



MINISTÈRE DE L'INTÉRIEUR

SECRÉTARIAT GÉNÉRAL DE LA ZONE DE DÉFENSE ET DE SÉCURITÉ SUD-OUEST  
SECRÉTARIAT GÉNÉRAL POUR L'ADMINISTRATION DU MINISTÈRE DE L'INTÉRIEUR SUD-OUEST  
DIRECTION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION  
CELLULE ZONALE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Site de la Préfecture d'AGEN Lot-et-Garonne (47)

**Cahier des Clauses Techniques Particulières.  
Création d'un système de mise en sûreté.**

**Fourniture et installation d'une solution de contrôle  
d'accès constituant la deuxième phase du système de  
défense global des locaux de la Préfecture**

Référence du CCTP	DSIC / PDE / 2024 du 30 juillet 2024
Rédacteurs	Stéphane DESLANDES – Jérôme COUEGNAT
Responsables techniques Adresse Téléphone E-mail	Bertrand SOUBIE 89 cours Dupré de Saint Maur 33000 Bordeaux 05 57 19 42 30 / 06 80 75 93 98 bertrand.soubie@interieur.gouv.fr
Date d'émission du cahier des charges Version	30/07/2024 1
Pièces jointes	//

# Table des matières

1. DESCRIPTION GÉNÉRALE DU PROJET.....	4
1.1. Objet de la consultation.....	4
1.2. Description batimentaire.....	4
1.3. Description synthétique des prestations.....	5
1.3.1 En cas de présence de parefeux.....	6
1.3.2. Principe retenu.....	7
1.3.3. prestation attendue.....	7
a) pour le contrôle d'accès :.....	8
b) pour le réseau, câblage et baie :.....	8
c) pour les serveurs.....	8
2. DESCRIPTION DE L'EXISTANT.....	10
2.1. Architecture existante.....	10
2.2. Systèmes installés.....	10
2.3. Énergie.....	10
3. DESCRIPTION DES PRESTATIONS A RÉALISER.....	11
3.1. Infrastructure réseau.....	11
3.1.1. Les répartiteurs.....	11
3.1.2. Le local serveur.....	11
3.1.3. Les baies.....	11
3.1.4. La dorsale optique.....	11
3.1.5. Le capillaire cuivre.....	11
3.1.6. Les éléments actifs.....	11
3.1.7. Implantation type des éléments dans les baies de sûreté.....	12
3.1.8. Baie du répartiteur et sous-répartiteurs.....	12
3.2. contrôle d'accès.....	13
3.2.1. Les accès.....	13
3.2.2. Les unités de traitement local (UTL).....	13
3.2.3. Les lecteurs de badges (LB).....	13
3.2.4. La serrurerie (Seulement SI NÉCESSAIRE).....	15
3.3. Maquette.....	17
3.4. Les ordinateurs de gestion.....	17
3.4.1. Les serveurs.....	17
3.4.2. Les stations.....	17
3.4.2.1. Les postes de gestion des badges et d'administration du contrôle d'accès.....	18
3.4.2.2. Le poste de visualisation.....	18
3.5 Courant faible, courant fort, Étiquetage.....	18
3.5.1. Courant faible.....	18
3.5.2. Courant fort.....	18
3.5.3. Étiquetage.....	18
3.5.4. Acteur.....	18
4. INTERFONCTIONNEMENT DES SYSTÈMES.....	19
5. EXPLOITATION DE LA SOLUTION.....	20
5.1. Gestion du Système.....	20
5.2. Exploitation par l'administrateur du système.....	20
5.2.1. Configuration des droits opérateurs.....	20
5.2.2. Gestion des journaux.....	21
5.3. Exploitation par le gestionnaire des badges.....	21
5.3.1. Gestion des badges.....	21
5.3.1.1. Personnalisation des badges utilisateurs.....	21
5.3.1.2. Gestion des profils.....	22
5.3.1.3. Type de badge (CAM).....	22
5.3.1.4. Invalidation des badges.....	23
5.3.1.5. État d'un badge.....	23
5.3.2. Gestion des rapports.....	23

5.4. Exploitation par les opérateurs.....	23
5.4.1. Gestion TYPE PC Sécurité (PCS).....	23
5.4.1.1. Aménagement du PCS.....	23
5.4.1.2. Gestion des enquêtes.....	24
5.4.1.3. Gestion de la cartographie.....	24
5.4.1.4. Gestion des alarmes.....	24
5.4.1.5. Gestion du scénario.....	25
5.4.2. Principe de gestion des réactions à événement.....	25
6. EXIGENCES SÉCURITAIRES.....	27
7. DÉMONTAGE.....	30
7.1. Dépose.....	30
7.2. Stockage.....	30
7.3. Recyclage.....	30
8. DOCUMENTATION.....	31
8.1. Documentation technique.....	31
8.2. Documentation d'administration et d'exploitation.....	31
8.3. Sauvegarde – Restauration.....	31
9. FORMATIONS.....	32
9.1. Formation des Administrateurs.....	32
9.2. Formation des Gestionnaires de Badges.....	32
9.3. Formation des Opérateurs.....	32
10. RECETTE.....	33
10.1. Recette de l'Infrastructure Réseau.....	33
10.1.1. Le contrôle visuel.....	33
10.1.2. Le contrôle fonctionnel.....	33
10.1.2.1. Tests des liaisons cuivre.....	33
10.1.2.2. Tests des liaisons optiques.....	34
10.2. Recette du courant fort.....	34
10.2.1. Le contrôle visuel.....	34
10.2.2. Le contrôle fonctionnel.....	34
10.3. Recette des différents systèmes.....	35
10.3.1. Le contrôle quantitatif et qualitatif.....	35
10.3.2. Le contrôle fonctionnel.....	35
10.4. Procès Verbal de recette.....	35
10.5. Les fiches de recette.....	35
10.6. VABF.....	35
10.7. VSR.....	36
10.8. Réception définitive.....	36
11. GARANTIE.....	37
11.1. Modalités.....	37
11.2. Interventions pendant la période de garantie.....	37
11.2.1. Définition de la gravité de l'incident.....	37
11.2.2. Garanties de temps de rétablissement (GTR).....	37
11.3. Mises à jour.....	37
11.4. Interventions après la période de garantie.....	37
12. ANNEXES.....	38
ANNEXE 1 : Principes concernant les équipements de l'installation et leur raccordement.....	38
ANNEXE 2 : Principes concernant le système de contrôle d'accès.....	38
ANNEXE 3 : Principes concernant la réglementation.....	38
ANNEXE 4 : Tableau des points de sûreté.....	39
ANNEXE 5 : Plan des points de sûreté.....	39

## 1. DESCRIPTION GÉNÉRALE DU PROJET

### 1.1. 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 la mise en sûreté de :

#### Adresse des travaux :

**Préfecture de Lot-et-Garonne**

**Place de Verdun**

**47920 Agen Cedex 9**

ATTENTION !

Les annexes ci-après et celles fournies en pièces jointes font partie intégrante de ce CCTP.

À ce titre, leurs prescriptions sont à appliquer, en fonction du périmètre de la prestation demandée, aussi bien pour l'établissement de la proposition financière et technique, que lors de la réalisation des travaux.

### 1.2. Description batimentaire

La préfecture de Lot et Garonne



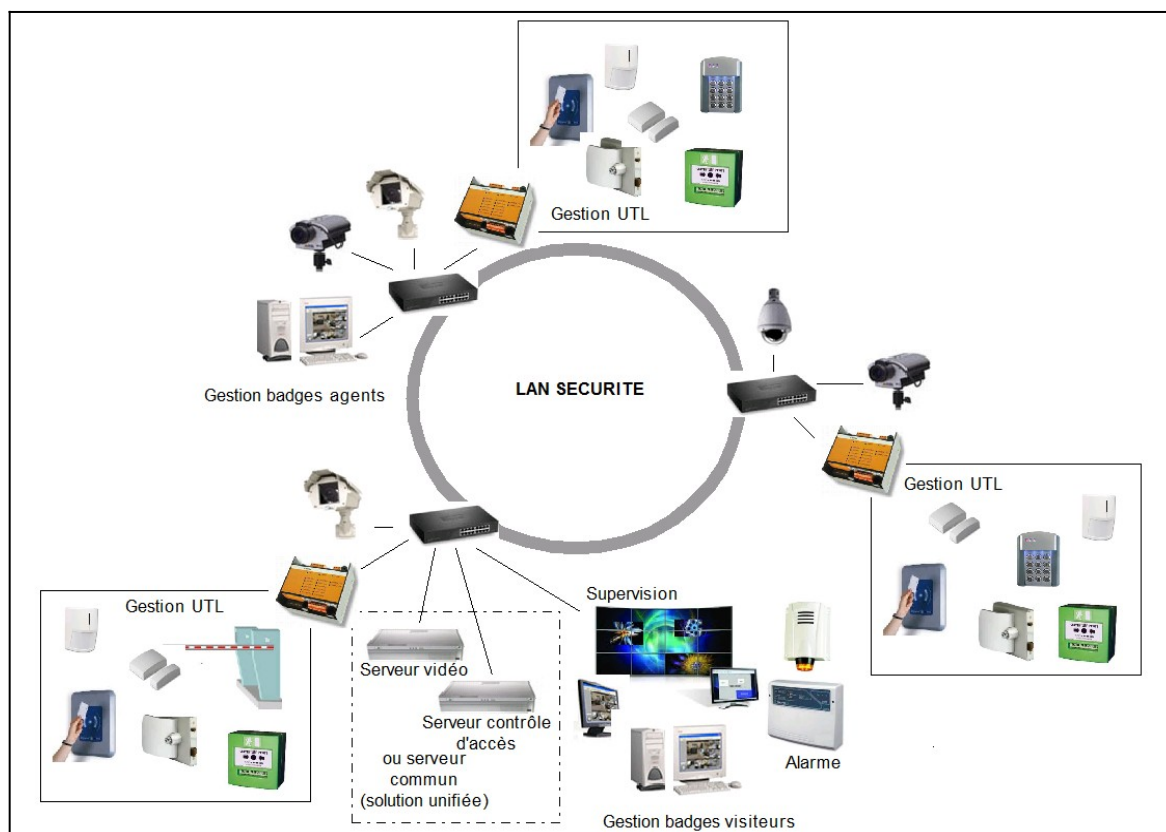
Le bâtiment historique (R+2-1) comporte une partie centrale, encadrée à l'Est par une aile en R+1 et à l'Ouest par une aile de type R+2-1. Les façades et toitures du bâtiment central sont classés « monument inscrit » par arrêté du 09 mai 1947.

Un ajout a été effectué dans les années 1960, relié au bâtiment ancien par une passerelle sur deux niveaux. Cette nouvelle structure « aile neuve » est de type R+3-1.

La superficie totale du site est de 33845m<sup>2</sup>.

Conformément aux demandes locales le présent CCTP inclura la totalité des bâtiments de la préfecture et de son parc.

### 1.3. Description synthétique 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.

**Toutes les liaisons entre les éléments du réseau sûreté (commutateurs, serveurs, stations, contrôle d'accès) seront filaires.**

**Aucun lien sans-fil ne sera admis, sauf spécification explicite contraire présente dans ce CCTP.**

Le périmètre de sécurité comprend, les abords limitrophes des bâtiments, les abords du quartier ainsi que la surveillance des toits, le cas échéant.

Le réseau Ethernet Sûreté sera destiné à accueillir les applications suivantes :

- Vidéosurveillance,
- Contrôle d'accès,
- Détection d'intrusion.

Le LAN sûreté physique sera constitué d'un commutateur Ethernet qui sera le cœur de concentration.

Le commutateur est de type distribution (équipé de ports SFP-1000Base-X), et « POE ».

Ce commutateur possède plusieurs ports 1000baseT pour le raccordement des périphériques critiques (serveur, station d'affichage ou autre).

Le commutateur servira de référence pour tous les raccordements de périphériques « Ethernet-IP ».

Il disposera d'un nombre suffisant d'interfaces gigabits pour supporter les équipements qui y seront raccordés.

Une réserve de 10 % d'interfaces de chaque type sera prévue pour une éventuelle extension.

Les règles de sécurité définies par le Haut Fonctionnaire de Défense (HFD/RCSSI) imposent une étanchéité stricte entre les flux vidéo extérieurs et le reste du Système d'Information de Sûreté (SIS) :

Afin d'assurer l'homogénéité du réseau et la compatibilité avec les composants actifs en service sur le site, les commutateurs Ethernet et pare-feu utilisés dans la solution figureront au catalogue des solutions informatique du Ministère de l'Intérieur.

Cette contrainte s'explique par l'obligation de respecter sur tous les sites du Ministère de l'Intérieur des préconisations d'architectures réseau précises et strictes, et basées sur des matériels validés pour leur aptitude à répondre à ces besoins.

Le respect de ces préconisations, tant du point de vue des éléments actifs est le prérequis incontournable à l'intégration du réseau de protection au réseau local du site objet du présent marché.

Les commutateurs des séries HP 5130 et HP 5140 (utilisation en niveau 2-accès) sont conformes et déployés actuellement par le Ministère de l'Intérieur.

**Les commutateurs seront fournis par l'administration, et configurés et installés en collaboration avec les techniciens du ministère de l'Intérieur.**

**Programmation des commutateurs :**

Le soumissionnaire devra fournir à l'issue de l'installation :

- Le plan d'adressage IP,
- Les protocoles mis en œuvre,
- Les ports origine et destination,
- Les fichiers TXT de chaque commutateur sous format électronique (\*.Txt),
- Les remarques éventuelles.

Le LAN sûreté sera constitué d'autant de réseaux virtuels (V-LANs) qu'il y aura de types de matériels installés. Les commutateurs Ethernet seront configurés par les techniciens du ministère en fonction de ces éléments.

Pour le contrôle d'accès / Détection d'intrusion, les V-LANs suivants seront créés :

- pour l'administration de contrôle d'accès,
- pour le serveur de contrôle d'accès,
- pour les UTL,
- pour les autres équipements éventuels.
- pour les alarmes

Le commutateur n'assurera en aucun cas le routage inter Vlan. Cette fonction sera exclusivement assurée par un pare-feu de niveau 3 qui aura la double fonction de filtrage et de routage des Vlan.

**1.3.1 En cas de présence de parefeux**

La fonction de routage inter Vlan sera exclusivement assurée par un pare-feu de niveau 3 qui aura la double fonction de filtrage et de routage des Vlan.

Les pare-feux du réseau Ethernet Sûreté devront être conformes aux préconisations du Ministère de l'Intérieur.

Les pare-feux des séries FORTINET Fortigate 60D/100D/200D/300D sont conformes et déployés actuellement par le Ministère de l'Intérieur.

**Le pare-feu sera fourni par l'administration, et configuré et installé en collaboration entre les techniciens du ministère de l'intérieur et ceux du soumissionnaire.**

Le soumissionnaire fournira les informations nécessaires à l'établissement d'une matrice de flux. Cette base servira à l'administration qui se chargera de la configuration des pare-feux.

Ces informations comprendront notamment :

- Les adresses IP source et destination,
- Les flux source et destination,
- Les 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.

Le soumissionnaire présentera ces renseignements dans le tableau joint en annexe dont l'administration lui communiquera une version électronique.

Compte tenu du délai de deux mois nécessaire à l'administration au traitement de ces informations pour leur mise en forme, et à l'intégration dans une base de données nationale, la mise en réseau de la solution de sûreté bâtiminaire, objet du présent CCTP, ne pourra pas intervenir avant l'issue de ces deux mois. Le soumissionnaire tiendra compte de ce délai et l'intégrera dans le calendrier de déploiement de la solution qu'il proposera.

Le réseau de sûreté devra être indépendant du réseau existant du site.

### **1.3.2. Principe retenu**

Le projet prévoit :

- la fourniture, installation, raccordement, mise en service d'un contrôle d'accès (câblage courants forts et faibles, éléments matériels actifs, passifs et logiciels).
- la dépose, stockage et/ou enlèvement du matériel obsolète,
- la fourniture de la documentation détaillée,
- la formation des personnels chargés de la gestion et l'exploitation du système mis en œuvre,
- la garantie sur le matériel et les logiciels comprenant la maintenance préventive, corrective, évolutive et adaptative du contrôle d'accès (architecture technique, logiciels) livrés.

La prestation devra respecter les mesures de sécurité (cf. § 6) et la réglementation en vigueur (cf. § 12 – Annexe 3).

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 « dwg ou pdf » seront remis au titulaire du marché pour mise à jour et confection du DOE à fournir dans le cadre de la recette (cf. § 10). La version logicielle sera à définir pour une lecture aisée des documents.

La prestation de serrurerie est intégrée dans ce CCTP. Son intégration dans le système de gestion du contrôle d'accès fait partie du présent CCTP.

Le soumissionnaire devra fournir, dans le dossier technique présenté dans son offre, toute certification ou agrément délivré par les constructeurs des matériels ou logiciels constituant son offre technique.

### **1.3.3. prestation attendue**

Celle-ci a pour but de protéger :

- Certains ouvrants,
- Les lieux de travail,
- Certains locaux sensibles, comme les bureaux du corps préfectoral, le centre opérationnel de défense et les locaux informatiques.

**À noter :** Les trois systèmes, existant ou à créer, à savoir la vidéosurveillance, l'anti-intrusion et le contrôle d'accès seront asservis les uns aux autres par un superviseur.

L'ensemble forme une solution de sûreté bâtiminaire globale, cohérente et pertinente dont la fourniture et l'intégration du métier de contrôle d'accès sont l'objet de ce CCTP (Phase 2).

Elle consiste à déployer :

- un réseau local, indépendant du réseau bureautique, dénommé « réseau sûreté (en DMZ) »
- le serveur principal, hébergeant en machines virtuelles les logiciels du contrôle d'accès, l'hyperviseur, et enfin les rôles serveurs associés à la cybersécurité tels que le service Radius (AD,LDAP,NPS),
- un serveur de secours du type PCA, hébergeant en machines virtuelles de façon identique les logiciels énumérés au point précédent y compris ceux associés à la cybersécurité,
- les stations de gestion du contrôle d'accès.

## **L'objet du présent CCTP concerne :**

### a) pour le contrôle d'accès :

Pour l'offre de base, il conviendra de fournir et installer, autant que de besoin tel que défini par la maîtrise d'ouvrage, lecteurs de badges afin de protéger et contrôler les 40 portes indiquées par l'administration en point 3.2.3, colonne « Offre », sous-colonne « 1 ». **(Le soumissionnaire devra reprendre certains équipements déjà installés comme les gâches électro-mécaniques, ventouses, et lecteurs de badges du fabricant Stid s'ils correspondent bien aux exigences de ce CCTP et sont compatibles avec la solution technologique portée par le soumissionnaire).**

Pour la première option, il conviendra de fournir et installer, autant que de besoin tel que défini par la maîtrise d'ouvrage, les lecteurs de badges afin de protéger et contrôler les 6 portes indiquées par l'administration en point 3.2.3, colonne « Offre », sous-colonne « 2 ».

Pour la seconde option, il conviendra de fournir et installer, autant que de besoin tel que défini par la maîtrise d'ouvrage, les lecteurs de badges afin de protéger et contrôler les 11 portes indiquées par l'administration en point 3.2.3, colonne « Offre », sous-colonne « 3 ».

L'ensemble des portes seront contrôlées par lecteur de badge en entrée et en sortie (éventuellement).  
La fourniture et l'installation, des unités de traitement de porte et des unités de traitement local à définir par le soumissionnaire.

La base de données du système de contrôle d'accès sera native SQL serveur sans Licence complémentaire.  
Les modules de portes (UTP) pourront être déportés et installés dans les locaux techniques proches des portes à défendre.

La solution de contrôle d'accès déployée doit permettre la mise en place de bus terrain sécurisé certifié ANSSI.  
Les UTLs seront installées à l'intérieur de la baie informatique de la solution de sûreté si possible. Mais impérativement dans des locaux techniques sécurisés.

La solution devra pouvoir gérer la technologie DESFIRE EV1/EV2/EV3 compatible carte agent architecturée autour de la puce JCOP version 4.5 et précédentes de la nouvelle carte agent et compatible avec l'ancienne puce OBHERTUR de l'ancienne carte.

### b) pour le réseau, câblage et baie :

Il sera évoqué lors des visites obligatoires, la possibilité de reprendre partiellement le câblage RS485.  
À première vue, cela ne semble pas réalisable puisque les UTLs seront géolocalisées dans des locaux sécurisés différents.

Tous les câblages, fibre optique ou Ethernet, en extérieur (façade) comme en intérieur dans les passages accessibles au public, seront protégés par des goulottes métalliques type oméga, ou gaine type Capriplast®.

### c) pour les serveurs

Le titulaire fournira l'ensemble des licences nécessaires au bon fonctionnement de la solution du contrôle d'accès.  
Les serveurs principal et redondant sont déjà opérationnels, dans le cadre de la rénovation du système de vidéosurveillance entreprise récemment en phase 1.

**Les serveurs de contrôle d'accès, principal et redondant, seront installés en machines virtuelles hébergées sur les deux machines citées ci-dessus.**

### d) Cybersécurité ( ANSSI et CCN ) :

Un service d'authentification RADIUS, local selon les directives de l'administration, est déjà présent sur le site, avec le protocole 802,1 X (avec certification EAP-TLS) sur le réseau de sûreté bâtimentaire afin garantir la sécurité des ports des commutateurs réseaux et autres équipements raccordés sur ce réseau.

Les ports non utilisés des commutateurs réseaux et autres équipements raccordés seront neutralisés logiquement par programmation et physiquement par des bouchons, même dans les baies de sûreté bâtimentaire.

Le serveur d'authentification Radius est implémenté en machine virtuelle sur le serveur physique principal de la solution de sûreté, et sur le serveur physique de secours (redondant).



L'architecture de protection en cybersécurité sera constituée en plus des briques déjà existantes d'une Brique de sécurité pour le Contrôle d'Accès :

- Chaîne de sécurité sans faille du badge jusqu'au serveur de gestion de la solution de CA.
- L'ensemble des matériels (UTL, modules d'extension, lecteurs,..) et logiciels proposés devront être conformes aux recommandations du guide de l'ANSSI : « SÉCURITÉ DES TECHNOLOGIES SANS CONTACT POUR LE CONTRÔLE DES ACCÈS PHYSIQUES » (Version du 04/03/2020) selon l'architecture 1 de façon native sans convertisseur.
- La solution devra être sécurisée de bout en bout, du badge jusqu'au serveur.

Les principes et fonctionnalités suivants devront être disponibles et réalisés par les équipements et logiciels fournis :

- Conforme ANSSI architecture 1,
- La solution devra être compatible avec le réseau VLAN, VPN du site,
- La solution devra être compatible avec l'annuaire LDAP du site pour la gestion des opérateurs et de leurs droits,  
Communications réseau IP cryptées TLS AES 256 bits et signées (intégrité et authentification) entre le serveur et les UTL d'une part et les postes clients d'autre part,
- Communications bus RS485 cryptées AES 128 bits et signées,
- Toutes les clés de communications sur IP et RS485 devront être changées périodiquement de manière automatique par le système sans action humaine pour durcir le cryptage contre toute malveillance,
- Le client final aura obligatoirement la maîtrise de sa clé de communication initiale, qui créera automatiquement les clés suivantes périodiquement, par la saisie, sur un poste client lourd, de cette clé (cérémonie des clés),
- Protection des attaques par déni de service (DoS) par le Firewall des automates UTL,
- Paramétrage de la configuration IP des UTL à travers un Web serveur embarqué sécurisé HTTPS, SSH,
- UTL compatible avec serveur radius 802.1X
- Le module de porte communiquera en bus RS485 crypté AES128 bits avec les lecteurs
- Le protocole SSCP V2 sera activé pour le chiffrement des flux de données entre les lecteurs de badge contrôlant les portes, et les unités de traitement de porte de la solution de contrôle d'accès

Le protocole FTP (File Transfert Protocol) sera désactivé et les guides de durcissement des constructeurs des équipements déployés seront appliqués.

**Le réseau déployé sera conforme au Cahier des Clauses Techniques Simplifiés de Cybersécurité pour les marchés publics (arrêté du 18/09/2018), au Règlement Général de Sécurité de l'ANSSI.**

## 2. DESCRIPTION DE L'EXISTANT

### 2.1. Architecture existante

LOCAUX TECHNIQUES PRÉVUS DANS CE PROJET				
Bâtiment	Nom du LT	Étage	Répartiteur	Descriptif
Principal AUTOCOM	LT AUTOCOM	R+2	Répartiteur général	RG (arrivées fibres opérateurs) Emplacement du serveur principal Point de raccordement du CA, des caméras et visiophones
Aile Est ACROPOL	LT AILE EST	RDC	Sous-répartiteur	Emplacement de la redondance du serveur VMS Point de raccordement du CA, des caméras et visiophones dans l'aile est
Principal SIDPC	LT SIDPC	R+2	Sous-répartiteur	Point de raccordement du CA situé dans l'aile centrale de la Préfecture Sous-sol, RDC et R+1
Résidence du SG	LT SG	RDC	Sous-répartiteur	Point de raccordement du CA, des caméras et visiophones situés au fond du parc
Aile Ouest Entrée Standard	LT AILE OUEST	RDC	Sous-répartiteur	Point de raccordement du CA, des caméras et visiophones situés au standard de la Préfecture et aile ouest RDC et R+1
Aile Ouest SIDSIC	LT SIDSIC	RDC	Sous-répartiteur	Point de raccordement du CA situé dans l'aile centrale de la Préfecture Sous-sol, RDC et R+1
Aile Neuve	LT AILE NEUVE	R+1	Sous-répartiteur	Point de raccordement du CA situés dans l'aile neuve de la Préfecture au sous-sol , RDC et R+1

CÂBLAGE CAPILLAIRE	
Nombre de prises non conformes	Indéfini
Catégorie de câblage	Catégorie 6a (actuellement)
Année de mise à niveau	Indéfini
RÉSEAUX SÛRETÉ	
Toutes les données liées à la sûreté, de chaque entité, sont véhiculées par un réseau local dénommé « réseau sûreté », inter-sites si besoin et physiquement séparé des réseaux bureautiques existants.	

### 2.2. Systèmes installés

CONTRÔLE D'ACCÈS				
Solution déployée		Structure		
		Bâtiment	Étage	Éléments
Préfecture d'Agen Lot et Garonne	Logiciel : e-Axes obsolète	Préfecture d'Agen	Tous les niveaux	Serveur CA (obsolète)
				Lecteurs ARC du fabricant STid Lecteurs LXS du fabricant STid

### 2.3. Énergie

Les locaux techniques sont alimentés par le réseau général ondulé 220 V, et groupe électrogène. Les baies hébergeant les serveurs « sûreté » sont équipées d'un onduleur autonome.

### 3. DESCRIPTION DES PRESTATIONS A RÉALISER

#### 3.1. Infrastructure réseau

Elle sera réalisée conformément aux caractéristiques et aux principes décrits dans l'annexe du présent CCTP dénommée :

#### **ANNEXE 1 : PRINCIPES CONCERNANT LES ÉQUIPEMENTS DE L'INSTALLATION ET LEUR RACCORDEMENT**

*Toutes les liaisons entre les éléments du réseau sûreté (lecteurs de badges, UTL, commutateurs, serveurs, stations, caméras) seront filaires. Aucun lien sans-fil ne sera admis, sauf spécification explicite contraire présente dans ce CCTP.*

##### **3.1.1. Les répartiteurs**

Comme indiqué dans le paragraphe 2.3, le réseau secouru y est distribué.

##### **3.1.2. Le local serveur**

Un serveur hôte hébergera en machines virtuelles les rôles de la solution de sûreté suivants :

- Gestion de la vidéosurveillance (existant),
- Gestion du contrôle d'accès,
- Le superviseur gérant l'ensemble des métiers précédents,
- Les services associés aux rôles de la cybersécurité dont le Radius.

Un serveur de secours est présent dans la solution de sûreté. Il héberge de façon identique en machines virtuelles les mêmes types de logiciels.

Il est équipé d'une source d'énergie secteur, un onduleur est déjà présent.

##### **3.1.3. Les baies**

Elles ne sont pas à fournir dans la présente prestation.

##### **3.1.4. La dorsale optique**

Le cas échéant

##### **3.1.5. Le capillaire cuivre**

Le cas échéant

Il fait partie des prestations répondant aux prescriptions de l'annexe du présent CCTP dénommée :

#### **ANNEXE 1 : PRINCIPES CONCERNANT LES ÉQUIPEMENTS DE L'INSTALLATION ET LEUR RACCORDEMENT**

*Tous les périphériques de type « Ethernet/IP » (Utlis) proposés dans la solution seront raccordés sur le répartiteur désigné par l'administration (dans la plupart des cas, le plus proche) par un lien « Ethernet » catégorie 6A / classe EA ou catégorie 7 respectant les règles de l'art.*

***L'établissement de ces liens fait partie*** des prestations répondant aux prescriptions de l'annexe 1 du présent CCTP précédemment citée.

##### **3.1.6. Les éléments actifs**

**Leur fourniture est exclue de la présente prestation.**

Le Ministère de l'Intérieur a dimensionné en première approche le nombre de commutateurs réseau à mettre en œuvre et les fournira, ainsi que le pare-feu nécessaire à l'établissement des liens sécurisés inter-sites.

Il fournira tous les éléments permettant la segmentation du réseau (Numéros de VLAN, adresses IP des LAN, masques de sous-réseaux, etc.) via son Bureau des Réseaux Fixes de la DSIC du SGAMI.

**Pour information :**

Le soumissionnaire dimensionnera définitivement l'architecture du réseau de sûreté à mettre en place en se conformant au besoin décrit dans le CCTP et aux principes décrits dans l'annexe 1.

### **3.1.7. Implantation type des éléments dans les baies de sûreté**

Ces implantations sont à respecter et à adapter en fonction du nombre de commutateurs et de liens cuivre RJ45 à câbler (exemple donné pour une installation de 24 liens sûreté RJ45 maximum dans des baies de hauteur 42U).

### **3.1.8. Baie du répartiteur et sous-répartiteurs**

Exemple :

HAUT		
	U	ÉLÉMENT
2U	42	Panneau télécom (opérateur)
	41	Passe cordons télécom
	40	Panneau sûreté 24 noyaux RJ45
	39	Passe cordons
	38	Commutateur sûreté 24 ports POE
	37	Passe cordons
2U	36	Pare-feu sûreté
	35	
		Vide
		Vide
		Vide
		Vide
		Vide
2U	18	KVM
	17	
	15	Vide
	14	Vide
	13	Vide
	12	Vide
	11	Vide
	10	Vide
	9	Vide
	8	Serveur solution vidéo et contrôle d'accès
	7	
	6	Vide
	5	
	4	Onduleur sûreté
	3	
	2	Bandeau arrière 6 PC 220v+T sur onduleur
	1	Bandeau arrière 6 PC 220v+T
BAS		

### **3.2. contrôle d'accès**

#### **ATTENTION !**

Il sera réalisé conformément aux principes décrits dans l'annexe à ce CCTP dénommé :

#### **ANNEXE 2 : PRINCIPES CONCERNANT LE SYSTÈME DE CONTRÔLE D'ACCÈS**

##### **3.2.1. Les accès**

Afin de mettre en correspondance les accès, les serrures et leur organe de contrôle (lecteur de badge et visiophone), ces éléments sont listés dans le tableau commun suivant :

##### **3.2.2. Les unités de traitement local (UTL)**

Le nombre d'unités de traitement local sera déterminé proportionnellement au nombre d'ouvrants à contrôler en respectant les règles de l'art émises par le constructeur (explication à fournir dans le CRT onglet CONTRÔLE D'ACCÈS).

Elles seront installées dans les locaux techniques désignés par l'administration pour bénéficier entre-autres de l'énergie secourue.

Afin de pouvoir en déterminer leur nombre, le soumissionnaire se reportera aux plans du bâtiment et sur les propositions de rattachement listées ci-dessous. A défaut, le soumissionnaire proposera une solution alternative qui devra être validée.

Un point d'accès « Ethernet » catégorie 6A / classe EA ou supérieur sera créé entre la ou les UTL présente(s) dans le local et la baie hébergeant le commutateur « sûreté ».

##### **3.2.3. Les lecteurs de badges (LB)**

Le présent lot doit la fourniture, la pose, le raccordement et l'intégration au système de contrôle d'accès des lecteurs de badges.

Précision sur les lecteurs de badges X : Le soumissionnaire devra préciser l'emplacement et le nombre de lecteurs de badge à fournir dans le tableau qui suit.

#### **Les lecteurs de badges liés au contrôle d'accès sont listés ci-après :**

**LBI** : Lecteur de badges intérieur

**LBE** : Lecteur de badges extérieur

**BM** : Boucle magnétique

**EC** : Entrée contrôlée

**SC** : Sortie contrôlée

Ouvrant	Flux	Réf. Lecteur de Badges	Quantités et type lecteur		Répart.	Offre		
			LBE	LBI		1	2	3
P01-AN-RDC-SCLER	EC	LB01		1	LT AILE NEUVE	X		
P03-AN-RDC-ESCALIER	EC	LB03		1	LT AILE NEUVE	X		
P05-AN-RDC-ACCUEIL	EC	LB05		1	LT AILE NEUVE			X
P06-AN-SS-DESCENTE-COURRIER	EC	LB06	1		LT AILE NEUVE	X		
P07-AN-SS-COUR-GARAGE	EC	LB07		1	LT AILE NEUVE	X		
P08-AN-SS-BADGEUSE	EC	LB08		1	LT AILE NEUVE	X		
P09-AN-SS-COULOIR	EC	LB09		1	LT AILE NEUVE	X		
P10-AN-SS-GARAGE	EC/SC	LB10		2	LT AILE NEUVE	X		
P11-AN-SS-ARCHIVES	EC	LB11		1	LT AILE NEUVE	X		
P12-AN-01-LTSIDSIC	EC	LB12		1	LT AILE NEUVE	X		

Ouvrant	Flux	Réf. Lecteur de Badges	Quantités et type lecteur		Répart.	Offre		
			LBE	LBI		1	2	3
P13-AN-01-GUICHET-BNE	EC	LB13		1	LT AILE NEUVE			X
P14-AO-RDC-ENTREE-DOLET	EC	LB14	1		LT AILE OUEST	X		
P15-AO-RDC-STANDARD	EC	LB15	1		LT AILE OUEST	X		
P16-AO-RDC-SRH	EC	LB16	1		LT AILE OUEST	X		
P17-AO-RDC-SRH-ESCALIER	EC	LB17		1	LT AILE OUEST	X		
P18-AO-RDC-SRH-HALL	EC	LB18		1	LT AILE OUEST	X		
P19-AO-RDC-ESCALIER-HONNEUR	EC	LB19	1		LT AILE OUEST	X		
P21-AO-RDC-HALL-PARKING	EC/SC	LB21	1	1	LT AILE OUEST	X		
P22-AO-RDC-FALLIERES-HALL	EC	LB22		1	LT AILE OUEST	X		
P23-AO-RDC-FALLIERES-PARC	EC	LB23		1	LT SIDSIC	X		
P25-BC-PORTE-PARC	EC/SC	LB25	1	1	LT SIDSIC	X		
P26-BC-ENTREE-COURCG	EC	LB26	1		LT SIDSIC	X		
P27-BC-RDC-PETITE-SAM	EC	LB27		1	LT AILE EST			X
P28-BC-RDC-GD-ESCALIER	EC	LB28	1		LT AILE EST			X
P29-BC-RDC-LTSIDSIC	EC	LB29		1	LT SIDSIC		X	
P31-BC-RDC-SIDSIC	EC	LB31		1	LT SIDSIC	X		
P32-AE-RDC-RESTAURATION	EC	LB32	1		LT AILE OUEST		X	
P34-BC-RDC-CHEF-SCIRE	EC	LB34		1	LT SIDSIC	X		
P35-BC-RDC-SCIRE	EC	LB35		1	LT SIDSIC	X		
P36-BC-RDC-SAM	EC	LB36		1	LT AILE EST		X	
P39-AE-RDC-AILE-EST	EC	LB39	1		LT AILE EST	X		
P40-AE-RDC-SGCD	EC	LB40	1		LT AILE EST	X		
P41-AE-RDC-SGCD-COUR	EC	LB41	1		LT AILE EST	X		
P43-AE-RDC-LT-AILE-EST	EC	LB43	1		LT AILE EST	X		
P44-BC-SS-BUANDERIE	EC	LB44	1		LT AILE EST	X		
P45-BC-SS-BUANDERIE-PARC	EC	LB45	1		LT AILE EST	X		
P46-AO-SS-IMPRIMERIE	EC	LB46		1	LT AILE OUEST			X
P47-BC-SS-LEROY	EC	LB47		1	LT SIDSIC			X
P48-AO-SS-SORTIE-PARC	EC	LB48		2	LT SIDSIC		X	
P49-BC-SS-CUISINE	EC	LB49		1	LT AILE EST		X	
P50-AN-01-HAUSMANN	EC/SC	LB50		2	LT AILE NEUVE	X		
P51-BC-01-CORPS-PREFECTORAL	EC	LB51		1	LT AUTOCOM	X		
P52-BC-01-SECGEN	EC	LB52		1	LT AUTOCOM	X		
P53-BC-01-SECPFT	EC	LB53		1	LT AUTOCOM	X		
P54-AO-01-CABINET	EC	LB54		1	LT SIDPC	X		
P55-AO-01-CABINET	EC	LB55		1	LT SIDPC	X		

Ouvrant	Flux	Réf. Lecteur de Badges	Quantités et type lecteur		Répart.	Offre		
			LBE	LBI		1	2	3
P56-AO-02-LTSIDC	EC	LB56		1	LT SIDPC		X	
P57-AO-02-SIDPC	EC	LB57		1	LT SIDPC	X		
P58-BC-02-AUTOCOM	EC	LB58		1	LT AUTOCOM	X		
P59-BC-02-COMBLES	EC	LB59		1	LT AUTOCOM	X		
P60-AO-02-COD	EC	LB60		1	LT SIDPC	X		
P62-AE-SS-COUR	EC	LB62	1		LT AILE EST	X		
P63-AN-SS-COURRIER	EC	LB63		1	LT AILE NEUVE			X
P64-AN-RDC-FALLIERES	EC	LB64		1	LT AILE NEUVE			X
P65-AN-01-ACCES-BNE	EC	LB65		1	LT AILE NEUVE			X
P66-AN-02-CERT	EC	LB66		1	LT AILE NEUVE			X
P67-AN-03-DCPPAT	EC	LB67		1	LT AILE NEUVE			X
ASCENSEUR	EC	LB02		1	LT AILE NEUVE	X		

### **3.2.4. La serrurerie (Seulement SI NÉCESSAIRE)**

**Le présent lot doit le raccordement et l'intégration au système de contrôle d'accès des serrures électriques.**

Le lot menuiserie est intégré dans le présent CCTP.

Le titulaire des lots sûreté devra proposer des solutions adaptées afin que huisseries, serrureries et contrôle d'accès assurent la pleine fonctionnalité de la solution globale de sûreté le cas échéant.

Les gâches sont **déconseillées**.

Toutes les portes sous contrôle d'accès seront équipées de dispositifs de verrouillages électriques (serrures simples ou motorisées, ventouses électromagnétiques 600kg) d'un niveau de sécurité équivalent au niveau de résistance à l'effraction de la porte concernée. Ces dispositifs doivent empêcher toute entrée illicite, y compris en cas de déclenchement du SSI, les sorties pouvant se faire librement dans tous les cas (hors zone de sûreté).

Si elles sont requises, seules les serrures électriques présentant les caractéristiques énoncées dans l'**ANNEXE 2** :

**PRINCIPES CONCERNANT LE SYSTÈME DE CONTRÔLE D'ACCÈS** sont admises.

#### **En cas d'installation de nouvelles serrures :**

Elles seront du type serrures électromécaniques.

Chaque serrure est commandable individuellement par les lecteurs de badges de ces accès.

Ces serrures seront munies d'une batterie de secours.

La porte sera munie d'une serrure de secours mécanique avec protège cylindre de norme A2P\* minimum, dont l'ébauche de clé est protégée.

Nota : Le service conviendra par avance avec le responsable des travaux, des conditions d'installation des serrures de secours définitives et de remise des clés correspondantes pour les portes du service. Celles-ci, ainsi que la carte propriétaire, devront être remises sous pli scellé opaque au chef du service des moyens logistiques (SMLA) ou son représentant. Les serrures de secours définitives ne devront en aucun cas être installées lors de la phase de travaux et aucune clé ne devra être en circulation.

#### **Les serrures électriques sont listées ci-après (si elles sont requises) :**

**EC** : Entrée contrôlée

**SC** : Sortie contrôlée

**Mode** : Voir ANNEXE 2 : PRINCIPES CONCERNANT LE SYSTÈME DE CONTRÔLE D'ACCÈS

**Le soumissionnaire devra préciser l'emplacement et le nombre de serrures à fournir dans un document qu'il remettra dans son offre.**

Ouvrant	Flux	Type de porte	Type de fermeture	Offre de base	Option
P01-AN-RDC-SCLER	EC	Porte changée	Electromécanique	X	
P03-AN-RDC-ESCALIER	EC	Porte changée	Electromécanique	X	
P05-AN-RDC-ACCUEIL	EC	Porte changée	Electromécanique		PSO1
P06-AN-SS-DESCENTE-COURRIER	EC	Porte blindée	Electromécanique	X	
P07-AN-SS-COUR-GARAGE	EC	Porte changée	Electromécanique	X	
P08-AN-SS-BADGEUSE	EC	Porte changée	Electromécanique	X	
P09-AN-SS-COULOIR	EC	Porte changée	Electromécanique	X	
P10-AN-SS-GARAGE	EC/SC	Porte changée	Electromécanique	X	
P11-AN-SS-ARCHIVES	EC	Porte changée	Electromécanique	X	
P12-AN-01-LTSIDSIC	EC	Porte changée	A créer	X	
P13-AN-01-GUICHET-BNE	EC	Porte changée	Electromécanique	X	
P14-AO-RDC-ENTREE-DOLET	EC	Porte ancienne	Ventouse	X	
P15-AO-RDC-STANDARD	EC	Porte changée	Electromécanique	X	
P16-AO-RDC-SRH	EC	Porte changée	Electromécanique	X	
P17-AO-RDC-SRH-ESCALIER	EC	Porte changée	Electromécanique	X	
P18-AO-RDC-SRH-HALL	EC	Porte ancienne	Electromécanique	X	
P19-AO-RDC-ESCALIER-HONNEUR	EC	Porte ancienne	Electromécanique	X	
P21-AO-RDC-HALL-PARKING	EC/SC	Porte changée	Electromécanique	X	
P22-AO-RDC-FALLIERES-HALL	EC	Porte ancienne	Ventouse	X	
P23-AO-RDC-FALLIERES-PARC	EC	Porte ancienne	Ventouse	X	
P25-BC-PORTE-PARC	EC/SC	Porte changée	Electromécanique	X	
P26-BC-ENTREE-COURCG	EC	Porte changée	Electromécanique	X	
P27-BC-RDC-PETITE-SAM	EC	Porte changée	A créer		PSO1
P28-BC-RDC-GD-ESCALIER	EC	Porte ancienne	Electromécanique		PSO1
P29-BC-RDC-LTSIDSIC	EC	Porte ancienne	A créer	X	
P31-BC-RDC-SIDSIC	EC	Porte ancienne	A créer	X	
P32-AE-RDC-RESTAURATION	EC	Porte changée	A créer	X	
P34-BC-RDC-CHEF-SCIRE	EC	Porte ancienne	A créer	X	
P35-BC-RDC-SCIRE	EC	Porte ancienne	A créer	X	
P36-BC-RDC-SAM	EC	Porte ancienne	A créer	X	
P39-AE-RDC-AILE-EST	EC	Porte ancienne	Electromécanique	X	
P40-AE-RDC-SGCD	EC	Porte ancienne	Electromécanique	X	
P41-AE-RDC-SGCD-COUR	EC	Porte changée	A créer	X	
P43-AE-RDC-LT-AILE-EST	EC	Porte ancienne	A créer	X	
P44-BC-SS-BUANDERIE	EC	Porte ancienne	Electromécanique	X	
P45-BC-SS-BUANDERIE-PARC	EC	Porte changée	Electromécanique	X	



Ouvrant	Flux	Type de porte	Type de fermeture	Offre de base	Option
P46-AO-SS-IMPRIMERIE	EC	Porte blindée	A créer		PSO1
P47-BC-SS-LEROY	EC	Porte ancienne	A créer		PSO1
P48-AO-SS-SORTIE-PARC	EC	Porte changée	A créer	X	
P49-BC-SS-CUISINE	EC	Porte à créer	A créer	X	
P50-AN-01-HAUSMANN	EC/SC	Porte changée	Electromécanique	X	
P51-BC-01-CORPS-PREFECTORAL	EC	Porte changée	Electromécanique	X	
P52-BC-01-SECGEN	EC	Porte changée	Electromécanique	X	
P53-BC-01-SECPFT	EC	Porte changée	Electromécanique	X	
P54-AO-01-CABINET	EC	Porte ancienne	Ventouse	X	
P55-AO-01-CABINET	EC	Porte changée	Electromécanique	X	
P56-AO-02-LTSIDSIC	EC	Porte changée	A créer	X	
P57-AO-02-SIDPC	EC	Porte blindée	Electromécanique	X	
P58-BC-02-AUTOCOM	EC	Porte changée	A créer	X	
P59-BC-02-COMBLES	EC	Porte ancienne	A créer	X	
P60-AO-02-COD	EC	Porte changée	Electromécanique	X	
P62-AE-SS-COUR	EC	Porte ancienne	Electromécanique	X	
P63-AN-SS-COURRIER	EC	Porte changée	A créer		PSO1
P64-AN-RDC-FALLIERES	EC	Porte ancienne	A créer		PSO1
P65-AN-01-ACCES-BNE	EC	Porte changée	A créer		PSO1
P66-AN-02-CERT	EC	Porte changée	A créer		PSO1
P67-AN-03-DCPPAT	EC	Porte changée	A créer		PSO1
ASCENSEUR	EC	Ascenseur	Machinerie ascenseur	X	

### **3.3. Maquette**

**Le but est de réaliser une maquette chez le constructeur de la solution proposée par le titulaire, et de vérifier sa conformité au présent CCTP. Cette maquette est exigée.**

### **3.4. Les ordinateurs de gestion**

Les caractéristiques techniques concernant les ordinateurs liés au contrôle d'accès sont définies dans l'annexe 2 pour les serveurs, enregistreur, stations, écrans simples ou de grande diagonale.

Le soumissionnaire devra préciser l'emplacement et le nombre d'ordinateurs à fournir dans un document qu'il remettra dans son offre.

#### **3.4.1. Les serveurs**

Les machines sont des serveurs DELL R550 4VM 26TB.

Le design exact de celles-ci sera fourni lors de la visite de site.

Le titulaire devra fournir la VM sur les serveurs physiques existants. Elle hébergera la solution de gestion du contrôle d'accès, la sécurisation des périphériques (RADIUS authentification 802.1x EAP-TLS), la gestion des utilisateurs et de l'exploitation (contrôleur de domaine & management système) et le superviseur.

#### **3.4.2. Les stations**

Le titulaire devra fournir ou reprendre les stations (Il existe déjà des stations pour le système de vidéosurveillance, elles peuvent être mutualisées avec le CA) voir avec le soumissionnaire.

#### 3.4.2.1. Les postes de gestion des badges et d'administration du contrôle d'accès

En plus des caractéristiques de l'annexe 2, ces 2 postes seront équipés chacun d'un lecteur RFID encodeur/enrôleur de la solution logicielle.

Ils permettront aux utilisateurs ayant les droits :

- d'enrôler les badges (carte Agent ou carte blanche).
- d'administrer le système de contrôle d'accès (affecter les droits).
- La gestion du fil de l'eau des événements.
- L'affichage de la cartographie avec action de verrouillage et déverrouillage des accès.

#### **Fournitures comprises dans la solution de gestion des badges :**

La carte sans contact, de format ISO 7816 avec capacité sans contact ISO 14443, utilisée pour l'identification aux contrôles d'accès est fondée sur la puce Mifare DesFire Ev1/EV2.

**Le titulaire devra la livraison de 150 badges**, PVC blanc, format ISO 7816 avec capacité sans contact ISO 14443, badge vierge, libre de droit, tel que sorti d'usine, sans modification de clés (clé maître notamment) ni de droits.

#### 3.4.2.2. Le poste de visualisation

En plus des caractéristiques de l'annexe 2, ce poste de travail sera équipé de 2 écrans plats LED avec bras ou support de fixation murale.

Il permettra :

- L'affichage de la cartographie avec action de verrouillage et déverrouillage des accès.
- La gestion du fil de l'eau des événements.

### **3.5 Courant faible, courant fort, Étiquetage**

#### **3.5.1. Courant faible**

Pour information :

Tous les périphériques de type « Ethernet/IP » (serveurs, stations, UTL, etc.) proposés dans la solution seront raccordés sur le répartiteur désigné par l'administration (et dans la plupart des cas, le plus proche) par un lien « Ethernet » catégorie 7 en respectant les règles de l'art.

#### **3.5.2. Courant fort**

Tous les organes de sûreté seront raccordés sur le réseau ondulé existant, désigné par l'administration, ou à la charge du titulaire en respectant les règles.

#### **Alimentation en énergie électrique ondulée et secourue :**

Le soumissionnaire utilisera les onduleurs installés dans chacune des baies lors de la phase 1 (déploiement de la vidéosurveillance).

#### **Voici les caractéristiques du ou des onduleurs :**

- format 19 pouces rackable
- raccordé à l'installation par un circuit 220 V-16 A 2P+T protégé par un disjoncteur différentiel 30mA hautement immunisé (type HI)
- branchement effectué sur la distribution électrique secourue désignée par l'administration
- bandeau électrique 6 prises 2P+T, au format 19 pouces, à fournir, intégrer dans la baie et raccorder sur sa sortie.
- l'onduleur devra maintenir l'alimentation électrique pour une durée minimale de 30 mn.

#### **3.5.3. Étiquetage**

Tous les matériels installés au titre du présent marché devront être identifiables au moyen d'une étiquette accessible et visible.

#### **3.5.4. Acteur**

Toutes ces prestations sont à la charge du titulaire.

#### **4. INTERFONCTIONNEMENT DES SYSTÈMES**

L'objectif de la solution est de superviser le système en proposant sur une interface unifiée, la vidéosurveillance existante, le contrôle d'accès et l'anti intrusion.

Cette solution sera constituée d'un superviseur qui permettra la gestion conjointe du contrôle d'accès, de la vidéosurveillance et de l'anti intrusion.

Tous les événements (identifiant, alarmes, sorties, entrées, états) liés à un point d'accès ou un point d'intrusion sont horodatés et enregistrés.

Le serveur de temps (NTP) sera la référence d'horodatage de l'ensemble de la solution, fourni par l'administration (pare-feu).

## 5. EXPLOITATION DE LA SOLUTION

### 5.1. Gestion du Système

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** » permet 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** » permet à un opérateur, sous-réserve de ses droits, d'administrer et gérer les profils, de produire des badges, etc.
- L'accès « **Opérateur** » permet 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.
- L'accès « **Opérateur d'extraction** » permet à un exploitant, sous-réserve de ses droits, de consulter les images, faire des recherches de séquences, extraire des images, etc. (pour le format)

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

### 5.2. Exploitation par l'administrateur du système

Le système doit permettre de définir des profils 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 à 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.

#### 5.2.1. 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 doit permettre la visualisation de son état mais inhibe les droits d'actions Ouverture/Fermeture.
- 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 contrôle et de sécurité » doit pouvoir :

- 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,

**Un opérateur « gestionnaire des badges » doit pouvoir :**

- 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.

**Un opérateur « extraction d'images » doit pouvoir :**

- Configurer son espace de travail ;
- Disposer d'un droit en écriture sur les ports USB de son espace de travail,
- Disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité,

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 doit permettre une gestion sécurisée des mots de passe des utilisateurs.

Le système de gestion des droits doit permettre 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).

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

### **5.2.2. Gestion des journaux**

La solution doit permettre 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) , Évènement 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).**

## **5.3. Exploitation par le gestionnaire des badges**

### **5.3.1. Gestion des badges**

#### **5.3.1.1. Personnalisation des badges utilisateurs**

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

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

- Nom
- Prénom
- Matricule
- Grade
- Fonction
- Observation
- Dates

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

La solution doit permettre 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 (webcam 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,
- Date,
- Entier,
- Images ou fichiers graphiques,
- Nombres décimaux,
- Texte.

La solution doit permettre l’association d’un porteur de carte et d’un groupe de porteurs avec plusieurs badges.

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 doit pouvoir permettre la création de fiches similaires. L’objectif est de pouvoir attribuer plusieurs badges à une même personne.

La solution doit permettre 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 doit permettre la gestion des erreurs à l’importation.

**Le serveur de contrôle d’accès doit permettre la gestion simultanée de 200 porteurs de badges au maximum.**

#### 5.3.1.2. Gestion des profils

La solution doit permettre la création de profils à partir de règles d’accès associées à des groupes de points d’accès.

La solution doit permettre l’association de porteurs ou des groupes de porteurs à des règles d’accès et des profils.

La solution doit permettre 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 recalculés automatiquement d’une année sur l’autre.

La solution doit permettre la gestion d’un grand nombre de profils (supérieur à 50).

#### 5.3.1.3. Type de badge (CAM)

### **LE LECTEUR DE BADGE DOIT ÊTRE COMPATIBLE AVEC LA CARTE AGENT DU MINISTÈRE DE L’INTÉRIEUR**

La solution doit permettre 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 à 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.

#### 5.3.1.4. Invalidation des badges

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

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

#### 5.3.1.5. État 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 hh:mn 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 hh:mn 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 hh:mn 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 hh:mn par nom_personne ».

#### 5.3.2. 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.

### 5.4. Exploitation par les opérateurs

#### 5.4.1. Gestion TYPE PC Sécurité (PCS)

##### 5.4.1.1. Aménagement du PCS

Un « poste de supervision » est à fournir ou reprendre pour gérer la sécurité du site.

Ce poste disposera de deux écrans :

- 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 :
- 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.).
- Sur le même écran, **une fenêtre** 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'acquiescement et la visualisation des alarmes, l'enregistrement numérique sur disque dur des événements du site).

#### 5.4.1.2. Gestion des enquêtes

La solution doit permettre la recherche d'événements-alarmes, mémo, signet, métadonnées et de visualiser la vidéo éventuellement associée à l'événement.

#### 5.4.1.3. 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 ces 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 doit permettre de zoomer dans le plan, de se diriger à 360.

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

La cartographie doit permettre :

- d'exécuter des actions de type glisser/déposer de la cartographie vers toute vignette d'affichage pour permettre de visualiser les événements liés à une porte par action de déposer d'une porte vers une fenêtre,
- 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 de la zone concernée.

Lorsqu'un événement se produit dans une zone qui est constituée 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.

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

- En rouge lors du déclenchement d'une alarme, restera en rouge tant que l'alarme ne sera pas acquiescée,
- En orange lors du déclenchement d'une panne.

#### 5.4.1.4. Gestion des alarmes

La solution doit permettre la définition d'une alarme ou d'un événement/alarme à partir de la combinaison d'événements détectés par le système, contact sec, détection d'ouverture, détection d'événements d'identification, d'événements natifs et programmables.

La solution doit permettre de paramétrer la notion d'alarme et d'événement pour pouvoir, sous réserve de ses possibilités, définir une alarme et un événement et éventuellement convertir une alarme en événement (et réciproquement).



Le système doit permettre une hiérarchisation des alarmes par niveau et une hiérarchisation des événements. La solution doit permettre la gestion de 10 niveaux d'alarmes et d'événements. Les niveaux d'alarmes doivent pouvoir être filtrés sur la console opérateur et affichés par des signes distinctifs (couleur, etc.).

Le terme alarme prioritaire utilisé dans ce document est une alarme de niveau 1.

Chaque alarme doit pouvoir être déclarée dans un champ de 1 à 255 caractères.

Le système doit permettre d'afficher une procédure à suivre en « alarme ».

Le système doit permettre de gérer des alarmes notifiées par l'opérateur.

Le système doit permettre une gestion des alarmes en cascades.

#### 5.4.1.5. Gestion du scénario

Le ministère souhaite la mise à disposition d'une interface simple pour créer des scénarii d'actions. Ces scénarios sont déclenchés soit par un ou une association d'événements (alarme/calendaire), soit manuellement par l'opérateur.

L'utilisateur peut pour un scénario nommé :

- Définir des actions sur des portes, passages, équipements,
- Portes et Points d'Accès : Les actions natives pour les équipements portes/points d'accès sont : Ouvrir, Fermer, Inhiber.
- Point Alarme : Les actions natives pour les équipements d'alarmes sont : Armer, Désarmer.

L'utilisateur peut pour un scénario nommé :

- Définir des actions sur des portes, passages.

Exemples de scénarii modifiables :

Scénario 1 : Exploitation « normale de jour »,

Scénario 2 : Exploitation « normale de nuit »,

Scénario 3 : Exploitation « normale de week-end et de jours fériés »,

Scénario 4 : Exploitation en situation normale exceptionnel prévisible (exemple élections, visites de personnalités, etc.),

Scénario 5 : Situation de crise.

Pour chaque scénario il sera possible de programmer les enregistrements à effectuer, les consignes à appliquer en cas d'alarme, etc.

Le passage d'un scénario à l'autre pourra indifféremment se faire automatiquement selon un programme horaire ou une action manuelle par un opérateur autorisé.

#### 5.4.2. Principe de gestion des réactions à événement

Les actions natives sont :

- Acquitter une alarme,
- Afficher un objet du système,
- Automatiser la production d'un rapport,
- Déclencher un scénario identifié par un nom,
- Diffuser un message audio depuis un fichier ou un micro,
- Ouvrir ou fermer la sortie relais d'un contrôleur.

Le système doit permettre d'adresser des actions natives et de définir par configuration avec un outil et/ou par programmation des actions « dédiées ».

Le système doit permettre d'associer une action à partir d'une liste d'actions.

Le système doit permettre de déclencher une action calendaire.

Le système doit permettre de déclencher une action programmée c'est-à-dire que toutes les actions sont activables sous la forme de trigger.

Le système doit permettre de déclencher une action à distance sur un autre sous système dans le cas de raccordement ou d'utilisation multi-sites.

La solution doit permettre à un utilisateur, par une action simple et sous réserve de ses droits, de n'importe quel poste client de :

- Activer / Désactiver un équipement,
- Consulter l'état d'un équipement,
- Créer/Supprimer un équipement,
- Inhiber les alarmes associées à un équipement,
- Ouvrir/Fermer un accès.

Ces actions peuvent être faites directement au niveau cartographique et simplement par l'intermédiaire de menu.

## 6. EXIGENCES SÉCURITAIRES

Les mesures de sécurité complémentaires suivantes sont à prendre en compte.

N°	Domaine	Description de la mesure	Bien(s) support(s) concerné(s)
1	Organisation de la sécurité des SI	Contrat de maintenance 5 j/7 – HO avec intervention sous 24H	UTL, 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, UTL, 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 administrateur MI est obligatoire	Serveur, UTL, 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, UTL, 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 liée au renouvellement	Lan Commutateurs, Serveur, UTL, 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, UTL, 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.	
8	Sécurité physique des locaux	Les équipements seront installés dans des locaux sécurisés par contrôle d'accès	UTL, 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.	Lan Commutateurs, Serveur, UTL, Poste admin, lecteurs
10	Sécurité physique des locaux	Sécuriser l'accès aux locaux sensibles (locaux techniques, ...), par la mise en œuvre d'un second mécanisme de contrôle (ex : digicode ou biométrie).  Avec deux mesures à mettre en œuvre : – une mesure technique pour la gestion des droits administrateurs applicatifs – une mesure pour le processus de validation des droits	Serveur, commutateurs
11	Architecture et exploitation des SI	Redondance des UTL et répartition des lecteurs d'une même zone sur plusieurs contrôleurs.	UTL, 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	Prévoir plusieurs badges administrateurs	Poste admin, Badges admin,
15	Architecture et exploitation des SI  Gestion de la continuité des SI	Sauvegarde quotidienne au minimum des données sensibles (clefs de lecture, profil, logs)	Équipe d'administration Serveur
16	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 antivirus quotidienne des serveurs	Serveurs, postes admin
17	Architecture et exploitation des SI	Mettre en place les correctifs de sécurité et upgrade applicatifs matériels	Serveurs, postes admin, UTL, Commutateurs, Lecteurs
18	Architecture et exploitation des SI	Autonomie des UTL par rapport aux serveurs : Les UTL doivent avoir une copie de la base des droits afin de continuer à fonctionner de manière autonome. Toutes les UTL pourront fonctionner sans perturbation en cas de perte de la liaison avec les équipements en amont.	UTL
19	Architecture et exploitation des SI	Mettre en œuvre un réseau physique dédié aux équipements contribuant à la mise en œuvre des systèmes de sécurisation. À 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, UTL, postes administrateur
20	Architecture et exploitation des SI	La communication entre le badge, la tête de lecture et l'UTL sera chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS27)	Lan Commutateurs, Serveur, UTL, Poste admin,
21	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 UTL.	Administrateur, UTL, lecteurs
22	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
23	Architecture et exploitation des SI	Sécuriser les BDD de type Oracle conformément aux PES	Serveur
24	Architecture et	Procéder au cloisonnement des ressources serveurs dans une DMZ	Serveur

	exploitation des SI	dédiée à cet effet	
25	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, UTL, postes administrateur, commutateurs
26	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 supprimés dès la fin de la prestation (cf procédure circuit arrivée/départ)	Serveur, postes administrateurs
27	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
28	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
29	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 comptes nominatifs prestataires)	Administrateur
30	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
31	Gestion de la continuité des SI	En cas de fonctionnement en mode dégradé (coupure électrique ou interruption des serveurs/UTL): garde statique, ouverture des accès stratégiques par clefs	Lecteurs, Lan Commutateurs, Serveur UTL, Système de verrouillage
32	Gestion de la continuité des SI	Assurer la continuité de la fonction administration du SI : gestion des congés, astreintes, ....	Équipes admin
33	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
34	Gestion de la continuité des SI	S'assurer de la disponibilité des matériels listés dans les fiches réflexes : (plate-forme de secours, ...),	Serveur
35	Gestion de la continuité des SI	Prévoir un stock de maintenance pour les commutateurs	Lan Commutateurs
36	Conformité et contrôle	Respect du « document de référence technique puce sans contact » rédigé par le SHFD	Lecteurs, Badges admin, Serveur, UTL, badges utilisateurs

## 7. DÉMONTAGE

### **7.1. 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. Si nécessaire des retouches de peinture devront être effectuées.

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.

L'administration se réserve le droit de conserver tout ou partie du matériel démonté.

Cette prestation sera définie avec le prestataire lors de la visite de site.

### **7.2. 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 responsable du service immobilier du site. Ce local permettra d'entreposer le matériel en attente d'installation ainsi que tout élément démonté.

### **7.3. Recyclage**

**Option 1 :** Recyclage par l'administration

Tout le matériel démonté sera stocké dans un local indiqué par l'administration qui se chargera de le recycler.

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 SSL.

## **8. DOCUMENTATION**

### **8.1. 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 (version électronique et papier),
- Le Dossier des Ouvrages Exécutés (D.O.E.) en trois exemplaires papier et version électronique comprenant :
  - L'emplacement de tous les équipements installés ( UTL, lecteurs et 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 et en format papier sous forme de classeur.

### **8.2. 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 applications,
- 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.

La documentation sera en version française.

### **8.3. 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.

## 9. FORMATIONS

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 lisible 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).

### **9.1. 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 scenarii,
- 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 4 personnes minimum.

### **9.2. 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 4 personnes minimum.

### **9.3. 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
- 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 du contrôle d'accès
- La gestion de badges « visiteurs »,
- La gestion des événements et alarmes,
- Et tout autre item proposé par le titulaire.

La formation sera assurée pour 4 personnes minimum.



## 10. 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 doit permettre 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.

### **10.1. Recette de l'Infrastructure Réseau**

#### **10.1.1. 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.

#### **10.1.2. 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.

##### **10.1.2.1. 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.

À 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 désappairage,
- 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.

#### 10.1.2.2. Tests des liaisons optiques

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

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

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.

### **10.2. Recette du courant fort**

#### **10.2.1. 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.

#### **10.2.2. 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.

### **10.3. Recette des différents systèmes**

Le contrôle d'accès, postes de travail, sera contrôlé et réceptionné.

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.

#### **10.3.1. 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.

#### **10.3.2. 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 du système et d'enregistrement/relecture des communications,
- Des fonctionnalités d'automatisation des ouvertures.

### **10.4. Procès Verbal de recette**

Le procès-verbal de recette comportera le compte-rendu des contrôles visuel et fonctionnel.

Il sera composé de deux 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 du système de CA 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.

### **10.5. 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.

### **10.6. 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. À 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. À 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.

#### **10.7. 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.

À 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.

#### **10.8. 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.

## **11. GARANTIE**

### **11.1. Modalités**

Le service demandeur doit préciser les actions à exécuter lors de la maintenance face à chaque type ou cas de panne.

La garantie 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 du client (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.

### **11.2. Interventions pendant la période de garantie**

#### **11.2.1. 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.
- Panne non urgente : Toutes les autres pannes sont considérées comme non urgentes.

#### **11.2.2. 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 24 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi).
- Panne non urgente : Elle devra être réparée dans les 48 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).

### **11.3. 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).

### **11.4. Interventions après la période de garantie**

En plus de renseigner le CRT onglet 11.GARANTIE & MAINTENANCE, le titulaire fournira un contrat type de maintenance pour une mise à jour logicielle majeure annuelle détaillé et chiffré basé sur les éléments du système déployé.

## 12. ANNEXES

Le présent CCTP est complété par une description détaillée sous forme 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. Tout ou partie des annexes sera fournie en fonction du périmètre de la prestation demandée dans le présent CCTP.

### ATTENTION !

**Les annexes ci-après et celles fournies en pièces jointes font partie intégrante de ce CCTP.**

**À ce titre, leurs prescriptions sont à appliquer, en fonction du périmètre de la prestation demandée, aussi bien pour l'établissement de la proposition financière et technique, que lors de la réalisation des travaux.**

#### **ANNEXE 1 : Principes concernant les équipements de l'installation et leur raccordement**

ANNEXE 1 :

Principes concernant les équipements de l'installation et leur raccordement.

Fichier de référence :

PREF47-controle d'accès-ANNEXE 1-CCTP SURETE SGAMI DSIC\_PRINCIPES CABLAGE EQUIPEMENTS  
RACCORDEMENT.pdf

#### **ANNEXE 2 : Principes concernant le système de contrôle d'accès**

ANNEXE 2 :

Principes concernant le système de contrôle d'accès

Fichier de référence :

PREF47-controle d'accès-ANNEXE 2-CCTP SURETE SGAMI DSIC\_PRINCIPES CONTROLE ACCES.pdf

#### **ANNEXE 3 : Principes concernant la réglementation**

ANNEXE 3 :

Principes concernant la 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 5, mis 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.

Fichier de référence :

PREF47-controle d'accès-ANNEXE 3-MI Normes et Reglementations Applicables V1-0.pdf

#### **ANNEXE 4 : Tableau des points de sûreté**

Cette annexe reprend l'ensemble des lecteurs de badges, existants et futurs, ainsi que leur positionnement sur le site, les ouvrants, les types de dispositifs de fermeture.

Fichier de référence :

PREF47-controle d'accès-ANNEXE 4-Liste des points sûreté.pdf

Ce document sera remis lors de la visite obligatoire du site.

#### **ANNEXE 5 : Plan des points de sûreté**

Les plans suivants seront remis sur site lors de la visite obligatoire :

- 2025-03-aile-neuve-R-1-CA.pdf
- 2025-03-aile-neuve-R0-CA.pdf
- 2025-03-aile-neuve-R+1-CA.pdf
- 2025-03-aile-centrale-R-1-CA.pdf
- 2025-03-aile-centrale-R0-CA.pdf
- 2025-03-aile-centrale-R+2-CA.pdf
- 2025-03-aile-centrale-R+1-CA.pdf