Spécifications de Paxton

Section trois
PaxLock Pro

PARTIE 1 GÉNÉRALITÉS

1.1 RÉSUMÉ

A. La section comprend

1. Contrôle d'accès électronique

B. Sections connexes

1. Contrôle d'accès
2. Interfaces de contrôle d'accès

C. Produits

1. Une serrure électronique sans fil ultramoderne pour améliorer la sécurité d'une installation.
2. Logiciel de contrôle d'accès pour la configuration, la maintenance et la surveillance de la serrure électronique {optionnel - Mode autonome disponible}.
3. Pont sans fil permettant la communication sans fil des événements et des paramètres de verrouillage entre le logiciel de contrôle d'accès et la serrure électronique {optionnel - Mode autonome disponible}.

D. Système

1. Les seuls produits requis sont la serrure électronique, qui doit permettre un contrôle d'accès autonome. Les ponts sans fil et le logiciel de contrôle d'accès peuvent être utilisés conjointement avec les serrures électroniques pour fournir des fonctionnalités supplémentaires en réseau.
    a. Des pont(s) sans fil et un logiciel de contrôle d'accès peuvent être ajoutés au système au point d'installation ou à tout moment.
    b. Des serrures électroniques peuvent être ajoutées à un système de contrôle d'accès existant à tout moment.
2. Le système doit prendre en charge un serveur qui stocke la base de données de contrôle d'accès contenant les informations sur l'utilisateur et le matériel ainsi que les paramètres de configuration.
3. Les produits ci-dessus doivent fournir une solution de contrôle d'accès qui répond à toutes les exigences spécifiées dans le présent document.
4. Lorsqu'il est utilisé conjointement avec un système de contrôle d'accès (ACS), le système doit permettre à la serrure électronique d'utiliser toutes ses caractéristiques et de fournir les caractéristiques supplémentaires énumérées dans la présente spécification.
5. L'ACS doit être évolutif, ce qui permet d'ajouter des serrures électroniques et d'autres matériels de contrôle d'accès provenant du même fabricant sans qu'il soit nécessaire de modifier ou d'affecter la fonctionnalité des serrures électroniques existantes.

1.2 EXIGENCES DU PROJET

A. Des serrures électroniques doivent être installées sur les portes à l'intérieur du site pour assurer le contrôle des accès.

B. Les serrures électroniques doivent satisfaire aux exigences du projet en matière de contrôle des accès.

C. Les serrures électroniques doivent pouvoir être installées sur un site doté d'un système de contrôle des accès existant.

D. Les serrures électroniques doivent pouvoir être installées avec du matériel et des logiciels de contrôle des accès supplémentaires pour former une solution complète de contrôle des accès.

E. Capacité globale de verrouillage électronique

1. La serrure électronique doit fournir une solution sans fil pour le contrôle des accès.

2. La serrure électronique doit pouvoir commander un seul point d'entrée et augmenter d'une porte à la fois, jusqu'à un minimum de 1000.

3. Chaque serrure électronique doit pouvoir gérer le matériel nécessaire pour sécuriser une porte.

4. Chaque serrure électronique doit fournir un contrôle d'accès dans une seule direction et permettre un accès libre dans l'autre sens.

F. L'équipement de contrôle d'accès fourni par le fabricant doit être « plug-and-play », permettant une installation rapide et simple.

G. Composants de la serrure électronique

1. Matériel, qui doit être constitué d'une serrure électronique sans fil alimenté par batterie, qui doit assurer le contrôle et la surveillance d'un point d'accès.

2. Communication, qui consiste en un routeur sans fil fourni par le fabricant de l'ACS, permettant à la serrure électronique de communiquer avec le logiciel de contrôle des accès. {Non requis pour la solution autonome}

H. La serrure électronique doit comporter au minimum les éléments suivants :

1. Contrôle des accès.

I. Lors de la communication avec un système de contrôle des accès, outre ce qui précède, la serrure électronique doit prévoir :

1. Rapports d'événements au logiciel de contrôle des accès.

2. Communication sans fil avec le logiciel de contrôle des accès.

3. Logiciel de configuration et de surveillance sans licence et mises à jour à vie sans frais.

4. Configuration du point d'accès et autorisation utilisateur.

1.3 DÉFINITIONS

A. Unité de contrôle des accès (ACU) : Unité de commande périphérique intelligente qui fournit l'interface entre le sous-système de gestion et de surveillance et les dispositifs installés sur le portail d'accès dans le but de restreindre l'accès et de surveiller l'état du portail.

B. 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 les accès, de contrôler et de surveiller l'activité de l'utilisateur et de l'appareil.

C. IP : Protocole Internet intégré à Microsoft Windows.

D. LAN : Réseau local.

E. Air libre : Sans obstruction ni interférence.

F. PC : Ordinateur personnel, utilisé comme station centrale, postes de travail et serveurs de fichiers.

G. PoE : Alimentation par Ethernet.

H. Lecteur : Lecteur de proximité, clavier ou lecteur biométrique qui capture les identifiants utilisées pour identifier un utilisateur.

I. Serveur : PC qui contient la base de données des utilisateurs et la configuration du système, qui exécute le logiciel système.

J. Site : Emplacement(s) où le système est installé.

K. Autonome : Possibilité de fonctionner sans communication entre eux ou avec un serveur central. Un élément autonome peut fonctionner seul, sans avoir besoin de matériel ou de logiciel supplémentaire.

L. TCP : Protocole de contrôle du transport intégré à Microsoft Windows.

M. Badge : L'identifiant délivré à une personne. Il peut s'agir d'un code PIN, ou d'un périphérique contenant un numéro codé, utilisé pour déterminer si l'accès sera accordé ou refusé.

N. USB : bus série universel.

O. WAN : réseau étendu.

P. Windows : Système d'exploitation par Microsoft Corporation.

Q. Poste de travail : PC utilisé pour accéder au logiciel système.

1.4 DESCRIPTION DU CONTRÔLE DES ACCÈS

A. Généralités

1. Les utilisateurs sont identifiés et traités par les moyens suivants :

a. Présentation d'un badge à un lecteur.

2. Le système ne doit pas utiliser de codes d'installation pour les informations d'identification des cartes. Chaque badge/identifiant doit avoir un chiffrement unique de 40 bits pour une sécurité élevée.

3. Lorsqu'il est administré à l'aide du logiciel de contrôle des accès, 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.

4. Les serrures électroniques doivent fonctionner sans communication entre elles ou avec un serveur central.

B. Logiciels de contrôle des accès

1. Lorsqu'il est utilisé conjointement avec un système de contrôle des accès et un pont sans fil, un logiciel de contrôle des accès doit être fourni par le fabricant sans frais supplémentaires.

2. La serrure électronique doit être configurable à l'aide du logiciel de contrôle des accès.

3. Le logiciel doit comporter :

a. Une interface utilisateur graphique et facile à utiliser

b. Accès à distance

c. Une application mobile, qui doit fournir au minimum les caractéristiques suivantes :

(i) Administration des utilisateurs

(ii) Rapports d'événements

(iii) Commande de porte

(iv) Appel

d. L'application mobile doit être disponible pour les appareils Android et iOS.

4. La licence de 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.

5. L'accès est restreint à l'aide d'un identifiant de l'opérateur protégé par mot de passe.

6. Nombre de PC requis

a. Il ne doit pas y avoir de limite au nombre de clients qui peuvent accéder au logiciel de configuration.

b. Il ne doit pas y avoir de limite au nombre d'appareils mobiles pouvant installer et exécuter l'application mobile Android et iOS.

1.5 EXIGENCES DE PERFORMANCE

A. L'équipement utilisé doit être couvert par une garantie du fabricant pendant au moins 5 ans. Les aspects suivants sont couverts :

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

B. Lorsqu'il est utilisé avec un pont sans fil et un logiciel de contrôle des accès :

1. L'équipement utilisé doit être fourni gratuitement à la mise à jour du firmware par le fabricant.
2. Toute modification apportée au logiciel de contrôle des accès sera automatiquement envoyée à la serrure électronique lors de sa prochaine mise en ligne.
3. La serrure électronique stocke au moins 16 000 événements lorsqu'il ne peut pas communiquer avec le serveur de contrôle des accès. Lorsque la communication est rétablie, tous les événements en suspens seront signalés au logiciel de contrôle des accès.
4. Les capacités du système de contrôle des accès doivent comporter au minimum :
    a. 1000 points d'accès
    b. 50 000 utilisateurs/badges

C. Lorsqu'il est utilisé sans pont sans fil ou logiciel (autonome) :

1. Les capacités du système de contrôle des accès doivent être au minimum :
    a. 1000 points d'accès
    b. 10 000 utilisateurs/badges

1.6 ASSURANCE DE LA QUALITÉ

A. Le fournisseur ACS offrira une garantie non proportionnelle de 5 ans pour couvrir les composants de serrure électronique 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. Toutes les serrures électroniques doivent être conformes aux normes suivantes :

1. EN 301-489 pour la compatibilité électromagnétique
2. ETSI EN 300 330 pour la transmission sans fil
3. ETSI EN 300 328 pour la transmission sans fil
4. IEC/EN 60950-1 pour la sécurité
5. BS EN1634 FD30 pour résistance au feu (portes coupe-feu de 30 minutes)
6. BS EN1634 FD60 pour résistance au feu (portes coupe-feu de 60 minutes)
7. BS EN179 pour évacuation d'urgence {Utilisé avec le kit d'accessoires EN179}
8. Directive sur la restriction des substances dangereuses (RoHS)

9. Directive basse tension (LVD)
10. Directive sur les équipements radioélectriques (RED)
11. Partie 15 des Règles de la FAC
12. IK10 pour la résistance aux chocs
13. UL10C pour résistance au feu {US}
14. UL294 pour la sécurité {US}

B. Les variantes externes de toutes les serrures électroniques, en plus de ce qui précède, doivent également être conformes aux normes suivantes :
1. IP55 pour la résistance à l'humidité
2. EN 60950-22 pour la sécurité

C. Tous les ponts sans fil doivent être conformes aux normes suivantes :
1. ETSI EN 300 328 pour la transmission sans fil
2. IEC/EN 60950-1 pour la sécurité intérieure
3. FCC, partie 15, sous-partie C, pour les radiateurs intentionnels
4. EN 301-489 pour les appareils radio
5. UL 60950-1 pour les équipements informatiques
6. Directive basse tension (LVD)
7. Directive sur la restriction des substances dangereuses (RoHS)
8. Directive sur les équipements radioélectriques (RED)
9. Normes RSS exemptées de licence ISDE

1.9 EXIGENCES GÉNÉRALES DE FONCTIONNALITÉ

A. Au moyen d'une serrure électronique, il doit être possible de contrôler l'accès par une porte :
1. Un détenteur de badge doit pouvoir présenter son badge à la poignée de porte pour obtenir un accès valide.
2. La présentation d'un identifiant non valide ne doit pas permettre l'accès.
3. Les utilisateurs doivent toujours être autorisés à sortir.

B. La serrure électronique doit être sans fil :
1. L'énergie doit provenir d'une source interne
2. Lorsque le logiciel de contrôle d'accès est utilisé, la communication de données avec le serveur doit être sans fil

C. Le logiciel de contrôle des accès doit enregistrer les événements d'entrée de porte.
1. Un événement doit être généré pour les éléments suivants :
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 le niveau de la batterie est faible.
2. Tous les événements doivent être estampillés de l'heure et de la date.
3. Tous les événements doivent contenir la porte à laquelle ils se rapportent.
4. Tous les événements de la serrure électronique doivent être communiqués au serveur en temps réel

D. La serrure électronique doit rester fonctionnelle lorsqu'elle est hors ligne
1. La serrure électronique doit prendre des décisions de contrôle des accès sans communication

avec un serveur.

2. La serrure électronique doit stocker les événements récents lorsqu'il est hors ligne, mettant à jour le serveur avec les événements lorsque la communication est rétablie.

a. Au moins 16 000 événements seront stockés dans la serrure électronique

E. Le logiciel de contrôle des accès doit surveiller l'autonomie de la batterie des serrures électroniques

1. Il doit être possible de visualiser la durée de vie restante de la batterie des serrures électroniques dans le logiciel ACS.

a. La durée de vie de la batterie doit être affichée sous la forme de 5 états.

1.10 EXIGENCES GÉNÉRALES RELATIVES AUX COMMUNICATIONS

A. Serrure électronique au pont sans fil

1. La serrure électronique doit pouvoir communiquer sans fil avec un pont sans fil.

a. La fréquence porteuse doit être de 2,4 GHz.

b. Chaque pont sans fil doit pouvoir communiquer avec au moins 10 serrures électroniques.

c. La distance à laquelle une serrure électronique peut être située à partir d'un pont sans fil doit être (en « air libre ») d'au moins 15m (50').

2. Toutes les communications sans fil doivent utiliser le chiffrement AES 128 bits.

B. Pont sans fil vers le système de contrôle des accès

1. La passerelle sans fil doit communiquer avec le système de contrôle des accès.

a. Le pont sans fil doit se connecter directement à un contrôleur sur RS485 {Paxton10}

b. Le pont sans fil doit se connecter directement au WAN/LAN en utilisant TCP/IP {Net2}

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

D. Aucune adresse manuelle n'est requise.

PARTIE 2 PRODUITS

2.1 FABRICANTS

A. {Supprimer si nécessaire} Fabricant acceptable : Paxton

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} [usapaxton.support]

d. {DE} [Paxton.gmbh.support]

B. Les composants de la serrure électronique doivent être disponibles auprès d'un fabricant unique afin d'assurer la compatibilité des produits.

C. Le fabricant de la serrure électronique doit également fournir un système de contrôle des accès (ACS) compatible avec la serrure électronique.

D. Le fabricant de la serrure électronique doit également fournir un système d'entrée de porte compatible avec l'ACS.

E. Les composants doivent être constitués des éléments suivants :

1. Logiciel de contrôle des accès. Le fabricant doit avoir à son emploi le personnel de génie logiciel qui rédige et gère le code de l'ACS, et doit conserver toutes les licences requises.

2. Serrures électroniques. Le fabricant des serrures électroniques doit être le même que pour le système de contrôle des accès et le logiciel de contrôle des accès.

3. Pont sans fil. Le fabricant des serrures électroniques doit également fournir un pont sans fil pour permettre aux serrures électroniques sans fil de communiquer avec un ACS.

F. Limites de substitution

1. Il doit être possible d'installer une serrure électronique dans un ACS [Paxton10] [Net2] existant.

2. Il doit être possible d'installer une serrure électronique en remplacement fonctionnel d'un lecteur et d'une serrure de porte existants.

2.2 CONDITIONS GÉNÉRALES RELATIVES À LA SERRURE ÉLECTRONIQUE

A. Il doit être possible d'incorporer la serrure électronique dans un ACS existant avec l'ajout d'un pont sans fil.

B. Le système doit comprendre des serrures électroniques à porte unique afin d'assurer une résilience maximale du système grâce à une intelligence entièrement distribuée.

C. La serrure électronique ne doit pas inclure de réglages de commutateur à régler.

D. La serrure électronique doit être fournie avec une garantie d'au moins cinq (5) ans.

E. Il doit être possible d'installer la serrure électronique sur toute porte d'une épaisseur comprise entre 35 mm et 62 mm (1,4 à 2,4 po).

2.3 CONDITIONS SPÉCIFIQUES RELATIVES À LA SERRURE ÉLECTRONIQUE

A. 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) EM4100/02

(iii) MIFARE Classic 1K

(iv) MIFARE Classic 4K

(v) MIFARE Ultralight
(vi) MIFARE Ultralight C
(vii) MIFARE Mini
(viii) MIFARE DESFire
(ix) MIFARE Plus
(x) HID Prox {L'activation peut être requise}

2. Les formats d'identifiants suivants doivent être pris en charge :
    a. Porte-clés
    b. Badge
    c. Carte ISO
    d. Watchprox
3. La plage de lecture doit atteindre un maximum de 55 mm (2,2 po).

B. Affichage

1. L'article doit accueillir 2 LED
    a. 1 x LED rouge
    b. 1 x LED verte
2. Les voyants doivent indiquer les événements suivants :
    a. Lecture d'identifiant valide — accès accordé
    b. Lecture d'identifiant non valide — accès refusé
    (i) Autorisations non valides
    (ii) Identifiant inconnu
    (iii) Identifiant interdit
    c. Mise à jour en cours
    d. Liaison au système
    e. Batterie faible
    f. Démarrage/sous tension

C. Audio

1. L'article doit contenir un émetteur de son pour la rétroaction sonore
2. Une tonalité doit sonner pour indiquer les événements suivants :
    a. Lecture d'identifiant valide — accès accordé
    b. Lecture d'identifiant non valide — accès refusé
    (i) Autorisations non valides
    (ii) Identifiant inconnu
    (iii) Identifiant interdit
    c. Mise à jour commencée
    d. Liaison au système
    e. Batterie faible
    f. Démarrage/sous tension
3. Il doit être possible de désactiver la rétroaction sonore

D. Interaction des utilisateurs

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

2. L'article doit comporter une poignée des deux côtés.

a. Les poignées doivent avoir un diamètre de 19 mm (0,75 po).

b. La poignée ne doit pas tourner de plus de 45 degrés dans une seule direction.

c. La poignée doit tourner d'au moins 30 degrés pour que le loquet puisse se rétracter complètement.

d. Sur le côté non sécurisé de la porte :

(i) La poignée doit être libre de tourner lorsque l'accès n'est pas autorisé.

(ii) Sur présentation d'un identifiant valide, tourner la poignée doit déverrouiller la porte.

e. Sur le côté sécurisé de la porte :

(i) La rotation de la poignée doit déverrouiller la porte permettant la sortie à tout moment.

3. Il doit être possible de configurer l'élément pour qu'il ne lise que les identifiants présentées lorsqu'un bouton est pressé

a. Cette configuration doit être configurée dans le logiciel ACS.

b. Le bouton doit être situé du côté non sécurisé de la porte.

c. Lorsqu'il est configuré pour fonctionner dans ce mode, l'article ne doit pas lire les badges de passage (dans un couloir occupé par exemple).

E. Boîtier de la serrure

1. La serrure électronique doit être adaptée à un boîtier standard de serrure à profil Euro.

2. Les boîtiers de serrure suivants doivent être supportés :

a. 48mm Euro

b. 72mm Euro

3. Le fabricant doit fournir une variante de produit qui n'a pas de remplacement de clé.

4. Le boîtier de la serrure doit être compatible avec un écartement de 55 mm (2,17 po).

F. Alimentation

1. L'article doit être alimenté par 4 piles alcalines AA 1,5 V

a. Les batteries doivent être situées du côté sécurisé de la porte.

2. L'autonomie de la batterie doit permettre au moins 55 000 opérations avant d'exiger un remplacement.

a. Les utilisateurs doivent toujours pouvoir sortir, quel que soit le niveau ou l'état de la batterie.

b. Lorsque les batteries doivent être remplacées, il doit être possible d'y accéder en utilisant des bornes de démarrage jumpstart situées sur la serrure électronique, conjointement avec un identifiant valide.

3. Le moteur de verrouillage doit être alimenté par l'alimentation électrique ACU.

4. 4 piles alcalines AA doivent être fournies avec l'article sans frais supplémentaires.

G. Température

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

a. Le côté interne/sécurisé de la serrure électronique doit fonctionner de manière fiable dans la plage de température comprise entre 0 °C et +49 °C (32 °F à +120 °F).

b. Le côté extérieur/non sécurisé de la serrure électronique doit fonctionner de manière fiable dans la plage de température comprise entre -20 °C et +55 °C (-4 °F à +131 °F).

H. Boîtier

1. L'article doit être élégant et moderne.
2. L'article doit avoir un aspect similaire des deux côtés de la porte.
3. L'article doit être disponible en 2 couleurs :
    a. Blanc
    b. Noir
4. L'article doit être disponible en 2 variantes :
    a. Interne
    b. Externe

I. Dimensions

1. L'article doit comporter la même empreinte sur les deux côtés de la porte.
2. Les dimensions (de chaque côté de la porte) ne doivent pas dépasser :
    a. Excluant la poignée :
    (i) Une largeur de 64 mm (2,4 po)
    (ii) Une hauteur de 127 mm (4,9 po)
    (iii) Une profondeur de 37mm (1,3 po)
    b. Y compris la poignée :
    (i) Une largeur de 155 mm (6,1 po)
    (ii) Une hauteur de 127 mm (4,9 po)
    (iii) Une profondeur de 93 mm (3,6 po)

J. Caractéristiques

1. L'article doit être économe en énergie et fonctionner en mode basse consommation.
2. L'article doit être stocké localement au minimum 10 000 identifiants.
3. L'élément doit pouvoir communiquer avec un système de contrôle des accès.
    a. L'article doit communiquer tous les événements en temps réel.
4. L'élément doit rester fonctionnel en mode hors connexion ou en mode autonome.
    a. L'article doit prendre des décisions en matière de contrôle des accès sans communication.
    b. L'article doit stocker les événements récents lorsqu'il est hors ligne, mettant à jour le système avec les événements lorsque la communication est rétablie.
    (i) L'article doit stocker au moins 16 000 événements hors ligne.
5. L'article doit signaler sa durée de vie de la batterie au système de contrôle des accès.
    a. Il doit être possible de visualiser la durée de vie restante de la batterie des serrures électroniques dans le logiciel ACS.
    (i) La durée de vie de la batterie doit être affichée en 5 états pour représenter la charge restante.
    b. La batterie faible doit être indiquée sur la serrure électronique

K. Autonome

1. La serrure électronique doit pouvoir fonctionner seule, sans communication avec d'autres serrures électroniques ou un serveur central.
2. La configuration des serrures électroniques doit être réalisée à l'aide de cartes de proximité avec fonctions programmées. Les cartes de configuration suivantes seront disponibles :

a. Carte d'inscription — pour inscrire des packs de badges

b. Heure d'ouverture de la porte — Pour configurer l'heure d'ouverture de la porte

c. Fonctionnement silencieux — Pour empêcher le verrouillage électronique d'émettre un son

3. Il doit être possible d'ajouter ultérieurement un pont sans fil et un logiciel de contrôle des accès pour permettre aux serrures électroniques de communiquer et d'être administrées par un serveur de contrôle des accès.

2.4 CONDITIONS SPÉCIFIQUES POUR LES BADGES

A. Le fabricant de l'ACS 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.

2.5 CONDITIONS SPÉCIFIQUES POUR LE PONT SANS FIL

A. Affichage

1. L'article doit accueillir 3 LEDs

a. 1 x LED verte

b. 1 x LED rouge

c. 1 x LED bleue

2. Les voyants DEL doivent indiquer ce qui suit :

a. Si l'article est alimenté

b. Activité sans fil et communication avec la serrure électronique sans fil

B. Alimentation

1. Un seul câble Ethernet doit être utilisé pour fournir à la fois de l'énergie et des données.

a. L'article doit être alimenté par le câble Ethernet à l'aide de PoE.

2. Lorsqu'il est alimenté :

a. L'article doit tirer une tension maximale de 30 V

b. L'article doit émettre un courant maximal de 300 mA

C. 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 +45 °C (32 °F à +113 °F).

D. Boîtier

1. Le fabricant doit fournir à l'article un boîtier de circuit imprimé en plastique blanc :

2. Il doit être possible de monter l'élément :

a. Sur un mur

b. Sur un plafond

c. Sur une backbox

3. Un kit de montage doit être fourni avec l'article pour le montage.

4. L'article doit être muni d'une antenne intérieure.

E. Dimensions

1. Les dimensions ne doivent pas dépasser :

(i) Une largeur de 164 mm (6,4 po)

(ii) Une longueur de 163 mm (6,4 po)

(iii) Une hauteur de 34 mm (1,3 po)

F. Le SCA doit prendre en charge au moins 100 ponts sans fil

G. Un pont sans fil doit supporter au moins 10 serrures électroniques

2.6 CONDITIONS GÉNÉRALES POUR LES LOGICIELS DE CONFIGURATION

A. Lors de la communication avec un ACS, il doit être possible de configurer les paramètres de serrure électronique suivants à partir du logiciel ACS :

1. Nom de la porte
2. Ouverture de la porte
3. Période de temps pendant laquelle garder la porte déverrouillée
4. Opération de verrouillage
    a. Configurer pour que ce soit déverrouillé chaque fois qu'un identifiant est présenté
    b. Configurer pour basculer le verrou en verrouillé/déverrouillé
5. Activer/désactiver le son

B. Les modifications apportées au logiciel de configuration doivent prendre effet lorsque la serrure électronique communique ensuite avec l'ACS.