BCEAO

BANQUE CENTRALE DES ETATS
DE L'AFRIQUE DE L'OUEST

CAHIER DES CHARGES

POUR LES TRAVAUX DE RÉALISATION DU DISPOSITIF DE SÛRETÉ DE L'AGENCE AUXILIAIRE DE LA BCEAO À ABENGOUROU EN REPUBLIQUE DE COTE D'IVOIRE

MAI 2022

Avenue Abdoulaye FADIGA
BP 3108 – Dakar - Sénégal

Tél. (221) 33 839 05 00 / Fax. (221) 33 823 93 35
courrier.bceao@bceao.int - www.bceao.int

1. Objet

La Banque Centrale des États de l'Afrique de l'Ouest (BCEAO) lance un appel d'offres pour les travaux de réalisation du dispositif de sûreté de l'Agence Auxiliaire de la BCEAO à Abengourou en République de Côte d'Ivoire dans le cadre du projet de réhabilitation dudit site.

Ces travaux visent à doter l'Agence d'un dispositif intégré de sûreté intelligent, fiable, efficace et exploitable à partir d'une plate-forme d'hypervision. Il s'agit de :

- la fourniture et l'installation d'une solution numérique de vidéosurveillance de haute définition ;
- la fourniture et l'installation d'un système de contrôle d'accès intégrable dans une plate-forme d'hypervision ;
- la fourniture et l'installation d'un système de détection d'intrusion intégrable dans une plate-forme d'hypervision ;
- la fourniture et l'installation d'un système d'hypervision de la sécurité banque ;
- la fourniture et l'installation de dispositifs de protection anti-véhicule bélier pour la mise en défense des accès ;
- la fourniture et l'installation d'équipements de haute sécurité pour le monitoring et le blocage à distance des portes fortes des locaux de conservation des valeurs ;
- la fourniture et l'installation d'équipements de radiocommunication UHF/VHF et HF numériques ;
- la fourniture et l'installation d'un système électronique de gestion des clés ;
- la fourniture et l'installation de bloc-portes offrant un niveau de résistance mécanique et pare-balle approprié ;
- la fourniture et l'installation de vitrages blindés avec des niveaux de résistance pare-balle en adéquation avec les risques couverts ;
- la fourniture et l'installation d'équipements d'inspection radioscopique et de détection de métaux sur les personnes et le fret ;
- la fourniture et l'installation d'un système de contrôle de rondes ;
- la formation du personnel, utilisateur, exploitant et administrateur du système ;
- la fourniture de l'ensemble des logiciels nécessaires ainsi que des licences d'exploitation associées ;
- le déplacement, la réinstallation et la dépose des installations existantes ainsi que la satisfaction des besoins temporaires de sûreté, selon chaque phase du projet de réhabilitation des locaux de l'Agence, décrite au point 4 du présent cahier des charges ;
- le nettoyage ou la remise en état des locaux et des infrastructures salis ou détériorés au cours des travaux.

L'ensemble des prestations nécessaires à l'exécution de ces travaux sera assuré dans des conditions en tout point conformes aux exigences du présent Cahier des Charges, et en particulier :

- l'installation et le paramétrage des équipements et des logiciels ;
- la réalisation de tous les raccordements nécessaires au bon fonctionnement des matériels, y compris les raccordements électriques et de mise à la terre ;
- les tests et essais de tous les équipements et installations mis en place ;

- la fourniture de la documentation complète en français ;
- le dossier des ouvrages exécutés (DOE) et les documents nécessaires à l'établissement du dossier d'intervention ultérieure sur l'ouvrage (DIUO) ;
- la maintenance des équipements et logiciels dans une logique de service après-vente.

Les installations et équipements à déployer doivent être adaptés, performants, modernes, évolutifs, ergonomiques et d'une maintenance aisée.

L'objectif du présent document est de préciser la consistance des travaux et présenter les spécifications fonctionnelles et techniques des installations et équipements. Il indique les caractéristiques a minima, auxquelles devront satisfaire les installations et équipements de sûreté, objet du présent appel d'offres.

Les solutions proposées doivent assurer la fiabilité et la durabilité techniques ainsi que la disponibilité du support de maintenance pour les installations, équipements et logiciels sur une période d'exploitation d'au moins dix (10) ans. Ces produits doivent être de marques réputées compatibles aux standards de sûreté.

2. Décomposition des travaux

Les travaux du lot de la sûreté porteront sur les volets ci-dessous qui sont indissociables :

- Volet 1 : Vidéosurveillance.
- Volet 2 : Mise en défense et système de contrôle d'accès.
- Volet 3 : Détection d'intrusion.
- Volet 4 : Système d'Hypervision.
- Volet 5 : Système électronique de gestion des clés.
- Volet 6 : Portes fortes et Serrures électroniques de haute sécurité.
- Volet 7 : Radiocommunication et interphonie.
- Volet 8 : Équipements d'inspection et de filtrage.
- Volet 9 : Système de contrôle de rondes.
- Volet 10 : Ensembles bloc-portes et menuiseries aluminium vitrées et blindées.

Les spécifications fonctionnelles et techniques des installations, équipements et logiciels concernés sont décrites dans la deuxième partie du présent document.

3. Limite de prestations avec les différents lots

Sont, notamment, visés et compris dans le montant forfaitaire des travaux du lot de la sûreté :

- la fourniture et l'installation, au Poste Central de Surveillance (PCS), de coffrets de protection électrique des équipements et installations ;
- la fourniture et l'installation de tous les coffrets de protection électrique des équipements et installations ;
- la fourniture et la mise en œuvre des canalisations (câbles, chemin de câbles, etc.) reliant les équipements et installations de sûreté aux coffrets de protection ;
- les travaux relatifs aux percements, saignées, fourreautages, scellements, rebouchages des trous et des saignées avec exécution des enduits ;
- les travaux afférents aux busages, tranchées et rebouchages des tranchées pour la mise en place des câbles enterrés ;
- le scellement des appareillages et des raccords divers en résultant ;

- la protection antirouille des différentes pièces en métaux ferreux livrées ;
- l'exécution des regards propres aux travaux du lot, le cas échéant, dont les implantations devront être soumises à la Banque Centrale.

En particulier, l'Entrepreneur attributaire fournira à la Banque Centrale, en temps utile et par volet, tous les plans d'exécution avec les indications nécessaires pour la réalisation des travaux.

4. Phasage des travaux

Les travaux de réhabilitation de l'Agence seront réalisés sur site occupé et se feront sur plusieurs phases. L'entrepreneur chargé de la réalisation du dispositif de sûreté devra s'y conformer et intégrer dans son offre l'ensemble des besoins temporaires de sûreté découlant du phasage des travaux de réhabilitation.

Les différentes phases se déclinent comme suit :

Phases	**Travaux de réhabilitation correspondants**	**Travaux sûreté à prévoir (non exhaustifs)**
Phase 1-A	Travaux bâtiments extérieurs : démolition des locaux infirmerie, restaurant et gymnase ; construction de caniveaux le long de la clôture. Travaux bâtiment fonctionnel : aménagement d'un PCS à l'étage et libération de l'espace du PCS actuel au RdC.	Installation nouveau sas d'accès dans le nouveau PCS, déplacement des installations et équipements de l'ancien PCS vers le nouveau.
Phase 1-B	Construction des bâtiments infirmerie, restaurant, gymnase, PCE et PCF. Transformation de l'extension	Réservations, fourreautage, tirage et installations des nouveaux équipements en fonction de l'avancement des travaux
Phase 2	Mise en service PCE Transformation de zones au RdC en salle de tri et en comptabilité Aménagement d'un guichet G.O temporaire Démarrage des travaux de la villa Chef d'Agence	Installation des équipements terminaux au nouveau PCS Fourniture et installation vitrage blindé, déplacement des anciennes caméras, boutons et pédales pour les G.O Installations nouveaux équipements dans nouvelle salle de tri
Phase 3	Transformation de zones au RdC en Caisse et Comptabilité Conservation d'un guichet à l'actuelle caisse et à l'actuelle comptabilité Finalisation des travaux de la villa Chef d'Agence	Déplacement et réinstallation des caméras dans les zones d'aménagement provisoire, protection lourde des guichets caisse et comptabilité, travaux neufs de vidéosurveillance et d'anti-intrusion de la villa Chef d'Agence.
Phase 4	Construction des locaux techniques, Parkings et PCF Démarrage travaux villa de passage Aménagement guichets G.O	Réservation, fourreautage, tirage de câble. Protection lourde, vidéosurveillance et anti-intrusion définitifs des guichets GO.
Phase 5-A	Travaux voirie & rénovation des locaux Police et courrier Finalisation des aménagements (1ère partie) des zones caisse, compta et hall.	Réservations, fourreautage, tirage et pose des équipements. Installation des équipements terminaux au nouveau PCS.
Phase 5-B	Travaux des zones caisse, compta et hall. (2ème partie) Conservation du box provisoire de la zone caisse Démolition et aménagement des locaux au 1er étage Finalisation des travaux de la villa de passage.	Réservations, fourreautage, tirage et pose des équipements. Maintien anciens équipements Réservations, fourreautage, tirage Pose des équipements de vidéosurveillance, anti-intrusion et protection lourde.

Phases	Travaux de réhabilitation correspondants	Travaux sûreté à prévoir (non exhaustifs)
Phase 6	Démolition actuel local Police Extension de la zone caveaux	Réservation et installation des équipements lourds
Phase 7	Transformation Caisse/Compta Aménagement définitif de la Compta Aménagement quai BP Mise en activité des locaux technique	Pose des équipements, essai et mise en service Réservations, fourreautage, tirage et pose des équipements.,
Phase 8	Transformation de l'ancienne zone énergie en archive/économat/magasin	Dépose des anciens équipements, Réservations, fourreautage, tirage et pose des équipements.
Phase 9	Rénovation 2ème étage. Aménagement bureaux Gouverneur et Chef d'Agence	Réservations, fourreautage, tirage et pose des équipements.
Phase 10	Réhabilitation du local GAB Aménagement 1er étage	Réservations, fourreautage, tirage et pose des équipements.

5. Prescriptions et réglementations

Les travaux décrits dans le présent lot devront être conformes aux normes et réglementations qui leur sont applicables.

Les équipements doivent être installés et solidement fixés sur leurs supports par les moyens prévus dans les notices constructeurs. Ils doivent comporter des indications suffisantes pour être identifiés sans risques d'erreurs (nom du fabricant, modèle, type, etc.).

Sont, notamment, applicables dans leur édition la plus récente, les documents suivants :

- le Code du travail du pays d'implantation du site ;
- tous Normes et Règlements du pays d'implantation du site, relatifs aux domaines considérés ;

les Normes Françaises :

- NFC EN 50132 : Systèmes d'alarme - système de surveillance CCTV à usage dans les applications de sécurité.
- NF C15-100 : Installations électriques à basse tension.
- UTE C 15-520 : Installations électriques à basse tension – guide pratique - canalisations - modes de pose – connexions.
- UTE C 15-900 : Installations électriques à basse tension – guide pratique - cohabitation entre réseaux de communication et d'énergie – installation des réseaux de communication.
- UTE C 18-510 : Recueil d'instructions générales de sécurité d'ordre électrique.
- C 12-100 : Textes officiels relatifs à la protection des travailleurs dans les établissements qui mettent en œuvre des courants électriques,
- C 20-010 : degré de protection du matériel électrique,
- C 48-410 : Système d'alarme - Détection d'intrusion - Fonction contrôleur enregistreur intégrée dans les centrales ou transmetteurs d'alarme,
- NF C 63.410 : ensembles d'appareillages basse tension montés en usine,
- NF C91.101 : perturbations radioélectriques et systèmes d'antiparasitage, textes officiels concernant le matériel alimenté en réseau de première catégorie et dont le rayonnement direct est faible,

- NF C91.104. : perturbations radioélectriques et systèmes d'antiparasitage et textes officiels concernant les appareils servant aux réceptions individuelles ou collectives des émissions et radiodiffusion sonore ou visuelle,
- NF C92.130 : appareils électroniques et appareils associés à usage domestique ou à usage général analogue, reliés à un réseau de règles de sécurité.
- NF P 25-362 : Fermetures pour baies libres et portails, Spécifications techniques, Règles de sécurité,
- C32-321 : Conformité des câbles de distribution basse tension,
- C32-201 : Conformité du conducteur de protection,

les Règles et référentiels APSAD :

- R31 : règle de prescription – télésurveillance,
- R81 : règle d'installation – détection d'intrusion,
- R82 : règle d'installation – vidéosurveillance,
- D83 : contrôle d'accès - document technique pour la conception et l'installation
- D32 : Cybersécurité - document technique pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique.

L'attributaire est tenu de respecter l'ensemble des règlements ci-dessus dont la liste n'est pas exhaustive. En cas de contradiction entre les règlements français et ceux du pays d'implantation, ce sont ces derniers qui prédominent.

Les installations seront réalisées dans les règles de l'art. Les équipements devront être robustes, conformes aux caractéristiques fonctionnelles et techniques décrites ci-après. En outre, leur maintenance devrait être aisée (sécurité, facilité d'accès, interchangeabilité des pièces). Leur durée de vie tenant compte des contraintes d'exploitation, devra être indiquée à la BCEAO.

5. Spécifications fonctionnelles et techniques des installations et équipements

5.1. Vidéosurveillance

Il s'agit de proposer une solution de vidéosurveillance « full IP et POE » assurant, notamment, les fonctions d'aide à la surveillance et à l'identification, d'assistance au contrôle de flux, de levée de doute, de contribution à la gestion d'activité, de détermination de l'origine d'un acte de malveillance, selon la zone d'implantation des équipements. Le soumissionnaire devra prévoir le démantèlement intégral du dispositif analogique existant proposer à la BCEAO une moins-value en contrepartie de sa reprise.

Le système de vidéosurveillance devra présenter au moins une intégrité de niveau 3 au sens de la règle APSAD R82. Les défaillances techniques ainsi que le masquage et le pivotement accidentels de caméra sont signalés.

La couverture vidéo, sans être exhaustive, doit concerner les zones ci-après :

- les façades extérieures de la concession au niveau de tous les accès et des parkings visiteurs ;
- l'entrée du local police ;
- le long des murs de clôture pour une détection de franchissement ;
- les abords de l'immeuble fonctionnel pour une détection d'approche ;
- les zones d'énergie (transformateurs, TGBT, groupes électrogènes, onduleurs, etc.) ;
- les locaux informatiques ;

- le local autocommutateur ;
- l'aire de travail des caveaux ;
- les sas banques primaires et Banque centrale ;
- etc.

Le réseau dédié sur lequel transitera les flux vidéo doit offrir une bande passante suffisante pour une transmission des images de qualité optimale en format compatible aux techniques de compression standard. Ce réseau devra comporter une sécurité des informations garantissant la disponibilité, la confidentialité et l'intégrité des données.

Le dispositif d'enregistrement devra être de type rackable avec un accès aux données et au paramétrage hiérarchisé et protégé par des mots de passe individuels. Les flux vidéo pourront être exportés sans dégradation de la qualité. Le système d'enregistrement restera en fonctionnement lors de ces opérations de copie des images. Il doit être associé à un journal, généré automatiquement sous forme électronique, qui conserve la trace de l'ensemble des actions effectuées sur les flux vidéo. La capacité de stockage devra permettre une conservation des images enregistrées sur une durée d'au moins 45 jours dans les conditions d'enregistrement en continu des caméras avec des exigences de restitution minimale de 12 images par seconde pour les caméras d'identification et 6 pour les autres.

Le système d'enregistrement sera installé dans un local technique situé à l'extérieur du PCS.

La visualisation en direct des images sera effectuée au PCS à l'aide d'un mur d'écrans de type BARCO ou équivalent. Un système de report sélectif sera prévu, notamment pour les bureaux des responsables des sites (Chef d'Agence et son Assistant), le Caissier, le Poste de Contrôle des Entrées (PCE), les bureaux des chargés de la sécurité et de l'informatique ainsi que le local Police.

Un clavier de commande IP avec écran couleur LCD tactile est prévu au PCS pour la gestion du système de vidéosurveillance.

L'Adjudicataire devra fournir, installer et configurer un serveur de gestion de la vidéosurveillance équipé d'un logiciel client/serveur permettant à l'utilisateur de visualiser, de gérer et d'enregistrer des vidéos à partir d'un nombre illimité de caméras IP tout en assurant l'optimisation de la bande passante et la gestion de stockage vidéo à court et à long terme.

Le logiciel permettra :

- la protection des données et la gestion du stockage ;
- l'enregistrement et la lecture à haute définition des vidéos, la distribution des vidéos pour les utilisateurs et la gestion des caméras ;
- la gestion de la bande passante et la visualisation à distance des caméras ;
- l'affichage dynamique des images de haute précision (Multi-Megapixels) ;
- l'accès en direct et la relecture simultanés par de multiples utilisateurs bénéficiant des droits requis ;
- l'investigation, la recherche, la cinétique et la détection de mouvement ;
- l'optimisation des ressources du système grâce à la configuration par caméra au niveau : compression / format / résolution de l'image / bande passante / nombre d'images par seconde / enregistrement sur activité / temps de rétention / fréquence d'archivage ;
- la compatibilité avec des caméras et des appareils ainsi que les formats standards de compression vidéo des principaux fabricants.

En outre, le système client doit offrir une interface utilisateur conviviale, pour les postes des administrateurs et opérateurs : l'accès à la vidéo, la gestion des alertes, la gestion des événements et le contrôle des affichages.

Les caissons de protection des caméras installées à l'extérieur devront avoir les caractéristiques de résistance aux influences externes ci-après : IP66 et IK10.

Le pupitre de commande et de monitoring des images devra permettre une exploitation ergonomique des installations et le respect des distances de surveillance des moniteurs qui doit correspondre à 3,5 fois la diagonale des écrans.

Les images reportées dans le local police concernent exclusivement celles des caméras installées au niveau des accès à la concession, les parkings extérieurs. Aucune autre caméra ne devrait pouvoir y être visualisée.

Des équipements de vidéosurveillance spécifiques sont prévus pour la chaîne de contrôle des fourgons (caméra portative).

La nature et le nombre des caméras seront déterminés par le soumissionnaire sur la base des plans fournis par la BCEAO et des spécifications techniques indicatives données sur le cadre de devis estimatifs joints en annexes.

Pour le cas particulier des zones de la Caisse, le système de vidéosurveillance devrait être physiquement et logiquement distinct de celui des caméras dédiées à la sécurité. Il sera composé des équipements et systèmes décrits ci-après.

5.1.1 Spécifications fonctionnelles et techniques des installations et équipements de vidéosurveillance de la Caisse

5.1.1.1 - Spécifications fonctionnelles

Il s'agit de proposer une solution de vidéosurveillance « full IP et POE » assurant, notamment, les fonctions d'aide à la surveillance et à l'identification, d'assistance au contrôle de flux, de levée de doute, de contribution à la gestion d'activité, de détermination de l'origine d'un acte de malveillance, selon la zone d'implantation des équipements.

Le système de vidéosurveillance de la Caisse doit être physiquement et logiquement distinct de celui des caméras dédiées à la sécurité.

Le système de vidéosurveillance devra présenter au moins une intégrité de niveau 4 au sens de la règle APSAD R82. Les défaillances techniques et les tentatives de vandalisme contre le système sont signalées.

L'Adjudicataire devra fournir, installer et configurer un serveur de gestion de la vidéosurveillance équipé d'un logiciel client/serveur permettant à l'utilisateur de visualiser, de gérer et d'enregistrer des vidéos à partir d'un nombre illimité de caméras IP tout en assurant l’optimisation de la bande passante et la gestion de stockage vidéo à court et à long termes.

Le réseau dédié sur lequel transitent les flux vidéo doit offrir une bande passante suffisante pour une transmission des images de qualité optimale en format compatible avec les techniques de compression standard. Ce réseau devra comporter une sécurité des informations garantissant la disponibilité, la confidentialité et l'intégrité des données.

Le système client doit offrir une interface utilisateur conviviale, pour les postes des administrateurs et opérateurs notamment l'accès à la vidéo, la gestion des alertes, la gestion des événements et le contrôle des affichages.

Un clavier de commande IP muni d'un écran couleur LCD tactile est prévu au bureau du Caissier pour la gestion du système de vidéosurveillance de la zone Caisse.

La station principale de visionnage/surveillance des images est installée dans le bureau du Caissier. Elle est composée d'au moins deux (02) moniteurs de 49 pouces et d'un poste de travail (workstation).

Une station permettant la visualisation des caméras d’ambiance de la Caisse, de la salle de tri et des quais de chargement/déchargement, est installée au PCS.

En outre, le dispositif de vidéosurveillance devra avoir les fonctionnalités et caractéristiques ci-après :

Couverture vidéo, caméras

La couverture vidéo, sans être exhaustive, doit concerner les zones ci-après :

- les zones de chargement et de déchargement des valeurs : quai Banque Centrale, quai banques primaires ;
- les zones de circulation du périmètre de sécurité de la Caisse : sas caveaux, couloirs des guichets grosses opérations, couloirs de la caisse courante et de la salle de tri ;
- les zones de traitement de valeurs : guichets des opérations, aires de tri, tables de contrôle, tables de reddition, locaux de perforation des billets, aires de préparation des valeurs aux caveaux ;
- etc.

Ces caméras auront une résolution d'au moins 3 Mégapixels.

Les caméras des zones de circulation et des accès devront permettre d'identifier sans équivoque les agents ainsi que l'ensemble des gestes effectués, y compris les gestes rapides.

Les caméras des zones de manipulation de valeurs (guichets des opérations, aires de tri, tables de contrôle, tables de reddition, aires de perforation des billets) doivent être installées à une bonne hauteur leur permettant, entre autres, de distinguer sans ambiguïté le nombre de ganses de chaque paquet de billets, de lire les étiquettes des paquets (modèle joint en annexe 2) et la valeur faciale des billets manipulés. A toutes fins utiles, il convient d'indiquer que la hauteur du faux plafond dans ces zones est de 3,5 mètres.

Sur chaque table de tri manuel, une caméra devra être affectée à la surveillance des activités d'au plus deux (2) agents de tri (trieuse ou contrôleuse).

Chaque machine de tri devra être surveillée par deux (2) caméras au moins et chaque cercleuse par une (1) caméra.

Chaque perforatrice devra être surveillée par deux (2) caméras.

Les caméras d'ambiance sont de type fixe, infra-rouge et devront permettre une surveillance intégrale des aires de traitement des valeurs.

Une caméra dôme motorisée est également prévue à la caisse courante et une autre à la salle de tri, pour le tracking et la levée de doute.

Report de la vidéosurveillance, moniteurs

Les moniteurs seront à haute performance au plan écologique (faible consommation énergétique, faible dégagement thermique) et d'un bon niveau de fiabilité. Ils devront restituer fidèlement les images des caméras (netteté et précision).

Un report de la vidéosurveillance de la zone de la Caisse est prévu dans les bureaux des Chefs d'Agence Auxiliaire et de leurs Assistants, des Caissiers, des Chefs de tri et des Caissiers des grosses opérations.

Dispositif de stockage, de sauvegarde et d'archivage

L'offre devra comporter une description détaillée du dispositif de stockage (type de disques proposés), de sauvegarde et d'archivage ainsi que des mécanismes de sécurité, notamment la détection et la prise en charge des vulnérabilités.

Le système d'enregistrement est prévu en double (nominal et backup) dont l'un est installé dans le local abritant les enregistreurs des images de la sécurité et l'autre dans un local dédié à la Caisse.

Le dispositif d'enregistrement devra être de type rackable avec un accès aux données et au paramétrage hiérarchisé et protégé par des mots de passe individuels. Les flux vidéo pourront être exportés sans dégradation de la qualité. Le système d'enregistrement restera en fonctionnement lors de ces opérations de copie des vidéos. Il doit être associé à un journal, généré automatiquement sous forme électronique, qui conserve la trace de l'ensemble des actions effectuées sur les flux vidéo.

Les enregistreurs devront présenter de hautes performances dans le domaine du respect de l'environnement (faible consommation électrique, faible dégagement thermique, faible niveau sonore). Ils devront être dotés d'une protection par une clé physique.

Les enregistreurs devront permettre un archivage simple et sécurisé sur des supports extractibles modernes, être faciles d'entretien, présenter un faible encombrement et une nuisance sonore réduite. Ils devront être dotés de supports amovibles permettant le stockage de séquences ciblées.

Le dispositif devra permettre une conservation des images enregistrées dans les conditions d'enregistrement en continu des caméras avec des exigences de restitution minimale de 12 images par seconde sur une durée de 90 jours pour les caméras des zones de traitement des valeurs et de 45 jours pour les autres zones.

Logiciel d'exploitation

Le logiciel d'exploitation du dispositif de vidéosurveillance devra permettre :

- la protection des données et la gestion du stockage ;
- l'enregistrement et la lecture à haute définition des vidéos, la distribution des vidéos pour les utilisateurs et la gestion des caméras ;
- la gestion de la bande passante et la visualisation à distance des caméras ;
- l'affichage dynamique des images de haute précision (Multi-Mégapixels) ;
- l'accès en direct et la relecture simultanés par de multiples utilisateurs bénéficiant des droits requis ;
- l'investigation, la recherche, la cinétique et la détection de mouvement ;
- l'optimisation des ressources du système grâce à la configuration par caméra au niveau : compression / format / résolution de l'image / bande passante / nombre d'images par seconde / enregistrement sur activité / temps de rétention / fréquence d'archivage ;
- la compatibilité avec des caméras et des appareils ainsi que les formats standards de compression vidéo des principaux fabricants.

En outre, il devra :

- être multi-utilisateurs ;
- disposer de fonctionnalités de post-visualisation étendues et comporter des fonctions avancées de planification, de configuration et de traitement des événements ;
- permettre un archivage des images, un enregistrement en continu et sur détection de mouvements dans l'image ;
- offrir la possibilité d'habilitation pour plusieurs niveaux d'accès et de manipulation ;
- offrir la possibilité de sauvegarder, de restituer et d'exporter les séquences vidéo sous les formats vidéo les plus courants (DIVX, AVI, MKV, MP4) sans en altérer la qualité.

5.1.1.2 - Spécifications techniques minimales des caméras

Les caméras devront être fixes, destinées à une utilisation intérieure et présenter les caractéristiques minimales suivantes :

Pour les zones de manipulation de valeurs

- Caméra fixe IP POE infrarouge ;
- Résolution Full HD 1080p, 25/30 images/s avec un capteur d'au moins 3 mégapixels ;
- fonction : jour/nuit ;
- objectif : mise au point et zoom ;
- réglage vidéo : luminosité, contraste, couleur, netteté, saturation, etc. ;
- température de fonctionnement : 0°C à +50°C.

Pour les accès et zones de circulation

- Caméra fixe IP POE infrarouge ;
- Résolution Full HD 1080p, 25/30 images/s avec un capteur d'au moins 3 mégapixels ;
- objectif : zoom varifocal ;
- réglage vidéo : luminosité, contraste, couleur, netteté, saturation, etc. ;
- température de fonctionnement : 0°C à +50°C.

Pour le «tracking» dans la caisse courante et dans la salle de tri

- Caméra IP POE dôme mobile PTZ ;
- Résolution Full HD 1080p, 25/30 images/s avec un capteur d'au moins 3 mégapixels ;
- fonction : jour/nuit ;
- objectif : zoom optique 25X, 6-140 mm, F1,6-F4,8
- réglage vidéo : luminosité, contraste, couleur, netteté, saturation, etc. ;
- température de fonctionnement : 0°C à +50°C.

Le soumissionnaire fournira :

- le schéma de principe du câblage indiquant de manière claire les spécifications des câbles utilisés ;
- le schéma de principe du système global, indiquant clairement tous les composants proposés.

5.2. Mise en défense et système de contrôle d'accès

Les travaux prévus concernent la fourniture et l'installation d'un système de mise en défense et de contrôle d'accès intégrable à un système d'hypervision.

Le système de mise en défense est constitué de bornes escamotables anti-terroristes interdisant tout passage non autorisé au niveau des points ci-après :

- Entrée secondaire,
- Sortie secondaire,
- Portail PCF côté concession.

Les bornes sont prévues en nombre suffisant de manière à empêcher l'accès de tout véhicule bélier, conformément à la norme PAS 68 ou équivalent. Ces bornes sont associées à des feux bicolores transmettant leur position.

S’agissant des bornes de l’entrée et de la sortie secondaires, elles seront mises en service par des commutateurs à clé installés dans les postes de garde correspondants et seront commandées par lecture de badges et leur retour à la position de défense asservi à la fermeture complète de la barrière associée.

Quant aux bornes installées au PCF, elles sont commandées par bouton à clé depuis le poste de garde dudit PCF.

Le système de contrôle d’accès est déployé à travers une architecture matérielle composée de lecteurs de badges, d'Unités de Traitement Locales, d'un poste Serveur et des postes clients ainsi que d'un logiciel.

Le lecteur devra avoir une consommation très faible (0,25W) et être de type proximité passif avec une distance de lecture de l’ordre de 3 à 5 cm. Il devra avoir un aspect soigné ainsi qu’une bonne résistance aux intempéries et aux dégradations extérieures.

Le soumissionnaire proposera tout le matériel nécessaire pour un service autonome de personnalisation des badges.

Le poste serveur sera raccordé sur un réseau de type Ethernet TCP/IP. Il disposera d’une capacité de stockage mémoire permettant le bon fonctionnement des applications. Les postes clients sont installés au PCE (2), au bureau du responsable de la sécurité (1). Ces postes devront avoir toutes les caractéristiques nécessaires pour un bon fonctionnement du système de contrôle d'accès.

Le logiciel de contrôle d'accès devra être compatible avec le système d'hypervision et permettre la mise en œuvre des fonctionnalités suivantes :

- gestion des détenteurs de badge ;
- assistants d’installation et de configuration rapides intégrés ;
- surveillance des événements d’accès en temps réel ;
- contrôle et réponse, y compris acquittement, suppression et annotation ;
- vue/rapport de suivi et de rassemblement ;
- annulation manuelle de fonctions et de programmes horaires :
    - ➔ modes porte : Verrouillé, Désactivé, PIN seul, Carte et PIN , Carte ou PIN , Carte seule ;
- fonctions de reporting avancées :
    - ➔ rapports prédéfinis ou personnalisés des mouvements des badges ;
    - ➔ rapports prédéfinis ou personnalisés du temps de présence des détenteurs de badges ;
    - ➔ programmation de l’envoi par e-mail des rapports prédéfinis ;
    - ➔ exportation au format HTML ou délimité par séparateurs, compatible aux tableurs ;
- traitement anti-passback :
    - ➔ hard ou soft par lecteur ;
    - ➔ annulation du mode apprentissage ;
- aide contextuelle ;

- plans dynamiques :
    - ➔ périphériques de contrôle d'accès ;
    - ➔ lien vers les plans ;
- numéros de badge jusqu'à 20 chiffres ;
- basculement du verrouillage pendant la programmation déverrouillage – mode heure du déjeuner ;
- basculement du verrouillage en dehors de la programmation – mode en dehors des heures ouvrées ;
- interrogation de la base de données des badges ;
- procédures par événement/programme définies par l'utilisateur ;
- 3 types de congés ;
- identification par badge multi-technologie ;
- événements d'alarme prioritaires ;
- logiciel multilingue incluant obligatoirement le français.

Les portails seront proposés en modèle industriel préfabriqué, motorisé, autoportant de préférence, avec incrustation d'un logo conforme à l'identité visuelle de la Banque Centrale.

Le soumissionnaire fournira l'ensemble des équipements nécessaires pour le contrôle d'accès au niveau des points ci-après, selon les plans détaillés communiqués par la BCEAO et les spécifications techniques fournies à titre indicatif dans le cadre de devis estimatifs, en annexes.

5.2.1 Poste de Contrôle des Entrées (PCE)

Deux (2) tourniquets simples Te et Ts pour l'entrée et la sortie des piétons, sont installés dans le hall côté piéton du bâtiment. Une portillon de secours est associée à chaque tourniquet.

Pour l'entrée et la sortie des véhicules, il est prévu :

- 2 portails principaux (métalliques, tôlés double faces) motorisés autoportants de type industriel avec logo ;
- 2 portails secondaires (grilles) motorisés autoportants de type industriel sans logo ;
- 2 barrières principales avec herse ;
- 2 barrières secondaires simples ;
- 4 bornes escamotables anti-véhicules béliers.

Les commandes à boutons des portails, barrières et bornes escamotables seront reportées au PCS où sera offerte la possibilité d'une prise en main prioritaire à l'aide d'un commutateur qui inhibera toute commande locale à partir du PCE.

Le système de contrôle d'accès présentera, au sens du document D83, une classe de reconnaissance de niveau II, une classe B du droit d'accès, une résistance aux attaques logiques d'au moins L2 et une résistance aux attaques destructives d'au moins de niveau III.

5.2.2 Poste de Contrôle des Fourgons (PCF)

La porte d'entrée au poste de garde du PCF est de type monobloc de résistance au souffle EPR2 et de résistance à l'effraction CR5, équipées d'un ferme porte hydraulique, d'un verrouillage et de commandes conformes aux exigences de sûreté. Les châssis seront adaptés à ce type d'ouvrants afin de respecter une homogénéité de structure.

Les Portails formant SAS d'accès des fourgons sont de type industriel autoportants, tôlés et barreaudés fermant hermétiquement les accès et ne présentant pas d'interstice.

Le premier portail est commandé à partir du poste de contrôle et le second portail par le PCS après exécution des opérations de contrôle des fourgons (caméra portative, borne d'authentification des convoyeurs). Le portail situé du côté intérieur de la concession est précédé dans le sas par deux bornes de protection anti-véhicule bélier (conforme à la norme PAS 68).

Les commandes à boutons des portails et des bornes anti-véhicule bélier seront reportées au PCS où sera offerte la possibilité d'une prise en main prioritaire à l'aide d'un commutateur qui inhibera toute commande locale à partir du PCF.

Le système présentera, au sens du document D83, une classe de reconnaissance de niveau II pour les piétons et de niveau III pour les convoyeurs, une classe C du droit d'accès, une résistance aux attaques logiques L3 et une résistance aux attaques destructives d'au moins de niveau III.

5.2.3 Bâtiment fonctionnel

Il est mis sous le contrôle du PCS, l'intégralité des accès périmétriques à l'immeuble fonctionnel. Toutes les portes situées sur la périmétrie des immeubles fonctionnels sont contrôlées à distance à partir du PCS où sont également renvoyées leurs positions physiques pour un contrôle permanent de leur état.

Il est installé à l'entrée du périmètre de sécurité, une barrière constituée d'un tourniquet à entrée/sortie. Le tourniquet est associé à une porte contrôlée pour le passage des objets encombrant et pour servir d'issue de secours en cas d'urgence.

Des déclencheurs manuels d'ouverture d'urgence aux couleurs conventionnelles (fond vert, écriture ou symbole blanc) et à double commande, sont prévus sur le côté intérieur de chaque porte du cheminement d'évacuation des locaux de la caisse. Chaque utilisation de ces commandes déclenche une alarme sonore au PCS et est tracée par le système de vidéosurveillance.

5.2.4 Local Informatique

Un contrôle d'accès bi-directionnel discriminé est mis en place au niveau de la porte d'accès principal à la zone avec un lecteur biométrique à l'entrée et un lecteur simple en sortie. Au niveau de l'entrée de la salle serveur, il est installé un contrôle d'accès de classe de reconnaissance de niveau III et de classe C du droit d'accès, avec une résistance aux actes de malveillance d'au moins de niveau III. Il est prévu un lecteur simple dans le sens de la sortie. Tous les lecteurs de sortie sont associés à des blocs d'ouverture d'urgence à double action.

5.2.5 Poste Centrale de Surveillance

L'entrée du PCS est équipée d'un SAS à unicité de passage + biométrie avec une tenue balistique du cadre certifiée classe FB6 selon norme européenne EN 1522. Passage L= 700 mm minimum et parois intérieures de résistance pare-balle classe BR6 NS (polycarbonate sur une face). La porte d'accès au sas présente un degré antieffraction P8B selon normes européenne EN 1063 et EN 356.

Le système présentera, au sens du document D83, une classe de reconnaissance de niveau III, une classe D du droit d'accès, une résistance aux attaques logiques L3 et une résistance aux attaques destructives d'au moins de niveau IV.

5.2.6 Autres Portails et portes

L'accès au quais de chargement/déchargement des fourgons Banque Centrale et des camions banques primaires s'effectuera à travers un portail barreaudé et tôlé 2 faces, de dimensions permettant le passage des véhicules sus-visés. Il est coulissants à commande duale PCS/Caisse.

Ce portail d'accès au quai banques primaires et banque centrale est motorisé et inter-verrouillé avec la porte située en aval du quai et menant au reste de l'immeuble fonctionnel.

Le soumissionnaire fournira, les équipements et installations dont les spécifications techniques données, à titre indicatif, figurent dans le cadre de devis estimatif en annexes.

5.3. Détection d'intrusion

Il sera mis en place une installation de détection d'intrusion pour détecter et signaler l'approche, la pénétration et/ou le déplacement d'un intrus dans les secteurs sensibles du site, notamment les locaux de la caisse, la zone de l'informatique, les locaux techniques dédiés à l'énergie électrique et à la communication, et les résidences de fonction.

Le matériel devra être NF A2P comportant 3 boucliers au sens de la règle APSAD R81. La centrale d'alarme, exclusivement de type filaire, d'une capacité suffisante, doit pouvoir assurer :

- une surveillance de pénétration de type 4 du bâtiment principal et des résidences de fonction ;
- une surveillance de mouvement de type 4 pour la comptabilité, le local informatique, la zone de traitement des valeurs, l'aire de stockage des valeurs ;
- une surveillance surfacique sur les 6 faces des aires de stockage des valeurs.

Elle commandera des sirènes intérieures judicieusement réparties et des sirènes extérieures. Les sirènes extérieures sont sonores et lumineuses. L'alimentation de la centrale doit avoir une autonomie suffisante.

Un transmetteur d'alarme approprié et offrant toutes les garanties de sécurité, doit permettre le report de l'alarme au cantonnement de la Force de Sécurité Publique compétent pour l'intervention.

L'unité de commande principale de la Centrale d'alarme est installée au PCS. Un report de l'information de la centrale est prévu dans les lieux ci-après :

- bureau du responsable du site ;
- bureau du responsable de la caisse ;
- bureau du responsable de la sécurité.

Un report lumineux et sonore est prévu dans chaque poste de garde et dans le local Police.

Des boutons d'alarme placés hors de vue du public sont installés dans tous les postes de gardes tenue par le personnel de la BCEAO (PCE, PCF).

Des boutons d'alarme et des pédales sont également prévus et judicieusement répartis dans les différents guichets (opérations diverses et gros paiements/versements).

Seules, les alarmes (détecteurs automatiques et boutons) de la zone de traitement des valeurs sont directement reportées au cantonnement (commissariat, caserne, etc.) distant de la FSP chargé de l'intervention. Toutes les autres alarmes sont restreintes au PCS et aux reports locaux. Leur transmission au cantonnement distant de la FSP est commandée manuellement à partir du PCS, en cas de besoin.

Une détection localisée dans la zone de traitement des valeurs, doit activer la commande de verrouillage des portes intérieures.

Les matériels du dispositif anti-intrusion sont auto-surveillés à l'arrachement et convenablement protégés contre les influences externes avec les indices IP et IK adéquats.

En sus de la détection d'intrusions, l'ensemble des aires de stockage est doté d'un système d'écoute constitué de microphones judicieusement répartis et d'une sortie de son installée au PCS.

Le système de détection couvrira également les résidences de fonction des Responsables d'Agence, à travers une partition autonome avec un clavier de report et de commande, une sirène extérieure, des détecteurs de présence et de bris de glace, des contacts de portes et de deux boutons d'alarme installés dans la chambre des parents et la loge des gardiens. L'Adjudicataire fournira pour chaque site, un simulateur de bris de vitre type FG701 ou équivalent. Le déclenchement d'une alarme à partir de cet îlot, sera transmis exclusivement au PCS du site.

Le soumissionnaire fournira, les équipements et installations dont les spécifications techniques, données à titre indicatif, figurent dans le cadre de devis estimatif en annexes.

5.4. Système d'hypervision

Il s'agit, sur la base d'une approche cohérente et intégrée de la sûreté, de mettre en place une solution dédiée de supervision graphique permettant de gérer l'ensemble des dispositifs électroniques de sûreté dont les modules (contrôle d'accès, détection d'intrusion et vidéosurveillance) sont autonomes.

Le système d'hypervision reposera sur une interface homme/machine ergonomique, conviviale, qui permettra de centraliser, contrôler et commander tous les dispositifs de sûreté. L'hyperviseur intégrera et analysera différents types d'informations : visualisation géographique, vues des caméras de vidéosurveillance, détecteurs d'intrusion, équipements de contrôle d'accès.

Il devrait notamment assurer les fonctions suivantes :

- gestion des alarmes selon leur type (contrôle d'accès, intrusion ou techniques, incendie) et/ou leur localisation géographique ;
- historiques, avec des critères d'extraction simple et exportables dans un fichier texte ou excel ;
- journal de bord permettant à l'opérateur de saisir librement en main courante un commentaire pour chaque événement ;
- animation de synoptiques représentant des vues et des niveaux des bâtiments ou des tableaux dynamiques permettant une exploitation conviviale avec icônes, animations, télécommandes, changement de couleurs, etc.

Le soumissionnaire fournira et assurera l'installation et le paramétrage :

- d'un logiciel d'hypervision (gestion intégrée des dispositifs de sûreté) avec les caractéristiques suivantes :
    - ➔ compatible ONVIF ;
    - ➔ capable de supporter : caméra IP, système de contrôle d'accès, contrôle PTZ, anti-intrusion, stockeur vidéo, etc. ;
    - ➔ plans synoptiques de supervision graphique ;
    - ➔ Multi-langues ;
    - ➔ Multi-utilisateurs ;
- d'un poste serveur avec des caractéristiques et une capacité de stockage mémoire permettant le bon fonctionnement des applications ;
- d'un Poste client installé au PCS avec des caractéristiques et une capacité de stockage mémoire permettant le bon fonctionnement des applications.

5.5. Système électronique de gestion des clés

L'entreprise devra fournir et installer au Poste Central de Surveillance (PCS), une armoire électronique de gestion des clés sensibles (traka ou key watchers), évolutive d'une capacité, d'au moins, 50 clés.

Le système devrait, au moins, avoir les fonctions ci-après :

- Contrôle d'accès aux clefs, avec données biométriques ;
- Rapport d'utilisation des clefs ;
- Inter-verrouillage ;
- Alarme sur clefs non retournées à l'échéance ;
- Historisation de tous les mouvements avec tri sélectif et statistiques.

Le soumissionnaire fournira, installera et paramétrera :

- une armoire de gestion électronique des clés ;
- un ordinateur de gestion.

5.6. Portes fortes et serrures électroniques de haute sécurité

Le soumissionnaire devra fournir et installer les portes fortes des locaux de conservation des valeurs (caveau et chambre forte caisse courante). Ces portes sont de type OPTEMA 180S de Fichet Bauche ou équivalent et associée à un trappon de secours de type OPTEMA 180S pour les caveaux et pour la chambre forte de la Caisse courante, une porte forte OPTEMA 180 avec un trappon OPTEMA 180.

Les portes des caveaux seront associées à des serrures électroniques de haute sécurité à code, multi-utilisateurs, avec identification biométrique et transcription cryptée des données. Ces serrures seront connectées sur le réseau informatique afin de pouvoir être verrouillées à distance.

Un logiciel de gestion centralisée des serrures électroniques pour leur monitoring à partir du poste principal existant installé au Siège de la BCEAO.

Une commande de blocage/déblocage devrait pouvoir être activée à partir du Siège, de manière sécurisée.

Les équipements à fournir sont :

- des portes fortes ;
- des trappons de secours ;
- des serrures électroniques IP de haute sécurité ;
- des logiciels de gestion d'installation et de paramétrage de serrures ;
- un logiciel de supervision des serrures ;
- des postes de travail.

5.7. Radiocommunication et interphonie

Il s'agira de fournir et installer des équipements de radiocommunication UHF/VHF et HF de type numérique, interconnectables à l'autocommutateur du site et offrant un système de géolocalisation des fourgons via les dispositifs HF.

Pour les équipements UHF/VHF destinés aux postes de sécurité, il est mis en place une base fixe et dix (10) radios portatives.

S'agissant des équipements HF, destinés aux opérations de convoyage de fonds, il est prévu l'installation, d'une base fixe à la structure en charge des convois et des stations mobiles sur les fourgons et les véhicules d'escorte.

Le système de voix et de données de géolocalisation devra être de type numérique avec une sécurité de cryptage AES 256 bits pour tout le réseau.

Le soumissionnaire fournira un logiciel sécurisé qui permettra de faire le suivi par GPS des mobiles (HF) avec un affichage graphique utilisateur sur des cartes importables en fichiers bitmap, JPG, ou équivalent. La supervision graphique de la position en temps réel de tous les fourgons et véhicules suiveurs, est assurée à partir de la station de l'Agence Principale de Niamey.

Il sera fourni et installé :

- des équipements de Radiocommunication UHF/VHF de technologie numérique ;
- des Bases numériques pour radio UHF/VHF ;
- une station relais pour base numérique UHF/VHF ;
- des Équipements de Radiocommunication HF numérique (antenne, bases fixes et mobiles) ;
- un Logiciel de géolocalisation HF.

5.8. Équipements d'inspection et de filtrage

Le soumissionnaire proposera des équipements de contrôle radioscopique à rayons X («X-ray») aux accès piétons au niveau du PCE et dans le hall public du bâtiment principal. Ces équipements seront associés à des détecteurs fixes et portatifs de masse métallique.

Il sera également prévu un appareil d'inspection des enveloppes et des petits paquets pour le contrôle de sécurité du courrier à son point de réception au niveau de chaque site.

Les équipements «X-ray» proposés devront être conformes aux normes internationales de santé et de sécurité en vigueur dont USA FDA X-Ray systems (Federal Standard 21CFR 1020.40) et « Health & Safety at Work Act » de 1974-section 6, amendé par le « consumer protection Act » de 1987. Le maximum de fuites de radiation tolérée est de moins de 0.1mR/hr (1µ Sv/hr) près des panneaux extérieurs.

Le soumissionnaire proposera également des miroirs convexes sur manche télescopique pour l'inspection de sûreté des véhicules à l'entrée des concessions.

En définitive, il fournira :

- un système de détection «X-ray» aux accès piétons ;
- des détecteurs de masse métallique ;
- des détecteurs portatifs de masse métallique ;
- des miroirs d'inspection de véhicules ;
- un appareil d'inspection des enveloppes et des petits paquets (scanner de courrier).

5.9. Système de contrôle de rondes

Il s'agit de fournir et d'installer un système électronique de surveillance, de communication et de contrôle de la bonne exécution des rondes. Le dispositif permettra de signaler plusieurs types d'informations concernant une opération de ronde : identité de l'agent, itinéraire de la ronde, points manquants, points incidents. Il doit être robuste, léger et de dimensions réduites.

En particulier, le soumissionnaire proposera les équipements ci-après :

- un logiciel de contrôle de ronde ;
- dix Lecteurs de contrôle de rondes ;
- quinze tag d'identification agents rondiers ;

- cent points de contrôle de rondes à encastrer et inarrachables ;
- des étiquettes de documentation de ronde ;
- un Ordinateur de gestion de contrôle de rondes.

5.10. Ensembles bloc-portes et menuiseries aluminium vitrées et blindées

Il s'agit, sur la base du plan fourni par la BCEAO, de proposer les blocs portes et les vitrages blindés selon les données ci-après :

- les baies des bâtiments du PCE, du poste de garde accès fourgons, du local Police et du Poste de Contrôle des Fourgons, sont équipées de châssis vitrés de sécurité pare-balles de classe FB6/BR6 NS au sens de la norme EN 1360 ;
- les ensembles verriers de la Caisse et de la Comptabilité, séparant l'intérieur des locaux des espaces réservés à la clientèle (FB4/BR4) ;
- les bloc-portes situés sur le cheminement d'évacuation d'urgence de la clientèle institutionnelle ;
- le bloc-porte de l'issue de secours du bâtiment fonctionnel.

Les issues de secours sont associées à des Terminaux d'Issues de Secours (TIS) constitués par des dispositifs d'urgence autonomes avec alarme de dissuasion pour limiter les abus de sorties non autorisées ou hors état d'urgence. Ces terminaux doivent permettre d'identifier que l'issue est contrôlée sous alarme déclenchée lors d'un déverrouillage d'urgence ou d'une tentative d'effraction. Ils sont compatibles avec le contrôle d'accès et les états électriques sont reportés au PCS afin de signaler une alarme et informer de l'état du verrouillage de chaque issue de secours. Le dispositif est doté d'un bouton réarmable protégé par un carter.

Un bouton lumineux facilement repérable, installé à moins de 1,3 m du sol doit permettre un déverrouillage d'urgence en combinaison avec la détection incendie ou une commande du PCS, pour un ordre de libération immédiate de l'issue. Ces dispositifs autonomes de déverrouillage manuel d'urgence pour issues de secours, compatibles avec le contrôle d'accès et la détection incendie, équipent toutes les portillons situés sur le cheminement d'évacuation de la clientèle des guichets des grosses opérations.

L'entreprise fournira, suivant le cadre de devis donné à titre indicatif en annexes :

- des ensembles châssis vitré FB6/BR6 NS ;
- des ensembles châssis vitré FB4/BR4 NS ;
- des bloc-portes CR5 ;
- des Terminaux d'issue de secours modèles TIS 100 ou équivalent.

6. Sécurité du système d'information du dispositif de sûreté

Une hygiène informatique minimale doit être assurée au niveau de l'architecture support associée au dispositif de sûreté (vidéosurveillance, contrôle d'accès, anti-intrusion et réseau TIP), conformément au guide édité par l'ANSSI en la matière et la série des normes ISO/CEI 27000, en vue de prémunir l'infrastructure contre les cyber-attaques.

La cartographie de l'architecture doit être fournie et le système d'information du dispositif de sûreté satisfaire, dans sa globalité, aux exigences ci-après dont la liste, donnée à titre indicatif, n'est pas exhaustive :

- les cheminements de câbles sont mis en place à l'intérieur des zones contrôlées ;
- les liaisons de communication entre les moyens physiques d'ouverture et les unités de traitement local sont des liaisons dédiées au système de sécurité ;
- les liaisons filaires sont surveillées de manière à garantir qu'aucune tentative de fraude ne puisse être réalisée ;

- la perte d'informations au niveau des liaisons doit être signalée et traitée comme une alarme ;
- la fibre optique doit être privilégiée pour les liaisons entre bâtiments ;
- la transmission des informations des systèmes de contrôle d'accès, de vidéosurveillance et de détection d'intrusions se fait sur des réseaux logiques dédiés à chacun de ces systèmes ;
- les protocoles de communication utilisés (algorithmes de chiffrement inclus) doivent être décrits, et particulièrement les principes de sécurisation et de vérification des échanges ;
- la communication entre le badge, la tête de lecture et l'UTL doit être chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS [19]) ;
- la communication entre l'UTL et le serveur de gestion du système doit être chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS [19]) ;
- les câbles servant pour la transmission des informations des systèmes de contrôle d'accès, de vidéosurveillance et de détection d'intrusions sont des câbles distinctement dédiés à ces systèmes ;
- les réseaux définis pour les systèmes de contrôle d'accès, de vidéosurveillance et de détection d'intrusions sont totalement indépendants du réseau informatique de la Banque autant pour les câbles que pour les équipements électroniques ou informatiques associés ;
- s'ils venaient à faire l'objet de vulnérabilités publiées, permettant de compromettre leur efficacité, les protocoles et algorithmes utilisés doivent pouvoir être remplacés par d'autres protocoles ou algorithmes ne faisant pas l'objet de vulnérabilités publiées et permettant de maintenir le niveau de sécurité des échanges ;
- le temps de réponse entre la présentation d'un badge et la réception de la commande d'ouverture de l'accès doit être inférieur à 0,5s ;
- le temps d'apparition d'une alarme sur une console d'exploitation (en service) doit être inférieur à 2s ;
- le temps de transmission d'une information d'accès au serveur de gestion du système doit être inférieur à 2s ;
- les protocoles réseaux utilisés sont obligatoirement sécurisés.

ANNEXE 1 – CADRES DE DEVIS ESTIMATIFS

TRES IMPORTANT : les informations fournies dans ces cadres indicatifs constituent une description minimale des solutions souhaitées. Il est attendu des soumissionnaires des offres en adéquation avec l'évolution de la technologie. Les marques et modèles sont aussi indicatifs.