMA, par la présente expertise souhaite sélectionner un bureau ayant une expérience avérée pour vérifier les configurations des équipements actifs du réseau et proposer des solutions pour optimiser et renforcer davantage la sécurité du réseau.

Cette expertise devra comprendre, sans se limiter aux aspects suivants :

- La vérification et l'optimisation de la configuration de tous les équipements actifs du réseau et notamment :
 - La configuration de l'IDS (intrusion detection system);
 - La configuration des pare-feu (Firewall);
 - La configuration du routage ;
- La mise en place des outils d'Audit du réseau et de monitoring issus des logiciels libres

7.3.4 Stratégie de sécurité

Cette politique de sécurité devra comprendre, sans se limiter aux aspects suivants :

- Comment assurer une meilleure confidentialité des données
- Comment garantir une meilleure disponibilité des données
- Comment préserver l'intégrité des données

Cette politique de sécurité globale sera accompagnée par la mise en place d'une charte de sécurité ou charte de bonne conduite que chaque utilisateur s'engagera à respecter ses dispositions pour garantir un niveau de sécurité élevé

7.3.5 Service de sécurité Hébergé / managé

7.3.5.1 La messagerie

Le service devra :

- ☞ Contenir des modules anti-Spam, Anti-Virus et analyse de contenu pour la protection des flux de messagerie.
- ☞ Disposer d'une infrastructure avec au moins 10 centres de traitement dans le monde : disponibilité de 99% et temps de traitement inférieur à 60 secondes pour les messages standards (de taille inférieur à 2Mo) ;
- ☞ Inclure un service de récupération après panne (Disaster Recovery),
- ☞ Déployer au moins 4 moteurs d'anti-virus dont un permettant l'analyse comportementale afin de lutter contre les virus inconnus (les virus connus étant traités par les moteurs standards) – technologie en coupure – obligation contractuelle de bloquer 99,9% des virus, un moteur anti-spam performant (obligation contractuelle de bloquer 95% des spam, une

analyse de contenu afin d'obtenir une politique de filtrage selon la taille des messages, leurs extensions et des termes lexicaux).

- ☛ Fournir des rapports de quarantaine pour tous les utilisateurs
- ☛ Support en Français
- ☛ Solution évolutive (possibilité de rajouter de licences supplémentaires)

La description détaillée de ce de service est indiquée dans la partie ci-dessous intitulée : **7.3.7.1**

LA QUALITE DES SERVICES DEMANDES - FILTRAGE MAIL

7.3.5.2 La navigation web

7.3.6 L'optimisation de la bande passante

Il s'agit d'une solution intégrée :

- ☛ Permettant de disposer en local d'un moyen de filtrage des URL (plus de 20 millions d'URL référencés),
- ☛ Etre obligatoirement sous forme d'une Appliance (solution intégrée) pour limiter le temps d'exploitation avec les fonctionnalités intégrées de proxy et proxy cache.

La description détaillée de ce de service est indiquée dans la partie ci-dessous intitulée : **7.3.7.2**

LA QUALITE DES SERVICES DEMANDES - FILTRAGE WEB

7.3.7 LA QUALITE DES SERVICES DEMANDES :

7.3.7.1 FILTRAGE MAIL

MFPMA FILTRAGE MAIL - CAHIER DES CHARGES	REPONSE [FOURNISSEUR]
<p>1 Objectifs</p> <p>l'Administration mauritanienne souhaite mettre en place une solution de filtrage hébergée des mails entrants et sortants (filtrage Mail). Cette solution sera proposée à l'administration mauritanienne..</p> <p>La solution devra :</p>	

<ul style="list-style-type: none"> - répondre aux besoins fonctionnels décrits dans ce document - s'adapter à l'architecture technique existante de l'Administration - ne pas nécessiter d'investissement (licence, matériel) et permettre une facturation par utilisateur 	
<p>Le "fournisseur" désigne le fournisseur de service.</p> <p>Le "Groupe" désigne l'ensemble des entités de l'Administration, site central et départements ministériels.</p> <p>Un "nom de domaine" désigne un domaine DNS publique déposé par l'administration (exemples : mauritania.mr, modernisation.gov.mr, etc.).</p>	
<h2 style="color: blue;">2 Besoins fonctionnels</h2>	
<h3 style="color: purple;">2.1 Filtrage - généralités</h3>	
<p>L'ensemble des règles et niveau de filtrage est paramétrable (dont activation/désactivation) pour les mails entrants comme pour les mails sortants :</p>	
<ul style="list-style-type: none"> - par utilisateur 	
<ul style="list-style-type: none"> - par groupe d'utilisateurs 	
<p>Pour chaque filtre, l'action sur les mails détectés positifs doit être paramétrable par groupe d'utilisateurs :</p>	
<ul style="list-style-type: none"> - suppression 	
<ul style="list-style-type: none"> - mise en quarantaine utilisateur ou administrateur 	
<ul style="list-style-type: none"> -détection et modification du sujet (flag) avant distribution 	
<ul style="list-style-type: none"> - nettoyage du corps du mail avant distribution 	
<p>De même, l'administrateur peut définir et personnaliser les notifications à l'expéditeur et/ou au destinataire.</p>	
<h3 style="color: purple;">2.2 Filtrage des mails entrants</h3>	
<p>Les vérifications doivent respecter l'enchaînement suivant : caractéristiques, antivirus et pièces jointes, antispam, contenu</p>	
<p>Filtre sur les caractéristiques du mail : rejet du mail avec notification expéditeur</p>	
<ul style="list-style-type: none"> - destinataire inconnu 	
<p>Filtre antivirus : mise en quarantaine administrateur des mails détectés</p>	
<ul style="list-style-type: none"> - plusieurs moteurs par signature et heuristique, et spyware dans les pièces jointes. Préciser le nombre de moteurs et les éditeurs. 	
<ul style="list-style-type: none"> - fichier joint chiffré (non analysables) : exemple archive ZIP protégée par mot de passe 	
<ul style="list-style-type: none"> - filtre anti-hameçonnage (phishing) : suppression des mails détectés 	
<p>Filtre sur les pièces jointes : distribution du mail avec suppression du fichier concerné, remplacé par un message texte personnalisable par l'Administration</p>	
<ul style="list-style-type: none"> - fichier joint exécutable et script 	

- fichier joint chiffré (non analysables, ex. archive protégée)	
Filter antispam : mise en quarantaine utilisateur des mails détectés	
- liste noire dynamique des relais de spam, dont PC zombies (adresses IP dynamiques)	
- analyse du contenu : lexical ou combiné : à préciser la technologie mise en œuvre	
- niveau de filtrage antispam configurable par groupe d'utilisateurs	
- liste blanche définie par l'administrateur (expéditeur, relais, nom de domaine) par groupe d'utilisateurs et Groupe	
- les listes blanches désactivent uniquement l'antispam, les autres filtres demeurent	
Filter sur le contenu :	
- liste de mots clés dans un mail, paramétrable par groupe d'utilisateurs : suppression ou mise en quarantaine administrateur ou détection avec notification administrateur	
- type de fichiers joint paramétrable par groupe d'utilisateur : distribution du mail avec suppression du fichier concerné, remplacé par un message texte personnalisable par l'administration	
Possibilité de désactiver le filtrage pour certaines adresses externes (destinataire) et internes (expéditeur l'administration).	
2.3 Filtrage des mails sortants	
Les vérifications doivent respecter l'enchaînement suivant : antivirus et pièces jointes, antispam	
- filtre antivirus : mise en quarantaine administrateur des mails détectés, avec notification administrateur	
- plusieurs moteurs par signature et heuristique, et spyware dans les pièces jointes. Préciser le nombre de moteurs et les éditeurs.	
- paramétrable : fichier joint chiffré (non analysables) : exemple archive ZIP protégée par mot de passe	
- détection de spam : l'Administration souhaite se prémunir de spams générés en interne intentionnellement. Quelle solution peut être proposée ? Par exemple, détection sur la fréquence d'envoi d'un même mail dans un délai réduit depuis une même adresse.	
Possibilité de désactiver le filtrage pour certaines adresses externes (destinataire) et internes (expéditeur l'Administration).	
2.4 Interface et fonctionnalités utilisateur	
Chaque utilisateur doit disposer d'un espace utilisateur en ligne afin de :	

- accéder à sa zone de quarantaine et consulter les mails en quarantaine	
- débloquer des mails en quarantaine détectés comme spam	
- modifier ses règles de filtrage : liste noire personnelle	
- modifier ses règles de filtrage : liste blanche personnelle	
L'interface utilisateur doit avoir une ergonomie simple et accessible à tout type de profil utilisateur	
L'interface utilisateur et l'aide doivent être disponibles en français.	
2.5 Interface et fonctionnalités administrateur	
Authentification sur le portail Web :	
- Pour les administrateurs : authentification mot de passe (verrouillage au-delà de 3 tentatives), avec filtrage IP	
- Affichage de la date et l'heure de la dernière connexion (avec adresse IP pour les administrateurs)	
L'administration - règles, quarantaine, reporting – peut se déléguer à des administrateurs locaux par nom de domaine. Cette délégation d'administration sera mise en place pour les filiales souhaitant être autonomes, avec une vue restreinte sur ses utilisateurs.	
L'administrateur doit avoir accès à l'ensemble des propriétés des mails entrants/sortants (filtrés ou pas) et données de connexion associées sur une semaine au minimum : en-tête SMTP, adresses IP de l'expéditeur et des relais.	
Une alerte mail ou SMS est envoyée aux administrateurs en cas de dysfonctionnement ou d'interruption du service	
L'interface d'administration, l'aide et la documentation doivent être disponibles en français, paramétrable selon l'administrateur.	
2.6 Reporting	
Reporting utilisateur : possibilité d'envoi de rapport personnalisé avec le nombre de mails bloqués et leur nature, à périodicité paramétrable par l'administrateur.	
Reporting administrateur : pour les mails entrants et sortants, par groupe d'utilisateurs et Groupe	
- nombre de mails reçus et délivrés	
- répartition en nombre de mails par nature (spam, virus, etc.)	
- nombre de mails récupérés en quarantaine par les utilisateurs	
- répartition du nombre de mails par type de pièce jointe	

- répartition du volume par type de pièce jointe	
- rapports en ligne, format tableaux et graphiques, exportables	
3 Niveaux de service attendu	
- taux de disponibilité supérieur à 99% sur une année 24H/365J	
- garantie de temps de rétablissement inférieur à 2H même en cas de sinistre majeur	
- support technique 24/7 en français par le fournisseur de service (et non le revendeur), réponse en moins de 2H si le service est indisponible	
4 Architecture technique	
4.1 Pré-requis	
Les flux réseaux entre le fournisseur et les serveurs l'Administration mauritanienne s'appuie sur le standard SMTP.	
Le déploiement et l'activation du service doit se faire par nom de domaine.	
Le routage vers les serveurs de messagerie Groupe ou locaux doit se baser obligatoirement sur le "short name" des utilisateurs.	
Pour un même utilisateur, le fournisseur doit savoir gérer une configuration asymétrique : mails entrants vers une passerelle l'Administration mauritanienne, mails sortants depuis une autre passerelle ou serveur de messagerie l'Administration mauritanienne	
Sécurité réseau :	
Possibilité de mettre en œuvre une authentification SMTP afin d'avoir une authentification croisée des passerelles l'Administration mauritanienne et le fournisseur.	
Continuité :	
- Flux entrant : en cas d'indisponibilité d'une passerelle ou d'un serveur de messagerie l'Administration mauritanienne, le fournisseur doit stocker les mails entrants. Préciser le délai maximum de stockage.	
- Flux sortant : le fournisseur doit disposer de plusieurs points d'accès vis-à-vis de l'Administration mauritanienne, géographiquement distants. Préciser dans la réponse les mécanismes et moyens en place permettant d'assurer la continuité de service du flux sortant.	
4.2 Intégration	
- centraliser : les règles et paramètres définis via le portail Web s'appliquent sur toutes les plates-formes de filtrage	
- consolider : les zones de quarantaines, les logs et les statistiques sont restituées sur un unique portail Web	

- aussi bien pour les utilisateurs (self-service) que pour les administrateurs	
Préciser le nombre et la localisation des points de présence et plates-formes de filtrage.	
Gestion des utilisateurs :	
Préciser les modalités de création / suppression :	
- enregistrement manuelle : import de fichiers XLS,CSV,LDIF	
- enregistrement automatique : préciser le protocole	
- autres solutions proposées à préciser	
Gestion des cas particuliers : solution proposée pour intégrer :	
- les adresses mail de service (contact@mauritania.mr)	
- les alias mail d'utilisateur (adresse secondaire)	
4.3 Déploiement	
Le fournisseur doit proposer une stratégie de déploiement et un planning de mise en œuvre adaptés au contexte technique de l'Administration mauritanienne (multi-serveurs de messagerie, multi-noms de domaine).	
Préciser le nombre de jours homme prévu sur site dans la prestation de mise en œuvre et de déploiement du service.	
Côté administrateur :	
- compétences techniques requises	
- formation à l'outil : modalités et durée	
Côté utilisateurs :	
- compétences techniques requises	
- formation à l'outil : modalités et durée	
Livrables à fournir :	
- description de l'architecture technique (FR,AN)	
- procédures d'administration (FR,AN)	
- guide utilisateur (AN, FR)	
- supports ou modèles de communication utilisateur (AN, FR)	
5 Prestation de service	
5.1 Contrat	
Le contrat de service doit inclure les clauses suivantes :	
- obligations de résultat du fournisseur de service	
- engagement sur les niveaux de service (temps de réponse : inférieur 60 s, taux de disponibilité : 99%, support : 24/24 FR) soumis à pénalités	

- conditions de renouvellement du service et de résolution du contrat	
- accord de confidentialité	
- protection des données à caractère personnel	
Certifications Qualité / Sécurité :	
6 Divers	
Autres fonctionnalités non mentionnées	
Commentaires	
Questions	

7.3.7.2 FILTRAGE WEB

<p style="text-align: center;">MFPMA</p> <p>FILTRAGE WEB - CAHIER DES CHARGES</p>	<p style="text-align: center;">REPONSE [FOURNISSEUR]</p>
<p>1 Objectifs</p> <p>Le MFPMA souhaite mettre en place une solution de filtrage anti-virus et anti-spyware en mode hébergée des flux Web entrants et sortants.</p> <p>Le MFPMA souhaite également, optimiser la bande passante en filtrant les URL et avoir les fonctionnalités de proxy, proxy cache sous forme d'Appliance</p> <p>Le "fournisseur" désigne le fournisseur de service. Le "Groupe" désigne l'ensemble des entités du MFPMA</p> <p>2 Filtrage Anti-Virus, Anti-Spyware service managé</p> <p>Configuration Proxy</p> <ul style="list-style-type: none"> - Chaînage de proxy - Chaînage pare-feu à proxy - Analyse des flux HTTP, FTP <p>Identification et enregistrement utilisateur</p> <ul style="list-style-type: none"> - Identification par NTLM - Enregistrement Individuel - Enregistrement en masse - Possibilité d'inviter un utilisateur au service <p>Reporting</p> <ul style="list-style-type: none"> - Type de rapports - Durée de disponibilité des rapports - Export de données - Format des rapports dont drilling down <p>Garantie de disponibilité du service</p> <ul style="list-style-type: none"> - Localisation des plateforme - Plateforme hautement disponible, indiquer le nombre - Disponibilité contractuel du service (minimum requis : 99%) - Temps de propagation d'une politique (minimum requis : 5 minutes) <p>Assistance technique</p>	

- Disponibiité 24/24, 7/7	
- Support en Français	
Moteur d'analyse	
- Nombre de moteurs anti-malware (minimum requis : 2)	
- Notification utilisateur en cas de blocage des pages verroulées	
- Garantie à 100% contre l'infection des virus connus et inconnus	
3 Appliance filtrage d'URL	
Configuration Hardware	
- Processeur Intel (minimum requis P4)	
- HDD 80 Go	
- 2 ports Ethernet GigE minimum	
- Ecran LCD	
- Format Appliance, pré-installation effectuée	
- Appliance configurable en haute disponibilité	
Gain de performance / Productivité	
- Fonctionnalité Proxy	
- Fonctionnalité Proxy-Cache	
Administration	
- Mise à jour automatique	
- Restauration rapide "restore to last good"	
- Interface graphique d'administration	
- Implémentation simple des règles (drag and droop)	
- Règles granulaires par groupes ou utilisateurs	
- Interfaçage annuaire (AD)	
- Autorisation par plages horaires	
Filtrage d'URL	
- Taille de la base de données (minimum requis : 20 millions d'URL référencés)	
- Nombre et pertinence des catégories	
- Prise en compte de contenu international et multi-culturel	
- Organisation interne afin de répertorier les sites	
- Classification dynamique des sites	
- Gestion et mise à jour des sites inconnus	
- Protection contre les sites peer-to-peer, IM, webmail, MI	
Reporting	
- Analyse du hardware	
- Tableau de bord synthétique (noombres de pages consultées, bande passante utilisée, top 10 des protocoles utilisés, catogories de sites...)	
Notification utilisateur	
- Page de notification en cas de blocage	
- Modification du contenu de la page	

Support	
- Support 24/24, 7/7	
- Modalités du support hardware	
- Support en français	
5 Prestation de service	
5.1 Contrat	
Le contrat de service doit être passé avec le fournisseur de service et non le revendeur.	
Le contrat de service doit inclure les clauses suivantes :	
- obligations de résultat du fournisseur de service	
- engagement sur les niveaux de service (taux de disponibilité, support) soumis à pénalités	
- conditions de renouvellement du service et de résolution du contrat	
- accord de confidentialité	
- protection des données à caractère personnel	
Certifications Qualité / Sécurité :	
6 Divers	
Autres fonctionnalités non mentionnées	
Commentaires	
Questions	

Cependant il est important pour le soumissionnaire de connaître davantage l'existant au niveau du Ministère de la Fonction Publique et de la Modernisation de l'Administration. Il est donné simplement ici quelques précisions sur le réseau vu la sensibilité de telles informations.

Il est par conséquent demandé au soumissionnaire de se rapprocher du Ministère de la Fonction Publique et de la Modernisation pour plus de détails.

7.3.8 Description de l'architecture existante

Dans le cadre de son programme de modernisation de l'administration le MFPMA a mis en place un réseau de type étoile bâti autour de l'immeuble du gouvernement et interconnectant tous les sites administratifs de la ville de Nouakchott. Le nœud central est bâti autour du Catalyst 4507 de Cisco tandis que les nœuds principaux sont bâtis autour des catalyst 3550-12G. Chaque nœud principal peut regrouper un ou plusieurs départements ministériels. Les liaisons entre le nœud central et les nœuds principaux sont redondantes. Toutes les artères de transmission inter nœud sont en fibres optiques monomodes ou multi modes. Environ 40 km sont enfouis à Nouakchott.

Un système de sécurité bâti autour de deux firewalls PIX de Cisco en failover et d'un détecteur d'intrusion est installé au niveau du site central. Tous les switches sont managés à partir du site central via Cisco Cluster Management Suite à travers une interface Web.

Ce réseau est interconnecté au Nœud de Mauritel (Opérateur des Télécommunications) par une liaison filaire de 2,048 Mbps.

Ce réseau transporte les services hébergés au niveau du DATA CENTER (VOIR ANNEXE A), c'est un centre situé au niveau de l'Immeuble du Gouvernement, héberge une plateforme d'une trentaine de serveurs

de haute gamme montée en rack. Ces serveurs hébergent la plus part des services et des applications utilisées par l'administration (sites web, Intranet, Applications, messagerie, accès sécurisés à l'internet...etc.).

Cette plateforme gère un parc composé d'environ 1500 ordinateurs, ce nombre est appelé à croître de manière continue au cours des prochains mois. En outre, 3000 prises sont déjà disponibles pour connecter autant de machines.

7.3.9 Listes de serveurs

Le tableau suivant illustre les rôles des différents serveurs de l'infrastructure ainsi leur appartenance aux différents réseaux.

Serveur	Réseau	Rôle
1	Externe	Serveur DNS publique, serveur de messagerie sous sendmail (mauritania.mr) (Redhat 9.0 Kernel 2.4)
2	Externe	Serveur Web1 hébergeant les anciens sites web (php, asp)
3	Externe	Serveur de sauvegarde pour l'objectif de remplacer l'ancien serveur
4	Périmètre	Serveur SMTP pour le scanning de virus des messages
5	Périmètre	Serveur SMTP pour le scanning de virus des messages
6	Périmètre	Serveur de pare-feu et proxy
7	Périmètre	Serveur de pare-feu et proxy
8	Frontal	Serveur pour accès à la messagerie de l'extérieur
9	Frontal	Serveur pour accès à la messagerie de l'extérieur
10	Frontal	Serveur relais SMTP interne et hébergeant les zones DNS externes
11	Frontal	Serveur relais SMTP interne et hébergeant les zones DNS externes
12	Dorsal	Serveur pour accès à la messagerie de l'intérieur
13	Dorsal	Serveur pour accès à la messagerie de l'intérieur
14	Dorsal	Contrôleur de domaine
15	Dorsal	Contrôleur de domaine
16	Dorsal	Premier nœud du cluster de messagerie 01
17	Dorsal	Second nœud du cluster de messagerie 02
18	Dorsal	Serveur Web Internet 1
19	Dorsal	Serveur Web Internet 2
20	Dorsal	Serveur Intranet
21	Dorsal	Serveur Web développement
22	Dorsal	Serveur Web Authoring
23	Dorsal	Serveur Sql Internet1
24	Dorsal	Serveur Sql Intranet
25	Dorsal	Serveur Sql Internet 2
26	Dorsal	Serveur MOM
27	Dorsal	Serveur SMS
28	Dorsal	Serveur SMS distribution et WSUS
29	Dorsal	Serveur d'Application
30	Dorsal	Serveur IGE
31	Dorsal	Serveur d'e-learning

7.3.10 Systèmes préinstallés :

Système d'exploitation: Windows 2003 Server, Entreprise, Français SP2

Autres Logiciels Microsoft :

- ISA Server 2004 avec SP2
- Exchange 2003 SP2, Entreprise, Français
- SMS 2003
- MOM 2005
- SQL 2000
- SharePoint portal
- Content Management Système

Solutions antivirus et antisпам:

- Sophos Antivirus
- Sophos puremessage pour les scans des messages

7.3.11 L'architecture physique de l'infrastructure :

Comme illustre La figure ci-dessous, l'architecture de l'infrastructure comporte les trois zones réseautiques suivantes :

- Une zone Externe pour les utilisateurs Internet;
- Une zone de Périmètre se composant des services publiés;
- Une zone Interne se composant de l'infrastructure interne de l'administration.

1. Zone Externe :

La zone externe se compose des éléments suivants :

- Les utilisateurs Internet accédant aux services publiés de l'administration via leur navigateur local sous les protocoles standards : HTTP, HTTPS, SMTP et DNS.
- Les ressources DNS du fournisseur de connexion Internet (ISP) utilisées pour résoudre les noms DNS externes

2. Zone Périmètre :

La zone Périmètre se compose des éléments suivants :

- Une sous zone de bordure avec les routeurs de connexion Internet qui offre un premier niveau de protection. En effet ces routeurs ne permettent l'accès au réseau de Périmètre que sur certains ports TCP/UDP définis et vers des adresses IP spécifiques.
- Une sous zone de Périmètre constitué des éléments suivants :
 - o Deux pare-feu physiques cisco PIX 515E qui permettent de contrôler le flux de données entre le réseau externe et le réseau de périmètre
 - o Des serveurs SMTP Scan pour inspecter les messages entrant et sortant et filtrer les messages infectés. Ce scénario se compose de deux serveurs SMTP Scan afin d'assurer un bon service de disponibilité.
 - o Des serveurs ISA Server 2004 pour une publication sécurisée des services Internet de l'administration. Ce scénario se compose de deux serveurs ISA afin d'assurer un bon service de disponibilité.

3. Zone Interne :

La zone Interne se compose de plusieurs sous zones ou sites sous forme des VLANS (un VLAN par Ministère). La séparation en sous zone des composants interne permet de sécuriser les différents éléments de manière indépendante et de sécuriser le flux entre les clients internes et les serveurs d'infrastructure

La structure logique du réseau actuel est illustrée dans la figure suivante :

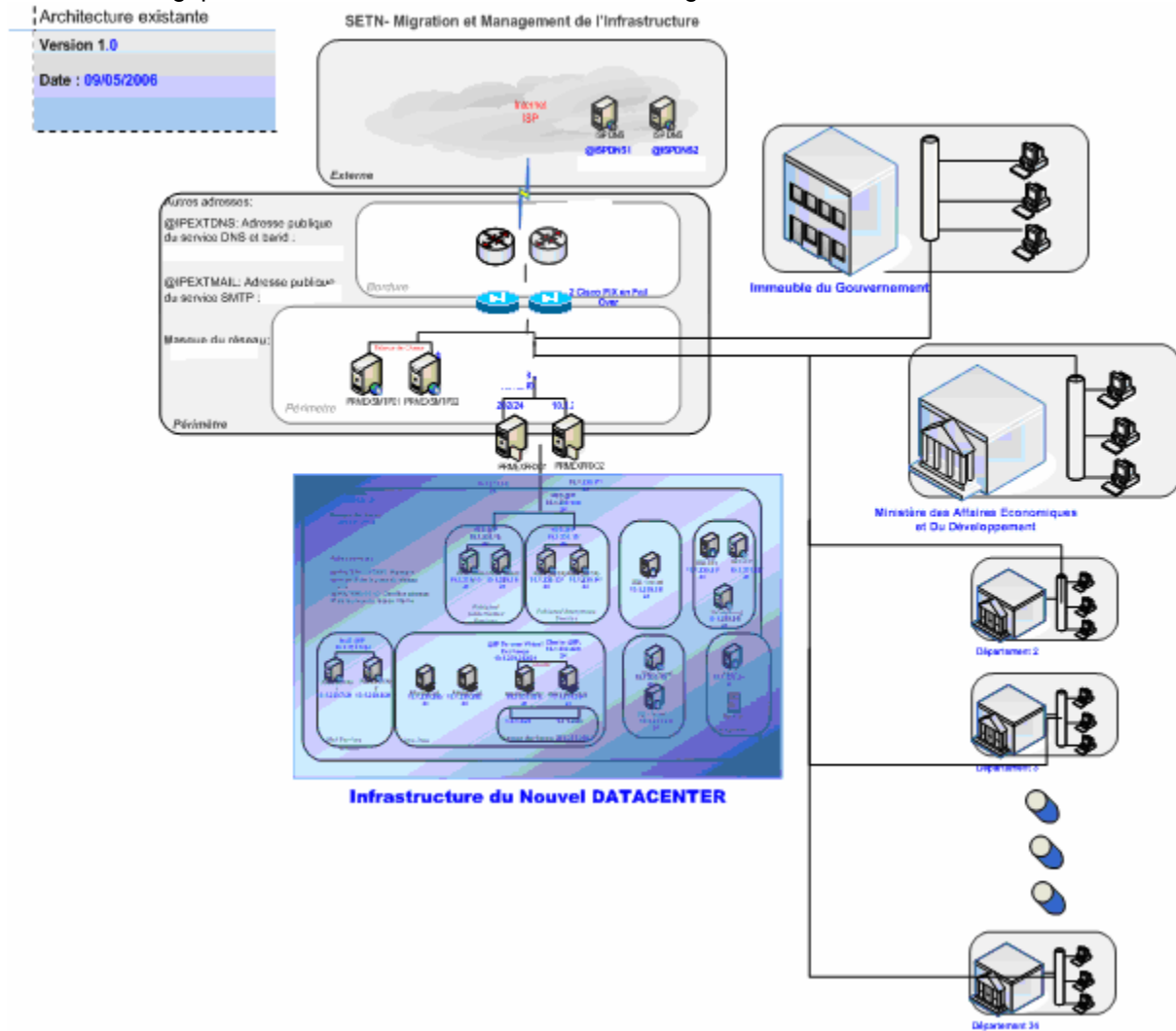


Figure 1 : Schéma logique du réseau actuel

Les caractéristiques de la structure du réseau actuel sont les suivantes :

- L'ensemble du réseau est bâti sur une infrastructure ETHERNET avec une fédération au niveau du MFPMA. Les autres sites sont reliés par des uplink en Fibre optique assurant le niveau distribution.
- Toutes les structures disposent d'un réseau local avec des postes de travail sous windows xp muni d'adresses IP dynamiques attribuées selon le VLAN du département.
- Les structures connectées au DATA CENTER telles qu'illustrées dans la figure 1 ci-dessus disposent d'une connexion sécurisée à Internet avec l'accès à une gamme de services talques (les sites web des ministères, Intranet des ministères, un système messagerie exchange...etc.)

7.3.12 LISTE DES EQUIPEMENTS RESEAUX

1 Catalyst 4706 qui interconnecte tous les départements ministériels au réseau Intranet
1 Catalyst Inside 3550 pour le réseau intranet
1 Catalyst Outside 2950 pour le réseau public (accès internet via la mauritel)
1 routeur Cisco 3700 série pour la connexion internet
2 pix Cisco 515E en failover pour la sécurité du réseau
1 IDS cisco pour la sécurité du réseau
1 routeur Cisco AS5300 pour la gestion de la téléphonie IP sur le réseau public
1 serveur Cisco Works pour la gestion des connexions FO
1 serveur Call manager pour la gestion de la téléphonie IP
6 catalysts 3550 12 G répartis en zone et interconnectant les différents départements ministériels au réseau intranet de l'administration. Chaque catalyst constitue un nœud principal
40 Swtichs Cisco 24 SMI et 90 switchs SMC connectant les différents utilisateurs aux différents réseaux locaux.

8 MODÈLE DE CURRICULUM VITAE

1. FONCTION PROPOSEE :

(Indiquer la fonction qu'exercera l'expert au sein de l'équipe et résumer brièvement les tâches qui lui seront confiées.)

2. ETAT CIVIL - PROFESSION :

Nom, prénoms :

Date de naissance :

Situation de famille :

Nationalité :

Profession actuelle :

Ancienneté dans le présent emploi :

3. FORMATION - DIPLOMES :

(Indiquer brièvement les établissements universitaires et autres institutions d'enseignement spécialisé fréquentés, avec types et dates des diplômes obtenus - Ne pas dépasser un quart de page.)

4. PRINCIPALES QUALIFICATIONS - EXPERIENCE :

(Indiquer en résumé la spécialisation et l'expérience de l'expert se rapportant le plus aux tâches qui lui seront confiées dans l'équipe proposée - Décrire le degré de responsabilité de l'expert dans des projets similaires, avec indication des dates et lieux - Ne pas dépasser une demi page.)

(date)

L'expert (*nom, cachet et signature*).

9 MODELE DE CAUTIONNEMENT PROVISOIRE

Attendu que (*nom du candidat*)

(ci-dessous désigné « le candidat »)

a soumis son offre en date du (*date du dépôt de l'offre*) pour la fourniture de (*identifier les prestations i*)

(ci-dessous désignée « l'offre »)

NOUS (*désignation de la banque*), ayant notre siège à (*adresse de la banque*)

(ci-dessous désignée « la banque »)

pour la somme de (*inscrire le montant*) que la banque s'engage à régler intégralement à (*l'Administration*), s'obligeant elle-même, ses successeurs et assignataires.

Les conditions de cette obligation sont les suivantes :

1. si le candidat retire son offre pendant la période de sa validité ;

ou :

2. si le candidat, s'étant vu notifier l'acceptation de son offre par (*l'Administration*) pendant la période de validité de l'offre :

- manque à signer ou refuse de signer le marché, alors qu'il est requis de le faire ; ou :

- manque à fournir ou refuse de fournir le cautionnement définitif, comme prévu dans les instructions aux candidats.

Nous nous engageons à payer à (*l'Administration*) un montant à concurrence du montant susmentionné, dès réception de sa première demande écrite, sans qu'elle soit tenue de justifier sa demande, étant entendu toutefois que, dans sa demande, le (*l'Administration*) précisera que le montant qu'il réclame lui est dû parce que l'une ou l'autre des conditions ci-dessus, ou toutes les deux, sont remplies.

La présente garantie demeurera valable jusqu'à l'expiration du délai de validité de l'offre. Toute demande relative à cette garantie devra parvenir à la banque au plus tard à la date susmentionnée.

DATE....SIGNATURE et AUTHENTIFICATION de la BANQUE.....

10 MODELE DE CAUTIONNEMENT DEFINITIF

A : *(nom et adresse de du Ministère)*

ATTENDU QUE *(nom de la Société)*

(ci-dessous désigné « le fournisseur»)

s'est engagé en exécution du marché n° *(référence du marché)* en date du à fournir

(description des prestations)

(ci-après désigné « le marché ») ;

ET QUE vous avez stipulé dans ledit marché que le fournisseur vous remettra une garantie bancaire d'une banque connue, du montant stipulé ci-après, comme garantie de la bonne exécution de ses obligations, conformément au marché ;

ET QUE nous avons convenu de donner une garantie au fournisseur;

DES LORS nous affirmons, par les présentes, que nous nous portons garants et responsables à votre égard, au nom du fournisseur, pour un montant maximum de *(montant de la caution en chiffres et en lettres)*, et nous nous engageons à vous payer, dès réception de votre première demande écrite déclarant que le fournisseur ne se conforme pas aux stipulations du marché, et sans argutie ni discussion, toute(s) somme(s), dans les limites de *(montant de la caution)* ci-dessus stipulée(s), sans que vous ayez à prouver ou à donner les raisons ni le motif de votre demande ou du montant indiqué ci-dessus.

La présente garantie est valable jusqu'à la réception définitive des travaux

DATE.....SIGNATURE et AUTHENTIFICATION de la BANQUE

11 MODÈLE DE CAUTIONNEMENT DE RESTITUTION D'AVANCE

A : *(nom et adresse du Ministère)*

Messieurs,

Conformément aux dispositions de l'article 88 du code des marchés publics, *(nom et adresse de la Société)* (ci-après désigné « le fournisseur ») déposera auprès de *(identité de l'Administration)* une garantie bancaire ayant pour objet de garantir une exécution correcte et loyale de ses obligations, conformément aux dispositions dudit article, et s'élevant à.....ouguiya *(montant de la caution en toutes lettres et en chiffres)*.

Nous, la *(nom et adresse de la banque)*, conformément aux instructions de la société, convenons de façon inconditionnelle et irrévocable de garantir, en tant qu'obligataire principal et pas seulement en tant que garant, le paiement à *(identité de l'Administration)* à première demande sans droit d'objection de notre part et sans sa première réclamation préalable au consultant, d'un montant ne dépassant pas *(montant de la caution en toutes lettres et en chiffres)*.

Nous convenons, en outre, qu'aucun changement ou additif ou aucune autre modification aux conditions du marché ou à l'un des documents constitutifs du marché qui peut être établi entre l'Agence Mauritanienne d'Information, ne nous libérera d'une obligation quelconque nous incombant en vertu de la présente garantie.

Cette garantie restera valable à partir du paiement reçu par le consultant selon le marché jusqu'à *(préciser la date)*.

Veillez agréer, Messieurs, l'assurance de notre considération distinguée.

DATE.... SIGNATURE et AUTHENTIFICATION DE LA BANQUE....