

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

ACCORD-CADRE DE TRAVAUX

Accord-cadre 913 26 24 - Accord cadre pour le remplacement du contrôle d'accès des bâtiments de l'Université de Limoges

Marché subséquent n°1

1. INTRODUCTION ET CONTEXTE	4
1.1. Préambule.....	4
1.2. Objet de la consultation.....	4
2. Présentation de l'établissement.....	5
3. PÉRIMÈTRE DU PROJET	5
3.1. Description de l'existant	5
3.2. Description synthétique des prestations	6
3.3. Responsabilité et confidentialité	6
3.4. Phase de préparation	7
3.4.1. Suivi de projet	7
3.4.2. Études d'exécution	7
3.4.3. Phase de réalisation, Hygiène et sécurité	8
3.4.4. Sécurité du site contre les actes de malveillance.....	8
3.5. Protection des ouvrages	8
3.5.1. Ouvrages existants.....	8
3.5.2. Ouvrages de l'entreprise.....	8
3.5.3. Nettoyage de chantier.....	9
3.5.4. Dépose	9
3.6. Dossier des ouvrages exécutés (DOE).....	9
3.7. Modalités de réception et de recette.....	10
3.7.1. Recette de l'infrastructure réseau et du courant fort (si nécessaire à la migration et à l'installation).....	10
3.7.1.1. Le contrôle visuel	10
3.7.1.2. Le contrôle fonctionnel.....	11
3.7.2. Recette du système de contrôle d'accès.....	12
3.7.2.1. Le contrôle quantitatif.....	12
3.7.2.2. Le contrôle qualitatif.....	12
3.7.3. Cahier de recette.....	12
3.8. Procès-verbal de recette	12
4. ZONES CONCERNÉES	13
5. FONCTIONNALITÉS ATTENDUES	14
5.1. Équipements matériels	14
5.1.1. Contrôleurs locaux	14
5.1.2. Équipements de portes.....	15
5.1.3. Commandes de portes	16
5.1.4. Paramétrages des accès	16

5.2.	Gestion centralisée	19
5.2.1.1.	Gestion multi-sites	20
5.2.1.2.	Gestion des profils	20
5.2.1.3.	L'état des badges	21
5.2.1.4.	Gestion des droits, des groupes	21
5.2.2.	Supervision et traçabilité	22
5.2.2.1.	Gestion des rapports (événements, alarmes, journaux...)	22
5.2.2.2.	Supervision graphique	24
5.3.	Interactivité avec des solutions tiers	25
6.	FORMATION.....	26
6.1.	Généralités	26
6.2.	Public concerné	26
6.3.	Contenu	26
7.	Garantie.....	27
8.	Maintenance et support.....	28
8.1.	Support technique, astreinte téléphonique	28
8.2.	Dépannage (maintenance corrective).....	28
8.3.	Maintenance préventive	29
8.4.	Mises à jour logicielles et matérielles	29
9.	Environnement.....	29
10.	Annexes.....	30

1. INTRODUCTION ET CONTEXTE

1.1. Préambule

Enjeu stratégique

Le projet a pour objectif de moderniser les infrastructures de sûreté de l'Université de Limoges. Il vise à intégrer les technologies les plus récentes et à assurer l'interopérabilité des systèmes de sécurité (vidéoprotection, détection intrusion, portiers vidéos, sécurité incendie) tout en garantissant une continuité de service optimale pour les étudiants, le personnel et les visiteurs.

Enjeu budgétaire de phasage

Le projet vise à migrer nos installations de CADIVS vers une solution unique. Cette migration s'effectuera suivant les budgets alloués aux différentes directions en charge de ce projet. Elle s'étalera donc sur une période qui pourra durer 10 ans maximum.

Le portage du projet est réalisé par 3 entités réunies en comité de pilotage : les Fonctionnaires Sécurité Défense (FSD), la Direction des Systèmes d'Informations (DSI), et la Direction de l'Immobilier, de l'environnement et de la logistique (DIEL)

Cadre réglementaire

- APSAD D83 (contrôle d'accès) et ANSSI-PA-72 (sécurisation des systèmes physiques). Ces références imposent des exigences strictes en matière de résistance aux intrusions, de traçabilité et de chiffrement des données. Les systèmes doivent être conçus pour résister aux attaques physiques et cyber, avec une attention particulière à la chaîne de sécurité (badges, lecteurs, logiciels, centrales d'accès).
- RGPD : La solution doit garantir l'anonymisation des logs et la protection des données personnelles (ex : historiques d'accès). La durée de conservation des données doit pouvoir être ajusté en fonction des évolutions de la législation.
- Accessibilité : Respect des normes PMR (Personnes à Mobilité Réduite).

1.2. Objet de la consultation

Le présent Cahier des Clauses Techniques Particulières (C.C.T.P) décrit les prestations visant à unifier les systèmes de contrôle d'accès installés à l'Université de Limoges dont les objectifs sont les suivants :

- sécurité : sécurisation des bâtiments (campus, bibliothèques, parking, locaux pédagogiques et de recherche, zones à usages restreints – ZRR),
- fluidité des déplacements : améliorer la gestion des flux de personnes,
- conformité : respecter les normes de sécurité et les réglementations en vigueur,
- centralisation et supervision : unifier les dispositifs de contrôle d'accès physique,
- évolutivité (nouvelles fonctionnalités envisagées à court et moyen terme).

L'Accord Cadre est composé d'un lot unique :

Fourniture, installation et paramétrage de contrôles d'accès par badges.

Les travaux sont réalisés dans des bâtiments classés en E.R.P, en Code du Travail et en ICPE. La prestation se fera en site occupé.

2. Présentation de l'établissement

L'université de Limoges possède des bâtiments sur 3 départements : la Haute-Vienne, la Corrèze et la Creuse. Ils se répartissent en plusieurs groupes de différents niveaux d'accès sécurisés :

- les zones à régime restrictif (ZRR, laboratoires de recherche),
- les zones administratives,
- les zones à usage pédagogiques (salles de cours, amphithéâtre,...)
- les zones tout public (bibliothèques, parking,...).

3. PÉRIMÈTRE DU PROJET

3.1. Description de l'existant

Depuis plus de dix ans, l'Université de Limoges a progressivement déployé des systèmes de contrôle d'accès, aboutissant à une infrastructure diversifiée et complexe. Les marques actuellement en place incluent Fichet-Gunnebo, Eden Senator, Vauban-Systèmes, Siemens et Vanderbilt. Cela reflète une évolution technologique et des choix adaptés aux besoins ponctuels de chaque période.

Le parc équipé compte plus de 800 lecteurs répartis sur l'ensemble des sites universitaires. Ces équipements sont pilotés via une quinzaine de serveurs virtualisés, intégrés à l'infrastructure informatique interne de l'établissement. Chaque serveur est dédié à la gestion d'une ou plusieurs zones géographiques, en fonction des systèmes et des marques déployés.

Problématiques identifiées

Hétérogénéité des systèmes : La coexistence de plusieurs marques et générations de matériel entraîne une fragmentation de la supervision et rend difficile une vision globale et centralisée du contrôle d'accès.

Manque de réactivité : En l'absence d'une supervision unifiée, l'université rencontre des difficultés à réagir rapidement en cas d'incident ou de besoin opérationnel urgent.

Vieillesse du parc : Un nombre significatif de lecteurs et de contrôleurs approche ou dépasse leur durée de vie optimale, ce qui pose des risques en termes de fiabilité, de sécurité et de maintenance.

3.2. Description synthétique des prestations

Le projet doit apporter une solution de sûreté des sites universitaires. Il sera unifié à terme avec les systèmes de détection d'intrusion et de vidéoprotection pour assurer la protection des biens selon les exigences fonctionnelles définies dans ce document tout en garantissant la sécurité des personnes conformément aux réglementations en vigueur.

La solution proposée remplace et/ou complète l'installation existante. Elle devra prendre en compte les spécifications des installations existantes (y compris badges existants) à l'université ainsi que les nouveaux points d'accès sécurisés.

Les prestations à réaliser concernent :

- La création d'accès sécurisés (gâches, ventouses, boutons de déverrouillage, ferme-porte, etc.), leur mise en service et leur raccordement au système de contrôle d'accès ;
- La reprise des matériels existants pour assurer la gestion du contrôle d'accès, de l'anti-intrusion et de la vidéoprotection ;
- La formation des personnels de l'université en charge de l'installation des matériels, le maintien en condition opérationnelle et la maintenance préventive de l'installation réalisée.

Pour l'exécution de ces prestations, sont compris :

- la fourniture et l'installation des équipements matériels et logiciels suivant le cahier des charges établi ;
- la reprise de tous les matériels compatibles avec la solution proposée ;
- la dépose soignée, avec stockage, des anciens matériels compatibles et/ou non compatibles avec la solution proposée ;
- la dépose, enlèvement et destruction, des anciens matériels non compatibles avec la solution proposée ;

Attention s'assurer de la suppression de toutes les données pouvant être stockées sur les éléments retirés

- les raccordements et la mise en service des éléments et du système ;
- la fourniture d'un DOE ;
- la garantie de 5 ans sur les matériels et 2 ans sur les logiciels avec clause de rétro-compatibilité pour les mises à jour logicielles ;
- la formation des personnels ;
- une prestation de maintenance préventive la première année.

3.3. Responsabilité et confidentialité

Le titulaire demeurera seul responsable des dégâts qui pourraient être occasionnés dans le cadre de cette opération. En outre, il devra se conformer au règlement intérieur et aux contraintes de fonctionnement de chaque site.

Les candidats s'engagent sur l'honneur à ne pas divulguer, même après la cessation de la prestation, les informations relatives au système d'information de l'Université de Limoges dont ils auraient eu connaissance dans le cadre du présent appel d'offre.

La copie, quel que soit le moyen utilisé, et la détention, en dehors des locaux de l'Université de Limoges, de documents administratifs sont rigoureusement interdits sauf autorisation écrite de l'administration.

Le titulaire est informé que sa prestation au sein de cette entité peut être soumise, sans préavis, à un contrôle de sécurité.

Il reconnaît être informé des conséquences prévues par la loi (code pénal, en particulier les articles 121-2, 411-1, 413-9 à 413-12 et 414-7 à 414-9) et les règlements administratifs, notamment pour le cas où sciemment ou par négligence, il laisserait lesdites informations parvenir à des personnes non autorisées à en connaître.

3.4. Phase de préparation

3.4.1. Suivi de projet

Un chef de projet sera désigné par le candidat. Il sera l'interlocuteur privilégié vis-à-vis du chef de projet de l'Université durant toute la durée du marché.

Le chef de projet assistera aux réunions de chantier assurant le suivi du déroulement de l'opération. Il assistera aussi à toutes les réunions autres que les réunions de chantier qui pourraient être organisées concernant le projet à l'initiative de l'université ou du titulaire.

L'entreprise devra fournir dans son mémoire technique le numéro de téléphone portable et le mail du chef de projet désigné.

3.4.2. Études d'exécution

Le titulaire aura en charge la production des études fondées sur le présent CCTP et des documents joints.

La réalisation ne pourra débuter qu'après approbation du dossier technique d'exécution par le maître d'ouvrage. Le dossier technique d'exécution sera constitué, au minimum, des éléments suivants :

- Les études de conception et de mise en œuvre justifiant les choix technologiques et en particulier la prise en compte des exigences liées à l'intégration des badges universitaires.
- La liste complète des matériels, accessoires et logiciels mis en œuvre ;
- Les documentations techniques des produits et agréments ;
- L'organisation du chantier et notamment :
 - Méthodologie,
 - Planning d'exécution précisant les ressources humaines utilisées,
 - Moyens techniques et humains.

- Les plans d'implantation des équipements ;
- Les schémas d'exécution et schémas unifilaires de raccordements courants fort et faible.

3.4.3. Phase de réalisation, Hygiène et sécurité

Le titulaire devra matérialiser les zones de chantier. Il devra également adapter les conditions de circulation des piétons et véhicules après accord du maître d'ouvrage.

L'entreprise sera tenue de respecter et d'appliquer en tout point les mesures préventives afin de limiter et d'éviter tous risques accidentels sur le chantier, conformément aux différentes lois et décrets.

Le titulaire établira avant toute intervention sur le chantier le Plan Particulier de Sécurité et de Protection de la Santé.

3.4.4. Sécurité du site contre les actes de malveillance

Le titulaire devra garantir la continuité de service des moyens de protection des bâtiments et des biens durant les travaux.

L'organisation des travaux devra garantir une protection effective à la fin de chaque journée de travail.

Des mesures de protection temporaires pourront être envisagées sous réserve d'être validées par l'Université.

3.5. Protection des ouvrages

Une attestation d'assurance décennale valide sera fournie par le candidat.

3.5.1. Ouvrages existants

Lors de toute exécution de travaux, le titulaire devra prendre toutes les dispositions et précautions utiles pour assurer dans tous les cas la conservation sans dommage des ouvrages existants contigus ou situés à proximité.

Ces prescriptions s'entendent tant pour les locaux dans lesquels sont réalisés des travaux que pour ceux utilisés pour le passage des personnels intervenant sous la responsabilité du titulaire.

Toutes ces protections devront être efficaces et devront être maintenues pendant toute la durée nécessaire. L'université se réserve toutefois le droit, si les dispositions prises par le titulaire lui semblent insuffisantes, d'imposer des mesures de protection complémentaires.

3.5.2. Ouvrages de l'entreprise

Le titulaire est responsable des ouvrages jusqu'à la réception. Il lui appartiendra donc d'assurer la protection et la surveillance des travaux ou installations et de faire toutes les réfections nécessaires, notamment pour une parfaite présentation lors de la réception.

3.5.3. Nettoyage de chantier

Le chantier devra toujours être maintenu en parfait état de propreté. Le titulaire aura à sa charge l'enlèvement à la décharge publique des gravats. Seront également à sa charge le nettoyage et le maintien en bon état de propreté des abords du chantier, des locaux utilisés pour le passage des ouvriers. En fin de chantier, le titulaire restituera les existants dans le même état de propreté que celui dans lequel il les a trouvés au démarrage du chantier.

3.5.4. Dépose

Les déposes liées à la réalisation de la solution sont à la charge du titulaire et devront respecter les points suivants :

- Ce démontage sera effectué soigneusement. Tous les câbles, colliers, attaches, ferrures seront enlevés et les trous rebouchés. Les anciennes prises encastrées seront obturées par des caches appropriés.
- Le maintien d'éléments dont le démontage entraînerait des dégradations trop importantes du point de vue esthétique (éclats de peinture, etc.) est soumis à l'accord de l'Université. Ces éléments seraient alors laissés sur place et, pour les câbles, coupés à ras, de manière à rendre leur inutilité évidente et à faciliter leur retrait lors de travaux futurs.

3.6. Dossier des ouvrages exécutés (DOE)

L'ensemble de la documentation, en français, fait partie intégrante de la prestation. Le DOE sera livré impérativement et au plus tard à la réception du chantier. Si à cette date le DOE n'était pas remis, la réception finale ne pourrait être prononcée.

L'ensemble de ces documents sera livré au format papier (2 exemplaires) et au format électronique. Les plans seront fournis aux formats dwg et pdf.

L'ensemble des documents techniques sera fourni avec, en préambule, une présentation globale de l'architecture mise en place et un index des pièces constituant le DOE.

Il comprendra au minimum les documents suivants :

- les schémas de principe généraux et détaillés des installations,
- les schémas de câblage détaillés de l'ensemble des dispositifs mis en œuvre,
- les plans d'implantation des équipements et de l'architecture du système (cheminement des câbles, UTL, lecteur de badge, etc.),
- la nomenclature précise (références produits, versions...) du matériel et des logiciels,
- la documentation technique complète de tous les matériels installés,
- les fiches de tests des équipements,
- les recommandations de maintenance à effectuer et la périodicité prévisible du remplacement des consommables,
- les notices d'utilisation des systèmes, et notamment :

- un manuel d'administration système et des applications;
- un manuel d'exploitation du système ;
- les consignes de sécurité pour le bon usage de la solution ;
- les procédures de sauvegardes.

3.7. Modalités de réception et de recette

La réception de la prestation est conditionnée par la fourniture des DOE et de la documentation détaillée de l'architecture et du système installé (spécifications techniques, paramétrages, configuration et exploitation, plan de recollement, etc.).

La recette technique se compose d'un contrôle d'inventaire, d'un contrôle visuel et d'un contrôle fonctionnel. La recette technique est l'opération qui permet de garantir au maître d'ouvrage que l'installation est conforme :

- au C.C.T.P. ;
- aux performances attendues,
- aux normes et réglementations en vigueur,
- au guide d'installation du constructeur pour l'obtention de la garantie,
- aux règles de l'art.

La partie d'infrastructure réseau Ethernet mise à disposition par l'Université ne fait pas partie de la recette. A contrario, tous les éléments installés, fournis et/ou configurés par le soumissionnaire pour l'utilisation de cette infrastructure sont inclus dans le périmètre de la recette.

3.7.1. Recette de l'infrastructure réseau et du courant fort (si nécessaire à la migration et à l'installation)

3.7.1.1. Le contrôle visuel

Après un contrôle quantitatif et qualitatif des composants fournis, le contrôle visuel portera sur la qualité générale de la prestation. On vérifiera notamment :

- le respect des contraintes d'environnement,
- la mise en œuvre des câbles,
- la fixation des éléments (baies, panneaux, prises, modules, supports, etc.),
- la mise à la terre des éléments,
- l'étiquetage et le repérage des différents éléments,
- l'aspect esthétique,
- le rebouchage.

3.7.1.2. Le contrôle fonctionnel

Le contrôle fonctionnel portera sur le comportement du système installé et plus particulièrement sur son aptitude à supporter les applications telles que définies dans le présent document.

La recette fonctionnelle comprend les tests et mesures effectués sur l'installation de manière exhaustive.

Tous ces résultats seront consignés dans le dossier de recette du pré-câblage au format électronique de type pdf.

Les tests de mesures à effectuer auront pour objet de vérifier que chaque paire est conforme d'une part, au plan d'installation, et d'autre part, à la qualité de transmission exigée.

A ce titre, le contrôle devra s'assurer pour chaque paire :

- du raccordement correct de chaque extrémité et de la continuité de chaque paire ;
- du respect des polarités et de l'absence de court-circuit entre les conducteurs ;
- de l'isolement par rapport à la terre et aux autres conducteurs ;
- de l'absence de dépairage ;
- de la résistance en boucle ;
- de l'exactitude de son identification par rapport aux plans d'installation.

Toutes les liaisons "cuivre" devront être testées en configuration "Permanent Link". Ces tests devront être conformes à la norme ISO/IEC 11801 Edition 2, le câblage conforme au standard EIA/TIA-568-B.

Chaque fiche de test devra au minimum indiquer :

- la date du test,
- l'identification du lien,
- l'affectation des paires (WIRE MAP),
- la longueur des paires,
- l'impédance,
- la résistance de boucle (DC LOOP RESISTANCE),
- la perte par insertion (INSERTION LOSS),
- la paradiaphonie (NEXT et PS NEXT),
- la télédiaphonie (FEXT et PS FEXT),
- le rapport Signal/Bruit (ACR et PS ACR / ELFEXT et PS ELFEXT),
- la perte par réflexion (RETURN LOSS),
- le délai de propagation (PROPAGATION DELAY),
- l'écart de propagation (SKEW).

En outre, la copie du certificat d'étalonnage ou la preuve d'achat (pour un appareil de moins d'un an) du testeur devra accompagner le rapport de test final.

L'ensemble de ces tests est à la charge du titulaire.

3.7.2. Recette du système de contrôle d'accès

3.7.2.1. Le contrôle quantitatif

Le titulaire s'engage à ce que la solution livrée soit protégée contre les virus et les logiciels malveillants connus au jour de l'installation. L'origine des installations, matériels ou logiciels et de leurs mises à jour doit pouvoir être garantie.

3.7.2.2. Le contrôle qualitatif

Le contrôle fonctionnel portera sur le comportement du système installé. La recette fonctionnelle comprend les tests effectués sur l'installation de manière exhaustive. Tous ces résultats seront consignés dans le dossier de recette.

La recette sera effectuée par l'administration en présence du titulaire. Le contrôle devra donc s'assurer :

- du bon fonctionnement individuel des unités de gestions et lecteurs de badge, et de manière générale de chacun des éléments fournis,
- du bon paramétrage et du bon fonctionnement des logiciels de gestion du système,
- des fonctionnalités du système,
- du bon fonctionnement du système dans sa globalité.

3.7.3. Cahier de recette

Toutes les exigences décrites dans les chapitres correspondant et dans les documents annexés sont testées à partir d'un cahier de recette qui sera défini durant les travaux préparatoires. Le titulaire proposera à l'université le cahier de recette que l'administration fait compléter et valider.

Les contrôles sont réalisés en présence du représentant du maître d'ouvrage notamment pour ce qui a trait aux performances des équipements.

3.8. Procès-verbal de recette

Le procès-verbal de recette comportera le compte-rendu des contrôles visuels et fonctionnels. La réception définitive des travaux ne sera prononcée qu'après l'exécution de l'ensemble des essais et contrôles du système installé et après la fourniture du DOE.

Si le procès-verbal fait état de réserves motivées par des omissions ou des imperfections, le titulaire disposera d'un délai de 15 jours pour exécuter les travaux nécessaires. Passé ce délai, le maître d'ouvrage pourra se réserver le droit de faire exécuter les travaux par une autre entreprise, aux frais, risques et périls du titulaire défaillant.

4. ZONES CONCERNÉES

La présente consultation portera sur la migration vers **une solution unique** pour l'ensemble des installations CADIVS de l'Université de Limoges. Les bâtiments de l'Université de Limoges sont répartis sur 3 départements : Haute Vienne, Creuse et Corrèze.

Marché subséquent n°1 : concerne les bâtiments jugés prioritaires par le maître d'ouvrage

- Bâtiment R (DSI) situé sur le campus de la Borie :
 - Migration serveurs (base de données, utilisateurs, ...)
 - Migration installation contrôle d'accès (lecteurs, ventouses, gâches, boutons poussoirs,...), portiers vidéos, alarme intrusion, vidéoprotection, ...
- IUT Egletons :
 - Migration serveurs (base de données, utilisateurs, ...)
 - Migration installation contrôle d'accès (lecteurs, ventouses, gâches, boutons poussoirs,...), portiers vidéos, alarme intrusion, vidéoprotection, ...
- IUT Tulle :
 - Migration serveurs (base de données, utilisateurs, ...)
 - Migration installation contrôle d'accès (lecteurs, ventouses, gâches, boutons poussoirs,...), portiers vidéos, alarme intrusion, vidéoprotection, ...
- IUT Brive :
 - Migration serveurs (base de données, utilisateurs, ...)
 - Migration installation contrôle d'accès (lecteurs, ventouses, gâches, boutons poussoirs,...), portiers vidéos, alarme intrusion, vidéoprotection, ...
- Services centraux :
 - Migration serveurs (base de données, utilisateurs, ...)
 - Migration installation contrôle d'accès (lecteurs, ventouses, gâches, boutons poussoirs,...), portiers vidéos, alarme intrusion, vidéoprotection, ...
- Projet OMEGA HEALTH :
 - Création d'une installation de contrôle d'accès, portiers vidéos, alarme intrusion, vidéoprotection.

Les autres bâtiments feront l'objet de marchés subséquents à la survenance du besoin

5. FONCTIONNALITÉS ATTENDUES

5.1. Équipements matériels

5.1.1. Contrôleurs locaux

La solution permet, sur les équipements contrôlés, l'identification par :

- lecteur de badge seul,
- clavier,
- lecteur de badge et clavier numérique,
- lecteur de badge et lecteur biométrique,
- lecteur biométrique,
- lecteur QR Code via Smartphone.

Chaque lecteur de badges de l'installation est relié au serveur par l'intermédiaire d'un contrôleur local.

Les Unités de Traitement Local (UTL) seront équipées d'une auto-protection qui intégrera la surveillance de l'ouverture et de l'arrachement du coffret et seront installées dans des locaux techniques sécurisés ou à défaut à l'intérieur du local contrôlé.

Toutes les liaisons de type Wiegand non chiffrées, entre un lecteur de badge et un autre équipement, sont interdites (UTL, contrôleur spécifique). La liaison avec le lecteur est réalisée en RS-485 ou en IP ou en Wiegand sécurisé. Cette liaison est, de préférence, bi-directionnelle de bout en bout.

Les contrôleurs communiqueront avec le serveur par liaison Ethernet TCP/IP impérativement. Les contrôleurs locaux (CL) IP doivent posséder leur propre alimentation (non POE).

Les contrôleurs locaux doivent disposer des interfaces d'entrée et de sortie en nombre suffisant pour pouvoir gérer :

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

Les contrôleurs locaux doivent pouvoir supporter la sauvegarde d'au moins 5000 événements en cas de perte du serveur. Ils doivent également disposer de LEDs permettant de visualiser l'état d'un contrôleur durant une opération de maintenance. En mode dégradé, les contrôleurs locaux fonctionnent en tant qu'unités autonomes.

Dans ce mode, les contrôleurs gèrent toutes les demandes d'accès et conservent un journal de toutes les activités (accès, entrées/sorties Tout ou Rien (ToR), alarmes, etc...). Les décisions d'accès sont prises en fonction des données stockées dans le contrôleur au moment de la perte de connexion.

Lorsque la communication est rétablie, les journaux d'activité sont transférés vers le serveur avec l'intégralité de l'historique d'activité (accès et entrées/sorties ToR).

Les contrôleurs locaux IP doivent pouvoir dialoguer de manière chiffrée avec les lecteurs de badges et s'authentifier mutuellement si des mécanismes de mise à jour de clés par le réseau sont disponibles. Ce dernier mode est un avantage à la solution.

Les unités de traitement ne seront pas POE, elles intégreront leur propre alimentation sauvegardée par batterie embarquée, l'alimentation UTL sera intégrée dans le coffret UTL et sera donc auto protégée par surveillance à l'ouverture et à l'arrachement du coffret. Cette alimentation disposera de 3 étages indépendants :

- 1 sortie : alimentation de l'ensemble de la partie électronique (cartes UTL, cartes d'extension et lecteurs),
- 1 sortie : charge de la batterie,
- 1 sortie : alimentation des organes de verrouillage. Chaque voie "organe de verrouillage" sera indépendante. La mise en défaut (court-circuit ou mise à la Terre) d'une voie ne devra mettre hors service que la voie concernée et ne devra pas impacter les autres voies.

Les fonctionnalités assurées en décision locale afin de garantir le fonctionnement en cas de coupure des liens avec le serveur seront :

- la gestion des badges (profils d'accès associés, date d'expiration),
- la gestion de l'environnement porte (porte maintenue ouverte trop longtemps et porte forcée, période d'ouverture automatique),
- la gestion des entrées/sorties (mise en/hors service sur période horaires, temporisations, activation de sortie sur alarme d'une entrée).

5.1.2. Équipements de portes

Toutes les portes faisant partie de la prestation sont ou seront équipées de contact d'ouverture (type magnétique). Ces équipements permettront de remonter l'information d'ouverture de la porte qui sera gérée par le contrôle d'accès (temps d'ouverture trop long,...). L'ensemble des accès sera équipé de ferme-porte, indispensable pour assurer la fermeture après chaque passage. (Ces ferme-portes sont à inclure dans l'offre.)

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

Les issues de secours doivent disposer côté intérieur d'un déclencheur manuel de couleur verte, type DMD permettant le déverrouillage de l'issue sans temporisation.

Le boîtier de déverrouillage de sécurité agit alors par rupture directe de l'alimentation du dispositif de verrouillage. Un contact supplémentaire de détection de rupture est nécessaire. La commande de déverrouillage est distincte de l'ouverture et est mémorisée sur les historiques du système comme alarme. Elle engendre une alarme prioritaire sur les postes d'exploitation opérateur et active une alarme sonore et éventuellement visuelle locale. La sortie nécessite le brisé du scellé du DMD et engage un acte de dégradation volontaire.

En cas d'incendie ou d'urgence, les sorties seront effectuées pour tous les organes par déclenchement manuel DMD (Art C046 règlement ERP)

Les portes peuvent être munies de contact magnétique d'ouverture en feuillure avec un circuit d'auto-protection et d'une bague d'isolement sur porte métallique. Les portes peuvent être munies de contact magnétique d'ouverture en applique.

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

5.1.3. Commandes de portes

Déclencheur Manuel de déverrouillage (DMD)

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

Le boîtier sera muni d'un capot avec scellé. Pour manœuvrer le boîtier, il sera obligatoire de casser le scellé. L'université disposera des outils pour remettre en place les scellés sur les boîtiers verts ouverts. Ces boîtiers seront installés en saillie, plombés, à membrane souple déformable, avec contact de signalisation d'état repris individuellement sur l'installation. Il sera prévu en installation intérieure ou extérieure.

Réarmement à clé du dispositif après activation. Buzzer intégré, voyant d'état.

Respect de la (réglementation CO 46), Norme NFS 61 937.

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

Bouton d'ouverture de porte (BOP)

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

Les boîtiers type de demande de sortie seront posés à 1,20m du sol fini.

5.1.4. Paramétrages des accès

Configuration des accès

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

- Nom physique/Nom logique,
- Délai d'attente de réarmement de la serrure,

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

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

- Activation des béquilles, du cylindre...,
- Boucle anti-sabotage,
- État du DAS (verrouillé/déverrouillé),
- Porte Ouverte/Porte Fermée/Porte Ouverte trop longtemps,
- Position de porte (contre pêne rentré), etc.

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

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

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

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

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

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

Asservissement des accès

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

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

La solution permet de gérer et changer dynamiquement le mode de contrôle du point d'accès en fonction d'événements (calendaires, automatiques comme les identifiants de personne, types de badge) ou d'actions manuelles.

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

Tous les événements associés sont affichables dans la console de gestion des alarmes/événements en fonction du paramétrage du système (affiché/furtif).

La solution de gestion des accès est conforme aux réglementations en matière de sécurité du bâtiment et notamment à la sécurité incendie.

Le système doit pouvoir cohabiter pour les issues de secours avec le système de sécurité incendie (SSI, NF S 61-931). Le système installé est conforme aux différentes règles NF et APSAD relatives à la sécurité incendie pour l'ensemble des équipements installés et du câblage.

Détecteurs d'ouverture

Les contacts d'ouverture sont de type magnétique certifié NF A2P type 3 et peuvent être montés en saillie, en feuillure du côté protégé des portes. Ces derniers disposent des jeux de cales adaptées.

Les détecteurs d'ouverture, adaptés aux supports sur lesquels ils seront installés, permettront la surveillance de tout type d'ouvrants, tant en nature de matériau qu'en type d'ouverture et délivreront les informations minimales suivantes :

- alarme ouverture,
- auto-protection.

Les détecteurs d'ouverture auront les caractéristiques minimales suivantes :

- Auto-protection à l'ouverture,
- Auto-protection à l'arrachement,
- Distance d'ouverture 1,5 cm minimum.

NB : Les portes à double vantail auront chaque vantail surveillé par un contact d'ouverture.

Anti-retour

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

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

- l'événement est seulement archivé,
- l'événement est archivé mais l'accès est refusé.

La fonctionnalité anti-retour est paramétrable par utilisateur ou groupe d'utilisateur et naturellement par secteur. L'opérateur peut accorder un accès malgré une détection anti-retour.

L'opérateur peut accorder l'accès à un groupe d'utilisateur malgré une détection d'anti-retour. L'anti-retour est de type time-back et pass-back.

5.2. Gestion centralisée

La solution est de type client/serveur, le nombre de clients simultanés, supportés par l'appliquatif, doit pouvoir être supérieur à 5 et doit permettre la gestion simultanée de 25 000 porteurs de badges actifs. Le système devra pouvoir gérer au minimum 500 lecteurs de badges.

Le serveur de contrôle d'accès doit pouvoir fonctionner dans trois modes :

- le mode en ligne,
- le mode hybride (certains contrôleurs locaux peuvent fonctionner en mode dégradé),
- le mode «complètement» dégradé.

En ligne, le serveur assure une communication à tout instant avec les contrôleurs locaux. Dans les versions dégradées, les contrôleurs locaux prennent en charge les décisions d'accès et tous les événements sont retransmis au serveur dès réception de la communication.

Le mode dégradé doit pouvoir fonctionner sans limite de durée ni perte de fonctionnalités au-cours du temps. Les badges autorisés présentés à un lecteur de badges concerné par un mode dégradé doivent pouvoir déverrouiller l'accès même s'ils n'ont jamais été présentés sur ce lecteur avant le mode dégradé.

La solution proposée devra être On-Premise. Elle doit impérativement :

- prendre en charge nos badges existants : badges de type Mifare Desfire EV3 2K (format carte de crédit en PVC), personnalisés et équipés d'une puce ISO/IEC 14443-1 avec chiffrement AES,
- s'interfacer avec nos systèmes centraux : connexion obligatoire à notre système de gestion de cartes (EsupSGC) ou, à défaut, à notre annuaire LDAP,
- permettre une automatisation complète : accès intégral aux API pour répondre à nos besoins en automatisation et en interopérabilité avec les autres outils de notre système d'information.

A minima, la solution permet la création de groupes d'utilisateurs en masse, soit par import de fichiers CSV, soit par synchronisation avec une base de données externe, afin de simplifier la gestion des droits et des accès."

Le détail des spécifications de l'infrastructure informatique à mettre à disposition pour l'installation de la solution logicielle devra être décrite avec précision (installation sur une infrastructure virtualisée ou physique, système d'exploitation, version, processeurs, mémoire, etc ...)

Toutes les APIs (Interface de programmation d'application), les connecteurs disponibles par le système seront décrites et devront être exploitables et utilisables sans restriction aucune par la D.S.I. Ils seront utilisables librement par les exploitants de la solution. Les documentations précises de leur utilisation, les mises à jour seront fournies pendant toute la durée de la maintenance de la solution.

Les bases de données et données associées de la solution logicielle seront utilisables et interrogeables sans restriction pendant toute la durée de vie du système.

Le prestataire organise un test de validation du protocole de sauvegarde, incluant un scénario de crash, pour garantir l'intégrité des données après restauration de la base.

5.2.1.1. Gestion multi-sites

La solution devra être capable de gérer plusieurs sites et/ou bâtiments en cloisonnant les droits d'accès selon les besoins.

L'administration précise les profils utilisateurs que devra gérer à minima la solution :

- l'accès « Administrateur système » permettant à un opérateur clairement désigné et habilité, de vérifier le bon état de fonctionnement du dispositif et d'en administrer l'ensemble (paramétrage, configuration, supervision, sauvegardes, lectures, cartographie...) ainsi que la visibilité des informations qu'il contient.
- l'accès « Gestionnaire de badges » permettant à un opérateur, sous-réserve de ses droits, d'administrer et gérer les profils, d'ajouter ou supprimer des droits à des badges, etc.
- l'accès « Opérateur » permettant à un exploitant, sous-réserve de ses droits, de consulter la cartographie, gérer des alarmes, ajouter ou supprimer des droits à des badges, gérer des portes.

5.2.1.2. Gestion des profils

Le système permet de définir des profils d'utilisateurs permettant de gérer des « droits » ou privilèges sur les objets Équipement/Événement/Alarmes/Actions/Espace de Travail dans l'applicatif.

Cette gestion doit, par exemple, quand l'objet est une action, permettre de définir des droits de Création/ Suppression / Exécution/ Modification.

Toutes les actions sur le système sont réservées et protégées par des droits liés au compte applicatif de l'opérateur. Il y a à minima trois types de droits :

- Le droit de lecture confère à un opérateur le pouvoir de visibilité.
- Le droit d'écriture confère à un opérateur un pouvoir d'action.
- Le droit de modification confère à un opérateur les droits de modification.

La solution permet la création de profils à partir de règles d'accès associées à des groupes de points d'accès.

La solution permet l'association de porteurs ou des groupes de porteurs à des règles d'accès et des profils.

La solution permet de paramétrer les droits d'accès en fonction des points d'accès et de plages horaires et calendaires :

- Les plages horaires comprenant chacune 3 intervalles par jour, pour chaque jour de la semaine. Une notion de "jours spéciaux" permettant de programmer des droits d'accès contextuels et non hebdomadaires sera prévue.

- Les jours fériés :
 - ponctuels,
 - annuels reconductibles, jours fériés calendrier français recalculé automatiquement d'une année sur l'autre.

La solution permet la gestion d'un grand nombre de profils (supérieur à 50).

La possibilité d'une gestion des accès aux locaux ou aux zones équipés de contrôle d'accès via le logiciel d'emploi du temps et de gestion des salles de l'université par le biais d'une API sera un plus.

Les comptes et groupes associés à ces profils devront être attachés aux comptes et groupes définis dans le système d'authentification globale de l'Université (annuaire ldap/AD).

En cas de fourniture d'une solution logicielle basée sur une application web, celle-ci devra obligatoirement supporter l'authentification centralisée via le protocole CAS (service SSO) de l'Université.

5.2.1.3. L'état des badges

L'interface de gestion permet de visualiser l'état des badges :

- Actif : Toutes les fonctions prévues
- Inactif : Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge inactivé le jj/mm/aa à hhmh par nom_personne ».
- Perdu : Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge déclaré perdu le jj/mm/aa à hhmh par nom_personne ».
- Volé : Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge déclaré volé le jj/mm/aa à hhmh par nom_personne ».
- Expiré : Le badge n'ouvre aucun accès. Sa présentation sur un lecteur déclenche une alarme précisant : « Badge bloqué le jj/mm/aa à hhmh par nom_personne ».

Les données d'état sont directement approvisionnées par l'application EsupSGC soit par un connecteur existant (API) soit par la mise en place d'un script spécifique.

Toutes les alarmes seront disponibles sur l'application serveur. Les paramétrages par l'envoi de mails automatiques sur certaines alertes seront disponibles.

5.2.1.4. Gestion des droits, des groupes

Les éléments suivants sont configurés en droits (profil par opérateur), pour permettre à minima les fonctions suivantes :

- Des droits sont gérés pour la création/visualisation/configuration des entités du système (utilisateur, badge, alarme, actions, rapport, équipement) ;
- Des droits sont gérés par équipement pour permettre la création, la visualisation, la configuration, le changement d'état (actif/inhibé) ;
- Un équipement (porte, lecteur de badge, détecteur) peut être en accès lecture seule ;

- Une porte en lecture seule permet la visualisation de son état mais inhibe les droits d'actions Ouverture/Fermeture ;
- Des droits sont gérés pour les éléments partagés ;
- Des droits sont gérés pour la création, la visualisation, le déclenchement des actions programmées ou natives ;
- Des droits sont gérés pour la création, la visualisation, la modification de l'espace de travail ;
- Des droits sont gérés pour l'accès aux applications de la solution.

Un opérateur gestionnaire de site doit pouvoir, au minimum :

- disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité ;
- disposer de droit en écriture sur un accès pour l'ouvrir/le fermer ;
- visualiser les caméras définies.

Seuls les opérateurs déclarés avec un profil « administrateur » disposent d'un accès en écriture sur tous les équipements.

Le système de gestion des droits est paramétrable. Le système permet une gestion sécurisée des mots de passe des utilisateurs.

Le système de gestion des droits permet de définir des droits relatifs à la définition/modification de l'espace de travail. La documentation doit fournir une description détaillée des possibilités natives offertes par le système de gestion des droits.

Accès temporaire visiteurs

La solution permettra de créer rapidement un Qrcode temporaire pour un accès amphithéâtre ou parking par exemple pour les participants d'un colloque. La durée maximale d'utilisation d'un accès temporaire par Qrcode sera de 4 jours.

Enrôlement rapide

La solution générera une notification lorsqu'un badge est présenté à un lecteur enrôleur afin d'y associer un utilisateur ainsi que des droits d'accès.

5.2.2. Supervision et traçabilité

5.2.2.1. Gestion des rapports (événements, alarmes, journaux...)

Les rapports standards d'activité courante seront à minima :

- liste des alarmes,
- historique des mouvements d'un utilisateur,
- historique des mouvements de badges,
- liste des badges non présentés dans telle zone depuis N jours (N paramétrable),

- historique des événements par type d'objet,
- taux d'utilisation des lecteurs.

Les rapports d'activité opérateurs seront à minima :

- historique des login,
- journal des acquittements trié par date, filtré pour tout ou partie des opérateurs.

Les rapports liés aux utilisateurs seront à minima :

- liste des badges,
- état des badges,
- liste des badges ayant accès à un ou plusieurs lecteurs,
- liste des badges venant à expiration à une date donnée,
- liste des badges appartenant à une série de groupe d'utilisateurs,
- liste des utilisateurs avec leur fiche d'identification,
- liste simplifiée des utilisateurs.

Les rapports/listing seront sous forme de fichier excel non verrouillé.

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

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

Le système permet une hiérarchisation des alarmes par niveau et une hiérarchisation des événements. Les niveaux d'alarmes doivent pouvoir être filtrés sur la console opérateur et affichés par des signes distinctifs (couleur, etc.). Le terme alarme prioritaire utilisé dans ce document est une alarme de niveau 1. Chaque alarme doit pouvoir être déclarée dans un champ de 1 à 255 caractères. Le système permet d'afficher une procédure à suivre en « alarme ».

Le système permet de gérer des alarmes notifiées par l'opérateur. Le système permet une gestion des alarmes en cascades. Le système sera relié à une messagerie ou un serveur de SMS local ou distant. Il devra permettre l'émission d'alarmes techniques par Email/SMS.

La solution permet la consultation de l'ensemble des actions effectuées sur le système que ce soit au niveau des postes clients ou au niveau du poste serveur mais selon les droits octroyés à l'utilisateur.

Les actions tracées sont à minima :

Système

- Arrêt / Lancement des services applicatifs (journalisation incluse);
- Arrêt critique sur incident ;

- Arrêt système par exploitant (identifiant, date/heure) ;
- Démarrage système par exploitant (identifiant, date/heure) ;
- Événement de ressources systèmes ;

Administration applicative

- Ajout/suppression d'équipements
- Gestion des comptes (création/suppression/modification des droits) Exploitation courante
- Heure de connexion, déconnexion ;
- Action sur un équipement ;
- Action sur un badge

La solution doit protéger cette traçabilité par son système de droits (profil).

5.2.2.2. Supervision graphique

Le système dispose d'un outil de cartographie permettant de localiser tous les équipements de sécurité (portillon, porte surveillée, contrôle d'accès, lecteur NFC, etc...) sur un plan. Le plan et ses équipements peuvent s'afficher à l'échelle (proportion respectées), par zone, par bâtiment et par étage.

La cartographie accepte les fonctions de zooms avant/arrière à partir de la molette de la souris (par exemple). Le système permet de zoomer dans le plan.

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

La cartographie permet d'exécuter des actions de type glisser/déposer de la cartographie vers toute vignette d'affichage pour permettre :

- de visualiser les événements liés à une porte par action de déposer d'une porte vers une fenêtre,
- de visualiser les photos des titulaires identifiés sur une porte par action de glisser déposer d'une porte vers une vignette d'affichage,
- Ouverture/fermeture/mise en service... de toute ou partie des équipements CADIVS depuis la cartographie.

La cartographie permet de proposer une aide contextuelle par équipement. il devra apparaître un encadré dans lequel devra figurer leur appellation, leur position (étage, zone de sûreté...) et les matériels associés.

Ce plan graphique, disponible sur les postes d'exploitation, servira en particulier à la visualisation des événements.

Par ailleurs, ces événements entraîneront une animation des éléments graphiques représentant les équipements des accès concernés.

Lorsqu'un événement se produit dans une zone dont l'accès est contrôlé, chaque équipement du système de contrôle d'accès qui aura déclenché l'alarme, sera automatiquement signalé par un changement de couleur et d'un clignotement sur la cartographie.

5.3. Interactivité avec des solutions tiers

Le titulaire devra fournir un système de contrôle d'accès et un logiciel de supervision pleinement compatibles et interopérables avec les équipements existants et futurs de vidéoprotection, de détection intrusion, de gestion des barrières, ainsi que tout autre dispositif de sûreté ou de sécurité du site.

Cette interopérabilité devra être assurée sans surcoût, sans modification substantielle des installations existantes et au moyen de protocoles et interfaces ouverts, garantissant la pérennité, l'évolutivité et l'intégration globale du système.

5.4. Vidéosurveillance

Dans le cadre de la sécurisation de certains sites sensibles, l'Université souhaite pouvoir déployer un dispositif de vidéoprotection complémentaire au système de contrôle d'accès.

Ce dispositif aura pour finalités :

- la protection des biens et des personnes,
- la levée de doute à distance,
- l'enregistrement d'événements liés aux accès,
- l'aide à la gestion des incidents de sûreté.

Couverture des zones: Les caméras devront être positionnées de manière à couvrir les points d'accès principaux, les zones à accès restreint, les cheminements stratégiques et les espaces présentant un niveau de risque identifié.

Qualité d'image

Les caméras devront offrir une résolution minimale de 2K (1440p) pour garantir une identification claire des individus et des événements. Les caméras devront être équipées de technologies adaptées aux conditions de luminosité variable (jour/nuit, intérieur/extérieur).

Intégration avec le système de contrôle d'accès

Le système de vidéoprotection devra être nativement interopérable avec le système de contrôle d'accès. À ce titre, il devra permettre :

- l'association des flux vidéo aux événements d'accès,
- la visualisation en temps réel lors de déclenchements (alarme, intrusion, accès refusé...),
- la corrélation des journaux d'événements.

Aucune technologie biométrique ne pourra être mise en œuvre sans validation préalable du cadre réglementaire applicable.

Stockage et conservation des données

Les enregistrements vidéo devront être stockés localement sur les infrastructures du système d'information de l'université et bénéficier d'un chiffrement de données et être uniquement accessibles aux personnes habilitées, conformément au RGPD et à la réglementation en vigueur sur la vidéoprotection.

Respect des normes

Le système devra être conforme aux normes EN 62676-4 (vidéosurveillance) et ISO/IEC 27001 (sécurité de l'information). Une attention particulière sera portée à la protection de la vie privée, avec des fonctionnalités de floutage automatique des visages si nécessaire.

6. FORMATION

6.1. Généralités

Une formation pour les personnels techniques amenés à travailler sur le système (installation et paramétrage des UTL, lecteurs,...).

Les formations seront assurées par des animateurs de formation spécialisés et habitués à ces types de formation. Elle se déroulera à temps plein sur le site de l'Université.

L'objectif est, qu'à l'issue de la formation, les personnels soient pleinement opérationnels dans le domaine de travail qu'ils doivent assurer.

Les supports de cours seront fournis en langue française, au format papier et au format électronique lisible à partir de logiciels libres.

6.2. Public concerné

La formation sera assurée pour au moins 6 personnels pour la partie exploitation/administration et 5 personnels pour la partie technique.

6.3. Contenu

La formation assurée devra aborder à minima les points suivants :

Partie administration / exploitation

- La gestion des comptes exploitants et opérateurs,
- La gestion des clés de chiffrement,
- La gestion du temps, des calendriers,
- La gestion des sauvegardes et restauration,
- La gestion des couches graphiques,
- Le stockage et exportation des données,
- L'exploitation du contrôle d'accès,
- La gestion des profils et des badges,
- La gestion des événements et alarmes,
- Tout autre item proposé par le titulaire.

Partie technique

Les personnels de l'université de Limoges à former auront un profil installateur et administrateur. La formation devra porter à minima sur les thèmes suivants :

Bases du contrôle d'accès :

- Principes de sécurité et sûreté,
- Types de contrôle d'accès (badges RFID, claviers à code, biométrie, mobile/NFC),
- Architecture d'un système (lecteurs, centrales, logiciels, réseau).

Installation :

- Câblage (courants faibles),
- Pose et raccordements de lecteurs, ventouses, gâches électriques,
- Alimentation et normes électriques,
- Intégration avec interphonie, vidéosurveillance, alarmes.

Paramétrage et logiciel

- Création des utilisateurs et droits d'accès,
- Gestion des plages horaires,
- Supervision et journal des événements,
- Création des équipements dans la base de données,
- Intégration des fonds de plan des composantes pour gestion depuis logiciel,
- Notions réseau (IP, LAN).

Maintenance et dépannage :

- Diagnostic de pannes,
- Tests et mises en service,
- Maintenance préventive.

Réglementation :

- Normes de sécurité,
- RGPD et protection des données (important pour badges et biométrie),
- Responsabilités de l'installateur.

Le titulaire peut adapter le contenu des formations sous réserve d'accord de l'université. Il indiquera dans sa réponse une durée de formation qu'il jugera adéquat pour répondre au besoin exprimé.

7. Garantie

La garantie couvre le démontage, le remplacement et le remontage de toute partie de la prestation ou de l'équipement qui serait, à l'usage, reconnue défectueuse, hors pièces

d'usure. Cette obligation inclut l'ensemble des frais induits par la remise en état ou le remplacement du matériel, et notamment les frais de déplacement, de main-d'œuvre, d'emballage et de transport, que les opérations soient réalisées sur le lieu d'utilisation de l'équipement ou que celui-ci soit, à la demande du candidat, retourné dans ses établissements.

La garantie couvre également, sans surcoût pour l'Université, les frais de main-d'œuvre et de déplacement du personnel intervenant dans le cadre de ces opérations.

Le candidat ne pourra en aucun cas refuser l'application de la garantie au motif de l'absence de contrat de maintenance préventive.

Un refus de prise en charge ne pourra être opposé que si le candidat démontre de manière objective, documentée et contradictoire que le dysfonctionnement résulte directement et exclusivement d'un manquement avéré aux conditions d'utilisation ou d'entretien prescrites par le constructeur, dûment justifié.

La garantie contractuelle prend effet à compter de la date de réception des prestations prononcée par l'administration. La réception technique du matériel sera quant à elle proclamée dès lors que les tests de réception seront estimés satisfaisants et que la qualité du matériel sera établie en accord avec les objectifs du marché.

8. Maintenance et support

8.1. Support technique, astreinte téléphonique

Une plate-forme téléphonique fonctionnant de 8H à 18H du lundi au vendredi hors jours fériés prendra en compte les incidents.

Les incidents seront enregistrés sous forme de tickets numérotés qui indiqueront :

- l'identité et la localisation du demandeur,
- le descriptif précis du dérangement,
- la date et l'heure de signalisation.

Chaque ticket devra faire l'objet d'une réponse au demandeur par le prestataire dans les 24 heures suivant l'émission de celui-ci.

8.2. Dépannage (maintenance corrective)

Les délais d'intervention pour dépannage devront prendre en compte le niveau de gravité de la situation. L'intervention de dépannage devra s'effectuer sous 5h pour un indice de gravité majeur (libre circulation des personnes, accès aux ZRR...) sans excéder 48h pour toute gravité jugée mineure. L'indice de gravité sera fixé par le maître d'ouvrage.

Sous réserve d'être justifiés, des délais supplémentaires pourront être consentis pour la remise en état définitive sans pour autant dépasser un délai de 5 jours ouvrés. L'entreprise devra prendre toutes les dispositions nécessaires pour respecter ces délais.

Stock de pièces détachées : Imposer un stock minimal sur site (ex : 5% des lecteurs, 10% des contrôleurs) pour les interventions urgentes.

8.3. Maintenance préventive

Les candidats proposeront dans leur offre une prestation de maintenance préventive pour la première année. Le contenu de cette prestation sera décrit dans la réponse du candidat en sachant que l'objectif pour l'université est d'avoir l'assurance d'un système pleinement opérationnel dès sa mise en place. Il est attendu à minima au titre de la maintenance préventive :

- une visite minimum dans l'année suivant la date de réception de système par l'université; cette visite, si elle est unique, devant intervenir dans le mois précédant la date anniversaire de la réception,
- un compte-rendu exhaustif indiquant l'état de fonctionnement de l'ensemble des éléments du système mis en place,
- les mesures à prendre pour corriger les éventuels dysfonctionnements constatés,

la mise à niveau aux dernières versions stables des différents logiciels fournis au titre de la prestation y compris micro- logiciels internes des équipements (UTL, lecteurs de badges, etc.).

8.4. Mises à jour logicielles et matérielles

La prise en charge des mises à jour du logiciel et/ou des matériels par le prestataire est souhaitable. Les conditions et la sécurisation des accès distants devront être effectués suivant la politique de sécurité informatique de l'université.

Dans le cadre du respect des règles ANSSI, les systèmes doivent faire l'objet de corrections permanentes des failles et vulnérabilités référencées (CVE), avec une veille active sur les mises à jour de sécurité.

9. Environnement

Le titulaire est tenu de fournir les données relatives aux émissions de CO2 associées aux produits incluant la phase de fabrications et de transport depuis le site de production jusqu'au lieu de livraison dans nos locaux.

Afin de limiter l'impact environnemental de l'équipement sur l'ensemble de son cycle de vie, le candidat devra préciser dans son offre :

- la durée minimale de disponibilité des pièces détachées, exprimée en années à compter de la mise en service de l'appareil ;
- la durée de vie estimée des pièces critiques, susceptibles d'entraîner l'arrêt de l'équipement en cas de défaillance ;
- le taux de réparabilité de l'appareil, exprimé en pourcentage, indiquant la part des pannes pouvant être réparées sans remplacement complet de l'équipement.

Ces éléments devront permettre d'apprécier la durabilité, la maintenabilité et la réparabilité de l'équipement proposé, dans une logique de réduction des déchets et d'allongement de la durée de vie des matériels.

Par ailleurs, dans le cadre de notre politique de maîtrise de l'énergie, le fournisseur devra fournir les informations sur la consommation énergétique, préciser le rendement énergétique, mentionner la classe énergétique conformément à la réglementation en vigueur et fournir les documents techniques justificatives.

10. Annexes

- **Plans des bâtiments** (zones à équiper) **sur demande** (envoyer une question via la consultation pour obtenir la liste des plans)
- **Liste des équipements existants** **sur demande** (envoyer une question via la consultation pour obtenir la liste des équipements actuellement en place)