Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA ZONE DE DÉFENSE ET DE SÉCURITÉ SUD

PRÉFET
DE LA ZONE
DE DÉFENSE
ET DE SÉCURITÉ
SUD

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

ANNEXE 2
Principes concernant le système de contrôle d'accès
2020

Les principes de déploiement des équipements ci-dessous servent de référence aux particularités du site décrites dans le document principal

CCTP SURETE – DESCRIPTIF DU PROJET

Table des matières

1. Généralités....4
1.1. Définitions....4
1.2. Spécifications ANSSI....4
1.3. Autres règles de sécurité....9
1.4. Intégration de l’antivirus....9
1.5. Synchronisation de l’heure....9
1.6. Logiciels et firmwares....9
1.7. Journalisation....9
1.8. Architecture....10
2. Architecture du système....10
2.1. Généralités....10
2.1.1. Système « Mono-site »....11
2.1.2. Système « Multi-sites »....11
2.2. Serveurs....11
2.2.1. Configuration matérielle des serveurs....11
2.2.2. Configuration logicielle des serveurs....12
2.3. Les stations....12
2.3.1. Configuration matérielle des stations....12
2.3.2. Configuration logicielle des stations....12
2.3.3. Poste de gestion des badges....12
2.3.4. Poste de gestion du contrôle d’accès....13
2.3.5. Poste de sécurité....13
2.4. Ecrans de grande diagonale....13
2.5. Prestation optionnelle....13
3. Unité de traitement local (UTL)....14
3.1. Généralités....14
3.2. Règles de l’art....15
3.3. Installation physique....15
3.4. Raccordement des périphériques....15
3.5. Raccordement logique....16
3.6. Accès au réseau local « Sûreté »....16
3.7. Prestation électrique....16
4. Périphériques de commande des accès....16
4.1. Lecteur de badges (LB) et support sans contact....16
4.1.1. Caractéristiques physiques....16

4.1.2. Caractéristiques logiques....17
4.1.3. Renouvellement des clés....18
4.2. Support biométrique (empreinte)....18
4.3. Contrôle des accès par visiophonie....19
4.3.1. Caractéristiques générales....19
4.3.2. Intégration à la solution vidéo....19
5. Équipements de portes....20
5.1. Généralités....20
5.2. Caractéristiques des serrures électromécaniques....20
5.2.1. Mode 1....20
5.2.1.1. Version 3 points....21
5.2.1.2. Version 1 point....21
5.2.1.3. Version 3 points pour passage intensif....22
5.2.1.4. Version 1 point pour passage intensif....22
5.2.2. Mode 2....23
5.2.2.1. Version 3 points....23
5.2.2.2. Version 1 point....24
5.2.3. Mode 3....24
5.2.3.1. Version 3 points....24
5.2.3.2. Version 1 point....25
5.3. Ventouses électromagnétiques....25
6. Déverrouillage des portes....26
6.1. Généralités....26
6.2. Déclencheur Manuel de déverrouillage (DMD) ou (BBG)....27
6.3. Bouton d'ouverture de porte (BOP)....27
7. Gestion des accès....27
7.1. Configuration des accès....27
7.2. Gestion des couloirs rapides à unicité de passage (CRUP)....28
7.3. Asservissement des accès....29
7.4. Anti-retour....30
7.5. Gestion du parking....30
7.5.1. Le filtrage efficace des véhicules....30
7.5.2. Le comptage des véhicules....31
7.6. Gestion des équipements de détection d'intrusion....31
7.7. Gestion des équipements d'anti-agression....31
7.8. Maquette....32

1. GÉNÉRALITÉS

Le système sera conforme à la règle **APSAD D83**.

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

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

1.1. Définitions

Un système de contrôle d'accès d'un site est composé de :

- un serveur de gestion du système ;

- une ou plusieurs Unités de Traitement Local (UTL) intégrant des modules d'extension soit en local, soit en déporté. Ces modules, reliés en BUS RS485 à l'UTL, permettent en général la gestion de 2 lecteurs de badges ;

- des lecteurs de badges Mifare Desfire Ev1 ou Ev2: ils communiquent en mode transparent, en bus RS485 chiffré, avec signal de vie. Ils peuvent être associés à un clavier.

1.2. Spécifications ANSSI

L'ensemble de la solution d'accès doit s'appuyer sur les recommandations du guide de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) [RFID ANSSI]. Le système de contrôle d'accès reposera uniquement sur l'architecture N°1 décrite dans ce document.

[RFID ANSSI] - Guide Sécurité des technologies sans contact pour le contrôle des accès physiques version de travail 1.0, 19 novembre 2012.

Dans l'attente d'une version consolidée, cette version de travail fera office de document de référence.

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

- Les mesures de niveau **L1 et L2** pour les sites **Préfectoraux ou de Sécurité Publique**

  (à l'exception des mesures concernant les visuels de la carte agent ainsi que celle concernant la CSPN des lecteurs),
- Les mesures de niveau **L1, L2 et L3** pour les **sites sensibles**.

<u>Spécifications, extraites de ce guide, à respecter pour</u> :

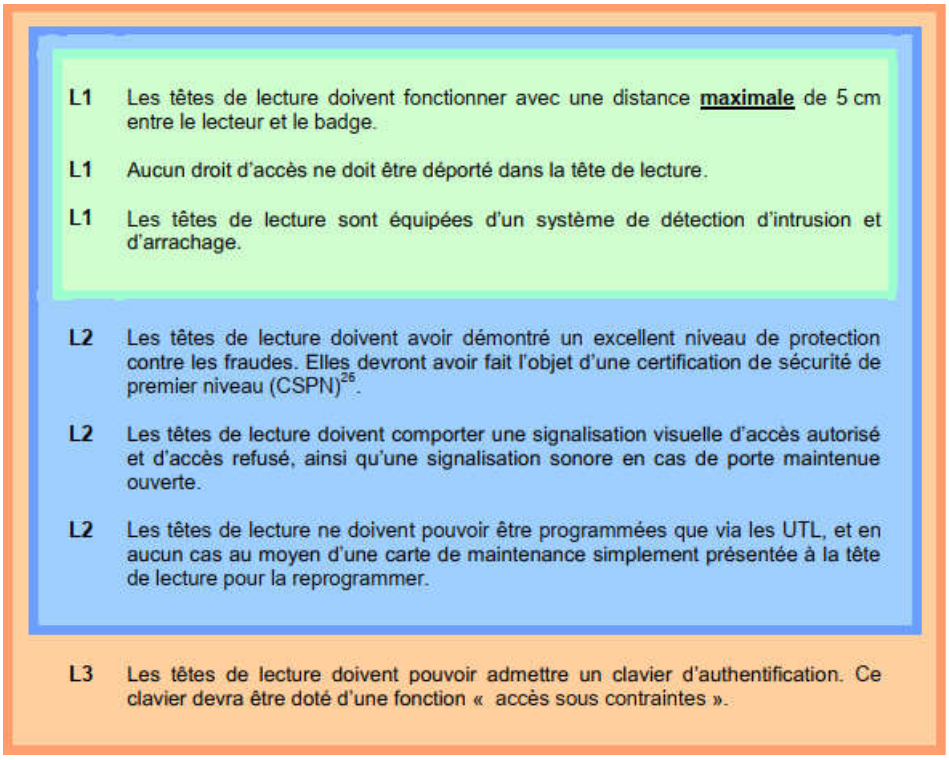
<u>- Technologies utilisées</u>



Le Tableau ci-dessous, extrait de ce guide, décrit la méthode d'identification/authentification à mettre en place pour les niveaux L1, L2 et L3 respectivement.

Résistance aux attaques logiques	**Méthode**	**Technologie**	**Caractéristiques**
-	Identification du badge, ou information mémorisée, ou élément biométrique.	Transpondeurs 125kHz et assimilés, cartes ISO14443 ou ISO15693 sans usage de la cryptographie ou à cryptographie défaillante ou propriétaire.	Facilement clonable
L1	Authentification du badge, clefs dérivées recommandées.	Carte ISO 14443, authentification à cryptographie symétrique.	Authentification reposant sur une clef commune ; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).
L2	Authentification du badge, clefs dérivées recommandées.	Carte ISO 14443, authentification à cryptographie symétrique.	Authentification reposant sur une clef dérivée d'une clef maîtresse ; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).
L3	Authentification du badge et du porteur par un second facteur (information mémorisée ou élément biométrique). Clef dérivées.	Carte ISO 14443, authentification à cryptographie symétrique. Saisie d'un code mémorisé ou d'un élément biométrique.	Authentification reposant sur une clef dérivée d'une clef maitresse ; Algorithmes et protocoles d'authentification connus et réputés (3DES, AES).

- les têtes de lecture

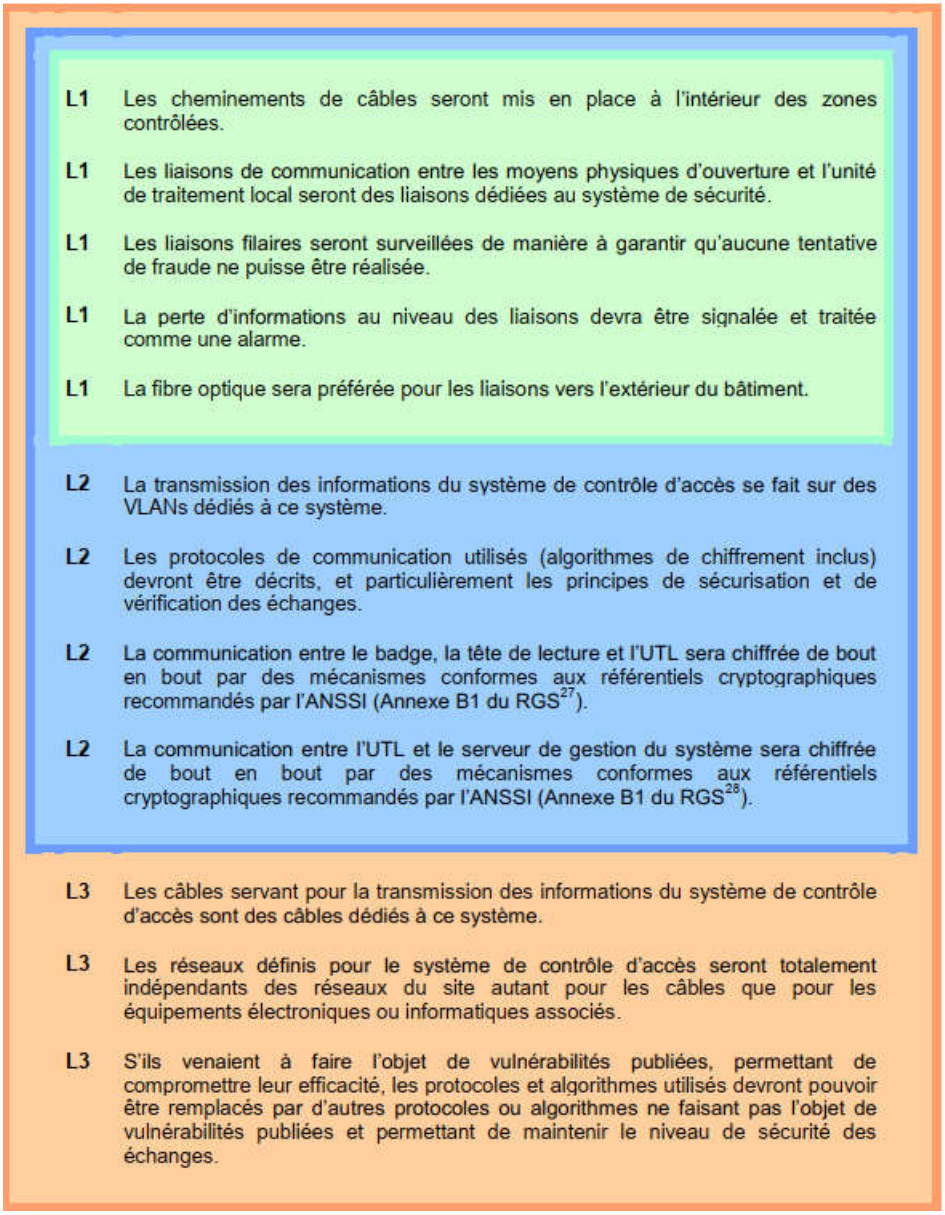


L'exigence relative à la Certification de Sécurité de Premier Niveau (CSPN) de l'ANSSI concernant les lecteurs sera précisée dans le «descriptif du projet».

- les UTL (Unité de Traitement Local)

L1	Les UTL et concentrateurs associés peuvent être associés en un seul et même équipement assurant les fonctions des deux.
L1	Les UTL analysent les droits du badge et délivrent l'ordre d'ouverture gâche ou actionneur.
L1	Pour leurs évènements et alarmes, les UTL assureront la datation.
L1	Les UTL transmettent les informations liées à la transaction, au serveur de gestion du système (UTS, GAC, ou autre équipement).
L1	Les UTL doivent émettre, vers le serveur de gestion du système, des informations sur les anomalies de fonctionnement qui leurs sont propres et sur les équipements qui leurs sont associés.
L1	Les UTL s'auto-surveilleront en générant des défauts internes. Ces alarmes seront datées et envoyées aux serveurs de gestion du système comme une alarme interne.
L1	Les UTL doivent réaliser des diagnostics fonctionnels sur les équipements qui lui sont associés.
L1	La sécurisation des UTL devra être cohérente avec la solution globale proposée.
L1	Les UTL sont installées à l'intérieur des zones qu'elles contrôlent.
L1	Les UTL sont équipées d'un système de détection d'intrusion et d'arrachage.
L1	Toutes les UTL pourront fonctionner sans perturbation en cas de perte de la liaison avec les équipements en amont.
L1	En cas de coupure de liaison avec le serveur de gestion du système, les UTL doivent pouvoir archiver temporairement un nombre d'alarmes ou d'événements compatible avec les exigences, puis assurer une mise à jour différée de l'archivage centralisé.
L1	En cas de coupure de liaison avec le serveur de gestion du système, les UTL doivent pouvoir gérer au minimum N badges.
L1	Les UTL possèderont une mémoire (contenant les instructions du traitement) type EPROM (*Erasable Programmable Read Only Memory*) ou RAM (*Random Access Memory*) sauvegardée par batterie (24 heures minimum).
L2	Les UTL doivent être capables de gérer « l'anti *pass-back* » des lecteurs qui lui sont associés.
L3	Pas d'exigence spécifique pour ce niveau.

- les réseaux et communications



A noter : les exigences indiquées sont complémentaires.

Pour atteindre un niveau de sécurité de **niveau L1**, il faut appliquer toutes les exigences du niveau **L1**.

Pour atteindre un niveau de sécurité de **niveau L2**, il faut appliquer toutes les exigences du niveau **L1 et** toutes celles du niveau **L2**.

Pour atteindre un niveau de sécurité de **niveau L3**, il faut appliquer toutes les exigences du niveau **L1**, du niveau **L2 et** toutes celles du niveau **L3**.

A la demande de l'administration, certaines mesures, notamment celles concernant le chiffrement de la communication entre l'UTL et le serveur de gestion du système ou la mise en œuvre de clés dérivées, peuvent être activées soit dès la mise en service de l'installation, soit en phase décalée.

1.3. Autres règles de sécurité

La configuration du serveur de gestion du système de contrôle d'accès , ainsi que les postes de travail relatifs au contrôle des accès, doivent être sécurisés par l'application des mesures habituelles de sécurité des systèmes d'information.

Pour tous les matériels constituant le système, les règles suivantes doivent être observées :

- Les modes de communication par liaison sans fil (WIFI ou autre) ainsi que les fonctionnalités associées doivent être désactivés.
- De la même manière, les équipements par liaison sans fil sont à proscrire
- Un cloisonnement logique doit être établi entre les sous-systèmes. L'interconnexion entre les sous-systèmes s'opèrent uniquement par l'intermédiaire d'un dispositif de routage/filtrage.
- Les mots de passe par défaut doivent être remplacés par des mots de passe spécifiques et robustes. Les systèmes doivent pouvoir gérer des mots de passe d'une longueur minimale de 10 caractères, avec des caractères alphabétiques minuscules et majuscules, des chiffres et des symboles.
- Les possibilités de communications vers des serveurs « internet » doivent être désactivées (ex : mise à jour, dns ….)
- Les fonctions et interfaces d'administration ainsi que les services non utilisés doivent être désactivés

Il est impératif que la solution respecte les contraintes sur les flux et les contraintes de sécurité.

Tous les flux générés par les équipements doivent être identifiés et décrits dans l'offre présentée par le soumissionnaire du marché.

1.4. Intégration de l'antivirus

Dans le cas où l'installation a accès à la plate-forme de l'antivirus de l'administration, les postes et serveurs faisant partie de l'installation doivent intégrer l'antivirus McAfee. L'antivirus est en mode géré. L'agent McAfee ainsi que le logiciel antivirus seront fournis par l'administration.

1.5. Synchronisation de l'heure

Dans le cas où l'installation a accès au serveur NTP de l'administration, les équipements IP faisant partie de l'installation doivent être synchronisés avec ce dernier. Les paramètres IP de synchronisation seront fournis par l'administration.

Si l'installation n'accède pas au serveur NTP de l'administration, un serveur de temps de référence doit être installé sur un des équipements de l'installation. Les autres équipements IP se synchronisent avec ce serveur de temps.

1.6. Logiciels et firmwares

Les équipements doivent disposer de la version la plus récente des logiciels et firmwares.

1.7. Journalisation

Le système doit gérer la journalisation des événements. La journalisation des événements est un processus automatique qui a pour but d'enregistrer les accès des utilisateurs ainsi que les opérations menées sur un système en identifiant l'auteur, la date, l'heure ainsi que la nature de l'opération.

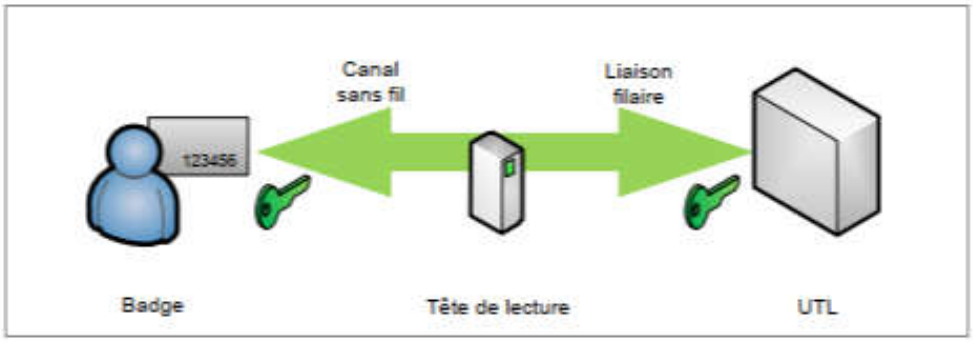
Les historiques relatifs aux accès et déplacements des utilisateurs sont conservés pendant une durée

glissante de 3 mois au terme de laquelle ils seront automatiquement supprimés.

La journalisation des opérations porte essentiellement sur l'administration et l'exploitation des équipements constituant le système du contrôle d'accès. Elle consiste notamment à sauvegarder la création, la modification et la consultation des données d'un système ou d'une application.

1.8. Architecture

Le système de contrôle d'accès ne reposera que sur l'architecture N°1 décrite dans le guide de l'ANSSI : tête de lecture transparente, authentification de bout en bout.



Architecture n°1 : tête de lecture transparente, authentification de bout en bout

Le badge, sécurisé, s'identifie et s'authentifie directement à l'UTL par l'intermédiaire de la tête de lecture qui transmet les messages sans les modifier, et ne participe pas au protocole cryptographique (tête de lecture dite « transparente »).

2. ARCHITECTURE DU SYSTÈME

2.1. Généralités

Le système sera bâti autour d'une solution de type client/serveur.

Le serveur peut être local dans le cas du système « mono-sites », ou sur un site principal distant pour les systèmes « multi-sites » dont la gestion est centralisée. Le document « descriptif du projet » indiquera le type de système choisi.

Le nombre de clients simultanés supportés par l'applicatif doit pouvoir être supérieur à 50.

Le serveur de gestion du système permet le traitement de 20 000 porteurs de badges actifs. Le système devra pouvoir gérer au minimum 4000 lecteurs de badges.

Le système de contrôle d'accès doit pouvoir fonctionner dans deux modes :

- Le mode en ligne,
- Le mode dégradé où certaines UTL fonctionnent en mode autonome

En ligne, le serveur assure une communication permanente avec les unités de traitement local (UTL).

Dans le mode dégradé, les UTL prennent en charge la gestion des accès et tous les événements sont stockés et retransmis au serveur dès rétablissement de la communication.

2.1.1. Système « Mono-site »

Le système « Mono-site » est une installation autonome. Cependant, il doit posséder tous les pré-requis permettant son intégration ultérieure dans une infrastructure centralisée du système « Multi-sites » détaillé dans le paragraphe ci-dessous.

La capacité de la solution sera spécifiée dans le document CCTP « descriptif du projet ».

2.1.2. Système « Multi-sites »

Le système « Multi-sites », avec un serveur centralisé, doit permettre de cloisonner les lecteurs par site et les usagers par entité.

Le système « Multi-sites » doit permettre aux opérateurs locaux d'exécuter en toute autonomie, depuis un poste client, les opérations d'administration et d'exploitation de la solution pour le périmètre local.

Le système « Multi-sites » doit permettre au gestionnaire local de gérer uniquement

- Les lecteurs de son ou ses sites
- Les usagers de son ou ses entités

Le système « Multi-sites » doit permettre la gestion de zones communes à plusieurs sites. Certains accès pourront en effet être gérés par plusieurs opérateurs gestionnaires.

De même un usager devra pouvoir appartenir à plusieurs entités et pourra de ce fait avoir accès à plusieurs sites. Un usager « Multi-site » pouvant accéder à plusieurs sites devra pouvoir recevoir ses droits d'accès de chaque opérateur gestionnaire pour chaque site ou par un gestionnaire principal ayant capacité à gérer tous les sites concernés.

La capacité de la solution sera spécifiée dans le document CCTP « descriptif du projet ».

2.2. Serveurs

2.2.1. Configuration matérielle des serveurs

Le serveur sera de type rackable et intégré dans la baie « sûreté » sauf avis contraire dans le document CCTP descriptif du projet. Il sera équipé de :

- Micro-processeur type Intel Xeon ou supérieur
- Disques durs système montés en « raid 1 »,
- Disques durs données montés en « raid 5 »,
- 16 Go mémoire minimum,
- Double alimentation,
- Carte réseau multiports gigabit Ethernet,
- Carte graphique standard multiports.

La solution devra disposer d'un dispositif de sauvegardes régulières du système de gestion. Les fichiers contenant les paramètres de configurations des équipements doivent également être sauvegardées.

La solution devra disposer d'un système de restauration de la sauvegarde.

Les procédures relatives à ces opérations seront fournies par le titulaire du présent lot.

Le soumissionnaire prévoira systématiquement des commutateurs clavier-écran-souris (Keyboard-Vidéo-Mouse, en abrégé KVM), pour permettre le partage d'un même clavier, souris et écran dans les baies « serveurs ». Cet équipement devra disposer de deux ports libres pour les futurs postes d'exploitation.

2.2.2. Configuration logicielle des serveurs

Ils seront équipés du système d'exploitation Windows Server 2016 ou supérieur, 64 bits. Le système d'exploitation doit être à jour des derniers correctifs de sécurité. La base de données est une base MS SQL 2016 ou supérieur de type 64 bits ou équivalent.

2.3. Les stations

La localisation des stations d'exploitation et de gestion des badges sera précisée sur les plans remis lors de la visite du site.

2.3.1. Configuration matérielle des stations

Les postes clients sont des micro-ordinateurs de type « tour ». Selon les cas, décrits dans le document « descriptif du projet », l'administration cliente peut fournir ces PC.

Les caractéristiques minimales des stations de gestion sont :

- processeur i5 - 3,7 Ghz
- mémoire Ram 4Go
- Ddur : 500 Go
- système d'exploitation 64 bits : W10 Entreprise
- écran LED 22''
- clavier et souris

La carte graphique doit être dédiée. Le nombre et le type de connecteurs (VGA, DVI, HDMI, DP [Display Port]) devront être précisés. Si le nombre d'écrans est supérieur au nombre de sortie graphique, prévoir une deuxième carte graphique.

En présence de ports DP sur le(s) carte(s) graphique(s) et sur l'(es) écran(s), le raccordement de la carte graphique sur l'écran doit être fait en DP.

Ils disposent d'un clavier filaire ergonomique et d'une souris filaire 2 boutons et molette.

2.3.2. Configuration logicielle des stations

Les stations seront équipées du système d'exploitation Windows 10 Entreprise 64 bits. Le système d'exploitation doit être à jour des derniers correctifs de sécurité.

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

2.3.3. Poste de gestion des badges

En plus des caractéristiques de configuration définies au paragraphe 2.3.1, ce poste sera équipé d'un lecteur RFID sur port USB compatible et du kit d'encodage de la solution proposée par le titulaire.

Il sera réservé au gestionnaire de badges et permettra l'encodage des badges, l'enrôlement des CAM (Cartes Agents Ministérielles) et des badges blancs.

2.3.4. Poste de gestion du contrôle d’accès

En plus des caractéristiques de configuration définies au paragraphe 2.3.1, il comportera une carte vidéo permettant le raccordement de 2 écrans distincts.

Il permettra :

- La gestion du contrôle d’accès
- L’affichage de la cartographie avec action de verrouillage et déverrouillage des accès,
- La gestion de la main courante des événements.

2.3.5. Poste de sécurité

Il comportera une carte vidéo permettant le raccordement de 2 écrans distincts.

Il permettra :

- L’exploitation du contrôle d’accès
- L’affichage de la cartographie avec action de verrouillage et déverrouillage des accès,
- La gestion de la main courante des événements.

En plus des caractéristiques de configuration définies au §2.3.1, ce poste pourra être équipé en option d’un lecteur RFID sur port USB compatible avec la solution d’encodage proposée par le titulaire, pour la délivrance de badges visiteurs.

2.4. Ecrans de grande diagonale

Ces écrans seront de technologie LED HD et disposeront des caractéristiques minimum :

- Diagonale de 43 pouces minimum,
- Résolution de dalle de 1920 x 1080 p minimum,
- Interfaces graphiques : VGA, DVI, HDMI, DP,
- HDMI conforme aux normes EDID et HDCP,
- Haut-parleurs intégrés,
- Fixation à la norme VESA,
- Luminosité minimale de 350 cd/m2,
- Contraste de 2000 : 1,
- Temps de réponse : 5 ms,
- PIP (incrustation d’images, Picture in picture),
- Usage intensif (affichage permanent).

2.5. Prestation optionnelle

Si demandé dans le document « descriptif du projet », le soumissionnaire mentionnera dans son offre les solutions de redondance du serveur permettant de s'affranchir de la défaillance d’un disque système. Il indiquera également si cette solution a une incidence sur le nombre de licences.

Cette redondance pourra être locale ou déportée. Dans ce dernier cas, le soumissionnaire indiquera la bande

passante à réserver sur le lien, nécessaire au bon fonctionnement.

3. UNITÉ DE TRAITEMENT LOCAL (UTL)

3.1. Généralités

Selon prescriptions dans le document « descriptif du projet », la solution devra permettre, sur les équipements contrôlés, l'identification par :

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

Les Unités de Traitement Local (UTL) seront équipées d'une autoprotection qui intégrera la surveillance de l'ouverture et de l'arrachement du coffret et seront installées de préférence dans des locaux techniques sécurisés.

Toutes les liaisons de type « Wiegand ou Clock/data », entre un lecteur de badge et un autre équipement, sont interdites (UTL, module d'extension). La liaison avec le lecteur est réalisée en RS-485 et chiffrée de bout en bout.

Dans le cas d'une primo-installation, la liaison UTL-lecteurs est en RS485, chiffrée de bout en bout sans adjonction d'interface entre le module de porte d'UTL et le lecteur.

Néanmoins, en cas d'extension/adaptation d'une solution existante, l'insertion d'une interface entre le module de porte et le lecteur est tolérée, à condition que cette dernière soit hébergée dans un local sécurisé (local technique de préférence).

Cette liaison est bidirectionnelle de bout en bout.

Les UTL communiqueront avec le serveur par liaison Ethernet **impérativement**.

Les modules de porte (MDP) doivent disposer des interfaces d'entrée et de sortie en nombre suffisant pour pouvoir gérer :

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

Les modules de porte (MDP) doivent disposer de LEDs permettant de visualiser leur état durant une opération de maintenance.

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

Dans ce mode, les UTL gèrent toutes les demandes d'accès et conservent un journal de toutes les activités (accès, entrées/sorties ToR, alarmes, etc.). Les droits d'accès sont accordés en fonction des données stockées dans l'UTL au moment de la perte de connexion.

Le système doit pouvoir conserver un historique d’au moins 5000 derniers événements en cas de perte de communication avec le serveur.

Lorsque la communication est rétablie, les journaux d'activité sont transférés vers le serveur avec l’intégralité de l’historique d’activité (accès et états des entrées/sorties). Le système doit fournir la possibilité d’effacer les clés sur autoprotection coffret ou manuellement (cas du retour usine).

Les modules d’extension communiquent avec les UTL et les lecteurs transparents en bus RS485 crypté. Ils embarquent un composant « coffre-fort » SAM/HSM dans lequel les clés sont stockées et protégées. Le composant SAM/HSM doit présenter un niveau de sécurité certifié ANSSI EAL5+.

La durée de conservation des événements devra être paramétrable jusqu'au seuil maximum de la réglementation en vigueur.

Les UTL intégreront leur propre alimentation sauvegardée par batterie embarquée.

L'alimentation sera auto-protégée par surveillance à l'ouverture et à l'arrachement du coffret. Cette alimentation disposera au minimum de 2 sorties indépendantes :

- alimentation de l'ensemble de la partie électronique (cartes UTL, cartes d'extension et lecteurs),

- charge de la batterie.

L’ alimentation des organes de verrouillage sera indépendante. La mise en défaut (court-circuit ou mise à la Terre) d'une voie ne devra mettre hors service que la voie concernée et ne devra pas impacter les autres voies.

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

- La gestion des badges (profils d'accès associés, date d'expiration),

- La gestion de l'environnement porte (porte maintenue ouverte trop longtemps et porte forcée, période d'ouverture automatique),

- La gestion des entrées/sorties (mise en/hors service sur période horaires, temporisations, activation de sortie sur alarme d'une entrée).

3.2. Règles de l’art

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 et les précisions portées sur les plans du bâtiment. A défaut, le soumissionnaire proposera une solution alternative qui devra être validée par l'administration.

3.3. Installation physique

Les UTL devront être installées dans les locaux techniques désignés lors de la visite de site ou sur plan (pour bénéficier entre-autres de l’énergie secourue). Le titulaire peut proposer la modification de leur implantation sous réserve de ne pas dégrader la sûreté de l'installation et d’obtenir l’accord de l’administration.

Les modules de portes pourront être installés dans des coffrets fermant à clé, équipés de l’anti arrachement. Ces coffrets ne devront pas être accessibles au personnel non habilité.

3.4. Raccordement des périphériques

En cas de remplacement d’un système existant, par souci d’économie, d’esthétique (câble encastré plutôt

qu'une pose en saillie), de minimisation de travaux de percement, le titulaire réemploiera, dans la mesure du possible la distribution existante, après vérification de son état général et avec l'accord de l'administration.

Il devra ainsi, selon nécessité :

- Prolonger câble par câble le raccordement des périphériques existants (contrôle d'accès et détection d'intrusion) entre l'implantation actuelle des UTL et leur futur emplacement.
- Protéger les boîtes de raccordement contre l'ouverture (dispositif d'autoprotection).

3.5. Raccordement logique

Le principe est de permettre la continuité de service entre l'ancien et le nouveau système sans coupure excessive par substitution un pour un des lecteurs de badges.

En cas de remplacement d'un système existant de technologie Mifare classique, il peut être demandé dans le descriptif du projet, la pose de lecteurs de badges (double tête). Dans ce cas, le titulaire proposera des lecteurs de badges compatibles Mifare classique et Desfire EV1.

En début de chantier, les nouveaux lecteurs de badges seront installés en lieu et place des anciens et configurés en technologie « Mifare ».

En fin de chantier, lorsque la nouvelle infrastructure sera opérationnelle, ils seront reprogrammés définitivement en version « Desfire EV1 » lors de la cérémonie des clés.

Remarque : S'il s'avère impossible de procéder à la réutilisation de l'ancien câblage et à la substitution et programmation des lecteurs de badges définies ci-dessus, le titulaire procédera au renouvellement complet du câblage et à la cohabitation momentanée des lecteurs de badges ancienne et nouvelle génération.

3.6. Accès au réseau local « Sûreté »

Un lien « Ethernet » catégorie 6A / classe EA sera créé entre la ou les UTL et la baie hébergeant le commutateur « sûreté » le plus proche.

3.7. Prestation électrique

Chaque UTL sera raccordée à l'installation par un circuit 220 V-16 A 2P+T protégé par un disjoncteur différentiel 30mA hautement immunisé (classe HI). Son branchement sera effectué sur le tableau de distribution électrique désigné par l'administration.

Ces circuits seront raccordés sur l'alimentation secourue du bâtiment si existant.

Chaque UTL sera raccordée sur une alimentation secourue par batteries.

4. PÉRIPHÉRIQUES DE COMMANDE DES ACCÈS

4.1. Lecteur de badges (LB) et support sans contact

4.1.1. Caractéristiques physiques

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

Les lecteurs seront en version Mifare DesFire Ev2, compatibles EV1.

Toutes les liaisons de type « Wiegand ou Clock/data », entre un lecteur de badge et un autre équipement, sont interdites (UTL, contrôleur spécifique).

La liaison avec le lecteur est réalisée par bus RS-485.

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

- Lecteur en veille (visuel),
- Passage autorisé (uniquement visuel),
- Passage non autorisé (visuel et sonore),
- Alarme de temporisation de porte ouverte dépassée (sonore).

Les lecteurs RFID devront être protégés à l'ouverture.

4.1.2. Caractéristiques logiques

La carte agent est en mode Random ID avec une « clé maîtresse carte » secrète. Ce dispositif de RandomID est activé par défaut sur les cartes agent servant de badges d'accès du personnel. En conséquence, Le système de contrôle d'accès doit supporter le mécanisme de RandomID.

En revanche, il n'est pas nécessaire d'implémenter le RandomID sur les badges visiteurs.

Le système doit être en mesure d'interagir avec les deux types de cartes.

La condition d'accès est réalisée par la lecture sécurisée d'un identifiant (numéro logique). La lecture de l'identifiant est conditionnée à l'authentification Mifare Desfire.

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

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

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

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

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

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

Les lecteurs doivent être transparents.

Le lecteur doit pouvoir traiter le protocole Mifare T=CL.

Le lecteur doit délocaliser (lecteur transparent) la partie antenne de la partie décodage RFID de manière à ce

que l’information sur le câble de liaison soit protégée par la clé de session utilisée entre l’antenne et la carte.

Les lecteurs **RFID et UTL** doivent être à jour des patchs de sécurité. Ces deux dispositifs font partie des éléments décrits dans le maintien en condition de sécurité. La détection d'une faille de sécurité nécessitera une mise à jour et des mesures correctives dans le cadre du déploiement et/ou du maintien en condition de sécurité de la solution.

Tous les composants utilisant un Sécurity Account Manager (SAM) devront montrer un canal sécurisé ainsi qu’un canal d’authentification avec le lecteur garantissant que le vol du SAM ne peut mettre en péril les secrets de la solution. Idéalement, le SAM est le composant de sécurité évalué.

La configuration des secrets des SAM ne doit pas nécessiter de clés privées dont l'administration n'aurait pas la propriété. Une procédure de configuration pour remettre les paramètres usine (qui peuvent être constructeur) sont nécessaires en cas d'initialisation et de retour du matériel.

Toutes les exportations de clés sont interdites.

Toutes les introductions de clés dans la solution doivent être sécurisées. **La clé ne doit pas être affichée en clair** sur les postes d’exploitation et de gestion du site.

En aucun cas, le titulaire ne doit connaître les clés de l’administration.

Idéalement, chaque clé peut être introduite par 1 ou 3 porteurs suivant sa sensibilité. Elles sont stockées sur support papier. Dans le cas ou la clé est introduite par plusieurs porteurs, la clé finale est reconstituée par des XOR successifs de chaque cryptogramme (*K=XOR[XOR[K1,K2],K3])*. La vérification de la bonne introduction de la clé K est effectuée par comparaison des 4 premiers octets du SHA-256 de la clé K. Cette introduction par plusieurs porteurs est un plus à la solution.

La solution devra permettre la configuration de la partie applicative «Encodage » pour garantir la compatibilité avec les AID, les clés applicative, lecture et écriture de l'administration.

Le titulaire doit fournir une **documentation** sur la gestion des clés incluant :

- La configuration des lecteurs/encodeurs et ou éléments à sécuriser (SAM),

- Le descriptif des clefs, index et noms utilisés dans les cartes et dans tous les lecteurs/ encodeurs d’identifiants et SAM,

- Une procédure de protection des secrets de la solution (cérémonie de clés) qui reprend les termes/noms/éléments techniques décrits dans les documents.

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

4.1.3. Renouvellement des clés

La solution doit permettre un renouvellement des clés par l'injection de nouvelles clés au poste d’encodage des badges. Cette solution doit permettre un basculement avec une période transitoire où deux jeux de clés sont utilisés sur les têtes de lecture. La procédure de migration est établie par le référent sûreté et appliquée sur toutes les têtes de lecture. Le mode permanent avec les nouvelles clés de lecture est alors mis en place après l'encodage du dernier badge du site. En mode permanent, et donc à la fin du processus de renouvellement, les UTL sont configurées pour ne lire que les nouvelles clés.

La modalité utilisée est définie avec l’administration durant la phase de conception.

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

4.2. Support biométrique (empreinte)

Les lecteurs RFID utilisés pour lire les informations biométriques sont soumis aux mêmes contraintes que

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

Conformément avec la législation CNIL, le stockage des données biométriques est réalisé dans le badge.

4.3. Contrôle des accès par visiophonie

4.3.1. Caractéristiques générales

Plusieurs cas se présentent :

- Les portiers audio sont à remplacer par un système de visiophonie.
- Le système de visiophonie est à créer ou à compléter

Dans le cas d'une nouvelle installation, il sera déployé de préférence un système de technologie IP qui aura les caractéristiques suivantes :

Platine Vidéo :

- Platine anti-vandale, de préférence encastrée si la configuration du site le permet,
- Impérativement muni de LED IR,
- Objectif grand-angle
- Technologie IP
- Si demandé dans le CCTP « descriptif du projet », ce portier pourra être associé à une caméra IP de l'installation.

De plus, la platine vidéo de rue, installée à l'entrée du public, sera conforme à la norme accessibilité des ERP (Loi 2014-789 du 10 juillet 2014).

- Boucle magnétique conforme à la norme NF EN 60118-4:2007
- Pictogrammes (appel en cours, parler, ouverture porte)
- Synthèse vocale (appel en cours, parler, ouverture porte)

Moniteur Vidéo :

- Ecran LED de 7 pouces minimum,
- Support mural ou de bureau,
- Commandes de portes par touches dédiés ou écran tactile

Le système peut comporter plusieurs platines ou plusieurs moniteurs. L'ensemble sera programmable à l'aide d'une interface Web.

Les adresses IP seront modifiées suivant le plan applicatif fourni par l'administration.

4.3.2. Intégration à la solution vidéo

Si demandé dans le descriptif du projet, le soumissionnaire proposera l' interfaçage du système de visiophonie avec le système de vidéo en place, afin d'enregistrer les images et de gérer, selon les cas, les accès à partir des postes d'exploitation sans utilisation de pupitre dédié.

Le son issu des platines de visiophones transitera par la carte audio du PC d'exploitation vidéo.

La restitution du son sur les écrans d'affichage des images sera privilégiée par rapport à des enceintes externes.

En aucun cas, le son ne sera enregistré.

5. ÉQUIPEMENTS DE PORTES

5.1. Généralités

Toutes les portes faisant partie de la prestation seront équipées d'un moyen de remontée d'information d'ouverture.

Ces informations (porte forcée, temps d'ouverture trop long,..) sont remontées par :

- des contacts en feuillure avec un circuit d'autoprotection et d'une bague d'isolement sur porte métallique
- des contacts en applique
- la serrure

Dans le cas de remplacement d'installation existante, aucun contact existant ne sera réutilisé.

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

L'ensemble des accès doit être équipé de ferme-porte, indispensable pour assurer la fermeture de la porte après chaque passage.

Les portes nécessitant le label DAS, de type Issue de secours (IS), seront munies de verrouillage normalisé NFS 61-937 et NF QE qu'il s'agisse de ventouse ou de serrure à sortie libre par béquille sur des portes à un vantail ou deux vantaux.

Les issues de secours doivent disposer côté intérieur d'un déclencheur manuel de couleur verte, type DMD permettant le déverrouillage de l'issue sans temporisation. Le boîtier de déverrouillage de sécurité agit alors par rupture directe de l'alimentation du dispositif de verrouillage. Un contact supplémentaire de détection de rupture est nécessaire. La commande de déverrouillage est distincte de l'ouverture et est mémorisée sur les historiques du système comme alarme. Elle engendre une alarme prioritaire sur les postes d'exploitation opérateur et active une alarme sonore et éventuellement visuelle locale. La sortie nécessite le brisé du scellé du DMD et engage un acte de dégradation volontaire.

Le principe de déverrouillage est développé au § 6.

5.2. Caractéristiques des serrures électromécaniques

Les caractéristiques des serrures seront adaptées à l'usage demandé par le maître d'ouvrage conformément aux trois modes de fonctionnement possibles, aux niveaux de résistance et aux fréquences d'utilisation ci-après décrits.

NB : Les titulaires du lot menuiserie et du lot courant faible devront s'assurer de l'adéquation en terme de PV coupe feu entre la porte et l'organe de verrouillage.

5.2.1. Mode 1

MODE 1 - Porte sous contrôle d'accès en entrée seule et sortie libre

5.2.1.1. Version 3 points

Version 3 points - Serrure à béquille contrôlée en entrée et sortie libre :

Afin d'assurer le bon fonctionnement du système de contrôle d'accès, il sera prévu un système de verrouillage électromécanique des portes concernées avec des niveaux de performances suivants :

Les portes seront équipées d'une serrure électromécanique assurant au minimum les mêmes fonctions qu'un verrouillage mécanique sur 3 points, à savoir une fermeture à la clé sur 3 points médians (pênes dormant) afin d'éviter la voilure de la porte. La résistance sera supérieure à 3 000 kg.

De plus, à chaque fermeture de porte, la serrure se verrouillera mécaniquement automatiquement afin d'assurer un niveau de sûreté constant à chaque porte « claquée ».

La serrure sera paramétrable afin de simplifier la pose : 100% réversible gauche / droite / tirant / poussant, émission ou rupture, bi tension 12 / 24 VDC.

La sortie se fera par simple abaissement de la béquille et en une seule manœuvre conformément au code du travail et aux normes ERP en vigueur (EN179).

En version émission de courant, la porte restera fermée et verrouillée même en cas de situation dégradée (absence de courant, foudre, panne, …) donc la porte restera en sûreté depuis l'extérieur tout en assurant la sortie libre.

Enfin, les informations suivantes devront être remontées au système de contrôle d'accès : porte fermée, porte verrouillée, ouverture à la clé (anomalie), abaissement de la béquille (sortie « conforme »), boucle anti-sabotage.

Axe obligatoire à 50mm au standard Français afin de faire évoluer le système sans modifier l'intégrité de la porte (y compris pour les portes coupe feu).

5.2.1.2. Version 1 point

Version 1 point - Serrure à béquille contrôlée en entrée et sortie libre :

Afin d'assurer le bon fonctionnement du système de contrôle d'accès, il sera prévu un système de verrouillage électromécanique des portes concernées avec des niveaux de performances suivants :

Les portes seront équipées d'une serrure électromécanique assurant au minimum les mêmes fonctions qu'un verrouillage mécanique, à savoir une fermeture à la clé sur un point médian (pêne dormant) afin d'éviter la voilure de la porte. La résistance sera supérieure à 1 000 kg.

De plus, à chaque fermeture de porte, la serrure se verrouillera mécaniquement automatiquement afin d'assurer un niveau de sûreté constant à chaque porte « claquée ».

La serrure sera paramétrable afin de simplifier la pose : 100% réversible gauche / droite / tirant / poussant, émission ou rupture, bi-tension 12 / 24 VDC.

La sortie se fera par simple abaissement de la béquille et en une seule manœuvre conformément au code du travail et aux normes ERP en vigueur (EN179).

En version émission de courant, la porte restera fermée et verrouillée même en cas de situation dégradée (absence de courant, foudre, panne, …) donc la porte restera en sûreté depuis l'extérieur tout en assurant la sortie libre.

Enfin, les informations suivantes devront être remontées au système de contrôle d'accès : porte fermée, porte verrouillée, ouverture à la clé (anomalie), abaissement de la béquille (sortie « conforme »), boucle anti-sabotage.

Axe obligatoire à 50mm au standard Français afin de faire évoluer le système sans modifier l'intégrité de la porte (y compris pour les portes coupe feu).

Pour les portes doubles vantaux, il sera prévu un verrou automatique mécanique (VAM) en remplacement de la crémone pompier afin d'éviter son utilisation abusive et une situation de porte fermée mais non verrouillée.

5.2.1.3. Version 3 points pour passage intensif

Version 3 points pour passage intensif - Serrure motorisée en entrée et sortie libre :

Afin d'assurer le bon fonctionnement du système de contrôle d'accès, il sera prévu un système de verrouillage électromécanique des portes concernées avec des niveaux de performances suivants :

Les portes seront équipées d'une serrure électromécanique assurant au minimum les mêmes fonctions qu'un verrouillage à la clé sur 3 points, a savoir une fermeture « à double tour » sur trois point médian afin d'éviter la voilure de la porte. La résistance sera supérieure à 3 000 kg.

De plus, à chaque fermeture de porte, la serrure se verrouillera mécaniquement automatiquement afin d'assurer un niveau de sûreté constant à chaque porte « claquée ».

La serrure sera paramétrable afin de simplifier la pose : 100% réversible gauche / droite / tirant / poussant, émission, bi tension 12 / 24 VDC.

Sur action du contrôle d'accès, le pêne dormant se déverrouille et permet l'ouverture de la porte par une poignée de tirage fixe (bâton de maréchal, aile de requin, …)

La sortie se fera par simple abaissement de la béquille et en une seule manœuvre conformément au code du travail et aux normes ERP en vigueur (EN179).

La porte restera fermée et verrouillée même en cas de situation dégradée (absence de courant, foudre, panne, …) donc la porte restera en sûreté depuis l'extérieur tout en assurant la sortie libre.

Enfin, les informations suivantes devront être remontées au système de contrôle d'accès : porte fermée, porte verrouillée, ouverture à la clé (anomalie), abaissement de la béquille (sortie « conforme »), boucle anti-sabotage.

Axe obligatoire à 50mm au standard Français afin de faire évoluer le système sans modifier l'intégrité de la porte (y compris pour les portes coupe feu).

Pour garantir son usage adapté aux trafics intensifs ou très intensifs, la serrure sera testée à 1 000 000 de cycles et 500 000 cycles sous charge de 5 kg (normes EN12209 et EN14846)

5.2.1.4. Version 1 point pour passage intensif

Version 1 point pour passage intensif - Serrure motorisée en entrée et sortie libre :

Afin d'assurer le bon fonctionnement du système de contrôle d'accès, il sera prévu un système de verrouillage électromécanique des portes concernées avec des niveaux de performances suivants :

Les portes seront équipées d'une serrure électromécanique assurant au minimum les mêmes fonctions qu'un verrouillage mécanique, a savoir une fermeture à la clé sur un point médian (pêne dormant) afin d'éviter la voilure de la porte. La résistance sera supérieure à 1 000 kg.

De plus, à chaque fermeture de porte, la serrure se verrouillera mécaniquement automatiquement afin d'assurer un niveau de sûreté constant à chaque porte « claquée ».

La serrure sera paramétrable afin de simplifier la pose et de diviser par 8 les lots de maintenance : 100% réversible gauche / droite / tirant / poussant, émission, bi tension 12 / 24 VDC.

Sur action du contrôle d'accès, le pêne dormant se déverrouille et permet l'ouverture de la porte par une poignée de tirage fixe (bâton de maréchal, aile de requin, …)

La sortie se fera par simple abaissement de la béquille et en une seule manœuvre conformément au code du

travail et aux normes ERP en vigueur (EN179).

La porte restera fermée et verrouillée même en cas de situation dégradée (absence de courant, foudre, panne, …) donc la porte restera en sûreté depuis l'extérieur tout en assurant la sortie libre.

Axe obligatoire à 50mm au standard Français afin de faire évoluer le système sans modifier l'intégrité de la porte (y compris pour les portes coupe feu).

Enfin, les informations suivantes devront être remontées au système de contrôle d'accès : porte fermée, porte verrouillée, ouverture à la clé (anomalie), abaissement de la béquille (sortie « conforme »), boucle anti-sabotage.

Pour garantir son usage adapté aux trafics intensifs ou très intensifs, la serrure sera testée à 1 000 000 de cycles et 500 000 cycles sous charge de 5 kg (normes EN12209 et EN14846)

5.2.2. Mode 2

MODE 2 - porte sous contrôle d'accès en sortie (version DAS), pas de contrôle d'accès côté entrée (secours à la clé)

5.2.2.1. Version 3 points

Version 3 points - Serrure à béquille contrôlée en sortie, version DAS :

Afin d'assurer le bon fonctionnement du système de contrôle d'accès, il sera prévu un système de verrouillage électromécanique des portes concernées avec des niveaux de performances suivants :

Les portes seront équipées d'une serrure électromécanique assurant au minimum les mêmes fonctions qu'un verrouillage à la clé sur 3 points, a savoir une fermeture « à double tour » sur trois point médian afin d'éviter la voilure de la porte. La résistance sera supérieure à 3 000 kg.

De plus, à chaque fermeture de porte, la serrure se verrouillera mécaniquement automatiquement afin d'assurer un niveau de sûreté constant à chaque porte « claquée ».

La serrure sera paramétrable afin de simplifier la pose : 100% réversible gauche / droite / tirant / poussant, rupture (DAS), bi tension 24 / 48 VDC

Pas de béquille côté entrée. La sortie est sous contrôlé d'accès, le verrouillage est désactivé sur déclencheur manuel en sortie d'issue de secours.

Côté intérieur, en situation dégradée ou sur asservissement à la détection incendie, la porte restera en position fermée mais sera libre d'ouverture par simple abaissement de la béquille.

Côté extérieur, il n'y aura pas de béquille mobile mais une plaque seule ou une poignée de tirage fixe, de ce fait et même en cas de situation dégradée, la porte restera fermée et verrouillée en interdisant l'accès et en assurant l'étanchéité du site.

Axe obligatoire à 50mm au standard Français afin de faire évoluer le système sans modifier l'intégrité de la porte (y compris pour les portes coupe feu).

Enfin, les informations suivantes devront être remontées au système de contrôle d'accès : porte fermée, porte verrouillée, ouverture à la clé (anomalie), abaissement de la béquille (sortie « conforme »), état du DAS, boucle anti-sabotage.

Pour les portes doubles vantaux, il sera prévu un verrou automatique mécanique (VAM) en remplacement de la crémone pompier afin d'éviter son utilisation abusive et une situation de porte fermée mais non verrouillée.

5.2.2.2. Version 1 point

Version 1 point - Serrure à béquille contrôlée et en sortie, version DAS :

Afin d'assurer le bon fonctionnement du système de contrôle d'accès, il sera prévu un système de verrouillage électromécanique des portes concernées avec des niveaux de performances suivants :

Les portes seront équipées d'une serrure électromécanique assurant au minimum les mêmes fonctions qu'un verrouillage mécanique, a savoir une fermeture à la clé sur un point médian (pêne dormant) afin d'éviter la voilure de la porte. La résistance sera supérieure à 1 000 kg.

De plus, à chaque fermeture de porte, la serrure se verrouillera mécaniquement automatiquement afin d'assurer un niveau de sûreté constant à chaque porte « claquée ».

La serrure sera paramétrable afin de simplifier la pose et de diviser par 8 les lots de maintenance : 100% réversible gauche / droite / tirant / poussant, rupture (DAS), bi tension 24 / 48 VDC

Pas de béquille côté entrée. La sortie est sous contrôlé d'accès, le verrouillage est désactivé sur déclencheur manuel en sortie d'issue de secours.

Côté intérieur, en situation dégradée ou sur asservissement à la détection incendie, la porte restera en position fermée mais sera libre d'ouverture par simple abaissement de la béquille.

Côté extérieur, il n'y aura pas de béquille mobile mais une plaque seule ou une poignée de tirage fixe, de ce fait et même en cas de situation dégradée, la porte restera fermée et verrouillée en interdisant l'accès et en assurant l'étanchéité du site.

Axe obligatoire à 50mm au standard Français afin de faire évoluer le système sans modifier l'intégrité de la porte (y compris pour les portes coupe feu).

Enfin, les informations suivantes devront être remontées au système de contrôle d'accès : porte fermée, porte verrouillée, ouverture à la clé (anomalie), abaissement de la béquille (sortie « conforme »), état du DAS, boucle anti-sabotage.

Pour les portes doubles vantaux, il sera prévu un verrou automatique mécanique (VAM) en remplacement de la crémone pompier afin d'éviter son utilisation abusive et une situation de porte fermée mais non verrouillée.

5.2.3. Mode 3

MODE 3 - porte contrôlée en entrée et en sortie (version DAS)

5.2.3.1. Version 3 points

Version 3 points - Serrure à béquille contrôlée en entrée et en sortie, version DAS :

Afin d'assurer le bon fonctionnement du système de contrôle d'accès, il sera prévu un système de verrouillage électromécanique des portes concernées avec des niveaux de performances suivants :

Les portes seront équipées d'une serrure électromécanique assurant au minimum les mêmes fonctions qu'un verrouillage à la clé sur 3 points, a savoir une fermeture « à double tour » sur trois point médian afin d'éviter la voilure de la porte. La résistance sera supérieure à 3 000 kg.

De plus, à chaque fermeture de porte, la serrure se verrouillera mécaniquement automatiquement afin d'assurer un niveau de sûreté constant à chaque porte « claquée ».

La serrure sera paramétrable afin de simplifier la pose et de diviser par 8 les lots de maintenance : 100% réversible gauche / droite / tirant / poussant, rupture (DAS), bi tension 24 / 48 VDC

L'entrée et la sortie seront contrôlées, les béquilles se libéreront sur déclencheur manuel en sortie d'issue de secours.

En situation dégradée ou sur asservissement à la détection incendie, la porte restera en position fermée mais sera libre d'accès par simple abaissement des béquilles.

Axe obligatoire à 50mm au standard Français afin de faire évoluer le système sans modifier l'intégrité de la porte (y compris pour les portes coupe feu).

Enfin, les informations suivantes devront être remontées au système de contrôle d'accès : porte fermée, porte verrouillée, ouverture à la clé (anomalie), abaissement de la béquille (sortie « conforme »), état du DAS, boucle anti-sabotage.

Pour les portes doubles vantaux, il sera prévu un verrou automatique mécanique (VAM) en remplacement de la crémone pompier afin d'éviter son utilisation abusive et une situation de porte fermée mais non verrouillée

5.2.3.2. Version 1 point

Version 1 point - Serrure à béquille contrôlée en entrée et en sortie, version DAS :

Afin d'assurer le bon fonctionnement du système de contrôle d'accès, il sera prévu un système de verrouillage électromécanique des portes concernées avec des niveaux de performances suivants :

Les portes seront équipées d'une serrure électromécanique assurant au minimum les mêmes fonctions qu'un verrouillage mécanique, a savoir une fermeture à la clé sur un point médian (pêne dormant) afin d'éviter la voilure de la porte. La résistance sera supérieure à 1 000 kg.

De plus, à chaque fermeture de porte, la serrure se verrouillera mécaniquement automatiquement afin d'assurer un niveau de sûreté constant à chaque porte « claquée ».

La serrure sera paramétrable afin de simplifier la pose et de diviser par 8 les lots de maintenance : 100 % réversible gauche / droite / tirant / poussant, rupture (DAS), bi tension 24 / 48 VDC

L'entrée et la sortie seront contrôlées, les béquilles se libéreront sur déclencheur manuel en sortie d'issue de secours.

En situation dégradée ou sur asservissement à la détection incendie, la porte restera en position fermée mais sera libre d'accès par simple abaissement des béquilles.

Axe obligatoire à 50mm au standard Français afin de faire évoluer le système sans modifier l'intégrité de la porte (y compris pour les portes coupe feu).

Enfin, les informations suivantes devront être remontées au système de contrôle d'accès : porte fermée, porte verrouillée, ouverture à la clé (anomalie), abaissement de la béquille (sortie « conforme »), état du DAS, boucle anti-sabotage.

Pour les portes doubles vantaux, il sera prévu un verrou automatique mécanique (VAM) en remplacement de la crémone pompier afin d'éviter son utilisation abusive et une situation de porte fermée mais non verrouillée.

5.3. Ventouses électromagnétiques

Ce type d'équipement peut-être mis en place sur des portes ne nécessitant pas un niveau de sûreté accrue, mais plutôt un filtrage de passage.

Les ventouses électromagnétiques doivent être alimentées en **24V/48V** DC par des alimentations indépendantes de l'alimentation des lecteurs. Elles sont secourues par batteries.

Ces ventouses peuvent être installées principalement sur des portes existantes. Généralement ces ventouses sont installées en applique, sur les dormants de porte. Cela ne nécessite pas de modification de la porte.

Les trois systèmes utilisés sont les ventouses électromagnétiques, les poignées simple-ventouse et les

bandeaux double-ventouses. La simple ventouse est généralement installée en haut d'une porte. Elle peut être associée à une gâche électromagnétique, pour une double sécurité et éviter une déformation de la porte.

Les poignées simple-ventouse sont privilégiés par rapport aux ventouses individuelles. Elles ont un impact moins important sur la déformation de la porte, car elles sont installées au niveau de la béquille. Les poignées doubles ventouses sont installées, en applique, principalement sur les portes donnant sur l'extérieur, la force du bandeau doit être de 2 fois 300 kg.

L'alimentation de la ventouse doit pouvoir être désactivée au moyen de déclencheurs manuels (DMD). Une attention particulière sera apportée aux portes donnant accès à des locaux borgnes. Un moyen de déverrouillage manuel devra également être installé à l'extérieur du local, non accessible au public (poste de garde, chef de poste, accueil,…)

Caractéristique à prendre en compte : en cas de coupure de l'alimentation de la ventouse, la porte reste déverrouillée. Dans certains cas, ces ventouses peuvent être associées à une serrure mécanique équipé d'un canon européen, pour fermeture en cas de dysfonctionnement du système.

6. DÉVERROUILLAGE DES PORTES

6.1. Généralités

La mise en œuvre d'un contrôle d'accès ne doit pas perturber, bloquer, neutraliser les dispositifs de libéralisation d'ouvrants installés au titre de la sécurité incendie.

Si le cas se présente, le titulaire devra obligatoirement en aviser l'administration qui dépêchera le service ou le coordonnateur en charge du volet « sécurité incendie ».

En cas d'incendie ou d'urgence, les portes des issues de secours seront déverrouillées, sauf avis contraire dans le document descriptif du projet, selon le cas, par :

- déclenchement manuel DMD (Art C046 règlement ERP),

- déverrouillage général déclenché par la Détection Incendie du Bâtiment (raccordement et câblage à prévoir dans la prestation),

- l'UGCIS (Unité de Gestion Centralisée des Issues de Secours),

- clé de secours en cas de coupure de courant.

Précision importante :

La requête d'une dérogation auprès du service départemental d'incendie et de secours permettra de valider les accès et les issues de secours ne pouvant pas être ouverts localement, mais commandés depuis le local du chef de poste et reliés au SSI.

Les portes correspondant à ces accès en entrée et sortie contrôlées ne seront pas ouvertes lors d'une détection d'incendie.

Le chef de poste détient alors une clé de secours permettant d'ouvrir ces portes en cas de coupure électrique.

Extrait du Référentiel Immobilier du Ministère de l'Intérieur :

La porte d'entrée à la zone de sûreté est commandée uniquement depuis le local du chef de poste (au moyen du système de contrôle d'accès général). Des visiophones permettent aux agents de solliciter l'entrée et la sortie.

Elle est équipée d'un système de verrouillage électrique à pêne entrant dans une gâche renforcée sur le dormant.

Contrairement à ce qu'imposeraient les consignes élémentaires de sécurité incendie, les accès et les issues de secours seront clos dans la zone de sûreté.

Ils sont commandés depuis le local du chef de poste.

Le chef de poste détient une clé de secours permettant d'ouvrir toutes les portes en cas de dysfonctionnement.

6.2. Déclencheur Manuel de déverrouillage (DMD) ou (BBG)

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

Le boîtier sera muni d'un capot avec scellé. Pour manœuvrer le boîtier, il sera obligatoire de casser le scellé. Le service du ministère de l'Intérieur disposera des outils pour remettre en place les scellés sur les boîtiers verts ouverts.

Boîtier en saillie à membrane souple déformable avec contact de signalisation d'état repris individuellement sur l'installation. Boîtier plombé de dé-condamnation et possibilité de mise en œuvre en intérieur comme en extérieur.

- Réarmement à clé du dispositif après activation,
- Buzzer intégré, voyant d'état,
- Respect de la (réglementation CO 46), Norme NFS 61 937.

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

6.3. Bouton d'ouverture de porte (BOP)

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

Les boutons de commande de sortie seront posés à 1,20 m du sol fini. Ils peuvent également être intégrés à la serrure motorisée.

7. GESTION DES ACCÈS

7.1. Configuration des accès

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

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

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

- Activation des béquilles,
- Activation du cylindre,
- Anomalie serrure,
- Boucle anti-sabotage,
- État du DAS (verrouillé/déverrouillé),
- Pêne sorti, Pêne rentré, serrure pilotée mécaniquement,
- Porte ouverte/ Porte fermée/ Porte ouverte trop longtemps,
- Position de porte (contre pêne rentré).

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

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

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

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

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

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

7.2. Gestion des couloirs rapides à unicité de passage (CRUP)

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

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

- Alarmes techniques de fonctionnement,
- Confirmation de passage,
- Forçage,
- Fraude à l'unicité de passage,
- Intrusion dans la zone de passage sans badgeage.

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

- Ouverture/fermeture,
- Ouverture Permanente/Fermeture Permanente.

La solution devra permettre, notamment, de gérer tous les états des dispositifs de passages

- Passage Ouvert/ Passage Fermé.

En conséquence, sur certains couloirs rapides, il sera possible de faire une demande d'ouverture après

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

La solution devra permettre de paramétrer les propriétés suivantes :

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

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

7.3. Asservissement des accès

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

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

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

- par identification à certaines périodes,
- par demande d'E/S à certaines périodes,
- par demande d'E/S validée par opérateur après identification durant certaines périodes,
- par demande d'E/S validée par opérateur après identification d'un type de profil durant certaines périodes.
- et non contrôlé à d'autres périodes (ouverture automatique ou non).

NB : La détection d'un type de profil devra être un événement natif du système.

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

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

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

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

7.4. Anti-retour

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

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

- L'événement est archivé,

- L'événement est archivé mais l'accès est refusé.

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

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

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

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

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

7.5. Gestion du parking

7.5.1. Le filtrage efficace des véhicules

La contrainte du nombre maximal de places allouées dans un parking impose la mise en œuvre de règles adaptées.

Un niveau supplémentaire de contrôle du type double passage géographique interdit permettra de vérifier le sens de passage (deux entrées de suite ne seront pas autorisées).

Dans le but d'éviter la fraude, deux fonctions complémentaires sont demandées :

- La fonction double passage géographique interdit qui prendra en compte le passage effectif du véhicule : le véhicule dont le conducteur vient de badger doit effectivement avoir franchi l'accès pour la prise en compte : "véhicule entré",

- Tout badge présenté ayant donné un passage effectif avec franchissement ne pourra plus obtenir d'autorisation à cet accès pendant une temporisation paramétrable.

7.5.2. Le comptage des véhicules

Le comptage du parking (nécessitant un seul lecteur en entrée) sera effectué :

- En entrée : badgeage d'un conducteur autorisé,

- En sortie : passage simple du véhicule sans badgeage du conducteur (avec confirmation de passage effectif).

7.6. Gestion des équipements de détection d'intrusion

La solution peut intégrer les équipements de détection d'intrusion via des entrées/sorties de type ToR, des liaisons BUS ou IP.

Les systèmes devront pouvoir être armés :

- En permanence,

- Certains jours à certaines périodes,

- Suivant l'existence de détection de certains événements : valeur de comptage à zéro,

- Sur action automatique ou utilisateur.

Les systèmes devront pouvoir être désarmés :

- Certains jours à certaines périodes,

- Suivant l'existence de détection de certains événements : valeur de comptage non nulle,

- Sur action automatique ou utilisateur.

Le système pour les locaux à sortie libre doit pouvoir détecter la gestion de l'utilisation du bouton de sortie ou de la béquille pour pouvoir armer un détecteur.

Le système pour les locaux à entrer dont l'entrée est contrôlée doit pouvoir désarmer les zones après une ouverture validée par le contrôle d'accès.

7.7. Gestion des équipements d'anti-agression

La solution peut intégrer des équipements permettant la notification d'une agression via des entrées/sorties de type ToR.

Principalement centralisés en zone guichet et bureau d'accueil ils permettront une notification d'alarme prioritaire sur les systèmes.

Ces alarmes permettront le déclenchement automatique de scénario type mentionnant la zone, activant la visualisation de la caméra mitoyenne avec pré-post enregistrement. C'est une alarme de niveau 1.

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

- Le système permet d'afficher une procédure à suivre en « alarme,

- Le système permet de gérer des alarmes notifiées par l'utilisateur,

- Le système permet une gestion des alarmes en cascades.

Le système ne sera pas relié à une messagerie. La possibilité existera néanmoins d'émettre des alarmes par

Email.

7.8. Maquette

Dans le cas d’un système complexe ou inconnu de nos services, le but est de réaliser, chez le constructeur de la solution proposée par l'attributaire du présent lot, la cérémonie des clés validant la conformité de cette solution au présent CCTP. Cette maquette sera exigée et permettra la mise en œuvre des fonctionnalités exigées par la Carte Agent Ministérielle.

Lors de cette cérémonie, seront réalisées les opérations listées ci-dessous :

- L'encodage d’une carte Agent,
- L'encodage d’une carte blanche (ou carte visiteur),
- La configuration des lecteurs de badges,
- L’enrôlement des deux types de carte,
- L'octroi de droits d'accès au porteur de carte,
- La vérification du bon fonctionnement.

A ce titre, le titulaire déploiera en son agence le matériel et logiciel nécessaires :

- Serveur avec logiciel de contrôle et solution d’encodage-enrôlement,
- Unité de traitement logique,
- Lecteur-encodeur de badges prévu dans la solution,
- Documentation support relative à la solution proposée,
- Cartes visiteurs au format Desfire EV1.

L’administration fournira les données indispensables à la réalisation des opérations :

- La clé applicative maître,
- Le numéro de l’AID,
- Les nouvelles clés de substitution.