Spécifications de Paxton

Section deux
Lecteurs Paxton10

PARTIE 1 GÉNÉRALITÉS

1.1 RÉSUMÉ

A. La section comprend

1. Contrôle d'accès électronique et gestion vidéo

B. Sections connexes

1. 28 10 00 Contrôle d'accès électronique et détection des intrusions
2. 28 13 00 Contrôle d'accès

C. Produits

{Supprimez ceux qui ne sont pas requis pour ce projet}

{Choisissez d'utiliser le nom du produit Paxton ou un nom général pour chaque}

1. Un [lecteur de proximité] [Lecteur Paxton10], qui doit lire une variété d'identifiants de proximité, y compris Bluetooth, pour vérifier et valider les utilisateurs.
2. Un [lecteur de proximité anti-vandale] [Lecteur anti-vandale Paxton10], qui doit lire une variété d'identifiants de proximité, y compris Bluetooth, pour vérifier et valider les utilisateurs, contenus dans un boîtier anti-vandale.
3. Un [lecteur de proximité et clavier] [Lecteur Clavier Paxton10], qui doit lire une variété d'identifiants de proximité, en plus de fournir des identifiants code et PIN, pour vérifier et valider les utilisateurs.
4. Un [lecteur de bureau] [Lecteur de bureau Paxton10], qui doit fournir une méthode d'inscription des badges de proximité au système à associer aux utilisateurs.

D. Système

1. Les lecteurs constituent une partie fondamentale d'un système de contrôle d'accès (SCA), assurant le contrôle et la surveillance des points d'accès sur le site installé.
2. Le système doit être évolutif, ce qui permet d'ajouter des lecteurs [et d'autres matériels de contrôle d'accès] du même fabricant.
3. Les lecteurs doivent être plug-and-play.

{Supprimez l'une des instructions suivantes qui ne sont pas vraies pour ce projet}

4. Le système doit contenir plusieurs points d'accès.
5. Le système doit contenir plusieurs dispositifs contrôlables.
6. Le système doit contenir plusieurs dispositifs surveillés.
7. Le système doit contenir des alarmes intrusion et incendie.
8. Le système doit contenir des caméras de vidéosurveillance.

1.2 EXIGENCES DU PROJET

{Supprimer/Modifier ceux qui ne s'appliquent pas à ce projet}

A. Un lecteur doit être installé à côté de chaque point d'accès à l'intérieur du site pour contrôler et surveiller son passage.

B. Les lecteurs doivent être installés à côté de l'entrée et de la sortie d'une zone afin de fournir une fonctionnalité anti-passback.

C. Chaque utilisateur se verra délivrer un badge.

1. Le système installé doit prendre en charge au moins 50 000 identifiants de badges uniques.

D. Un lecteur doit être installé pour armer et désarmer une alarme intrusion.

E. Les lecteurs doivent avoir un seul câble qui fournit à la fois l'alimentation et la communication.

F. Les lecteurs combinés au système doivent satisfaire aux exigences du projet en matière de contrôle d'accès.

G. {Supprimer si nécessaire} Les lecteurs doivent être installés sur un site doté d'un système [Paxton10 existant.

H. {Supprimer si nécessaire} Les lecteurs doivent être installés avec du matériel et des logiciels [Paxton10] supplémentaires pour former une solution complète de contrôle d'accès.

I. Capacité générale de lecture

1. Les lecteurs doivent fournir une méthode d'identification des utilisateurs.
2. Chaque lecteur doit être en mesure de communiquer les données d'identification à son matériel de contrôle.
3. Le système doit prendre en charge au moins 4 lecteurs pour chaque point d'accès contrôlé.
4. Les lecteurs doivent fournir un retour pour l'accès accordé et l'accès refusé au détenteur du badge.

J. Composants des lecteurs :

1. Le lecteur, qui doit fournir au système les informations d'identification de l'utilisateur.
2. Le contrôleur, qui fournit la base de données d'utilisateurs et le traitement pour refuser ou autoriser l'accès.

K. Capacité générale du système

1. Le système surveille et contrôle l'accès aux installations au moyen de contrôleurs d'accès électroniques utilisant des lecteurs de cartes, des dispositifs digicodes et des smartphones. Il doit être mis en œuvre au moyen d'une architecture TCP/IP utilisant l'approche du contrôleur électronique pour une porte via l'infrastructure PoE.
2. Le système doit être capable de surveiller les points d'alarme, de contrôler les dispositifs de sortie et de gérer le contrôle d'étages des ascenseurs. Le système doit maintenir une piste d'audit de l'activité de l'opérateur et de toutes les activités de contrôle d'accès et d'alarme.
3. Le système doit pouvoir commencer par une seule porte et étendre d'une porte à la fois jusqu'à un maximum de 1000 portes.
4. Chaque contrôleur doit être en mesure de gérer le matériel nécessaire pour sécuriser une porte. Si l'entrée et la sortie sont requises, un seul contrôleur est requis.
5. Chaque contrôleur tient à jour une base de données d'informations complète permettant la prise de décisions hors-ligne et de façon distribuée, sans point unique de défaillance.
6. Les contrôleurs doivent utiliser la technologie IPv6, prenant en charge la détection et l'adressage automatiques et le plug-and-play.
7. Le système permet un nombre illimité de postes de travail pour la programmation et l'administration du système, y compris la gestion des bases de données, la production de rapports et la surveillance d'activité en temps réel.
8. Aucune clé de licence ni aucun frais ne sera exigé pour accéder au logiciel d'administration, et aucune installation ne sera requise sur le serveur ou sur un poste de travail.
9. Le système doit prendre en charge au moins 50 000 identifiants uniques.

L. Le système doit fournir au minimum les éléments suivants :

1. Contrôle d'accès
2. Surveillance de l'état de la porte (Porte forcée, porte laissée ouverte)

3. Vidéosurveillance
4. Gestion de vidéo
5. Rapports d'événements
6. Plans du site / Synoptiques graphiques
7. Déclencheurs et actions
8. Anti-passback
9. Intégration des alarmes intrusion
10. Surveillance de l'alarme incendie
11. Rapports d'appel et de rassemblement
12. Accès à distance
13. Application smartphone pour le contrôle du système
14. Application smartphone pour l'administration des utilisateurs
15. Lecteur d'inscription des identifiants
16. Différentes technologies de lecteur de proximité, y compris Bluetooth
17. Logiciels sans licence et mises à jour à vie sans frais
18. Interphone / Station d'entrée vidéo
19. Serrures sans fil

1.3 DÉFINITIONS

A. ABS : Acrylonitrile butadiène styrène — un polymère thermoplastique.
B. Anti-passback : Terme permettant d'empêcher le partage ou le « passage en arrière » d'un badge dans le but de permettre aux personnes non-autorisées d'accéder à un site.
C. AWG (American Wire Gauge) : Unité de mesure du diamètre des fils.
D. Navigateur : Programme informatique utilisé pour visualiser et interagir de manière graphique avec les données à un emplacement sur le réseau connecté.
E. Client : PC capable d'afficher et de gérer la base de données système.
F. COM (Commun) : Contact sur un relais de connecteur E/S.
G. Contrôleur : Unité de commande périphérique intelligente qui fournit l'interface entre le sous système de gestion et de surveillance et les dispositifs installés, dans le but de restreindre l'accès, de contrôler et de surveiller l'activité de l'utilisateur et des appareils.
H. DDR3 (Double Data Rate type 3) : Type de RAM avec une interface à bande passante élevée.
I. Dispositif : Caméra vidéo, lumière, alarme, point d'accès ou tout autre élément avec lequel on peut interagir, soit en contrôlant son action ou son résultat, soit en surveillant sa sortie ou son état.
J. Stockage Edge : L'enregistrement de séquences vidéo directement sur la caméra.
K. EMC : Compatibilité électromagnétique.
L. Système Entry (système de vidéophonie audio/vidéo) : Système, autonome ou intégré, composé de platines et de moniteurs permettant l'accès par voie de communication vidéo et audio.
M. FCC : Commission fédérale des communications.
N. E/S : Entrée / Sortie, relative aux périphériques où une entrée est utilisée pour surveiller l'état haut/bas d'un signal, et une sortie est constituée d'un relais capable de mettre un dispositif en marche / arrêt.
O. IC : Industrie Canada.

P. IP : Protocole Internet intégré à Microsoft Windows.
Q. LAN : Réseau local.
R. Mbps : Mégabits par seconde
S. Moniteur : Matériel permettant à un occupant de valider l'entrée d'un utilisateur via une confirmation audio ou vidéo.
T. N.C. (Normalement fermé) : Contact sur un relais de connecteur E/S.
U. N.O. (Normalement ouvert) : Contact sur un relais de connecteur E/S.
V. Occupant ou résident : L'utilisateur d'un moniteur d'un lecteur.
W. Air libre : Sans obstruction ni interférence.
X. Platine : Matériel utilisé pour déterminer si un utilisateur connu est autorisé à accéder au bâtiment, et utilisé comme méthode de communication permettant aux utilisateurs inconnus de communiquer avec les occupants d'un bâtiment.
Y. PC : Ordinateur personnel, utilisé comme poste de travail, pour accéder au logiciel du système.
Z. PoE : Alimentation par Ethernet.
AA. RAM (Random Access Memory) : Type de stockage utilisé pour le logiciel pour stocker les données temporaires, requis pour le bon fonctionnement et l'utilisation du logiciel.
BB. Lecteur : Lecteur de proximité, digicode ou lecteur biométrique qui capture les identifiants utilisés pour identifier un utilisateur.
CC. RoHS : Restriction des substances dangereuses.
DD. Appel : liste de contrôle de présence des utilisateurs connus pour avoir été dans une zone spécifiée.
EE. RS-485 : Norme TIA/EIA pour les communications multipoints.
FF. CNR-210 : Norme CI pour les appareils radio exemptés de licence.
GG. CNR-GEN : Norme CI pour les exigences générales et renseignements relatifs à la certification des appareils radio.
HH. Serveur : PC qui contient la base de données des utilisateurs et la configuration du système, qui exécute le logiciel système.
II. SIP : Protocole d'initiation de session.
JJ. Disque SSD (Solid State Drive) : périphérique de stockage qui utilise une mémoire flash et n'a pas de pièces mobiles.
KK. Système : Matériel et logiciel à installer, combinés à tout matériel et logiciel existant, pour répondre aux exigences du projet.
LL. TCP : Protocole de contrôle du transport intégré à Microsoft Windows.
MM. Badge : L'identifiant délivré à une personne. Il peut s'agir d'un code PIN, ou d'un périphérique contenant un numéro encodé, utilisé pour déterminer si l'accès sera accordé ou refusé.
NN. Déclencheurs et actions : Composant logiciel qui permet de créer des règles pour exécuter des fonctionnalités personnalisées.
OO. UDP : Protocole de datagramme utilisateur intégré à Microsoft Windows.
PP. UL : Laboratoires des assureurs.
QQ. Monocast : Communication où l'information est adressée à un seul destinataire.
RR. UPS : Alimentation sans interruption.

SS. USB : Universal Serial Bus. Port de communication trouvé sur la plupart des ordinateurs.

TT. Résistant au vandalisme / anti-vandale (VR) : Propriété d'un article qui identifie l'article comme étant durable et résistant aux attaques.

UU. Visiteur : Utilisateur non autorisé / inconnu. Ou l'utilisateur d'un panneau.

VV. WAN : réseau étendu.

WW. Wiegand : principe magnétique breveté qui utilise des fils spécialement traités intégrés dans la carte d'identification. Également connu sous le nom de format de sortie de données de lecteur et signal Wiegand.

XX. Windows : Système d'exploitation de Microsoft Corporation.

YY. Station de travail : PC utilisé pour accéder au logiciel système.

ZZ. Site : l'emplacement ou les emplacements dans lesquels le système est installé.

1.4 DESCRIPTION DU SYSTÈME

A. Généralités

1. Le système surveille et restreint les déplacements des utilisateurs via les points d'accès.
2. Le système doit enregistrer et gérer les enregistrements des caméras vidéo IP situées sur le site
3. Les utilisateurs seront identifiés et traités par l'un de ces moyens :
    a. Présentation d'un badge à un lecteur
    b. Présentation d'un smartphone ou d'une tablette à un lecteur
    c. Saisie d'un code PIN unique sur un clavier
    d. Confirmation visuelle et / ou sonore d'un occupant des lieux
    e. Combinaison du susmentionné
4. Le système ne doit pas exiger de codes d'installation pour les identifiants cartes. Chaque badge/identifiant doit avoir un cryptage unique pour une sécurité élevée.
5. Le système doit prévoir des numéros de série de cartes uniques, de sorte que l'utilisateur n'aura pas besoin de déterminer la prochaine séquence de cartes à acheter.
6. Un PC doit être utilisé pour administrer le système de contrôle d'accès.
    a. Un mot de passe est requis pour se connecter et limite les activités qu'un exploitant est autorisé à exercer.
7. Des applications mobiles doivent être disponibles pour le contrôle du système et l'administration des utilisateurs.
    a. Les applications mobiles seront disponibles pour les appareils Android et iOS.

B. Matériel

1. Le matériel doit être composé de :
    a. Un serveur
    b. Contrôleurs de porte
    c. Contrôleurs vidéo
    d. Caméras vidéo
    e. Panneaux périphériques d'alarme
    f. Cartes d'interface sans fil {Requis pour PaxLock}
    g. Lecteurs de proximité
    h. Lecteurs digicodes

i. Lecteurs de bureau

j. Unités d'alimentation

2. Tout le matériel doit être plug-and-play.

3. Tous les périphériques matériels doivent être clairement étiquetés et identifiés pour faciliter l'installation.

4. L'équipement utilisé doit être fourni la mise à jour du firmware gratuitement par le fabricant.

C. Logiciel

1. La base de données système contenant toutes les informations relatives au matériel et aux utilisateurs doit être conservée sur le serveur.

2. Le serveur héberge le logiciel du système et fournit un lien Web permettant d'accéder au système et de le configurer.

a. Le logiciel doit être accessible à un nombre illimité de postes de travail sans installation.

b. Le logiciel doit être accessible à l'aide de la dernière version des navigateurs suivants :

(i) Google Chrome

(ii) Safari Apple

3. L'accès au logiciel est restreint à l'aide d'une connexion opérateur protégée par mot de passe.

4. L'accès au logiciel est autorisé en fonction des besoins et du rôle de chaque administrateur.

5. Le logiciel doit comporter :

a. Une interface utilisateur graphique.

b. Info-bulles sur chaque commande pour l'information de l'utilisateur.

c. Prise en charge des appareils mobiles, tablettes et ordinateurs de bureau.

d. Multi-utilisateurs et multi-tâches pour permettre la réalisation simultanée d'activités indépendantes et de surveillance sur différents postes de travail.

6. La licence du système doit porter sur l'ensemble du système et doit inclure la capacité pour les ajouts futurs qui se situent dans les limites de taille du système indiquées dans la présente section. Il n'y aura pas de frais de licence ni de droits de renouvellement annuels.

D. Ensemble de caractéristiques

1. Le système et les logiciels associés doivent fournir au minimum les éléments suivants :

a. Contrôle d'accès

b. Enregistrement et gestion vidéo

c. Intégration d'une caméra IP tierce

d. Prise en charge des caméras PTZ

e. Mur vidéo

f. Exportation de vidéo

g. Exportation d'un instantané vidéo

h. Signets vidéo

i. Recherche intelligente

j. Recherche dans la vidéo

k. Contrôle de la vitesse de lecture vidéo

l. Intégration d'alarme intrusion

m. Intégration d'alarme incendie

n. Importation d'utilisateurs
o. Cartes graphiques
p. Tableaux de bord personnalisés
q. Favoris des utilisateurs
r. Affichage automatique de l'image utilisateur sur PC à l'utilisation de la carte
s. Appel et regroupement
t. Notifications d'appel par e-mail
u. Rapports d'appel sur smartphone
v. Déclencheurs et actions pour obtenir une fonctionnalité personnalisée ou unique
w. Anti-passback
x. Permissions Multi-sociétés
y. Prise en charge de plusieurs technologies de lecture, y compris Bluetooth
z. Gestion des sites distants
aa. Application mobile Android et iOS pour la gestion de site
bb. Application mobile Android et iOS pour l'identification de l'utilisateur (badge Bluetooth)
cc. Connexion logicielle sécurisée à l'aide de HTTPS
dd. Paramètres de gestion des données pour gérer la protection des données
ee. Logiciel disponible en plusieurs langues

2. Ces fonctionnalités doivent être fournies sans frais supplémentaires ni abonnement

1.5 EXIGENCES DE PERFORMANCE

A. Toute modification apportée à l'intérieur du logiciel est automatiquement communiquée à tout le matériel intelligent de contrôle d'accès, les modifications appropriées prenant effet immédiatement.

B. Traitement distribué :

1. Le système est un système de traitement entièrement distribué de sorte que les informations (y compris l'heure, la date, les codes valides, les niveaux d'accès et les données similaires) soient téléchargées auprès des contrôleurs de telle manière que chaque contrôleur prend des décisions de contrôle d'accès pour cet emplacement.

2. Si les communications vers le serveur sont perdues, tous les contrôleurs doivent automatiquement mettre en mémoire tampon les transactions d'événements jusqu'à ce que les communications soient restaurées, à ce moment là les événements mis en mémoire tampon seront téléchargés sur le serveur.

C. Capacités du système :

1. Le système doit prendre en charge au maximum :

a. 1000 points d'accès.
b. 1000 caméras vidéo.
c. 50 000 utilisateurs, chacun possédant un identifiant unique.
d. Niveaux d'accès illimités et règles.
e. Rapports illimités

1.6 ASSURANCE DE LA QUALITÉ

A. Les lecteurs utilisés doivent bénéficier gratuitement des mises à jour du firmware du fabricant.

B. Les lecteurs sont couverts par une garantie du fabricant pendant au moins 5 ans. Les aspects suivants sont couverts :

1. Électrique
2. Électronique
3. Composant
4. Mécanique

C. Le fournisseur du système doit offrir une garantie non proportionnelle de cinq ans pour couvrir les composants du lecteur et inclure toutes les mises à niveau logicielles.

1.7 DOCUMENTS CONNEXES

A. Le système doit interagir avec d'autres parties physiques de l'installation et toute construction neuve ou rénovée.

B. Lors de la détermination de l'emplacement de la quincaillerie, l'installateur doit respecter tous les codes et lois du bâtiment appropriés concernant la sécurité des personnes et la construction.

1.8 CONFORMITÉ

A. Le système doit être conforme avec :

1. Le Règlement Général sur la Protection des Données (RGDP) 2018
2. EN60839-11-1 Grade 1
3. EN60839-11-1 Grade 2

B. [Les lecteurs de proximité] [lecteurs Paxton10] doivent respecter les normes suivantes :

1. EN 301 489-1 pour EMC {EU}
2. EN 300 330 pour la radio {EU}
3. EN 60950-1 pour la sécurité {EU}
4. IEC/EN 60950-1 pour la sécurité {ROW}
5. FCC Partie 15C pour la radio {US}
6. UL294 pour la sécurité {US}
7. CNR-GEN, 210 pour la radio {Canada}
8. CS C22.2 NO 205-M1983 pour la sécurité {Canada}
9. IP67 pour la résistance à l'humidité

C. [Les lecteurs digicodes] [lecteurs clavier Paxton10] doivent être conformes aux normes suivantes :

1. EN 301 489-1 pour EMC {EU}
2. EN 300 330 pour la radio {EU}
3. EN 60950-1 pour la sécurité {EU}
4. IEC/EN 60950-1 pour la sécurité {ROW}
5. FCC Partie 15C pour la radio {US}
6. UL294 pour la sécurité {US}
7. CNR-GEN, 210 pour la radio {Canada}
8. CS C22.2 NO 205-M1983 pour la sécurité {Canada}
9. IP67 pour la résistance à l'humidité

10. IK10 pour la résistance aux chocs

D. [Les lecteurs anti-vandalisme] [lecteurs anti-vandale Paxton10] doivent être conformes aux normes suivantes :

1. EN 301 489-1 pour EMC {EU}
2. EN 300 330 pour la radio {EU}
3. EN 60950-1 pour la sécurité {EU}
4. IEC/EN 60950-1 pour la sécurité {ROW}
5. FCC Partie 15C pour la radio {US}
6. UL294 pour la sécurité {US}
7. CNR-GEN, 210 pour la radio {Canada}
8. CS C22.2 NO 205-M1983 pour la sécurité {Canada}
9. IP67 pour résistance à l'humidité
10. IK10 pour la résistance aux chocs

E. Les lecteurs de bureau doivent être conformes aux normes suivantes :

1. EN 301 489-1 pour EMC {EU}
2. EN 300 330 pour la radio {EU}
3. IEC/EN 60950-1 pour la sécurité {EU}
4. FCC Partie 15C pour la radio {US}
5. CNR-GEN, 210 pour la radio {Canada}
6. UL/CSA 62368-1 pour la sécurité {US/Canada}

1.9 EXIGENCES GÉNÉRALES DE FONCTIONNALITÉ

A. En utilisant un lecteur de proximité, il doit être possible de lire les identifiants d'un utilisateur.

1. Un titulaire d'un identifiant doit être en mesure de présenter son badge ou son appareil intelligent au lecteur pour obtenir un accès valide à un point d'accès.
    a. La présentation d'un identifiant non valide ne doit pas permettre l'accès.
2. Le titulaire d'un identifiant doit pouvoir présenter son badge au lecteur pour contrôler un dispositif.
    a. La présentation d'un identifiant non valide ne doit pas agir sur l'appareil.
3. Une rétroaction visuelle doit être fournie à l'utilisateur sur présentation d'un identifiant.
    a. Les retours doivent indiquer si l'identifiant est valide ou non valide pour l'action envisagée.
4. Une rétroaction audible doit être fournie à l'utilisateur sur présentation d'un identifiant.
    a. Les retours doivent indiquer si l'identifiant est valide ou non valide pour l'action envisagée.

B. À l'aide d'un lecteur de code, l'utilisateur doit pouvoir saisir un code PIN ou un code pour s'identifier.

1. Il doit être possible d'utiliser un code PIN ou un code conjointement avec un badge de proximité ou un dispositif intelligent afin d'améliorer davantage la sécurité.
2. Le système requiert un mode d'authentification de l'utilisateur approprié pour l'appareil ou le point d'accès à interagir. Le mode de fonctionnement change automatiquement à différents moments de la journée ou des jours de la semaine en fonction de sa configuration.

C. Tous les lecteurs utilisés sur le périmètre externe du site doivent être classés IK10 pour la sécurité.

D. Il doit être possible de mettre en correspondance les lecteurs pour répondre aux exigences du

projet :

E. Les lecteurs doivent être connectés au contrôleur :

1. Les lecteurs doivent communiquer avec le contrôleur.
2. Les lecteurs doivent être alimentés par le contrôleur.

F. Le système doit enregistrer les entrées et les événements de l'appareil.

1. Un événement doit être généré pour l'activité d'entrée de porte suivante :
    a. Après la lecture d'un identifiant valide, lorsque la porte est déverrouillée.
    b. Après la lecture d'un identifiant non valide, lorsque la porte n'est pas déverrouillée.
    c. Lorsque la porte est forcée.
    d. Lorsque la porte est laissée ouverte.
    e. Lorsque plusieurs chiffres incorrects sont saisis sur un lecteur digicode, ce qui entraîne une alarme de piratage.
2. Un événement doit être généré pour l'activité d'alarme d'intrus suivante :
    a. Après la lecture d'un identifiant valide, lorsque l'alarme est armée.
    b. Après la lecture d'un identifiant valide, lorsque l'alarme est désarmée.
    c. Après la lecture d'un identifiant non valide.
3. Un événement doit être généré pour l'activité de l'appareil suivante :
    a. Après la lecture d'un identifiant valide, lorsque l'appareil est allumé ou désactivé.
    b. Après la lecture d'un identifiant non valide.
4. Tous les événements doivent être estampillés de l'heure et de la date.
5. Tous les événements doivent contenir la porte ou le dispositif auquel ils se rapportent.
6. Tous les événements doivent être communiqués au serveur en temps réel

G. Le système doit être polyvalent :

1. Le système reste opérationnel tant que le serveur est hors ligne.
2. Chaque contrôleur et ses lecteurs restent opérationnels tant que le réseau ou les autres contrôleurs ne sont pas disponibles.
3. Chaque contrôleur doit être équipé d'une batterie de secours afin de maintenir le fonctionnement de celui-ci et de ses lecteurs en cas de panne de courant. {Retirez si aucune batterie n'est installée}
    a. La batterie doit être surveillée par le système et fournir l'état actuel de la batterie et la charge dans l'interface utilisateur.

1.10 EXIGENCES GÉNÉRALES RELATIVES AUX COMMUNICATIONS

A. Contrôleur vers lecteur

1. Les lecteurs doivent communiquer avec un contrôleur au moyen du câble suivant, ou équivalent technique, :
    a. 22AWG, paire torsadée 4 noyaux
    i) La longueur maximale du câble doit être de 100 m (328 pi)
2. Tous les lecteurs doivent être munis d'un câble à paires torsadées 4 noyaux de 5 m (16,4 pi) de 22AWG sans frais supplémentaires.
3. Tous les lecteurs doivent communiquer à l'aide d'un protocole RS485.

4. Chaque contrôleur doit prendre en charge au moins deux lecteurs filaires.
5. Les lecteurs doivent être automatiquement détectés par le contrôleur.
6. Aucun adressage manuel n'est requis.

B. Ordinateur vers lecteur de bureau

1. Les lecteurs de bureau doivent communiquer avec un PC client via le câble suivant :
   a. Mini USB vers USB
2. Le lecteur de bureau doit entrer des données dans le logiciel Paxton10 via un PC client.
3. Le lecteur de bureau doit être plug-and-play, utilisant la sortie clavier.

C. Le système utilise des protocoles de mise en réseau normalisés pour permettre l'installation sur l'infrastructure de l'entreprise.

PARTIE 2 PRODUITS

2.1 FABRICANTS

A. Fabricant acceptable : Paxton {Supprimer si nécessaire}

1. Adresse e-mail : {Supprimer les options qui ne sont pas obligatoires}
   a. {UK} [support@paxton.co.uk]
   b. {FR} [support@paxtonaccess.fr]
   c. {US} [supportUS@paxton-access.com]
   d. {DE} [verkauf@paxton-gmbh.de]
   e. {NL} [support@paxton-benelux.com]
2. Numéro de téléphone :
   a. {UK} [01273 811011]
   b. {FR} [01 57 32 93 56]
   c. {US} [877.438.7298]
   d. {DE} [0251 2080 6900]
   e. {NL} [076 3333 999]
3. Skype :
   a. {UK} [Paxton.support]
   b. {FR} [Paxton.benelux.support]
   c. {US} [USAaxton.support]
   d. {DE} [Paxton.gmbh.support]

B. Substitutions : Non autorisées. {Supprimer si nécessaire}

C. Les composants du système doivent être disponibles auprès d'un fabricant unique afin d'assurer la compatibilité des produits.

D. Le fabricant du lecteur doit également fournir un système de contrôle d'accès.

E. Le fabricant du lecteur doit également fournir un système d'entrée de porte.

F. Limites de substitution

1. Il doit être possible d'installer un lecteur dans un système [Paxton10] existant.
2. Il doit être possible d'installer un lecteur en remplacement fonctionnel d'un lecteur existant.

2.2 EXIGENCES SPÉCIFIQUES POUR LES BADGES

A. Le fabricant du lecteur doit être en mesure de fournir des badges Paxton HiTag2 125kHz.

1. Les badges fournis doivent contenir une méthode d'authentification pour dissuader la copie et l'utilisation non autorisée de badges.

2.3 CONDITIONS PARTICULIÈRES POUR LE LECTEUR [PAXTON10] {Supprimer au besoin}

A. Caractéristiques

1. L'article doit comporter une technologie de lecture multiformat, fournissant simultanément la prise en charge de plusieurs formats d'identifiants.

2. L'article doit contenir une prise en charge Bluetooth à faible consommation d'énergie (BLE) pour permettre la communication avec les appareils mobiles et portables.

3. L'article doit permettre une installation rapide et facile.

4. L'article doit être économe en énergie, en utilisant un mode veille à faible puissance avec réveil capacitif.

5. L'article doit être classé IP pour une utilisation externe.

B. Identification des identifiants

1. L'article doit contenir un lecteur de proximité.

a. Au minimum, la technologie de badge suivante doit être prise en charge :

i) Paxton Hitag2 125 kHz

ii) EM4100/02

iii) EM4200

(iv) Sony FeliCa Lite-S

(v) MIFARE 1K

(vi) MIFARE 4K

vii) MIFARE Ultralight/C

viii) MIFARE DESFire/EV1

(ix) MIFARE Mini

(x) HID 125kHz

(xi) Bluetooth Smart

b. Toutes les technologies de badges ci-dessus doivent être prises en charge simultanément.

c. Les formats d'identifiants suivants doivent être pris en charge :

(i) Carte ISO

(ii) Clamshell

(iii) Minifob/porte-clés

(iv) Proxidisc

(v) Watchprox

(vi) Badge mains libres

(vii) Smartphone

(viii) Appareil intelligent Bluetooth

(ix) Appareil portable Bluetooth

d. La portée de lecture du badge, à température intérieure, pour chaque type de badge doit être au minimum :

(i) Hitag2

1. Carte ISO — 2,2” (57mm)
2. Clamshell — 2,2” (57mm)
3. Minifob — 1,1” (29mm)
4. Proxdisc — 1,7” (43mm)
5. Watchprox — 0,5” (12mm)

(ii) EM

1. Minifob EM — 1” (26mm)
2. Proxdisc EM — 1,3” (32 mm)
3. Carte ISO EM4100 — 1,7” (43mm)
4. Carte ISO EM4200 — 1,2” (30 mm)

(iii) MIFARE

1. Magnadata 1443 1k — 1,5” (39mm)
2. Magnadata 1443 4k — 1,6” (40 mm)
3. NXP Classic 1K — 1,8” (45 mm)
4. NXP Classic 4K — 1,5” (38 mm)
5. Magnadata DESFire — 1,1” (29 mm)
6. NXP PLUS S — 1,2” (30 mm)
7. NXP Ultralight — 1,7” (44 mm)
8. R5 — 1” (26mm)
9. Felica — 1,4” (36mm)

(iv) HID

1. 36 bits — 1,3” (34mm)
2. 34 bits — 1,1” (29mm)
3. 26 bits — 1,3” (32mm)

e. La portée de lecture Bluetooth doit être configurable dans le logiciel du système.

(i) Les modes Bluetooth suivants doivent être disponibles :

1. Bluetooth désactivé
2. Mode à courte portée/badge
3. Toucher pour entrer / portée de poche
4. Longue portée

C. Alimentation électrique

1. L’article doit fonctionner à partir de l’alimentation en courant continu fournie par le contrôleur.

a. Aucune source d’alimentation supplémentaire ne doit être requise.

2. La tension de fonctionnement ne doit pas dépasser 12 V CC.
3. La consommation électrique au ralenti ne doit pas dépasser 0,5 W.

a. Il doit être possible de désactiver les communications Bluetooth, ce qui peut réduire encore la consommation d’énergie.

D. Communication

1. Il doit être possible de placer le lecteur à une distance d’au moins 328 pi (100 m) du contrôleur sans que la communication ne devienne altérée.

2. L'élément doit instancier sa présence au contrôleur pour permettre une détection automatique.

a. L'article doit communiquer son numéro de série et son type de lecteur.

3. L'article doit communiquer son état fonctionnel à la demande du contrôleur.

4. L'élément doit communiquer des données de badges de divers formats et longueurs.

5. L'élément doit communiquer avec des badges en utilisant :

a. Fréquence radio de 125 kHz

b. Fréquence radio de 13,56 MHz

c. Fréquence radio de 2,4 GHz

E. Affichage

1. L'article doit être doté d'un affichage LED élégant.

a. Il ne doit comporter qu'une seule LED RVB.

2. La LED doit indiquer les états et événements suivants :

a. Lecture d'identifiant valide

b. Lecture d'identifiant non valide

(i) Autorisations non valides

(ii) Identifiant inconnu

(iii) Identifiant interdit

c. Armement d'alarme d'intrus

d. Alarme intrusion armée

e. Alarme intrusion désarmée

f. Porte déverrouillée

g. Sortie activée

3. La LED doit rester allumée par défaut pour permettre de localiser le lecteur dans des environnements non éclairés.

a. Il doit être possible de désactiver la LED en cas d'inactivité.

F. Audio

1. L'article doit contenir un buzzer Piezo pour un retour sonore

2. Une tonalité doit sonner pour indiquer les événements suivants :

a. Lecture d'identifiant valide — accès accordé

b. Lecture d'identifiant valide — accès refusé

(i) Autorisations non valides

(ii) Identifiant inconnu

(iii) Identifiant interdit

3. Il doit être possible de désactiver la rétroaction sonore pour assurer un fonctionnement silencieux.

G. Température

1. L'article doit satisfaire aux normes de température requises pour un produit externe

a. L'élément doit fonctionner de manière fiable dans la plage de température comprise entre -31 °F et +150,8 °F

(-35°C à +66°C).

H. Boîtier

1. L'article doit être élégant et moderne.
2. L'article doit être discret.
3. Il ne doit pas y avoir de fixations visibles sur l'article.
4. Le matériau du boîtier doit être composé de PC et d'ABS
5. L'article doit être disponible en noir
6. Les options de montage suivantes doivent être disponibles :
    a. Montage en surface

I. Dimensions

1. Les dimensions ne doivent pas dépasser :
    a. Une largeur de 1,9 po (49 mm)
    b. Une hauteur de 4,1 po (104 mm)
    c. Une profondeur de 0,6 po (17,2 mm)

2.4 CONDITIONS PARTICULIÈRES POUR LECTEUR DIGICODE [PAXTON10] {Supprimer au besoin}

A. Caractéristiques

1. L'article doit comporter une technologie de lecture multiformat, fournissant simultanément la prise en charge de plusieurs formats d'identifiants.
2. L'article doit contenir une prise en charge Bluetooth à faible consommation d'énergie (BLE) pour permettre la communication avec les appareils mobiles et portables.
3. L'article doit contenir un Code à 12 touches, permettant de prendre en charge les identifiants PIN et Code.
4. L'élément doit fournir une prise en charge de l'authentification à deux facteurs.
    a. Les modes de fonctionnement d'authentification suivants doivent être disponibles :
    (i) Badge uniquement
    (ii) PIN seulement
    (iii) Code seulement
    (iv) Badge + PIN
    (v) Badge + Code
    (vi) Badge ou code PIN
    (vii) Badge ou code
    (viii) Badge ou PIN ou code
    b. Il doit être possible d'avoir un mode de fonctionnement spécifié pour des horaires spécifiés.
5. Le système doit générer un événement d'alarme de piratage de clé après 20 appuis de touches sans PIN ou code valide.
6. L'article doit permettre une installation rapide et facile.
7. L'article doit être économe en énergie, en utilisant un mode veille à faible puissance avec réveil capacitif.
8. L'article doit être classé IP pour une utilisation externe.
9. L'article doit être classé IK pour la résistance au vandalisme.

B. Identification des identifiants

1. L'article doit contenir un lecteur de proximité.
    a. Au minimum, la technologie de badge suivante doit être prise en charge :

(i) Paxton Hitag2 125 kHz

(ii) EM4100/02

(iii) EM4200

(iv) Sony FeliCa Lite-S

(v) MIFARE 1K

(vi) MIFARE 4K

(vii) MIFARE Ultralight/C

(viii) MIFARE DESFire/EV1

(ix) MIFARE Mini

(x) HID 125kHz

(xi) Bluetooth Smart

b. Toutes les technologies de badges ci-dessus doivent être prises en charge simultanément.

c. Les formats d'identifiants suivants doivent être pris en charge :

(i) Carte ISO

(ii) Clamshell

(iii) Minifob/porte-clés

(iv) Proxidisc

(v) Watchprox

(vi) Badge mains libres

(vii) Smartphone

(viii) Appareil intelligent Bluetooth

(ix) Appareil portable Bluetooth

d. La portée de lecture du badge, à température intérieure, pour chaque type de badge doit être au minimum :

(i) Hitag2

1. Carte ISO — 2" (52 mm)
2. Clamshell — 2,2" (55 mm)
3. Minifob — 0,9" (24mm)
4. Proxdisc — 1,5" (37mm)
5. Watchprox — 0,4" (10 mm)

(ii) EM

1. Minifob EM — 0,9" (24mm)
2. Proxdisc EM — 1,2" (30 mm)
3. Carte ISO EM4100 — 1,5" (38mm)
4. Carte ISO EM4200 — 1" (26 mm)

iii) MIFARE

1. Magnadata 1443 1k — 1,6" (40mm)
2. Magnadata 1443 4k — 1,7" (42mm)
3. NXP Classic 1K — 1,7" (43mm)

4. NXP Classic 4K — 1,5” (37mm)
5. Magnadata DESFire — 1,1” (29mm)
6. NXP PLUS S — 1,1” (28mm)
7. NXP Ultralight — 1,8” (46mm)
8. R5 — 0,9 » (24mm)
9. Felica — 1,4” (36mm)

(iv) HID

1. 36 bits — 1,3” (34mm)
2. 34 bits — 1,1” (29mm)
3. 26 bits — 1,3” (32mm)

e. La portée de lecture Bluetooth doit être configurable dans le logiciel du système.

i) Les modes Bluetooth suivants doivent être disponibles :

1. Bluetooth désactivé
2. Mode à courte portée/badge
3. Toucher pour entrer /portée de poche
4. Longue portée

2. L’article doit contenir un clavier.

a. Les formats d’identifiants doivent être pris en charge :

(i) PIN

(ii) Code

b. Chaque utilisateur peut se voir attribuer un code PIN

(i) La longueur du code PIN du système doit être configurable pour répondre aux exigences de sécurité du projet.

(ii) Tous les code PIN du système doivent avoir la même longueur.

(iii) Le système doit prendre en charge une longueur du code PIN de 4 à 8 chiffres.

(iv) Il doit y avoir au moins 100 000 000 combinaisons de code PIN possibles.

(v) Un utilisateur peut définir son propre code PIN.

(vi) Les code PIN doivent être utilisés pour identifier l’utilisateur qui a obtenu l’accès.

c. Chaque dispositif peut se voir attribuer un code

(i) Le système doit prendre en charge des codes de longueur comprise entre 4 et 8 chiffres.

(ii) Le système doit prendre en charge des codes de longueurs différentes.

(iii) Chaque appareil peut se voir attribuer plusieurs codes.

(iv) Le même code peut être utilisé sur plusieurs dispositifs.

(v) Il doit y avoir au moins 111 110 000 combinaisons de codes possibles.

(vi) Les codes doivent être génériques et ne permettent pas d’identifier l’utilisateur. L’utilisateur ne doit être identifié que s’il utilise une méthode d’authentification badge + code.

C. Alimentation électrique

1. L’article doit fonctionner à partir de l’alimentation en courant continu fournie par le contrôleur.

a. Aucune source d’alimentation supplémentaire ne doit être requise.

2. La tension de fonctionnement ne doit pas dépasser 12 V CC.

3. La consommation électrique au ralenti ne doit pas dépasser 0,5 W.

a. Il doit être possible de désactiver les communications Bluetooth, ce qui peut réduire encore la consommation d'énergie.

D. Communication

1. Il doit être possible de placer le lecteur à une distance d'au moins 328 pi (100 m) du contrôleur sans que la communication ne devienne altérée.

2. L'article doit instancier sa présence au contrôleur pour permettre une détection automatique.

a. L'article doit communiquer son numéro de série et son type de lecteur.

3. L'article doit communiquer son état fonctionnel à la demande du contrôleur.

4. L'article doit communiquer des données de badges de divers formats et longueurs.

5. L'article doit communiquer avec des badges en utilisant :

a. Fréquence radio de 125 kHz

b. Fréquence radio de 13,56 MHz

c. Fréquence radio de 2,4 GHz

E. Affichage

1. L'article doit être doté d'un affichage LED élégant.

a. Il ne doit comporter qu'une seule LED RVB.

2. La LED doit indiquer les états et événements suivants :

a. Lecture d'identifiant valide

(i) Badge valide

(ii) code PIN valide

(iii) Code valide

b. Lecture d'identifiant non valide

(i) Autorisations non valides

(ii) Identifiant inconnu

(iii) Identifiant interdit

(iv) Alarme de piratage de clés

c. Authentification à deux facteurs

(i) Nécessite un code PIN pour remplir la demande

(ii) Exige un code pour remplir la demande

d. Armement d'alarme intrus

e. Alarme intrus armée

f. Alarme d'intrus désarmée

g. Porte déverrouillée

h. Sortie activée

3. La LED doit rester activée par défaut pour fournir un support pour localiser le lecteur dans des environnements non éclairés.

a. Il doit être possible de désactiver la LED en cas d'inactivité.

F. Audio

1. L'article doit contenir un buzzer Piezo pour un retour sonore
2. Une tonalité doit sonner pour indiquer les événements suivants :
    a. Lecture d'identifiant valide — accès accordé
    b. Lecture d'identifiant valide — accès refusé
    (i) Autorisations non valides
    (ii) Identifiant inconnu
    (iii) Identifiant interdit
4. Il doit être possible de désactiver la rétroaction sonore pour assurer un fonctionnement silencieux.

G. Température

1. L'article doit satisfaire aux normes de température requises pour un produit externe
    a. L'élément doit fonctionner de manière fiable dans la plage de température comprise entre -31 °F et +150,8 °F
    (-35°C à +66°C).

H. Boîtier

1. L'article doit être élégant et moderne.
2. L'article doit être discret.
3. Il ne doit pas y avoir de fixations visibles sur l'article.
4. Le matériau du boîtier doit être composé de PC et d'ABS
5. Le matériau du clavier doit être en silicone durci
6. L'article doit être disponible en noir
7. Les options de montage suivantes doivent être disponibles :
    a. Montage en surface
    b. Montage US Backbox (via un adaptateur backbox)

I. Dimensions

1. Les dimensions ne doivent pas dépasser :
    a. Une largeur de 2,5 po (63,8 mm)
    b. Une hauteur de 4,1 po (104 mm)
    c. Une profondeur de 0,7 po (18,2 mm)

2.5 CONDITIONS PARTICULIÈRES POUR LE LECTEUR [PAXTON10] RÉSISTANT AU VANDALISME {Supprimer au besoin}

A. Caractéristiques

1. L'article doit comporter une technologie de lecture multiformat, fournissant simultanément la prise en charge de plusieurs formats d'identifiants.
2. L'article doit contenir une prise en charge Bluetooth à faible consommation d'énergie (BLE) pour permettre la communication avec les appareils mobiles et portables.
3. L'article doit permettre une installation rapide et facile.
4. L'article doit être économe en énergie, en utilisant un mode veille à faible puissance avec réveil capacitif.
5. L'article doit être classé IP pour une utilisation externe.
6. L'article doit être classé IK pour une résistance au vandalisme.

B. Identification des identifiants

1. L'article doit contenir un lecteur de proximité.

a. Au minimum, la technologie de badge suivante doit être prise en charge :

i) Paxton Hitag2 125 kHz

ii) EM4100/02

iii) EM4200

(iv) Sony FeliCa Lite-S

(v) MIFARE 1K

(vi) MIFARE 4K

vii) MIFARE Ultralight/C

viii) MIFARE DESFire/EV1

(ix) MIFARE Mini

(x) HID 125kHz

(xi) Bluetooth Smart

b. Toutes les technologies de badges ci-dessus doivent être prises en charge simultanément.

c. Les formats d'identifiants suivants doivent être pris en charge :

(i) Carte ISO

(ii) Clamshell

(iii) Minifob/porte-clés

(iv) Proxidisc

(v) Watchprox

(vi) Badge mains libres

(vii) Smartphone

(viii) Appareil intelligent Bluetooth

(ix) Appareil portable Bluetooth

d. La portée de lecture du badge, à température intérieure, pour chaque type de badge doit être au minimum :

(i) Hitag2

1. Carte ISO — 2,2" (57mm)
2. Clamshell — 2,2" (57mm)
3. Minifob — 1,1" (29mm)
4. Proxdisc — 1,7" (43mm)
5. Watchprox — 0,5" (12mm)

(ii) EM

1. Minifob EM — 1" (26mm)
2. Proxdisc EM — 1,3" (32 mm)
3. Carte ISO EM4100 — 1,7" (43mm)
4. Carte ISO EM4200 — 1,2" (30 mm)

(iii) MIFARE

1. Magnadata 1443 1k — 1,5" (39mm)
2. Magnadata 1443 4k — 1,6" (40 mm)
3. NXP Classic 1K — 1,8" (45 mm)

4. NXP Classic 4K — 1,5” (38 mm)
5. Magnadata DESFire — 1,1” (29 mm)
6. NXP PLUS S — 1,2” (30 mm)
7. NXP Ultralight — 1,7” (44 mm)
8. R5 — 1” (26mm)
9. Felica — 1,4” (36mm)

(iv) HID

1. 36 bits — 1,3” (34mm)
2. 34 bits — 1,1” (29mm)
3. 26 bits — 1,3” (32mm)

e. La portée de lecture Bluetooth doit être configurable dans le logiciel du système.

(i) Les modes Bluetooth suivants doivent être disponibles :

1. Bluetooth désactivé
2. Mode à courte portée/badge
3. Toucher pour entrer /portée de poche
4. Longue portée

C. Alimentation électrique

1. L’article doit fonctionner à partir de l’alimentation en courant continu fournie par le contrôleur.
    a. Aucune source d’alimentation supplémentaire ne doit être requise.
2. La tension de fonctionnement ne doit pas dépasser 12 V CC.
3. La consommation électrique au ralenti ne doit pas dépasser 0,5 W.
    a. Il doit être possible de désactiver les communications Bluetooth, ce qui peut réduire encore la consommation d’énergie.

D. Communication

1. Il doit être possible de placer le lecteur à une distance d’au moins 328 pi (100 m) du contrôleur sans que la communication ne devienne altérée.
2. L’élément doit instancier sa présence au contrôleur pour permettre une détection automatique.
    a. L’article doit communiquer son numéro de série et son type de lecteur.
3. L’article doit communiquer son état fonctionnel à la demande du contrôleur.
4. L’élément doit communiquer des données de badges de divers formats et longueurs.
5. L’élément doit communiquer avec des badges en utilisant :
    a. Fréquence radio de 125 kHz
    b. Fréquence radio de 13,56 MHz
    c. Fréquence radio de 2,4 GHz

E. Affichage

1. L’article doit être doté d’un affichage LED élégant.
    a. Il ne doit comporter qu’une seule LED RVB.
2. La LED doit indiquer les états et événements suivants :
    a. Lecture d’identifiant valide
    b. Lecture d’identifiant non valide
    (i) Autorisations non valides

(ii) Identifiant inconnu

(iii) Identifiant interdit

c. Armement d'alarme d'intrus

d. Alarme intrus armée

e. Alarme d'intrus désarmée

f. Porte déverrouillée

g. Sortie activée

3. La LED doit rester allumée par défaut pour permettre de localiser le lecteur dans des environnements non éclairés.

a. Il doit être possible de désactiver la LED en cas d'inactivité.

F. Audio

1. L'article doit contenir un buzzer Piezo pour un retour sonore

2. Une tonalité doit sonner pour indiquer les événements suivants :

a. Lecture d'identifiant valide — accès accordé

b. Lecture d'identifiant valide — accès refusé

(i) Autorisations non valides

(ii) Identifiant inconnu

(iii) Identifiant interdit

3. Il doit être possible de désactiver la rétroaction sonore pour assurer un fonctionnement silencieux.

G. Température

1. L'article doit satisfaire aux normes de température requises pour un produit externe

a. L'article doit fonctionner de manière fiable dans la plage de température comprise entre -31 °F et +150,8 °F

(-35°C à +66°C).

H. Boîtier

1. L'article doit être discret..

2. Le matériau du boîtier doit être composé de PC, d'ABS et d'ASTM B86

3. Les options de montage suivantes doivent être disponibles :

a. Montage en surface

I. Dimensions

1. Les dimensions ne doivent pas dépasser :

a. Une largeur de 2,3 po (57,6 mm)

b. Une hauteur de 4,2 po (106 mm)

c. Une profondeur de 0,8 po (19,5 mm)

2.6 CONDITIONS SPÉCIFIQUES POUR LE LECTEUR DE BUREAU

A. Caractéristiques

1. Le lecteur de bureau doit faciliter l'attribution de badges aux utilisateurs.

2. Le lecteur de bureau doit lire plusieurs types et formats de badges de proximité.

3. Le lecteur de bureau doit identifier les badges/identifiants qui ont déjà été attribuées aux utilisateurs.

4. Le lecteur de bureau élimine le besoin de connaître le numéro de chaque badge.

5. Dans les systèmes comportant plusieurs PC clients, le système doit pouvoir prendre en charge plusieurs lecteurs de bureau.

6. Le lecteur de bureau doit générer un ID unique à partir de chaque badge présenté.

7. Le lecteur de bureau doit produire un ID unique à partir d'une variété de formats et de longueurs.

B. Interaction des utilisateurs

1. Le lecteur de bureau doit fonctionner en mode intuitif :

a. Lorsqu'un badge/identifiant non attribué est présenté, le logiciel système crée automatiquement l'enregistrement de l'utilisateur et l'écran utilisateur pour entrer les informations de l'utilisateur ainsi que d'autres paramètres de sécurité.

b. Lorsque l'opérateur est déjà dans une fiche d'utilisateur et qu'un badge/identifiant non attribué est présenté, le logiciel doit afficher l'option permettant d'ajouter le badge/identifiant à la fiche en question.

c. Lorsqu'un badge/identifiant existant est présenté au lecteur de bureau, le logiciel récupère et affiche automatiquement la fiche d'utilisateur associée à cet utilisateur. Si plusieurs badges/identifiants sont attribués à cet utilisateur, le logiciel doit mettre en évidence celui présenté.

2. Le lecteur doit être plug & play.

C. Lecteur de proximité

1. L'article doit contenir un lecteur de proximité.

a. Au minimum, la technologie de badge suivante doit être prise en charge :

(i) Paxton HiTag2 125KHz

(ii) HID 125KHz

(iii) EM4100/02

(iv) EM4200

(v) Sony FeliCa Lite-S

(vi) MIFARE 1K

(vii) MIFARE 4K

(viii) MIFARE Ultralight / C

(ix) MIFARE DESFire / EV1

(x) MIFARE Mini

b. Toutes les technologies de badges ci-dessus doivent être prises en charge simultanément.

c. Les formats d'identifiants suivants doivent être pris en charge :

(i) Carte ISO

(ii) Clamshell

(iii) Minifob / keyfob

(iv) Proxidisc

(v) Watchprox

(vi) Badge mains libres

D. Alimentation

1. L'article doit être alimenté par USB.

E. Communication

1. Le lecteur de bureau doit se connecter à un PC via un câble mini USB vers USB.

F. Affichage

1. L'article doit être doté d'un affichage LED élégant.
2. Les LED doivent indiquer les états suivants :
    a. Article alimenté ou prêt à l'emploi
    b. Lecture des identifiants

G. Température

1. L'article doit satisfaire aux normes de température requises pour un produit interne.
    a. L'article doit fonctionner de manière fiable dans la plage de température comprise entre 0 °C et +49 °C (32 °F à 120 °F)

H. Boîtier

1. L'article doit être élégant et moderne.
2. Le produit doit être disponible en noir

I. Dimensions

1. Les dimensions du lecteur de bureau ne doivent pas dépasser :
    a. Une largeur de 115 mm (4,5 po)
    b. Une hauteur de 19 mm (0,7 po)
    c. Une profondeur de 75 mm (3 po)

FIN DE LA SECTION

MIFARE®, MIFARE® Classic, DESFire®, MIFARE® Plus et MIFARE® Ultralight C sont des marques commerciales de NXP B.V.
Felica® est une marque déposée de Sony Corporation.
HID est une marque déposée de HID Global Corporation.
Intel® est une marque déposée d'Intel Corporation.
Microsoft et Windows sont des marques déposées de Microsoft Corporation.
Bluetooth est une marque déposée de Bluetooth SIG.