Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFÈTE DE L'ESSONNE

ÉVRY le 10 Juin 2016

Rédacteur : Olivier BERGER, Nicolas LAURO
Coordonnées : 01 69 91 90 72 /
nicolas.lauro@essonne.gouv.fr

Cahier des Clauses Techniques Particulières
C.C.T.P.
REMPLACEMENT ET EXTENSION DU SYSTEME DE CONTRÔLE DES ACCÉS DE LA PRÉFECTURE DE L'ESSONNE ET DE LA CITE ADMINISTRATIVE ET INTERFONCTIONNEMENT SUR DES POINTS EN COMMUN AVEC LE CONSEIL DÉPARTEMENTAL DE L'ESSONNE

Marché passé en procédure adaptée en application du décret n°2016-360 du 25 mars 2016 relatif aux marchés publics.

Le présent document comporte :
- 52 pages numérotées de 1 à 52

DIFFUSION INTERNE

Sommaire

1 TERMINOLOGIE

Afin d'éviter toute confusion, les termes suivants seront utilisés :

- Lecteur de badge : élément permettant de capter l'information issue d'un badge pour la transmettre à la centrale de contrôle d'accès ;
- Unité de contrôle d'accès (UCA) comprend le système pour les ouvertures de porte et le contrôleur d'accès. Équivaut à Unité de traitement local (UTL).
- Contrôle d'accès : système qui permet de contrôler l'accès à un site par l'audio, la vidéo, des badges ou des codes.
- Serveur de gestion des accès
- Les postes clients : postes pour l'administration ou la gestion du système.

Le soumissionnaire précisera le contenu de ces éléments et des éléments de sa proposition.

2 DESCRIPTION GENERALE DU PROJET

2.1 OBJET DE LA CONSULTATION

Le présent document décrit les prestations à exécuter, fixe les règles d'ingénierie et les spécifications techniques à respecter ainsi que les composants à mettre en œuvre, pour le remplacement et l'extension du contrôle d'accès actuel de la Cité administrative par la mise en œuvre d'un système de gestion des accès compatibles avec les cartes agents sécurisées de la :

PREFECTURE DE L'ESSONNE
Boulevard de France
CS 10701

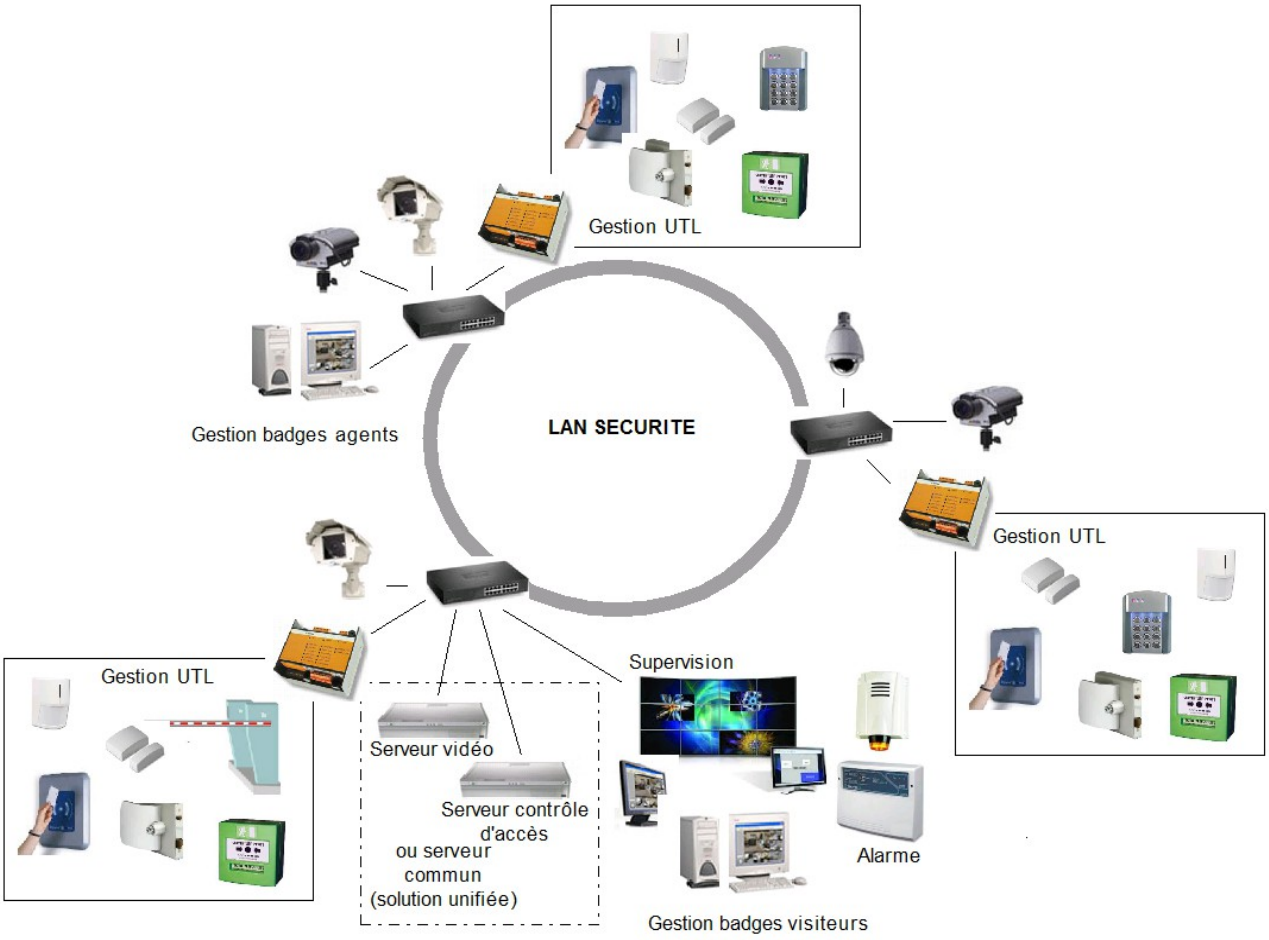
91010 Evry cedex

Ce système devra être utilisable sur l'ensemble de la Cité administrative et dans des parties communes avec le Conseil Départemental de l'Essonne.

Ce projet s'intègre dans une solution globale de sécurité et devra permettre à terme d'avoir une vision globale d'exploitation et être compatible avec des systèmes de vidéoprotection et de détection d'intrusion dans deux PC de sécurité distincts que sont le PC de la préfecture au synoptique et le PC du conseil départemental .

2.2 DESCRIPTION SYNTHETIQUE DES PRESTATIONS

Le système est prévu pour apporter une solution de sécurité unifiée et ouverte en assurant la préservation des biens et des personnes, un renforcement de la protection des biens contre tout acte de vandalisme, contre les dégradations et contre toute agression.



La zone de sécurité comprend la périphérie de la cité administrative (préfecture et bâtiment administratif), la périmétrie des bâtiments de la cité administrative et l'intérieur des bâtiments et les résidences préfectorales.

2.2.1 Prestation de base

Le projet prévoit principalement les points suivants :

- fourniture, installation, raccordement et mise en service d'un contrôle d'accès (câblage courants forts et faibles, éléments matériels actifs et passifs et logiciels) selon la liste annexée, le câblage du courant faible sera chiffré en option ;
- le logiciel et le paramétrage de deux postes informatiques (fournis par la préfecture, en option le titulaire chiffrera la fourniture de ces deux postes) pour la supervision et la gestion des contrôles d'accès de la préfecture et de la Cité administrative et des points communs ;
- fourniture des équipements matériels et logiciels nécessaires à la programmation et à l'édition de tickets à usage unique et/ou de badges permettant des droits d'accès temporaires ;
- dépose, stockage et/ou enlèvement du matériel obsolète ;
- fourniture de la documentation détaillée ;
- formation des personnels chargés de la gestion et l'exploitation du système mis en œuvre ;
- garantie sur le matériel et les logiciels comprenant la maintenance préventive, corrective, évolutive et adaptative du système de contrôle d'accès (architecture technique, logiciels…) livré ;

La prestation devra respecter les mesures de sécurité (cf : §8) et la réglementation en vigueur.

Les plans et documents nécessaires à l'élaboration du projet seront remis par l'administration ou son représentant lors de la visite de site.

Les fonds de plans au format Autocad (dwg) seront remis au titulaire du marché pour mise à jour et confection du DOE à fournir dans le cadre de la recette.(cf §). La version logicielle sera à définir pour une lecture aisée des documents.

La prestation de serrurerie fera l'objet d'une consultation distincte pour ce qui concerne le choix, la pose et le réglage des serrures, en revanche l'intégration au système fait partie du présent CCTP.
Le soumissionnaire devra prendre contact avec le pôle sécurité et sûreté des sites aux fins d'obtention des documents et des rendez-vous. (téléphone : 01 69 91 91 28; veronique.bosch@essonne.gouv.fr,)

Le soumissionnaire devra préciser si des éléments sont manquants pour un bon fonctionnement sécurisé de l'ensemble.

2.2.2 Prestation optionnelle

La prestation optionnelle comprend :

- option A : Réfection du câblage des contrôles d'accès existants en préfecture et cité administrative ;
- option B : câblage des contrôles d'accès supplémentaires et communs ;
- Option C : Fourniture et installation d'un dispositif complet pour la préfecture et la cité administrative avec des lecteurs de badge biométriques (empreintes digitales ou par la reconnaissance de l'iris ou autre), les coûts unitaires des différents type de lecteurs seront précisés, le soumissionnaire précisera les avantages et inconvénients par rapport à la prestation de base;
- Option D : Sur les huit points en commun à la Préfecture et au Conseil départemental, fourniture, installation, raccordement et mise en service d'un contrôle d'accès (câblage courants forts et faibles, éléments matériels actifs et passifs et logiciels) avec à terme une double gestion Préfecture et Conseil Départemental ;
- Option E : la fourniture de deux postes informatiques de gestion et de supervision
- Option F : changement des type de verrouillage de portes : Le soumissionnaire chiffrera le remplacement des loquets électromagnétiques et des ventouses par des gâche électriques
- Option G : mise en place de contacts de détection de portes ouvertes. La liste des portes concernées sera fournie lors de la visite de site,

Option relative à la maintenance du système de contrôle d'accès :
* Option 1 : contrat de maintenance pour la Cité Administrative et les points en commun avec le conseil départemental à l'issu de la période de garantie.

3 DESCRIPTION DE L'EXISTANT

Deux entités sont bien distinctes : la Cité Administrative et le Conseil Départemental.

3.1 BÂTIMENTS

Les différents bâtiments de la Cité administrative sont situés Boulevard de France à Evry :

- préfecture de l'Essonne ;
- bâtiment administratif ;
- bâtiment RIA (restaurant Inter administratif) ;
- quatre résidences ;
- Postes de contrôle 2 et 3
- un parking extérieur

3.2 ACCES PÉRIPHÉRIQUES OU COMMUNS

Huit Accès Communs entre Cité administrative et le Conseil Départemental :
La cité administrative possède des accès périphériques dont certains sont communs avec le conseil départemental :

- PC6 : entre le conseil départemental et le rez de chaussée (parking supérieur) de la préfecture : accès piéton et accès véhicule;
- PC5 : portail entre le conseil départemental et la préfecture (proche résidences) : accès piéton et accès véhicule ;
- 3 étages en commun : 1er étage, 2ème étage et 3ème étage
- Toîts : au 4ème étage TourB
- Vides sanitaires : au sous-sol
- PC1 : rue des Mazières, tourniquet (réalisation ultérieure)

3.3 CÂBLAGE

La préfecture dispose d'un câblage catégorie 6A, avec un répartiteur général et 5 sous-répartiteurs répartis au sein de la préfecture.

La future architecture du système de contrôle d'accès pourra s'appuyer sur les locaux existants.

Les liaisons entre les lecteurs de badge et les centrales de gestion sont réalisées avec du câble de type téléphone 3 ou 4 paires.

Les unités de contrôle d'accès existantes sont connectées sur un réseau spécifique indépendant du réseau informatique de la préfecture.

Les nouvelles unités de contrôle d'accès seront connectées au réseau informatique de la préfecture sur un VLAN dédié.

Le soumissionnaire vérifiera que le câblage existant est suffisant pour raccorder les nouveaux équipements, si ce n'est pas le cas, le soumissionnaire devra préciser ce qui manque et devra le chiffrer dans la prestation.

3.4 LOCAUX TECHNIQUES

Il y a environ 17 unités de contrôle d'accès situées dans différents placards de la préfecture. Le

soumissionnaire devra vérifier que le nombre d'unité de contrôle d'accès est suffisant par rapport à l'état de l'art et aux règles en vigueur pour les lecteurs existants et préciser le nombre d'unité de contrôle d'accès supplémentaires à installer. Ainsi, le soumissionnaire devra préciser le nombre et le positionnement des unités de contrôle d'accès nécessaires pour assurer les prestations demandées et permettre les extensions demandées et les évolutions ultérieures sur la Cité administrative.
Le matériel informatique et réseau se trouve dans un local technique à côté du PCS.

3.5 CONTRÔLE D'ACCÈS

Le contrôle d'accès actuel est composé de plusieurs types de lecteurs de badge, d'unité de contrôle d'accès répartis au sein de la cité administrative et d'un serveur de gestion des accès situé dans un bureau du pôle sécurité de la préfecture.
A terme, il y aura deux contrôles d'accès distincts, celui géré par la Préfecture au sein de la Cité administrative et celui géré par le Conseil départemental. Ces contrôles d'accès disposeront de lecteurs en commun, mais avec une validation spécifique à chaque entité. Ces contrôles d'accès doivent pouvoir interagir avec le système de vidéoprotection et anti-intrusion.
La liste de l'existant et des nouveaux accès demandés est précisée en annexe. On distingue les accès Cité administrative existants, les nouveaux accès et les accès communs avec le conseil départemental.

Si le soumissionnaire constate des omissions dans cette liste qui influerait sur le coût de la prestation, il doit le spécifier dans la proposition financière.
Il existe plusieurs types de lecteurs en place : lecteurs de piste magnétique, lecteurs sans contact. L'emplacement des lecteurs existants n'est pas modifié.
Le dispositif commande des gâches électriques, des ventouses électromagnétiques , un portier qui permettent l'ouverture des portes ainsi que des portes coulissantes. Toutes les portes équipées de ventouses disposent d'un bouton poussoir pour la sortie. Pour certaines portes un déclencheur manuel vert permet en cas de secours l'ouverture de la porte.

Contrôles d'accès existants :

- 43 lecteurs sans contact
- 26 ventouses
- 12 gâches
- 1 portier
- 3 portes coulissantes

Contrôles d'accès à créer :

- 57 lecteurs :
- 27 gâches
- 2 portillons
- 2 portails
- 1 tourniquet4 barrières
- 2 portes coulissantes

Les emplacements des contrôles d'accès seront précisés sur les plans remis lors de la visite de site obligatoire. La présente consultation ne porte que sur la fourniture et la pose des contrôles d'accès, les menuiseries font l'objet d'un CCTP séparé..

3.6 ENERGIE

Le matériel actuellement en place est alimenté par du courant secouru 24V.
Les unités de gestion disposent d'une batterie et ne sont pas alimentées par câble Ethernet (POE),

4 EQUIPEMENTS DE L'INSTALLATION ET RACCORDEMENT

4.1 PRESTATION

Dans le cadre de l'option relative à la réfection du câblage des contrôles d'accès la prestation suivante sera réalisée. La solution sera conforme aux règles APSAD D83.

Le titulaire fournit, pose et raccorde tous les types de câbles et équipements nécessaires à l'alimentation électrique et au transport des informations traitées par les équipements du système de sécurité),

- fourniture, pose et raccordement de câbles 4 paires catégorie 6A pour les liens IP,
- fourniture, pose et raccordement de câbles multi-paires 6/10 adaptés pour les BUS RS- 485,
- fourniture, pose et raccordement de câbles électriques,
- fourniture, pose et raccordement de tous les cheminements (gaines, chemins de câble en dalle marine, génie civil,etc...) et percements nécessaires. Les travaux de génie civil sont à intégrer dans la prestation.
- fourniture, pose et raccordement de boîtiers IP 66 étanche,

Par ailleurs, le soumissionnaire doit être sensibilisé aux risques éventuels de phénomène naturel (foudre, inondation, etc.) et à cet égard, ses offres doivent proposer une protection adaptée à l'ensemble des équipements, assortie éventuellement d'une garantie contractuelle qu'il précisera.
En aucun cas, les câbles du réseau local existant ne pourront être utilisés. Seuls les câbles reliant les éléments de terminaison aux UCA pourront être conservés.

4.2 AMÉNAGEMENT DES LOCAUX

Les éléments techniques (serveurs, éléments actifs),de la solution seront concentrés dans les locaux techniques existants. Les autres éléments (postes de supervision, contrôleurs d'accès, encodeurs, etc..) seront placés dans des bureaux sécurisés à définir.

4.3 CÂBLAGE

4.3.1 Câbles cuivre

Les câbles de catégorie 6A seront impérativement, de type F/UTP ou U/FTP, 100 ohms, LSOH ou LSZH conforme à la norme ISO/IEC, classe Ea 11801 2nd Ed.Am2 et devront permettre la transmission au minimum à 500 MHz sur 90 m .

Ces câbles seront raccordés sur des bandeaux de brassage équipés de RJ45.

4.4 RÈGLES D'INSTALLATION

Le principe de câblage devra particulièrement prendre en compte les éléments suivants :

- les traversées de parois par des canalisations devront être obturées de manière à reconstituer le degré coupe feu de la paroi ;
- les canalisations ne devront pas traverser des locaux présentant des risques particuliers d'incendie, risques BE2 tels que définis la norme NFC15.100 ;
- les câbles courant-faible ne seront pas installés à moins de 1,80 m des transformateurs et des câbles électriques de forte puissance ;
- les câbles courant-faible seront distants des appareils d'éclairage fluorescent d'au moins 30 cm ;
- aucune installation de câbles apparents ne sera admise, sans soumission du projet et avis préalable du Maître d'œuvre ;

- Dans les faux plafonds et les planchers techniques le cheminement des câbles se fera soit dans des chemins de câble type dalle marine (obligatoirement si cheminement parallèle de plus de 10 câbles) soit sous canalisation type fourreau, gaine ICT, tube Iro, etc.
- En dehors du chemin de câble ou des goulottes, les câbles seront protégés sur toutes leur longueur par une gaine ICT ou Tube IRO. Toutes les traversées de dalles et murs seront protégées par des gaines ou fourreaux. Le soumissionnaire devra prendre à sa charge les percements.
- L'ensemble des gaines et tube IRO seront de couleur homogène sur l'ensemble du chantier (à valider par la maîtrise d'œuvre)
- Dans les parties apparentes (façades, bureaux, etc..) le cheminement se fera de façon à respecter l'esthétique des locaux, et sera le plus discret possible, dans des goulottes, plinthes, tubes Iro , etc.. d'une couleur appropriée. Dans les zones sensibles (hall d'entrée, façades,..) des essais de support et de couleur pourront être demandés au titulaire afin que le maître d'œuvre puisse valider les cheminements et matériels avant l'exécution des travaux
- Les câbles seront attachés par colliers dans les chemins de câbles (maximum 10 par toron), à raison de :
  - une attache tous les 5 m pour les parcours horizontaux,
  - une attache tous les 1 m pour les parcours verticaux,
  - une attache de part et d'autre des dérivations ou changement de direction.
- les câbles seront d'un seul tenant à l'intérieur des chemins de câbles (boîtes de raccordement et épissures non admises),
- le changement de direction des chemins de câbles et conduits, se fera par l'intermédiaire d'éléments préfabriqués pour obtenir une finition parfaite,
- les chemins de câbles verticaux seront pourvus de couvercles de protection,
- le cheminement des câbles de liaison s'effectuera dans le chemin de câbles courants faibles distants des chemins de câbles courants forts d'au moins 30 cm. Une attention particulière sera apportée à la disposition des câbles (les éloigner au maximum des appareils générateurs d'interférences), dans le cas où l'écartement ne pourra être respecté, une protection adaptée contre les perturbations électromagnétiques (chemin de câble tôle marine, capoté,..) sera mise en place.
- Si nécessaire, les travaux de génie civil (réalisation de tranchées) seront à intégrer, ainsi que toutes les protections et cheminements (gaines, filet de protection,..).
- tous passages risquant de détériorer les câbles seront évités (arrêtes coupantes, angles vifs, température élevée, etc.),
- le matériel installé devra respecter les préconisations du constructeur (conditions de voisinage, mode de pose, etc.),
- les circuits de puissance et de commande devront être protégés séparément,
- dans le cas où des croisements de canalisations électriques avec des canalisations de plomberie ou de chauffage seraient inévitables, toutes les dispositions réglementaires concernant le risque d'une mise sous tension accidentelle seront observées,
- le cheminement des câbles de liaison s'effectuera obligatoirement sous chemins de câbles pour un cheminement parallèle supérieur à 5 câbles ou conduits. Pour les autres cheminements le passage respectera le niveau de finition requis dans la zone considérée. (Incorporé dans les parties nobles, sous tube rigide dans les locaux techniques, etc.),
- l'ensemble des chemins de câble courants faibles seront mis à la terre du bâtiment à l'aide d'un câble de cuivre nu de 10mm² minimum avec fixation tous les 6 m au plus et à chaque changement de direction sur l'ensemble des chemins de câble existant ou à installer
- Les éléments des chemins de câble seront raccordés entre eux par éclisses de même type avec boulons poêliers galvanisés.
- L'ensemble des câbles extérieurs sera protégé à l'aide d'une gaine métallique.
- les câbles "courants forts" et "courants faibles" seront posés dans leurs canalisations respectives (mélange des "courants forts" / "courants faibles" interdit).

- Les raccordements électriques des organes principaux (UCA, interfaces anti intrusion et contrôle d'accès, alimentation secourue,…) seront à raccorder directement sur des tableaux électriques.
- Les raccordements type multiprises sont à proscrire

4.5 RACCORDEMENT ET PROTECTION

Le principe de raccordement et protection des câbles devra particulièrement prendre en compte les éléments suivants:

- tous les connecteurs, cuivres et optiques seront intégrés dans les baies ou coffrets au moyen de bandeaux au format 19'' adaptés.

Par souci d'homogénéité, et sauf indication contraire, les noyaux, les connectiques et les bandeaux RJ45 devront être conformes à ceux déjà installés.

- l'arrivée des câbles pourra être réalisée en partie supérieure ou inférieure des éventuelles armoires et coffrets et ceci au travers des plaques amovibles munies d'un presse-étoupe,
- l'ensemble des conducteurs des câbles devra être raccordé aux deux extrémités, même ceux de réserve,
- tous les blindages des câbles seront mis à la terre en un point unique afin d'éviter les boucles de courant ;
- tous les conducteurs (courants forts) seront raccordés sur des borniers séparés par fonction et dûment repérés (Indication de la fonction et numérotation par suite logique de nombres),
- les câbles d'alimentation et de transport de l'information des systèmes d'alarme seront protégés contre toute tentative de sabotage
- il est indispensable que toutes les connectiques RJ45 de la solution soient sécurisées par des prises adaptées munies de clés. Il en est ainsi des connexions aux postes clients, caméra, UCA, interphone.

4.6 REPÉRAGE

Le principe de repérage des câbles devra particulièrement prendre en compte les éléments suivants :

Les étiquettes seront imprimées et non manuscrites afin de permettre une lecture facile.
Les étiquettes seront positionnées dans l'insert prévu au niveau des supports de connecteurs RJ45.
Toutes les liaisons impliquées dans la solution (RJ 45, Bus …) doivent être clairement repérées sur les connecteurs (tenant et aboutissant).
Le repérage devra permettre d'identifier clairement la fonction du câble ainsi que l'origine et la destination,

4.6.1 La prise côté baie de distribution

Les prises des bandeaux RJ45 seront repérées par les informations suivantes :

- ✔ Utilisation : usage étiqueté V (vidéo), A (contrôle d'accès), I (intrusion), PC (poste client);
- ✔ Etage de la prise (sauf site sur 1 seul niveau) ;
- ✔ et N° de prise de 01 à xx.

4.6.2 La prise terminale

Les prises terminales seront repérées par les informations suivantes :

- ✔ REP-U-n-xx
- ✔ REP : si plusieurs répartiteurs dans le bâtiment RG, SR0...
- ✔ U (utilisation) : usage étiqueté V , A, I,;

- ✔ n : numéro d'étage (ss, 0,1,2) (sauf site sur 1 seul niveau)
- ✔ xx : numéro de prise dans l'étage

La numérotation respectera le plan d'implantation des prises remis au moment de la visite (cf. synoptique en annexe).

4.6.3 Les câbles

L'ensemble des câbles sera repéré par des étiquettes gravées inaltérables, placées aux tenants et aboutissants, à chaque changement de direction, en traversée de plancher ou cloison et régulièrement (tous les 10 m) sur les parcours horizontaux et verticaux (à l'exception des câbles cheminant en apparent).

4.7 BRASSAGE

4.7.1 Cordons de brassage cuivre

Le Soumissionnaire proposera la fourniture de cordons 4 paires, blindés, d'impédance caractéristique 100 Ohms, catégorie 6A, équipés d'une prise RJ 45 mâle blindée à chaque extrémité, à raison d'un cordon par liaison fournie.
Des clips de couleur seront fournis avec les cordons.
Ils permettront de différencier :

- les prises destinées au système de vidéo-protection.
- les prises destinées au système de contrôle d'accès.
- les prises destinées au système d'intrusion.
- les prises destinées aux client/serveur
- les prises destinées au système de visiophonie

4.7.2 Cordons de brassage optique

Les cordons optiques posséderont les mêmes caractéristiques que la fibre optique installée.
Ils seront équipés de connecteurs SC-LC.

4.8 DIMENSIONNEMENT

Les chemins de câbles et goulottes qui seront mis en œuvre, devront pouvoir offrir une réserve minimale de 30% du nombre de câbles correspondant à la capacité câblée de l'ensemble des équipements existants et nouveaux.
Chaque percement devra être soumis à l'accord du maître d'œuvre et aura une réserve de passage supplémentaire de 30% par rapport au nombre de câbles à acheminer. Le choix des emplacements de chaque percement devra faire l'objet d'un examen particulier
Le soumissionnaire devra garantir, par sa conception et ses modalités de mise en œuvre, la possibilité d'extension de l'installation, objet du présent CCTP. Une telle extension devra être réalisable sans modification aucune, de la structure du système mis en œuvre.

4.9 FINITIONS

Le soumissionnaire devra avant réception, parfaire ses installations pour que celles-ci soient esthétiques et propres.
Il devra veiller particulièrement à :

- la clarté du repérage,
- la propreté du câblage,

- l’esthétique des matériels apparents,
- la réfection des supports après dépose éventuelle des équipements existants.

Le soumissionnaire sera responsable entre autres, de tous les travaux de colmatage des trémies ou percements qu'il effectuera ou utilisera dans les cloisons et planchers. Il devra s'attacher pour ces rebouchages, à employer des matériaux permettant de restituer les degrés de stabilité au feu des ouvrages séparatifs. La fiche technique du ou des produits utilisés sera transmise au responsable sécurité incendie du site et sera également intégrée à la documentation remise à l’issue des travaux.

4.10 ENERGIE

Les économies en termes de consommation énergétique sont à prendre en compte dans l'étude.
Le titulaire fournira et installera :

- les câbles courant fort nécessaires à la prestation,
- le raccordement et la fourniture de prises en courant fort si nécessaire pour ce qui a trait à l’alimentation :
  - des postes de travail, écrans dans le poste de garde et bureaux des huissiers
  - des postes clients ;

L'alimentation en courant fort se fera à partir des tableaux électriques les plus proches. Chaque départ sera repéré et protégé par un disjoncteur adapté fourni par le prestataire.
La solution doit comporter des onduleurs pour assurer un secours minimum de 30 minutes d’utilisation de tous les équipements.
Ces onduleurs seront raccordés sur l’alimentation secourue du site (par groupe électrogène).
Dans les baies informatiques, il sera préférable d'intégrer des onduleurs rackables au format 19".
Chaque onduleur fournit par le prestataire sera administrable et supervisable par le réseau.
Une remontée d'alarme sera signalée au PC Sécurité en cas de défaillance du circuit électrique.

4.11 BÂTIMENTAIRE

Ce paragraphe s’applique pour les options F et G.

4.11.1 Menuiserie/Maçonnerie/Finition

Le titulaire doit installer, raccorder, gérer les équipements à installer et, dans ce cadre doit veiller à la conduite de travaux de réfection, percement, rebouchage, finition pour une qualité bâtimentaire parfaite égale à l’origine et avant intervention.
Il est rappelé que tous les travaux de génie civil liés à la prestation sont à intégrer.

4.11.2 Serrurerie

Les serrures seront raccordées avec le système de contrôle d'accès, et seront à même de donner tout ou partie des commandes ou informations suivantes en fonction du modèle de serrure retenue :
Activation de la béquille intérieure.

- Position du pêne.
- Position de porte (contre pêne rentré + pêne sorti).
- Activation du cylindre.
- Boucle anti-sabotage.

La pose de portes et de serrures n'entre pas dans le périmètre des prestations de ce CCTP.

Seul le raccordement et l'intégration au système est prévu.
Pour ce faire, le présent CCTP prévoit :

- l'alimentation courant faible (inférieure à 50 volts) pour les équipements de serrure.

La tension d'alimentation fournie devra être adaptée par le soumissionnaire au lot serrurerie

- les entrées/ sorties nécessaires au raccordement au système de contrôle d'accès ;
- la configuration du système par rapport aux informations fournies par les serrures
- la fourniture et l'intégration des détecteurs d'ouverture
- le point de raccordement de la serrure au contrôleur local

Le point de raccordement sera positionné au niveau du faux plafond (s'il existe) avec la réserve de câble nécessaire.

L'emplacement exact du point de raccordement est à coordonner avec le lot serrurerie

Le présent CCTP ne prévoit ni les serrures, ni les câbles, ni les conduits de liaisons de la serrure au point de raccordement fourni.

Le périmètre qui n'est pas du lot « sécurité » est :

- Mise en place, pose, mise en jeu, réglage, finition des travaux d'accueils de la serrure et du passe câble sur les portes à intégrer ou à créer au niveau des faux plafonds « en zone sécurisée » avec la réserve de câbles nécessaire (3 m) pour pouvoir intégrer toutes les informations transmises par les serrures. Les goulottes adaptées sur le chemin serrure - faux-plafonds ne sont pas à la charge du lot « sécurité ».
- Mise en place des règles et fourniture des clés physiques

4.12 ARCHITECTURE

Les contrôles d'accès seront connectés sur les commutateurs Ethernet de la préfecture, sur un VLAN dédié.

4.12.1 Réseau local : LAN

Périmètre des prestations :

L'administration définira les numéros de Vlans ainsi que les plans d'adressage IP qui respecteront la politique d'adressage du ministère de l'intérieur.

Ces informations comprendront notamment :

les adresses IP source et destination ;

les flux source et destination ;

ports origine et destination ;

les protocoles ;

les débits ;

les fréquences (flux permanent ou ponctuel) ;

les remarques éventuelles ;

tout paramétrage autorisé pour assurer le fonctionnement sécurisé de la solution.

5 SYSTEME DE CONTROLE D'ACCES

Le système sera conforme à la règle APSAD D83.

La solution de contrôle d'accès sera ouverte et distribuée par différents installateurs.

Quelle que soit la solution proposée, l'assemblage intégré de logiciels doit être éprouvé et distribué par différents installateurs.

L'ensemble de la solution d'accès doit respecter les recommandations du guide de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) [RFID ANSSI] et décrire ces écarts par rapport à ce guide. La solution devra être examinée par l'ANSSI dans le cadre du Certificat de Sécurité de Premier Niveau (CSPN).

[RFID ANSSI] *- Guide sur la sécurité des technologies sans contact pour le contrôle d'accès, version de travail 1.0, 19 Novembre 2012. Dans l'attente d'une version consolidée, la version de travail fait office de document de référence.*

Pour la mise en œuvre du Guide ANSSI sur le contrôle d'accès par puce sans contact, le MI demande d'appliquer :

- *les mesures de niveau L1 et L2 pour les sites de type Préfecture (à l'exception des mesures concernant les visuels de la carte agent)*
- *les mesures de niveau L1, L2 ET L3 pour les sites sensibles.*

PES Génériques V2 n°12/061 du 11 décembre 2012, disponible sur le site intranet de la DSIC http://dsic.mi Ce document sera délivré par le RSSI de la préfecture lors de la visite du soumissionnaire.

5.1 SERVEURS

5.1.1 Prestation de base

La solution est une solution de type client/serveur, le nombre de clients simultanés, supportés par l'applicatif, doit pouvoir être supérieur à 3.

Le serveur de contrôle d'accès permet la gestion simultanée de 2000 porteurs de badges actifs. Le système devra pouvoir gérer au minimum 100 lecteurs de badges

Le système central de contrôle d'accès est constitué d'un serveur fonctionnant en mode 64 Bits . La base de données est une base SQL de type 64 bits.Le système est Windows Server 2012.

Le serveur de contrôle d'accès doit pouvoir fonctionner dans trois modes :

- le mode en ligne,
- le mode hybride dans lequel certains contrôleurs locaux fonctionnent en mode dégradé
- le mode «complètement» dégradé.

En ligne, le serveur assure une communication à tout instant entre les contrôleurs locaux. Dans les versions dégradées, les contrôleurs locaux prennent en charge les décisions d'accès et tous les événements sont retransmis au serveur dès réception de la communication.

L'administration des serveurs et leur localisation sont précisés sur les plans remis lors de la visite du site.

La solution doit pouvoir disposer d'un système de sauvegarde de toutes les données.

La solution doit disposer d'un système de restauration de la sauvegarde. Les procédures relatives à

ces opérations sont fournies par le titulaire.

5.1.2 Prestation complémentaire

Le soumissionnaire présentera **en complément** dans son offre les solutions de redondance de l'unité centrale permettant de s'affranchir de la défaillance d'un disque dur ou du PC hébergeant l'applicatif de l'unité centrale. Cette option aura de l'incidence sur le mode opérationnel du système.

5.2 CONTRÔLEURS LOCAUX

La solution permet, sur les équipements contrôlés, l'identification par :

- lecteur de badge seul
- clavier
- lecteur de badge et clavier numérique
- lecteur biométrique

Chaque lecteur de badges de l'installation est relié au serveur par l'intermédiaire d'un contrôleur local.

Les Unités de contrôle d'accès (UCA) seront équipées d'une auto-protection qui intégrera la surveillance de l'ouverture et de l'arrachement du coffret et seront installées dans des locaux techniques sécurisés.

Toutes les liaisons de type Wiegand non chiffrées, entre un lecteur de badge et un autre équipement, sont interdites (UCA, contrôleur spécifique). La liaison avec le lecteur est réalisée en RS-485 ou en IP ou en Wiegand sécurisé.

La liaison UCA-lecteurs est chiffrée de bout en bout sans adjonction de module entre le lecteur et l'UCA.

Cette liaison est, de préférence, bi-directionnelle de bout en bout.

Les UCA communiqueront avec le serveur par liaison Ethernet TCP/IP impérativement.

Les contrôleurs locaux (CL) IP peuvent être PoE.

Les contrôleurs locaux doivent disposer des interfaces d'entrée et de sortie en nombre suffisant pour pouvoir gérer :

- l'identification en entrée et en sortie ;
- l'asservissement d'une serrure électrique ou électromagnétique ;
- la récupération d'un déclenchement de Détection Manuel de Déverrouillage (DMD) ;
- la gestion des contacts d'Ouverture de Porte (DOP) ;
- la gestion d'au moins un bouton de demande de sortie par porte;
- la gestion de l'alarme d'auto-protection ;
- la gestion des alarmes d'énergie (défaillance alimentation, défaillance batterie) ;
- la gestion des détecteurs d'intrusion.

Les contrôleurs locaux doivent pouvoir supporter la sauvegarde d'au moins 5000 événements en cas de perte du serveur

Ils doivent disposer de LEDs permettant de visualiser l'état d'un contrôleur durant une opération de maintenance.

En mode dégradé, les contrôleurs locaux fonctionnent en tant qu'unités autonomes.

Dans ce mode, les contrôleurs gèrent toutes les demandes d'accès et conservent un journal de toutes les activités (accès, entrées/sorties Tout ou Rien (ToR) , alarmes, etc…). Les décisions d'accès sont prises en fonction des données stockées dans le contrôleur au moment de la perte de connexion.

Lorsque la communication est rétablie, les journaux d'activité sont transférés vers le serveur avec l'intégralité de l'historique d'activité (accès et entrées/sorties ToR).

Les contrôleurs locaux IP doivent (si possible) pouvoir dialoguer de manière chiffrée avec les lecteurs de badges et s'authentifier mutuellement si des mécanismes de mise à jour de clés par le réseau sont disponibles. Ce dernier mode est un avantage à la solution

Le flux entre le lecteur RFID et le contrôleur d'accès peut être chiffré. Le contrôleur d'accès peut disposer d'un Secure Application Module (SAM) ou d'une autre solution de manière à ce que le bus de données transporte des données protégées par un niveau de sécurité équivalent à celui porté par la transaction RFID (transaction air/air).

La durée de conservation des événements, alarmes et vidéos est paramétrable jusqu'au seuil correspondant au maximum des réglementations en vigueur.

Tous les événements associés aux points d'accès supervisés par le système vidéo sont liés aux images correspondantes et accessibles par simple clic dans l'interface de supervision.

Les UCA pourront gérer les accès et l'intrusion.

Si les unités de traitement ne sont pas POE, elles intégreront leur propre alimentation sauvegardée par batterie embarquée, l'alimentation UCA sera intégrée dans le coffret UCA et sera donc auto protégée par surveillance à l'ouverture et à l'arrachement du coffret. Cette alimentation disposera de 3 étages indépendants :

- 1 sortie : alimentation de l'ensemble de la partie électronique (cartes UCA, cartes d'extension et lecteurs),
- 1 sortie : charge de la batterie,
- 1 sortie : alimentation des organes de verrouillage. Chaque voie "organe de verrouillage" sera indépendante. La mise en défaut (court-circuit ou mise à la Terre) d'une voie ne devra mettre hors service que la voie concernée et ne devra pas impacter les autres voies.

Les fonctionnalités assurées en décision locale par l'UCA afin de garantir le fonctionnement en cas de coupure des liens avec le serveur seront :

- la gestion des badges (profils d'accès associés, date d'expiration),
- la gestion de l'environnement porte (porte maintenue ouverte trop longtemps et porte forcée, période d'ouverture automatique),
- la gestion des entrées/sorties (mise en/hors service sur période horaires, temporisations, activation de sortie sur alarme d'une entrée).

5.3 ÉQUIPEMENTS DE PORTES

Le soumissionnaire présentera **en option G** dans son offre la mise en place de contacts de détection de porte ouverte,

Les portes deux vantaux doivent disposer d'un détecteur d'ouverture sur chaque vantail.

5.4 COMMANDES DE PORTES

5.4.1 Déclencheur Manuel de déverrouillage (DMD)

Le déclencheur manuel sera de couleur verte. Sa fonction d'interrupteur sera intercalée sur la ligne de télécommande assurant la dé-condamnation des issues en cas d'urgence par rupture directe de tension du dispositif de verrouillage.

Le boîtier sera muni d'un capot avec scellé. Pour manœuvrer le boîtier, il sera obligatoire de casser le scellé. La préfecture disposera des outils pour remettre en place les scellés sur les boîtiers verts ouverts. Ces boîtier seront installés en saillie, plombés, à membrane souple déformable, avec contact de signalisation d'état repris individuellement sur l'installation. Il sera prévu en installation intérieure ou extérieure.

- Réarmement à clé du dispositif après activation.

- Buzzer intégré, voyant d'état.
- Respect de la (réglementation CO 46), Norme NFS 61 937.

Sortie contact supplémentaire d'utilisation pour retour vers le contrôle d'accès.

5.4.2 Bouton d'ouverture de porte (BOP)

Bouton poussoir assurant la dé-condamnation temporisée des accès avec sortie contrôlée ou des accès avec dispositif de fermeture à rupture. La fonction sera clairement identifiée par un symbole sur le bouton poussoir.

Les boîtiers type de demande de sortie seront posés à 1,20m du sol fini.

5.5 GESTION DES ACCÈS

5.5.1 Configuration des accès

La solution permet de paramétrer les propriétés suivantes, associées à une porte :

- Nom physique/Nom logique ;
- Délai d'attente de réarmement de la serrure ;
- Délai d'attente d'événements de porte entrebâillée (durée max de déverrouillage avant alarme) ;
- Définition du type de sortie (contrôlée ou non);
- Association porte/caméra ;
- Temps d'inhibition du réarmement de la serrure sur ouverture par un (des) badge(s) résident(s) et réarmement dès fermeture de la porte.

La solution permet de gérer tous les états des portes et des équipements associés (lecteur d'identifiant, détecteur ouverture, équipement de serrure) :

- Activation des béquilles ;
- Activation du cylindre ;
- Anomalie serrure ;
- Boucle anti-sabotage ;
- État du DAS (verrouillé/déverrouillé) ;
- Pêne sorti, Pêne rentré, serrure piloté mécaniquement ;
- Porte Ouverte/Porte Fermée/Porte Ouverte trop longtemps;
- Position de porte (contre pêne rentré) ;
- Etc…

La solution permet d'ouvrir/fermer/inhiber un accès sous réserve des droits de l'utilisateur depuis la cartographie ou depuis une liste nominative d'équipement.

Le contrôle d'accès est vrai à toute heure et période d'exploitation.

En mode normal, l'accès au local ou à la zone est obtenu par validation de badge. L'accès peut être également équipé d'un vidéo portier.

En mode contrôlé en entrée, sortie libre : la sortie est obtenue par action sur d'un bouton poussoir ou par action sur une béquille.

En mode contrôlé en entrée et en sortie: la sortie est obtenue par lecture d'identifiant.

Le temps d'ouverture excessif peut activer une pré-alarme sonore et visuelle locale à l'accès. Cet événement est mémorisé sur les historiques du système et engendre une alarme sur les postes d'exploitation opérateur.

5.5.2 Gestion des Couloirs Rapides à Unicité de Passage (CRUP)

La solution permet une gestion fine et intelligente des couloirs rapides ou d'autres dispositifs de passage (hormis les portes « standards ») de type tripode, sas, etc….

La solution permet, notamment, de gérer toutes les alarmes et sorties des dispositifs de passage:

- Alarmes techniques de fonctionnement;

- Confirmation de passage;
- Forçage;
- Fraude à l'unicité de passage;
- Intrusion dans la zone de passage sans badgeage;

La solution permet, notamment, de gérer toutes les entrées des dispositifs de passages :

- Ouverture/fermeture;
- Ouverture Permanente/Fermeture Permanente;

La solution permet, notamment, de gérer tous les états des dispositifs de passages :

- Passage Ouvert/Passage Fermé;

En conséquence, sur certains couloirs rapides, il sera possible de faire une demande d'ouverture après identification pour un type de badge et l'ouverture sera réalisée manuellement par un poste applicatif client disposant des droits d'ouverture du couloir. Le titulaire propose la création d'un onglet adapté à cette fonction contenant l'affichage de la fonction « vidéo-badging », fil de l'eau des événements, bouton d'ouverture du dispositif de passage.

La solution permet de paramétrer les propriétés suivantes :

- Nom physique/Nom logique ;
- Délai d'attente de réarmement de serrure ;
- Délai d'attente d'événements de passage entre ouvert (durée max de déverrouillage avant alarme) ;
- Association des alarmes ;
- Typologie de la sortie/sens de passage ;
- Horaire durant lequel le passage est contrôlé en entrée/sortie ;
- Horaire durant lequel l'entrée est autorisée ;
- Horaire durant lequel la sortie est autorisée ;
- Association point passage/caméra.

Tous ces dispositifs peuvent fonctionner en entrée et/ou en sortie.

Les tableaux récapitulatifs définissant le nombre et l'emplacement des couloirs rapides seront remis lors de la visite de site

5.5.3 Asservissement des accès

La solution permet de gérer des points d'accès contrôlés sans identification mais par :

- Bouton d'ouverture entrée/sortie;
- Bouton de demande d'entrée/sortie et dans ce cas l'ouverture de l'accès est donnée par l'opérateur disposant des droits suffisants;

La solution permet de gérer et changer dynamiquement le mode de contrôle du point d'accès en fonction d'événements (calendaires, automatiques comme les: identifiant de personne, type de badge) ou d'actions manuelles. Un point d'accès peut être géré :

- Par identification à certaines périodes;
- Par demande d'E/S à certaines périodes;
- Par demande d'E/S validée par opérateur après identification durant certaines périodes;
- Par demande d'E/S validée par opérateur après identification d'un type de profil durant certaines périodes;

NB : La détection d'un type de profil **est** donc un événement **natif du système**.

Et non contrôlé à d'autres périodes (ouverture automatique ou non).

Lorsque la biométrie est présente elle viendra de préférence avec le complément d'un badge.

Les équipements d'accès sont liés à des caméras positionnées en aval et/ou en amont. Tous les événements d'accès peuvent être indexés à des enregistrements vidéo. Un équipement d'accès peut être surveillé et associé à un groupe de caméras.

Tous les événements (identifiant, alarmes, sorties, entrées, états) liés à un point d'accès sont horodatés, enregistrés. Ces événements indexent les flux vidéo des caméras associées au point d'accès.

Tous les événements associés sont affichables dans la console de gestion des alarmes/événements en fonction du paramétrage du système (affiché/furtif). Certains événements persistants (porte ouverte trop longtemps, équipement hors/service, etc..) sont affichables avec un cycle délimité par une constante de temps paramétrable.

La solution de gestion des accès est conforme aux réglementations en matière de sécurité du bâtiment et notamment à la sécurité incendie. Le système doit pouvoir cohabiter pour les issues de secours avec le système de sécurité incendie (SSI, NF S 61-931). Le système installé est conforme aux différentes règles NF et APSAD relatives à la sécurité incendie pour l'ensemble des équipements installés, du câblage, ainsi que pour l'ensemble des futures interfaces avec le SSI. Le système de SSI n'entre pas dans le périmètre de la solution mais les équipements installés permettent de récupérer les événements SSI (disponibilité des E/S suffisantes). La prestation consiste à la mise à disposition d'un câble raccordable sur le boîtier aux normes SSI en cas de déverrouillage automatique par le Centralisateur de Mise en Sécurité Incendie (CMSI).

5.5.4 Anti-retour

La solution prend en charge la gestion anti-retour. Lorsqu'un retour est détecté, un événement anti-retour est déclenché.

La solution prend en charge les types d'événements anti-retour suivants :

- l'événement est seulement archivé ;
- l'événement est archivé mais l'accès est refusé.

La fonctionnalité anti-retour est paramétrable par utilisateur ou groupe d'utilisateur et naturellement par secteur.

L'opérateur peut accorder un accès malgré une détection anti-retour.

L'opérateur peut accorder l'accès à un groupe d'utilisateur malgré une détection d'anti-retour.

La solution permet de gérer l'anti-retour en entrée et/ou en sortie de manière à pouvoir ou non autoriser une sortie si l'entrée n'a pas été validée. La solution permet le réglage horaire de gestion de l'anti-retour de manière à autoriser ou à ne pas autoriser une sortie le jour J+1 même si l'entrée à été faite le jour J. L'anti-retour est de type time-back et pass-back.

Sur un dispositif de passage, la solution permet une gestion intelligente du passage en ne validant l'accès du badge qu'après une confirmation physique d'un passage par le dispositif de passage. Le but est naturellement de ne pas bloquer une personne (si l'anti retour est activé) si elle n'a pas franchi l'obstacle avant le délai existant (time-out) et réglable dans le dispositif (couloir rapide par exemple). La confirmation physique du passage est réalisée par le couloir rapide, pour ce type d'équipement, et interprétée par la solution pour ne pas bloquer une personne n'ayant pas franchi les portes.

5.5.5 Contrôle des accès

5.5.5.1 Lecteur de badges (LB) et Support Sans Contact

On notera :

- les **lecteurs type A** : les lecteurs gérés par la Préfecture (Cité Administrative) (clé chiffrée A);
- les **lecteurs type B** : les lecteurs gérés par le Conseil Départemental (clé chiffrée B) ;
- les **lecteurs type C** : les lecteurs communs à la Cité Administrative et au conseil départemental avec une gestion à double validation (deux clés A et B distinctes).

A titre d'exemple, une personne devant accéder à une zone Cité Administrative en provenance d'une zone du Conseil départemental devra être habilité par la préfecture, à l'opposé une personne souhaitant accéder à une zone de la préfecture devra être habilité par le conseil départemental. Les lecteurs de type C pourront être utilisés par les personnels de la Cité Administrative et du Conseil Départemental, mais auront une gestion distincte des accès : l'une par la Préfecture, l'autre par le Conseil départemental.

Le soumissionnaire détaillera le fonctionnement des types de lecteurs A et C .

Pour les parties communes (PC5, PC6 et les portes d'accès communes aux 3 étages des bâtiments « Préfecture » et « Hôtel du Département) :

Dans un premier temps, les 5 lecteurs communs qui auront à terme une double gestion Conseil départemental et Préfecture seront connectés de façon transitoire sur le système de contrôle d'accès de la préfecture, jusqu' à ce que le conseil départemental dispose de son propre système de contrôle d'accès.

Ensuite et lorsque le conseil départemental disposera de son propre système de contrôle d'accès, ces 5 lecteurs communs devront être reconnectés au système de contrôle d'accès du conseil départemental.

La carte sans contact, de taille ISO 7816, utilisée pour l'identification aux contrôles d'accès est fondée sur la puce Mifare DesFire Ev1 2k , 4k, 8k avec chiffrement AES.

Le titulaire livre un quantitatif de 1000 badges de 2k minimum, blanc PVC, avec les exigences suivantes :

Format ISO 7816;

Badge vierge, libre de droit, tel que sortie d'usine sans modification de clés (clé maître notamment) et de droits .

La carte agent est en mode Random ID avec une clé maître carte secrète. La condition d'accès est réalisée par la lecture sécurisée d'un identifiant (numéro logique). La lecture de l'identifiant est conditionnée à l'authentification Mifare Desfire pour vérification de l'accès en lecture à cet identifiant.

La solution doit permettre la création du fichier d'identifiant avec une clé applicative qui devra être modifiée pour le cas où la carte est livrée par un partenaire ayant ouvert le container applicatif avec une clé temporaire « partagée ». Les cartes agents sont livrées avec une application crée (AID) et définit pour N clés. La clé 0 est la clé applicative. Toutes les cartes agents sont livrées avant enrôlement avec les N clés ayant une valeur dite de clé applicative « partagée ». Ces N clés sont à modifier par le processus enrôlement.

Les cartes « blanches » fournies par le titulaire sont à personnaliser de manière identique aux cartes agents et l'application (AID) est à créer par enrôlement. La PICC Master Key des cartes blanches est à modifier. Il ne doit rester aucune clé usine NxP dans ces cartes « blanches » et les cartes agents.

La structure, contenant l'identifiant, transmise entre la carte et le lecteur doit être d'une longueur suffisante. Elle est inscrite durant l'encodage qui est dans le périmètre du titulaire. La solution garantit l'unicité de l'identifiant associé à un seul badge. L'identifiant est révocable autant aléatoire que possible ou introduit manuellement. Il n'est pas inscrit graphiquement sur le badge.

Deux clés sont indispensables pour la gestion des droits d'accès aux fichiers de configuration de la carte. La clé R de lecture et la clé RW et W. Les droits R/W et W sont donc gérés par une clé unique.

Le droit Changement d'accès (droit Ch) est fixé à « Refuse » « Denied ».

La solution d'encodage des cartes agents, visiteurs, badge de configuration et/ou des SAM peut être une solution indépendante de la solution de contrôle d'accès. Idéalement, elle est intégrée. La solution doit permettre de pouvoir créer un fichier identifiant supplémentaire par application dans le cas d'introduction de clé supplémentaire utilisée en cas de compromission ou de renouvellement.

Les lecteurs d'identifiants (de porte ou enrôleur) contiennent uniquement les secrets qui leurs sont nécessaires. Il est nécessaire pour les lecteurs d'avoir, soit des lecteurs de type Radio-frequency identification (RFID) hautement sécurisés (disposant de SAM), soit des lecteurs RFID dont les clés seront en RAM et volatile de manière à ce qu'un arrachage de lecteur ou une coupure de courant détruise la trace de la clé maître pour empêcher sa compromission, soit par préférence des lecteurs « transparents ».

Les lecteurs RFID doivent être protégés contre l'arrachement. Ils doivent disposer de LED (Vert, Rouge) permettant une signalisation visuelle et d'un beeper permettant la signalisation sonore :.

- lecteur en veille (visuel),
- passage autorisé (**uniquement visuel),**
- passage non autorisé (visuel et sonore).
- Alarme de temporisation de porte ouverte dépassée (sonore)

Les lecteurs RFID doivent être protégés à l'ouverture de « face » comme de « dos » s'ils disposent de secrets. Le lecteur doit pouvoir traiter le protocole Myfare T=CL.
Le lecteur peut délocaliser (lecteur transparent) la partie antenne de la partie décodage RFID de manière à ce que l'information sur le câble de liaison soit protégée par la clé de session utilisée entre l'antenne et la carte.
Les lecteurs, UCA doivent être à jour de tous les patchs de sécurité. Ces deux dispositifs font partis des éléments décrits dans le maintien en condition de sécurité. La détection d'une faille de sécurité nécessitera une mise à jour et des mesures correctives dans le cadre du déploiement et ou du maintien en condition de sécurité de la solution.
Les têtes de lecture doivent avoir démontré un excellent niveau de protection contre les fraudes. Elles devront avoir fait l'objet d'une Certification de Sécurité de Premier Niveau (CSPN) ou être engagée dans cette démarche de premier niveau. (vérifiable sur le site de l'A.N.S.S.I.)
Tous les composants utilisant un Sécurity Account Manager (SAM) devront montrer un canal sécurisé ainsi qu'un canal d'authentification avec le lecteur et/ou UCA garantissant que le vol du SAM ne peut mettre en péril les secrets de la solution. Idéalement, le SAM est le composant de sécurité évalué.
La configuration des secrets des SAM ou des badges de configuration des lecteurs ne doit pas nécessité de clés privées dont l'administration n'auraient pas la propriété. Par exemple, les clés de lecture des badges de configuration sont la propriété unique de l'administration. Un badge de configuration et une procédure pour remettre les paramètres usine (qui peuvent être constructeur) sont nécessaires en cas d'initialisation et de retour du matériel.
Toutes les exportations de clés sont interdites.
Toutes les introductions de clés dans la solution doivent être sécurisées. La clé n'est jamais affichée en clair mais uniquement une partie de son « HASH ». L'algorithme de calcul du HASH est standard type SHA-256.
En aucun cas, le titulaire ne doit connaître les clés de l'administration.
Idéalement, chaque clé peut être introduite par 1 ou 3 porteurs suivant sa sensibilité. Elles sont stockées sur support papier. Dans le cas ou la clé est introduite par plusieurs porteurs, la clé finale est reconstituée par des XOR successifs de chaque cryptogramme (*K=XOR[XOR[K1,K2],K3]*).
La vérification de la bonne introduction de la clé K est effectuée par comparaison des 4 premiers octets du SHA-256 de la clé K. Cette introduction par plusieurs porteurs est un plus à la solution.

Le titulaire proposera à l'officier de sécurité une typologie décrivant la sensibilité des clés de sa solution, leurs modes de gestions/renouvellement. Cette typologie permet en phase de conception d'arrêter la procédure de mise à la clé et de définit le nombre de porteur par clé.
La solution permet la configuration de la partie applicative cartes pour garantir la compatibilité avec les AID et les clés de production et «partagées» de l'administration.
Le titulaire doit fournir une documentation sur la gestion des clés incluant :

- La configuration des lecteurs/enrôleurs et ou éléments à sécuriser (SAM);
- La configuration des badges de configuration des lecteurs et des enrôleurs.
- Le descriptif des clefs, index et noms utilisés dans les cartes et dans tous les lecteurs/enrôleurs d'identifiants et SAM.
- Une procédure de mise à la clé des secrets de la solution (cérémonie de clés) qui reprend les termes/noms/éléments techniques décrits dans les documents.

Aucune réception du système ne peut être envisagée si ces conditions ne sont pas respectées.

5.5.5.2 Renouvellement des clés

La solution doit permettre un renouvellement des clés par l'injection de nouvelles clés au poste d'enrôlement du bureau des badges. Cette solution permet un basculement avec une période transitoire ou deux jeux de clés sont utilisés sur les têtes de lectures programmées. La procédure de migration est établie par l'officier de sécurité et appliquée sur toutes les têtes de lecture. Le mode permanent avec les nouvelles clés de lecture est alors mis en place après l'encodage du dernier badge du site. En mode permanent et donc à la fin du processus de renouvellement les têtes de lecture sont configurées pour ne lire que les nouvelles clés.
La modalité utilisée est définie avec l'officier de sécurité durant la phase de conception.
Aucune réception du système ne peut être envisagée si ces conditions ne sont pas respectées.
Le contrôle d'accès de la préfecture dispose d'une clé bien distincte de celle du conseil départemental.

5.5.5.3 Support biométrique (empreinte ou iris)

Les lecteurs RFID utilisés pour lire les informations biométriques sont soumis aux mêmes contraintes que les lecteurs d'identifiants d'accès. Une partie de la mémoire des cartes est personnalisable pour y inscrire de manière sécurisée les minuties d'au moins 2 doigts par personne. Le système réalise l'authentification par comparaison des minuties en mode 1:1.. Le lecteur biométrique doit pouvoir réaliser l'authentification en moins de deux secondes. Les lecteurs RFID peuvent, en complément, respecter le standard FIPS-201 pour ce qui à trait au formatage des données des minuties.

6 INTERFONCTIONNEMENT DES SYSTEMES

Ce CCTP relatif au remplacement et à l'évolution du système de contrôle d'accès à la Cité administrative de l'Essonne s'intègre dans un projet global de sécurisation de la Cité administrative avec des points communs avec le conseil départemental.
Aussi, le soumissionnaire devra proposer un système de contrôle d'accès permettant une gestion avec des interactions avec la vidéoprotection et les alarmes.
Par exemple, un accès sur un lecteur de badge doit permettre le déclenchement d'une caméra.
Le soumissionnaire précisera les éléments pris en compte.
L'objectif de la solution est d'une part de fédérer une application traditionnelle de contrôle d'accès et, d'autre part, de superviser le système en proposant sur une interface unifiée la gestion des accès, alarmes et vidéo.
Cette solution peut être constituée d'un superviseur client de deux systèmes disjoints : contrôle d'accès et vidéo-protection.
Au terme « hyperviseur », ce document préfère utiliser le terme interface utilisateur.

Tous les événements (identifiant, alarmes, sorties, entrées, états) liés à un point d'accès ou un point d'intrusion sont horodatés et enregistrés. Ces événements indexent les flux vidéo des caméras associées au point d'accès ou d'intrusion.

- Tous les événements associés aux points d'accès supervisés par le système vidéo sont liés aux images correspondantes et accessibles par simple clic dans l'interface de supervision.
- Les alarmes sont couplées au système vidéo pour l'enregistrement, la levée de doute avec pré-positionnement sur les zones en alarme est naturellement l'interface de traitement et d'acquittement.
- Les alarmes sont affichées avec toutes les possibilités vidéo associées de la visualisation des points de fuite.
- Le serveur de temps sera la référence d'horodatage de l'ensemble de la solution.

7 EXPLOITATION DE LA SOLUTION

7.1 GESTION DU SYSTÈME

7.1.1 Présentation des profils utilisateurs

L'administration précise les profils utilisateurs en vigueur dans le cadre de la gestion des dispositifs plus généralement de sûreté :

- l'accès « **Administrateur système** » permettant à un opérateur clairement désigné et habilité, de vérifier le bon état de fonctionnement du dispositif et d'en administrer l'ensemble (paramétrage, configuration, supervision, sauvegardes, lectures, cartographie…) ainsi que la visibilité des informations qu'il contient.
- l'accès « **Gestionnaire de badges** » permettant à un opérateur, sous-réserve de ses droits, d'administrer et gérer les profils, de produire des badges, etc. En aucun cas le profil « Gestionnaire de badges» ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système.
- l'accès « **Opérateur** » permettant à un exploitant, sous-réserve de ses droits, de consulter la cartographie, gérer des alarmes, produire des badges, gérer des portes, ainsi que de consulter les fiches réflexe, etc. En aucun cas le profil « Opérateur» ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système.

L'implantation des différents terminaux se fera en fonction du choix retenu par le maître d'ouvrage.

7.1.2 Configuration matérielle

Les postes clients sont des PC de type « tour ». Les postes utilisés pour la visualisation des caméras posséderont des capacités d'affichage de 6 flux vidéo 25 i/s au format 720p en H.264 à minimum 2Mbps pour offrir un affichage équivalent à une qualité analogique fluide, sans effet de pixellisation, et seront équipés d'un joystick manuel chacun.

Ils disposent d'un clavier filaire ergonomique, du lecteur de carte à puce à contact (carte agent) utilisé à l'identification de l'utilisateur sur l'applicatif et d'une souris filaire 2 boutons et molette.

Le système d'exploitation des postes clients proposés devra être validé par la DSIC.

Les postes clients sont configurés de manière à ce que les éventuels composants (port USB, CD-ROM, etc..) non nécessaires à l'utilisation du système permettant l'extraction ou l'insertion de données soient désactivés hormis pour l'administrateur.

Les protections du Bios contre les démarrages sur des supports amovibles doivent être activées. Les fonctionnalités d'Autorun sont désactivées (cf . CERTA-2006-INF-006-004).

7.1.2.1 Poste de sécurité

En plus des caractéristiques du paragraphe ci-dessus, le poste de travail sera équipé de 3 écrans plats LED de 22 pouces. Il permettra :.

- Le pilotage de l'ensemble des caméras et l'affichage des images en cascade ou en mosaïque au choix de l'opérateur, avec possibilité d'afficher en plein écran l'une ou l'autre des caméras par un simple clic de souris.
- L'affichage de la cartographie avec action de verrouillage et déverrouillage des accès
- la gestion de la main courante des événements

7.1.2.2 Poste de visualisation (client léger)

En plus des caractéristiques du § 7.1.2, le poste de travail « client léger » sera équipé d'un écran plat LED de 22 pouces et permettra le pilotage de l'ensemble des caméras et l'affichage des images en cascade ou en mosaïque au choix de l'opérateur, avec possibilité d'afficher en plein écran l'une ou l'autre des caméras par un simple clic de souris.

7.1.2.3 Poste de gestion des badges

En plus des caractéristiques du § 7.1.2, le poste de gestion des badges sera équipé d'un écran plat LED de 22 pouces et permettra aux utilisateurs ayant les droits de gérer le système de contrôle d'accès.

Ce poste sera équipé d'un lecteur RFID pour la personnalisation des badges

7.2 EXPLOITATION PAR L'ADMINISTRATEUR DU SYSTÈME

Le système permet de définir des profils d'utilisateurs permettant de gérer des « droits » ou privilèges sur les objets Équipement/Événement/Alarmes/Actions/Espace de Travail dans tous les applicatifs utilisés. Cette gestion doit, par exemple, quand l'objet est une action, permettre de définir des droits de Création/ Suppression / Exécution/ Modification.

Toutes les actions sur le système sont réservées et protégées par des droits liés au compte applicatif de l'opérateur. Il y a a minima trois types de droits :

- Le droit de lecture confère à un opérateur le pouvoir de visibilité.
- Le droit d'écriture confère à un opérateur un pouvoir d'action.
- Le droit de modification confère à un opérateur les droits de modification.

7.2.1 Configuration des droits opérateurs

Les éléments suivants sont configurés en droits (profil par opérateur), pour permettre à *minima* les fonctions suivantes ;

Des droits sont gérés pour la création/visualisation/configuration des entités du système (utilisateur, badge, alarme, actions, fiche de porteur, rapport, équipement) ;

Des droits sont gérés par équipement pour permettre la création, la visualisation, la configuration, le changement d'état (actif/inhibé) ;

- Un équipement (porte, lecteur de badge, détecteur) peut être invisible à un utilisateur ;
- Un équipement (porte, lecteur de badge, détecteur) peut être en accès lecture seule ;
- Une porte en lecture seule permet la visualisation de son état mais inhibe les droits d'actions Ouverture/Fermeture ;

Des droits sont gérés pour les éléments partagés

- Inférioriser des commandes joystick ;
- Priorisation sur l'accès à des écrans et vignettes des murs d'images;
- Accès en lecture seule sur la définition des écrans et vignettes des murs d'image;
- Accès en modification seule sur la définition des écrans et vignettes des murs d'image;

Des droits sont gérés pour la création, la visualisation, le déclenchement des actions programmées ou natives ;

Des droits sont gérés pour la création, la visualisation, la modification de l'espace de travail ;

Des droits sont gérés pour l'accès aux applications de la solution.

Un opérateur « poste de garde » doit pouvoir, au minimum :

- disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité ;

- disposer de droit en écriture sur un accès pour l'ouvrir/le fermer ;
- visualiser certaines caméras.

Un opérateur « bureau des badges » doit pouvoir au minimum :

- configurer son espace de travail ;
- créer/modifier des profils, des groupes de porteurs, des porteurs de badge ;
- disposer d'un droit en écriture sur des accès pour l'ouvrir/le fermer ;
- disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité ;
- disposer des droits de lecture/écriture/modification des équipements d'accès.
- éditer un badge.

Seuls les opérateurs déclarés avec un profil « administrateur » disposent d'un accès en écriture sur tous les équipements.

Le système de gestion des droits est paramétrable. Le système permet une gestion sécurisée des mots de passe des utilisateurs.

Le système de gestion des droits permet de définir des droits relatifs à la définition/modification de l'espace de travail.

Le système doit avoir une gestion des droits permettant de gérer des équipements partagés ou des informations partageables, que ce soit dans le cadre de « raccordements » (fédération, déport, supervision multi-site) ou dans le cadre d'utilisation locale (partage de la motorisation des caméras, des murs d'images).

La documentation doit fournir une description détaillée des possibilités natives offertes par le système de gestion des droits

7.2.2 Gestion des journaux

La solution permet la consultation de l'ensemble des actions effectuées sur le système que ce soit au niveau des postes clients ou au niveau des postes serveurs mais selon les droits octroyés à l'utilisateur.
Les actions tracées sont à minima :
Système

- Arrêt / Lancement des services applicatifs (journalisation incluse);
- Arrêt critique sur incident ;
- Arrêt système par exploitant (identifiant, date/heure) ;
- Démarrage système par exploitant (identifiant, date/heure) ;
- Evènement de ressources systèmes;

Administration applicative

- Ajout/suppression d'équipements
- Gestion des comptes (création/suppression/modification des droits)

Exploitation courante

- Heure de connexion, déconnexion ;
- Action sur un équipement ;
- Action sur un badge

La solution doit protéger cette traçabilité par son système de droits (profil).

7.3 EXPLOITATION PAR LE GESTIONNAIRE DES BADGES

7.3.1 Gestion des badges

7.3.1.1 ***Personnalisation des badges utilisateurs***

La solution permet la gestion de porteurs de badges et de groupes de porteurs de badge. Les groupes de porteurs sont des listes de porteurs crées par direction/service ou site.

La solution permet de paramétrer les propriétés suivantes d'un porteur de carte :

- Nom ;
- Prénom ;
- Matricule ;
- Fonction, bâtiment, étage, bureau, service, poste téléphonique, émail ;
- Date et lieu de naissance ;
- Société, service, fonction ;
- Nationalité ;
- Adresse (n°, rue, code postal, ville, pays) ;
- Pièce d'identité présentée (type, n°, date et organisme de délivrance) ;
- Véhicule (immatriculation) ;
- Conduite à tenir et observation (255 caractères) ;
- Grade ;
- Dates (remise de badge, début et fin de validité, restitution de badge) ;

Les champs nominatifs acceptent toutes les lettres donc les caractères accentués et ponctuations utilisés dans la langue française.

La solution permet la gestion de :

- Champs personnalisés (au moins 15) ;
- Date d'activation/ Date d'expiration ;
- Gestion d'une photo capturée à partir d'un périphérique numérique (web cam ou caméra de vidéo surveillance) ou importé par fichier ;
- Statut (profil activé ou désactivé, perdu, volé, bloqué, etc..) ;

Les champs personnalisables sont des entités type :

- Booléen
- Dates
- Entiers
- Images ou fichiers graphiques
- Nombre décimaux
- Texte

La solution permet l'association d'un porteur de carte et d'un groupe de porteurs avec un modèle de badge.

La solution détecte les doublons à partir du nom, prénom, date de naissance et/ou service, société.

Tous les champs ne sont pas obligatoirement renseignés. Les champs de la fiche de porteurs de badge doivent pouvoir être obligatoires ou non.

La solution empêche la création de fiches similaires. L'objectif est d'empêcher l'attribution de deux badges à une personne.

La solution permet d'activer ou d'inhiber un badge ou un groupe de badges manuellement sous réserve des droits utilisateur.

La photo imprimée sur le badge doit être sans déformation et conforme au cadrage réalisé. La déformation d'image est interdite, le facteur d'échelle doit être conservé.

La solution doit permettre le réglage d'un cadre de base au taille réglementaire passeport et paramétrable. Le cadre doit pouvoir faire 2,4 x 3,2 cm. Ce paramétrage doit être conservé.

L'historique de la fiche de porteurs de badge doit comprendre les événements d'impression de carte.

La solution permet la gestion des erreurs à l'importation.

Le serveur de contrôle d'accès permet la gestion simultanée de 2000 porteurs de badges.

Gestion des profils

La solution permet la création de profils à partir de règles d'accès associées à des groupes de points d'accès.

La solution permet l'association de porteurs ou des groupes de porteurs à des règles d'accès et des profils.

La solution permet de paramétrer les droits d'accès en fonction des points d'accès et de plages horaires et calendaires :.

- 32 plages horaires comprenant chacune 3 intervalles par jour, pour chaque jour de la semaine. Une notion de "jours spéciaux" permettant de programmer des droits d'accès contextuels et non hebdomadaires sera prévue.
- 32 jours fériés :

  - ponctuels,

  - annuels reconductibles, jours fériés calendrier français recalculé automatiquement d'une année sur l'autre

La solution permet la gestion d'un grand nombre de profils (supérieur à 50)

7.3.1.2 Type de badge

LE BADGE DOIT ETRE COMPTATIBLE AVEC LA CARTE AGENT DU MINISTERE DE L'INTERIEUR (cf : § 4.5.5.1)

La solution permet la gestion de différents types de badge portés par des modèles de badge différents. On différenciera naturellement le type de badge, des droits ou profils liés à chaque badge.

Pour simplifier les choses et pour ne pas dévoiler d'informations vitales, il existe au niveau de la personnalisation des badges a minima les catégories suivantes pour les personnes :

- Badge P : badge nominatif pour les permanents toutes directions confondues ; La personnalisation graphique varie pour les badges de la classe P.
- Badge V : badge non nominatif, journalier, pour des visiteurs occasionnels externes.

Les droits d'accès associés aux badges V sont définis par le bureau des badges. Ce sont des droits minimums.

7.3.1.3 Invalidation des badges

La solution permet de rendre automatiquement invalide un badge à la fin de sa période de validité. Cette fonction est particulièrement mise en service pour les badges journalier V.

La solution permet de bloquer un badge lorsqu'il n'est pas utilisé pendant une durée supérieure à un temps paramétré (de l'ordre de 2 mois). Cette fonctionnalité peut être activée sur certains profils ou badges.

La solution permet d'invalider n'importe quel badge de la solution sous réserve d'avoir les droits utilisateur

7.3.1.4 Etat d'un badge

L'opérateur disposant des droits peut, en recherchant un badge (recherche multicritères à partir d'un nom/numéro d'identifiant) décider de positionner le badge comme :

Actif	Toutes les fonctions prévues
Inactif	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge inactivé le jj/mm/aa à hhmn par *nom_personne* ».
Perdu	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge déclaré perdu le jj/mm/aa à hhmn par *nom_personne* ».
Volé	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge déclaré volé le jj/mm/aa à hhmn par *nom_personne* ».
Expiré	Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge bloqué le jj/mm/aa à hhmn par *nom_personne* ».

7.3.2 Gestion des rapports

Les rapports standards d'activité courante seront :

- liste des alarmes,
- historique des mouvements d'un utilisateur,
- historique des mouvements de badges,
- liste des badges non présentés dans telle zone depuis N jours (N paramétrable),
- historique des événements par type d'objet,
- taux d'utilisation des lecteurs.

Les rapports d'activité opérateurs seront :

- historique des login,
- journal des acquittements trié par date, filtré pour tout ou partie des opérateurs.

Les rapports liés aux utilisateurs seront :

- liste des badges,
- état des badges,
- liste des badges ayant accès à un ou plusieurs lecteurs,
- liste des badges venant à expiration à une date donnée,
- liste des badges appartenant à une série de groupe d'utilisateurs,

- liste des utilisateurs avec leur fiche d'identification,
- liste simplifiée des utilisateurs.

7.4 EXPLOITATION PAR LES OPÉRATEURS

7.4.1 Gestion à partir du PC Sécurité (PCS)

7.4.1.1 Aménagement du PCS

Un « poste de supervision » est à fournir pour gérer la sécurité du site à partir du PC Sécurité situé au synoptique de la préfecture.

Il disposera de trois écrans: (cf § 7.1.2)

le premier écran affichera le plan graphique renseigné du site, en 2D avec noms des lieux, numéro de l'étage, nom ou numéro de la pièce, type et qualité des moyens, ainsi que la disposition des moyens mis en place tels que caméra, détecteur/contrôleur d'ouverture de porte, détecteur de mouvement, le lancement de commandes directes (mise en/hors service de point d'entrée, activation de sortie, déverrouillage d'accès, etc.),

le second, affichera les images de l'ensemble des caméras, en cascade ou en mosaïque au choix de l'opérateur, avec possibilité d'afficher en plein écran l'une ou l'autre des caméras par un simple clic de souris.

le troisième présentera une fiche « main courante » précisant les événements du jour (prévus, arrivés, en cours, etc.), les incidents types, la conduite à tenir, les mesures prises qui permettent de prévoir, organiser et gérer la sécurité au quotidien en cas d'événement, qu'il soit anodin ou grave. Il sera aussi celui qui permettra l'acquittement et la visualisation de l'historique des alarmes, la gestion manuelle et automatique des caméras, le pilotage de l'éclairage, l'utilisation des prépositions des caméras sur le plan graphique, l'enregistrement numérique sur disque dur des événements du site).

Dans le cas d'une installation d'un second PC de Sécurité, identique à celui décrit ci-dessus, le fonctionnement de l'ensemble devra pouvoir être simultané, toutefois le soumissionnaire indiquera si ce mode de fonctionnement n'est pas réalisable. Il proposera alors un fonctionnement permettant l'activation de l'un ou l'autre de ces équipements (fonctionnement en HO et HNO)

Un poste déporté au PC Sécurité du conseil départemental sera proposé en option et le soumissionnaire précisera la sécurité associée.

Le soumissionnaire proposera en option la fourniture d'un écran 42 pouces pour la visualisation des images (loge du concierge) Cet écran sera à technologie LED et disposera des caractéristiques minimum :

Résolution de dalle de 1920 x 1080 p

Luminosité minimale de 500cd/m2

Contraste de 1500000 : 1

Temps de réponse : 5ms

incrustation d'image, Picture in picture (PIP)

Gestion des enquêtes

La solution permet la recherche d'événements-alarmes, mémo, signet, méta data et de visualiser la vidéo éventuellement associée à l'événement.

Gestion de la cartographie

Le système dispose d'un outil de cartographie dynamique permettant de localiser tous les équipements de sécurité (caméra, portillon, porte surveillée, contrôle d'accès, lecteur RFID, haut parleur, sirène, détecteur de présence, etc...) sur un plan. Le plan et ses équipements peuvent s'afficher à l'échelle (proportion respectées), par zone, par bâtiment et par étage.

La cartographie accepte les fonctions de zooms avant/arrière à partir de la molette de la souris (par exemple). Le système permet de zoomer dans le plan, de se diriger à 360°.

Le système dispose d'une cartographie multi sites et multi niveau.

La cartographie permet d'exécuter des actions de type glisser/déposer de la cartographie vers toute vignette d'affichage pour permettre :

1) de visualiser une caméra par action de déposer d'une caméra vers une vignette d'affichage;

2) de visualiser les événements liés à une porte par action de déposer d'une porte vers une fenêtre;

3) de visualiser les photos des titulaires identifiés sur une porte par action de glisser déposer d'une porte vers une vignette d'affichage;

La cartographie permet de proposer une aide contextuelle par équipement. il devra apparaître un encadré dans lequel devra figurer leur appellation, leur position (étage, zone de sûreté...) et le moyen de détection (détecteur, détecteur/contrôleur, caméra fixe, mobile etc.).

Ce plan graphique, disponible sur les postes d'exploitation, servira en particulier à la visualisation des événements.

Par ailleurs, ces événements entraîneront une animation des éléments graphiques représentant les équipements (barrières infrarouges, détecteurs d'intrusion, caméras etc.) de la zone concernée.

Lorsqu'un événement se produit dans une zone qui est constituée d'une (ou plusieurs) caméra(s) et/ou d'une barrière infrarouge ou autre détecteur de mouvement, chaque équipement de la zone de détection, qui aura déclenché l'alarme, sera automatiquement signalé par un changement de couleur et d'un clignotement sur la cartographie .

Exemple: la caméra de visualisation passe en rouge de même que le (ou les) faisceau(x) franchi(s) reliant deux barrières infrarouges, etc...).

Par contre, ce changement de couleur sera différent suivant l'état du système :

en rouge lors du déclenchement d'une alarme et restera en rouge tant que l'alarme ne sera pas acquittée,

- en orange lors du déclenchement d'une panne.

8 EXIGENCES SÉCURITAIRES

Tableau des mesures de sécurité :complémentaires à prendre en compte.

1	Organisation de la sécurité des SI	Contrat de maintenance 5j/7 – HO avec intervention sous 24H	UCA, serveurs, lecteurs

2	Organisation de la sécurité des SI	Ajouter à l'ensemble des marchés publics les clauses de sécurité établies par la DSIC (cf site SSI DSIC)	Serveur, UCA, postes administrateur
3	Organisation de la sécurité des SI	Exiger une enquête de sécurité sur les prestataires. Conformément aux PES, les administrateurs encadrent les prestataires pour chaque intervention technique. Pour les travaux nécessitant un accès aux locaux techniques, la présence d'un admin MI est obligatoire	Serveur, /UCA, postes administrateur
4	Organisation de la sécurité des SI	Interdire la télémaintenance depuis les locaux d'une entreprise privée. La maintenance du SI devra se faire in situ (clause à ajouter au CCTP)	Serveur, commutateur, UCA, lecteurs
5	Évaluation de la sensibilité et protection des documents	Protection des clefs de lecture Idéalement : La clé de lecture est répartie sur plusieurs porteurs ; sécurité liée à la gestion (introduction dans la solution) sécurité et inviolabilité des équipements de stockage des clés (lecteurs, coffres pour les badges de configuration éventuels, base de données éventuelles, etc..) sécurité lié au renouvellement ;	Lan Commutateurs, Serveur , UCA, Poste admin , Badges admin, lecteurs, Équipes admin, Badges utilisateurs,
6	Évaluation de la sensibilité et protection des documents	Les clefs et en particulier la clef de lecture, ne doivent en aucun cas être communiquées aux installateurs	Lan Commutateurs, Serveur , UCA, Poste admin , Badges admin, lecteurs, Équipes admin, Badges utilisateurs,
7	Ressources humaines	Formation et sensibilisation des administrateurs SIC aux PES et mesures de sécurité « Contrôles d'accès » et des gestionnaires d'accès aux règles de gestion des accès (P3S)	
8	Sécurité physique des locaux	Les équipements seront installés dans des locaux sécurisés par contrôle d'accès	UCA, Poste admin , Badges admin
9	Sécurité physique des locaux	Alimentation électrique secourue – onduleur, groupe électrogène – Climatisation – Détection incendie. En cas de coupure électrique, les portes ou portiques devront rester, par défaut, en position fermée.(et verrouillées voir sécurité incendie)	Lan Commutateurs, Serveur , UCA, Poste admin , lecteurs,
10	Sécurité physique des locaux	Sécuriser l'accès aux locaux sensibles (locaux techniques,...), par la mise en œuvre d'un second mécanismes de contrôle (ex : digicode ou biométrie). Avec deux mesures à mettre en œuvre : - une mesure technique pour la gestion des droits administrateur applicatifs - une mesure pour le processus de validation des droits	Serveur, commutateurs
11	Architecture et exploitation des SI	Redondance des UCA et répartition des lecteurs d'une même zone sur plusieurs contrôleurs.	UCA, lecteurs
12	Architecture et exploitation des SI	Redondance lecteurs : Utilisation d'un autre accès en cas d'indisponibilité d'un lecteur	Lecteur
13	Architecture et exploitation des SI	Redondance des commutateurs, architecture sécurisée Une architecture 2 minimum serait souhaitable pour disposer des moyens de sécurisation nécessaires. L'objectif est d'assurer un niveau de disponibilité maximum sur les commutateurs avec une durée d'indisponibilité maximum de 24 heures.	Commutateur LAN
14	Architecture et exploitation des SI	Redondance du poste administrateur permettant la gestion des accès	Poste admin
15	Architecture et exploitation des SI	Prévoir plusieurs badges administrateurs	Poste admin , Badges admin,
16	Architecture et exploitation des SI Gestion de la continuité des SI	- Sauvegarde quotidienne au minimum des données sensibles (clefs de lecture, profil, logs) - Copie physique du disque système à chaque modification importante (stocké dans un local éloigné et sécurisé)	Équipe d'administration Serveur

17	Architecture et exploitation des SI	Mettre en place et vérifier le bon fonctionnement des mises à jour automatiques de l'antivirus de façon régulière sur l'ensemble des équipements informatiques. Appliquer la politique de configuration ministérielle Procéder à une analyse antivirale quotidienne des serveurs	Serveurs, postes admin
18	Architecture et exploitation des SI	1. Mettre en place les correctifs de sécurité et upgrade applicatifs matériels	Serveurs, postes admin, UCA, Commutateurs, Lecteurs
19	Architecture et exploitation des SI	Autonomie des UCA par rapport aux serveurs : Les UCA doivent avoir une copie de la base des droits afin de continuer à fonctionner de manière autonome. Toutes les UCA pourront fonctionner sans perturbation en cas de perte de la liaison avec les équipements en amont.	UCA
20	Architecture et exploitation des SI	Mettre en œuvre un réseau physique dédié aux équipements contribuant à la mise en œuvre des systèmes de sécurisation. A défaut, une solution basée sur les technologies VPN IPSEC (dont la configuration devra être conforme aux recommandations de l'ANSSI) sera mise en œuvre. L'objectif étant d'isoler les enclaves du système de contrôle d'accès (sous forme de DMZ) et les interconnecter entre elles par VPN IPSEC. Aucune interconnexion ne devra être possible entre le RGT et les enclaves « Contrôle d'accès » entre les VLANs RGT (serveur, postes de travail, …) d'un site et les enclaves « Contrôle d'accès »	Lan Commutateurs, serveur, UCA, postes administrateur
21	Architecture et exploitation des SI	La communication entre le badge, la tête de lecture et l'UCA sera chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS27)	Lan Commutateurs, Serveur , UCA, Poste admin ,
22	Architecture et exploitation des SI	Les outils d'administration devront intégrer les protocoles SSL/TLS. Ces protocoles seront également appliqués pour les échanges entre les lecteurs et les UCA.	Administrateur, UCA, lecteurs
23	Architecture et exploitation des SI	Protection physique des lecteurs : Les têtes de lecture devront être équipées d'un système de détection d'intrusion et d'arrachage, leurs fixations devront être renforcées.	Lecteurs
24	Architecture et exploitation des SI	Sécuriser les BDD de type Oracle conformément aux PES	Serveur
25	Architecture et exploitation des SI	Procéder au cloisonnement des ressources serveurs dans une DMZ dédiée à cet effet	Serveur
26	Gestion des autorisations ou accès logique aux ressources	Restreindre l'accès aux interfaces d'administration aux seuls administrateurs explicitement identifiés et authentifiés (ex : filtrage réseau, FW,...)	Serveur, UCA, postes administrateur, commutateurs
27	Gestion des autorisations ou accès logique aux ressources	Interdire l'accès aux fichiers de données aux prestataires Créer des comptes nominatifs pour les prestataires. Ces comptes devront être supprimer dès la fin de la prestation (cf procédure circuit arrivée/départ)	Serveur, postes administrateurs
28	Gestion des autorisations ou accès logique aux ressources	Journalisation des opérations réalisées par les administrateurs et installateurs Journalisation des actions sur le système de contrôle d'accès (création de badge, ouverture d'autorisation d'accès à des locaux, création d'utilisateurs dans la BDD, …)	Serveur, postes admin
29	Gestion des autorisations ou accès logique aux ressources	Prévoir des badges temporaires ainsi qu'une procédure ad-hoc de délivrance et restitution de ces badges	Badges utilisateurs

30	Gestion des autorisations ou accès logique aux ressources	Utilisation de comptes nominatifs et de la carte agent pour l'authentification des administrateurs. Les comptes nominatifs des prestataires devront être activés/désactivés suivant les besoins d'intervention (cf procédure spécifique compte nominatifs prestataires)	Administrateur
31	Gestion des autorisations ou accès logique aux ressources	Renouvellement des clefs et procédures de plusieurs porteurs Les clés sont classées par niveau de sensibilité. Idéalement les clés les plus sensibles (clé de lecture,etc.) sont réparties sur plusieurs porteurs Le système prévoit une gestion de renouvellement de clés minimisant les impacts fonctionnels	Badges utilisateur, badges administrateur
32	Gestion de la continuité des SI	En cas fonctionnement en mode dégradé (coupure électrique ou interruption des serveurs/UCA): garde statique, ouverture des accès stratégiques par clefs	Lecteurs, Lan Commutateurs, Serveur UCA, Système de verrouillage
33	Gestion de la continuité des SI	Assurer la continuité de la fonction administration du SI : gestion des congé, astreintes, ….	Équipes admin
34	Gestion de la continuité des SI	Rédiger des fiches réflexes à appliquer en cas d'activation du plan de reprise d'activité (PRA) - S'assurer que les logiciels listés dans les fiches réflexes soient disponibles	Serveur
35	Gestion de la continuité des SI	S'assurer de la disponibilité des matériels listés dans les fiches réflexes : (plate-forme de secours, ...),	Serveur
36	Gestion de la continuité des SI	Prévoir un stock de maintenance pour les commutateurs	Lan Commutateurs
37	Conformité et contrôle	Respect du « document de référence technique puce sans contact » rédigé par le SHFD	Lecteurs, Badges admin, Serveur , UCA, badges utilisateurs

9 DEMONTAGE

9.1 DÉPOSE

Le démontage comprend la dépose des installations devenues inutiles (lecteurs de badges, fixations, réglettes de câblage, câbles, boîtes de distribution, prises, serrures, etc.), supports de câbles inclus (tubes, goulottes, plinthes, moulures, etc.). Ce démontage sera effectué soigneusement. Tous les câbles colliers, attaches, ferrures seront enlevés et les trous rebouchés. Les anciennes prises encastrées seront obturées par des caches appropriés.
Le maintien de certains câbles dont le démontage entraînerait des dégradations trop importantes du point de vue esthétique (éclats de peinture, etc ...) est soumis à l'accord du maître d'ouvrage. Ces câbles seraient alors laissés sur place et coupés à ras, de manière à rendre leur inutilité évidente et à faciliter leur retrait lors de travaux futurs.
Cette prestation sera définie avec le soumissionnaire lors de la visite préalable de site.

9.2 STOCKAGE

Un local fermant à clé sera mis à disposition du titulaire par l'administration. Son emplacement sera défini lors de la visite de site en accord avec le pôle des moyens généraux de la Préfecture.
Ce local permettra d'entreposer le matériel en attente d'installation ainsi que tout élément démonté.

9.3 RECYCLAGE

Recyclage par le titulaire

Le soumissionnaire prendra à sa charge l'enlèvement et le recyclage de tout matériel démonté comme indiqué au § 11.1.

Une exception sera faite pour tout élément contenant des données sensibles (disque dur, etc...). Les disques durs ne peuvent en aucun cas quitter le périmètre du site et seront remis à l'administration qui se chargera de les détruire. Aucune donnée ne peut être dupliquée sur tout support hors du site conformément aux recommandations SSI.

10 DOCUMENTATION

10.1 DOCUMENTATION TECHNIQUE

Le titulaire du marché devra mettre à disposition une documentation complète sur les systèmes mis en œuvre comprenant :

- ✔ les documentations techniques en français des matériels installés
- ✔ le Dossier des Ouvrages Exécutés (D.O.E .) comprenant :
  - l'emplacement de tous les équipements installés (caméras, détecteurs , UCA, postes clients. …. ;
  - le cheminement des câbles posés (courant fort et faible);
  - les plans mis à jour au format dwg et ou pdf ;
    Ce document devra revêtir le timbre « DIFFUSION RESTREINTE »

Toutes les pièces constituant cette documentation seront fournies en français sous forme de fichier électronique lisibles à partir de logiciels libres.

10.2 DOCUMENTATION D'ADMINISTRATION ET D'EXPLOITATION

Le titulaire du marché devra mettre à disposition une documentation d'exploitation des différents systèmes mis en œuvre comprenant :

- Un manuel d'administration système et des application;
- Un manuel d'exploitation de chaque système ;
- Une procédure de reprise des activités du système couvrant notamment l'arrêt forcé des équipements, leur redémarrage sur incident .
- Les consignes de sécurité pour le bon usage de la solution ;
- Un guide de mise en place du système d'information.

La documentation est en version française.

Sauvegarde - Restauration

Le titulaire du marché devra mettre à disposition une documentation sur les procédures de sauvegarde et restauration des données permettant :

* une sauvegarde journalière, hebdomadaire
* une sauvegarde/restauration différentielle, incrémentielle et complète

11 FORMATIONS

Le service demandeur doit préciser les formations souhaitées et par type de profil des personnels exploitants.

Les formations seront assurées par des animateurs de formation spécialisés et habitués à ces types de formation.

Elles se dérouleront à temps plein sur le site du client

L'objectif est, qu'à l'issue de la formation, les personnels soient pleinement opérationnels dans le domaine de travail qu'ils doivent assurer.

Les supports de cours seront fournis en langue française, au format papier et au format électronique lisibles à partir de logiciels libres. Ils seront classifiés en «DIFFUSION RESTREINTE»

Le titulaire proposera le contenu ainsi que la durée et le nombre de sessions qui seront adaptées au nombre de participants dans chaque domaine (administrateurs et exploitants).

11.1 FORMATION DES ADMINISTRATEURS

Le module dédié à la formation des administrateurs leur permettra d'appréhender complètement les systèmes mis en œuvre pour ce qui concerne l'installation, la configuration et l'utilisation des différentes applications avec en particulier :

- La gestion des comptes exploitants
- La gestion des clés de chiffrement
- La gestion du temps
- La gestion des calendriers
- La gestion des scénarii
- La gestion de l'antivirus
- La gestion des sauvegardes
- La gestion des images
- Le stockage et exportation des données
- et tout autre item proposé par le titulaire

La formation sera assurée pour **10** personnes

11.2 FORMATION DES GESTIONNAIRES DE BADGES

Le module dédié à la formation des gestionnaires de badges leur permettra d'appréhender complètement les systèmes mis en œuvre pour ce qui concerne l'enrôlement, la configuration et l'utilisation des badges avec en particulier :

- La gestion des profils
- La gestion des badges
- La gestion du temps
- La gestion des calendriers
- et tout autre item proposé par le titulaire

La formation sera assurée pour **15** personnes

11.3 FORMATION DES OPÉRATEURS

Le module dédié à la formation des opérateurs leur permettra d'utiliser de manière optimale les différentes applications mises à disposition avec en particulier :

- la présentation des équipements des postes PCS (stations, murs d'images, imprimantes),
- la présentation du poste de travail : les différentes fenêtres, agencement des écrans...,
- le démarrage et l'arrêt des stations de travail,
- la connexion et la déconnexion aux applications,
- l'exploitation de la vidéo-protection, de l'alarme, du contrôle d'accès et de la visiophonie,
- la gestion de badges « visiteurs »,
- la gestion des événements et alarmes,
- et tout autre item proposé par le titulaire.

La formation sera assurée pour **20** personnes

12 RECETTE

La réception de la prestation est conditionnée par la fourniture de la documentation détaillée des architectures et des systèmes installés (spécifications techniques, paramétrages, configuration et exploitation, plan de recollement, fiches réflexes, etc..) ;

La recette technique se compose d'un contrôle d'inventaire, d'un contrôle visuel et d'un contrôle fonctionnel.

La recette technique est l'opération qui permet de garantir au maître d'ouvrage que l'installation est conforme :

- ✔ au C.C.T.P. ;
- ✔ aux performances attendues,
- ✔ aux normes et réglementations en vigueur,
- ✔ au guide d'installation du constructeur pour l'obtention de la garantie,
- ✔ aux règles de l'art.

12.1 RECETTE DE L'INFRASTRUCTURE RÉSEAU

12.1.1 Le contrôle visuel

Après un contrôle quantitatif et qualitatif des composants fournis, le contrôle visuel portera sur la qualité générale de la prestation. On vérifiera notamment :

- ✔ le respect des contraintes d'environnement,
- ✔ la mise en œuvre des câbles,
- ✔ la fixation des éléments (baies, panneaux, prises, modules, supports, etc.),
- ✔ la mise à la terre des éléments,
- ✔ l'installation des éléments actifs,
- ✔ l'étiquetage et le repérage des différents éléments,
- ✔ l'aspect esthétique,
- ✔ le rebouchage.

12.1.2 Le contrôle fonctionnel

Le contrôle fonctionnel portera sur le comportement du système installé et plus particulièrement sur son aptitude à supporter les applications telles que définies dans le présent document. Pour ce qui concerne le câblage, ce contrôle comprendra notamment, pour chaque liaison permanente (permanent link), la mesure des paramètres définis dans la norme ISO/IEC 11801 2ème édition 1er amendement.
La recette fonctionnelle comprend les tests et mesures effectués sur l'installation de manière exhaustive.
Tous ces résultats seront consignés dans le dossier de recette du pré-câblage au format électronique de type pdf.

12.1.2.1 Tests des liaisons cuivre

Les tests de mesures à effectuer auront pour objet de vérifier que chaque paire est conforme d'une part, au plan d'installation, et d'autre part, à la qualité de transmission exigée.
A ce titre, le contrôle devra s'assurer pour chaque paire :

- ✔ du raccordement correct de chaque extrémité et de la continuité de chaque paire ;
- ✔ du respect des polarités et de l'absence de court-circuit entre les conducteurs ;
- ✔ de l'isolement par rapport à la terre et aux autres conducteurs ;
- ✔ de l'absence de dépairage ;
- ✔ de la résistance en boucle ;

- ✔ de l'exactitude de son identification par rapport aux plans d'installation.

Toutes les liaisons "cuivre" devront être testées en configuration "**Permanent Link**". Ces tests devront être conformes à la norme ISO/IEC 11801 Edition 2, le câblage conforme au standard EIA/TIA-568-B.

Chaque fiche de test devra au minimum indiquer :
• la date du test,
• l'identification du lien,
• l'affectation des paires (WIRE MAP),
• la longueur des paires,
• l'impédance,
• l'affectation des paires (WIRE MAP),
• la résistance de boucle (DC LOOP RESISTANCE),
• la perte par insertion (INSERTION LOSS),
• la paradiaphonie (NEXT et PS NEXT),
• la télédiaphonie (FEXT et PS FEXT),
• le rapport Signal/Bruit (ACR et PS ACR / ELFEXT et PS ELFEXT),
• la perte par réflexion (RETURN LOSS),
• le délai de propagation (PROPAGATION DELAY),
• l'écart de propagation (SKEW).

En outre, la copie du certificat d'étalonnage ou la preuve d'achat (pour un appareil de moins d'un an) du testeur devra accompagner le rapport de test final.

- ✔ L'ensemble de ces tests est à la charge du titulaire.

12.1.2.2 Tests des liaisons optiques

Deux mesures, dans les deux sens et à des longueurs d'ondes différentes selon le tableau ci-dessous.

Tests des liaisons optiques

- Toutes les liaisons optiques devront être testées dans les deux sens à l'aide d'un réflectomètre FO (OTDR) suivant le standard ISO/IEC 14 763-3. Ces mesures ont pour but de s'assurer qu'aucune anomalie n'est présente sur la liaison optique :
- défaut de raccordement,
- atténuation élevée,
- début de cassure ou contrainte.
- Chaque fiche de test devra au minimum indiquer :
- la date du test,
- l'identification du lien,
- la longueur de la fibre,
- l'atténuation mesurée (ainsi que les valeurs de chaque connecteur)
- la longueur d'onde pour le test,
- la direction dans laquelle le test a été réalisé.

L'ensemble de ces tests est à la charge du titulaire.

	Multimode		Monomode	
Longueur d'onde (nM)	850	1300	1310	1550
Atténuation maximum (dB/kM)	3,5	1,5	1,0	1,0

12.2 RECETTE DU COURANT FORT

12.2.1 Le contrôle visuel

. On vérifiera notamment :

- ✔ le respect des contraintes d'environnement,
- ✔ le cheminement des câbles,
- ✔ la mise en œuvre des câbles, fixation, connexion,
- ✔ la mise à la terre des éléments,
- ✔ l'étiquetage et le repérage,
- ✔ le rebouchage.

12.2.2 Le contrôle fonctionnel

Le contrôle fonctionnel portera sur :

- le comportement en fonctionnement normal,
- le comportement de l'installation en mode dégradé : coupure de l'énergie et vérification de la continuité de service correspondant aux dimensionnements des onduleurs.

12.3 RECETTE DES DIFFÉRENTS SYSTÈMES

Chaque système : contrôle d'accès, postes de travail, sera contrôlé et réceptionné indépendamment.

Toutes les exigences décrites dans le chapitre correspondant sont testées à partir d'un cahier de recette qui sera défini durant les travaux préparatoires. Le titulaire propose à l'administration le cahier de recette que l'administration fait compléter et valider.

Les contrôles sont réalisés en présence du représentant de l'administration notamment pour ce qui a trait aux performances des équipements (détecteur et caméras) qui peuvent être mesurées spécifiquement par des tests d'intrusion.

12.3.1 Le contrôle quantitatif et qualitatif

Chaque matériel fourni par le titulaire sera comptabilisé et ses caractéristiques comparées à l'offre initiale.

Le titulaire s'engage à ce que la solution livrée soit protégée contre les virus et les logiciels malveillants connus au jour de l'installation.

L'origine des installations, matériels ou logiciels et de leurs mises à jour doit pouvoir être garantie.

12.3.2 Le contrôle fonctionnel

- Le contrôle fonctionnel portera sur le comportement du système installé.
- La recette fonctionnelle comprend les tests effectués sur l'installation de manière exhaustive.
- Tous ces résultats seront consignés dans le dossier de recette.
- La recette sera effectuée par l'administration en présence du titulaire.
- Le contrôle devra donc s'assurer :
  - ✔ des unités de gestions et lecteurs de badge,
  - ✔ du bon paramétrage et du bon fonctionnement des logiciels de gestion du système,

- ✔ des fonctionnalités de visualisation et d'automatisation des ouvertures.

12.4 PROCÈS VERBAL DE RECETTE

Le procès verbal de recette comportera le compte-rendu des contrôles visuel et fonctionnel.
Il sera composé de 2 parties distinctes :

- ✔ Infrastructure,
- ✔ Systèmes de sécurisation.

La réception définitive des travaux ne sera prononcée qu'après l'exécution de l'ensemble des essais et contrôles des systèmes de sécurités installés et après la fourniture d'un dossier technique complet comprenant en particulier la nomenclature des équipements, les plans de câblage et de raccordement, les notices d'exploitation et d'entretien.

Si le procès-verbal fait état de réserves motivées par des omissions ou des imperfections, le titulaire disposera d'un délai de 15 jours à définir avec le maître d'ouvrage pour exécuter les travaux nécessaires. Passé ce délai, le maître d'ouvrage pourra se réserver le droit de faire exécuter les travaux par une autre entreprise, aux frais, risques et périls du titulaire défaillant.

12.5 LES FICHES DE RECETTE

Les fiches de recette, fournies par le titulaire et complétées par l'administration, comprennent :

- la méthodologie et les procédures de tests ;
- la description des tests ;
- les procès verbaux.

Ces trois étapes sont définies en concertation avec le titulaire.

12.6 VABF

La vérification d'aptitude et de bon fonctionnement (VABF) porte sur le respect des spécifications du CCTP et des résultats des tests. La VABF sera conduite par le titulaire, un représentant de l'administration, assistée par la MOE.
La durée de la VABF est de 30 jours ouvrés à partir de la validation de la recette.

Un procès verbal est établi par la maîtrise d'ouvrage pour la validation de la VABF, conjointement avec le titulaire, à l'issue des opérations de validation, et propose pour l'administration une décision qui mentionne selon les cas :

- La réception sans réserve valant constat d'aptitude et de bon fonctionnement,
- La réception avec réserves (ajournement),
- Le rejet.

Ce procès verbal cosigné est transmis au pouvoir adjudicateur, qui notifie sa décision au titulaire dans un délai de 30 jours ouvrés.

La décision d'ajournement prévoit le délai imparti au titulaire pour remédier aux dysfonctionnements constatés. A l'issue de ce délai, une nouvelle procédure de validation de la VABF sur site est mise en place. Suite à cette nouvelle procédure, si des dysfonctionnements sont constatés, il sera procédé au rejet définitif de la prestation. Dès lors, la résiliation du marché aux torts exclusifs du titulaire peut être prononcée.

La décision d'acceptation avec réserves fixe le délai de levée des réserves. A cette issue, il sera procédé à de nouvelles vérifications. Il sera alors établi un procès verbal de levée de réserves. Le

constat d'aptitude et de conformité technique est dès lors réputé acquis à la date de l'établissement du premier procès verbal.

12.7 VSR

La période de vérification de service régulier (VSR) est d'une durée de 60 jours ouvrés à compter de la date de réception de la VABF; elle est reconductible une fois, en cas d'ajournement. Elle est destinée à vérifier le bon fonctionnement des systèmes de sécurité dans les conditions d'exploitation définies par l'administration, avec la qualité de service définie dans le CCTP.

En cas de dysfonctionnement, l'administration peut être amenée à prononcer des réserves. Le titulaire doit remédier à ces problèmes dans un délai de 15 jours ouvrés. Un procès verbal de vérification de service régulier est établi à l'issue de cette période de VSR, après correction des éventuels dysfonctionnements, et fourniture de l'ensemble des livrables.

A l'issue, en cas de dysfonctionnements toujours constatés, l'ajournement de l'admission peut être prononcé, avec mise en demeure de les corriger. En cas de carence du titulaire dans les délais impartis, il est procédé au rejet définitif de la solution. Le rejet n'est prononcé par l'administration qu'après constat contradictoire de ces dysfonctionnements. La résiliation du marché aux torts exclusifs du titulaire, ou la mise en régie aux frais et risques de ce dernier, peut dès lors être prononcée.

En tout état de cause, la réception définitive n'est effective qu'après constat de la livraison de l'ensemble des documents requis. Elle fait l'objet d'une décision expresse de l'administration, qui intervient au plus tard dans le délai de 15 jours ouvrés à compter du constat de levée de réserves ou de levée des motifs d'ajournement prononcés dans le cadre de cette VSR.
Elle est ensuite notifiée au titulaire.

12.8 RÉCEPTION DÉFINITIVE

La réception définitive de la solution n'est prononcée qu'après remise des documents permettant la prise en charge des installations par le Maître d'Ouvrage et au terme de la VSR.

Dans le cas où le Maître d'Ouvrage serait amené à prendre possession des installations sans la remise de ces documents, les installations sont exploitées suivant les instructions de l'entreprise et sous sa responsabilité, sans que cette dernière puisse prétendre à indemnisation

13 GARANTIE

13.1 MODALITÉS

La garantie est d'une durée de 2 ans débute à compter de la réception définitive de l'installation.

Elle comprend l'échange de pièces, la main d'œuvre et les déplacements, à l'exception des disques durs qui font l'objet d'un cas particulier :

Les disques durs remplacés ne peuvent en aucun cas quitter le périmètre du site et sont remis à un représentant de la Préfecture (contre décharge si besoin). Aucune donnée ne peut être dupliquée sur tout support hors du site.

Durant la période de garantie, le titulaire s'engage à remplacer à l'identique, à réparer ou à modifier toutes les pièces ou éléments reconnus défectueux. Il doit corriger les erreurs constatées au sein des logiciels fournis.

Les modalités d'accès à la maintenance seront mises en place par le titulaire qui fournira la procédure de signalisation des dérangements.

Les incidents seront enregistrés sous forme de tickets numérotés qui indiqueront :

- l'identité et la localisation du demandeur ;
- le descriptif précis du dérangement ;
- la date et l'heure de signalisation;

La télémaintenance est proscrite, si la résolution de l'incident n'est pas possible d'une manière simple et rapide par assistance téléphonique, le dépannage devra se faire par déplacement d'un technicien.

13.2 INTERVENTIONS PENDANT LA PÉRIODE DE GARANTIE

Au préalable, une liste de techniciens devra être fournie au service sécurité avant toute intervention (Nom, prénom, date et lieu de naissance). Cette liste devra être renouvelée tous les 3 mois dans le cadre de l'enquête administrative.

13.2.1 Définition de la gravité de l'incident

Deux niveaux de gravité d'incident sont définis :

- Panne urgente:

Une panne urgente correspond à une panne rendant le système complètement inexploitable ou sur les accès sensibles.

- Panne non urgente:

Toutes les autres pannes sont considérées comme non urgentes.

13.2.2 Garanties de temps de rétablissement (GTR)

- Panne urgente (option 1):

Elle devra être réparée dans les 4 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi)

- Panne urgente (option 2):

Elle devra être réparée dans les 4 heures suivant la signalisation de l'incident en mode 7 jours sur 7, 24 heures sur 24.

- Panne non urgente :

Elle devra être réparée dans les 16 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi).

Le début de la période prise en compte dans le cadre des garanties de rétablissement correspond aux date et heure de signalisation d'incident (ticket horodaté).

13.3 MISES À JOUR

Pendant la période de garantie, les mises à jour préconisées par le constructeur ou permettant de corriger une anomalie pourront être installées après accord préalable de l'administration

Une procédure de mise à jour sera définie pour maintenir le service opérationnel (définition d'un plan de repli pendant la mise à jour, choix d'un moment propice dans la journée …)

13.4 MESURES PREVENTIVES

Pendant la période de garantie, une visite annuelle préventive, conforme aux règles APSAD sera réalisée par le titulaire.

13.5 INTERVENTIONS APRÈS LA PÉRIODE DE GARANTIE

A l'issue de la période de garantie, l'administration procédera à une consultation pour un marché de maintenance pluri-annuel.

14 ANNEXES

Le présent CCTP est complété par une description détaillée d'annexes qui serviront à l'établissement de la proposition financière et technique, notamment par des plans de l'existant en matière de protection des bâtiments. Ces annexes seront fournis lors de la visite obligatoire de la Cité administrative.

14.1 ANNEXE 1 : SYNOPTIQUE DU PROJET

Un synoptique du projet sera remis lors de la visite sur site par l'administration

14.2 ANNEXE 2 : PLANS

Un document comportant les plans sera remis lors de la visite sur site.

14.3 ANNEXE 3 : RÉCAPITULATIF DES ÉQUIPEMENTS

Cette annexe décrit les contrôles existant, les contrôle d'accès supplémentaires souhaités et les contrôles d'accès commun préfecture et conseil départemental.

- le type d'équipement souhaité (platine, moniteur, écran, ..)
- les commandes d'ouverture à mettre en place ou à conserver
- les observations

14.4 ANNEXE 4 : RÉPONSES TECHNIQUES DU SOUMISSIONNAIRE

Cette annexe Cadre de Réponse Technique (CRT) est à remplir obligatoirement dans le cadre de la réponse technique et vient en complément de la réponse au CCTP.

14.5 ANNEXE 5 : BORDEREAU DES PRIX

Cette annexe, fournie par l'administration, est à remplir obligatoirement dans le cadre de la réponse technique et vient en complément de la réponse au CCTP.

14.6 ANNEXE 6 : RÉGLEMENTATION

Cette annexe présente les textes et réglementation en vigueur dans le cadre de la sécurisation des sites et vient en complément du CCTP.
Les prestations, services, matériels et installations doivent être conformes aux normes, règlements et décrets (éditions en vigueur à la date de signature du marché) et respecteront les règles de l'art applicables dans leur dernière édition complétées de leurs additifs.
Les documents de référence sont des documents pouvant être utilement consultés pour élaborer les offres et projets de contrat ainsi que pour l'exécution du contrat.
Pour chaque paragraphe de l'annexe 6, mise à part la hiérarchie des textes législatifs et réglementaire qui s'applique, les références sont citées dans leur ordre hiérarchique. En cas de contradiction, les premières références citées l'emportent sur les suivantes.

D'une manière générale, le titulaire du contrat doit respecter l'ensemble des textes réglementaires - lois, décrets, arrêtés, circulaires - et para-réglementaires - normes, document technique unifié (DTU), avis techniques et solutions techniques.
Le soumissionnaire est tenu d'informer l'administration de toute discordance entre le CCTP et les règles énoncées ou non dans cette annexe, ainsi que de toutes les questions qui pourraient être une source de litige par la suite.