TERMES DE REFERENCE
POUR L'INSTALLATION D'UN SYSTEME
DE VIDEO SURVEILLANCE ET DE CONTROLE D'ACCES
AU SIEGE DE L'OAPI

Juin 2016

1- Contexte

L'Organisation Africaine de la Propriété Intellectuelle (OAPI) est une organisation intergouvernementale spécialisée dans le domaine de la propriété intellectuelle. Elle est constituée à ce jour de dix-sept (17) Etats membres et son siège est à Yaoundé.

L'OAPI a pour missions :

- la délivrance des titres de propriété industrielle;
- la contribution à la promotion de la protection de la propriété littéraire et artistique;
- la mise à disposition de la documentation et la diffusion de l'information ;
- la formation en propriété intellectuelle ;
- la participation au développement économique des Etats membres.

Au regard du caractère sensible des données gérées par l'Organisation, la sécurité des biens et de l'accès aux informations est une composante primordiale de son activité. Pour cette raison, l'OAPI souhaite investir dans une solution permettant d'assurer la vidéo surveillance et le contrôle d'accès.

La proposition doit pouvoir exploiter la convergence entre la vidéosurveillance et le contrôle d'accès; les deux solutions devant totalement être interopérables.

L'objet du présent document est de définir les termes de référence relatifs à l'installation d'un système de vidéo surveillance et de contrôle d'accès au siège de l'OAPI.

Le document définit le cadre de la prestation demandée pour répondre aux besoins notamment en termes de performances, fiabilité et respect des normes.

2- Description de l'existant

Le bâtiment à protéger comprend : trois (3) sous-sols pour les parkings, un rez-de-chaussée et sept (7) étages. Il est équipé d'un réseau informatique de type VDI de dernière génération bâti autour des technologies Cisco.

Les équipements du réseau sont répartis entre onze (11) locaux techniques intermédiaires (LTI) dont huit (8) situés à l'une des extrémités de chaque pallier

et trois (3) dans les sous-sols et le local technique principale (LTP) situé dans la salle serveur.

Les switches aux niveaux des LTI sont de type Cisco 2960 POE 24 ports et ceux du cœur du réseau situé au LTP sont de type Cisco 3750 12 S avec 12 ports fibre optique. La liaison entre chaque LTI et le LTP est une dorsale en fibre optique.

3- Zones sensibles et malveillances associées

Les zones à contrôler sont :

- les zones des bureaux situées à chaque étage
- le hall central
- les sous-sols
- l'extérieur (façades avant, arrière et latérale)

avec comme malveillances potentielles identifiées :

- le vol de biens matériels
- le vol d'information
- autre malveillance volontaire (destruction de biens, altération des données, etc.)

4- Définition du besoin

Dans le but de sécuriser le site contre les intrusions et autres types de malveillances, l'OAPI souhaite mettre en place un système de vidéosurveillance couplé à un système de contrôle d'accès. Le système devra permettre :

- la consultation des enregistrements et des contrôleurs de badge sur une plateforme matérielle mutualisée ;
- l'identification des personnes se retrouvant dans une zone donnée ;
- la conservation des enregistrements (conservation souhaitée : 30 jours) ;
- une interopérabilité logicielle entre les 2 lots techniques (Vidéo←→C.A.).

Le système à installer devra être à mesure de couvrir les besoins au niveau de sécurité souhaité.

Les objectifs en matière de sécurité sont :

OBJECTIF n°1 – Surveiller les accès principaux et les zones de circulation dans le bâtiment

- Caméra discrète s'intégrant à l'architecture du bâtiment (mini dôme compact)
- Gestion des circulations dans le bâtiment (audit des enregistrements)
- Enquêter en cas d'incident de sécurité ou de vol

OBJECTIF n°2 – Surveiller les Zones de Parking

- Dissuasion contre la malveillance (au travers d'une caméra mini dôme visible)
- Relecture des enregistrements

OBJECTIF n°3 – Surveillance extérieure

- Dissuasion contre la malveillance (au travers d'un dôme PTZ visible)
- Surveillance des zones extérieures

Le listing des équipements est décrit dans le tableau ci-après :

EQUIPEMENTS VIDEO	**Quantité / Objectif 1**	**Quantité / Objectif 2**	**Quantité / Objectif 3**	**TOTAL**
Nombre de caméras par objectif	24	15	10	**49**
Nombre de postes de visualisation des caméras	2	2	Utilisation du poste cité en Objectif 2	**4**
Serveurs d'enregistrements	1	Utilisation du poste cité en Objectif 1	Utilisation du poste cité en Objectif 1	**1**

EQUIPEMENTS CONTRE D'ACCES	Lecteur Etage	Lecteur Salle informatique	Lecteur porte centrale	Total
Nombre de contrôleurs	15	2	1	**18**
Nombre de lecteurs de badge	30	4	2	**36**
Bouton de sortie	15	2	1	**18**
Déclencheur Manuel (boitier brise-glace)	15	2	1	**18**
EQUIPEMENTS RESEAU				
Switch CISCO 2960 POE 24 ports	4			**4**
Panneau de brassage Legrand	5			**5**
Accessoires de câblage				

5- Descriptif de la solution

5.1- Besoin en cameras

Caméras Objectif 1 : Les caméras de l'Objectif 1 seront des caméras "de circulation" elles seront au minimum de type Axis P3214-V ou Samsung SND6011R à 15ips (images par seconde) ou équivalent.

Caméras Objectif 2 : Les caméras de l'Objectif 2 seront des caméras "de sécurité" elles seront au minimum de type AXIS P3363-V 6mm ou Samsung SNV5084 à 15ips (images par seconde) ou équivalent.

Caméras Objectif 3 : Les caméras de l'Objectif 3 seront des caméras "environnementales" elles seront au minimum de type AXIS Q6044-E ou Samsung SNP6200RH à 15ips (images par seconde) ou équivalent.

5.2- Solution VMS et «hardware»

Dans le cadre de ce projet nous avons qualifié pour la partie VMS un logiciel de type Milestone XProtect Professional ou équivalent qui :

- permet une intégration d'un maximum de marques de caméras ;
- soit une plateforme logicielle ouverte capable de s'interfacer avec divers lots techniques tels que le contrôle d'accès ou l'intrusion et bien d'autres encore ;
- permet une gestion conviviale et en multifenêtrage du mur d'image.

Le hardware associé devra remplir les fonctions suivantes :

- posséder un logiciel middleware permettant : une installation rapide du VMS, une solution de back-up intégrée, tous les outils de découverte des principaux fabricants de caméras;
- gérer les applications VMS + Contrôles d'accès en centralisé sur le même serveur type IPRack ou équivalent ;
- gérer les applications d'exploitation VMS + contrôle d'accès sur une même station de travail type IPbox ou équivalent ;
- Avoir une solution RAID 5 (hardware et non pas logicielle) dédiée sur le serveur.

5.3- Solution de contrôle d'accès

La solution de Contrôle d'accès devra disposer des fonctionnalités suivantes :

- une UTL (Unité de traitement local) par porte, permettant d'éviter un blocage de toutes les portes du bâtiment au cas où toutes les portes auraient été gérées par une seule UTL;
- chaque UTL devra alimenter le lecteur de badge en POE;
- chaque UTL devra distribuer par porte : un lecteur de badge, un bouton de sortie et un déclencheur manuel;
- un dispositif de personnalisation et de reprogrammation des badges;
- un dispositif d'impression associé.

Le logiciel de contrôle d'accès de type NET2PRO ou équivalent, devra être interfacé avec le logiciel de VMS.

5.4- Flux vidéo, liaisons et sécurité réseau

Le réseau existant est subdivisé en plusieurs VLAN dont l'un est dédié au flux vidéo et au contrôle d'accès.

La pose du câble reliant les équipements d'extrémité (caméras, contrôleurs, etc) au réseau tout comme la fourniture et l'installation du matériel complémentaire cité plus haut font partie de la présente consultation.

Pour cela, les soumissionnaires devront justifier de leur compréhension du réseau logique existant et de leur capacité à intégrer leur prestation dans le système actuellement en place. Ils devront en outre justifier de la présence dans leurs équipes du personnel ayant des qualifications requises pour intervenir sur un tel réseau.

5.5- Visualisation

La visualisation des flux vidéo en temps réel et en relecture, ainsi que le pilotage du contrôle d'accès se feront sur des machines équipées au besoin de deux (2) écrans.

Ces station de travail seront de type IPbox ou équivalent, et permettront de mutualiser les applications de vidéo protection et de contrôle d'accès.

5.6- Certification et autorisation du fabricant

Les soumissionnaires du marché devront justifier dans leur offre la possession des certifications de la part des fabricants listés dans le présent document à savoir Milestone ou équivalent, Axis/Samsung ou équivalent, IPbox ou équivalent, etc.

Les certificats devront nécessairement être signés par les fabricants eux-mêmes.

Il est également recommandé de joindre le certificat d'origine des produits et il est souhaitable que ces produits proviennent des pays membres de l'union européenne, des USA, du Japon ou de la République de Corée.

6- Transfert de compétences

L'exploitation du système étant assurée par les équipes de l'OAPI, la présente consultation inclue une prestation de formation pour au moins dix (10) personnes couvrant notamment les aspects suivants :

- le suivi des opérations usuelles;
- l'administration du système;
- le paramétrage des fonctions clés.

Cette formation devra durer le temps nécessaire pour que ces personnes soient à mesure de maîtriser les installations et user d'un savoir-faire sans assistance de la part du prestataire.

7- Garantie et Maintenance du système

Outre les garanties légales qui s'appliqueront aux équipements, la consultation intègre de base les prestations de maintenance suivantes :

- Maintenance des équipements par échange anticipé;
- Mises à jour mineures;
- Mises à jour contextuelles et dynamiques;
- Assistance à l'accès au support technique.

La période de garantie est fixée à un an. Pendant la période de garantie, en plus des visites mensuelles d'entretien préventif, le prestataire devra procéder aux réparations y compris les pièces de rechange.

8- Constitution du dossier et critères d'évaluation

Les offres devront contenir :

- ✓ une copie certifiée conforme de l'extrait d'inscription au registre de commerce ;
- ✓ la situation vis-à-vis de l'administration fiscale ;
- ✓ la situation vis-à-vis de la Caisse Nationale de Prévoyance Sociale ;
- ✓ la soumission faisant connaître les noms, prénoms, qualité, domicile, nationalité du soumissionnaire, la dénomination et le siège du bureau, s'il s'agit d'une personne morale ;
- ✓ les moyens humains et matériels (joindre les CV du personnel et les attestations d'appartenance) ;
- ✓ les références techniques, nature des travaux déjà réalisés, dates, lieux et preuves ;
- ✓ les agréments de représentation s'il y a lieu ;
- ✓ le justificatif de paiement des frais de participation à l'appel d'offres d'un

montant de 100.000 FCFA versé dans le compte de l'OAPI ouvert à ECOBANK sous le numéro 10029000200110132600051802 clé 25 ;

- ✓ l'offre financière devra contenir les coûts estimatifs en francs CFA, hors taxe et hors douane.

Les offres devront parvenir à l'adresse : OAPI, Place de la Préfecture Nlongkak, B.P. 887 Yaoundé - Cameroun, Tél. +237 222 20 57 00, au plus tard le 15 juillet 2016 à 12h00.

Elles devront obligatoirement être présentées sous plis fermés portant uniquement la mention : «**Appel d'offres public en vue du choix d'une entreprise pour l'installation d'un système de vidéo surveillance et de contrôle d'accès au siège de l'OAPI. (A n'ouvrir qu'en commission) ».**

L'OAPI choisira librement l'offre du soumissionnaire qui lui paraîtra la suivant les critères ci-après :

N°	**Critères**	**Note**
1	Présentation générale de l'offre	/5
2	Compréhension des objectifs de la mission	/20
3	Références professionnelles du soumissionnaire et de son personnel clé.	/30
4	Eléments du coût (conditions et facilités de paiement)	/35
5	Chronogramme d'intervention	/10
	TOTAL	/**100**

L'ouverture des offres aura lieu le 15 juillet 2016 à 15 heures au siège de l'OAPI.

Les résultats du présent appel d'offres seront publiés à l'adresse : www.oapi.int.

En cas d'annulation de l'appel d'offres, les soumissionnaires ne pourront prétendre à aucune indemnité.