



**REPUBLIQUE TUNISIENNE**

\*\*\*\*

**MINISTERE DE L'ENSEIGNEMENT SUPERIEUR  
ET DE LA RECHERCHE SCIENTIFIQUE**

\*\*\*\*\*

**UNIVERSITE DE MONASTIR**

\*\*\*\*

**ISIMa**

---



---

**Consultation N°01-2025 PAQ-DGSE ISIMa**

**Acquisition de matériels de sécurité informatique au profit de  
l'Institut Supérieur d'informatique de Mahdia**



Août 2025

# Consultation N°01-2025 PAQ-DGSE ISIMa

## Acquisition de matériels de sécurité informatique (Pare-feu, solution d'administration centralisée, services et formation)

### ARTICLE 1 : OBJET

L'institut supérieur d'informatique de Mahdia se propose de lancer une consultation pour l'acquisition d'un **lot unique** comportant des matériels et des services selon les spécifications suivantes :

LOT N°	Désignation Article	Quantité
01	Pare-feu	01
	Solution d'administration centralisée	01
	Services (installation, configuration, garantie et assistance)	01
	Formation (administration et configuration du pare-feu)	01

Et ce, selon les conditions et spécifications techniques minimales mentionnées dans le présent cahier des charges.

### ARTICLE 2 : QUALIFICATION DES SOUMISSIONNAIRES

Le soumissionnaire doit répondre aux conditions minimales suivantes :

#### 1. Références du soumissionnaire

- Avoir réalisé au moins cinq (05) projets de mise en place de pare-feux avec une solution d'administration durant les cinq (05) dernières années.
- Fournir des preuves (procès-verbaux, attestations, ou documents officiels).

#### 2. Personnel à affecter pour la réalisation du projet

- Chef de projet :
  - Diplôme d'ingénieur informatique (ou équivalent).
  - Expérience d'au moins cinq (05) ans dans la gestion de projets IT.
  - Certification constructeur *Network Security Architect/Expert* (ou équivalent valide).
  - Justificatifs obligatoires à fournir.

#### 3. Aspect service

- Installation, configuration et mise en place des Firewalls sur le site de l'ISIMA
- Installation et configuration de la solution d'administration centralisée.
- Assistance technique pour la résolution des problèmes techniques.

### **ARTICLE 3 : PIECES CONSTITUTIVES DE L'OFFRE**

L'offre est constituée par :

1. Le dossier technique.
2. Le dossier financier.

Le dossier technique et le dossier financier sont mis dans une enveloppe extérieure fermée et scellée, portant en plus de l'adresse de l'institut supérieur de gestion la mention suivante :

**« NE PAS OUVRIR – CONSULTATION N°01-2025 PAQ-DGSE ISIMa – Relative à l'Acquisition de matériels de sécurité informatique au profit de l'institut supérieur d'informatique de Mahdia »**

### **ARTICLE 4 : DELAI DE VALIDITE DES OFFRES**

Tout soumissionnaire sera lié par son offre pendant soixante (60) jours à compter du jour suivant la date limite fixée pour la réception des offres. Pendant cette période, les prix proposés par le soumissionnaire seront fermes et non révisables.

### **ARTICLE 5 : VARIATION EN NATURE ET EN QUANTITE ADMISE**

La commission de dépouillement est passible de diminuer des quantités ou de rejeter des articles inscrits dans la présente consultation sous prétexte d'insuffisance du budget ou des prix excessifs.

### **ARTICLE 6 : DELAI D'EXECUTION**

Le délai global d'exécution commence à partir du lendemain de la date de la notification de la commande. Ce délai est fixé à soixante (45) jours et couvre la livraison, l'installation et la mise en marche des équipements en question.

### **ARTICLE 7 : ANALYSE ET CHOIX DES OFFRES**

L'évaluation des offres s'effectuera, par lot, en deux étapes :

1. Classement des offres financières.
2. Vérification de la conformité des offres techniques du soumissionnaire ayant présenté l'offre financière la moins-disante.

### **ARTICLE 8 : CONFORMITE DU MATERIEL**

Les équipements livrés doivent être conformes aux caractéristiques et spécifications techniques présentées dans l'offre. L'administration se réserve le droit de faire appel à des experts ou techniciens pour examiner les équipements à réceptionner.

## **ARTICLE 9 : DELAI POUR PROCEDER A LA RECEPTION DU MATERIEL**

L'administration doit procéder à la réception provisoire du matériel dans un délai maximum de quinze (15) jours à compter de la date de la livraison. La réception définitive sera prononcée à l'expiration du délai de garantie.

## **ARTICLE 10 : MODE DE PAIEMENT**

Le paiement sera effectué conformément à la réglementation en vigueur et aux conditions suivantes :

- Livraison du matériel conforme.
- Test de bon fonctionnement.
- PV de réception provisoire signé.
- Attestation de garantie d'un an au minimum.
- Mandatement dans un délai maximum de 30 jours après régularisation du dossier.

## **ARTICLE 11 : GARANTIE**

Le soumissionnaire garantit les équipements pendant au minimum un (01) an à compter de la réception provisoire. La garantie couvre équipements, pièces de rechange, accessoires, main d'œuvre et déplacement. **Une retenue de garantie de 5%** sera prélevée sur le paiement à effectuer, en garantie de la bonne exécution du marché. La retenue de garantie n'est payée au titulaire du marché qu'après la réception définitive des équipements et services et la mise en marche suite à l'expiration du délai de garantie mentionne ci-dessus et lorsqu'il aura justifié de l'accomplissement de toutes les obligations consécutives du marché. La retenue de garantie peut être remplacée par une caution personnelle et solidaire rédigée conformément au modèle présenté à l'annexe n° 6. La retenue de garantie doit être émise par une institution financière ayant reçu un agrément du ministre chargé des finances.

## **ARTICLE 12 : PENALITES DE RETARD**

Pour chaque jour de retard, non justifié par écrit, le soumissionnaire devra payer une pénalité de **1% par jour** sur le montant du lot en retard. Ces pénalités ne doivent pas excéder **5% du montant TTC** du lot concerné.

## **ARTICLE 13 : REGLEMENTATION APPLICABLE**

Pour tout ce qui n'est pas stipulé, l'exécution de la commande sera régie par :

- Le code de la comptabilité publique.
- Le décret n° 2014-1039 du 13 Mars 2014 portant réglementation des marchés publics.

## **ANNEXES**

- Annexe 1 : Formulaire des propositions techniques.
- Annexe 2 : Bordereau des prix.
- Annexe 3 : Déclaration sur l'honneur concernant l'exercice en tant qu'agent public.
- Annexe 4 : Déclaration sur l'honneur de non influence.
- Annexe 5 : Soumission par lot.
- Annexe 6 : Modèle d'engagement d'une caution personnelle et solidaire à produire au lieu et place de la retenue de garantie

## Consultation N°01-2025 PAQ-DGSE ISIMa

### Acquisition de matériels de sécurité informatique au profit de l' Institut supérieur d'informatique de Mahdia

#### ***Annexe 1 : Formulaires des propositions techniques***

#### **Lot 1 , Article 1 : Pare-feu(Quantité : 1)**

Caractéristiques	Caractéristiques minimales exigées	Caractéristiques proposées
<b>Identification</b>		
Marque et Modèle	À préciser	
Type et Format	<ul style="list-style-type: none"> <li>▪ Appliance Physique dédiée.</li> <li>▪ Boîtier 19" rackable avec kit de montage en rack inclus</li> </ul>	
Double alimentation	Oui	
Durée de vie	La commercialisation du pare- feu ainsi que tous ses composants y compris la licence doit être garantie, par le constructeur, pour une période minimale de cinq (05) ans (attestation exigée)	
Licence	<p>La Licence du Firewall proposée doit être activée au nom de ISIMA, valide pendant un (01) an et doit garantir les fonctionnalités suivantes:</p> <ul style="list-style-type: none"> <li>▪ Contrôle Applicatif</li> <li>▪ Détection et Protection contre les intrusions (IPS)</li> <li>▪ Protection Antivirus / Antimalwares</li> <li>▪ Filtrage WEB</li> <li>▪ Anti-Spam</li> <li>▪ Prévention contre les attaques Zéro Day et les Attaques APT</li> </ul>	
Firmware	Le Firewall proposé doit être livré avec la dernière version stable du firmware publiée par le constructeur.	
<b>Généralités</b>		
Firewall Technologie Stateful Inspection	Oui	
Fonction VPN IPSEC	Oui	
Fonction VPN SSL	Oui	
Fonction de Filtrage DNS	Oui supporté	
Possibilité de diviser le pare-feu en plusieurs pare-feux totalement indépendant.	Oui, incluant tous les fonctionnalités du firewall	
<b>Performances</b>		
Débit de traitement en clair	39 Gbps	

Débit du firewall avec contrôle applicatif	6,5 Gbps	
Débit d'inspection NGFW (FW + IPS + contrôle applicatif)	3 Gbps	
Débit Threat Protection	2,8 Gbps	
Débit de traitement en VPN IPSEC	34 Gbps	
Débit de traitement IPS	5 Gbps	
Débit avec Inspection SSL	3 Gbps	
Nombre de connexions simultanées	2,5 Million	
Nombre de nouvelles connexions par seconde	130 000	
Nombre des instances virtuels supportés	10	
<b>Interfaces</b>		
Nombre d'interfaces 1 Gbps (RJ45)	16 x 10/100/1000 Interfaces (RJ-45)	
Nombre de ports 10 GE SFP+	4 ports	
Nombre de ports 1 GE SFP	8 ports	
Nombre de ports Management	01	
Nombre de ports HA	01	
Nombre de ports Console	01 (câble originale inclus)	
Nombre de ports USB	01	
<b>Protocoles</b>		
Routage	<ul style="list-style-type: none"> <li>• Statique et Dynamique IPV4,</li> <li>• Statique et Dynamique IPV6</li> <li>• Routage Inter VLANs</li> <li>• VRRP</li> <li>• Link Failure Control</li> <li>• Multi-link Agregation (802.3ad)</li> </ul>	
Support du multicast	Oui	
Protocoles d'administration	SNMP V2, V3	
<b>Fonctionnalités de Protection</b>		
Critères de règles de filtrage	Par interface, par service, par adresse IP, par port, par groupe, par utilisateur (source, destination)	
<b>Protocoles supportés sous la technologie proposée</b>	http(s), SMTP, FTP	
<b>Translation d'adresses (NAT)</b>	Oui	
<b>Translation de ports (PAT) supportée</b>	Oui	
<b>Filtrage et contrôle d'accès aux zones « DMZ »</b>	Oui	

<b>Prévention des attaques DoS et DDoS</b>	Oui	
<b>Détection de spoofing</b>	Oui	
<b>Détection de scan des ports</b>	Oui	
<b>SD-WAN</b>	Oui	
<b>Fonctionnalité d'authentification</b>		
Base d'utilisateurs locale	Oui	
Interopérabilité avec les serveurs d'authentification existants	RADIUS, LDAP, Active Directory	
<b>Qualité de service</b>		
Mécanismes de qualité de service (gestion de la bande passante et priorisation du trafic)	Oui	
Contrôle par adresse IP/groupe IP	Oui	
<b>VPN</b>		
Nombre des tunnels VPN Site-To-Site supportés	2000	
Nombre des tunnels VPN Client-To-Site supportés	15 000	
Tunnels VPN Site-to-Site	Protocole utilisé	IPSec
	Algorithmes de chiffrement	AES, 3DES
	Algorithmes de hachage	MD5, SHA-1
Tunnels VPN Client-to-Site	Protocole utilisé	IPSec
	Algorithmes de chiffrement	AES, 3DES
	Algorithmes de hachage	MD5, SHA-1, SHA-2
Supporte le standard X509 V3	Oui	
<b>Administration</b>		
Configuration, administration et monitoring, définition et mise en œuvre de la politique de sécurité à travers une interface web sécurisée.	Oui	
Méthodes d'administration sécurisées	<b>Oui, SSL ou SSH</b>	
Edition et modification de la configuration	<b>Oui</b>	
Mise à jour du software du	<b>Oui</b>	

Firewall		
Génération et envoi de Logs	<b>Oui</b>	
Format des logs	<b>Syslog</b>	
Etat du système et des interfaces	<b>Oui</b>	
<b>Système de prévention et de Détection d'intrusion</b>		
Prévention, détection et arrêt en temps réel des tentatives d'intrusions	Oui	
Possibilité de corrélation des attaques	Oui	
Prévention et détection des attaques comme : Denial-of-service (DoS), TFN, SYN floods, Back Orifice, failed login attempts, et TCP hijacking	Oui	
Prévention et détection avancées contre les virus et les malwares	Oui	
Identification et reconnaissance des attaques basées sur les vulnérabilités	Oui	
Informations relatives aux attaques (types d'attaques, user, source,...)	Oui	
Notification et reporting en temps réel des alertes	Oui	
Notification directe à l'administrateur en cas de mise à jour et en cas d'alertes	Oui	
Type de remontée des alertes	SMTP, alerte sur console, SNMP	
Mise à jour de la base des signatures	Oui (automatique et manuelle)	
<b>Système de Protection AntiVirus / AntiMalware</b>		
Modes d'inspection	Mode Fichier et Mode Flux	
Protocoles à inspecter	http(s), FTP, SMTP(s), IMAP, POP3(s), messagerie instantanée (IM)	
Méthodes de Détection des virus	<ul style="list-style-type: none"> <li>• par signature</li> <li>• par analyse comportementale</li> </ul>	
Mise à jour du moteur	Oui (automatique et manuelle)	
Filtrage et contrôle de sécurité	Blocage de tout type de virus, des spywares, des adwares, des trojans et de tout trafic web et ftp malveillant.	
	Analyse des contrôles ActiveX et Java	

	Filtrage de contenu : Internet Messaging, Streaming, ICQ, trafic audio, trafic vidéo	
	Blocage et contrôle des pop-ups et du phishing	
<b>Mises à jour des fichiers de signature et des bases URL</b>	<ul style="list-style-type: none"> <li>• Manuelles</li> <li>• Automatiques</li> <li>• Programmées</li> </ul>	
<b>Système de Protection AntiSpam</b>		
Protection Email complète contre les vulnérabilités du service de Messagerie, la menace et la fuite d'information	Oui	
Blocage de fichiers par définition d'extension et de taille	Oui	
<b>Système de Protection Web/URL</b>		
Filtrage URL	Blocage statique (par site, par domaine, par mot clé,...)	
	Blocage par catégorie	
	Contrôle par période de temps (heures et jour)	
<b>Haute disponibilité</b>		
Haute disponibilité	<ul style="list-style-type: none"> <li>• Active/passive</li> <li>• Active/Active</li> <li>• Cluster</li> </ul>	
<b>Management et Logging</b>		
Administration et logging	En mode web ou graphique sécurisé	
	Alerts via SMTP et Logs	
Notification par e-mail	Oui	
Supervision du trafic en temps réel	Oui	
<b>Licences et Mise à jour</b>		
Licences d'activation et de Mise à jour Software et Hardware pour toutes les fonctionnalités demandées	Validités des licences est 3 ans.	

Fait à..... Le.....  
(Signature et cachet du soumissionnaire)

**Lot 1 , Article 2 : Solution d'administration centralisée des pare-feu (Quantité: 1)**

Désignation	Caractéristiques Techniques minimales demandées	Caractéristiques Techniques proposées
<b>Exigences générales</b>		
Marque	À préciser	
Modèle	A indiquer	
Type	Solution logicielle	
Version	Dernière version stable	
Architecture	multi-tenante	
Compatibilité	Compatible avec les pare-feux proposée	
Licences	Administration complète et à distante de 10 pare-feux physique ou logique	
Durée de licence	Les licences perpétuelles avec support de 3 ans	
Durée de vie	La commercialisation et les mises à jour de la solution d'administration ainsi que tous ses composants y compris la licence doit être garantie, par le constructeur, pour une période minimale de cinq (05) ans (attestation exigée)	
<b>Administration</b>		
Administration, gestion et surveillance des équipements de la plateforme de sécurité de l'ISIMA	<ul style="list-style-type: none"><li>• Centralisé</li><li>• Via une interface Web sécurisée (HTTPS)</li><li>• Console unifié</li></ul>	
Mode ligne de commande	Oui	
Création d'objets réutilisables communs sur un ensemble de firewalls	Oui	
Backup et restauration de la configuration des pare-feux	Oui	
Possibilité de création de prototype de configurations pour simplifier le déploiement de nouveau pare-feu	Oui	
Visualisation de l'ensemble des sites et des équipements associés sur une carte géographique	Oui	
Gestion des règles de routage	Oui	

Découverte automatique de la topologie du réseau	Oui	
Support de la haute disponibilité	Oui	
Administration fondée sur les rôles (RBAC)	Oui	
Possibilité de la configuration en utilisant des workflow	Oui	
Mise à jour de la base des signatures des applications	Oui automatique	
Création des signatures d'application personnalisée	Oui	
Fixation de la bande passante pour certains trafics d'applications et de services.	Oui	
Accès centralisé aux informations des applications, des utilisateurs et du contenu qui passe par les pare- feux	Oui	
Compatibilité SNMP	Oui, V1/V2C/V3	
Génération de statistiques à partir des journaux d'un ou plusieurs pare- feux sous forme de graphiques	Oui	
Analyse et investigation du Traffic réseaux et des incidents de sécurité	Oui avec reporting centralisés	
Détection et monitoring de la congestion du réseau	Oui	
<b>Visibilité</b>		
Tableaux de bord proposés	<ul style="list-style-type: none"> <li>• La qualité des liaisons WAN</li> <li>• L'utilisation de la bande passante</li> </ul>	
<b>Sécurité</b>		
IPSec VPN et SSL VPN supporté	Oui	
Accès sécurisé aux équipements gérés.	Oui	
Authentification des utilisateurs supportée	<ul style="list-style-type: none"> <li>• Base d'utilisateurs locale</li> <li>• Serveurs d'authentification (Radius, LDAP, active Directory)</li> <li>• PKI</li> </ul>	
La solution doit fournir des données et métriques exploitables pour réaliser des audits de sécurité	Oui	

Fait à..... Le,.....

(Signature et cachet du soumissionnaire)

### Lot 1 , Article 3 : Services

Désignation	Caractéristiques exigées		Éléments de Réponse
Garantie	Durée	1 an	
	Prestations couvertes	<ul style="list-style-type: none"> <li>• Installation, configuration et mise en place des Firewalls sur le site de l'ISIMA</li> <li>• Installation, configuration de la solution d'administration centralisée</li> <li>• Assistance technique de l'équipe pour la résolution des problèmes techniques.</li> </ul>	
Délai de livraison, d'installation et de mise en service	Maximum 60 jours <b>calendaires</b> décomptés à partir du lendemain de la notification de l'ordre de service.		
Délai de déclenchement de la session de formation	Maximum 15 jours <b>calendaires</b> décomptés à partir du lendemain de la notification de l'ordre de déclenchement de la session de formation.		

### Lot 1 , Article 4 : Formation

Désignation	Caractéristiques exigées	Valeurs proposées
Thème	Administration et configuration du pare-feu	
Guide et manuel de formation	Documentation officielle du constructeur	
Formateur	Certifié par le constructeur niveau Network Security Architect/Expert ou équivalent.	
Nombre de personnes à former	02	
Nombre de jours	05	

Fait à..... Le,.....

(Signature et cachet du soumissionnaire)

**Consultation N01-2025 PAQ-DGSE ISIMa**

**Acquisition de matériels de sécurité informatique au profit de l' Institut supérieur  
d'informatique de Mahdia**

**Annexe n° 2 :**

**BORDEREAU DES PRIX**

Lot N°	Articles	Qté	%TVA	Prix Unitaire DT		Prix Total TTC DT	
				Hors TVA	TTC	Hors TVA	TTC
01	Pare-feu	01					
	Solution d'administration centralisée	01					
	Services (installation, garantie, assistance)	01					
	Formation	01					
<b>Total</b>							

Le montant total du lot est arrêté à la somme de :

.....  
..... TTC (en toutes lettres)

Fait à..... Le,.....

(Signature et cachet du soumissionnaire)

**Consultation N01-2025 PAQ-DGSE ISIMa**

**Acquisition de matériels de sécurité informatique au profit de l' Institut supérieur  
d'informatique de Mahdia**

**Annexe 3 :**

**DECLARATION SUR L'HONNEUR CONCERNANT L'EXERCICE EN TANT QU'AGENT PUBLIC  
AU SEIN DE L'ADMINISTRATION**

Je soussigné (1) .....

agissant en tant que (2) .....

de la Société (3) .....

déclare sur l'honneur que je n'étais pas un agent public au sein du Ministère de l'Enseignement Supérieur  
et de la Recherche Scientifique ayant cessé mon activité depuis moins de cinq ans.

Fait à..... Le,.....

(Signature et cachet du soumissionnaire)

---

(1) Nom et prénom du signataire.

(2) Qualité du signataire.

(3) Raison sociale de la Société.

**Consultation N01-2025 PAQ-DGSE ISIMa**

**Acquisition de matériels de sécurité informatique au profit de l' Institut supérieur  
d'informatique de Mahdia**

**Annexe 4**

**DECLARATION SUR L'HONNEUR DE NON INFLUENCE**

Je soussigné (1) .....

agissant en tant que (2) .....

de la Société (3) .....

déclare sur l'honneur et m'engage de ne pas faire par moi-même ou par personne interposée, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusion du marché/commande et des étapes de sa réalisation.

Fait à..... Le,.....

(Signature et cachet du soumissionnaire)

Consultation N01-2025 PAQ-DGSE ISIMa

Acquisition de matériels de sécurité informatique au profit de l' Institut supérieur d'informatique de Mahdia

Annexe 05

**SOUMISSION**  
**Lot N°.....**

Je soussigné (1) .....  
agissant en qualité de (2) ..... de la Société (3) .....  
sise au (4) .....  
Boîte Postale : ..... Code Postal : ..... Ville : .....  
Téléphone : ..... Fax:..... E-Mail : .....  
Usine(adresse): .....  
Adresse et Site INTERNET : .....  
Registre de commerce N° : ..... Ville : .....  
Matricule fiscale : .....  
Affiliation à la CNSS N° : .....  
Domiciliation bancaire : .....  
C.C.B/C.C.P. N°: .....

Certifie avoir recueilli, par mes propres soins et sous mon entière responsabilité, tous renseignements nécessaires à la parfaite exécution de mes éventuelles obligations telles qu'elles découlent des différentes dispositions du présent cahier de charge relatif à la consultation N04-2025 --ISIMa pour l'Acquisition de matériels de sécurité informatique au profit de l' Institut supérieur d'informatique de Mahdia et je m'engage sur l'honneur que les renseignements fournis ci-dessus sont exacts.

Le montant de ma soumission est de :

Montant Hors Taxes : ..... Dinars Tunisiens HTVA

Montant de la TVA : ..... Dinars Tunisiens.

Soit un Total Toutes Taxes Comprises de :

(en chiffres) : ..... DT TTC

(en toutes lettres) : ..... DT TTC

Le délai d'exécution global pour le Lot N° 01 est fixé à ..... jours y compris dimanches et jours fériés, compté à partir du lendemain de la date de notification de la commande.

La durée de garantie du Lot N° 01 est de ..... comptée à partir de la date de réception provisoire.

Fait à..... Le,.....

(Signature et cachet du soumissionnaire)

## Consultation N01-2025 PAQ-DGSE ISIMa

### Acquisition de matériels de sécurité informatique au profit de l' Institut supérieur d'informatique de Mahdia

#### Annexe 6 :

### Modèle d'engagement d'une caution personnelle et solidaire à produire au lieu et place de la retenue de garantie

(Marché assorti d'un délai de garantie et d'une retenue de garantie)

Je soussigné- nous soussignés <sup>(1)</sup> .....

Agissant en qualité de <sup>(2)</sup> .....

1) Certifie — Certifions que <sup>(3)</sup> ..... a été agréé par le ministre chargé des finances en application de l'article 113 du décret n° 2014-1039 du 13 mars 2014, portant réglementation des marchés publics, que cet agrément n'a pas été révoqué que <sup>(3)</sup> ..... a constitué entre les mains du trésorerie général de Tunisie suivant récépissé n° ..... en date du ..... le cautionnement fixe de cinq mille dinars (5000 dinars) prévu par l'article 113 du décret susvisé et que ce cautionnement n'a pas été restitué.

2) Déclare me-déclarons nous, porter caution personnelle et solidaire, <sup>(4)</sup> ..... domicilié à <sup>(5)</sup> ..... Au titre du montant de la retenue de garantie auquel ce dernier est assujéti en qualité de titulaire du marché n° ..... passé avec <sup>(6)</sup> ..... en date du ..... enregistré à la recette des finances <sup>(7)</sup> ..... relatif à <sup>(8)</sup> .....

Le montant de la retenue de garantie, s'élève à .....% du montant du marché, ce qui correspond à ..... Dinars (en toutes lettres), et à ..... Dinars ..... (en chiffres).

3) M'engage- nous nous engageons solidairement, à effectuer le versement du montant garanti susvisé et dont le titulaire du marché serait débiteur au titre du marché susvisé, et ce, à la première demande écrite de l'acheteur public sans que j'ai (nous ayons) la possibilité de différer le paiement ou soulever de contestation pour quelque motif que ce soit et sans une mise en demeure ou une quelconque démarche administrative ou judiciaire préalable.

4) En application des dispositions de l'article 108 du décret n° 2014-1039 susvisé, la caution qui remplace la retenue de garantie devient caduque après que le titulaire du marché ait accompli toutes ses obligations, et ce, à l'expiration du délai de quatre mois à compter de la date de <sup>(9)</sup> .....

Si le titulaire du marché a été avisé par l'acheteur public, avant l'expiration du délai susvisé, par lettre motivée et recommandée ou par tout autre moyen ayant date certaine, qu'il n'a pas honoré tous ses engagements, il est fait opposition à l'expiration de la caution. Dans ce cas, la caution ne devient caduque que par main levée délivrée par l'acheteur public.

Fait à ....., le .....

(1) Nom(s) et prénom(s) du (des) signataire(s).

(2) Raison sociale et adresse de l'établissement garant.

(3) Raison sociale de l'établissement garant.

(4) Nom du titulaire du marché.

(5) Adresse du titulaire du marché.

(6) Acheteur public.

(7) Indication des références d'enregistrement auprès de la recette des finances.

(8) Objet du marché.

(9) Réception définitive des commandes ou expiration du délai de garantie.

