

MARCHE PUBLIC DE TRAVAUX



Remplacement du contrôle d'accès pour les sites de Lyon

N° de procédure :

Cahier des Clauses Techniques Particulières

1	PREAMBULE	4
1.1.1	L'Acoss	4
1.1.2	Organisation administrative de l'ACOSS	4
1.1.3	Allotissement :	4
1.1.4	SITES CONCERNES :	4
1.1.5	Site Principal ACOSS Lyon Saint Priest	4
1.1.6	Site ACOSS Lyon Feyzin	5
2	DISPOSITIONS COMMUNES	5
2.1.1	OBLIGATIONS DU TITULAIRE	5
2.2	Matériels	6
2.3	Connaissance des lieux et du dossier de consultation des entreprises	6
2.4	Missions du soumissionnaire	7
2.4.1	Organisation du projet	7
2.4.2	Délais et plannings de réalisation	7
2.5	Contraintes d'interventions	7
2.6	Accès aux locaux	8
2.7	Livraison des matériels	9
2.8	Contraintes de phasage des travaux	9
2.9	Relations avec les entreprises d'exploitation et de maintenance des sites	9
2.10	Etat des lieux	9
2.11	Réunions sur site	9
2.12	Qualité et origine du matériel	9
2.13	Contraintes résultant des textes en vigueur et de l'assurance légale	10
2.14	Echantillons / Matériels	10
2.15	Garantie de réalisation et de fonctionnement	11
2.16	Levées de réserves	11
2.17	Sécurité et protection de la santé	11
2.18	Documentation	11
2.19	Règles d'installations	11
2.20	Percement, rebouchage, Menuiserie	11
2.21	Remise en état après intervention	12
2.22	Réception des travaux	12
2.22.1	Généralités	12
2.22.2	Dossier des Œuvres Exécutés D.O.E	12

2.22.3	Dossier de récolement	13
2.23	Contrôle technique de l'installation	13
2.23.1	Vérifications techniques incombant aux entreprises	13
2.24	Essais, mise en service, OPR (Opérations Préalables à la Réception)	13
2.25	Garantie de parfait achèvement	13
2.25.1	Délai de garantie	13
2.25.2	Etendue de la garantie	14
2.26	Garanties	14
2.27	OBLIGATIONS DU TITULAIRE en matière de sécurité des Systèmes d'Information.	14
2.27.1	Politique de Sécurité	14
2.27.2	Organisation de la Sécurité de l'Information	14
2.27.3	Exigences Réseau	15
2.27.4	Mesures de sécurité	15
2.27.5	Destruction des données	15
2.27.6	Devoir de conseil en matière de sécurité	15
2.27.7	Mise à jour et nouvelles versions de logiciels	16
2.27.8	Traitement des obsolescences	16
2.27.9	Correctifs de sécurité	16
3	DESCRIPTIF TECHNIQUE DES PRESTATIONS COMMUN A L'ENSEMBLE DES SITES	16
3.1.1	Exigences	16
3.2	Solutions logicielles	17
3.2.1	L'outil de supervision	17
3.2.2	Le contrôle d'accès	18
3.2.3	Equipements informatiques	20
3.2.4	Les lecteurs de badges	21
3.2.5	Autres technologies d'identifications	21
3.3	Transfert de compétences et Formation	21
3.4	Migration et intégration de la base actuelle	22
3.5	Modification ou rajout de matériel compatible avec la solution.	22

1 PREAMBULE

Ce document constitue le cahier des conditions techniques particulières (CCTP) de la procédure adaptée de l'ACOSS (nom juridique), identifiée publiquement par la marque Urssaf Caisse nationale depuis janvier 2021.

Il concerne la fourniture et le remplacement d'un système de contrôle d'accès pour les sites de Lyon (ST Priest et Feyzin).

1.1.1 L'Acoss

L'Acoss ou Urssaf Caisse nationale gère la trésorerie de chacune des 4 branches de la Sécurité sociale (Maladie, Famille, Vieillesse, Accidents du travail – maladies professionnelles) afin de leur permettre de fonctionner au quotidien.

Dans le cadre du financement du régime général, les missions de l'Acoss et du réseau des Urssaf permettent donc, notamment, de financer la prise en charge ou le remboursement des soins médicaux, d'indemnités en cas d'arrêt maladie, de congé maternité ou d'accidents du travail ainsi que le paiement des retraites de base et des allocations familiales des bénéficiaires du régime général de la Sécurité sociale.

Au sein de l'ACOSS, la Direction des Systèmes d'Information (DSI) a la charge de la politique informatique de la Branche Recouvrement (élaboration et mise en œuvre des schémas directeurs et des plans informatiques annuels), de l'attribution des missions et des moyens, et du pilotage de l'ensemble des activités.

Par ailleurs, elle assure la réalisation de certaines missions opérationnelles de maîtrise d'œuvre (MOE) sur le Système National de Production des URSSAF, et sur les systèmes informatiques et bureautiques de la caisse nationale.

Sous la tutelle de l'état Français, l'ACOSS a été identifiée comme Opérateur de Services Essentiels (OSE).
A ce titre, elle doit répondre à des exigences renforcées en matière de sécurité des systèmes d'information, sous le contrôle de l'ANSSI, dont elle applique les prescriptions et les recommandations.

1.1.2 Organisation administrative de l'ACOSS

L'ACOSS est actuellement basée sur 11 sites géographique différents :
Montreuil, Lille, Caen, Nantes, Toulouse, Montpellier, Marseille, Biot, Valbonne, Lyon et Nancy.

1.1.3 Allotissement :

Le présent marché se compose d'un seul lot pour les :

- **Sites ACOSS Lyon (St Priest et Feyzin)**

1.1.4 SITES CONCERNES :

1.1.5 Site Principal ACOSS Lyon Saint Priest

Le site de Lyon Saint Priest, concerné par le présent CCTP, se compose d'un immeuble de bureau sur R+2 de 8048 m² en pleine propriété.

La zone de travaux se situe principalement au rez-de-chaussée de l'immeuble pourvu d'un data center avec des accès extérieurs côté portail pour les voitures et les piétons (portillon) et côté accueil (portillon) pour un accès piéton.

Adresse du chantier :

ACOSS Lyon
590 Cours du 3^{ème} Millénaire
69800 SAINT PRIEST

La personne en charge du suivi de cette opération est le responsable du site, Monsieur Nouredine BADREDDINE, joignable au 07 64 51 03 16 ou son adjointe, Madame Catherine GALAUP joignable au 06 07 71 74 21 ou Monsieur Guillaume BUARD, joignable au 04 72 89 21 03.

1.1.6 Site ACOSS Lyon Feyzin

Le site de Feyzin, concerné par le présent CCTP, se compose d'un immeuble de bureau R+3 de 3073 m² en pleine propriété.

La zone de chantier se situe au rez-de-chaussée de l'immeuble avec un data center.

Adresse du chantier :

ACOSS FEYZIN
Rue Jacques Monod
69320 FEYZIN

La personne en charge du suivi de cette opération est le responsable du site, Monsieur Nouredine BADREDDINE, joignable au 07 64 51 03 16 ou son adjointe, Madame Catherine GALAUP joignable au 06 07 71 74 21 ou Monsieur Guillaume BUARD, joignable au 04 72 89 21 03.

2 DISPOSITIONS COMMUNES

2.1.1 OBLIGATIONS DU TITULAIRE

Le titulaire se doit de signaler toute erreur, omission, imprécision, contradiction ou ambiguïté qu'il pourrait déceler dans les documents faisant partie de la présente consultation.

Toute fourniture non explicitement demandée, mais nécessaire au bon fonctionnement des installations, aux respects des règles de l'art d'installation, est due au titre du marché.

Le soumissionnaire ne pourra arguer d'une omission, d'une erreur ou d'une imprécision dans la description ou la figuration des ouvrages pour ne pas exécuter le travail dans les règles de l'art, ou pour réclamer un supplément à son prix forfaitaire.

Bien que cette liste ne soit ni exhaustive, ni limitative, le soumissionnaire doit :

- Les études techniques d'exécution pour l'ensemble du projet,
- Les missions d'encadrement de ses intervenants,
- Les installations de chantier propres au présent marché,
- La supervision et l'organisation de ses travaux,
- Les travaux provisoires rendus nécessaires par le phasage de l'opération,
- Les déposes et démolitions et recyclages préalables nécessaires à l'installation des nouveaux équipements,
- Le nettoyage et l'enlèvement des gravats après chaque intervention,
- Les étanchéités coupe-feu liées à ses travaux (calfeutrement après passage dans un mur, une cloison ou une dalle),
- Les dispositifs de sécurité et équipements adaptés
- Les protections spécifiques anti-poussières, anti-vibration liées à ses travaux,

- Toutes les sujétions résultant de l'impératif de continuité d'exploitation des matériels informatiques et de la présence du personnel du site pendant les travaux,
- Les interventions de nuit et/ou les week-ends pour le respect du planning et des contraintes de continuité de service de la production informatique de l'ACOSS, y compris les déclarations de travail,
- La remise en état ou la réparation des ouvrages que ces ouvriers ou préposés auraient pu détériorer,
- D'une façon générale, tous les ouvrages décrits dans le présent cahier des charges.

2.2 Matériels

Le soumissionnaire doit tenir compte également des difficultés d'approvisionnements et de mise en œuvre.

Le soumissionnaire reconnaît, par le fait même de son offre, qu'il a pris parfaitement connaissance des sujétions de toute nature qu'il pourra rencontrer en cours d'exécution.

Il devra expressément tenir compte des ouvrages et travaux de son corps de métier, indispensable à la parfaite exécution et à la finition complète des prestations pour la réalisation des lots, ceci conformément aux règles de l'art et aux règlements en vigueur.

Le marché ayant un caractère forfaitaire, Le soumissionnaire doit impérativement :

- Avoir au préalable pris connaissance des lieux dans le détail,
- Avoir vérifié et modifié le cas échéant les descriptifs en cas d'erreur, notamment par sous-évaluation (aucun supplément ne sera dû au titre d'une insuffisance dans le descriptif du présent cahier des charges),
- Effectuer les métrés et indiquer les quantitatifs sous la forme du bordereau de prix de la DPGF (Décomposition de Prix Générale et Forfaitaire) jointe au présent document.

Il appartiendra au soumissionnaire de s'assurer complètement de la faisabilité de ses solutions en regard, entre autres, des aspects réglementaires, de la faisabilité technique et des contraintes liées au délai d'opération et aux contraintes d'exploitation de l'ACOSS.

Le soumissionnaire prévoit une méthodologie et toutes les dispositions de mise en œuvre nécessaires pour réaliser l'installation des équipements.

2.3 Connaissance des lieux et du dossier de consultation des entreprises

Le soumissionnaire est réputé :

- Avoir pris connaissance du dossier de consultation des entreprises, de tous les plans et documents utiles, de tous les éléments généraux et locaux, en relation avec l'exécution du marché.
- Avoir apprécié exactement toutes les conditions d'exécution des ouvrages et s'être parfaitement et totalement rendu compte de leur nature, de leur importance et de leurs particularités.
- Avoir procédé à une visite détaillée des lieux et avoir pris parfaite connaissance de toutes les conditions physiques et de toutes les sujétions relatives aux lieux des travaux, aux accès et aux abords, à la topographie et à la nature des terrains, à l'exécution des travaux à pied d'œuvre, à l'organisation et au fonctionnement du chantier.
- Avoir pris connaissance des moyens de communication et de transport, lieu d'extraction des matériaux et stockage, ressource en main d'œuvre, énergie électrique, eau, installation de chantier, éloignement des décharges publiques ou privées, etc...
- Avoir examiné toutes les indications des documents du Dossier de Consultation des Entreprises, notamment celles données par les plans, les dessins d'exécution et le cahier des charges, s'être assuré qu'elles sont suffisantes et concordantes, et s'être entouré de tous renseignements éventuels auprès du maître d'ouvrage.

Le soumissionnaire demandera au maître d'ouvrage tous les renseignements qui lui sembleront nécessaires à l'établissement de son offre.

En conséquence, le soumissionnaire ne pourra jamais arguer que des erreurs ou omissions le dispense d'exécuter tous les travaux concernant son corps d'état et l'oblige à demander un supplément de prix.

2.4 Missions du soumissionnaire

2.4.1 Organisation du projet

Éléments attendus à la consultation

Les éléments attendus sont les suivants :

- Diagnostic de l'existant,
- Note méthodologique d'intervention sur des sites en fonctionnement,
- Un calendrier détaillé des installations,
- Un délai d'approvisionnement de la fourniture du matériel,
- Etudes techniques :
 - Fiches techniques,
 - Notes de calculs,
 - Plans et schémas d'implantation,
 - Plans d'Exécution,
 - Plans de synthèse.
- Organigramme des intervenants du projet et les CV,
- Références en matière d'installation de contrôle d'accès,
- Attestation de 1er niveau de certification CNPN,
- Installateurs certifiés pour réaliser, dans les règles de l'art, l'installation de solutions qualifiées ANSSI conformément aux recommandations.

2.4.2 Délais et plannings de réalisation

Le délai global d'exécution sera à déterminer à compter de la date donnée par l'ordre de service.

Les délais indiqués sur le planning prévisionnel tiendront lieu d'engagement des titulaires vis-à-vis de la réalisation des travaux.

L'optimisation financière des travaux doit être une constante intégrée dans la démarche du soumissionnaire.

Le délai global de réalisation de cette opération constitue également un enjeu important.

2.5 Contraintes d'interventions

Les interventions pourront être réalisées en locaux occupés. En conséquence, l'entreprise devra prendre toutes les dispositions utiles afin d'assurer la sécurité des intervenants et du personnel. Les dégagements ainsi que les issues de secours des locaux devront être constamment praticables. Aussi, l'entreprise devra tenir compte des périodes d'ouverture et de fermeture de l'établissement pour planifier ses interventions. Cette planification établie par l'entreprise sera proposée pour accord au responsable de site. Ces dispositions seront réputées incluses dans l'offre de l'entreprise.

Les travaux bruyants tels que les percements importants, carottages, ... devront être réalisés en dehors des heures de travail. En conséquence, l'entreprise devra tenir compte des horaires d'ouverture et de fermeture de l'établissement pour planifier ses interventions. En règle générale, ces interventions pourront avoir lieu avant 8 heures ou après 17 heures. Cette planification établie par l'entreprise sera proposée pour accord au responsable de site. Ces dispositions seront réputées incluses dans l'offre de l'entreprise.

Le fonctionnement des services de l'organisme ne doit pas être perturbé. Les entreprises devront donc prendre en compte les éléments suivants :

- La circulation des véhicules et des personnes est soumise au Code de la Route à l'intérieur du site. De plus, elle est soumise à la réglementation intérieure propre à l'établissement et aux directives éventuelles du responsable de site.
- L'entreprise ne devra causer aucun dommage aux installations existantes. Dans le cas, où par accident, elle causerait de tels dommages, elle en devrait la réparation immédiate.
- Tout entrepreneur devra prévoir :
 - Les méthodes d'exécution de ses prestations,
 - L'utilisation des matériels,
 - La mise en œuvre d'ouvrages provisoires,
 - De ne pas perturber le fonctionnement du site et prévenir tout risques et nuisances.
 - Etc.
- Le stockage de matériels et matériaux pourra être autorisé par le responsable de site, à condition que celui-ci ne soit ni inflammable ni explosif. Le stockage est à l'entière responsabilité des entreprises. Ces éventuels dépôts de matériaux ou matériels devront toutefois tenir compte de la nécessité impérieuse de prévenir tous les incendies susceptibles de se propager au bâtiment.

L'ensemble de ces dispositions, à prendre par les entreprises, a pour objet d'assurer la continuité de fonctionnement :

En aucun cas, il ne sera toléré un arrêt intempestif des matériels environnementaux liés aux salles et serveurs informatiques existants sur chaque site à l'exploitation du bâtiment.

Par conséquent, les travaux de toute nature devront faire l'objet d'une attention particulière dans les locaux suivants :

Salles informatiques,

Locaux techniques (électriques et climatisation, ...).

PC sécurité

Contrainte de continuité de fonctionnement et de sécurité des sites pendant les travaux

Ces contraintes visent tout particulièrement les points suivants :

Le maintien de fonctionnement opérationnel sans dégradation de services,

Le filtrage des accès et le maintien de la sécurité périmétrique et périphérique des bâtiments existants, et plus particulièrement les salles critiques,

Le maintien de l'accessibilité des sites pour les personnels ou intervenants extérieurs de l'ACOSS pendant toute la durée des travaux,

L'absence de tout risque pour les personnels ou intervenants extérieurs.

Le maintien des accès pompiers réglementaires aux bâtiments, le respect des mesures de sécurité d'intervention,

Accords préalables et obligatoires du Maître d'Ouvrage pour les interventions représentant un risque pour la production informatique,

Accords préalable et obligatoires du Maître d'Ouvrage pour les interventions dans les zones sensibles et critiques (salles informatiques, TGBT, ...),

Respect du planning des arrêts et fonctionnements en mode dégradé des installations,

Interventions hors heures ouvrées et/ou en week-end non exclues,

Interventions sans soudure dans le bâtiment.

2.6 Accès aux locaux

Le soumissionnaire se conformera aux procédures internes de chaque site.

2.7 Livraison des matériels

Des précautions particulières sont prises par le soumissionnaire pour la livraison des matériels dans les locaux, notamment par l'établissement d'un protocole de chargement/déchargement.

2.8 Contraintes de phasage des travaux

Les sites resteront en exploitation pendant les travaux, ce qui induit des contraintes de phasage importantes et la mise en œuvre de moyens de secours.

2.9 Relations avec les entreprises d'exploitation et de maintenance des sites

Les entrepreneurs sont tenus d'effectuer les demandes nécessaires auprès des entreprises d'exploitation et de maintenance des sites pour l'exécution de leurs travaux.

Ces demandes devront être signalées au Maître de l'ouvrage.

Ce point concerne en particulier :

- Toute modification d'installation existante,
- Toute coupure provisoire ou définitive de réseau (courants forts/courants faibles),
- Toute suppression de partie d'installation,
- Etc.

2.10 Etat des lieux

L'entreprise est réputée avoir vu les lieux et s'être rendu compte de leur situation exacte, de l'importance et de la nature des travaux à effectuer et de toutes les difficultés et sujétions pouvant résulter de leur exécution.

Les renseignements donnés dans le présent C.C.T.P. et dans les différents documents joints constituent des éléments d'information qu'il appartiendra, si nécessaire, aux titulaires, de compléter sous sa responsabilité.

2.11 Réunions sur site

La présence du titulaire aux réunions organisées par le Maître d'Ouvrage ou son représentant sera obligatoire.

Il sera organisé une réunion de lancement des travaux, des réunions de chantier ainsi qu'une réunion de réception des installations.

Les dates de convocation à ces réunions obligatoires seront communiquées ultérieurement et en temps utile par le Maître d'ouvrage ou son représentant.

2.12 Qualité et origine du matériel

Tous les éléments de l'installation devront être neufs, en parfait état de fonctionnement et conformes aux normes en vigueur et au présent descriptif.

Ils devront être garantis par leur constructeur pour l'utilisation envisagée, livrés sur le chantier dans leurs emballages d'origine s'ils ne font pas partie d'un assemblage préalable et/ou munis de leurs étiquettes et accessoires d'origine.

Les éléments de l'installation devront avoir une estampille ou un certificat de qualité délivré par un organisme officiel chaque fois qu'une telle qualification existe.

Dans le cas où il n'existe aucune norme de l'UTE et ISO EN NF concernant le matériel utilisé, celui-ci devra répondre aux règlements ou spécifications techniques générales ou particulières correspondant à l'usage auquel il est destiné.

Les normes européennes seront respectées. Cette disposition concerne entre autres le gros matériel et les conducteurs.

Tout appareil ne répondant pas à ces exigences sera refusé. Le matériel indiqué au mémoire technique sera celui installé sur site.

2.13 Contraintes résultant des textes en vigueur et de l'assurance légale

Le soumissionnaire s'engage à respecter les règlements, règles professionnelles, DTU et Normes en vigueur au moment de la soumission publiée par le C.S.T.B. dans le R.E.E.F. ainsi que les règlements locaux et règles d'hygiène et de sécurité.

Il n'emploiera que des matériaux traditionnels ou des matériaux non traditionnels ayant fait l'objet d'un avis technique du C.S.T.B. ou d'une enquête spécialisée d'un Bureau de Contrôle et acceptés en garantie par les assureurs.

Application des normes françaises. Liste non exhaustive des normes, règlements, décrets, DTU et arrêtés à respecter :

- Réglementation relevant du code du travail,
- Décret 72.1120 du 14 novembre 1972 relatif au contrôle et à l'attestation de la conformité des installations électriques intérieures, aux règlements et normes en vigueur (J.O. du 20/11/1972),
- Arrêté du 26 février 2003 relatif aux circuits et installations de sécurité. Ses annexes I et II et ses commentaires,
- NFC 12.100 (protection des travailleurs),
- NFC 13.100 (installations électriques Haute Tension),
- Norme sécurité incendie NFS 61 931 à 940 arrêtés du 02 février 1993,
- NFC 03.103 symbole synoptique pour schémas électriques,
- A la norme NFC 20.010 relative au degré de protection des matériels électriques,
- En 50173 (courants faibles),
- Normes NFC 91.082 relatives à la compatibilité électromagnétique environnement industriel.
- EN 550022 CEM,
- NFC 15.100 (installations électriques Basse Tension),
- D.T.U en vigueur dans la profession,
- Règles APSAD D83,

Ces lois, décrets, codes et règlements sont considérés comme faisant partie du marché et s'appliquent comme s'ils étaient tous énumérés.

Le soumissionnaire s'engage à informer en temps utile le Maître d'ouvrage des incompatibilités éventuelles entre lesdits décrets, codes, normes, lois et règlements et les exigences des spécifications et plans.

2.14 Echantillons / Matériels

Aucune commande de matériel ne peut être passée par le soumissionnaire sinon à ses risques et périls avant l'acceptation du maître d'ouvrage.

Notes particulières sur les marques de références :

Les types et marques des appareils cités dans le présent document seront donnés à titre indicatif de manière à situer le niveau de la prestation à l'exception de certains équipements imposés par le maître d'ouvrage pour des raisons :

- De cohérence dans la maintenance globale des installations (matériels existants),
- De cohérence vis-à-vis du stock de pièces détachées existants.

Le soumissionnaire pourra proposer des produits techniquement équivalents, tant en qualité qu'en performance.

Dans tous les cas, les matériels proposés par le soumissionnaire retenu pour réaliser les travaux devront obtenir l'agrément des représentants de la maîtrise d'ouvrage.

Dans l'hypothèse où un produit proposé par le soumissionnaire serait jugé de qualité inférieure ou moins performant à celui référencé dans le présent document, celui-ci sera tenu de fournir le matériel préconisé sur le document contractuel et ceci sans pouvoir prétendre un supplément de prix.

Après l'accord des représentants de la maîtrise d'ouvrage sur les matériels et signature du marché, le soumissionnaire ne pourra effectuer aucun remplacement sans une autorisation écrite.

2.15 Garantie de réalisation et de fonctionnement

L'entreprise garantit d'une façon formelle la parfaite réalisation des travaux faisant l'objet de la présente spécification technique, suivant les Règles de l'Art et en tenant compte de tous les règlements et décrets en vigueur.

L'entreprise s'engage à remplacer, réparer ou modifier, à ses frais exclusifs, toutes les fournitures et tous les ouvrages reconnus défectueux. La responsabilité du titulaire couvrira également, et dans les mêmes conditions, toutes les fournitures et tous les ouvrages qu'il sous-traitera.

2.16 Levées de réserves

Après émission du PV de réception du Maître d'ouvrage, tous les travaux, les interventions du Maître d'ouvrage nécessaires et complémentaires à la levée des réserves seront à la charge du titulaire.

2.17 Sécurité et protection de la santé

Le présent chantier fait l'objet de dispositions de sécurité et de protection de la santé conformément aux articles R 4512-2 et 4514-1 du Code du travail.

Dans ce cas, l'entreprise et ses éventuels sous-traitants devront établir, avant leurs interventions et conjointement avec l'entreprise utilisatrice, un Plan de Prévention (PDP).

2.18 Documentation

Les offres seront accompagnées d'une documentation technique détaillée en français des matériels proposés ainsi que des certificats de conformité aux normes en vigueur.

De plus, les titulaires fourniront dans leur offre les synoptiques des installations ainsi que les plans d'implantation détaillés.

2.19 Règles d'installations

Les travaux objet du présent document doivent être réalisés en tenant compte des cheminements prévus pour les courants forts/faibles existants ou à réaliser et de la mise en œuvre d'un réseau de masse maillé. Pour ce faire, l'entrepreneur prendra toutes les précautions nécessaires afin que les règles de cheminement soient respectées.

Les rayons de courbure doivent être supérieurs à 4 cm. Les câbles sont fixés dans le chemin de câble à l'aide d'attaches Velcro placés tous les 4 mètres en parcours horizontal, et tous les 2 mètres en parcours vertical. L'utilisation de colliers est tolérée sous réserve qu'ils ne contraignent pas les câbles (les colliers doivent être justes glissant).

Toute contrainte mécanique exercée sur le câble peut modifier irrémédiablement ses caractéristiques électriques.

L'installateur respectera les précautions suivantes lors de la réalisation de l'installation :

- Respecter les rayons de courbure (minimum 6 à 8 fois le diamètre du câble)
- Éviter les vrilles du câble (utilisation obligatoire d'un dérouleur de touret),

2.20 Percement, rebouchage, Menuiserie

Les percements seront réalisés avec une aspiration évitant la propagation des poussières.

Dans chaque percement, il sera procédé à la pose d'un fourreau en PVC dont le diamètre sera adapté au besoin et conforme aux règles de l'art.
Le rebouchage sera réalisé avec des matériaux incombustibles ayant le même degré, norme Euro-Class, que la paroi concernée.

Rappel : Le percement des poutres sera formellement interdit.

Les éventuels travaux de menuiserie pour l'installation de la solution resteront à la charge du titulaire.

2.21 Remise en état après intervention

Au fur et à mesure de l'avancement des travaux et à la demande du Maître d'ouvrage, les entreprises seront tenues de procéder régulièrement et à leur frais, au nettoyage des zones de travaux pour débarrasser les déchets provenant de ses prestations.

De même, les entreprises seront tenues d'enlever à leur frais au fur et à mesure de l'exécution des travaux dont elles ont la charge, les gravats, déchets, débris, emballages ou autres qui proviendront de l'exécution de ses travaux.

L'application de ces prescriptions sera exigée avec une grande rigueur par le Maître d'ouvrage.

En cas de refus de se soumettre à cette obligation, le Maître d'ouvrage, pour ces nettoyages, substituera au personnel de l'entreprise responsable toute personne ou société de son choix, dont la rémunération sera retenue sur le paiement des situations de travaux.

En cours de chantier, il sera demandé aux entreprises l'enlèvement du matériel et des matériaux sans emploi.

Les installations de chantier, le matériel et les matériaux en excédant devront être évacués dans un délai de cinq jours suivant la demande du Maître d'ouvrage.

En cas de refus de se soumettre à cette obligation, le Maître d'ouvrage, pour ces évacuations, substituera au personnel de l'entreprise responsable, toute personne ou société de son choix, dont la rémunération sera retenue sur le paiement des situations de travaux.

2.22 Réception des travaux

2.22.1 Généralités

La réception des installations a pour but d'évaluer la conformité des installations, avec les spécifications techniques, à l'égard des règles de l'art et aux normes en vigueur. Cette prestation sera à réaliser avec le Maître d'Ouvrage ou son représentant et fera l'office d'une fiche de réception de l'installation.

Les points suivants seront contrôlés :

- La conformité des équipements techniques.
- Les quantitatifs livrés et installés.
- Le repérage et étiquetage de l'installation.
- La pose des câbles et notamment le respect des rayons de courbures.
- La conformité du dossier des ouvrages exécutés.

2.22.2 Dossier des Œuvres Exécutés D.O.E

En fin d'exécution des travaux et avant réception des ouvrages, chaque entrepreneur devra fournir le "Dossier des Ouvrages Exécutés".

L'ensemble des documents graphiques sera remis sous format DWG pour Autocad.

Les supports plans, sous format DWG Autocad, seront fournis à la demande des entreprises par le Maître d'Ouvrage.

Ce dossier sera établi en 3 exemplaires et un exemplaire reproductible (version papier) ; il sera remis au Maître de l'Ouvrage.

2.22.3 Dossier de récolement

Les dossiers de récolement devront être fournis le jour de la réception sur chaque site.

Les dossiers de récolement seront fournis en 3 exemplaires papiers et 3 exemplaires informatiques par site.

Le dossier de récolement intégrera notamment :

- La fourniture de plans des installations électriques mis à jour.
- L'entreprise devra fournir tous plans d'exécution et notes de calcul nécessaires à la parfaite réalisation des travaux.
- L'ensemble des plans sera fourni au Maître d'ouvrage pour approbation.
- Les mises à jour en fonction des modifications "chantier" seront prises en compte et donneront lieu, si elles sont significatives, à une nouvelle publication d'approbation.

2.23 Contrôle technique de l'installation

2.23.1 Vérifications techniques incombant aux entreprises

Le contrôle interne auquel sont assujetties les entreprises doit être réalisé à différents niveaux :

- Au niveau des fournitures quel que soit leur degré de finition, l'entrepreneur s'assurera que les produits commandés et livrés sont conformes aux normes et spécifications du marché,
- Au niveau du stockage, l'entrepreneur s'assurera que celles des fournitures qui sont sensibles aux agressions des agents atmosphériques et aux déformations mécaniques sont convenablement protégées,
- Au niveau de la fabrication, de la mise en œuvre et des essais, le responsable des contrôles internes de l'entreprise vérifiera que tout est conforme aux D.T.U. et exécutés dans les règles de l'Art,

De plus, en cours de travaux ou à leur achèvement, chaque fois qu'il le juge nécessaire, le maître d'ouvrage ou son représentant peut procéder à des opérations de contrôles.

2.24 Essais, mise en service, OPR (Opérations Préalables à la Réception)

L'entreprise doit assurer l'ensemble des essais y compris toutes les sujétions qui conduiront à la vérification totale du bon fonctionnement et de la bonne mise en œuvre des travaux exécutés. Durant les études d'exécution, l'entreprise fournira la liste complète des essais qu'elle prévoit de réaliser au Maître d'ouvrage pour validation.

2.25 Garantie de parfait achèvement

2.25.1 Délai de garantie

Pendant une période minimum de deux ans à compter de la date de réception, l'entreprise garantira ses travaux dans les conditions indiquées ci-après :

- L'entreprise devra remédier à toutes les imperfections, malfaçons et désordres découverts dans les deux ans suivant la réception des travaux.

Lorsque la réception n'a pu être prononcée, cette période de garantie se trouve prolongée d'office jusqu'au jour où cette réception est effectivement prononcée.

2.25.2 Etendue de la garantie

Au titre de la garantie, l'entrepreneur doit la réparation et éventuellement le remplacement à titre gratuit (fourniture et pose) de toute partie du matériel qui, au cours du délai de garantie, serait reconnue défectueuse.

Les défauts constatés ou les accidents survenus sont notifiés à l'entreprise pour qu'il puisse entreprendre les réparations dans un délai fixé par le Maître d'ouvrage.

Passé ce délai, le Maître d'ouvrage peut faire procéder d'office et aux frais de l'entrepreneur, aux réparations nécessaires sans préjudice des dommages et intérêts qui lui seraient réclamés si le défaut de réparation causait un accident ou un préjudice.

2.26 Garanties

Les prestations de maintenance seront totalement couvertes pendant toute la période de garantie.

Les titulaires décriront dans leur offre les garanties supplémentaires et les prestations associées disponibles pour tous les éléments matériels concernés.

Le constructeur devra également s'engager à fournir, pendant une période de 10 ans, tous les éléments de matériel nécessaires à la maintenance et à l'extension des systèmes proposés.

2.27 OBLIGATIONS DU TITULAIRE en matière de sécurité des Systèmes d'Information.

2.27.1 Politique de Sécurité

Bien que cette liste ne soit ni exhaustive, ni limitative, le soumissionnaire doit :

- Disposer d'une PSSI complète, documentée et approuvée formellement par sa direction.
- S'engager à ce que toute personne (employé, prestataire) en contact avec son SI ait connaissance de sa « charte utilisateurs du SI » et de sa politique de sécurité.
- Être conforme à sa PSSI durant toute la durée de la prestation pour l'ACOSS.

2.27.2 Organisation de la Sécurité de l'Information

Le titulaire doit :

- Mettre en œuvre des procédures et dispositifs de sécurité pour se protéger contre le traitement non autorisé ou illégal, le transfert à un tiers, la perte ou la destruction d'informations appartenant à l'ACOSS,
- Disposer d'un référent sécurité en charge de l'application et du maintien de la PSSI,
- Son PSSI doit définir avec précision les rôles et les responsabilités pour les activités liées à la sécurité de l'information.

Il est souhaité que le Titulaire définisse et mette en œuvre les processus de sécurité fondamentaux suivants :

- Évaluation des risques liés à l'information,
- Réponse à incident,
- Sensibilisation à la sécurité,
- Gestion des correctifs,
- Surveillance des vulnérabilités,
- Gestion des fournisseurs,
- Gestion des incidents.
- Corriger dans des délais acceptables par l'ACOSS les problèmes pouvant entraîner une violation majeure de la sécurité.

2.27.3 Exigences Réseau

La DSI Urssaf dispose d'une plateforme technique spécifique pour contrôler les accès aux réseaux « Campus » du Recouvrement.

Son rôle est double :

- authentifier chaque device (appareil ou dispositif) se connectant sur les réseaux locaux des organismes,
- authentifier et ouvrir des accès réseau aux usagers et aux administrateurs techniques.

Elle repose sur la solution ISE (Identity Services Engine) du constructeur Cisco, basée sur le protocole de sécurisation normé 802.1x.

Les authentications sont jouées :

- par le biais de protocoles possédant différents niveaux de sécurité (EAP-MD5, EAP-MSCHAPV2, EAP-TLS, EAP-PEAP...)
- en s'appuyant sur des annuaires (Active Directory, ENTRA ID, LDAP...)
- ou par d'autres méthodes de plus bas niveau.

L'Acoss souhaite que les équipements proposés au travers du marché disposent d'une ou plusieurs méthodes d'authentications.

Le Candidat détaillera les possibilités et garanties d'interopérabilité avec la solution de contrôle d'accès décrite, en précisant les avantages et inconvénients de chacune.

2.27.4 Mesures de sécurité

Le titulaire sensibilise son personnel, intervenant dans le cadre des prestations, à la sécurité de l'information, des systèmes d'information et à l'ensemble des mesures de sécurité définies par l'acheteur ou s'imposant à ce dernier. Le titulaire veille notamment à ce que son personnel intervenant dans le cadre des prestations respecte les stipulations du présent marché concernant la sécurité.

2.27.5 Destruction des données

Au terme de l'exécution du marché ou en cas de résiliation, le titulaire restitue sans délai à l'acheteur une copie de l'intégralité des données confiées par lui dans le cadre de la prestation. Une fois la restitution effectuée, le titulaire détruit, dans un délai de trois mois, les éventuelles copies de données détenues dans son système d'information, y compris les données ayant fait l'objet de sauvegardes ou d'un archivage. La restitution et la destruction des données sont constatées par un procès-verbal daté et signé par le titulaire. Les procédés de destruction sont conformes aux réglementations en vigueur.

2.27.6 Devoir de conseil en matière de sécurité

Le titulaire et l'acheteur qui, à l'occasion de l'exécution du marché, ont connaissance d'informations ou reçoivent communication de documents ou d'éléments de toute nature, présentant un caractère confidentiel, sont tenus de prendre toutes mesures nécessaires, afin d'éviter que ces informations, documents ou éléments ne soient divulgués à un tiers qui n'a pas à en connaître. Une partie ne peut demander la confidentialité d'informations, de documents ou d'éléments qu'elle a elle-même rendus publics.

Le titulaire doit informer ses sous-traitants des obligations de confidentialité et des mesures de sécurité qui s'imposent à lui pour l'exécution du marché. Il doit s'assurer du respect de ces obligations par ses sous-traitants.

Ne sont pas couverts par cette obligation de confidentialité les informations, documents ou éléments :

- qui étaient dans le domaine public au moment de leur divulgation ou que l'acheteur aurait lui-même rendus publics pendant l'exécution du marché,

- signalés comme présentant un caractère non confidentiel et relatifs aux prestations du marché,
- qui ont été communiqués au titulaire par un tiers ayant légalement le droit de diffuser ces informations, documents ou éléments, comme le prouvent des documents existant antérieurement à leur divulgation.

2.27.7 Mise à jour et nouvelles versions de logiciels

Mises à jour et nouvelles versions de logiciels : Lorsque les prestations comprennent la livraison de logiciels standards ou de logiciels spécifiques, elles comprennent également, pendant la durée du marché, la livraison des mises à jour qui leur sont apportées ainsi que la livraison des nouvelles versions.

Le prix de ces mises à jour ou de ces nouvelles versions est inclus dans le prix du marché.

2.27.8 Traitement des obsolescences

Le titulaire installe et maintient les dispositifs du service dans des versions stables et à jour de leurs correctifs de sécurité et conformément à la procédure de maintien en condition de sécurité. Les versions installées doivent être des versions supportées sauf si celles-ci empêchent la réalisation du service. Il vérifie l'impact de l'installation des mises à jour sur le système d'information du service. Dans le cas où l'impact de l'installation ne permet pas la réalisation du service, le titulaire en documente les raisons, et définit et met en œuvre des mesures de réduction des risques.

2.27.9 Correctifs de sécurité

Une vérification d'aptitude (VA) ou une vérification de service régulier (VSR) peut être refusée si des composants ne sont pas à jour des correctifs de failles de sécurité publiés par l'éditeur depuis un délai supérieur à trois mois. L'acheteur définit les fréquences des livraisons en coordination avec les équipes d'exploitation, en fonction des différentes criticités des vulnérabilités concernées.

Le titulaire s'assure que l'application des correctifs de sécurité ne modifie pas les performances du système, en modifiant si besoin et à ses frais le système pour maintenir le niveau de performance malgré l'application du correctif.

3 DESCRIPTIF TECHNIQUE DES PRESTATIONS COMMUN A L'ENSEMBLE DES SITES

3.1.1 Exigences

La solution proposée devra répondre aux problématiques d'un site de type "Tertiaire et Data Center O.S.E* (Opérateur de Services Essentiels)" et devra être compatible avec nos badges actuels qui utilisent une technologie sans contact (les spécificités de ces badges seront communiquées aux entreprises candidates lors de la visite de site (**annexe 1**))

*Un OSE fournit un service essentiel (SE) dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

Les sites énoncés dans ce marché seront munis d'un système de contrôle d'accès et d'un outil de supervision global qui sera commun aux deux sites.

Les dispositifs de contrôle d'accès répondront à une logique de zonage du site et de hiérarchisation des droits d'accès avec une compatibilité avec le système anti-intrusion.

Le système proposé sera de marque **Synchronic**, ou techniquement équivalent et sera impérativement un système centralisé temps réel, qualifié et certifié ANSSI CSPN.

Le système sera impérativement capable de centraliser la gestion de la sécurité, de plusieurs sites distants géographiquement.

Son exploitation offrira la simplicité d'un système dans l'optimisation des tâches et sera paramétrable par l'exploitant. Le système devra être particulièrement modulaire et extensible et devra aussi bien fonctionner sur une architecture de type BUS de terrain (RS485) que sur une architecture native TCP/IP.

Il sera basé sur une architecture à différents niveaux :

- Niveau 1 : Les terminaux terrain (têtes de lecture pour le contrôle d'accès, contacts ...). Ce matériel ne pourra être propriétaire, il sera impérativement basé sur des standards du marché (Compatible RFID Mifare 1K et 4K et DESFire EV2/EV3),
- Niveau 2 : Les Concentrateurs et/ou Centrales permettant la gestion des périphériques en local et garantissant une autonomie de fonctionnement en cas de perte de réseau d'exploitation ou de serveur,
- Niveau 3 : Le logiciel d'exploitation qui se devra convivial et permettra le paramétrage du système dans sa globalité et l'exploitation temps réel des différents « métiers » de la Sûreté souhaités (Contrôle d'accès, détection intrusion, GTC, Vidéosurveillance,)

Les systèmes, quelle que soit leur version, devront être compatibles pour fonctionner nativement en mode MODBUS/TCP.

Les trajets des câbles seront définis lors de la visite, en utilisant au maximum les chemins existants (chemins de câbles CFA, fourreaux) **dès lors qu'ils respectent les recommandations de l'ANSSI** et seront complétés si nécessaire.

L'utilisation de câble réseau sera de type 4 paires torsadées catégorie 6a classe Ea minimum pour 10 Gbps sur 100 m.

Le titulaire devra assurer la dépose des anciens lecteurs et équipements de l'ancienne solution, à l'exception du câblage non apparent. Cette intervention inclut :

- Les anciens lecteurs remplacés,
- Les équipements des accès dont le contrôle est supprimé, notamment les ventouses, les déclencheurs manuels et les boutons poussoirs,
- La dépose des boîtiers d'alimentation centralisés dans le PCS.

De plus, le titulaire devra réaliser les finitions liées à l'installation et à la dépose (enduit, peinture, pose de caches) afin d'assurer une intégration harmonieuse des nouveaux équipements.

3.2 Solutions logicielles

3.2.1 L'outil de supervision

Le poste de gestion et de supervision sûreté installé offrira une interface de gestion unique pour l'opérateur afin de gérer l'ensemble des informations en provenance des différents équipements de sûreté.

Son logiciel répondra aux spécifications techniques suivantes :

- Disposer d'une visualisation sur l'état de l'installation,
- Archiver les événements dans une base de données pour pouvoir les analyser ultérieurement,
- Visualiser et contrôler la liste des défauts en cours,
- Disposer d'une fonction facilitant l'exploitation de l'historique des événements,
- Importer et exporter des états et des historiques.

3.2.2 Le contrôle d'accès

3.2.2.1 La solution devra être conforme aux préconisations ANSSI

3.2.2.1.1 Contrôle des zones critiques

Le système proposé devra être capable de répondre en tout point aux préconisations de l'ANSSI et à terme, à celles du SDSSI (cf. annexes 3 et 4) qui précisent entre autres les éléments suivants :

- L'authentification du badge des zones critiques doit reposer sur une clé commune ou dérivée d'une clé maîtresse. L'utilisation d'une puce Mifare DESFire EV2/EV3 est donc la solution la plus adaptée.
- Aucune information ne doit circuler en clair sur le canal sans fil et la liaison filaire, les liaisons de type Data-Clock/Wiegand sont donc à proscrire.
- La tête de lecture ne doit contenir aucun secret (niveau 1 ANSSI), ou sinon elle doit avoir fait l'objet d'une étude de sécurité approfondie (niveau 2 ANSSI).

3.2.2.1.2 Contrôle des autres zones

Le système proposé devra répondre à minima à un contrôle d'accès compatible avec notre système et aux prescriptions de l'annexe 1.

3.2.2.1.3 Le logiciel d'administration du contrôle d'accès

Il devra être fourni avec un module de marque Synchronic ou techniquement équivalent.

L'administration et le transfert des clés de chiffrements vers les lecteurs se feront de manière centralisée depuis le poste d'administration.

Toutes les solutions à base de badge de configuration à présenter devant chaque lecteur seront à proscrire. La solution devra permettre de gérer simultanément deux types de badge encodé différemment, soit avec deux applications distinctes (AID) soit deux fichiers différents dans la même application, et ceci afin de permettre de s'affranchir de toute compromission clé ou de renouvellement de clé. Il sera livré avec un lecteur USB pour l'enrôlement et l'encodage des badges utilisateurs.

3.2.2.1.4 UTL

Les unités de traitement locales nécessaires à l'installation devront être situées dans un local sécurisé conformément aux préconisations ANSSI. Les emplacements privilégiés par la maîtrise d'ouvrage sont la salle nommée CNA en annexe 2 (rouge foncé sur plan) pour le site de Saint-Priest et la salle DSN pour le site de Feyzin. Ces emplacements seront toutefois à confirmer avec le titulaire.

3.2.2.3 Le logiciel d'administration

Le logiciel proposé pour la gestion des accès sera de type de marque **Synchronic** ou techniquement équivalent.

Le logiciel de contrôle d'accès sera en architecture client/serveur. Il disposera d'une interface graphique conviviale, ergonomique et devra être évolutif pour permettre de gérer de 1 à plus de 10 000 lecteurs pour une capacité d'utilisateurs pouvant atteindre jusqu'à 20 000 utilisateurs.

Principales caractéristiques nécessaires :

- Moteur de base de données ouverte et non propriétaire type MySQL ou SQL Server,
- Architecture Client / Serveur multipostes,
- Gestion des accès par site, zone et secteur,
- Fonctions Anti-Pass Back, Anti-Time Back, mono ou multi-centrales,
- Tous types de technologies d'identification (DESFire, Mifare, IClass, 125KHz, Biométrie, radio...),
- Module d'importation manuelle ou automatique d'utilisateurs à partir de différentes sources (synchronisation sur une base de données RH) :
 - Fichier Excel,
 - Connexion à une base de données tierce via lien ODBC,
 - Annuaire LDAP.
- Traçabilité de toutes les actions effectuées depuis l'application d'administration,
- Module de personnalisation de badge intégré,
- Encodage des badges DESFire / Mifare intégré dans l'application,
- Compatible avec les environnements virtualisés (VmWare, Citrix)
- Orienté Multisites, Multi-Organismes
- Interfaçage armoires à clés Traka

Le logiciel permettra également les évolutions ou extensions suivantes :

- Client web
- Gestion de visiteur
- Module de comptage
- Redondance à chaud
- Personnalisation de badges

3.2.2.4 Extensions logicielles

Le logiciel de contrôle d'accès devra également intégrer les fonctionnalités suivantes :

– Client Web

Une application intranet sera prévue. Cette application fonctionnera depuis un navigateur internet (Firefox, Edge, Chrome...). Elle permettra d'administrer les droits du contrôle d'accès depuis n'importe quel poste informatique du réseau. Elle aura les possibilités suivantes :

- Gestion des utilisateurs :
 - Ajout/Modification
 - Affectation de familles
 - Assignment d'identifiants
- Gestion des grilles horaires
 - Ajout/Modification/Suppression de grilles horaires
- Visualisation et assignation des droits
- Gestion des exploitants
 - Ajout/Modification
 - Activation/Désactivation
- Fil de l'eau, avec personnalisation de l'affichage
- Recherche d'historique
- Ouverture d'accès (Télécommandes)

– Module de comptage

L'application de contrôle d'accès disposera d'un module de comptage permettant de connaître en temps réel et de façon nominative, le nombre de personnes présentes sur site ou dans une zone. Ce module devra gérer plusieurs zones de comptage. Une zone de comptage étant constituée de deux ensembles de lecteurs définis en entrée et en sortie. Ces lecteurs pourront être de type anti passback ou non et repartis sur plusieurs contrôleurs. La fonction point de rassemblement devra être intégrée à l'application, ainsi en cas d'alerte le logiciel sera en mesure d'éditer automatiquement la liste des personnes présentes sur site mais n'ayant pas badgé sur les lecteurs de rassemblements. Ce module pourra être installé sur plusieurs postes informatiques. Il disposera en outre des fonctionnalités suivantes :

- Comptage sur plusieurs zones,
- Affichage du nombre de personnes présentes ainsi que leur nom,
- Report sur application mobile ou impression automatique des personnes présentes en cas d'alarme,
- Module statistique pour la visualisation du taux d'occupation par zone de comptage.

L'activation de l'anti-pass back et le comptage des accès devront pouvoir être basés sur deux critères :

- Une authentification réussie par badge.

Un accès effectivement réalisé, pour les dispositifs capables de transmettre cette information au système (ex. : couloirs de passage avec détection de franchissement).

– Redondance à chaud

Afin de se prémunir contre toutes défaillances du serveur d'application et de maintenir un très haut niveau de disponibilité, la solution devra disposer d'un mécanisme de redondance à chaud permettant de basculer automatiquement vers un serveur de secours en cas de défaillance du serveur principal (cluster de serveur hébergé sur deux sites distants).

– Interfaçage base LDAP, AD

Le système de contrôle d'accès devra pouvoir s'interfacer sur l'annuaire LDAP de l'entreprise afin de permettre une synchronisation en temps réel de sa base de données utilisateurs.

– Personnalisation de badges

Le module de personnalisation de badges sera intégré nativement dans l'application de contrôle d'accès. Il permettra de réaliser plusieurs masques d'impressions (personnel interne, prestataire, visiteur...). L'impression se fera par lot ou dans la fiche utilisateur directement depuis l'application du contrôle d'accès.

3.2.3 Equipements informatiques

Les équipements informatiques seront à la charge du maître d'ouvrage et disposeront des caractéristiques techniques suivantes :

1] Serveurs :

- Serveur physique ou virtuel avec à minima un système Windows server 2019 voire la version la plus récente de cet OS
- Le titulaire du marché devra préciser les caractéristiques des serveurs hébergeant la solution (Capacité mémoire, disque ...)

2] Postes d'exploitations :

Ils répondront aux caractéristiques demandées par l'éditeur de la solution, basé sur un système d'exploitation Windows 11

3.2.4 Les lecteurs de badges

3.2.4.1 Mifare DESFire EV2 / EV3

Les lecteurs de badges proposés seront de technologie Mifare classic 1K et 4K DESFire EV2.EV3

Lecteur mode "transparent"

Les lecteurs de badges proposés devront fonctionner en mode dit "Transparent" (le lecteur ne doit pas intervenir dans le chiffrement des données). Ils auront pour autres caractéristiques :

- Liaison RS485 haute sécurité avec les unités de traitements
- Système anti-arrachement
- Fonctionne avec les puces (Compatible RFID Mifare 1K et 4K et DESFire EV2.EV3)
- Bornier de raccordement
- Compatible plot d'encastrement
- Antivandale (IK10) / IP65

Dans le cadre d'accès nécessitant un haut niveau de sécurité, des lecteurs/claviers RS485 pourront être proposés afin d'être conforme aux recommandations L3 du chapitre "tête de lecture" du guide de l'ANSSI. Ils auront pour autres caractéristiques :

- Liaison RS485 haute sécurité avec les unités de traitements
- Double authentification badge + code
- Système anti-arrachement
- Fonctionne avec les puces (Compatible RFID Mifare 1K et 4K et DESFire EV2.EV3)
- Bornier de raccordement
- Compatible plot d'encastrement
- Antivandale (IK10) / IP65

Badges formats cartes de crédits

Les badges seront aux formats cartes de crédits.

Ils devront être multi applications, sécurisée et comporter une puce au format MIFARE® DESFire® EV2.EV3, avec 2Ko de stockage minimum. Le lecteur ne devra en aucun cas utiliser le numéro de série du badge comme identifiant.

Fourniture de cent (100) cartes mifare vierge 1K et 4K à destination des visiteurs et mainteneurs.

3.2.5 Autres technologies d'identifications

3.2.5.1 Lecteurs d'intégration :

Des équipements de lecture des badges supplémentaires seront installés à un poste de travail dédié à l'encodage, ainsi qu'à deux postes destinés à l'enrôlement.

Les PC nécessaires à l'encodage et à l'enrôlement seront fournis par la maîtrise d'ouvrage.

3.3 Transfert de compétences, Formation, et accompagnement

La prestation doit inclure les formations suivantes :

- Formation « utilisateurs » 6 personnes,
- Formation « admin » 4 personnes.

Le titulaire du marché devra assurer un accompagnement technique et méthodologique pour la définition et la mise en œuvre de la charte d'encodage du système de contrôle d'accès.

À ce titre, il devra :

Analyser les besoins spécifiques du maître d'ouvrage en matière d'encodage des supports

Définir la structure d'encodage en conformité avec les normes et standards en vigueur

Fournir un document détaillé décrivant la charte d'encodage retenue

L'ensemble de ces prestations devra être réalisé en concertation avec le maître d'ouvrage et validé avant toute mise en production du système de contrôle d'accès.

3.4 Migration et intégration de la base actuelle

Un fichier de type Excel ou csv sera fourni par la MO et devra être intégrées par le titulaire (base utilisateur droits)

3.5 Modification ou rajout de matériel compatible avec la solution.

Conformément au CCAP, il pourra être intégré par voies d'avenants du matériel complémentaire référencé ci-dessous. Le prix comprendra les pièces, la main d'œuvre d'installation et le paramétrage du logiciel.

Prestations compatibles avec la solution
Lecteur simple
Lecteur double authentification (Carte et clavier)
Lecteur longue distance
UTL (Unité de Traitement Local)
Modules de commandes des systèmes de verrouillage
Mètre linéaire câble CFA et CFO
Système de verrouillage par ventouse électromagnétique
Bouton poussoir de commande du système de verrouillage
Déclencheur manuelle ouverture d'urgence (boîtier vert)
Contact d'ouverture
Achat de cartes Bi-technologies MIFARE 1K + Desfire vierges