

NORMES ET REGLEMENTS APPLICABLES

A-CONTROLE D'ACCES ET ANTI INTRUSION.

A-I Philosophie générale

L'Université de BORDEAUX a mis en œuvre un dispositif de sûreté constitué d'une organisation humaine et de systèmes de sûreté.

Ce document traite des systèmes de sûreté et de leur installation. Ils sont composés d'équipements de contrôle d'accès, de détection d'intrusion, d'anti intrusion, vidéo-surveillance, de serveurs informatique et postes clients de supervision.

Les équipements associés, liés à la protection du patrimoine bâti et non bâti hormis ceux présents dans ce document seront abordés au cas par cas dans les programmes fonctionnels et techniques des opérations, ou, au moment de la formulation du besoin dans le cas d'établissement d'un devis.

Les objectifs principaux de la mise en place des systèmes de sûreté du dispositif de sûreté de l'Université de BORDEAUX et ses partenaires sont :

- De contrôler et filtrer le flux de personnes en gérant les accès (contrôle d'accès),
- D'empêcher et/ou détecter la pénétration des personnes indésirables sur le site (détection intrusion-anti intrusion)

L'Université s'est pourvue d'un ensemble de systèmes d'un même constructeur avec un unique relais informatique de programmation et supervision. Les architectures matérielle et logicielle sont uniformes. L'Université développera son dispositif de sécurité dans cette logique d'uniformité matérielle, logicielle et architecturale.

Dans ce but, ce document définit les règles et prescriptions concernant les équipements et les travaux d'installation des systèmes de sûreté sur les sites de l'université de BORDEAUX et ses partenaires dont les caractéristiques doivent correspondre à une approche cohérente avec la mise en œuvre des équipements et des fonctions du dispositif de sûreté existant.

Les systèmes devront se connecter nativement au serveur MICRO-SESAME de TIL-TECHNOLOGIES présent à l'Université de Bordeaux.

Le fournisseur du système de contrôle d'accès et intrusion devra être le développeur et le concepteur, des parties logicielle et matérielle.

Pour la fiabilité d'approvisionnement des matériels, et dans une démarche environnementale, une préférence sera donnée aux systèmes conçus et fabriqués en France.

Les caractéristiques attendues sont :

- **Compatibilité et ouverture** : Les équipements et matériels proposés pour un système si différent de l'existant seront totalement compatible avec toutes les technologies d'identification (badges, biométrie, etc..) du système existant. Ils permettront également de gérer les alarmes techniques et de superviser des automates et autres équipements techniques en protocole MODBUS RTU ou OPC.

- **Flexibilité** : Les fonctions de sécurité avancée (antiretour, contrôle renforcé, code sous contrainte, etc...) seront préprogrammées, mais le système possédera une capacité de programmation pour permettre la mise en œuvre d'automatismes adaptés à chaque site et à chaque client. Ces automatismes pourront avoir un caractère permanent ou conditionnel (par exemple : gestion de mode crise, etc...).
- **Modularité** : Le système pourra assurer une gestion multi-site et multi-client / multi-entité. Les fonctions de gestion des accès, de gestion de la détection intrusion, d'animation des synoptiques, de gestion des visiteurs, de traçage de courbes, de gestion des rondes, de personnalisation des badges et de communication inter-systèmes, seront assurées par des modules logiciels provenant du même constructeur et donc parfaitement intégrés. Les logiciels de parties tierces ne seront pas admis.
- **Fiabilité** : Le système permettra une gestion intelligente de la maintenance. Notamment, Alarmes sur défaillance (envoi de messages SMS, télémaintenance, etc...). Il proposera des modes, secours, manuel etc... Toutes solutions assurant la continuité de service.
- **Intégration horizontale et verticale** : Des interfaces ou passerelles vers d'autres systèmes (incendie, G.T.B et vidéo protection (GENETEC)) permettront une meilleure intégration des fonctions de sûreté / sécurité. Des passerelles informatiques permettront d'aligner automatiquement la base de données des badges avec celle du service du personnel afin d'éviter les doubles saisies.

A-II Architecture matérielle

A-II.1 ENTITES CONSTITUTIVES DU SYSTEME

- **Niveau 0** : Capteurs, relais : les détecteurs d'ouverture, volumétrique, bris de vitre, sirène, lecteurs de badges, **modules déportés**, autres **équipements terminaux**.
- **Niveau 1** : Automates de terrain sur réseau Ethernet : ici les Unités de Traitement Locales des informations et/ou les centrales d'alarmes.
- **Niveau 2** : Système de supervision serveur et postes clients éventuels.

A-II.1.1 ENTITES DE NIVEAU 0

Alimentation électrique de entités.

Les alimentations principales et leur secours utilisés pour les entités de niveau 0 leur seront dédiées. L'utilisation d'une source commune et de son secours pour des équipements de niveau 0 et 1 est absolument proscrite.

Les lecteurs biométriques

Il devra être proposé des lecteurs d'empreintes digitales adaptés et compatibles avec l'outil de supervision installé Micro Sésame. Ils seront associés selon leur positionnement au module de commande TILLYS le plus proche, le raccordement bus sera sécurisé en communication OSDP.

Matériel :

Ils embarqueront un clavier avec écran et un lecteur de cartes sans contact MIFARE et DESFIRE.

- Lecteur biométrique et clavier, intérieur
- Lecteur biométrique et clavier, extérieur (IP65)

Ces lecteurs biométriques demandés doivent fonctionner aussi bien en mode identification (données biométriques stockées en base de données dans les lecteurs), qu'en mode authentification (données biométriques stockées dans le badge). C'est l'université qui définira le mode de stockage des données, au

cas par cas.

L'environnement de porte

- Boutons-poussoirs de sortie

Les lecteurs seront positionnés pour permettre une ouverture en entrée seulement, la sortie étant libre par pression sur boutons-poussoirs.

- BBG vert (bris de glace)

Conforme à la norme EN 54-11 et la NFS61-936. Déclencheurs manuels à membrane déformables avec indicateur d'alarme (visuel et sonore). Le BBG devra être fixé à 1.3 m par rapport au sol.

Il comportera deux contacts :

- Un contact pour la coupure de l'alimentation de la serrure libérant la porte et relié au SSI
- Un contact d'information pour un report vers la supervision du contrôle d'accès.

- Détecteur d'Ouverture porte (DO)

Chaque ouvrant devra avoir son DO intégré au système de verrouillage (serrure) ou en supplément sur l'accès si non existant pour être relié à une entrée du système de contrôle d'accès qui pourra contrôler, superviser l'état de l'accès et déclencher les alarmes type « effraction porte » et « porte ouverte trop longtemps »

Le câblage du DO devra être du type EQUI avec résistances, afin de remonter l'autoprotection.

- Verrouillages de base

Les portes extérieures devront être équipées à minima de bandeaux de ventouses conformes avec la hauteur de la porte à savoir minimum 2500mm. Le Ral de couleur des bandeaux devra être au choix du client.

Les portes intérieures devront être équipées à minima, si les PV coupe-feu le permettent, de bandeaux ventouse 400 à 600mm centrés au milieu de la porte.

Cas échéant, la validation devra être effectuée par la D2S dans un souci de maîtrise des coûts de maintenance.

Pour la conformité avec les normes appliquées à la réception de public aux universités, les portes seront associées avec bouton-poussoir de sortie et bris de glace vert.

L'asservissement de chaque issue de secours à la détection incendie sera obligatoire.

En effet l'université mettra à disposition la liste des entreprises SSI habilitées sur le(s) site(s) concerné(s), l'entreprise devra ordonner et suivre ces travaux d'asservissements, afin que la conformité incendie du bâtiment soit décernée.

Toute alarme émise par un des équipements de la porte (serrure, ventouse, lecteur, BP, etc) devra déclencher l'enregistrement du flux vidéo par la caméra associée, à T-30 secondes.

Le raccordement des capteurs intrusion

Dans une logique de réduction des coûts de câblage et d'économie d'énergie, les capteurs (contacts de porte, détecteurs volumétriques...) seront raccordés à un ou plusieurs modules d'acquisition, **via des bus RS485 sécurisés et autoalimentés.**

Chaque module d'acquisition comportera 2 bus RS485, permettant chacun le raccordement de 32 capteurs.

Le bus pourra être bouclé, afin de limiter le risque de perte de connexion en cas de rupture physique. Le module d'acquisition devra être en mesure de détecter la coupure et le court-circuit du bus.

Pour le raccordement des capteurs, le constructeur mettra à disposition des transpondeurs, facilement intégrables dans les contacts et radars en lieu et place des résistances d'équilibrage. Chaque transpondeur aura un numéro d'identification unique, la transmission entre le transpondeur et le module d'acquisition sera crypté. Toute tentative de sabotage sera immédiatement détectée.

Les lecteurs debadges

Les lecteurs de badges seront de la gamme Evolution de TIL ou équivalent.

Ils permettront de lire plusieurs technologies : MIFARE® Classic, MIFARE® DESFire® EV1, MONEO, selon les normes ISO14443 A/B niveau 1 à 4.

Il devra être proposé plusieurs gammes de lecteurs selon le niveau de sécurité souhaité :

- Lecture sécurisée : lecture de l'identifiant des badges sécurisé et protégé par une clé. Cette clé sera dans le lecteur et protégée par un mécanisme d'effacement automatique des clés en cas d'arrachement,
- Lecture & communication sécurisée conforme aux préconisations de l'ANSSI architecture 1 :
 - Les lecteurs ne contiennent aucune clé, lecteur dit « transparent »,
 - Lecture de l'identifiant des badges sécurisé et protégé par une clé,
 - Cette clé est contenue dans un coffre-fort HSM/SAM certifié ANSSI EAL5+ dans le module de porte, qui gère le lecteur (voir chapitre ANSSI). Ce module de porte devra être installé dans une baie ou dans un coffret autoprotégé et placé dans un local technique sécurisé,
 - Communication cryptée RS485 AES128 bits directe entre le lecteur, jusqu'à ce module de porte sans convertisseur ou interface. Ainsi les communications seront protégées à l'extérieur du local technique contre toute tentative malveillante,
 - Une analyse périodique de la communication (signal de vie) entre le lecteur et son module déporté lecteur devra permettre de déclencher une alarme si cette communication tombe et de la transmettre à l'UTL et à la supervision centralisée.

Sécurité de la solution & maîtrise des clés de cryptage :

Pour les lecteurs avec lecture sécurisée, la solution devra **obligatoirement** permettre au client final de maîtriser, définir, conserver les paramétrages de sécurité des lecteurs dont ses clés, connues que de lui. L'installateur, le mainteneur ne devront pas avoir connaissance de ses clés.

La solution devra permettre au client final de saisir ses paramètres et ses clés à travers un IHM sur un poste client et un logiciel qui devra être disponible uniquement sur un PC dans un local sécurisé.

Le client final devra être assisté par l'intégrateur ou le constructeur pour le paramétrage au vu des points techniques. Les données critiques à saisir comme mot de passe, clés de sécurité se feront par le client final seul à travers une cérémonie des clés.

La solution devra également permettre de protéger la clé « maître » par la méthode de diversification des clés. Cela consistera à générer une clé différente présente dans chaque badge à partir d'une même clé maître « Card Master Key » et de son UID selon une méthode standard de diversification type « NXP AES128 bits ».

Si le client utilisateur ne souhaitait pas gérer les clés de cryptage nécessaires à la lecture sécurisée des badges, la solution proposée devra permettre de recevoir des lecteurs déjà programmés par le constructeur uniquement. L'installateur, l'intégrateur et le mainteneur ne devront toujours pas avoir connaissance de ses paramètres.

La gamme de lecteurs devra se décliner en plusieurs versions dans chaque niveau de sécurité :

- Version étroite pour montants de porte,
- Version avec clavier pour du contrôle d'accès renforcé (badge + code),
- Version avec écran tactile qui affiche un clavier « tournant » : les chiffres ne sont jamais à la même place.

Les versions Claviers (touches ou écran) doivent permettre de gérer les modes :

- badge + code pour tout le monde tout le temps ou au-delà d'un niveau de crise,
- badges pour le personnel, et des codes pour les visiteurs.

Pour les lecteurs extérieurs, les lecteurs devront avoir un aspect soigné, ainsi qu'une bonne résistance aux intempéries et aux dégradations extérieures. Les lecteurs devront être au minimum anti-vandales IK10, IP65 (hors connectique) et leurs températures de fonctionnement de -10°C à +60°C.

Les lecteurs de badges seront de type proximité passif avec une distance de lecture de l'ordre de 3 à 6 cm. Ils pourront être installés, jusqu'à une distance d'environ 70 mètres de l'UTL.

Une version lecteur de table (lecteur enrôleur avec liaison USB boîtier) sera disponible pour le (ou les) poste(s) de supervision. Le lecteur enrôleur de table pourra intégrer les paramètres de sécurité pour pouvoir lire les badges.

Précaution d'installation :

Les lecteurs ne devront pas être fixés sur une surface métallique (forte diminution de la distance de lecture). Dans les situations qui l'imposaient (mur en béton armé), il faudra informer le client, et faire des tests et prévoir éventuellement des entretoises entre le lecteur et le mur.

Respecter une distance de 30 cm entre 2 lecteurs sur un même plan ou dos à dos sur une même

A-II.1.2 ENTITES DE NIVEAU 1

Alimentation électrique de entités.

Les alimentations principales et leur secours utilisés pour les entités de niveau 1 leur seront dédiées. L'utilisation d'une source commune et de son secours pour des équipements de niveau 0 et 1 est absolument proscrite.

Les Unités de Traitement Local (UTL) en contrôle d'accès et intrusion

L'ensemble des matériels (UTL, modules d'extension, lecteurs,...) et logiciels proposés devront être conformes aux recommandations du guide de l'ANSSI : « SÉCURITÉ DES TECHNOLOGIES SANS-CONTACT POUR LE CONTRÔLE DES ACCÈS PHYSIQUES » (Version du 19/11/2012), selon l'architecture 1 de façon native sans convertisseur.

La solution devra être sécurisée de bout en bout, du badge jusqu'au serveur.

Les principes et fonctionnalités suivants devront être disponibles et réalisés par les équipements et logiciels fournis :

- Conforme ANSSI architecture 1,
- La solution devra être compatible avec le réseau VLAN, VPN du site,
- La solution devra être compatible avec l'annuaire LDAP du site pour la gestion des opérateurs et de leurs droits,
- Communications réseau IP cryptées TLS AES 256 bits et signées (intégrité et authentification) entre le serveur et les UTL d'une part et les postes clients d'autre part,
- Communications bus RS485 cryptées AES 128 bits et signées,
- Toutes les clés de communication sur IP et RS485 devront être changées périodiquement de manière automatique par le système sans action humaine pour durcir le cryptage contre toute malveillance,
- Le client final aura **obligatoirement** la maîtrise de sa clé de communication initiale, qui créera automatiquement les clés suivantes périodiquement, par la saisie, sur un poste client lourd, de cette clé (cérémonie des clés),
- Protection des attaques par déni de service (DoS) par le Firewall des automates UTL,
- Paramétrage de la configuration IP des UTL à travers un Web serveur embarqué sécurisé HTTPS, SSH,
- UTL compatible avec serveur radius 802.1X
- Le module de porte communiquera en bus RS485 crypté AES128 bits avec les lecteurs
- Le module de porte devra **obligatoirement** avoir **un composant SAM/HSM certifié ANSSI EAL5+ soudé sur cette carte** comme imposé, pour leurs besoins propres, par les sites de haute sécurité (ministère des Armées...)
- Ce composant SAM/HSM sera le coffre-fort qui contiendra les clés de l'applicatif « contrôle d'accès » des badges. Ces clés devront être téléchargées depuis un poste client lourd, jusqu'aux modules SAM/HSM pour faciliter la diffusion des clés et pouvoir éventuellement changer les clés de tous les modules depuis le système central, comme demandé dans le guide ANSSI,
- Le client final aura **obligatoirement** la maîtrise de ses propres clés pour toutes les applications du badge (accès, restaurant,...) par la saisie, sur un poste client lourd, de ses clés (cérémonie des clés) **obligatoirement** sur une seule IHM conçue pour cet objectif.
- Cette IHM devra permettre **obligatoirement** de gérer toutes les clés avec une notion de site / organisme possible par clé pour pouvoir différencier les clés par site / organisme, comme demandé dans le guide ANSSI,
- Le principe de diversification des clés devra pouvoir être disponible, activable, et devra permettre au client final de choisir sa formule par un padding personnalisable
- Lecture possible sur le même lecteur transparent jusqu'à 4 types de cartes DESFIRE EV1 (ex carte très haute sécurité corporate + carte sécurisée d'une filiale + carte sécurisée d'un site spécifique),
- Les lecteurs seront conformes ANSSI architecture 1, «lecteur transparent» (aucune clé de cryptage stockée dans le lecteur) et IP65, IK10, pour lire des badges DESFIRE EV1,
- Les lecteurs devront aussi exister en version lecteur + clavier pour identifier une personne, pour un contrôle d'accès renforcé, conforme ANSSI architecture 1, pour lire des badges DESFIRE EV1,
- toutes les entrées seront équilibrées pour l'intrusion **ET le contrôle d'accès** pour détecter les éventuels sabotages

- Le firmware des automates sera téléchargeable depuis les postes clients lourds pour permettre la maintenance corrective et évolutive. Ce firmware sera signé pour valider son intégrité et son authentification.

Les UTL proposées seront de type TILLYS NG ou équivalent. Elles devront permettre la **gestion combinée du contrôle d'accès et de la détection intrusion**, permettant ainsi des automatismes et des asservissements optimisés entre les deux fonctions, des économies d'achat et d'installation.

Elles assureront également des asservissements particuliers tels que la gestion de sas ou d'ouvrants et la gestion des alarmes techniques.

Véritable automate, chaque UTL sera :

- programmable permettant souplesse et adaptation du système aux besoins présents et futurs
- autonome dans la gestion des accès, et intrusion en mode nominal et dégradé
- de **conception industrielle obligatoire** : T : -10°C à + 55°C, alimentation de 10 à 28 Vdc, bornier débrochable, entrée universelle paramétrable (TOR, comptage, équilibrée 4 états ou 5 états) signalisation d'état par LED sur chaque bus, réseau, alim, entrée
- configurable au niveau réseau par un **Web serveur embarqué sécurisé HTTPS**
- d'une **capacité minimum de** :
 - **10 000 badges**, 10 000 événements
 - **8 lecteurs de badge**
 - 1 Prise RJ45 10/100 Mb natif pour être raccordé directement sur un réseau Ethernet avec la possibilité d'un VLAN (réseau local virtuel)
 - 32 jours fériés, **128 programmes horaires**, 32 groupes de points intrusion,
 - **1 à 3 bus RS485 avec une topologie de câblage ouverte (bus, étoile, toile d'araignée) et une longueur jusqu'à 600 mètres obligatoirement** pour avoir une liberté d'installation & d'implantation, et/ou récupérer au mieux les câblages existants.
 - Gérer des modules déportés selon les capacités à gérer sur ses bus RS485 permettant une architecture distribuée ou centralisée
- Devra pouvoir se fixer **sur rail DIN** à intégrer dans une armoire spécifique ou coffret TIL TECHNOLOGIES
- Alimentée par une alimentation chargeur 230Vac/12VDC de **4A minimum** qui permet de :
 - Charger une batterie de 7 AH
 - Avoir les informations défaut secteur, défaut batterie basse, absence de batterie

Sur certains accès extérieurs le demandant, les centrales seront avec l'option XL afin de permettre l'accès aux 70000 étudiants du campus.

Les UTL assureront :

- La gestion combinée du contrôle d'accès et de l'intrusion sans solution tiers
- La mise en œuvre d'automatismes d'ouvrants multiples, tels que gestion de sas, double sens, d'asservissements de type logique combinatoire et événementiel, etc...
- La mise en/hors surveillance des zones intrusions au choix par badgeage sur lecteur, plage horaire, clavier tactile avec éjection des points, asservissements sur entrées. Chaque usager devra être limité dans ses zones intrusions accessibles.
- La remontée des informations de panne ou de malveillance : arrachement, ouverture de coffret autoprotégé, défaut de communication et d'alimentation (secteur, batterie basse, chargeur)
- ultérieurement si le besoin venait, la **transmission à un télésurveilleur par IP** en protocoles ID **contact de toutes les alarmes intrusion (détection) et de contrôle d'accès** directement sans transmetteur physique additionnel. Les synthèses d'alarmes sont exclues. Enfin, le constructeur devra fournir **un certificat de conformité avec ESI et Azur soft** répandus chez les télésurveilleurs.
- **Les UTL devront obligatoirement dialoguer directement entre elles**, sur le ou la partie du réseau Ethernet restant fonctionnelle, pour assurer la gestion antiretour sur plusieurs UTL. Tout système ne permettant pas d'assurer cette fonctionnalité ne sera pas retenu, car il est primordial d'avoir la meilleure continuité opérationnelle possible en l'absence de serveur.

Des modules déportés, eux-mêmes raccordés aux bus des UTL, assureront :

- Température de fonctionnement : -10°C à + 55°C, alimentation de 10 à 28 Vdc,
- Borniers débrochables facilitant le raccordement et la maintenance,
- entrée universelle paramétrable : TOR, comptage, équilibrée 4 états ou 5 états,
- signalisation d'état par LED sur chaque bus, réseau, alim, entrée
- Module déporté conforme ANSSI architecture 1 pour gérer 2 lecteurs de badge transparents (sans clé) pour 2 portes en entrée ou 1 porte en entrée/sortie : 2 bus lecteur RS485 crypté AES128 bits avec son propre fusible réarmable, 9 entrées équilibrées libres de paramétrage (accès, intrusion,

GTB), 2 sorties relais avec choix entre NO/NF et supportant une charge, jusqu'à 2A ou 48 Vdc ou 60 W maxi, composant HSM/SAM certifié ANSSI EAL5+ soudé,

- Module Déporté Intrusion ou GTB permettant de gérer 16 entrées équilibrées qui doivent proposer plusieurs jeux de résistance pour la surveillance de ligne,
- Module déporté disposant de 8 sorties relais avec choix entre NO/NF et supportant une charge jusqu'à 2A ou 48 Vdc ou 60 W maxi.

Le fonctionnement en mode dégradé

Les UTL posséderont et pourront traiter toutes les informations nécessaires à un fonctionnement autonome.

Les autorisations de passage, antiretour, gestion de plages horaires, stockage des informations et événements, broadcast et partage d'informations seront assurés **même en cas de déconnexion du réseau Ethernet**. Lors de la reconnexion du réseau, les informations seront restituées automatiquement au PC serveur.

Sécurité

Fonctionnalité très importante : lors d'un téléchargement, les UTL devront continuer à fonctionner normalement, c'est-à-dire lire les badges, exécuter les automatismes embarqués dans l'UTL (commande de la gâche par exemple), et remonter les événements sur le superviseur en temps réel. Tout système ne permettant pas d'assurer cette fonctionnalité ne sera pas retenu.

A-II.1.3 ENTITES DE NIVEAU 2

Serveur

Les installations seront à raccorder obligatoirement sur le serveur université existant. En effet le PC sécurité université possède une supervision unique et ne prendra pas en compte de nouvelles architectures.

Au cas où le système ne serait pas raccordé sur le serveur existant et donc au PC sécurité, les universités se refusent d'accepter de nouveaux sites après installation.

Dans le cas d'un site distant ou l'installation d'un nouveau serveur indépendant est obligatoire, le système proposé aura une architecture logicielle Client / Serveur. Ce poste serveur sera raccordé sur un réseau de type Ethernet TCP/IP. Il supervisera le dialogue avec les centrales et les postes clients raccordés sur le réseau Ethernet TCP/IP. Il disposera d'une capacité de stockage mémoire permettant le bon fonctionnement des applications.

Le logiciel de contrôle d'accès, intrusion et supervision sera installé sur ce poste, permettant 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 système pourra gérer au minimum 4 096 lecteurs de badges avec une capacité d'extension de 200% et surveiller jusqu'à 40 000 points logiques ou analogiques répartis sur un ou plusieurs sites. En configuration de base, le système devra pouvoir gérer au moins 128 postes clients lourds ou bien dynamiques et légers en connexion TSE.

Poste de travail client

Le ou les postes clients lourds seront raccordés sur le même réseau sûreté que le poste serveur. Ils auront les mêmes capacités de gestion que le poste serveur.

Configuration typique pour le poste client d'une installation moyenne :

- Micro-ordinateur compatible PC (3 GHz),
- Carte Ethernet Gigabit
- 8 Go de RAM
- Disque dur SSD 100 Go minimum
- Écran plat TFT 24", résolution 1920 x 1024 au minimum, (Full HD)
- Clavier, souris, **Windows 10 pro**
- 2 ports USB **3.0**,
- Licence client Microsoft SQL.

A-II.2 ARCHITECTURE DE COMMUNICATION ET RESEAU

Les liaisons radio sont proscrites

Les entités de niveau 0, lecteurs de badges, détecteurs intrusion, etc... seront raccordés sur des modules déportés, eux-mêmes raccordés aux UTL par un bus de terrain RS485.

Pour limiter les problèmes de **ce bus RS485** les installations raccordées en étoiles, ou en toiles d'araignées sont proscrites, les épissures et autres raccordements entre équipements sont proscrits.

Les modules déportés seront installés dans des locaux adaptés des bâtiments, l'installation de modules à l'extérieur des bâtiments dans des équipements techniques comme les fûts de barrières de parking, les chambres de tirages, les boîtes de dérivation etc. Sont proscrites. Si obligation les Armoires extérieures étanches feront l'objet d'une approbation de l'Université et devront présenter toutes les garanties concernant les risques climatiques, de malveillance, et auto-protégées.)

Les entités de niveau 1, Les UTL, seront raccordées directement sur un réseau Ethernet et communiqueront directement avec le serveur sans passerelles ou adaptateurs. L'installation d'UTL à l'extérieur des bâtiments dans des équipements techniques comme les fûts de barrières de parking, les chambres de tirages, les boîtes de dérivation etc. Sont proscrites. Si obligation les Armoires

extérieures étanches feront l'objet d'une approbation de l'Université et devront présenter toutes les garanties concernant les risques climatiques, de malveillance, et auto-protégées.)
Les entités de niveaux 2, serveur, postes client et les consoles de programmation sont existants. Leur installation est réalisée par l'Université.

Dans le cas d'un réseau Ethernet dédié à la sûreté préexistant sur le site :

Dans le cas du réseau Ethernet banalisé de l'Université, la communication s'effectue par le biais d'un V-LAN dédié. Il appartient à l'entreprise de réaliser les travaux de câblage nécessaires selon les prescriptions de l'Université.

La charte informatique ci jointe en annexe définit les attentes de l'Université, elle doit être respectée à la lettre.

Les branchements des câblages verticaux sur les installations de l'Université et l'adressage IP se font sur demande auprès du référent sûreté de l'Université

A-II.3 ARCHITECTURE DE CABLAGE

Câblage liaison RS 485

Câblage.

-Le câble utilisé sera conforme aux prescriptions du fabricant de l'équipement concerné tout en étant conforme en tout point au câblage normé pour une liaison standard RS 485 dans sa performance la plus haute.

-Dans le cas d'une impossibilité de répondre aux deux conditions ci-dessus, il sera mis en place deux câbles pour répondre aux attendus.

-Les liaisons entre équipements se feront sans épissures ni dérivation en « ligne droite », les raccordements en étoiles et toiles d'araignée sont proscrites.

Équipements annexes au câblage.

-Les répéteurs de signaux et changeur de genre seront installés dans des locaux adaptés des bâtiments, leur installation à l'extérieur des bâtiments dans des équipements techniques comme les fûts de barrières de parking, les chambres de tirages, les boîtes de dérivation etc. Sont proscrits.

Si obligation, des Armoires extérieures étanches pourront être utilisées en dernier recours, elles feront l'objet d'une approbation de l'Université et devront présenter toutes les garanties concernant les risques climatiques, de malveillance, et seront auto-protégées.).

-L'alimentation de ces équipements fera l'objet des mêmes exigences de secours que les équipements concernés.

Câblage Ethernet.

Le câblage devra répondre aux exigences de la charte informatique de l'Université ci jointe en annexe.

Nota bene

Une seule connexion Ethernet par câble.

L'utilisation de répéteurs ou concentrateurs sont proscrits

Condition de pose et réalisation des travaux

Des documents d'exécution seront rendus et soumis à l'approbation de l'université.

A-II.1.4 SERRURES MOTORISEES ET BLOCS PORTES

BLOC-PORTE ANTI-EFFRACTION CR4 CERTIFIE A2P LOCAUX TECHNIQUES

Bloc-porte antieffraction classe CR4 selon norme NF EN1627 (PV émis par un laboratoire indépendant à fournir) et certifié A2P CR4 bloc-porte locaux techniques.

Le bloc-porte est composé d'un bâti tubulaire permettant de nombreuses configurations de pose, d'un vantail affleurant à structure métallique avec profil anti-dégondage toute hauteur et de paumelles à roulement à billes. Il ne devra pas avoir de barre de seuil, afin de permettre un accès aisé.

Il sera équipé de :

- Serrure motorisée 4 points à pêne crochet et encastrée dans l'ouvrant
- Gestion électronique du cylindre permettant la détection des attaques et le blocage du cylindre à distance
- Fonctionnement à sécurité négative (à émission de courant). La porte doit rester verrouillée même en cas de coupure d'alimentation.
- Pêne demi-tour anti-rebond pour garantir la fermeture de la porte en toute situation
- Connexion par BUS RS485 et communication par protocole propriétaire
- Cylindre européen double entrée haute sûreté Protec² avec 3 clés brevetées
- Poignée de tirage extérieure avec bloc de protection cylindre
- Palette de sortie libre EXEA conforme à la norme EN179 avec bouton de sortie intégré
- Ferme-porte encastré conforme à la norme EN 1154 avec réglage de la force, de la vitesse initiale, de l'à-coup final, et frein à l'ouverture.
- Rejet d'eau si la porte donne sur l'extérieur
- Finition gris RAL7031, ou blanc RAL 9010 selon choix du Maître d'Ouvrage.

OPTION : Pare-balle FB4 selon la norme européenne EN 1522

OPTION : Résistance au feu EI260

OPTION : microviseur simple ou pare-balle

OPTION : Palette de sortie contrôlée EXEA Control

BLOC-PORTE ANTI-EFFRACTION CR3

Bloc-porte antieffraction classe CR3 selon norme NF EN1627 (PV émis par un laboratoire indépendant à fournir).

Le bloc-porte est composé d'un bâti tubulaire permettant de nombreuses configurations de pose, d'un vantail affleurant à structure métallique avec profil anti-dégondage toute hauteur et de paumelles à roulement à billes. Il ne devra pas avoir de barre de seuil, afin de permettre un accès aisé.

Il sera équipé de :

- Serrure motorisée 4 points à pêne crochet et encastrée dans l'ouvrant
- Gestion électronique du cylindre permettant la détection des attaques et le blocage du cylindre à distance
- Fonctionnement à sécurité négative (à émission de courant). La porte doit rester verrouillée même en cas de coupure d'alimentation.
- Pêne demi-tour anti-rebond pour garantir la fermeture de la porte en toute situation
- Connexion par BUS RS485 et communication par protocole propriétaire
- Cylindre européen double entrée haute sûreté Protec² avec 3 clés brevetées
- Poignée de tirage extérieure avec bloc de protection cylindre
- Palette de sortie libre EXEA conforme à la norme EN179 avec bouton de sortie intégré
- Ferme-porte encastré conforme à la norme EN 1154 avec réglage de la force, de la vitesse initiale, de l'à-coup final, et frein à l'ouverture.
- Rejet d'eau si la porte donne sur l'extérieur
- Finition gris RAL7031, ou blanc RAL 9010 selon choix du Maître d'Ouvrage.

La même gamme de bloc-porte devra équiper l'ensemble des accès de niveau antieffraction CR3 ou CR4 que les portes soient simples ou double-vantail, coupe-feu et/ou issues de secours afin de faciliter la maintenance et assurer une harmonisation esthétique et des équipements.

OPTION : double vantail

OPTION : Coupe-feu 30 minutes

OPTION : Microviseur simple ou coupe-feu

OPTION : Ferme-porte encastré

OPTION : Palette de sortie contrôlée EXEA Control

SERRURE MOTORISÉE MULTIPPOINTS HAUTE SÉCURITÉ – SORTIE LIBRE

Afin d'assurer la sécurité des lieux et le bon fonctionnement du système de contrôle d'accès, il sera prévu

un système de verrouillage multipoints motorisé [encastré dans] des portes concernées, y compris sur les portes coupe-feu.

Elles disposeront des caractéristiques et performances suivantes :

- Serrure 4 points avec crochets en acier monobloc 9mm
- Résistance à l'effraction d'une valeur supérieure à 1,3 tonne par pêne
- Testées à 1 million de cycles pour un usage très intensif
- Alimentation bi-tension 12V-24V
- Consommation maximum de 1.4A en courant d'appel moteur
- La serrure devra impérativement être toutes mains (droite/gauche et poussant/tirant) pour que la maintenance ultérieure puisse être effectuée par un seul et unique modèle.
- Sortie par simple abaissement de la béquille et en une seule manœuvre conformément au Code du travail. Cette béquille sera donc toujours active.
- Déverrouillage rapide impérativement inférieur à 0,5 seconde.
- Verrouillage mécanique et automatique à chaque fermeture de porte
- La porte doit rester fermée et verrouillée même en cas de mode dégradé (absence de courant, foudre, panne...) pour empêcher tout accès de l'extérieur.
- 3 organes de manœuvre indépendants pour assurer une sécurité optimum des biens et des personnes: moteur – clé – béquille
- Connexion au système de contrôle d'accès par BUS RS485 pour assurer une sécurité maximum des données. Remontée des informations de la serrure sur le système de contrôle d'accès par un protocole propriétaire.

La mise en œuvre des serrures sera adaptée en fonction du support de la porte (bois, métal ou verre).

Il appartient au présent lot de s'assurer que les équipements soient mis en place conformément au procès-verbal du fabricant de serrures.

L'alimentation et le raccordement au contrôle d'accès sont dus par le lot électricité.

SERRURE MOTORISÉE MULTIPOINTS A ENCASTRER A SÉCURITÉ NÉGATIVE – SORTIE LIBRE POUR PORTE A TRAFIC INTENSIF

Les portes contrôlées seront équipées de serrures électriques motorisées multipoints encastrées dans l'ouvrant, composées du coffre de serrure, de la gâche, d'un câble multipair de 6 mètres avec connecteur rapide et d'un boîtier de raccordement électronique déporté.

Elles disposeront des performances suivantes :

- Résistance à l'effraction d'une valeur supérieure à 1 tonne par pêne
- Testées à 50000 manœuvres
- Alimentation bi-tension 12V-24V
- Déverrouillage rapide impérativement inférieur à 0,7 seconde.
- La serrure devra impérativement être toutes mains (droite/gauche et poussant/tirant) pour que la maintenance ultérieure puisse être effectuée par un seul et unique modèle.
- Verrouillage automatique en 3 points sécurisé par le contre pêne de sécurité et le pêne demi-tour afin d'empêcher les sorties de pêne accidentelles, et rappel automatique du pêne s'il est sorti porte ouverte.
- Temporisation d'ouverture réglable 2 à 15 secondes ou maintien ouvert sans limites de temps sur signal maintenu
- Axe et entraxe, respectivement à 50mm/70mm (menuiseries bois) et 35mm/92mm (menuiseries alu, PVC, métal), selon le standard français (autres refusés).
- Produit certifié (CE) selon normes EN179 pour les fermetures d'urgence et EN1125 pour les fermetures anti paniques.

Les serrures seront raccordées avec le système de Contrôle d'accès (Ordre à temporiser), et seront aptes à recevoir les commandes ou donner les informations suivantes :

- Activation de la béquille intérieure.
- Position du pêne (entrée/sortie)
- Position de porte (contre pêne rentré + pêne sorti).
- Activation du cylindre.
- Boucle anti-sabotage.

Sur les portes à deux battants, il sera prévu un contact d'alarme sur le battant semi-fixe pour signaler son ouverture. Ce contact sera raccordé sur l'électronique du lecteur accès ou de la centrale intrusion.

La liaison entre huisserie et battant sera faite par flexible invisible.

Les dispositifs seront alimentés directement par les alimentations des lecteurs de contrôle d'accès.

La mise en œuvre des serrures sera adaptée en fonction du support de la porte (bois, métal ou verre).

Il appartient au présent lot de se rapprocher du lot menuiserie intérieure et/ou serrurerie afin de s'assurer

que les blocs-portes assurent le degré coupe-feu ou pare-flamme demandé au lot menuiserie intérieure et/ou serrurerie, et pour que les équipements soient mis en place conformément au procès-verbal du fabricant de serrure.

OPTION :

Les serrures devront être équipées d'un KIT ensemble barreur composé d'une béquille extérieure et d'une barre antipanique inox intérieur. L'ensemble devra être conforme à la norme EN1125

SERRURE MOTORISÉE MULTIPOINTS EN APPLIQUE A SÉCURITÉ NÉGATIVE – SORTIE LIBRE POUR PORTE A TRAFIC INTENSIF

Les portes contrôlées seront équipées de serrures électriques motorisées multipoints posées en applique. Le bandeau finition inox sera composé du coffre de serrure, de la gâche, d'un câble multipaires de 6 mètres avec connecteur rapide et d'un boîtier de raccordement électronique déporté.

Elles disposeront des performances suivantes :

- Résistance à l'effraction d'une valeur supérieure à 1 tonne par pêne
- Testées à 50000 manœuvres.
- Alimentation bi-tension 12V-24V.
- Déverrouillage rapide impérativement inférieur à 1 seconde.
- La serrure devra impérativement être toutes mains (droite/gauche et poussant/tirant) pour que la maintenance ultérieure puisse être effectuée par un seul et unique modèle.
- Verrouillage automatique en 3 points sécurisés par le contre pêne de sécurité et le pêne demi-tour afin d'empêcher les sorties de pêne accidentelles, et rappel automatique du pêne s'il est sorti porte ouverte.
- Temporisation d'ouverture réglable 2 à 15 secondes ou maintien ouvert sans limites de temps sur signal maintenu
- Axe et entraxe, respectivement à 50mm/70mm (menuiseries bois) et 35mm/92mm (menuiseries alu, PVC, métal), selon le standard français (autres refusés).
- Produit certifié (CE) selon normes EN179 pour les fermetures d'urgence et EN1125 pour les fermetures anti paniques.

Les serrures seront raccordées avec le système de Contrôle d'accès (Ordre à temporiser), et seront aptes à recevoir les commandes ou donner les informations suivantes :

- Activation de la béquille intérieure.
- Position du pêne (entré/sorti)
- Position de porte (contre pêne rentré + pêne sorti).
- Activation du cylindre.
- Boucle anti-sabotage.

La liaison entre huisserie et battant sera faite par flexible métal en applique diamètre intérieur 11mm.

Les dispositifs seront alimentés directement par les alimentations des lecteurs de contrôle d'accès.

La mise en œuvre des serrures sera adaptée en fonction du support de la porte (bois, métal ou verre).

Il appartient au présent lot de se rapprocher du lot menuiserie intérieure et/ou serrurerie, afin de s'assurer que les blocs-portes assurent le degré coupe-feu ou pare-flamme demandé au lot menuiserie intérieure et/ou serrurerie, et pour que les équipements soient mis en place conformément au procès-verbal du fabricant de serrures.

SERRURE MOTORISÉE 1 POINT A SÉCURITÉ NÉGATIVE – SORTIE LIBRE POUR PORTE A TRAFIC INTENSIF

Les portes contrôlées seront équipées de serrures électriques motorisées à encastrer dans l'ouvrant, composées du coffre de serrure, de la gâche et d'un câble multipaires de 6 mètres avec connecteur rapide. Conformément à la norme EN14846, elles disposeront des performances suivantes :

- Résistance à l'effraction d'une valeur supérieure à 1 tonne par pêne
- Alimentation bi-tension 12V-24V
- Déverrouillage rapide impérativement inférieur à 0,7 seconde
- La serrure devra impérativement être toutes mains (droite/gauche et poussant/tirant) pour que la maintenance ultérieure puisse être effectuée par un seul et unique modèle.
- Verrouillage automatique en 2 points sécurisé par le contre pêne de sécurité et le pêne demi-tour afin d'empêcher les sorties de pêne accidentelles, et rappel automatique du pêne s'il est sorti porte ouverte.
- Temporisation d'ouverture réglable 2 à 15 secondes ou maintien ouvert sans limites de temps sur signal maintenu
- Axe et entraxe, respectivement à 50mm/70mm (menuiseries bois) et 35mm/92mm (menuiseries alu, PVC, métal), selon le standard français (autres refusés).
- Produit certifié (CE) selon normes EN179 pour les fermetures d'urgence et EN1125 pour les fermetures anti paniques.

Les serrures seront raccordées avec le système de Contrôle d'accès (Ordre à temporiser), et seront aptes à recevoir les commandes ou donner les informations suivantes :

- Activation de la béquille intérieure.
- Position du pêne (entré/sorti)
- Position de porte (contre pêne rentré + pêne sorti).
- Activation du cylindre.
- Boucle anti-sabotage.

Sur les portes à deux battants, il sera prévu un contact d'alarme sur le battant semi-fixe pour signaler son ouverture. Ce contact sera raccordé sur l'électronique du lecteur accès ou de la centrale intrusion. La liaison entre huisserie et battant sera faite par flexible invisible.

Les dispositifs seront alimentés directement par les alimentations des lecteurs de contrôle d'accès.

La mise en œuvre des serrures sera adaptée en fonction du support de la porte (bois, métal ou verre).

Il appartient au présent lot de se rapprocher du lot menuiserie intérieure et/ou serrurerie afin de s'assurer que les blocs-portes assurent le degré coupe-feu ou pare-flamme demandé au lot menuiserie intérieure et/ou serrurerie, et pour que les équipements soient mis en place conformément au procès-verbal du fabricant de serrures.

OPTION :

Les serrures devront être équipées d'un KIT ensemble barreur composé d'une béquille extérieure et d'une barre antipanique inox intérieure. L'ensemble devra être conforme à la norme EN1125.

SERRURE ÉLECTRIQUE 1 POINT A CONTRÔLE DE BÉQUILLE EXTÉRIEURE – SORTIE LIBRE

Les portes contrôlées seront équipées de serrures électriques à contrôle de béquille à encastrer dans l'ouvrant, composées du coffre de serrure, de la gâche, d'un câble multipaires de 6 mètres avec connecteur rapide, et d'une paire de carrés séparés.

- La sortie s'effectuera par la béquille intérieure toujours active.
- Entrée par béquille active ou inactive selon l'état électrique (paramétrable émission-rupture)
- Conformées à la norme EN14846, elles disposeront des performances suivantes :
- Résistance à l'effraction d'une valeur supérieure à 1 tonne par pêne
- Alimentation bi-tension 12V-24V
- La serrure devra impérativement être toutes mains (droite/gauche et poussant/tirant) pour que la maintenance ultérieure puisse être effectuée par un seul et unique modèle.
- Verrouillage automatique en 2 points sécurisé par le contre pêne de sécurité et le pêne demi-tour afin d'empêcher les sorties de pêne accidentelles.
- Axe et entraxe, respectivement à 50mm/70mm (menuiseries bois) et 35mm/92mm (menuiseries alu, PVC, métal), selon le standard français (autres refusés).

Les serrures seront raccordées avec le système de Contrôle d'accès (Ordre à temporiser), et seront aptes à recevoir les commandes ou donner les informations suivantes :

- Activation de la béquille intérieure.
- Position du pêne (entré/sorti)
- Position de porte (contre pêne rentré + pêne sorti).
- Activation du cylindre.
- Boucle anti-sabotage.

Sur les portes à deux battants, il sera prévu un contact d'alarme sur le battant semi-fixe pour signaler son ouverture. Ce contact sera raccordé sur l'électronique du lecteur accès ou de la centrale intrusion.

La liaison entre huisserie et battant sera faite par flexible invisible.

Les dispositifs seront alimentés directement par les alimentations des lecteurs de contrôle d'accès.

La mise en œuvre des serrures sera adaptée en fonction du support de la porte (bois, métal ou verre).

Il appartient au présent lot de se rapprocher du lot menuiserie intérieure et/ou serrurerie afin de s'assurer que les blocs-portes assurent le degré coupe-feu ou pare-flamme demandé au lot menuiserie intérieure et/ou serrurerie, et pour que les équipements soient mis en place conformément au procès

SERRURE ÉLECTRIQUE MULTIPOINTS A CONTRÔLE DE BÉQUILLE EXTÉRIEURE – SORTIE LIBRE

Les portes contrôlées seront équipées de serrures électriques à contrôle de béquille à encastrer dans l'ouvrant, composées du coffre de serrure, de la gâche, d'un câble multipaires de 6 mètres avec connecteur rapide, et d'une paire de carrés séparés.

- La sortie s'effectuera par la béquille intérieure toujours active.
- Entrée par béquille active ou inactive selon l'état électrique (paramétrable émission-rupture)
- Conformées à la norme EN14846, elles disposeront des performances suivantes :
- Résistance à l'effraction d'une valeur supérieure à 1 tonne par pêne
- Alimentation bi-tension 12V-24V

- La serrure devra impérativement être toutes mains (droite/gauche et poussant/tirant) pour que la maintenance ultérieure puisse être effectuée par un seul et unique modèle.
- Verrouillage automatique en 2 points sécurisé par le contre pêne de sécurité et le pêne demi-tour afin d'empêcher les sorties de pêne accidentelles.
- Axe et entraxe, respectivement à 50mm/70mm (menuiseries bois) et 35mm/92mm (menuiseries alu, PVC, métal), selon le standard français (autres refusés).

Les serrures seront raccordées avec le système de Contrôle d'accès (Ordre à temporiser), et seront aptes à recevoir les commandes ou donner les informations suivantes :

- Activation de la béquille intérieure.
- Position du pêne (entré/sorti)
- Position de porte (contre pêne rentré + pêne sorti).
- Activation du cylindre.
- Boucle anti-sabotage.

Sur les portes à deux battants, il sera prévu un contact d'alarme sur le battant semi-fixe pour signaler son ouverture. Ce contact sera raccordé sur l'électronique du lecteur accès ou de la centrale intrusion.

La liaison entre huisserie et battant sera faite par flexible invisible.

Les dispositifs seront alimentés directement par les alimentations des lecteurs de contrôle d'accès.

La mise en œuvre des serrures sera adaptée en fonction du support de la porte (bois, métal ou verre).

Il appartient au présent lot de se rapprocher du lot menuiserie intérieure et/ou serrurerie, afin de s'assurer que les blocs-portes assurent le degré coupe-feu ou pare-flamme demandé au lot menuiserie intérieure et/ou serrurerie, et pour que les équipements soient mis en place conformément au procès-verbal du fabricant de serrures.

LECTEURS AUTONOMES BÉQUILLE OU CYLINDRE SANS-FIL CONNECTES EN TEMPS RÉEL SUR LE SYSTÈME DE CONTRÔLE D ACCÈS EXISTANT :

Le système de sûreté globale centralisé (contrôle d'accès, vidéo, détection intrusion) devra impérativement intégrer nativement une gamme complète de solutions de type cylindres, béquilles et serrures électroniques sans fil temps réel.

L'architecture sera impérativement basée sur :

- - Des Hubs radio RS485 raccordés à des UTL de contrôle d'accès (les Hubs ne pourront gérer plus de 8 produits dans un environnement de 25 mètres) qui dialogueront en zigbee sécurisé avec les produits sans fil. Des produits sans fil de type :
 - Béquilles électroniques sur plaque
 - Poignées électroniques sur rosaces
 - Cylindres électroniques

Les produits intégreront des piles standards au lithium, afin que celles-ci puissent être changées par l'exploitant sans nécessité de faire appel au fabricant (piles disponibles dans le commerce).

Les lecteurs devront permettre la lecture indifférente de badges de différentes technologies en 13.56MHz (les différentes technologies de badges pourront cohabiter sur le même site).

Ils répondront aux caractéristiques minimales suivantes :

Cylindres électroniques Temps réel

Ils seront impérativement de type cylindre européen avec bouton mécanique intérieur pour déverrouillage conforme au code du travail.

Le bouton extérieur sera équipé d'une signalisation lumineuse tri couleur indiquant la prise en compte puis la validation ou non du badge, cette led devra être visible sur le périmètre du bouton pour garantir une acquisition malgré la présence du badge devant le bouton.

La tête de lecture devra impérativement permettre un embrayage du cylindre en moins de 0.5 seconde sur badge autorisé.

Afin d'assurer une maintenance efficace sur les portes équipées de lecteurs de contrôle d'accès sans fil, les événements suivants devront être remontés en temps réel sur les synoptiques graphiques du contrôle d'accès ou au fil de l'eau sans aucune manipulation de l'utilisateur sur le superviseur :

- niveau batterie basse,
- perte de la liaison sans fil entre le hub et le lecteur,
- lecteur absent (ou endommagé),
- problème de communication entre le contrôleur de porte et le hub de communication,

La traçabilité des badgeages se fera impérativement en temps réel dans le fil de l'eau de la supervision sans action manuelle sur le logiciel.

En cas de piles trop faibles pour faire fonctionner l'équipement, une connexion sera disponible sous le capot du cylindre pour brancher un élément de secours standard par micro USB (pas de solution de secours propriétaire).

Le produit intégrera des piles standards au lithium, afin que celles-ci puissent être changées par l'exploitant sans nécessité de faire appel au fabricant (piles disponibles dans le commerce).

Le produit aura une faible consommation, afin de garantir une durée de vie minimum des piles de 2 ans (à 10 ouvertures par jour).

Le cylindre devra pouvoir être installé aussi bien sur des portes intérieures qu'extérieures protégées avec un degré minimum IP54 et plage de températures de -20°C à +45°C (pour des questions de maintenance, un seul type de produit pour ces deux configurations intérieures et extérieures).

Il sera possible à tout moment depuis la gestion centralisée de donner un ordre d'ouverture à distance du produit.

Des plages horaires d'ouverture libre par rotation du cylindre seront gérables directement depuis le logiciel de contrôle d'accès.

Dans l'objectif de limiter le nombre de systèmes d'exploitation et de simplifier la formation des utilisateurs, toutes les réponses ne permettant pas la gestion des droits d'accès et informations sur le poste central du fournisseur de contrôle d'accès ne pourront être prises en compte.

Pour des raisons de sécurité, tous les systèmes impliquant le stockage d'informations dans le badge de l'utilisateur seront refusés.

Ensembles plaques Béquilles électroniques Temps réel

Ils seront de type béquille électronique au standard français entraxe 70 mm pour les portes pleines ou entraxe 92 mm pour les profils étroits.

Les plaques béquilles pourront être choisies avec percement pour cylindre de secours au profil européen ou sans.

Le produit sera complètement réversible (droite, gauche, poussant, tirant) afin de permettre une bonne gestion du SAV et de la maintenance.

Pour assurer une pérennité dans le temps, le produit devra impérativement être fixé en traversant avec au minimum 2 piliers de fixation en points haut et bas.

La plaque béquille extérieure sera équipée d'une tête de lecture intégrée avec signalisation lumineuse tri couleur indiquant la prise en compte puis la validation ou non du badge. Un signal sonore pourra également être paramétré pour l'accessibilité PMR.

La tête de lecture devra impérativement permettre un embrayage de la béquille en moins de 0.5 seconde sur badge autorisé.

Afin d'assurer une maintenance efficace sur les portes équipées de lecteurs de contrôle d'accès sans fil, les événements suivants devront être remontés en temps réel sur les synoptiques graphiques du contrôle d'accès ou au fil de l'eau sans aucune manipulation de l'utilisateur sur le superviseur :

- niveau batterie basse,
- perte de la liaison sans fil entre le hub et le lecteur,
- lecteur absent (ou endommagé),
- problème de communication entre le contrôleur de porte et le hub de communication,
- béquille abaissée

La traçabilité des badgeages se fera impérativement en temps réel dans le fil de l'eau de la supervision sans action manuelle sur le logiciel.

En cas de piles trop faibles pour faire fonctionner l'équipement, une connexion sera disponible en façade du lecteur pour brancher un élément de secours standard de type micro USB (les solutions propriétaires seront proscrites).

Le produit intégrera des piles standards au lithium, afin que celles-ci puissent être changées par l'exploitant sans nécessité de faire appel au fabricant (piles disponibles dans le commerce).

Le produit aura une faible consommation, afin de garantir une durée de vie minimum des piles de 4 ans (à 30 ouvertures par jour).

Suivant les modèles, la béquille sera destinée à un usage intérieur (IP52 0 à 60°C) ou extérieur (IP54 -25 à 60°C).

Sur certains accès, le produit pourra être équipé d'un dispositif de débrayage automatique de la béquille, afin d'éviter les dégradations des produits par casse des carrés (au-delà d'une certaine pression sur la béquille, celle-ci se débraye automatiquement pour éviter tout risque de casse).

Afin d'augmenter la sécurité, les produits seront également disponibles avec clavier intégré. Le mode de fonctionnement pourra être le suivant :

- Badge seul
- Code seul
- Badge + code
- Mode crise avec code sous contrainte

Il sera possible à tout moment depuis la gestion centralisée de donner un ordre d'ouverture à distance du produit.

Des plages horaires d'ouverture libre seront gérables directement depuis le logiciel de contrôle d'accès.

Celles-ci pourront, suivant le paramétrage, être conditionnées ou non par un premier badgeage autorisé.

À tout moment, le mode de fonctionnement pourra être paramétré depuis la supervision pour permettre :

- unbadgeage systématique (porte claquée, porte verrouillée)

- un double badgeage pour mise en passage libre
- un déclenchement de plage horaire
- ...

La béquille intégrera également une fonction dite « escape return » permettant de paramétrer un temps pendant lequel un utilisateur peut faire marche arrière (pour pallier par exemple à l'oubli de son badge dans le local concerné).

Sur certains accès, la béquille sera équipée d'un bouton intérieur sur la plaque pour déclencher le mode dit « Privacy ». Ce mode empêche l'accès depuis l'extérieur par une personne étrangère. L'accès reste cependant toujours possible, pour des raisons de sécurité, avec un badge dédié configuré dans le système de contrôle d'accès.

Dans l'objectif de limiter le nombre de systèmes d'exploitation et de simplifier la formation des utilisateurs, toutes les réponses ne permettant pas la gestion des droits d'accès et informations sur le poste central du fournisseur de contrôle d'accès ne pourront être prises en compte.

Pour des raisons de sécurité, tous les systèmes impliquant le stockage d'informations dans le badge de l'utilisateur seront refusés.

Poignées électroniques sur rosaces temps réel

Ils pourront s'adapter sur les portes pleines par fixation directe au travers des percements rosaces traversant.

Les produits seront livrés avec des carrés de 7 et 8mm, afin de s'adapter aux profils français et européen.

Le design sera un point important et sera approuvé par le maître d'ouvrage. Afin d'homogénéiser l'esthétisme sur l'ensemble du bâtiment, une gamme de béquillage mécanique au design assorti devra être proposée par le fournisseur.

Le produit pourra s'adapter sans modification sur des portes de différentes épaisseurs. Le fournisseur sera à même de proposer des rosaces pour le cylindre de secours en profil européen ou aveugle.

Le lecteur de badges sera intégré directement dans la béquille et nécessitera une pile LITHIUM CR123 standard du marché.

La tête de lecture devra impérativement permettre un embrayage de la béquille en moins de 0.5 seconde sur badge autorisé.

Afin d'assurer une maintenance efficace sur les portes équipées de lecteurs de contrôle d'accès sans fil, les événements suivants devront être remontés en temps réel sur les synoptiques graphiques du contrôle d'accès ou au fil de l'eau sans aucune manipulation de l'utilisateur sur le superviseur :

- niveau batterie basse,
- perte de la liaison sans fil entre le hub et le lecteur,
- lecteur absent (ou endommagé),
- problème de communication entre le contrôleur de porte et le hub de communication,

La traçabilité des badgeages se fera impérativement en temps réel dans le fil de l'eau de la supervision sans action manuelle sur le logiciel.

En cas de piles trop faibles pour faire fonctionner l'équipement, une connexion sera disponible en façade du lecteur pour brancher un élément de secours standard de type micro USB (les solutions propriétaires seront proscrites).

Le produit aura une faible consommation, afin de garantir une durée de vie minimum des piles de 4 ans (30 ouvertures par jour).

Il sera possible à tout moment depuis la gestion centralisée de donner un ordre d'ouverture à distance du produit.

Des plages horaires d'ouverture libre seront gérables directement depuis le logiciel de contrôle d'accès.

Celles-ci pourront, suivant le paramétrage, être conditionnées ou non par un premier badgeage autorisé.

À tout moment, le mode de fonctionnement pourra être paramétré depuis la supervision pour permettre :

- unbadgeage systématique (porte claquée, porte verrouillée)
- un double badgeage pour mise en passage libre
- un déclenchement de plage horaire.

Les portes extérieures devront être équipées de bandeaux de ventouses conformes avec la hauteur de la porte à savoir minimum 2500mm. Le Ral de couleur des bandeaux devra être au choix du client.

Les portes intérieures devront être équipées, si les PV coupe-feu le permettent, de bandeaux de ventouses 400 à 600mm centrés au milieu de la porte.

Cas échéant, la validation devra être effectuée par la direction du patrimoine de l'université dans un souci de maîtrise des coûts de maintenance.

Pour la conformité avec les normes appliquées à la réception de public aux universités, les portes seront associées avec bouton-poussoir de sortie et bris de glace vert.

L'asservissement de chaque issue de secours à la détection incendie sera **obligatoire**.

En effet l'université mettra à disposition la liste des entreprises SSI habilitées sur le(s) site(s) concerné(s), l'entreprise devra ordonner et suivre ces travaux d'asservissements, afin que la conformité incendie du —

bâtiment soit décernée.

Toute alarme émise par un des équipements de la porte (serrure, ventouse, lecteur, BP, etc) devra déclencher l'enregistrement du flux vidéo par la caméra associée, à T-3secondes.

Chaque profil pourra être défini par une date de début et de fin de validité. Un porteur de badge pourra ainsi avoir plusieurs profils actifs en même temps. Un niveau de priorité permettra de définir les accès autorisés.