

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

ANNEXE 2 Principes concernant le système de contrôle d'accès

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

CCTP SÛRETÉ – DESCRIPTIF DU PROJET

Table des matières

1. Généralités.....	5
1.1. Définitions.....	5
1.2. Spécifications ANSSI.....	5
1.3. Certificat de sécurité de premier niveau ANSSI.....	9
1.3.1. Exigence de certification.....	9
1.3.2. Consistance de la certification.....	10
1.3.3. Solutions de contrôle d'accès certifiées.....	10
1.4. Qualification ANSSI.....	11
1.4.1. Consistance de la qualification.....	11
1.4.2. Niveaux de qualification.....	12
1.4.3. Solutions de contrôle d'accès qualifiées.....	12
1.5. Autres règles de sécurité.....	12
1.6. Intégration de l'antivirus.....	13
1.7. Synchronisation de l'heure.....	13
1.8. Logiciels et firmwares.....	13
1.9. Journalisation.....	13
1.10. Architecture.....	14
2. Architecture du système.....	14
2.1. Généralités.....	14
2.1.1. Système « Mono-site ».....	15
2.1.2. Système « Multi-sites ».....	15
2.2. Serveurs.....	15
2.2.1. Configuration matérielle des serveurs.....	15
2.2.2. Configuration logicielle des serveurs.....	16
2.3. Les stations.....	16
2.3.1. Configuration matérielle des stations.....	16
2.3.2. Configuration logicielle des stations.....	16
2.3.3. Poste de gestion des badges.....	16
2.3.4. Poste de gestion du contrôle d'accès.....	17
2.3.5. Poste de sécurité.....	17
2.4. Ecrans de grande diagonale.....	17
2.5. Prestation optionnelle.....	18
3. Unité de traitement local (UTL).....	18
3.1. Généralités.....	18
3.2. Règles de l'art.....	19
3.3. Installation physique.....	19

3.4. Raccordement des périphériques.....	20
3.5. Raccordement logique.....	20
3.6. Accès au réseau local « Sûreté ».....	20
3.7. Prestation électrique.....	20
4. Périphériques de commande des accès.....	21
4.1. Lecteur de badges (LB) et support sans contact.....	21
4.1.1. Caractéristiques physiques.....	21
4.1.2. Caractéristiques normatives de la Carte Agent JCOP3.....	22
4.1.3. Caractéristiques logiques.....	28
4.1.4. Renouvellement des clés.....	29
4.2. Support biométrique (empreinte).....	29
4.3. Contrôle des accès par visiophonie.....	30
4.3.1. Caractéristiques générales.....	30
4.3.2. Intégration à la solution vidéo.....	30
5. Équipements de portes.....	31
5.1. Généralités.....	31
5.2. Caractéristiques des serrures électromécaniques.....	31
5.2.1. Mode 1.....	32
5.2.1.1. Version 3 points	32
5.2.1.2. Version 1 point	32
5.2.1.3. Version 3 points pour passage intensif.....	33
5.2.1.4. Version 1 point pour passage intensif	34
5.2.2. Mode 2	34
5.2.2.1. Version 3 points	34
5.2.2.2. Version 1 point.....	35
5.2.3. Mode 3.....	36
5.2.3.1. Version 3 points.....	36
5.2.3.2. Version 1 point	36
5.3. Ventouses électromagnétiques.....	37
6. Déverrouillage des portes.....	37
6.1. Généralités.....	37
6.2. Déclencheur Manuel de déverrouillage (DMD) ou (BBG).....	38
6.3. Bouton d'ouverture de porte (BOP).....	39
7. Gestion des accès.....	39
7.1. Configuration des accès.....	39
7.2. Gestion des couloirs rapides à unicité de passage (CRUP).....	40
7.3. Asservissement des accès.....	41

7.4. Anti-retour.....	41
7.5. Gestion du parking.....	42
7.5.1. Le filtrage efficace des véhicules.....	42
7.5.2. Le comptage des véhicules.....	42
7.6. Gestion des équipements de détection d'intrusion.....	42
7.7. Gestion des équipements d'anti-agression.....	43
7.8. Maquette.....	43

1. GÉNÉRALITÉS

Le système sera conforme au référentiel APSAD D83 ou équivalent (Contrôle d'accès – Document technique pour la conception et l'installation).

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 :

- d'un serveur de gestion du système ;
- d'une ou plusieurs Unités de Traitement Local (UTL) intégrant des modules d'extension dans un local sécurisé, -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 éprouvés avec la carte agent ministérielle: 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). Le système de contrôle d'accès reposera uniquement sur l'architecture N°1 décrite dans ce document.

Guide ANSSI du 10 octobre 2023:

RECOMMANDATIONS SUR LA SÉCURISATION DES SYSTÈMES DE CONTRÔLE D'ACCÈS PHYSIQUE ET DE VIDÉOPROTECTION

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

- Ses recommandations suivantes :

R35 Éviter l'usage de badges virtuels sur ordiphone

R36 Protéger les accès aux têtes de lecture

R37 Protéger les flux d'authentification du porteur entre le dispositif associé à la tête de lecture et l'UTL

R38 Protéger l'accès physique aux UTL

R39 Contrôler minutieusement les interventions effectuées sur les UTL

R40 Chiffrer et authentifier les flux émis et reçus par les UTL

R41 Implémenter en priorité la configuration type n°1

R42 Sécuriser le centre de gestion des contrôles d'accès (GAC)

- Ses exigences qui sont spécifiées par niveau de résistance aux attaques logiques. Ces niveaux de résistance (notés de L1 à L3) correspondent aux niveaux de sûreté définis de manière commune avec le CNPP.

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

Les mesures de niveau **L1, L2 et L3** pour les **sites sensibles**.

La correspondance entre le niveau de sûreté et la résistance aux attaques logiques est détaillée dans le tableau D.1 qui indique également les méthodes d'authentification et les technologies de badge associées qui sont conseillées pour chaque niveau de résistance logique.

Niveaux de sûreté	Niveaux de résistance aux attaques logiques	Méthode d'authentification	Technologies
I	-	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.
II	L1	Authentification reposant sur une clé commune; Algorithmes et protocoles d'authentification connus et conformes au RGS (AES ⁴³).	Cartes ISO14443, authentification à cryptographie symétrique.
III	L2	Authentification du badge reposant sur une clé dérivée d'une clé maîtresse ou sur une bi-clé asymétrique; Algorithmes et protocoles d'authentification connus et conformes au RGS (AES ⁴³).	Cartes ISO14443, authentification à cryptographie symétrique ou asymétrique.
IV	L3	Authentification du badge reposant sur une clé dérivée d'une clé maîtresse ou sur une bi-clé asymétrique; Algorithmes et protocoles d'authentification connus et conformes au RGS (AES ⁴³); Authentification du porteur par un second facteur (information mémorisée ou élément biométrique).	Cartes ISO14443, authentification à cryptographie symétrique ou asymétrique; Saisie d'un code mémorisé ou d'un élément biométrique.

TABLE D.1 – Correspondance entre niveau de sûreté et niveau de résistance aux attaques logiques

A noter : les exigences indiquées sont complémentaires et cumulatives.

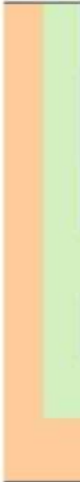
Pour atteindre un niveau de sécurité de **niveau L1**, il faut appliquer toutes les exigences du niveau **L1**.

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.

Spécifications, extraites de ce guide, à respecter pour :

- Les têtes de lecture

Résistance aux attaques logiques		Spécification
	L1	Les têtes de lecture doivent fonctionner avec une distance maximale de 5 cm entre le lecteur et le badge.
	L1	Aucun droit d'accès ne doit être déporté dans la tête de lecture.
	L1	Les têtes de lecture sont équipées d'un système de détection d'intrusion et d'arrachage.
	L2	Les têtes de lecture doivent avoir démontré un excellent niveau de protection contre les fraudes. Elles doivent avoir fait l'objet d'une certification de sécurité de premier niveau (CSPN).
	L2	Les têtes de lecture doivent comporter une signalisation visuelle d'accès autorisé et d'accès refusé, et doivent activer une signalisation sonore en cas de porte maintenue ouverte ou de porte forcée.
	L2	Les têtes de lecture ne doivent pouvoir être programmées que via les UTL, et en aucun cas au moyen d'une carte de maintenance simplement présentée à la tête de lecture pour la reprogrammer.
	L3	Les têtes de lecture doivent pouvoir admettre un clavier d'authentification. Ce clavier doit être doté d'une fonction « accès sous contraintes ».

L'exigence relative à la Certification de Sécurité de Premier Niveau (CSPN) de l'ANSSI dans laquelle sont ciblés les lecteurs de badges sera rappelée dans le « descriptif du projet ».

- Les UTL (Unité de Traitement Local)

Résistance aux attaques logiques	Spécification
L1	Les UTL analysent les droits du badge et délivrent l'ordre d'ouverture à la gâche ou à l'actionneur.
L1	Les UTL assurent la datation des événements et des alarmes.
L1	Les UTL transmettent les informations liées à la transaction, au serveur de gestion du système (GAC, UTS, ou autre équipement).
L1	Les UTL doivent émettre, vers le serveur de gestion du système, des informations sur les anomalies de fonctionnement qui leur sont propres et sur les anomalies des équipements qui leur sont associés.
L1	Les UTL s'auto-surveillent en générant des défauts internes. Ces alarmes sont 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 leur sont associés.
L1	La sécurisation des UTL doit 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 peuvent 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 la durée de coupure maximum retenue, 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 possèdent une mémoire (contenant les instructions du traitement) type EPROM ⁴⁴ ou RAM ⁴⁵ sauvegardée par batterie (24 heures minimum).
L2	Les UTL doivent être capables de gérer « l'anti pass-back » ⁴⁶ des lecteurs qui lui sont associés.
L3	Pas d'exigence spécifique pour ce niveau.

44. Erasable Programmable Read Only Memory.

45. Random Access Memory.

46. Fonction qui évite qu'une personne entre deux fois dans une zone sans en être sortie au préalable.

- Les réseaux et communications

Résistance aux attaques logiques	Spécification
L1	Les cheminements de câbles sont mis en place à l'intérieur des zones contrôlées.
L1	Les liaisons de communication entre les moyens physiques d'ouverture et l'unité de traitement local sont des liaisons dédiées au système de sécurité.
L1	Les liaisons filaires sont surveillées de manière à garantir qu'aucune tentative de fraude ne puisse être réalisée.
L1	La perte d'informations au niveau des liaisons doit être signalée et traitée comme une alarme.
L1	La fibre optique doit être privilégiée pour les liaisons entre bâtiments.
L2	La transmission des informations du système de contrôle d'accès se fait sur un réseau logique dédié à ce système.
L2	Les protocoles de communication utilisés (algorithmes de chiffrement inclus) doivent être décrits, et particulièrement les principes de sécurisation et de vérification des échanges.
L2	La communication entre le badge, la tête de lecture et l'UTL doit être chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS [19]).
L2	La communication entre l'UTL et le serveur de gestion du système doit être chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS [19]).
L3	Les câbles servant pour la transmission des informations du système de contrôle d'accès sont des câbles dédiés à ce système.
L3	Les réseaux définis pour le système de contrôle d'accès sont totalement indépendants des réseaux du site autant pour les câbles que pour les équipements électroniques ou informatiques associés.
L3	S'ils venaient à faire l'objet de vulnérabilités publiées, permettant de compromettre leur efficacité, les protocoles et algorithmes utilisés doivent pouvoir être remplacés par d'autres protocoles ou algorithmes ne faisant pas l'objet de vulnérabilités publiées et permettant de maintenir le niveau de sécurité des échanges.

À 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. Certificat de sécurité de premier niveau ANSSI

1.3.1. Exigence de certification

La Politique Générale de la Sécurité Numérique (PGSN) du ministère de l'Intérieur du 28.01.2022 stipule que :

- « Tous les « systèmes d'information de sûreté » entrent également dans le périmètre de la présente PGSN-MI : systèmes de contrôle d'accès physique et de détection intrusion, [...], systèmes de vidéosurveillance, etc. ».
- « L'accès aux zones internes (autorisées uniquement au personnel du centre informatique ou aux visiteurs accompagnés) et restreintes (autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) doit reposer sur un **dispositif de contrôle d'accès physique. Ce dispositif doit s'appuyer sur des produits qualifiés**, lorsqu'ils sont disponibles, et bénéficier d'un maintien en condition de sécurité rigoureux. ».

- « Un système de gestion de la sécurité du SI de sûreté (s'inspirant de la norme ISO 27001) assure le maintien en condition de sécurité. **L'emploi de produits labellisés, quand ils existent ou ceux recommandés par l'ANSSI, est fortement recommandé.** ».
- « **Le Titulaire veille à privilégier les solutions logicielles ou matérielles labellisées (qualifiées ou certifiées) par l'ANSSI** sur les **systèmes d'information qu'il serait amené, dans le cadre du marché, à mettre en œuvre pour ses propres besoins ou concevoir pour les besoins de l'Acheteur.** Si le produit final vise une qualification après la notification du marché, il est fortement recommandé que le jalon J0 du processus de qualification soit franchi préalablement. ».

En conséquence des recommandations et exigences de l'ANSSI ainsi que du cadre édicté par la PGSN du ministère de l'Intérieur, **seuls** les produits de fabricants bénéficiant au minimum d'un **certificat de sécurité de premier niveau (CSPN) de l'ANSSI, sont acceptés** pour les installations de systèmes de contrôle d'accès des sites du ministère de l'Intérieur. Il appartient à l'installateur de vérifier que le fabricant de la solution de contrôle d'accès, qu'il propose dans son offre, est certifié par l'ANSSI.

1.3.2. Consistance de la certification

La certification de sécurité de premier niveau permet d'attester que le produit a subi avec succès une évaluation de sécurité par un centre d'évaluation agréé par un CESTI, l'évaluation ayant pour caractéristiques principales :

- d'analyser la conformité du produit à ses spécifications de sécurité ;
- de mesurer l'efficacité des fonctions de sécurité ;
- d'être conduite en temps et en ressources humaines (charge) contraintes.

1.3.3. Solutions de contrôle d'accès certifiées

ATTENTION :

Le Certificat de Sécurité de Premier Niveau a une validité de 3 ans.

Certains constructeurs étaient certifiés et sont en cours de renouvellement de leur certificat, donc ne le sont plus aujourd'hui. Nous admettons donc que leur matériel soit toujours valable à condition que ces constructeurs nous apportent la preuve écrite de leur démarche de certification en cours.

Certains constructeurs ne fabriquent que des lecteurs de badges ou que des UTL. D'autres produisent le lecteur de badges, l'UTL et la solution logicielle. Il faut analyser chaque solution dans sa globalité.

Vous trouverez sur le site de l'ANSSI la liste des solutions certifiées actuellement (certification en cours de validité).

<https://cyber.gouv.fr/produits-certifies>

En date du 23 février 2023, les constructeurs titulaires d'un Certificat de Sécurité de Premier Niveau sont les suivants (la DSIC a testé avec succès la mise en œuvre d'installations des constructeurs en vert et est en cours de validation de ceux en orange) :

Commanditaire	Produit certifié	Référence certification	Date certification	Lecteur	UTL	GAC (Gestion des Accès Contrôlés)	Testé DSIC
SYNCHRONIC	UTL pour XSecur'-Evo Version 1.1	2022/08	06/07/2022	STid	x		x
TIL TECHNOLOGIES	MICRO-SESAME Version M.S. V2021.1.0.11539, TILLYS-CUBE V5.1.2.8556, MLP2 V5.0.0.1757	2022/04	26/04/2022	STid	x		x
NEDAP FRANCE SAS	Nedap AEOS Version 2021.2	2022/05	08/04/2022	NEDAP	x		x
ELSYLOG	COSMOS (UTL SYRIUS 2P2L-EXT version 1661z, UTL ORION 4P-8L-EXT version 1661z) Version 4.6.0.96	2021/33	14/01/2022	STid	x		
OMNITECH SECURITY	UTL ULS PoE Secured UTL ULS PoE Secured	2021/06	16/03/2021	Omnitech	x		x
Secure systems & services	Evolynx-ITL iPerflex V8.2.1a4	2020-39	25/11/2020	STid	x		x
ARD SAS	Ensemble UTL et lecteurs de badges pour ARD Access Haute Sécurité, Version 2.1.1	2020/21	09/06/2020	ARD	x		x
ELSYLOG	SYRIUS-2P2L-IP-EXT Version 1660f	2020/03	09/06/2020	STid	x		

Et ceux certifiés dans le passé (certification périmée en date) : <https://cyber.gouv.fr/produits-certifies-archives>

Commanditaire	Produit certifié	Référence certification	Date certification	Lecteur	UTL	Logiciel	Testé DSIC
Gunnebo Electronic Security	Gunnebo SMI Version CSPN_01-02	2018/12	15/10/2018	ProStyl	x	x	x
Synchronic	Xsecur' version UG V13-20-00 / UTP-Sec V2-10-00 / TLS V2-20-00	2018/20	01/10/2018	STid	x		x
GENETEC Inc.	Synergis Cloud Link version HW : SY-CLOUDLINK-312-CSPN / SW : 10.7.411.8 (2018-04-18)	2018/21	25/09/2018	HID STid	x		
Systèmes et Technologies Identification (STid)	Lecteur RFID LXS W33-E/PH5-7AD Version 1.1	2013/08	24/10/2013	x			x

1.4. Qualification ANSSI

1.4.1. Consistance de la qualification

La qualification est la **recommandation par l'État français** de produits ou services de cybersécurité éprouvés et approuvés par l'ANSSI.

Elle atteste de leur conformité aux exigences réglementaires, techniques et de sécurité promues par l'ANSSI en apportant une garantie de robustesse du produit et de compétence du prestataire de service, et d'engagement du fournisseur de solutions à respecter des critères de confiance :

L'évaluation de robustesse d'un produit et de la compétence d'un prestataire

Pour les produits, l'évaluation de la robustesse consiste à éprouver leur capacité à résister à des attaques informatiques selon un contexte d'emploi et un niveau de menace définis.

Pour les services, l'évaluation de la compétence d'un prestataire de services permet de démontrer son

aptitude à identifier et maîtriser les menaces et risques pour satisfaire les exigences inscrites dans des référentiels métiers.

L'évaluation de la confiance

Pour les produits comme pour les services, la confiance est évaluée dans le cadre du processus de qualification et de son suivi. L'évaluation de la confiance consiste à éprouver la capacité du fournisseur à respecter sur le long terme un ensemble d'engagements pris auprès de l'ANSSI tels que :

- pour les produits : confidentialité et protection des données confiées par l'utilisateur de la solution, correction des failles et vulnérabilités, etc.
- pour les services : maintien des compétences.

1.4.2. Niveaux de qualification

Pour les produits, il existe trois niveaux de qualification :

- **Le niveau élémentaire :**
Le produit doit résister à un attaquant disposant de compétences techniques basiques et de ressources limitées.
- **Le niveau standard :**
Le produit doit résister à un attaquant disposant de compétences techniques avancées et de ressources importantes.
- **Le niveau renforcé :**
Le produit doit résister à un attaquant disposant de compétences techniques sophistiquées et de ressources illimitées ainsi que d'un soutien étatique et/ou de groupes criminels.

1.4.3. Solutions de contrôle d'accès qualifiées

Vous trouverez sur le site de l'ANSSI la liste des produits qualifiés actuellement (certification en cours de validité) : <https://www.ssi.gouv.fr/liste-produits-et-services-qualifies>

Au 1^{er} février 2023 :

Commanditaire	Produit qualifié	Référence qualification	Date de début / fin de qualification	Niveau	Logiciel	Testé DSIC
SYNCHRONIC	UTL pour XSecur'-Evo Version 1.1	2593	13-12-2022 / 13-12-2025	élémentaire	x	x

1.5. 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.

1.6. 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 ministériel en vigueur. Celui-ci est en mode géré. L'agent ainsi que le logiciel de l'antivirus ministériel en vigueur seront fournis par l'administration.

1.7. 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.

1.8. Logiciels et firmwares

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

1.9. Journalisation

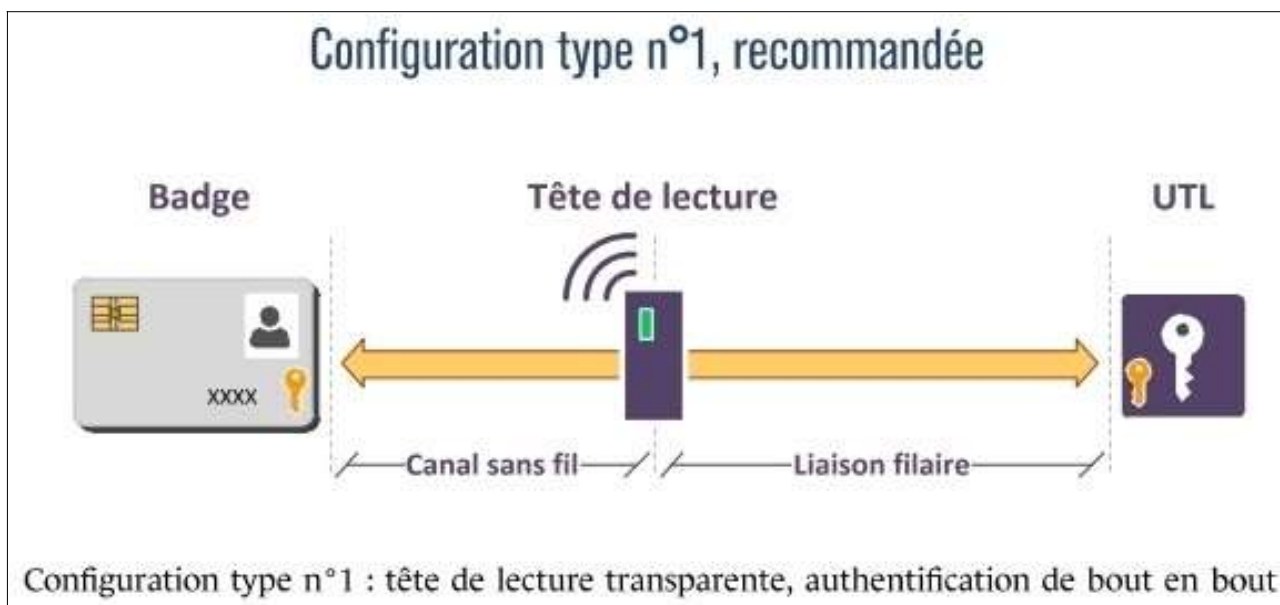
Le système doit gérer la journalisation des événements. La journalisation des événements est un processus automatique qui a pour but d'enregistrer les accès des utilisateurs ainsi que les opérations menées sur un système en identifiant l'auteur, la date, l'heure ainsi que la nature de l'opération.

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.

1.10. Architecture

Le système de contrôle d'accès ne reposera **que** sur la configuration type n°1 décrite dans le guide de l'ANSSI : 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'appliquatif 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 serveur assure une communication permanente avec les unités de traitement local (UTL).
- Le **mode dégradé** où certaines UTL fonctionnent en mode autonome : 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.

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.

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 multi ports 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 sauvegardés.

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 pourra prévoir 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 de la dernière version du système d'exploitation compatible avec la solution en 64 bits. Le système d'exploitation doit être à jour des derniers correctifs de sécurité. La base de données sera une base MS SQL compatible avec la version logicielle du serveur. Les versions devront être évolutives dans le temps.

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 caractéristiques minimales des stations de gestion pour une utilisation courante de type poste client ou monoposte sont :

- CPU : benchmark 8000 points type i3 – 10100 ou supérieur
- Mémoire : 4Go minimum
- Espace disque disponible : 500 Go minimum
- Système d'exploitation 64 bits Dernière version Windows Entreprise compatible avec la solution et maintenable à jour
- Ecran 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.

En cas d'affichages multiples, le soumissionnaire fournira des écrans équipés de connectiques identiques et ayant des capacités et des résolutions identiques.

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 dernier système d'exploitation Entreprise 64 bits compatible avec la solution et maintenable à jour. 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, permettra l'encodage puis l'enrôlement des badges blancs, des

CAM (Cartes Agents Ministérielles) après le pré-encodage sur un applicatif du Ministère par un autre type d'utilisateur.

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 minimums :

- Diagonale de 43 pouces minimum,
- Résolution de dalle de 1920 × 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, 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 le besoin exprimé, 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.

La liaison UTL-lecteurs est en RS-485, chiffrée de bout en bout sans adjonction d'interface entre le module de porte d'UTL et le lecteur.

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 au moins 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 :

- une pour l'alimentation de l'ensemble de la partie électronique (cartes UTL, cartes d'extension et lecteurs),
- l'autre pour la 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. À 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, 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.

Remarque : Le titulaire fournira à l'administration la liste exhaustive de tous les ports et flux nécessaires au bon fonctionnement de la solution. Il devra également se rapprocher du constructeur afin de disposer de la dernière liste à jour.

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 un bus RS-485 chiffré.

Les lecteurs RFID devront être protégés contre l'arrachement. Ils doivent disposer de LED (Vert, Rouge) permettant une signalisation visuelle et d'un biper 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 normatives de la Carte Agent JCOP3

Identification du produit de l'IN GROUP :

ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD
qualifiée sur le composant P6022J VB (version v7b4).

La carte agent de la deuxième génération est une carte JCOP3 (JAVA CARD OPEN PLATFORM 3).

La carte comporte plusieurs applets (CHIPDOC3, AS ECC, DESFIRE EV1). La carte permet des communications en sans contact et en contacts.

Les tests électriques, mécaniques, d'environnement et d'impression ont été réalisés par l'IN GROUP LABORATOIRE.

La carte a été vérifiée en conformité normative par un laboratoire d'essais indépendant et accrédité COFRAC ISO 17025.

Les normes vérifiées sont :

ISO 7816 (1-2-3-4-6-8-9-11-15) (classe A, B et C)

ISO14443-A, ISO10373-6 (rétro-modulations partie haute et partie basse sur l'amplitude, tests de la résonance et du coefficient de surtension, bande passante et PPS des vitesses de communication)

Les normes suivantes ont été qualifiées par des plans de tests associés :

ISO/IEC 9796-2, ISO/IEC 9797-1 -2, ISO/IEC 10116, FIPS PUB 180-1 ISO/IEC 9564-1,

Les normes suivantes ont été qualifiées par des résultats de plans de tests mécaniques associés :

ISO10373-1,-2,-3, ISO/CEI 7810

Les normes suivantes ont été qualifiées par les résultats des plans de tests MRZ associés :

ICAO Doc 9303 part 5, part 6

Les normes suivantes ont été qualifiées par les résultats des plans de tests d'environnement associés :

ISO/CEI 21789-1 : 201, ISO/CEI 21789-2 : 2011,

Les normes suivantes ont été acquises par conception :

ISO 7811 (ISO1, ISO2, ISO3)

ISO/IEC 7812 -1

Les normes sur la cryptographie RSA et signatures sécurisées ont été acquises par vérification avec des vecteurs de tests spécifiques aux normes citées :

PKCS#1 V2.1

PKCS#15

prEN 14890-1 -2

prEN 15890 -1 -2 -3

NIST 800_38B

Spécifications documentaires associées à la conception de la carte agent

Les spécifications suivantes ont été utilisées pour le développement des services JCOP3 :

- Service AS ECC (applet) :
 - EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS AS ECC identification Authentification Signature V2 révision A02
 - Profil de personnalisation P145 SPT006 (IN GROUPE)
 - Spécifications de gestion des clés P145 SPT 004 (IN GROUPE)
 - Spécifications fonctionnelles P145 SPT 001 (IN GROUPE)
- Service DESFIRE EV1 (applet): Base MF3ICD81 de la société NXP
- Services Authentification, Signature, confidentialité JCOP3 : ChipDoc 3.0 de la société NXP

Conformité aux exigences réglementaires, techniques et de sécurité

Rapport de certification et qualification:

ANSSI-CC-2020/48 ChipDoc V2 on JCOP 3 P60 in SSCD configuration (Version v7b4_2)

DECISION DE QUALIFICATION AU NIVEAU RENFORCE : N°1830/ANSII/SDE

Rapport d'évaluation critères communs:

« ChipDoc V2 on JCOP3 P60 » en version v7b4_2 sur composant P6022 Y VB

Certificate number : CC-20-98209 TÜV Rheinland Nederland B.V.

Conformité aux profils de protection :

BSI-CC-PP-0059-2009-MA-01 v2.0.1

BSI-CC-PP-0075-2012 v1.0.2

Cible de sécurité : ANSSI-CIBLE-CC-2017 (ChipDoc P60 on JCOP3 SEDIC P60(OSB)SSCD)

I. Descriptifs techniques

La nouvelle carte agent est constituée d'un seul composant de la famille P60 de NXP, d'un logiciel masqué et d'applets chargées. Les références exactes de la carte agent sont :

**ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD
qualifiée sur le composant P6022J VB version v7b4).**

La carte JCOP3 est industrialisée par l'IN GROUP pour le Ministère de l'intérieur.

C'est une carte JCOP3 de NXP, dual interfaces, composée d'un service IAS ECC et d'un service DESFIRE EV1 limité par le SHFD en nombre d'AID et en nombre de fichiers.

L'applet IAS ECC peut fonctionner totalement en mode contact mais elle peut aussi fonctionner en partie en mode sans contact explicite. L'applet est gérée comme un service et peut être activée ou désactivée par le « card manager » de la JCOP3.

L'applet DESFIRE EV1 fonctionne qu'en mode sans contact implicite. L'applet est gérée comme un service et peut être que désactivée par le « card manager » de la JCOP3.

L'activation est implicite. L'UID de la carte est configuré en random, c'est-à-dire que la valeur de l'UID est différente à chaque mise en utilisation.

**RAPPEL : Ce n'est pas une carte DESFIRE.
C'est une carte java JCOP3 multi-applicatives.**

II. Détection hardware de la carte agent en mode contact.

L'ATR indique des informations d'expertise de la carte mais n'indique pas des informations applicatives :

Les octets protocolaires indiquent une carte pouvant travailler en protocole contact T=0, en T=1 et en mode contactless T=15.

Son interface hardware en mode contact indique une possibilité de travailler en bi-tensions soit en 5V soit en 3V (la troisième tension 1,8V fonctionne mais n'est pas utilisée à ce jour.

Ce mode est réservé pour une utilisation future avec des produits «nomade low voltage »).

La carte ne fonctionne pas entre 5V et 3V (choix configuré en mode step).

Les vitesses de transmission en mode contact dépendent du lecteur. Elles peuvent aller jusqu'à 161290 bits/s si la fréquence du lecteur est de 5 Mhz (valeur maximale indiquée dans la norme ISO7816).

La partie contactless est traitée dans le compte-rendu d'essais et de sa conformité aux tests de la norme ISO10373-6.

La carte accepte une identification SFI (attention seule une partie spécifiée est autorisée) en mode contact et en mode contactless (sauf attribut forçant le mode contact).

La carte ne comporte qu'une voie logique, c'est à dire qu'elle ne peut pas travailler en mode contact et en mode sans contact en même temps. De plus elle n'est pas prévue par sa mono voie à travailler avec une voie SWP.

La détection de la JCOP3 par Windows entraîne une fonction de propagation des certificats de la carte vers les magasins des certificats.

Rappel :

Le service DESFIRE EV1 n'est pas accessible en mode « contact » car les spécifications ne sont pas compatibles avec la norme réservée au mode à contact.

III. Détection hardware de la carte par le lecteur RFID.

La carte agent JCOP3 est une carte JAVA multi-applicatives ayant 2 applets actives.

- La carte agent JCOP3 en mode sans contact est en mode implicite c'est-à-dire que l'applet DESFIRE EV1 est active dès l'activation du champ magnétique.

Si le **premier octet** émis par le lecteur (octet de CLASS) vers la carte est **un octet de CLASS DESFIRE** alors le « card manager » verrouille l'applet DESFIRE EV1.

Si le **premier octet** émis par le lecteur n'est **pas une valeur de CLASS DESFIRE** alors l'applet DESFIRE est désactivée et l'applet IAS ECC est alors activé.

Dans le cas où cette valeur n'est pas comprise comme un octet de CLASS IAS ECC alors le « card manager » désactive également l'applet IAS ECC. N'ayant plus d'autre applet à sélectionner alors la carte se verrouille et répond **un statut d'erreur « 6884 »**.

Une mise en hors champs est alors obligatoire par le logiciel du poste de travail.

Si le **premier octet** émis par le lecteur (octet de CLASS) vers la carte est **un octet de CLASS IAS ECC** alors le « card manager » verrouille l'applet IAS ECC.

Si le **premier octet** émis par le lecteur n'est **pas une valeur de CLASS DESFIRE ni IAS ECC** alors le « card manager » de la carte désactivera aussi l'applet IAS ECC.

N'ayant plus d'applet activée, le « card manager » répondra à toutes les futures APDU reçues avec le **statut d'erreur : SW= 6884**.

Une mise en hors champs est alors obligatoire par le logiciel du poste de travail.

IV. Notes techniques sur les dysfonctionnements.

- La plupart des dysfonctionnements vient de lecteurs obsolètes ne pouvant plus être mis à jour.
- De nombreux **lecteurs multi applicatifs** ne respectent pas les séquences de mise en champ et de mise en hors champ entre deux changements de protocole comme le demande la norme ISO 14443. Rappel normatif, le changement de protocole A, B, B' et C est autorisé. Après la sélection d'un protocole ISO (A, B, B') on sélectionne une application. En cas de non réponse, la carte/badge/smartphone est rejetée en coupant le champ puis en réactivant celui-ci afin de détecter une autre application et ainsi de suite afin de trouver la bonne application.
- Pour faciliter la détection il est conseillé soit de désactiver la recherche automatique d'un protocole, soit de forcer la priorité sur une application voulue (exemple le service DESFIRE).
- Le fonctionnement non conforme du lecteur avec WINDOWS lors des échanges en trame CCID provoque des arrêts de communication avec la carte agent.

Pour rappel la carte JCOP3 est une carte JAVA avec des certificats et ce n'est pas une carte DESFIRE EV1. Windows va détecter une carte JAVA et via les commandes CCID va demander la propagation des certificats puis va réinitialiser correctement l'environnement du lecteur comme lors de la détection de la carte.

V. Exemples d'anomalies normatives des lecteurs RFID lors d'une connexion à une carte agent JCOP3.

1) Exemple d'un lecteur multi-protocole provoquant **une erreur de communication**

Étape 1 :

Détection de la carte agent JCOP3.

Étape 2 :

Activation du champ magnétique du lecteur (La carte est en mode implicite et le service DESFIRE est activé).

Étape 3

Test 1er protocole : exemple recherche de CALYPSO

SELECT MF CALYPSO

> **94** A4 00 00 02 3F 00 00

< **6E 00**

L'APDU n'est pas reconnu par DESFIRE actif, le premier octet **94** reçu par la carte provoque une désactivation du service DESFIRE et une activation du service IAS ECC. Celui-ci traite ce premier octet **94** et n'est pas reconnu par l'IAS ECC provoquant également la désactivation du service IAS ECC. Le « card manager » de la carte JAVA va refuser cette APDU en répondant par un statut 6E 00. **A partir de cette étape la carte n'a plus d'applet activé et ne pourra répondre que par un statut d'erreur.** Seule une réinitialisation du champ (donc de la carte pourrait débloquent cet état)

Le lecteur va poursuivre sa recherche de protocole sans réinitialiser le champ magnétique (erreur ISO14443)

Test 2^e protocole : exemple recherche iCLASS

Select MF iCLASS

> 80 A6 00 00 03 00 00 00 00

< **68 84**

Le « card manager » n'ayant plus d'applet active va répondre à toutes les APDUs reçues par le statut « 68 84 ».

Conclusion : impossible de sortir de la boucle sans une coupure du champ.

2) Exemple d'un lecteur multi-protocole **sans erreur de communication** :

Étape 1 :

Détection de la carte agent JCOP3.

Étape 2 :

Activation du champ magnétique du lecteur (La carte est en mode implicite et le service DESFIRE est activé).

Étape 3 :

Test 1^{er} protocole : exemple recherche de CALYPSO

SELECT MF CALYPSO

> 94 A4 00 00 02 3F 00 00

< **6E 00**

L'APDU n'est pas reconnu par DESFIRE actif, le premier octet **94** reçu par la carte provoque une désactivation du service DESFIRE et une activation du service IAS ECC. Celui-ci traite ce premier octet **94** et n'est pas reconnu par l'IAS ECC provoquant également la désactivation du service IAS ECC. Le « card manager » de la carte JAVA va refuser cette APDU en répondant par un statut 6E 00.

Étape 4 :

Le lecteur coupe alors le champ magnétique, puis le réactive.

Le lecteur va poursuivre sa recherche de protocole.

Test 2^e protocole : recherche iCLASS

Select MF iCLASS

> 80 A6 00 00 03 00 00 00 00

< **6E 00**

Étape 5 :

Le lecteur coupe le champ magnétique, puis le réactive.

Le lecteur va poursuivre sa recherche de protocole.

Test 3^e protocole : recherche DESFIRE

SELECT MF DESFIRE

> 90 5A 00 00 03 00 00 00 00

< **91 00**

L'APDU est reconnue par le service DESFIRE actif (mode implicite), le premier octet **90** reçu par la carte provoque un verrouillage du service DESFIRE par le « card manager » et poursuit l'analyse de l'APDU. L'APDU SELECT MF est décodée et exécutée correctement par le service DESFIRE permettant l'émission du statut OK soit **91 00**.

VI. Conclusion

La carte agent émule exactement une carte DESFIRE EV1 si le lecteur émet toujours le premier octet CLASS de l'APDU des spécifications DESFIRE dès l'activation du champ magnétique de celui-ci.

À partir de cette étape, le lecteur est conforme et les travaux d'intégration de la carte agent peuvent être réalisés par une simple carte DESFIRE EV1 par un industriel en la configurant avec un UID à valeur aléatoire par la commande décrite dans les spécifications DESFIRE EV1.

Le nombre de clés et leurs valeurs ainsi que les keysetting sont paramétrés en fonction d'un usage spécifique (AID défini avec le MI).

La carte JCOP 3 doit être remplacée progressivement par la carte JCOP 4.5.

Le mode de fonctionnement de la JCOP 4.5 est le même que la JCOP 3.

4.1.3. 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 Random ID.

En revanche, il n'est pas nécessaire d'implémenter le Random ID 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 patches 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 Security 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 où la clé est introduite par plusieurs porteurs, la clé finale est reconstituée par des XOR successifs de chaque cryptogramme ($K = \text{XOR}[\text{XOR}[K1, K2], K3]$). 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 applicatives, 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.

4.1.4. 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 a trait au formatage des données des minuties.

Conformément à la législation du RGPD sur le traitement de données à caractère personnel, **aucune donnée biométrique ne sera collectée ou enregistrée par le système de contrôle d'accès. Le stockage des données biométriques sera réalisé dans le badge.**

La biométrie, comme la saisie d'un code, est souvent utilisée en tant que **second facteur permettant d'authentifier** un porteur de badge.

Ceci permet d'atteindre le niveau de sûreté le plus élevé défini par l'ANSSI et le CNPP (niveau IV de sûreté et niveau L3 de résistance aux attaques logiques). Les têtes de lecture permettant d'atteindre le niveau L3 de résistance aux attaques logiques doivent donc pouvoir admettre un clavier d'authentification ou un lecteur biométrique dotés d'une fonction « accès sous contrainte » (voir paragraphe 1.2 Spécifications ANSSI).

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 :

- Écran 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, 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 termes 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 » et sera donc dotée d'un dispositif anti-rebond pour les serrures en applique et encastrées.

Pour les serrures en applique, le pêne demi-tour devra garantir la fermeture de la porte.

Pour les serrures encastrées, le contre-pêne de sécurité donnera l'ordre d'éjection automatique du pêne dormant et le blocage du pêne demi-tour double action.

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 50 mm au standard Français sur les portes métalliques et serrures à profil étroit sur les portes en aluminium avec un axe minimum de 30 mm et un entraxe de 92 mm.

Dans le cas d'une porte soumise à un procès verbal, il faudra veiller à ne pas effectuer de percements ou d'autres actions mettant en péril la conformité de celui-ci (portes coupe-feu par exemple).

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 » et sera donc dotée d'un dispositif anti-rebond pour les serrures en applique et encastrées.

Pour les serrures en applique, le pêne demi-tour devra garantir la fermeture de la porte.

Pour les serrures encastrées, le contre-pêne de sécurité donnera l'ordre d'éjection automatique du pêne

dormant et le blocage du pêne demi-tour double action.

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 50 mm au standard Français sur les portes métalliques et serrures à profil étroit sur les portes en aluminium avec un axe minimum de 30 mm et un entraxe de 92 mm.

Dans le cas d'une porte soumise à un procès verbal, il faudra veiller à ne pas effectuer de percements ou d'autres actions mettant en péril la conformité de celui-ci (portes coupe-feu par exemple).

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, à 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 » et sera donc dotée d'un dispositif anti-rebond pour les serrures en applique et encastrées.

Pour les serrures en applique, le pêne demi-tour devra garantir la fermeture de la porte.

Pour les serrures encastrées, le contre-pêne de sécurité donnera l'ordre d'éjection automatique du pêne dormant et le blocage du pêne demi-tour double action.

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 sur pression d'un bouton ou par simple abaissement de la béquille 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, 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 » pour les serrures en applique et encastrées.

Pour les serrures en applique, le pêne demi-tour devra garantir la fermeture de la porte.

Pour les serrures encastrées, le contre-pêne de sécurité donnera l'ordre d'éjection automatique du pêne dormant et le blocage du pêne demi-tour double action.

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 50 mm 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 contrôle 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 contrôle 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, à 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, 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 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 privilégiées 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.
- Respect de la norme sécurité système incendie en vigueur

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.

À 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 ou EV2

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.