



1C avenue des Frères Lumière – CS 78242 – 69372 Lyon cedex 08

Direction de l'Immobilier et de la Logistique

Direction du Numérique

ACCORD-CADRE DE TRAVAUX

MARCHÉ UJM 2025-32

TRAVAUX D'EXTENSION ET MAINTENANCE DU SYSTÈME DE CONTRÔLE D'ACCÈS DE L'UNIVERSITÉ JEAN MOULIN LYON 3

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES
(CCTP)

ARTICLE 1. OBJET DE LA CONSULTATION – DISPOSITIONS GÉNÉRALES	4
1.1. IDENTIFICATION DU POUVOIR ADJUDICATEUR.....	4
1.2. OBJET DU MARCHÉ.....	4
1.3. LIEUX D’EXECUTION.....	5
1.4. ORGANISATION DE LA MAITRISE D’OUVRAGE	5
1.5. EXPRESSION DES BESOINS	5
1.6. CONTRAINTES SPECIFIQUES	6
1.6.1. <i>Contraintes d’infrastructure</i>	6
1.6.2. <i>Maîtrise des solutions présentes à l’université</i>	6
1.6.3. <i>Périodes d’ouverture et fermeture</i>	6
1.6.4. <i>Contraintes de nettoyage</i>	6
1.6.5. <i>Respect des règles de l’université Jean Moulin Lyon 3</i>	6
1.7. DECOMPOSITION EN LOTS.....	7
1.8. GARANTIES.....	7
ARTICLE 2. OBLIGATIONS RÉGLEMENTAIRES	7
2.1. RESPECT DES LEGISLATIONS APPLICABLES LIEES A L’INSTALLATION.....	7
2.1.1. <i>Loi Informatique et Libertés</i>	7
2.1.2. <i>Secret professionnel, protection des données sensibles</i>	7
2.1.3. <i>Lois, règlements, normes</i>	8
2.1.4. <i>Propriété des données, accès à la base de données</i>	8
2.2. RESPECT DES LEGISLATIONS APPLICABLES LIEES AU BATIMENT	8
2.2.1. <i>Bâtiment ERP</i>	8
2.2.2. <i>Accessibilité</i>	8
ARTICLE 3. SÉCURITÉ DES BIENS ET DES PERSONNES	8
3.1. RESPONSABILITE GENERALE.....	9
3.2. COACTIVITE	9
3.3. CARTE PROFESSIONNELLE	9
ARTICLE 4. SÉCURITÉ INFORMATIQUE	9
4.1. CONFORMITE AUX NORMES DE SECURITE ET D’HOMOLOGATION	9
4.2. COMMUNICATION DE LA SOLUTION DE CONTROLE D’ACCES	10
4.3. CONNEXION DU TITULAIRE A LA SOLUTION DE CONTROLE D’ACCES.....	10
4.4. BADGE DU TITULAIRE POUR LA SOLUTION DE CONTROLE D’ACCES.....	11
ARTICLE 5. SPÉCIFICATIONS TECHNIQUES DU SYSTÈME DE CONTRÔLE D’ACCÈS	11
5.1. GENERALITES	11
5.2. TYPE D’HEBERGEMENTS DE LA SOLUTION.....	12
5.2.1. <i>Solution hébergée en interne (pour information)</i>	12
5.3. POSTES D’EXPLOITATION	12
5.4. ENROLEUR/ENCODEUR DE BADGE	13
5.5. PERSONNALISATION DES BADGES	13
5.6. FONCTIONNALITES	13
5.7. SUPERVISION GRAPHIQUE ANIMEE.....	15
5.8. OUVERTURE ET EVOLUTIVITE DU LOGICIEL	16
5.8.1. <i>Interactivité avec les applicatifs de ressources humaines ou autres</i>	16
5.8.2. <i>Connecteur LDAP</i>	17
5.8.3. <i>Connecteur AD ou Azur AD</i>	17
5.9. GESTION MULTISITES (CLOISONNEMENT MULTI-SOCIETES)	17
5.10. PARTAGE DE ZONE COMMUNE.....	17
5.11. DEPLOIEMENT ET EVOLUTION POSSIBLES.....	17
5.11.1. <i>Gestion des visiteurs</i>	18
5.11.2. <i>Borne d’accueil</i>	18
ARTICLE 6. MATÉRIEL DE TERRAIN.....	19

6.1. TETE DE LECTURE ARD.....	20
6.2. DEPLOIEMENT MATERIEL POSSIBLE -	20
6.2.1. Caméra LAPI Tatille.....	20
6.2.2. Adaptation avec des supports d'identification tiers	21
6.2.3. Module D1 Carte d'interface CAN Lecteur	21
6.2.4. Clavier à code.....	21
6.2.5. Télécommande HF	22
6.2.6. Tête de lecture BLE ou QR Code	22
ARTICLE 7. ACCÈS « ONLINE ».....	22
7.1. LES ROUTEURS DE COMMUNICATION	23
7.2. LES BEQUILLES AX SIMONS VOSS	23
7.3. LES BEQUILLES SMARTHANDLE AX ADVANCED.....	24
7.4. SMARTLOCKER AX DE SIMONS VOSS	24
7.5. LES CYLINDRES AX DE SIMONS VOSS.....	24
7.6. CADENAS AX DE SIMONS VOSS	25
7.7. BADGES	26
ARTICLE 8. DÉPLOIEMENT POSSIBLE - LES IDENTIFIANTS VIRTUELS	26
ARTICLE 9. PRESTATIONS RELATIVES À LA PROPOSITION FINANCIÈRE.....	27
9.1. ÉTABLISSEMENT DU DEVIS.....	27
9.2. ANNEXE 2A A L'ACTE D'ENGAGEMENT - FRAIS GENERAUX	27
9.2.1. Main d'œuvre.....	27
9.2.2. Déboursé fournitures	28
9.2.3. Déplacement.....	28
9.3. ANNEXE 2B A L'ACTE D'ENGAGEMENT – BPU BORDEREAUX DES PRIX UNITAIRES	28
9.3.1. Partie Contrôle d'accès : fourniture seule	28
9.3.2. Partie Contrôle d'accès : Fourniture pose et mise en service	28
9.3.3. Partie équipement informatique et logiciels.....	29
9.3.4. Partie électricité Contrôle d'accès.....	29
9.4. ANNEXE 2C A L'ACTE D'ENGAGEMENT - RABAIS	29
9.5. PLANNING	30
9.6. ÉTUDES.....	30
9.7. EXECUTION DES PRESTATIONS.....	30
9.8. NETTOYAGE DES ZONES DE TRAVAUX	31
9.9. DOSSIER DES OUVRAGES EXECUTES	31
9.10. RECEPTION DES OUVRAGES	31
ARTICLE 10. PRESTATIONS RELATIVES À LA DÉCOMPOSITION DE PRIX GLOBAL ET FORFAITAIRE	31
10.1. ANNEXE 3 A L'ACTE D'ENGAGEMENT - MAIN D'ŒUVRE	32
10.1.1. Maintenance Préventive	32
10.1.2. Maintenance corrective et service d'astreinte	33
10.1.3. Formation.....	34
10.2 ANNEXE 3 A L'ACTE D'ENGAGEMENT - LOGICIEL	35
10.2.1 Ard Access	35
10.2.2 UTL et équipements radio	36
10.3 ANNEXE 3 A L'ACTE D'ENGAGEMENT - MATERIEL.....	36
10.3.1 Base de quantification.....	36
10.3.2 Unité de traitement local UTL	37
10.3.3 Système radio.....	38
10.3.4 Verrouillage de porte	38
10.3.5 Pilotage d'équipement embarqué.....	39
10.4 GESTION DE LA MAINTENANCE	40
10.4.1 GMAO.....	40
10.4.2 Rapport de visite de maintenance.....	40
10.4.3 Tenue de la documentation du système.....	40

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)

ARTICLE 1. OBJET DE LA CONSULTATION – DISPOSITIONS GÉNÉRALES

1.1. Identification du pouvoir adjudicateur

Personne publique contractante : L'Université Jean Moulin Lyon 3

Représentant du pouvoir adjudicateur, en vertu de l'article L.712-2 du Code de l'Education (loi du 10 août 2007), et de l'article 5 des statuts de l'Université Jean Moulin Lyon 3 adoptés en Conseil d'Administration du 6 juillet 2015 par délibération n° D2015-07-10-Ins : Le Président de l'Université

Personne habilitée à recevoir les documents devant être adressés au pouvoir adjudicateur : La Directrice des Affaires Financières et des Achats – DGSA-DAFA ou La Responsable du Service des Achats.

Comptable assignataire des paiements : L'Agent Comptable de l'Université.

1.2. Objet du marché

Le patrimoine de l'université Jean Moulin est étendu (près de 120 000m²) et réparti sur 3 sites géographiques : les sites de la Manufacture des Tabacs et le site des Quais à Lyon et le site de la Charité à Bourg en Bresse.

En 2019, un état des lieux a fait apparaître l'hétérogénéité des systèmes de contrôle d'accès. Celui-ci a permis l'élaboration d'un plan d'actions pluriannuel de déploiement incluant des installations nouvelles, des extensions et des remises en état homogènes, programmées sur les années à venir.

Le présent marché d'installation et de maintenance de contrôle d'accès permet de décliner le plan d'actions, afin de poursuivre l'homogénéisation des systèmes en place avec comme objectif à terme un système unique, se référant à la base RH de l'université et aux autres systèmes d'information de l'établissement.

La solution retenue et implantée à l'université est la solution ARD ACCESS de l'entreprise ARD. Cette solution est couplée à la gamme SMARTINTEGO de l'entreprise SIMONSVSOS.

L'Université confie donc au(x) titulaire(s), qui accepte(nt) aux conditions énumérées ci-dessous :

- La fourniture des équipements du contrôle d'accès ;
- La fourniture des logiciels de gestion de ces équipements conformément aux fonctionnalités attendues ;
- La mise en œuvre des solutions validées ;
- La fourniture des prestations associées ;
- La maintenance des équipements physiques et logiciels installés ;
- L'installation des nouveaux équipements.

Le présent cahier des charges répond à plusieurs exigences :

- Uniformiser les systèmes et les caractéristiques techniques des différents équipements ;
- Permettre aux usagers d'accéder simplement dans un ou plusieurs bâtiments de l'université ;
- Permettre aux personnes habilitées en cas d'urgence d'intervenir durant les périodes de fermeture (congés) et en dehors des heures d'ouverture au public ;
- Maintenir la gestion des différents accès au niveau le plus judicieux (groupe de personnels, direction, composantes, enseignants...) ;
- Avoir des procédures communes et connues de tous ;
- Permettre une maintenance réactive et un déploiement opérationnel ;
- Être en conformité avec les différentes réglementations (déclarations informatiques et libertés, code ERP, accessibilité, RGPD etc.).

Par ailleurs, le ou les titulaire(s) a (ont) une obligation de résultat et de qualité de service envers les usagers consistant à garantir, pendant toute la durée du marché, des conditions optimales d'intervention, de fonctionnement et de sécurité des installations.

Ces prestations, fournitures et prestations intellectuelles permettront de satisfaire aux besoins de l'Université Jean Moulin Lyon 3 tels que décrits dans le présent document, mais également d'anticiper et répondre aux besoins futurs.

Le titulaire est réputé connaître parfaitement les installations qu'il prend en charge ou il devra démontrer à travers sa candidature ses compétences pour la mise en œuvre et la maintenance d'équipements du fabricant ARD. Cette démonstration peut se faire par la fourniture, lors de la remise de l'offre, de certifications, formations....

Les installations déployées sur les sites sont rattachées au système ARD ACCESS de la société ARD. L'application multi-site supervise l'ensemble des sites et gère l'ensemble des lecteurs de badges filaires, radios ...

L'application ARD ACCESS assure la supervision des installations, permet la programmation centralisée ou locale des automatismes, la configuration des équipements de terrain et le paramétrage des profils d'accès.

L'application est hébergée sur l'infrastructure virtualisée des services centraux de l'université Jean Moulin Lyon 3 (UJM Lyon 3).

Les postes de gestion locale, implantés sur les différents sites, communiquent en IP en mode « Full web » avec l'application.

En conséquence, à partir de cette prise en charge, le titulaire du marché renonce à faire état des difficultés provenant de la non connaissance des produits, logiciels, de la qualité du matériel, de l'exécution et la mise en œuvre de produits similaires et de la conformité des installations.

Par ailleurs, le présent CCTP ne pouvant contenir l'énumération rigoureuse et la description de tous les matériaux, ouvrages, détails ou dispositifs, il reste entendu que seront compris dans le prix proposé, non seulement toutes les prestations indiquées aux pièces du marché, mais aussi celles implicitement nécessaires pour rendre l'ouvrage conforme à sa destination, à son parfait achèvement suivant toutes les règles de l'Art, des règlements et normes en vigueur.

1.3. Lieux d'exécution

- Manufacture des Tabacs - 1 avenue des Frères Lumière, 69008 Lyon ;
- Palais de l'Université - 15 quai Claude Bernard, 69007 Lyon ;
- Palais de la Recherche - 18 rue Chevreul, 69007 Lyon ;
- Bâtiment Cavenne - 28 rue Cavenne, 69007 Lyon ;
- Bâtiments Athéna - 74 rue Pasteur, 69007 Lyon ;
- Bâtiments Dugas - 7 rue Chevreul, 69007 Lyon ;
- IUT Jean Moulin - 88 rue Pasteur, 69007 Lyon ;
- MILC - 35 rue Raulin, 69007 Lyon ;
- Site de la Charité - 2 rue du 23e R.I, 01000, Bourg-en-Bresse.

1.4. Organisation de la maîtrise d'ouvrage

La maîtrise d'ouvrage est assurée conjointement par la Direction de l'Immobilier et de la Logistique (DIL), et la Direction du Numérique (DNUM) de l'Université Jean-Moulin Lyon 3.

Au sein de ces services, le responsable cellule électricité et systèmes automatisés, le responsable du Pôle exploitation maintenance et le responsable du pôle métiers, sont les interlocuteurs exclusifs de ce marché. Le prestataire ne recevra de consigne de personne d'autre.

1.5. Expression des besoins

Le présent document (CCTP) a pour but de préciser la nature et l'étendue des prestations qui devront être mises en œuvre pour satisfaire les demandes de l'Université Jean Moulin Lyon 3.

Le candidat est invité à se reporter à :

- 1) L'annexe 2 *Proposition financière (constitué de trois onglets)* de l'acte d'engagement :

- a) A - Frais généraux
- b) B - BPU
- c) C – Rabais

2) L'annexe 3 DPGF de l'acte d'engagement (forfait payé à terme échu au trimestre)

Les quantités commandées sur la base de ce DPGF sont susceptibles d'évoluer chaque année. En effet, les quantités renseignées dans le présent document sont celles correspondant à la première année d'exécution du marché.

Les articles 9 et 10 du présent CCTP précisent le niveau de prestation attendu.

1.6. Contraintes spécifiques

1.6.1. Contraintes d'infrastructure

Le titulaire sera réputé avoir pris connaissance des contraintes techniques de tous ordres imposées par le système d'information existant de l'Université Jean Moulin Lyon 3 et en avoir tenu compte dans sa proposition.

Le titulaire sera réputé avoir pris connaissance des contraintes techniques de tous ordres imposées par la morphologie des divers bâtiments (contrainte architecturale, accès, grande hauteur...) et en avoir tenu compte dans sa proposition.

1.6.2. Maîtrise des solutions présentes à l'université

L'université est dotée de la solution ARD ACCESS de l'entreprise ARD. Cette solution est couplée à la gamme SMARTINTEGO de l'entreprise SIMONSVOS. La gestion de ces deux solutions, sur les volets technique et numérique, nécessite de la part des intervenants une capacité et une connaissance avérées.

Afin de se prémunir d'éventuels désordres causés par le titulaire, il est demandé aux candidats de fournir dès la remise des offres les attestations de formation dispensées par les fabricants ARD et SIMONSVOS. La formation devra dater de moins d'un an.

1.6.3. Périodes d'ouverture et fermeture

L'université est ouverte toute l'année pour travaux avec un système d'astreinte permettant aux entreprises d'intervenir y compris pendant les deux fermetures. Des fermetures administratives à Noël et en été permettent un travail de qualité sans interférence avec le public.

Une mobilisation estivale (juillet et août) et aux vacances de Noël (20 décembre au 6 janvier environ) doit donc être prise en compte par le prestataire, qui ne pourra faire valoir des absences d'effectifs ou des durées de chantiers plus longue sur ces périodes.

1.6.4. Contraintes de nettoyage

L'université possède un marché de nettoyage avec une société. Le matériel est entreposé dans des locaux dits « Ménage ». Il sera formellement interdit au prestataire du marché Contrôle d'accès d'utiliser le matériel sur site. L'entreprise doit laisser des chantiers/interventions propres et doit être équipée personnellement de l'ensemble du matériel dont elle a besoin, y compris pour les moyens d'accès.

1.6.5. Respect des règles de l'université Jean Moulin Lyon 3

Les dispositions du décret n° 92-158 du 20 février 1992 sont applicables.

Chaque année, un plan de prévention écrit sera rédigé par l'Université et le titulaire avant le commencement des prestations, à l'issue d'une visite préalable du chantier.

Le plan de prévention décrira notamment les risques particuliers encourus et les mesures de prévention envisagées (cf. article 3.1)

Le personnel doit obligatoirement être muni d'une carte d'identité de son entreprise.

Dans le cadre du travail en ERP, le titulaire doit protéger ses installations, tout comme le public du site occupé, avec tous moyens qui lui sembleront adaptés et en cohérence avec le plan de prévention établi en début d'année, et ce à ses propres frais (balisages, protections affichages...).

1.7. Décomposition en lots

Ce marché est un marché unique comportant des prestations d'installation et de maintenance. Ces opérations distinctes sur le terrain, mais liées par un même objectif de résultat et de bon fonctionnement des installations font partie intégrante de ce même marché. Elles seront décrites aux paragraphes 9 et 10 de ce CCTP.

1.8. Garanties

Le titulaire assure une garantie pièces, main d'œuvre, et déplacement pour la fourniture de sa solution pour une durée minimum d'un an, comme partie intégrante de ses prix. Les modalités de garanties des logiciels sont définies par l'article 8 du CCAP.

Pour chaque prestations les garanties seront les suivantes :

Les logiciels et UTL fournis sont réputés garantis pour une période de 12 mois après leur mise en exploitation, sauf pour les failles de sécurité et bugs qui devront être corrigées jusqu'à la fin de vie de la version majeure du logiciel. Chaque version majeure devra avoir un cycle de vie d'au moins quatre ans. Pour information l'université Jean Moulin possède actuellement la Version V2.13.4 ARD ACCESS.

Point de départ de garantie : La date de réception définitive des prestations/interventions constitue le point de départ des garanties.

ARTICLE 2. OBLIGATIONS RÉGLEMENTAIRES

Plusieurs réglementations sont applicables à ce type de prestations, certaines liées à l'installation elle-même, d'autres au type de bâtiment dans lequel elle est installée.

2.1. Respect des législations applicables liées à l'installation

2.1.1. Loi Informatique et Libertés

Le titulaire s'engage à ce que la solution proposée et les modalités de mise en œuvre et d'utilisation satisfassent aux obligations légales dont dispose la loi informatique et libertés du 6 janvier 1978 modifiée, notamment aux articles 34 (resp. 35) portant obligation au responsable de traitement (responsabilité au sous-traitant) de préserver la sécurité et la confidentialité des données, ceci dès la notification du marché.

Le titulaire s'engage à transmettre toutes les informations permettant de mettre en évidence sa conformité aux dispositions du Règlement UE n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données) et plus particulièrement les article 23, 28 et 29.

En tant que sous-traitant, le titulaire fournira à l'Université Jean Moulin Lyon 3 tous les éléments et documents contractuels nécessaires à l'accomplissement de ces formalités dans un délai de 15 jours calendaires à compter de la demande de l'Université Jean Moulin Lyon 3.

2.1.2. Secret professionnel, protection des données sensibles

Le titulaire s'engage à respecter les règles du secret professionnel pour ce qui concerne l'accès aux

Informations personnelles auxquelles il accèderait dans le cadre de sa mission. Plus généralement, il s'engage à la plus grande discrétion sur toutes les informations auxquelles il aura accès durant l'exercice de sa mission.

Cette obligation de secret professionnel et de discrétion continue devra s'exercer au-delà de la durée du marché.

2.1.3. Lois, règlements, normes

Le titulaire veillera à respecter les lois et règlements qui s'appliquent dans le cadre de l'exercice de sa mission. En aucun cas, le titulaire ne doit contrevenir à ceux-ci. Il veillera également à ce que les matériels installés dans le cadre de sa prestation respectent les normes de sécurité en vigueur. Il veillera également à ce que ces matériels respectent toutes les réglementations en matière de respect de l'environnement.

Outre les prescriptions contenues au présent CCTP, tous les ouvrages et matériaux seront soumis aux prescriptions des documents suivants :

- Documents Techniques Unifiés (DTU),
- Normes françaises AFNOR.

L'entreprise devra obligatoirement tenir compte dans son offre de prix de l'organisation de la coordination de la sécurité et de la protection de la santé de ses travailleurs. Ces obligations sont fixées dans la loi 93-1418 du 31 décembre 1993 (L 235.1 à 5) et le décret 94-1159 du 26 décembre 1994 (R 238.3 à 10 et R 238.16 à 19).

2.1.4. Propriété des données, accès à la base de données

En tout état de cause l'Université Jean Moulin Lyon 3 reste propriétaire exclusive des données et doit pouvoir en disposer librement dans un format exploitable. La structure des bases de données mises en œuvre, doit être connue des services de l'Université Jean Moulin Lyon 3 et permettre la portabilité vers une autre solution logicielle. La libre disponibilité des données pour l'Université Jean Moulin Lyon 3 fait donc partie intégrante de l'offre du prestataire. Le titulaire est tenu de respecter l'intégralité des propositions faites dans son offre (notamment son Modèle Conceptuel de Données – MCD).

Le prestataire choisi s'engage à respecter les dispositions du RGPD. Il doit communiquer les modalités de transfert et sécurisation des données transmises par l'Université. Le prestataire doit informer le pouvoir adjudicateur de la manière dont il conserve les données et le temps de conservation.

Par ailleurs, s'il recourt aux sous-traitants, le prestataire devra expliquer la manière dont sera gérée cette sous-traitance (cf. annexe 6 « RGPD » à l'AE).

2.2. Respect des législations applicables liées au bâtiment

Pour chaque installation, le titulaire devra tenir compte du statut du ou des bâtiments dans lesquels cette installation sera développée, et appliquer pour chacun des types de bâtiment la réglementation qui lui est propre.

2.2.1. Bâtiment ERP

Pour les bâtiments recevant du public ERP, le titulaire devra respecter le règlement de sécurité contre l'incendie relatif aux établissements recevant du public, et devra prendre connaissance, pour chaque bâtiment, de ces caractéristiques : son type et sa catégorie.

2.2.2. Accessibilité

Pour tous les bâtiments, la loi pour l'égalité des droits et des chances, la participation et la citoyenneté de personnes handicapées s'appliquent. En ce sens le titulaire s'engage à positionner les périphériques de porte (lecteur de badge, poigné, bouton...) conformément à cette réglementation.

ARTICLE 3. SÉCURITÉ DES BIENS ET DES PERSONNES

3.1. Responsabilité générale

Avant toute intervention du titulaire sur site, il sera établi, conjointement entre le titulaire et l'Université Jean Moulin Lyon 3, un plan de prévention des risques définissant :

- L'ensemble des risques liés à l'intervention ;
- Les mesures mises en place pour supprimer ou maîtriser ces risques ;
- Les acteurs " titulaire, université, tierce personne" chargée de mettre en œuvre ces mesures.

La surveillance des opérations sera assurée par le titulaire du présent marché qui devra, en outre, établir tous les dispositifs de signalisation et de sécurité dans l'emprise du chantier. À aucun moment, les accès engageant le chantier ne seront encombrés.

Le titulaire s'engage :

- à enseigner au personnel placé sous son autorité les diverses consignes de sécurité générales et particulières propres à l'établissement et à contrôler fréquemment que ces consignes sont parfaitement connues des intéressés ;
- à mettre à la disposition du personnel placé sous son autorité des outils, matériels et moyens de prévention conformes à la réglementation en vigueur et à leur faire connaître les consignes liées à leur emploi ;
- à faire savoir à son personnel que les prestations seront arrêtées si les consignes de sécurité prévues n'étaient pas respectées ;
- à ne consommer ni alcool ni cigarette dans les locaux de l'université ;
- à ne pas emprunter ou utiliser les équipements de l'université (plate-forme, échafaudage).

Toute disposition sera prise par le titulaire pour les éventuelles prestations en hauteur.

3.2. Coactivité

En cas de coactivité avec d'autres entreprises, l'Université Jean Moulin Lyon 3 se réserve la possibilité de désigner un coordonnateur en matière de sécurité et de protection de la santé, ou CSPS.

3.3. Carte professionnelle

Le personnel doit obligatoirement être muni d'une carte d'identité de son entreprise.

ARTICLE 4. SÉCURITÉ INFORMATIQUE

L'ensemble de la solution d'accès doit respecter les recommandations du guide de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), i.e. les recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection annexé au présent CCTP (cf. annexe 2 du CCTP).

En particulier le titulaire devra appliquer les mesures de niveau L1 de l'annexe D contenu dans le guide ANSSI (cf. annexe 2 du CCTP).

En plus des recommandations précédentes, une vigilance particulière devra être apportée sur les points spécifiques concernant la sécurité informatique, des points suivants :

4.1. Conformité aux normes de sécurité et d'homologation

Le logiciel proposé doit être conforme aux normes internationales de sécurité de l'information, en particulier la norme ISO/IEC 27001 et au règlement général sur la protection des données RGPD. Le fournisseur doit démontrer que le logiciel et ses processus de développement respectent les critères suivants :

- Gestion de la Sécurité de l'Information : Le fournisseur doit disposer d'une documentation complète de la politique de sécurité, des processus et des contrôles en place pour protéger les données.
- Évaluation et Gestion des Risques : Le logiciel doit avoir été soumis à une évaluation des risques de sécurité, avec des mesures de protection adaptées pour atténuer ces risques. Le fournisseur

doit fournir des preuves de cette évaluation, incluant les méthodologies employées et les résultats obtenus.

- Contrôles de Sécurité Intégrés : Le logiciel doit inclure des contrôles de sécurité, tels que le contrôle d'accès, la gestion des incidents de sécurité, la cryptographie, la gestion des vulnérabilités, et la protection des données en transit et au repos.
- Homologation de Sécurité : Le fournisseur doit être en mesure de fournir tous les documents nécessaires pour l'obtention d'un accord d'homologation de sécurité, conformément au décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. Cela inclut, mais n'est pas limité à, des rapports de tests de sécurité, des audits de conformité, et des déclarations de sécurité.
- Maintien et Mise à Jour de la Sécurité : Le fournisseur doit s'engager à maintenir et mettre à jour régulièrement le logiciel pour assurer sa conformité continue aux normes de sécurité, y compris la gestion proactive des vulnérabilités et la fourniture de correctifs de sécurité en temps opportun.

4.2. Communication de la solution de contrôle d'accès

La transmission des informations du système de contrôle d'accès se fait sur des VLANs dédiés à ce système, dont la gestion est assurée par la DNUM. Le titulaire devra fournir les informations nécessaires à l'établissement d'un diagramme de flux. Cette base servira à la DNUM qui se chargera de la configuration des éléments actifs. Ces informations comprendront notamment :

- Les adresses IP source et destination ;
- Les adresses MAC
- Les flux source et destination ;
- Les ports origine et destination ;
- Les protocoles ;
- Les débits ;
- Les fréquences (flux permanent ou ponctuel) ;
- Les remarques éventuelles ;
- Tout paramétrage nécessaire pour assurer le fonctionnement sécurisé de la solution...

4.3. Connexion du titulaire à la solution de contrôle d'accès

L'université confiera au titulaire les vecteurs techniques sécurisés permettant de se connecter à la solution de contrôle d'accès pour réaliser les prestations prévues au présent CCTP :

- Identifiant nominatif
- Accès sécurisé par VPN

Pour cela, le titulaire fournira à l'université la liste nominative des personnes qui agiront sur le système ainsi que les informations suivantes :

- NOM
- Prénom
- Entreprise
- Fonction
- Numéro de téléphone
- Adresse courriel

Le titulaire devra mettre à jour cette liste chaque fois que cela sera nécessaire, de sa propre initiative. En outre, le titulaire assume la responsabilité de toute action réalisée par les intervenants figurant sur cette liste, y compris les sous-traitants, co-traitants, partenaires..., pour lesquels il aurait demandé la création d'accès. En cas de divulgation d'identifiant (quelles qu'en soit les circonstances) le titulaire s'engage à demander sans délais la suspension des accès auprès des services de l'université.

Pour la création des comptes informatiques Il sera demandé au titulaire de signer les documents dont un exemple figure en annexe 3 et 4 du CCTP :

- Charte d'accès distant aux ressources informatiques de l'Université Jean Moulin – Lyon 3 ;
- Engagement de confidentialité prestataire extérieur.

4.4. Badge du titulaire pour la solution de contrôle d'accès

L'université confiera au titulaire un badge d'accès permettant la réalisation des prestations prévues au présent CCTP. Chaque intervenant disposera d'un badge nominatif. Le support physique pourra soit être fourni par l'université, soit directement configuré avec la carte professionnelle de l'intervenant (sous réserve de compatibilité).

Pour cela, le titulaire fournira à l'université la liste nominative des personnes qui agiront sur le système ainsi que les informations suivantes :

- NOM
- Prénom
- Entreprise
- Fonction
- Numéro de téléphone
- Adresse de courriel
- Identifiant technique de la carte professionnel

Le titulaire devra mettre à jour cette liste chaque fois que cela sera nécessaire de sa propre initiative.

En outre le titulaire assume la responsabilité de toutes actions réalisées par les intervenants figurant sur cette liste y compris les sous-traitants ; co-traitants ; partenaires... pour lesquels il aurait demandé un badge. En cas de perte du badge (quel qu'en soit les circonstances) le titulaire s'engage à demander sans délai la suspension des accès auprès des services de l'université.

Afin d'accomplir sa mission les accès par badge du titulaire sont extrêmement permissifs. Compte tenu des droits d'accès attachés aux cartes confiées au titulaire, ce dernier s'engage à une vigilance maximale. Il est rappelé que chaque intervenant agit en son nom et s'interdit donc de confier son badge à quiconque ce soit. D'autre part les autorisations d'accès attachées à ce badge ne dispensent en aucun cas l'intervenant de se présenter auprès du poste de sécurité ou du donneur d'ordre avant chaque intervention.

ARTICLE 5. SPÉCIFICATIONS TECHNIQUES DU SYSTÈME DE CONTRÔLE D'ACCÈS

Un système de contrôle des accès physiques est un dispositif ayant pour objectif de filtrer les flux d'individus souhaitant pénétrer à l'intérieur d'un site, d'un bâtiment ou d'un local. Un système de contrôle d'accès permet de restreindre l'accès selon des zones, des plages horaires prédéfinies et avec une traçabilité intégrale des déplacements. Il est constitué de moyens permettant d'autoriser les entrées et sorties de zones sensibles aux seules personnes qui ont le droit d'y accéder.

Un système de contrôle d'accès assure trois fonctions primaires :

- L'identification et l'authentification ;
- Le traitement des données ;
- Le déverrouillage.

Ces fonctions sont assurées en chaque point où l'accès est contrôlé.

Dans le cas d'un système de contrôle d'accès utilisant des technologies sans contact, quatre éléments support principaux interviennent :

- Le badge (ou support similaire) ;
- Le lecteur (tête de lecture) ;
- L'unité de traitement local (UTL) ;
- Le serveur de gestion du système.

5.1. Généralités

Le système de contrôle d'accès logiciel actuellement en place sur le site : **solution ARD ACCESS de la société ARD** est basé sur une technologie de carte à lecture sans contact au standard Mifare Desfire (ISO 14443-A). Il reposera sur le réseau Ethernet TCP/IP de l'établissement, sur lequel seront raccordées les Unités de traitement Locales (UTL). Le réseau Ethernet TCP/IP sera programmé avec un réseau virtuel (VLAN) dédié à la sûreté et par conséquent inaccessible depuis le reste du réseau informatique.



Les unités de contrôle doivent permettre de déployer des lecteurs de badges **RFID filaires** (gamme de lecteur ARD C3 ou équivalent) et **radio** (gamme Smartintego de SimonsVoss ou équivalent).

Les fonctionnalités à assurer sont à minima :

- Suivre en temps réel l'état du dispositif (alarmes et défauts techniques),
- Suivre en temps réel les mouvements d'entrée/sortie des accès,
- Consulter les différents journaux historiques : accès, alarmes techniques, maintenance et événements système.

Ces fonctionnalités sont accessibles depuis un simple navigateur internet sur PC.

5.2. Type d'Hébergements de la solution

5.2.1. Solution hébergée en interne (pour information)

Solution déjà existante à l'université : Ce mode d'hébergement consiste à installer le logiciel sur un serveur de l'infrastructure réseau du site, la solution pourra être installée sous la forme d'une machine virtuelle sur les serveurs existants, fournie par le client, ou encore sur un serveur déjà prêt à l'emploi fourni par le fabriquant.

5.3. Postes d'exploitation

La solution devra obligatoirement être orientée « client léger », **aucune installation du logiciel ne sera réalisée sur les postes d'exploitation et de supervision**. Ceux-ci se connecteront au serveur par l'intermédiaire d'un navigateur après saisie du Login et du Mot de passe de l'exploitant.

Les facultés minimales offertes sont :

- La gestion du fichier des porteurs de carte,
- La gestion de l'historique des événements,
- La surveillance de l'état des portes (fermée, ouverte, ouverture prolongée, forcée),
- L'enregistrement, l'archivage et l'édition des événements,
- La gestion de groupes d'utilisateurs,
- La gestion de zones de sûreté,
- L'intégration de paramétrages calendaires et horaires prenant en compte les jours fériés,

Configuration minimum du ou des postes client :

- Processeur Intel core i3 minimum ou équivalent,
- RAM de 8 Go minimum,
- Disque dur de 80 Go minimum,
- Ecran 19" (21" conseillé pour les postes de supervision),

- 1 Port Ethernet 100/1000 Base T,
- 1 Port USB disponible,
- Windows 10, 32 ou 64 bits

Le Maître d'Ouvrage fournira les postes de gestion ; le soumissionnaire décrira les caractéristiques et performances du matériel nécessaire.

5.4. Enrôleur/encodeur de badge

L'enrôleur de badge sera composé d'un lecteur de table connecté sur le port USB du poste de gestion ; il permettra d'enrôler le badge et, selon le contexte de l'application, d'appeler la fiche du porteur, de visualiser ses droits d'accès...



5.5. Personnalisation des badges

Le module de personnalisation des badges devra posséder les fonctionnalités suivantes :

- Préparation du fond de carte (possibilité de modification grâce à l'éditeur intégré),
- Importation du logo, nom, prénom, numéro de matricule, etc...
- Impression directe sur l'imprimante à sublimation,
- Impression de pictogrammes.

Imprimante Zenius Expert d'Evolis ou équivalent avec à minima :

- Impression sublimation thermique simple face couleur et monochrome, bord à bord, pour cartes plastique au format ISO CR80 - ISO 7810 (53,98 mm x 85,60 mm),
- Résolution standard 300 x 300 dpi,
- Encodeur de cartes RFID intégré,
- Environ 140 cartes/h (couleur YMCKO),
- Chargeur et réceptacle de 50 cartes (en 0,76mm),
- Raccordement USB et Ethernet.



1 Kit de nettoyage pour imprimantes Evolis

- Contenu : 5 cartes adhésives et 5 bâtonnets
- Fréquence entretien : Un nettoyage toutes les 1000 cartes



1 Ruban 5 panneaux YMCKOK pour imprimante Primacy 2

- Permet l'impression 200 cartes recto couleur avec overlay de protection et ver



5.6. Fonctionnalités

Le logiciel de contrôle d'accès sera en langue française.

Tous les logiciels et licences associées seront à charge du présent lot.

Le présent lot aura à sa charge la programmation du système de contrôle d'accès. Le logiciel de contrôle d'accès devra permettre à la fois de paramétrer, d'exploiter les badges et de visualiser des alarmes, défauts et états de fonctionnement du système sur des vues IHM représentant les plans du bâtiment par niveaux et par zones.

Le logiciel de supervision constituera un environnement graphique homogène, intégré et convivial.

Les informations remontées sur le logiciel de supervision seront affichées en temps réel sur des plans graphiques animés représentatifs du bâtiment (plans architectes éventuellement épurés pour une meilleure lisibilité). Il sera prévu 1 plan par niveau. Tous les niveaux seront intégrés dans le logiciel, y compris les niveaux non équipés de contrôle d'accès.

Le logiciel de supervision permettra l'horodatage et l'historisation de tous les événements dans une base de données située sur le serveur de contrôle d'accès.

Les fonctionnalités suivantes seront possibles :

- Visualisation du journal fil de l'eau de l'ensemble des événements survenant sur le système (changement d'état des équipements, apparition /disparition de défauts techniques, détection connexion opérateurs...),
- Horodatage des acquittements, heures et dates d'apparition, de disparition...,
- Gestion des profils opérateurs et déclaration de nouveaux opérateurs,
- Recherche en différé des données archivées en base de données, par date, types d'événement...,
- Impression des rapports de recherche.

Le système mis en œuvre permettra la gestion d'au minimum (sans ajout de licences complémentaires) de :

- 1 000 lecteurs de badges répartis sur un ou plusieurs sites ;
- 1 poste clients ;
- 100 000 badges.

A minima, les fonctionnalités suivantes seront disponibles sur le système :

➤ **Fonctionnalités propres au contrôle d'accès :**

- Création de badges ;
- Création de profils ;
- Gestion des visiteurs ;
- Gestion multi-badges (possibilité de gérer depuis une même fiche badge un nombre illimité d'identifiant : lecteur 13.56 MHz, QR code, smartphone, tags UHF parking, lecture de plaques...) ;
- Personnalisation et impression des badges ;
- Recherches par n° badges, nom, profils, événements... ;
- Visualisation de l'état de chaque porte sous contrôle d'accès (verrouillé, inhibé, effraction, porte ouverte trop longtemps, défaut...) ;
- Effectuer des commandes d'ouverture ponctuelles ou automatisées sur les portes, inhiber ou forcer les lecteurs depuis les plans synoptiques... ;
- Gestion d'effets sas ;
- Gestion de l'anti-pass-back (local et global), de l'anti-time-back ;
- Gestion intégrée de cylindres ou béquilles sans fil (en off-line et en on-line par l'intermédiaire de passerelles sans fil) ;
- Gestion intégrée des armoires à clé type TRAKA ;
- Comptage par zone ;
- Visualisation de l'état du système sur les plans graphiques ;
- Statistiques des passages et exports manuels ou automatisés par mail ou des fichiers à plats.

➤ **Fonctionnalités complémentaires :**

- Envoi automatique de courriels sur événement (détection intrusion, passage de badge interdit...) ;
- Gestion d'ascenseurs/monte-charge paramétrable avec asservissement des étages (ne nécessite aucune intervention technique pour modification du principe de fonctionnement) suivant niveau sélectionné sur le pupitre de commandes à prédestination/boîtiers à boutons et autorisation du contrôle d'accès ;
- Fonctionnement avec une application mobile ARD Mobile (ou équivalent) pour smartphone iOS ou Android avec notifications, supervision simplifiée et pilotage à distance.

➤ **Le système devra permettre les fonctionnalités suivantes :**

- Paramétrage de groupes d'utilisateurs,
- Paramétrage de tranches horaires,
- Programmation des jours fériés et des congés,
- Date de validité des badges,
- Archivage des événements,
- Sauvegarde des données depuis l'interface utilisateur,
- Plusieurs niveaux d'autorisation d'accès (minimum 4).

Les paramétrages seront faits de façon conviviale par le biais de fenêtres type Windows.

À chaque porteur de badge sera attribué un profil d'autorisation. Ce profil lui donnera accès à une porte ou à un ensemble de portes défini par jour de semaine ou jour d'exception dans des intervalles de temps graphiquement définissables. À tout moment, le profil d'un porteur de badge pourra être modifié manuellement ou automatiquement.

À chaque badge pourra être associé plusieurs profils différents de façon à limiter le nombre de profils nécessaire à l'exploitation du bâtiment. Néanmoins, le nombre de profils ne devra pas être limité par le logiciel afin de ne pas contraindre l'exploitant s'il souhaite faire évoluer le système.

Les synoptiques seront organisés selon une arborescence. Le sommet de cette arborescence comprendra une vue générale (Vue d'accueil) de présentation du bâtiment.

Les différents éléments du contrôle d'accès (portes contrôlées, issues de secours, contacts de portes...) apparaîtront sur les synoptiques représentant les différents niveaux du bâtiment sous la forme de symboles de couleur et animés.

Lors de l'apparition d'une alarme, le synoptique correspondant s'affichera automatiquement et le symbole du point en alarme passera en couleur rouge et clignotera.

L'anti-pass-back et anti-time-back devront pouvoir être définis sur certains lecteurs.

Le module de personnalisation des badges devra posséder les fonctionnalités suivantes :

- Préparation du fond de carte (possibilité de modification grâce à l'éditeur intégré),
- Importation du logo, nom, prénom, numéro de matricule, etc...,
- Impression directe sur l'imprimante à sublimation,
- Impression de pictogrammes.

5.7. Supervision graphique animée

En complément de la supervision classique, le logiciel supervisera toute l'installation de sûreté par une représentation de supervision de plans graphiques homogène, intégrée et conviviale et des vues IHM représentant les plans du bâtiment par niveaux et par zones.

Les plans Autocad exportés au format SVG pourront-être importés et exploités dans le gestionnaire de synoptiques.

Si besoin les systèmes suivants seront également supervisés par le système de contrôle d'accès :

- Centrale d'alarme avec périphériques NF&A2P ;
- Vidéosurveillance (interface avec le système de vidéosurveillance à prévoir).

Le logiciel de supervision constituera un environnement graphique homogène, intégré et convivial.

Les informations remontées sur le logiciel de supervision seront affichées en temps réel sur des plans graphiques animés représentatifs du bâtiment (plans architectes éventuellement épurés pour une meilleure lisibilité). Il sera prévu 1 plan par niveau. Tous les niveaux seront intégrés dans le logiciel, y compris les niveaux non équipés de contrôle d'accès.

Le logiciel de supervision permettra l'horodatage et l'historisation de tous les événements dans une base de données située sur le serveur de contrôle d'accès.

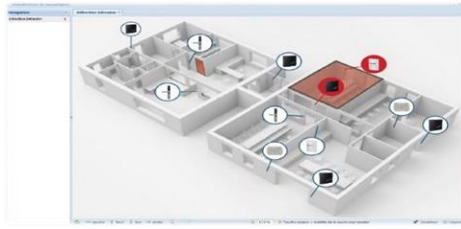
Les fonctionnalités suivantes seront possibles :

- Visualisation du journal fil de l'eau de l'ensemble des événements survenant sur le système (changement d'état des équipements, apparition /disparition de défauts techniques, détection connexion opérateurs...),
- Horodatage des acquittements, heures et dates d'apparition, de disparition...,
- Gestion des profils opérateurs et déclaration de nouveaux opérateurs,
- Recherche en différé des données archivées en base de données, par date, types d'événement...
- Visualisation de l'état de chaque porte sous contrôle d'accès (verrouillé, inhibé, effraction, porte ouverte trop longtemps, défaut...)
- Effectuer des commandes d'ouverture ponctuelles ou automatisées sur les portes, inhiber ou forcer les lecteurs depuis les plans synoptiques...
- Visualisation de l'état du système sur les plans graphiques.

Les synoptiques seront organisés selon une arborescence. Le sommet de cette arborescence comprendra une vue générale (Vue d'accueil) de présentation du bâtiment, la représentation graphique se fera sous forme de plans hiérarchiques et sous forme de tableau de bord

Les différents éléments du contrôle d'accès (portes contrôlées, issues de secours, contacts de portes...) apparaîtront sur les synoptiques représentant les différents niveaux du bâtiment sous la forme de symboles de couleur et animés qui par simple clic droit sur l'objet à commander autoriseront l'ouverture à distance.

Lors de l'apparition d'une alarme, le synoptique correspondant s'affichera automatiquement et le symbole du point en alarme passera en couleur rouge et clignotera.



5.8. Ouverture et évolutivité du logiciel

Le logiciel de contrôle d'accès pourra évoluer par l'ajout de fonctions (visiteurs, ...) et de connecteurs (intrusion, vidéosurveillance, ...).

La solution sera modulaire : l'ajout de périphériques sera aisé et sans impact sur la solution implantée ; l'ajout de plans animés, gestion de visiteurs ou autres fonctions sera possible.

Par ses connecteurs, la solution devra proposer des passerelles vers les systèmes de vidéosurveillance, d'anti-intrusion ou d'interphonie en proposant des scénarios différents suivant l'évènement remonté au système (actions caméras, ...).

Une liste de connecteurs de gestion du matériel ou de passerelles vers des applications tierces devra être disponible ou pouvoir être développée pour s'interfacer et se synchroniser avec le logiciel de contrôle d'accès :

- Gestion d'armoire à clé sécurisé (Traka, Ecos),
- Gestion des ascenseurs qui ont leur propre protocole (Kone, Mitsubishi),
- Authentification (SSO Azure AD, SSO CAS), pour permettre à ces systèmes informatiques de s'assurer de la légitimité de la demande d'accès,
- Gestion des calendriers (gestion emploi du temps ADE Campus, Octime, Pronote),
- Gestion et réservation de ressources (réservation de salle ARD Booking, accès visiteur pour salle de réunion Office 365, espace de coworking Cosoft , Heberg, ID Access Booking Web , Instant Booking Sharing Cloud, réservation de salle Affluence, Planitech),
- Importé et/ou exporté des usagers/utilisateurs vers ou depuis le logiciel de contrôle d'accès (import usagers ou/et utilisateur depuis annuaire AD ou Azure AD, import/export automatique CSV des usagers),
- Synchroniser la solution avec des Hyperviseurs ou des superviseur tiers (PRYSM, SMS Partner),
- Gestion de la GTB (Modbus TCP/IP),
- Gestion des parcs automobiles (Accor, Scheidt-Bachmann),
- Interaction avec la monétique (GEC monétique).

Le client restera propriétaire de ces données qui lui seront propres conformément au RGPD (Règlement Général sur la Protection des Données).

Le logiciel possèdera des fonctions d'exports permettant de générer des fichiers à plat qui eux, pourront être exploités par un autre logiciel et assurer l'interopérabilité.

5.8.1. Interactivité avec les applicatifs de ressources humaines ou autres

La capacité à échanger des données entre systèmes applicatifs est un impératif. Le logiciel de contrôle d'accès ARD Access ou équivalent devra garantir une parfaite synchronisation des différentes bases de données et d'éviter les saisies multiples : restauration, copieurs, distributeurs de boissons, gestion du parc automobile,

Le logiciel de contrôle d'accès ARD Access, devra mettre en œuvre un composant **ARD COM** ou équivalent pour intégrer une messagerie inter-applicative, intégrant les standards de communication avec les applications tierces et restant ouvert dans la mesure du possible.

Le logiciel de contrôle d'accès ARD Access ou équivalent devra pouvoir proposer les fonctionnalités suivantes :

- Web services SOAP pour interopérabilité avec logiciels tiers,

- Fonctions d'exports permettant de générer des fichiers à plat qui eux, pourront être exploités par un autre logiciel via de l'import/export (provisioning par échange de fichiers plats selon une structure de données ARD au format CSV),
- Provisioning par appel d'une requête, vue ou procédure stockée du système d'information (ex : système de ressources humaines) ...

5.8.2. Connecteur LDAP

Le logiciel ARD Access devra intégrer dans son offre un connecteur LDAP (LDAP ou Active Directory) afin d'automatiser la connexion au logiciel aux utilisateurs autorisés dans ARD Access et l'import des usagers.

5.8.3. Connecteur AD ou Azur AD

Le logiciel ARD Access devra intégrer dans son offre un connecteur Azur AD (Azure Active Directory) afin d'automatiser la connexion au logiciel aux utilisateurs autorisés dans ARD Access et l'import des usagers. Afin de renforcer la sécurité, l'authentification multi acteur basée sur les mécanismes Azur AD pourra être proposée en option.

La solution logicielle ARD Access pourra être provisionnée de plusieurs manières :

- CSV Simple ;
- CSV Multiple ;
- Requête SQL ;
- Requête LDAP ou AD ;
- API.

L'export CSV permettra de mettre à disposition des fichiers csv contenant les porteurs ou les groupes en fonction de l'abonnement sélectionné

5.9. Gestion multisites (cloisonnement multi-sociétés)

Pour des sites distants interconnectés, la solution intégrera l'option multisites. L'architecture proposée centralisera plusieurs installations sur un seul serveur de contrôle d'accès capable de gérer plusieurs sites ou bâtiments et de cloisonner les accès de connexion des utilisateurs.

Il suffit d'établir une liaison de type ETHERNET TCP/IP sécurisée afin d'assurer une communication avec le serveur de contrôle d'accès central installé sur le site principal avec les sites éloignés géographiquement ou séparés fonctionnellement (administration, Bourg en Bresse et les sites lyonnais...).

Matériel préconisé : connecteur ARD licence gestion multisites

5.10. Partage de zone commune

L'autorisation entre deux installations voisines différentes pour que les collaborateurs puissent accéder aux zones communes est rendu possible via un échange entre les deux serveurs de contrôle d'accès. Un import des porteurs, groupes, identifiants et accès autorisés depuis un serveur principal vers un autre serveur qui sera réalisé en temps réel.

L'un des 2 serveurs restera maître concernant la gestion de ses accès (PNG de l'accueil, les ascenseurs, les parkings, ...).

Matériel préconisé : connecteur ARD Master

5.11. Déploiement et évolution possibles

5.11.1. Gestion des visiteurs

La solution sera conçue pour renforcer la sécurité du site tout en améliorant l'organisation et l'image du service d'accueil.

La solution ARD Access ou équivalente proposera la gestion des visiteurs. Cette fonction permet la planification et la gestion des flux, sur le site contrôlé en accès, des personnes extérieures.

La fonctionnalité « gestion des visiteurs » proposera différents modules dont certains devront être débrayables afin de répondre au mieux aux exigences du Maître d'ouvrage :

- Les visites pourront être enregistrées à la volée ou planifiées par un organisateur. Le motif de la visite, les horaires prévus, les droits d'accès à attribuer aux visiteurs ou groupes de visiteurs associés à la visite seront mémorisés.
- Les visiteurs seront identifiés via un badge personnalisé ou préétabli, à puce électronique ou virtuel pour le contrôle d'accès ou simple badge papier ou cartonné avec identification visuelle. Identité, photo, appartenance à une société, n° de pièce d'identité, les informations renseignées sur les visiteurs seront personnalisables. L'affectation d'un QR code, un code clavier ou l'immatriculation véhicule pourront venir en substitution du badge.
- Le système comprendra un mécanisme de notification permettant si besoin d'inviter les participants par courriel (avec QR code ou code clavier).
- Le visité devra être notifié lors du badgeage du visiteur sur un lecteur autorisé à son arrivée.
- Il offrira une vue complète de l'activité sous forme de clichés instantanés à l'écran (liste et nombre de visiteurs présents sur site, liste des visites terminées ou à venir, liste des cartes collectées par l'avaleur de badge, liste des visites restant à valider, etc.) ou sous forme de rapport exploitables sous Excel.
- Un panel de périphériques sera disponible : lecteur de pièces d'identité avec OCR, avaleur de cartes pour la restitution du badge d'accès au départ du visiteur, imprimante réinscriptible, etc.

Un visiteur (personne physique ou un groupe de personnes) disposera de droits d'accès précis à certaines zones uniquement ou simplement être accompagné sans avoir de support d'identification propre.

Dans le cas où le visiteur dispose de droits d'accès précis, il pourra accéder à ces zones à l'aide d'un support d'identification qui lui a été attribué et qui peut être un badge (personnalisé graphiquement ou non), un QR Code, un code clavier ou un numéro de plaque d'immatriculation.

Le visiteur ne pourra accéder au site que s'il a été invité par une personne connue de la solution de contrôle d'accès (organisateur de la visite) pour une période limitée dans le temps, faisant donc l'objet d'une visite enregistrée dans ARD Access.

La gestion des visiteurs pourra être faite manuellement en utilisant l'interface utilisateur de l'AVB ou via les APIs des Web Services SOAP du logiciel ARD Access ou équivalent.
de QR Code...)

5.11.2. Borne d'accueil

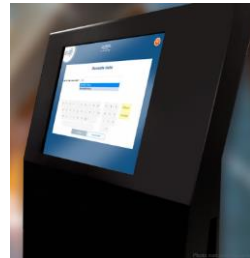
Une borne Jazz d'accueil de marque ARD ou équivalente interfacée au logiciel ARD Access ou équivalent pourra être proposée sur laquelle la personne visitée pourra enregistrer les coordonnées de son visiteur lui permettant de prévenir de son arrivée.

Cette borne offrira les fonctions suivantes :

- Préenregistrement du visiteur :
 - L'enregistrement de l'organisation d'un prochain rendez-vous (date, heure, nom du visiteur, société du visiteur) s'effectue simplement grâce à un plug-in dans l'agenda Outlook du collaborateur.
 - Le visiteur est informé via Outlook du rendez-vous et recevra de façon automatique quelques éléments comme le plan d'accès au site, les consignes sanitaires, les heures d'ouverture/fermeture ainsi qu'un QR CODE qui lui permettra de s'identifier sur la borne lors de son arrivée.
- Accueil des visiteurs sur site :

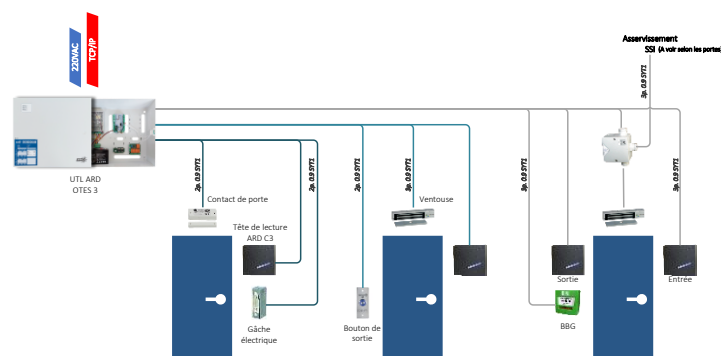


- L'hôtesse d'accueil à la visibilité sur son support (tablette, PC...) des visiteurs pré-enregistrés et peut joindre le personnel visité afin de l'informer de l'arrivée de son rendez-vous.
 - Le visiteur pourra également s'enregistrer de façon autonome en présentant son QR Code sur la borne interactive ; l'hôte est informé automatiquement de l'arrivée de son visiteur par mail.
 - Si le visiteur n'a pas son QR code, il a la possibilité à partir de la borne d'accueil de l'imprimer en saisissant son email.
- Accueil des visiteurs non enregistrés dans la solution :
 - Si le visiteur n'est pas enregistré, il a la possibilité depuis la borne d'accueil de rechercher son hôte ou l'accueil de la société. Un formulaire lui permet d'enregistrer ses coordonnées (nom/société/coordonnées) et après validation du visité, un QR code lui est imprimé.
- Demande de visite interactive pour les rendez-vous non programmés.



ARTICLE 6. MATÉRIEL DE TERRAIN

Les Unités de Contrôle de type OTES 3 ou équivalent devront pouvoir gérer 3 accès complets en entrée ou en entrée/sortie avec sorties relais intégrées (gâche électrique, ventouses, barrières parking, porte ascenseur, etc.) et devront avoir des entrées pour le raccordement d'équipement de contrôle d'accès ou intrusion (contact de porte, contact d'autoprotection, BG vert, bouton poussoir de sortie, détecteurs volumétriques ou de choc...).



Les unités de contrôle seront installées dans les gaines techniques des bâtiments. Elles devront pouvoir mémoriser 8000 lignes d'historique, 50 000 usagers et avoir une autonomie complète en cas de perte de communication avec le serveur. À la reconnexion, elles devront restituer automatiquement les événements au serveur, par exemple : badges acceptés ou refusés, ouverture trop longue au-delà d'une durée paramétrable, boîtier de décondamnation activé, défauts techniques, défaut de communication d'un équipement sur le bus, défaut présence secteur, batterie basse, etc.

Elles disposeront d'une batterie assurant une autonomie de fonctionnement d'environ 3 heures en cas de panne secteur.

Le titulaire précisera dans une note de calcul l'autonomie attendue.

Des modules d'extension devront être disponibles pour permettre d'étendre la capacité initiale de l'Unité.

Ces modules permettront :

- De gérer 2 accès supplémentaires (module 6E/2S),
- De piloter 8 sorties supplémentaires (module 8S),
- De prendre en compte 8 entrées supplémentaires (module 8E).

L'alimentation devra être suffisamment dimensionnée pour alimenter les verrouillages de 3 accès sans qu'il soit nécessaire d'ajouter une alimentation supplémentaire pour les verrouillages.

L'UTL devra disposer de base d'un emplacement carte SAM, permettant de migrer sur une solution sécurisée avec hébergement des clés de chiffrements dans un coffre-fort physique de type SAM sécurisé et préconisé par l'ANSSI, sans avoir à remplacer le matériel proposé dans la solution de base.

Les Unités de Contrôle devront pouvoir être fournies sous forme de coffret auto-protégé pour un usage intérieur ou sous forme d'armoire étanche pour l'extérieur.

Cette UTL sera fournie dans un coffret à l'esthétique soignée, avec autoprotection et indication « led » de bon fonctionnement en façade. Il pourra être proposé également l'installation de ces modules dans des boîtiers rackables 19" pour la mise en baie informatique.

Ces UTL seront installés, selon les cas, dans des armoires ou des locaux techniques.

6.1. Tête de lecture ARD

Les lecteurs de badges seront robustes et résistants aux vandalismes, ils seront étanches en extérieur; un modèle étroit permettant une fixation sur le montant des portes et un modèle à encastrer dans les boîtes d'encastrement de 60 pour cloisons intérieures devront être disponibles et laissés au choix du Maître d'Ouvrage.



Les lecteurs intégreront une LED bicolore indiquant le résultat de la lecture du badge : Vert=accès autorisé, Rouge=accès refusé. Un voyant clignotant à intervalle régulier indiquera le bon fonctionnement du lecteur (LED de vie).

Ils pourront évoluer vers des lecteurs « transparents » au sens de l'ANSSI – architecture N°1, c'est-à-dire qu'ils ne devront stocker aucun secret par simple mise à jour du micro logiciel.

Les lecteurs pourront être associés à des claviers 12 touches anti vandales IP65 directement raccordés aux lecteurs et permettant ainsi la saisie d'un code PIN assurant l'identification de l'utilisateur.

Modèle préconisé : C3 d'ARD ou techniquement équivalent

6.2. Déploiement matériel possible -

6.2.1. Caméra LAPI Tatille

L'identification des usagers via la plaque d'immatriculation de leur véhicule sera possible dans la solution de contrôle d'accès ARD Access ou équivalent.

Le logiciel de contrôle d'accès ARD Access ou équivalent permettra de gérer plusieurs numéros de plaque par usager et les Unités de Traitement Logiques (UTL) ARD OTES ou équivalents qui communiqueront avec les capteurs de reconnaissance de plaque (les capteurs sont des caméras spécialisées intégrant un logiciel de reconnaissance des numéros minéralogiques) de marque Tatille ou équivalent.

Lorsque le capteur détectera une plaque minéralogique, il transmettra par IP le numéro de plaque à l'UTL ARD OTES ou équivalent qui déclenchera l'ouverture de la barrière si l'utilisateur associé à ce numéro de plaque dispose des droits d'accès.



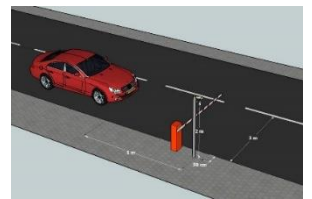
Caméra ANPR avec 8 LED Infrarouge 850nm et capteur optique de 2Mpx, permettant une lecture de plaque jusqu'à 8 mètres et pour une vitesse maximale de 70km/h.

Fournie avec un bras de fixation murale ou support poteau (en option), et complètement intégrée au logiciel ARD Access ou équivalent : les plaques d'immatriculation autorisées seront déclarées au même titre que les badges dans le logiciel.

Cette caméra LAPI offre une simplicité d'utilisation à toutes les personnes autorisées à entrer sur les parkings du site.

Afin de prévoir les risques de mauvaise lecture des plaques d'immatriculation (plaque en mauvais état, plaque sale ou enneigé), il est proposé un lecteur de base ARD C3 raccordé à l'Otes 3.

S'il n'est pas possible de créer une voie dédiée pour les motos, deux capteurs par voie (un pour les plaques avant, l'autre pour les plaques arrière) devront être prévus.



6.2.2. Adaptation avec des supports d'identification tiers

La solution sera fondée sur la technologie ISO/IEC 14443-1 de type Mifare / Mifare Desfire.

Dès qu'une carte à puce sera détectée, l'UID ou l'identifiant sécurisé contenu dans la puce sera lu et remonté comme s'il avait été saisi au clavier ; la fiche de l'utilisateur porteur de la carte – si elle existe – apparaîtra immédiatement.

Selon le contexte et le paramétrage du cycle de vie de la carte, le système proposera différents choix à la détection d'une carte :

- Affectation ou désaffectation de la carte à un usager.
- Mise en opposition.
- Personnalisation, etc.

La solution pourra également gérer :

- La solution de lecture des plaques minéralogique VEGA Basic de Tattile.
- L'identification biométrique par empreintes digitales (système Sigma Lite ex Morpho).
- L'identification par transpondeurs UHF (technologie STID).
- L'identification par smartphone en Bluetooth via les lecteurs ARD appropriés

6.2.3. Module D1 Carte d'interface CAN Lecteur

La carte d'interface Lecteur permet de raccorder des lecteurs tiers, des claviers anti-vandales et plus généralement tout type d'équipement répondant aux protocoles de type Clock&Data ou Wiegand.

- Protocole Clock-Data ou Wiegand
- Raccordement Sur bornier à vis débrochable coté contrôleur. Sur fils coté lecteur
- Dimensions 40 x 40 x 25 mm (en boîtier surmoulé)

6.2.4. Clavier à code

L'accès se fera par digicode, le code pouvant être changé facilement à chaque convocation depuis le logiciel.

- Protocole WIEGAND 26 ou 30 bits, DATA/CLOCK,
- Robuste en zamac chromé mat, - IP67 (intérieur ou extérieur),
- Dimensions 116 x 86 x 22 mm.



Pour la solution ARD, un petit module D1 carte d'interface CAN y sera associé.

6.2.5. Télécommande HF

Les accès parking seront équipés de récepteurs de télécommandes. Les télécommandes seront gérées dans le logiciel de contrôle d'accès au même titre que les badges. Toute solution proposant un système autonome ne sera pas admise. Les télécommandes auront une portée d'au moins 25 m, elle fonctionneront avec des piles CR2032 sur une fréquence de 433.92 MHz. Les télécommandes seront vues comme des badges dans l'application de contrôle d'accès. Il sera possible de leur attribuer des dates de validité et des droits d'accès au même titre que les badges.



6.2.6. Tête de lecture BLE ou QR Code

Les usagers munis d'une invitation pourront accéder aux parkings en présentant leur badge virtuel ou leur QR Code (imprimé ou via leur smartphone).

Les lecteurs Bluetooth (BLE) ou/et QR code seront totalement intégrés dans la solution de contrôle d'accès ; Une interface (Webservices) permettra de transférer les autorisations d'accès (Identité du visiteur, date de la visite) depuis le logiciel de gestion de réservation.

Pour la solution ARD, un petit module D1 carte d'interface CAN y sera aussi associé.



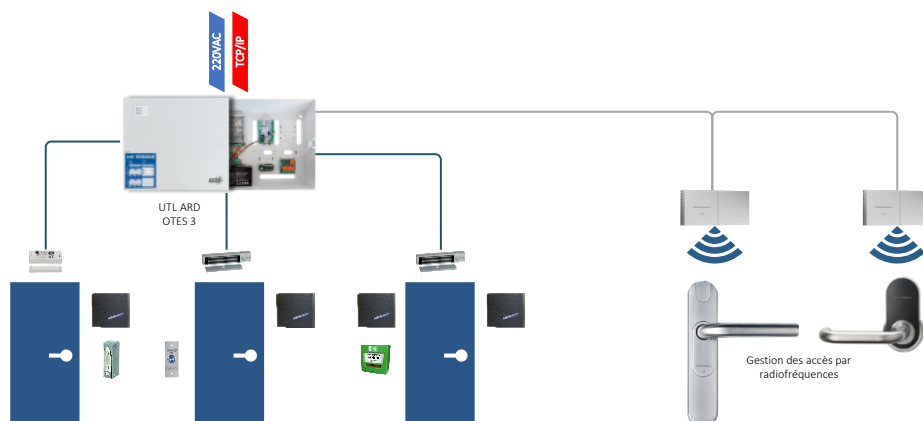
Cette gamme de lecteurs peut être adapté suivant les besoins :

- Lecteur ARC 13,56 MHz + QR Code + BLE – TTL
- Lecteur ARC 13,56 MHz + QR Code – TTL
- Lecteur ARC 13,56 MHz + BLE – TTL

ARTICLE 7. ACCÈS « ONLINE »

La solution doit permettre de déployer :

- Des lecteurs de badges **RFID filaires** (gamme de lecteur ARD C3 ou équivalent) ,
- **Et/ou** des lecteurs de badges **sans fil** afin de garantir une pérennité du système,



Le système de contrôle d'accès devra justifier l'intégration à minima du fabricant de verrouillages autonomes :

- Béquilles et cylindres électroniques de marque Simons Voss gamme Smartintego ou AX ou équivalent

7.1. Les Routeurs de communication

L'ensemble du système devra fonctionner en temps réel par liaison radio 868 MHz entre les routeurs et les organes de verrouillage électronique (Béquilles Smartintego ou cylindres Smartintego).

Cette moyenne fréquence ne pourra interférer avec d'autres bandes passantes (type WIFI ou Bluetooth en 2,4Ghz) et matériels informatiques en place sur le site. L'ensemble des informations liées aux systèmes s'effectueront en temps réel en émission et réception.

Le routeur assurera la connexion parfaite du cylindre et de la béquille au système de contrôle d'accès centralisé des bâtiments. Il pourra, dans certaines configurations avoir le rôle de répéteur entre un nœud de passerelle et le matériel de fermeture électronique. Il aura un champ de portée de 30 mètres et pourra actionner jusqu'à 16 fermetures.

Il pourra s'installer en sous face des faux plafonds son esthétique permettra une installation directe sur un mur apparent.

Routeur radio RS485 pour communication directe avec les UTL. La topologie de câblage devra être scrupuleusement respectée (section des conducteurs, nature du câble, résistance de terminaison...)

Sur les portes sensibles, les routeurs pourront remonter aux UTL des informations comme les états de la porte (ouverte/fermée, verrouillée / déverrouillée), ces dernières devant être équipées du système Door Monitoring



7.2. Les béquilles AX Simons Voss

Les béquilles électroniques radio SIMONSSVOSS sur rosace pourront s'adapter sur des serrures existantes, toute électronique avec l'énergie intégrée. Ces béquilles sur rosaces seront fixées par des vis traversantes selon les standards français en vigueur.

Les béquilles auront une autonomie minimum de 180 000 manœuvres grâce à 4 piles lithium CR2450 minimisant ainsi les coûts d'exploitation et de maintenance du matériel. Les piles seront positionnées dans l'électronique cotée extérieure de la porte permettant un changement rapide des piles sans aucun tournevis. La béquille électronique sur rosace, tête vers le haut pour porte d'épaisseur jusqu'à 60mm.



Afin de s'adapter aux portes intérieures nouvelles ou existantes, la béquille électronique devra être en carré de 7mm.

La tête de lecture pourra lire des badges sécurisés de technologie Mifare et Mifare Desfire ainsi que l'UID selon la norme ISO 14443 A et B. La tête de lecture devra pouvoir lire 5 paramétrages de cartes différents.

Elles seront indépendantes et pourront se poser sur une porte intérieure et extérieure.

Les informations d'autorisations d'accès, d'état des piles et la qualité du signal radio devront être transmises au système tierce via les routeurs radio.

En cas de coupure de communication avec le routeur radio, la béquille électronique devra fonctionner avec une liste blanche de badges autorisés. Cette liste blanche sera de 250 badges en version intégrés et 128 en version construction. Pendant la coupure de communication avec le routeur radio la béquille enregistrera le passage des 1000 derniers badges de la liste blanche.

Elles pourront être mises en lieu et place de béquilles mécaniques. Le déverrouillage des béquilles se fera par l'action d'un badge. Le changement des piles s'effectuera sans démontage de la béquille.

La béquille électronique intégrera un contact anti-arrachement du capot afin de signaler les actes de vandalisme et de piratages.

Pour des raisons de sécurité, la tête de lecture de la béquille électronique ne devra pas être intégrée à la poignée, évitant ainsi sa détérioration par des coups extérieurs.

Options disponibles : Il pourra être livré des rosaces avec trous européens pour montage d'un cylindre mécanique, rosaces borgnes où aucunes rosaces, les béquilles électroniques pourront être de couleur Argent/blanc, Pour épaisseur de porte jusqu'à 200mm

Option : Béquille sur plaque AXE 195mm et barre-antipanique :

Utilisation des trous de fixation existants en entraxe 195mm.
Plaque en inox pour cacher les traces de l'ancienne béquille.

7.3. Les béquilles Smarthandle AX ADVANCED

Les béquilles électroniques radio SIMONSSVOSS sur plaque pourront s'adapter sur des serrures existantes, toute électronique avec l'énergie intégrée. Ces béquilles sur plaques seront fixées par des vis traversantes selon les standards français en vigueur.

Les béquilles auront une autonomie minimum de 180 000 manœuvres grâce à 4 piles lithium CR2450 minimisant ainsi les coûts d'exploitation et de maintenance du matériel. Les piles seront positionnées dans l'électronique cotée extérieure de la porte permettant un changement rapide des piles sans aucun tournevis. La béquille électronique sur rosace, tête vers le haut pour porte d'épaisseur jusqu'à 60mm.

Afin de s'adapter aux portes intérieures nouvelles ou existantes, la béquille électronique devra être en carré de 7 mm entraxe 195mm.

La tête de lecture pourra lire des badges sécurisés de technologie Mifare et Mifare Desfire ainsi que l'UID selon la norme ISO 14443 A et B. La tête de lecture devra pouvoir lire 5 paramètres de cartes différents.

Elles seront indépendantes et pourront se poser sur une porte intérieure et extérieure IP66.

Les informations d'autorisations d'accès, d'état des piles et la qualité du signal radio devront être transmises au système tierce via les routeurs radio.

En cas de coupure de communication avec le routeur radio, la béquille électronique devra fonctionner avec une liste blanche de badges autorisés. Cette liste blanche sera de 250 badges en version intégrés et 128 en version construction. Pendant la coupure de communication avec le routeur radio la béquille enregistrera le passage des 1000 derniers badges de la liste blanche

Elles pourront être mises en lieu et place de béquilles mécaniques. Le déverrouillage des béquilles se fera par l'action d'un badge. Le changement des piles s'effectuera sans démontage de la béquille



7.4. Smartlocker AX de Simons Voss

Les verrous de casiers seront de la marque SIMONSSVOSS, tout électronique avec l'énergie dans la partie extérieure du verrou. Les verrous auront une autonomie minimum de 60 000 manœuvres grâce à 2 piles AA 1,5V.

Ils seront indépendants et pourront se poser uniquement à l'intérieur et possèdera la fonction BLE.

La tête de lecture pourra lire des badges de technologie Mifare et Mifare Desfire.

Les autorisations d'accès, minimum 100 groupes horaires, minimum 1 000 derniers passages.

Les verrous de casiers n'auront pas d'introduction de clé possible. Ils pourront être mis en lieu et place de verrous mécaniques sans aucune intervention spécifique.

Le déverrouillage des verrous de casiers se fera par l'action d'un badge.

Le changement des piles s'effectuera sans démontage du verrou.



7.5. Les cylindres AX de Simons Voss

Les cylindres seront de type européen de la marque SIMONSSVOSS, tout électronique avec l'énergie dans le bouton du cylindre. Les cylindres auront une autonomie minimum de 100 000 manœuvres grâce à 2 piles lithium CR2450. Les cylindres devront être modulables, il sera possible de les rallonger ou de les

raccourcir. Les cylindres pourront supporter des températures comprises entre -25°C à + 65°C et devront être IP67.

La tête de lecture pourra lire des badges de technologie Mifare et Mifare Desfire ainsi que l'UID selon la norme ISO 14443 A et B. La tête de lecture devra pouvoir lire 5 paramétrages de cartes différents et possèdera la fonction BLE.

Les cylindres n'auront pas d'introduction de clé possible. Ils pourront être mis en lieu et place de cylindres mécaniques sans aucune intervention spécifique. Afin de pouvoir s'adapter sur des menuiseries étroites, le diamètre des boutons ne devra pas excéder 32mm.

Les cylindres de fermeture avec module électronique seront conçus pour un montage dans les portes suivant la norme DIN 18250 avec profil standard européen suivant la norme DIN 18251 et allongeables par tranche de 5mm par côté. Les cylindres devront être protégés contre les attaques externes. La résistance doit être éprouvée aux attaques : classification supérieure 2 selon la norme DIN EN 15684.

Le changement des piles s'effectuera sans démontage du cylindre de la porte. Les informations d'autorisations d'accès, d'état des piles et la qualité du signal radio devront être transmis au système tierce via les routeurs radio. En cas de coupure de communication avec le routeur radio, le cylindre électronique devra fonctionner avec une liste blanche de badges autorisés. Cette liste blanche sera de 250 badges en version intégrés et 128 en version construction. Pendant la coupure de communication avec le routeur radio le cylindre enregistrera le passage des 1000 derniers badges de la liste blanche.



Versions de cylindres AX numériques :

- **Cylindre à double bouton AX Confort**

Le côté intérieur du cylindre est couplé en permanence. Les portes peuvent donc être ouvertes de ce côté sans badge. Est souvent utilisé pour les portes de bureaux, d'appartements ou d'entrée.

- **Demi-cylindre AX**

Les demi-cylindres conviennent pour les portes qui ne sont accessibles ou ne peuvent être fermées que d'un seul côté. Ils sont également utilisés dans les interrupteurs à clé et les armoires.



7.6. Cadenas AX de Simons Voss

Les cadenas radio seront de la marque SIMONSSVOSS, tout électronique avec l'énergie dans le bouton du cadenas. Les cadenas auront une autonomie minimum de 100 000 manœuvres grâce à 2 piles lithium CR2450.

Ils seront indépendants et pourront se poser en extérieur.

Les cadenas pourront supporter des températures comprises entre -25°C à + 65°C.

La tête de lecture pourra lire des badges sécurisés de technologie Mifare et Mifare Desfire ainsi que l'UID selon la norme ISO 14443 A et B. La tête de lecture devra pouvoir lire 5 paramétrages de cartes différents.

Les cadenas n'auront pas d'introduction de clé possible. Ils pourront être mis en lieu et place de cadenas mécaniques sans aucune intervention spécifique.

Le déverrouillage des cadenas se fera par l'action d'un badge.

Le changement des piles s'effectuera sans démontage du cadenas de la porte.

Les informations d'autorisations d'accès, d'état des piles et la qualité du signal radio devront être transmises au système tierce via les routeurs radio.

En cas de coupure de communication avec le routeur radio, le cylindre électronique devra fonctionner avec une liste blanche de badges autorisés. Cette liste blanche sera de 250 badges en version intégrés et 128 en version construction. Pendant la coupure de communication avec le routeur radio le cylindre enregistrera le passage des 1000 derniers badges de la liste blanche.



7.7. Badges

Les badges seront de type Mifare Desfire Ev2 EV3 au format carte de crédit en P.V.C. et pourront être personnalisés par une imprimante à sublimation, selon les besoins des systèmes applicatifs, ils deviendront le support d'identification sécurisé multiservices idéal (une carte pour plusieurs usages).

La puce sera de technologie ISO/IEC 14443-1 de type Mifare DesFire EV1 avec chiffrement AES, un produit certifié critère commun EAL4+ conforme aux recommandations de l'ANSSI.

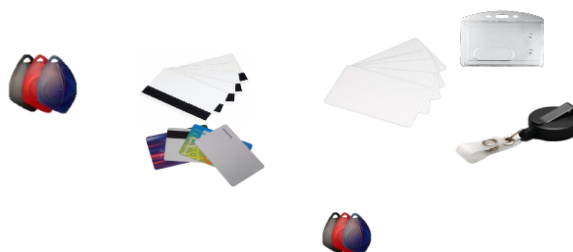
Les badges incorporeront une puce et une antenne, avec une technologie particulièrement adaptée aux usages sans contact (identification au contrôle d'accès, services de restauration, transport, gestion des temps, etc.).

Les cartes seront livrées blanches mais, sur demande, elles pourront être livrées prêtes, personnalisées en une, deux, trois ou quatre couleurs (quadrichromie) selon le visuel choisis, avec une zone réinscriptible, un pavé de signature et lamination (pour permettre une personnalisation ultérieure via une imprimante à sublimation thermique).

Les accès seront contrôlés avec des badges Mifare Desfire, les lecteurs liront l'identifiant protégé de l'applicatif dans la carte Mifare Desfire.

Ils pourront être fournis avec des étuis sécuritaires rigides et transparents, d'aspect poli sur les 2 faces. Un ergot bloque la carte une fois insérée dans l'étui.

Il pourra être proposé en option des accessoires pour protéger les cartes et faciliter leur usage quotidien. Sur demande du client un format jeton porte clef non personnalisable pourra remplacer ou compléter le format carte.



ARTICLE 8. DÉPLOIEMENT POSSIBLE - LES IDENTIFIANTS VIRTUELS

En vue de la dématérialisation des cartes d'accès une solution de badge virtuel est en cours de réflexion.

La solution permettra de dématérialiser dans une application mobile (un smartphone iOS ou Android quel que soit l'opérateur mobile) l'identification pour l'usage des services disponibles sur le site.

L'utilisateur d'une entreprise ou d'un établissement présentera son smartphone devant le lecteur filaire ou une serrure électronique compatible et accède ainsi aux services suivants :

- Bâtiments, locaux, bureaux, accueil des visiteurs sur un ou plusieurs sites ;
- Accès aux parkings, bornes de recharge pour véhicule électrique, ascenseurs, parcmètres, portails, ... ;
- Accès à des ressources internes : imprimantes, salles de réunion, restaurant d'entreprise, distributeurs automatiques...

La solution de contrôle d'accès ARD Access ou équivalent devra gérer des badges virtuels sur smartphone et pour plusieurs marques :

- Stid,
- Orange Pack ID.

La création et l'affectation des ID Mobiles des utilisateurs devront être réalisées directement depuis l'application de contrôle d'accès. Toute solution nécessitant l'accès à un portail séparé ne sera pas acceptée.

L'envoi ou la mise à jour de l'ID Mobile (désactivation, expiration, changement...) devra être automatique vers le smartphone de l'utilisateur via le réseau 3G/4G (ou WiFi) et :

- En temps réel,
- Prise en compte immédiatement, permettant un accès rapide (ou une révocation des accès) à une porte.

Il sera possible de stocker plusieurs identifiants mobiles sur le smartphone de manière sécurisée grâce à un chiffrement AES 128 des échanges radio.

Si l'utilisateur change de smartphone, il lui suffira de télécharger l'application sur son nouveau smartphone et il recevra automatiquement ses ID sans aucune manipulation. Les ID sur son ancien smartphone seront désactivés.

La solution simple et sécurisée de contrôle d'accès par smartphone intégrera :

- Le logiciel central de gestion des accès ARD Access ;
- Le système central de diffusion des ID Mobiles dans les smartphones des utilisateurs (quel que soit l'opérateur mobile) ;
- L'application mobile Orange Pack-ID disponible pour iOS ou Android ;
- Le matériel de contrôle d'accès, compatible avec un large choix de types d'accès (portes filaires, serrures électroniques, béquilles électroniques, barrières, ascenseurs...)

Le Mobile ID permet de dématérialiser les services d'accès dans une application mobile. L'application vient en complément ou en remplacement du système de contrôle d'accès existant et peut s'utiliser en complément de badges MIFARE Classic ou DESFire existants.

L'utilisation et le paramétrage devra être simple à déployer :

- Le gestionnaire créera un badge virtuel aux usagers dans le logiciel de contrôle d'accès ;
- L'usager recevra un email de téléchargement de l'application « Pack ID ». Une fois l'application installée, le serveur lui transmettra son badge virtuel sécurisé ;
- L'usager n'aura plus qu'à présenter son smartphone devant le lecteur d'accès pour entrer ;
- Si l'usager change de smartphone, son badge virtuel sera automatiquement transféré sur son nouveau smartphone.

La solution sera disponible sous forme d'un abonnement annuel. Suivant les besoins et les quantités d'utilisateurs, différents packs d'identifiants badges virtuels seront disponibles par palier de 50 / 100 / 200 / 500 / 1000 / 2000 / 4000.

Pour pouvoir dématérialiser les badges, les lecteurs concernés par ce type d'identification devront obligatoirement être en technologie BLE (Bluetooth Low Energy),

ARTICLE 9. PRESTATIONS RELATIVES À LA PROPOSITION FINANCIÈRE

9.1. Établissement du devis

Pour chaque opération le pouvoir adjudicateur formule une demande de devis. Le titulaire, après avoir visité la future installation, émet un devis détaillé par courriel au maître d'ouvrage sous deux semaines calendaires.

Si ce délai n'est pas tenable par le prestataire, ce dernier fait une demande de prolongement du délai auprès du responsable de la cellule électricité et systèmes automatisés de la DIL qui donnera son accord et proposera une date de remise de devis ultérieure aux deux semaines réglementaires ou pas.

En cas de non remise du/de devis dans les délais impartis des pénalités seront susceptibles d'être appliquées, voir article 9-1.1 du CCAP.

Les prix figurant au devis sont basés sur les modalités définies à l'annexe 2 Proposition financière de l'acte d'engagement (constitué de trois onglets) de l'acte d'engagement :

- A - Frais généraux
- B - BPU
- C- Rabais

9.2. Annexe 2A à l'acte d'engagement - frais généraux

9.2.1. Main d'œuvre

En dehors des prestations prévues dans le cadre du BPU (Annexe 2A), le candidat doit préciser pour les autres interventions (travaux hors BPU, études, calculs, plans, schémas et notices nécessaires, déposes d'installations...), le taux horaire.

9.2.2. Déboursé fournitures

Les prestations ne figurant pas au BPU (Annexe 2A), seront payés pour ce qui est de la fourniture et des matériaux, au prix d'achat réel hors TVA, majoré du coefficient entreprise. Le titulaire s'engage sur un pourcentage de déboursé fourniture. Sa proposition est ferme sur la durée totale du marché. Ce coefficient n'est donc pas soumis aux revalorisations annuelles.

9.2.3. Déplacement

Le candidat indique ses frais de déplacement nécessaire à l'intervention. Ces frais s'entendent pour un **aller-retour journalier** d'intervention. Ces propositions sont fermes sur la durée totale du marché, Ces frais ne sont donc pas soumis aux revalorisations annuelles.

Pour chaque devis, le titulaire estimera avec la plus grande sincérité les frais de déplacement nécessaire pour mener à bien l'opération qui lui est confiée. La formalisation d'une commande par le pouvoir adjudicateur rendra définitif les frais de déplacement exprimés dans le devis correspondant.

9.3. Annexe 2B à l'acte d'engagement – BPU bordereaux des prix unitaires

Tout le matériel fourni sera neuf et présentera toutes les garanties de bon fonctionnement. Le choix sera fait en tenant compte des spécifications du présent CCTP et des conditions d'utilisation et d'environnement.

L'entreprise est tenue de conserver la capacité à réparer ou remplacer par des équipements équivalents, tous les équipements fournis dans le cadre du projet, et ce pour une durée minimale de 5 ans à compter de la réception de chaque matériels (le titulaire est engagé par la proposition faite dans son offre).

9.3.1. Partie Contrôle d'accès : fourniture seule

Le matériel décrit dans les articles 5, 6 et 7 du présent CCTP ou strictement équivalent, est fourni au pouvoir adjudicateur sans frais inhérent à la mise en œuvre.

Cette partie du BPU permet l'acquisition de matériel spécifique soit pour exécuter une réparation dans le cadre du forfait de maintenance, soit pour constituer un stock de maintenance par anticipation. Le pouvoir adjudicateur se réserve également la possibilité d'installer ce matériel par ses moyens propres (équipe interne...).

9.3.2. Partie Contrôle d'accès : Fourniture pose et mise en service

Le matériel décrit dans les articles 5, 6 et 7 du présent CCTP ou strictement équivalent, est fourni au pouvoir adjudicateur pose et mise en service incluse. Pour chaque article le prix doit tenir compte de l'ensemble des éléments nécessaires à la mise en œuvre en bonne ordre de marche. Les prix incluent donc :

- La sélection du modèle adapté ;
- La main d'œuvre ;
- L'installation en tous lieux et tout support ;
- L'étiquetage ;
- Les percements ;
- Les rebouchages ;
- Les retouches de peintures ;
- Le masquage des traces d'anciens organes ;
- Les accessoires de fixation ;
- Les accessoires de raccordement ;
- Fourniture des piles et des batteries ;
- Les accessoires de finition et d'étanchéité ;
- La reconstitution des parois coupe feux ;
- La fourniture des documentations technique ;
- La fourniture des certificats de conformité de toute nature ;
- La fourniture des autotests et PV de mise en service ;

- Liste non exhaustive...

Cette partie du BPU permet l'acquisition et la mise en œuvre de matériel spécifique dans le cadre de travaux confié au titulaire. Ce dernier assure une prestation d'ensemble conformément à l'opération menée par le pouvoir adjudicateur.

9.3.3. Partie équipement informatique et logiciels

Les solutions décrites à l'article 5 du présent CCTP ou strictement équivalentes, sont fournis au pouvoir adjudicateur. Les prix comprennent la fourniture des logiciels, du matériel et la configuration y compris sur site en parfait ordre de marche.

Les développements ou les configurations dont le coût de main d'œuvre sont directement liées au périmètre du projet feront l'objet d'une plus-value quantifiée via l'annexe 2A - Frais généraux.

9.3.4. Partie électricité Contrôle d'accès

Le matériel décrit ou strictement équivalent, est fourni au pouvoir adjudicateur pose avec mise en service incluse. Pour chaque article le prix doit tenir compte de l'ensemble des éléments nécessaires à la mise en œuvre en bonne ordre de marche. Les prix incluent donc :

- La sélection du modèle adapté ;
- La main d'œuvre ;
- L'installation en tous lieux et tout support ;
- L'étiquetage ;
- Les percements ;
- Les rebouchages ;
- Les retouches de peintures ;
- Le masquage des traces d'anciens organes ;
- Les accessoires de fixation ;
- Les accessoires de raccordement ;
- Les accessoires de finition et d'étanchéité ;
- La reconstitution des parois coupe feux ;
- La fourniture des documentations technique ;
- La fourniture des certificats de conformité de toute nature ;
- La fourniture des autotests et PV de mise en service ;
- Liste non exhaustive...

Cette partie du BPU permet l'acquisition et la mise en œuvre de matériels nécessaires pour interconnecter les éléments du système de contrôle d'accès.

Le titulaire veillera à implanter du matériel judicieusement sélectionné pour maintenir une cohérence des installations sur lequel il intervient. Tout particulièrement lorsqu'il ajoute des éléments dans les armoires électriques ou dans les baies informatiques.

La sélection du matériel devra être conforme aux normes en vigueur, et tenir compte des préconisations de chaque constructeur. Une attention particulière devra être observée pour les liaisons entre les équipements au regard des spécifications afin d'assurer la compatibilité des organes entre eux. Les liaisons véhiculant des informations de type data devront être résilientes aux perturbations électromagnétiques.

9.4. Annexe 2C à l'acte d'engagement - rabais

Lorsque le montant total HT du devis est compris dans l'une des tranches de rabais R1 à R4, la remise en pourcentage s'applique au devis.

Le candidat est informé du fait que ce dispositif vise à prendre en compte la diversité des opérations susceptibles de lui être confiés.

9.5. Planning

Le planning est défini lors d'une réunion préparatoire avant la prestation. Une phase d'étude et de préparation est discutée et évaluée. La date convenue de fin de prestations est reportée sur le bon de commande à la rubrique « date de livraison ».

Pour information, l'Université précise que l'accès aux locaux est possible même pendant les périodes de fermeture de l'Université : trois semaines en août, et dix jours en décembre.

Le titulaire devra disposer d'équipes suffisantes pour donner suite en temps utile aux commandes de prestations de l'université Jean Moulin.

La réception des prestations se fera après avoir reçu les DOE du chantier et que les nouveaux équipements aient été intégrés à une éventuelle base de gestion de maintenance ou GMAO.

Pour mémoire, le dépassement des délais sera soumis à des **pénalités de retard**, (cf. art 9-1 du CCAP).

9.6. Études

Tous les plans et descriptifs devront être validés par le maître d'ouvrage avant l'exécution des prestations, sur supports papiers et numériques.

L'entreprise aura à sa charge les études de faisabilité et d'adéquation relatives aux sujets suivants :

- Les emplacements selon zonage et les choix définitifs des équipements de contrôle d'accès et des différents procédés de fixation adaptés aux différents matériaux constituant les supports ;
- La définition de l'indice de Protection des équipements installés à l'extérieur selon le niveau d'exposition aux contraintes extérieures ;
- La définition du niveau de protection au rayonnement UV ;
- Les solutions de raccordements des divers équipements entre eux, aux réseaux courant fort et faible (transmission des données) des bâtiments ;
- Les méthodes d'intervention sur la voirie et dans les bâtiments publics ;
- Le prestataire aura à sa charge l'étude et la mise en œuvre des moyens nécessaires pour assurer la continuité du niveau de sûreté du ou des bâtiments pendant la phase des prestations.

Pour les opérations de plus de dix portes devant être équipées, les études devront être faites par anticipation à la rédaction du devis. En effet, l'intégration dans un écosystème existant doit être prise en compte. Le temps d'étude anticipé sera rétribué dans le cadre des travaux qui suivront. Le pouvoir adjudicateur s'engage à prendre en charge les frais d'études dans le cas où les travaux ne seraient pas réalisés.

9.7. Exécution des prestations

Le titulaire doit réaliser des installations complètes en parfait état de marche.

Il doit prévoir l'exécution de toutes les prestations nécessaires et les liaisons complémentaires entre les divers équipements.

Les canalisations électriques basse tension et les canalisations de détection incendie, câblage réseaux, et audiovisuel ne doivent en aucun cas emprunter les mêmes conduits ou les mêmes logements des moulures ou les mêmes compartiments de goulottes.

Par ailleurs, les installations seront exécutées conformément au présent CCTP, à la réglementation en vigueur et suivant les règles de l'art de la profession.

Les percements des recoupements coupe-feu (cloisons et planchers) seront rebouchés à l'aide des matériaux restituant le coupe-feu d'origine.

Le câblage des installations en Courant Fort et Courant faible sera à la charge du titulaire.

Le titulaire est responsable de ses installations jusqu'à la fin des prestations et la prise en charge de celles-ci par le Maître d'Ouvrage.

9.8. Nettoyage des zones de travaux

Compte tenu du fait que les prestations vont se dérouler sur un site occupé, l'entreprise devra procéder au nettoyage journalier des zones d'intervention, en évacuant ses déchets. Préalablement à la réception de fin d'intervention, l'entreprise devra procéder à un nettoyage approfondi de ses zones de prestations. En cas de mauvaise exécution du nettoyage, l'université se réserve la possibilité de faire exécuter une prestation de nettoyage aux frais de l'entreprise.

9.9. Dossier des Ouvrages Exécutés

Dès la fin des prestations et avant la réception, le prestataire sera tenu d'effectuer tous les essais et réglages qui permettront de livrer une installation en ordre de fonctionnement dans un délai de 1 mois après la réception (date de mise en service indiquée sur la Fiche de Réception faisant foi).

Le dépassement des délais sera soumis à des **pénalités de retard**, (cf. art 9-1 du CCAP).

Préalablement à la réception, le prestataire doit remettre au Maître d'Ouvrage, sous la forme de D.O.E., un dossier complet en un exemplaire numérique (format DWG et PDF.) et en un exemplaires papiers.

Fourniture des plans et descriptifs des installations réalisées :

- Un plan par niveau détaillé, avec équipements et câblage de la nouvelle installation, raccordements électriques,
- Les fiches techniques des différents composants de l'installation,
- Les notices d'instruction, de montage et de maintenance des différents composants de l'installation.

Après chaque opération, le titulaire doit mettre à jour les synoptiques et plans de récolement du système.

9.10. Réception des ouvrages

La réception des ouvrages exécutés est prononcée lors d'un rendez-vous sur site. Les constats et réserves éventuels sont consignés dans un document. Le pouvoir adjudicateur et le titulaire conviennent d'une date pour lever les réserves.

La date portée sur la fiche de réception correspond à la mise en service de l'installation. Cette date constitue le point de départ des garanties.

ARTICLE 10. PRESTATIONS RELATIVES À LA DÉCOMPOSITION DE PRIX GLOBAL ET FORFAITAIRE

La prestation de maintenance comprend l'ensemble du système de contrôle d'accès existant à l'université, mais également les ajouts futurs commandés sur la base du BPU.

Le titulaire est informé que le contrôle d'accès peut également être enrichi dans le cadre d'autres opérations pluridisciplinaires comme c'est le cas actuellement.

Par exemple :

- CPER de Bourg en Bresse phases 2 et 3,
- Opération tiers lieux,
- Centre de recherche.

Dans ce cas, le pouvoir adjudicateur mettra en relation le titulaire et les installateurs de ces opérations, pour définir en amont les limites des prestations et organiser la coactivité. Lorsque le délai de garantie dû par l'installateur est purgé, les nouveaux équipements sont intégrés au contrat de maintenance à la date anniversaire.

À ce jour, les points d'accès sont répartis sur les trois sites de l'université :

- Site de la Manufacture des tabacs (Lyon 8^e) ; constitué des bâtiments Manufacture, maison du directeur et maison du gardien ;
- Site des Quais du Rhône (Lyon 7^e), constitué des bâtiments Palais, Cavenne, Athéna, Dugas, Chevreul, IUT, et MILC ;

Service des Achats – DAFA – 1 C avenue des Frères Lumière CS 78 242 - 69372 LYON cedex 08

achats@univ-lyon3.fr

- Site de La Charité (Bourg en Bresse), constitué du bâtiment principal.

Le site de La Charité est en cours d'extension : réhabilitation d'une partie du bâtiment existant et de la chapelle, ainsi que la construction d'un amphithéâtre.

Le tableau ci-dessous donne le nombre de points d'accès par bâtiment :

Total points d'accès Palais	70
Total points d'accès Dugas	18
Total points d'accès Athéna	28
Total points d'accès Chevreul	34
Total points d'accès Manu	285
Total points d'accès Directeur	7
Total points d'accès Cavenne	6
Total points d'accès MILC	73
Total points d'accès IUT	47
Total points d'accès Charité	23
Total points d'accès	591

La prestation de maintenance décrite dans cet article se réfère au DPGF (annexe 3 de l'acte d'engagement). La prestation est rémunérée chaque trimestre.

Les quantités commandées sur la base du DPGF sont susceptibles d'évoluer chaque année à la date anniversaire. En effet, les quantités renseignées dans ce document sont celles correspondants à la première année d'exécution du marché.

10.1. Annexe 3 à l'acte d'engagement - Main d'œuvre

10.1.1. Maintenance Préventive

Les prestations de maintenance préventive seront effectives lors des visites planifiées d'un commun accord entre les services de la DIL et le prestataire du marché. La prestation est exécutée durant les heures ouvrées du lundi au vendredi.

Le prestataire doit effectuer une visite préventive par année sur l'ensemble des bâtiments de l'Université décrits ci-dessus.

Les candidats seront incités à proposer et décrire un plan de maintenance précis et un planning prévisionnel dans leur réponse technique. Ce plan de maintenance pourra être associé aux prestations décrites ci-dessous s'il apporte de la valeur ajoutée à ces opérations.

Sous 3 mois suite à la notification du marché, le titulaire devra effectuer une visite initiale afin de prendre en compte l'ensemble des systèmes et matériels installés sur les sites de l'université. Cette visite initiale lui permettra de saisir dans son système de GMAO ou autre système de reporting, les équipements, marques, localisations et d'appréhender les locaux.

Cette visite initiale doit aussi permettre de proposer au maître d'ouvrage la liste des éléments à mettre en stock sur site.

10.1.1-1 *Stock de maintenance*

Le premier stock jugé utile après analyse commune des besoins identifiés sur les différents sites de l'université sera mis en place au sein des locaux de la DIL. Ce stock sera validé et financé par la DIL.

Le titulaire du marché devra veiller au réassort des produits utilisés lors des dépannages ou des visites de maintenance préventive. Il veillera à ce que l'approvisionnement des pièces manquantes au stock soit réalisé sous 8 jours ouvrés. Un devis relatif aux équipements utilisés dans l'année sera établi avant la date anniversaire et sera transmis à la DIL pour édition d'un bon de commande.

S'il advenait qu'une panne ne puisse être résolue du fait d'un délai de réassort dépassé, une pénalité journalière serait appliquée du premier jour de la panne jusqu'à remise en service de l'équipement et/ou réassort (cf. Art 9-1.5 et 9-1.9 du CCAP).

10.1.1-2 Amélioration

Les visites de maintenance préventive sont l'occasion de faire évoluer certaines fonctionnalités du système : petite modification de câblage, variant de programmation, modification graphique... Ces évolutions s'entendent sans ajout de matériel et ne pouvant excéder 8h de main d'œuvre. Le titulaire doit donc intégrer ce temps dans sa réponse.

Pour des évolutions plus conséquentes, le prestataire du présent marché à un rôle de conseil important auprès des services de l'université. Il doit se positionner pour apporter toutes modifications et améliorations aux équipements en place, selon les usages pratiqués au sein de l'université. Il devra être capable d'analyser, décrire et proposer de nouveaux produits, de nouveaux process, les associations possibles avec d'autres systèmes connectés, etc.

Tous les frais d'amélioration qui pourront en découler seront à la charge de l'Université.

Dans ce cadre, un temps d'échange sur le marché, sur les prestations effectuées, les désordres rencontrés, les problématiques diverses et variées et améliorations, sera programmé chaque année au mois de juin. Un rapport global sera alors remis aux services de la DIL.

10.1.2 Maintenance corrective et service d'astreinte

Les interventions de maintenances correctives nécessitant une intervention sur les sites de l'université sont rétribuées forfaitairement à l'année. Les frais de déplacement sont inclus au forfait. Le titulaire intervient donc chaque fois que cela est nécessaire pour corriger tout désordre qui lui serait signaler. Chaque signalement doit être traité indépendamment, c'est-à-dire que les délais d'intervention sont appréciés au regard de la date et heure de chaque signalement.

10.1.2-1 Délais

Tous les dépassements de délais entraîneront des pénalités (voir article 9-1 du CCAP).

En cas de dysfonctionnement ou panne sur la solution logiciel et UTL, les délais d'interventions sont les suivants :

- Sur une panne générale du système, une assistance Hotline doit être disponible de 7h30 à 21h00 du lundi au vendredi ;
- Sous 2h00 après appel à la Hotline, un technicien/ingénieur/informaticien devra avoir rappelé les personnels de la DIL/DNUM ayant demandé assistance ;
- Le remise en service et un retour normal à l'utilisation des équipements déployés sur site devra se faire sous 4h00 maximum après le délai de 2h expiré pour assistance Hotline.

Sur une panne logiciel dite « minime » (alarme intempestive, perte de communication ou autres...) n'engendrant pas de réel problème d'accès et d'utilisation des équipements en place sur site, la prise en compte de la demande de dépannage par mail ou appel téléphonique des personnels de la DIL, ou de la DNUM devra être effective sous 4h pour une réponse apportée/solution/remise en état sous 48h00 après cette prise en compte.

En cas de dysfonctionnement ou panne sur la solution matérielle [hors logiciel], nécessitant une intervention rapide dite « urgente », le titulaire est tenu par les engagements suivants :

- Les interventions dites « urgentes » ont lieu du lundi au vendredi de 7h30 à 21h00 sous 4h00 après appel ou notification écrite ;
- Les interventions dites « urgentes » ont lieu les week-ends et jours fériés sous 8h00 après appel ou notification écrite ;
- Le délai de remise en service suite à une intervention en urgence sera porté à 4h supplémentaires suite à l'arrivée sur site du technicien.

En cas de dysfonctionnement ou panne sur la solution matérielle [hors logiciel], et hors urgence, le délai d'intervention est de 2 jours ouvrables à compter de son signalement par appel ou écrit de la part du

pouvoir adjudicateur. Le délai de remise en service sera porté à 1 journée ouvrable supplémentaire suite à l'arrivée sur site du technicien.

10.1.2-2 Procédures d'exploitation particulières en cas de fonctionnement dégradé

On définit le fonctionnement dégradé, comme le fonctionnement du système de manière partielle suite à un dysfonctionnement complet ou partiel des éléments qui le composent. Le titulaire du marché peut être sollicité pour accompagner le pouvoir adjudicateur et mettre en œuvre des mesures compensatoires en cas de fonctionnement dégradé.

Plusieurs types d'évènements peuvent se produire et entraîner un fonctionnement dégradé. Les évènements peuvent aussi se cumuler. Il convient de faire face à chaque situation en définissant les bonnes procédures dès la mise en place du système.

Il sera donc attendu que l'architecture proposée permette dans les scénarios suivants, un comportement sécurisé lors de :

Panne d'une tête de lecture (lecteur de badge) :

- Le prestataire du système veillera à ce que les services techniques de la DIL, aient constamment des têtes de lecture en stock pour garantir leur remplacement le plus rapidement possible.

Panne d'une UTL :

- La problématique est la même que pour une tête de lecture défaillante, à la différence que plusieurs têtes de lecture (celles contrôlées par l'UTL) seront non opérationnelles.

Panne du serveur ou du logiciel de gestion du système d'accès :

- Les UTL doivent avoir une copie de la base des droits afin de continuer à fonctionner de manière autonome.
- Pendant la panne, la création de badges et leur révocation n'est pas possible, ni la génération des rapports ou la consultation des évènements.

Cette situation en mode dégradé est fortement critique, et le système devra être remis en fonctionnement conformément aux délais décrits à l'article 10.1.2-1 du CCTP.

Coupure électrique :

Afin de gérer un incident de coupure électrique les conditions suivantes doivent être vérifiées.

- Vérifier manuellement le verrouillage de chaque porte sensible (portes extérieures des sites, et portes intérieures donnant accès à des zones sensibles) afin de s'assurer que les batteries ont bien pris le relais d'alimentation et assurent le verrouillage des portes.
- Il est à rappeler que lorsque la durée de la panne excède l'autonomie sur batterie des éléments supports du système de contrôle d'accès, la panne relève de l'incident grave. Il convient de porter une attention particulière aux portes qui pourraient rester verrouillées alors que la réglementation sur la sécurité des personnes en impose le déverrouillage

10.1.3 Formation

La formation proposée s'adaptera en fonction des besoins identifiés. Le programme de formation sera alors défini par la DIL et/ou la DNUM et élaboré avec le prestataire. Les sessions sont calibrées pour une durée de 4h permettant de former jusqu'à cinq collaborateurs de l'université.

En plus de cette session il est prévu une formation du personnel et une assistance au démarrage de l'ensemble des matériels installés, et la fourniture de la documentation technique et d'exploitation relative aux différents matériels et logiciels installés, en langue française qui comprend :

- La fourniture des plans, notes de calcul, diagrammes, et de tous les documents relatifs ;
- L'exécution des prestations, sur support papier et informatique ;
- Les plans sur support informatique seront au format DWG, les autres documents seront fournis au format DOC, XLS, et pouvant être modifiés et au format PDF non modifiable.

Les temps de maintenance préventive sur site concourent également à la formation des agents de l'université au travers de temps d'échange ou d'accompagnement sur le terrain.

10.2 Annexe 3 à l'acte d'engagement - Logiciel

Ce paragraphe s'attache à détailler la prestation relative aux logiciels. Pour la description technique des logiciels implantés ou susceptibles de l'être, se reporter aux articles 5, 6 et 7 du présent CCTP.

Le titulaire a la charge de l'ensemble des composants logiciels nécessaires au bon fonctionnement et au paramétrage de la solution dans son ensemble.

10.2.1 Ard Access

10.2.1-1 *Contrat de maintenance et d'assistance constructeur*

Le titulaire souscrit, auprès du constructeur de la solution ARD ACCESS et pour le compte exclusif de l'université, un contrat de maintenance et d'assistance. La forme juridique de cette souscription est laissée à l'appréciation du candidat dans le respect des règles en vigueur.

Lors d'une visite de maintenance préventive et chaque fois que cela sera nécessaire, le constructeur doit réaliser le contrôle du logiciel et des composants qui y sont rattachées :

- Logiciel principal ARD ACCESS ;
- Les modules installés ;
- Les connecteurs ;
- Les outils de paramétrages ;
- Les bases de données ;
- L'interaction avec d'autres solutions.

10.2.1-2 *Maintenance logiciel attendu :*

- Sauvegarde du système ;
- Sauvegarde des bases de données ;
- Stockage en lieu sûr des fichiers de sauvegarde ;
- Vérification de la concordance de la base de données ;
- Vérification de l'intégrité du logiciel d'application ;
- Vérification de la configuration ;
- Vérification des synoptiques, plans ;
- Inventaires ;
- Corrélation de l'identification des organes ;
- Essais de bon fonctionnement ;
- Test de communications entre les organes et le serveur ;
- Propositions d'optimisations.

Cette liste est non exhaustive. Le candidat, de par son expertise, démontrera plus finement sa capacité dans son mémoire technique.

10.2.1-3 *Assistance due au titre du marché*

Sont dues, au titre du présent marché, l'assistance constructeur à distance, chaque fois que cela est nécessaire. Le titulaire fournira au pouvoir adjudicateur les modalités d'accès à cette assistance dans le mois qui suivra la signature du marché.

La nature des sollicitations sont diverses. La liste ci-dessous fournit quelques exemples :

- Explication / accompagnement concernant le fonctionnement du logiciel ;
- Fourniture de documentation détaillée ;
- Bugs éventuels ;
- Aide au paramétrage ;
- Problème de droit d'accès ;
- Assistance pour la mise en place d'interfaçages avec des solutions tiers ;
- Conseil aux utilisateurs.

10.2.1-4 Mise à jour

L'Université Jean Moulin Lyon 3 exige un maintien en condition de sécurité pour ses systèmes de contrôle d'accès, au même titre que pour tout autre système d'information.

Le titulaire doit donc :

- Notifier la présence de vulnérabilité sur les produits dont il a la charge, dans les 48h après le signalement du défaut.
- Proposer la mise en place immédiate de mesures palliatives et un plan de déploiement rapide des correctifs dès lors qu'ils ont été publiés par l'éditeur des logiciels, dans les 48h après le signalement du défaut.

Sont dues, au titre du présent marché, les mises à jour de la solution ARD ACCESS.

Avant toute intervention il est communiqué au pouvoir adjudicateur un suivi des versions majeures et mineures. Ce suivi devra mettre en avant les différences entre les versions déployées et les versions compatibles avec le système le plus récent.

Après validation du pouvoir adjudicateur, les dernières versions mineures et correctif de sécurité sont systématiquement installées dans les meilleurs délais par le titulaire.

Une mise à jour majeure est due au titre du présent marché. Une planification spécifique sera étudiée en amont, afin d'organiser le déploiement en parallèle de la solution actuelle. Lorsque la nouvelle version est pleinement fiabilisée, le transfert définitif est organisé après validation du pouvoir adjudicateur. Le coût de cette mise à jour est lissé sur les quatre ans d'exécution. La rétribution de la mise à jour majeure est lissée à la DPGF sur les quatre années d'exécution.

10.2.2 UTL et équipements radio

Afin de fiabiliser les produits et de lutter contre le gaspillage, ou l'obsolescence programmée, il est prévu un maintien en condition optimale de fonctionnement des solutions logiciels propres au matériel.

10.2.2-1 Firmware

En ce sens sont dues les mises à jour systématiques des firmwares, des UTL et des dispositifs de verrouillage sans fil des fabricants ARD et SimonVoss, déjà installés à l'université ou déployés dans le cadre de travaux neufs.

10.2.2-2 Diagnostique par le constructeur

Lorsque le titulaire se heurte à une limite technique ne lui permettant pas d'aller plus avant dans un diagnostic de dysfonctionnement, il devra organiser à ses frais une intervention du constructeur compétant pour diagnostiquer et résoudre le désordre constaté. Le pouvoir adjudicateur refusera le remplacement de matériel dont le diagnostic présente un doute ou restant inexpliqué.

10.3 **Annexe 3 à l'acte d'engagement - Matériel**

Ce paragraphe s'attache à détailler la prestation relative au matériel. Pour la description technique du matériel implanté ou susceptible de l'être, se reporter aux articles 5, 6 et 7 du présent CCTP.

10.3.1 Base de quantification

10.3.1-1 Méthode de quantification

L'extraction de la liste du matériel configuré dans le logiciel ARD ACCESS sert de base de quantification pour le matériel.

Vous trouverez ci-dessous un extrait :

Site ARD ACCES V2 : Lyon 3 - Jean Moulin
Version AVB 2.13.4
Date de l'export 08/04/2025 14 :30

Récapitulatif de la configuration matérielle par type et sous-type

Type	Sous-type	Nombre
Centrale	OTES2	72
Centrale	OTES3	41
Lecteur	Lecteur filaire (ARD ou Système tiers)	194
Lecteur	Serrure autonome (INTEGO)	405
Hub	Hubs Intego	182

Le cumul des deux typologies de lecteurs représente le nombre de portes équipées. Le candidat est toutefois informé que certaines portes disposent d'un double lecteur.
Les quantitatifs ainsi obtenus sont reportés au DPGF (annexe 3 de l'acte d'engagement).

10.3.1-2 Révision du périmètre à maintenir

La révision du périmètre matériel à maintenir est annuel à date anniversaire du présent marché. Pour ce faire le titulaire réalisera une extraction conformément à la méthode présentée précédemment pour mettre à jour son offre tarifaire. Il soumettra cette offre au pouvoir adjudicateur pour validation. Par souci de simplification la révision des quantités doit obligatoirement être présentée en même temps que la révision des prix décrite au CCAP.

10.3.2 Unité de traitement local UTL

Lors d'une visite de maintenance préventive, le technicien doit réaliser le contrôle de chaque sous-ensemble. On entend par là les unités de traitement local UTL et les organes qui y sont rattachés :

- UTL et extensions ;
- Lecteur de badges ;
- AES alimentation de secours ;
- Liaison électrique raccordée à l'UTL.

10.3.2-1 Contrôle et essais attendus :

- Dispositif d'alimentation et fusible ;
- Batteries ;
- Cartes d'extension ;
- Ensemble de filerie et raccordement de toute nature ;
- Fixations ;
- Intégrité mécanique ;
- Etiquetages ;
- Corrélation de l'identification des organes ;
- Mesures et essais de bon fonctionnement ;
- Test de communications entre les organes et vis-à-vis du serveur ;
- Vérification de la configuration.

Cette liste est non exhaustive. Le candidat, de par son expertise, démontrera plus finement sa capacité dans son mémoire technique.

10.3.2-2 Pièce d'usure dues au titre du marché

Sont dues, au titre du présent marché, les pièces d'usures. Lors d'une visite de maintenance préventive, le titulaire devra disposer du matériel d'usure courante pour effectuer le remplacement au fur et à mesure de la visite. Sont donc à prévoir :

- Les batteries des UTL ;
- Les batteries des AES ;

Service des Achats – DAFA – 1 C avenue des Frères Lumière CS 78 242 - 69372 LYON cedex 08
achats@univ-lyon3.fr

- Les fusibles ;
- La petite quincaillerie ;
- Les accessoires de raccordement ;
- Les dispositifs de marquage.

Le titulaire évacuera à ses frais les batteries usagées dont il aura assuré le remplacement. La date de remplacement des batteries sera indiquée sur le rapport de maintenance établi à l'issue de la campagne de maintenance, ainsi que sur l'étiquette de suivi collée sur l'UTL.

10.3.3 Système radio

Lors d'une visite de maintenance préventive, le technicien doit réaliser le contrôle de chaque sous-ensemble. On entend par là les HUB radio et les organes de verrouillage qui y sont rattachées :

- HUB
- Béquille radio sur rosace
- Plaque béquille radio
- Cylindre radio
- Cadenas radio
- Autre solution radio implanté ultérieurement

10.3.3-1 *Contrôle et essais attendus :*

- Lecteur de badge
- Batteries
- Fixations
- Intégrité mécanique
- Corrélation de l'identification des organes
- Mesures et essais de bon fonctionnement
- Test de communications entre les organes et vis-à-vis du serveur
- Vérification de la configuration
- Mise à jour de la Liste blanche
- Intégrité de la base de données IKP

Cette liste est non exhaustive. Le candidat de par son expertise démontrera plus finement sa capacité dans son mémoire technique.

10.3.3-2 *Pièces d'usure dues au titre du marché*

Sont dues au titre du présent marché les pièces d'usures. Lors d'une visite de maintenance préventive Le titulaires devra disposer du matériel d'usure courante pour effectuer le remplacement au fur et à mesure de la visite.

Sont donc à prévoir :

- Les batteries / piles des dispositifs de verrouillage radio
- La petite quincaillerie
- Les outils spécifiques nécessaire à l'intervention (ces outils restent la propriété du titulaire)

10.3.4 Verrouillage de porte

Lors d'une visite de maintenance préventive le technicien doit réaliser le contrôle de chaque sous ensemble. On entend par là tous les éléments périphériques d'un point d'accès :

- Serrure mécanique de tout type
- Serrure électromécanique de tout type
- Verrouillage électromagnétique de tout type
- Lecteur de badges
- Boîtier de décondamnation vert
- Bouton ou assimilé
- Capteur de position
- Liaison électrique raccordé

10.3.4-1 Contrôle et essais attendu :

- Dispositif d'alimentation et fusible
- Carte électronique
- Ensemble de filerie et raccordement de toute nature.
- Fixations
- Intégrité mécanique
- Etiquetages
- Corrélation de l'identification des organes
- Mesures et essais de bon fonctionnement
- Test de communications entre les organes et vis-à-vis du serveur
- Vérification de la configuration
- Essais de bon fonctionnement mécanique
- Réglages et graissage mécanique
- Le nettoyage nécessaire au bon fonctionnement

Cette liste est non exhaustive. Le candidat de par son expertise démontrera plus finement sa capacité dans son mémoire technique.

10.3.4-2 Pièce d'usure dues au titre du marché

Sont dues au titre du présent marché les pièces d'usures. Lors d'une visite de maintenance préventive Le titulaires devra disposer du matériel d'usure courante pour effectuer le remplacement au fur et à mesure de la visite. Sont donc à prévoir :

- Les fusibles
- La petite quincaillerie
- Les accessoires de raccordement
- Les dispositifs de marquage
- Les celés pour boîtier de décondamnation vert
- Les produit de nettoyage et de lubrification

10.3.4-3 Pièce d'usure fournie au titulaire

Afin de limiter les interactions entre les divers corps de métier le titulaire aura la charge du remplacement des serrures mécaniques pour les portes gérées par le contrôle d'accès. Le service de maintenance de l'université dispose des principaux modèles de serrures (Multibat monopoint pêne ¼ tour, axe à 50, serrures à larder Stremmer, Métalux ...). Lorsque cela s'avère nécessaire l'université fournira au titulaire la serrure de remplacement. L'installation de la serrure est dû au titre du présent marché.

10.3.5 Pilotage d'équipement embarqué

Lors d'une visite de maintenance préventive le technicien doit réaliser le contrôle de chaque sous ensemble. On entend par là gestion des ascenseurs, des portails et asservissements au système de sécurité incendie :

- Ordre de commande
- Acquisition d'état
- Lecteur de badges
- Boîtier de décondamnation vert
- Liaison électrique raccordé

10.3.5-1 Contrôle et essais attendu :

- Carte électronique
- Relayage
- Ensemble de filerie et raccordement de toute nature.
- Fixations
- Intégrité mécanique
- Etiquetages
- Corrélation de l'identification des organes
- Mesures et essais de bon fonctionnement
- Test de communications entre les organes et vis-à-vis du serveur

- Vérification de la configuration

Cette liste est non exhaustive. Le candidat de par son expertise démontrera plus finement sa capacité dans son mémoire technique.

10.3.5-2 Pièces d'usure dues au titre du marché

Sont dues au titre du présent marché les pièces d'usures. Lors d'une visite de maintenance préventive Le titulaires devra disposer du matériel d'usure courante pour effectuer le remplacement au fur et à mesure de la visite. Sont donc à prévoir :

- Les fusibles
- Les accessoires de raccordement
- Les dispositifs de marquage

10.3.5-3 Limite de prestation et coactivité

Le candidat est informé que le pouvoir adjudicateur a confié la maintenance des ascenseurs, des portails et du système de sécurité incendie à plusieurs prestataires. En ce sens le titulaire veillera à ce que ces actions n'ont pas d'incidence pour les autres prestataires.

Chaque fois que cela sera nécessaire et en concertation avec chacune des parties le pouvoir adjudicateur pourra organiser des interventions communes de plusieurs prestataire. Ces interventions visent à traiter les éléments situés en limite de prestation des uns et des autres. Ce type d'intervention est dû au titre du présent marché.

10.4 Gestion de la maintenance

10.4.1 GMAO

Une Gestion de Maintenance Assistée par Ordinateur (GMAO) est demandée pour un suivi de l'ensemble des prestations mise en œuvre sur ce marché :

- Demandes d'interventions des gestionnaires DIL
- Suivi sur classeur/portefeuille des actions opérées par le mainteneur
- Reporting, données terrains, statistiques, alarmes...
- Gestion des stocks
- Documentations techniques disponibles, plans notices, rapports d'interventions, comptes-rendus avec photos...
- Intégration d'un inventaire de matériel existant, avec localisation sur site, identifications...
- Gammes de maintenance, plannings...

10.4.2 Rapport de visite de maintenance

A l'issue de chaque interventions un rapport d'intervention est rédigé par le technicien. Il sera transmis au maître d'ouvrage pour signature et remarques éventuelles sous cinq jours ouvrés.

Y seront consignés, les observations faites au cours de la visite et le détail des prestations effectués :

- Synthèse des dysfonctionnements constatés
- Ensemble des opérations effectuées
- Mesures à prendre pour améliorer le système avec évaluation financière.
- ...

10.4.3 Tenue de la documentation du système

La complexité d'un tel système implique de tenir à jour l'ensemble des éléments documentaires qui permettent de faire vivre l'écosystème. Le titulaire assurera donc le récolement des divers éléments au fur et à mesure de ses prestations ;

- Mise à jour des notices
- Mise à jour des plans et des synoptiques
- Tableaux de suivi des équipements
- Récupération d'informations manquantes
- ...

Service des Achats – DAFA – 1 C avenue des Frères Lumière CS 78 242 - 69372 LYON cedex 08

achats@univ-lyon3.fr