

Annexe 3 : Description du marché Contrôle d'accès de l'UCBL.

Lieu(x) d'exécution :

L'exécution des prestations est attendue sur tous les campus et sites d'implantation de l'université Claude Bernard Lyon 1 à l'exception du bâtiment Neurocampus situé sur le site du Vinatier et du bâtiment CENS-ELI situé sur le site de Lyon-Sud.

Pour une description complète du patrimoine de l'université, reportez-vous sur **l'annexe 1 et 2 de ce document**.

Utilisateurs concernés par l'achat :

Le contrôle d'accès est une technique qui consiste à conditionner l'entrée d'un bâtiment ou d'un local interne à une autorisation d'accès. L'ensemble du personnel (permanents, contractuels, hébergés, vacataires, stagiaires) et tous les étudiants (toutes formations confondues) ainsi que des prestataires et visiteurs sont amenés à badger avec leur carte CUMUL. Actuellement il y a **51924** porteurs de cartes dans la base du contrôle d'accès.

Périmètre fonctionnel de la prestation :

Le Contrôle d'accès est un projet transversal faisant appel à plusieurs services au sein de l'université :

- La Direction du Patrimoine pour les prestations de maintenance (préventive et corrective) et la conduite des travaux,
- La Direction de la sécurité pour tous les aspects de sécurisation des bâtiments, horaires ouvrées et étendues, les Zones à Régime Restrictif (ZRR),
- La Direction Générale des Services pour les procédures lors des fermetures administratives,
- Le Service Logistique de Proximité concernant le gardiennage et les prestations de services pour les ménages,
- La recommandation du Service de Prévention est sollicitée pour les sorties à risques,
- La Direction du Système d'Information programme les droits d'accès, gère le serveur (logiciel et matériel) et est chargée du suivi global de la prestation.

Les acteurs du marché :

Service en charge de la consultation	Direction des Achats – Pôle Fournitures et services Bâtiment JV Daubié 43 Bd du 11 novembre 1918 69622 Villeurbanne Cedex
Représentant du pouvoir adjudicateur	Direction du Service Informatique
Services prescripteurs	DIRPAT et Direction Sécurité

Description technique de la prestation :

L'université s'est dotée depuis 2008 du système de gestion centralisée du contrôle d'accès SIPASS de la société SIEMENS (depuis la partie matérielle a été rachetée par la société VANDERBILT). À ce jour **1627** lecteurs de badge (principalement de la gamme Architect STID) sont installés pour contrôler l'accès aux portes extérieures et intérieures des bâtiments, au choix d'un étage dans un ascenseur ainsi qu'aux barrières des parkings. A partir de 2017 tous les lecteurs ont été mis à jour (ou le cas échéant remplacés) afin qu'ils puissent lire aussi bien les cartes MIFARE CLASSIC (UID codés sur 4 octets) que

les cartes MIFARE DESFIRE EV2 (UID codés sur 7 octets) utilisées par le CROUS ou la COMUE de Lyon. Les droits d'accès des utilisateurs ne sont pas déterminés pour chaque individu, mais en fonction de la structure d'appartenance de cet individu. Les informations relatives à la structure d'appartenance sont puisées dans le référentiel de l'établissement.

Les matériels périphériques (VANDERBILT) sont constitués de **88** contrôleurs ACC (dont 37 type G2 ACC5102, 39 type G1 ACC5100, 10 ACC-AP, 2 ACC-lite), 873 modules de raccordement (838 DRI, 16 ERI 8 OPM, 11 DRI(embarque)). Le contrôleur permet de faire la liaison entre le serveur de contrôle d'accès et les équipements terminaux. Il sera relié au serveur SIPASS via le réseau informatique de l'université en RJ45. Il connecte les modules de raccordement DRI, ERI ou OPM via un bus RS485

La version actuelle du logiciel 2.76 n'est plus supportée (plus de support technique de SIEMENS) et le système informatique (version OS, SQL) sera aussi bientôt en fin de support. La nouvelle gamme de licence proposée par SIEMENS impose à l'UCBL de **migrer vers la version 2.95** pour pouvoir commander des nouveaux lecteurs. L'UCBL considère également les possibilités de changer de logiciel de contrôle d'accès pour avoir par la suite une architecture pérenne.

Le rôle du prestataire dans le prochain marché :

Le prestataire intégrateur veillera à ce que le système du contrôle d'accès ainsi que les systèmes associés soient correctement mis en œuvre, intégrés et gérés. Il est aussi source de conseil sur les tendances technologiques et les options qui nous concernent et apporte des idées notamment des solutions de sécurité susceptibles de nous convenir.

Les prestations attendues sont :

- La maintenance corrective et évolutive du logiciel SIPASS. La version actuelle la 2.76 n'est plus supportée, le prestataire devrait nous présenter en option à son offre une proposition de migration logicielle vers 2.95. Pour les prestataires proposant une nouvelle solution il nous faudrait en plus de la future solution, l'engagement de l'interopérabilité avec le système actuel et nous présenter une roadmap de migration vers la nouvelle solution choisie.
- La proposition et la mise en place d'une solution de contrôle d'accès centralisée : La qualité du produit, sa pérennisation, sa flexibilité et son évolutivité devront permettre une amélioration des services (l'authentification, l'autorisation et la traçabilité) ainsi qu'une continuité de service des dispositifs mis en place au sein de l'Université (envoi de code pin(8 chiffres) hebdomadaire à une liste de messagerie pour l'ensemble des barrières, envoi de notification à un Responsable de groupe d'accès, gestion des cartes visiteurs). La synchronisation avec le référentiel de l'université est obligatoire. L'UCBL a une préférence pour un constructeur qui développe aussi bien son logiciel que les matériels périphériques avec des interfaces nécessaires pour assurer l'interopérabilité avec d'autres produits ou l'ajout des fonctionnalités futures.
- La fourniture, la pose, le raccordement, la mise en service et les essais en condition normale d'exploitation des lecteurs de badges, des gâches électriques, des ventouses, des serrures électroniques...etc...
- La fourniture du dossier des ouvrages exécutés (DOE)
- La pose et le raccordement des câbles nécessaires.
- La fourniture et la pose des équipements de serrurerie nécessaires.
- La fourniture et la pose de la porte adaptée selon le cas (porte extérieure ou intérieure)
- La réalisation d'asservissement des lecteurs de badge et des systèmes d'ouverture des portes à certains systèmes d'alarme ou de sécurité incendie.
- La maintenance préventive des lecteurs des portes extérieures et des barrières des parcs de stationnement.
- La maintenance corrective de tous les équipements de contrôle d'accès existants et futurs.
- La tenue à jour et à disposition de l'université, d'un inventaire technique de tous les équipements installés ainsi que toutes les interventions associées et leurs états (demandée, prise en compte, en cours, en attente, Traitée).
- L'exploitation des équipements de contrôle d'accès : les contrôleurs, les modules de raccordement

Contraintes liées à l'exécution :

La mise en place d'un POC est une étape essentielle dans le cas de changement de solution.

Les membres de l'équipe du futur prestataire doivent être certifiés par le constructeur choisi et le prestataire doit s'assurer que l'UCBL est en mesure d'avoir un dialogue direct avec le constructeur et ses développeurs.

Il est fortement souhaité que les membres de l'équipe du futur prestataire affectés au projet UCBL aient des expériences solides de l'environnement SIEMENS et d'une connaissance approfondie de l'état de l'art dans le câblage des bus de données pour le contrôle d'accès.

Le prestataire doit travailler avec les prestataires désignés dans le cadre des travaux de rénovation de bâtiments ou restructuration/construction (sur le domaine de la DOUA) ou de la Requalification et restructuration (Domaine de Rockefeller) étant entendu que seul le prestataire choisi par l'université à l'autorisation de programmer et connecter les lecteurs au logiciel centralisé.

Sauf cas exceptionnel, les prestations se font en zone occupée par conséquent le prestataire est tenu de prendre en compte lors de leur intervention l'emploi du temps des usagers ou le besoin en sécurisation.