KeyPad Plus

Clavier numérique sans fil avec prise en charge des cartes et des porte-clés sans contact.

Gestion sans contact, sans compromis sur la fiabilité

KeyPad Plus associe est un condensé de technologie de cryptage de pointe et d'expérience utilisateur perfectionnée, dans un outil permettant une gestion du système sécurisée et simplifiée. Armez et désarmez Ajax, activez le mode Nuit et gérez des groupes spécifiques avec une carte Pass ou un porte-clés Tag[1].

- Lecteur de de carte Pass et de porte-clés Tag
- Indicateurs du mode de sécurité
- Clavier tactile

KeyPad Plus est pris en charge par les panneaux de contrôle Hub Plus, Hub 2 et Hub 2 Plus

Système de protection des données de pointe

Pour identifier les utilisateurs rapidement et en toute sécurité, KeyPad Plus intègre la technologie DESFire®. C'est la meilleure solution sans contact permettant d'identifier un utilisateur par carte ou porte-clés du marché.

DESFire® est basé sur la norme internationale ISO 14443 et combine le cryptage 128 bits global et la protection contre la copie. Cette technologie est utilisée pour le transfert de capitaux européens et pour l'accès aux systèmes de la NASA.

En savoir plus sur les avantages de DESFire

Une micropuce intelligente

Du point de vue de l'utilisateur, l'accès sans contact est simple. Il suffit de passer une carte ou un porte-clés devant le clavier pour désarmer le système. Mais cette simplicité cache une technologie impressionnante. Les cartes Pass et porte-clés Tag sont équipées de puces DESFire®. Nous les avons comparées aux puces utilisées dans la plupart des systèmes d'accès dans le monde.

Puce	EM-Marin	MIFARE® Classic®	MIFARE® DESFire®
Utilisation	Systèmes d'accès simples : barrières,	Systèmes d'accès combinés, où des	Systèmes avec accès multi-niveau dans les

	interphones, chambres d'hôtel.	informations supplémentaires sont stockées sur la puce : clubs de fitness, centres de loisirs.	institutions gouvernementales, internationales et militaires.
Cryptage	Non	Chiffrement de flux Crypto-1 avec une taille de clé de 48 bits. *Plusieurs études ont démontré qu'il est possible de pirater ce type de chiffrement avec des outils en vente libre.*	Cryptage triple DES et cryptage matériel AES avec clé de 128 bits. *Il faudrait plusieurs supercalculateurs et des millions d'années pour la pirater.*
Mémoire	Pas de mémoire intégrée	Jusqu'à 4 Ko de mémoire intégrée, ce qui permet de stocker des données sur les paiements, la date d'expiration de la carte, et les utilisateurs.	Jusqu'à 8 Ko de mémoire intégrée, ce qui permet de stocker les données d'utilisateur et d'accéder aux clés de plusieurs systèmes de sécurité.

Autonomie exceptionnelle

Le tout nouveau firmware du KeyPad Plus permet d'exploiter de façon optimale les piles préinstallées. Même si la fonction d'identification sans contact est utilisée quotidiennement, le clavier peut fonctionner pendant 3,5 ans sans avoir besoin de remplacer les piles. Et si le lecteur de cartes et de porte-clés est désactivé, l'autonomie des piles peut atteindre 4,5 ans. KeyPad Plus avertit le centre de télésurveillance et les utilisateurs en avance lorsque les piles doivent être remplacées.

Gestion des accès à distance

Réglez des codes d'accès personnels pour savoir qui a désarmé le système, et quand il a été désactivé : le nom d'utilisateur est affiché dans la notification et dans le journal d'événements.

Pass et Tag peuvent également être attribués à un utilisateur spécifique, et il est possible de limiter les autorisations de gestion du système à des groupes spécifiques, où leur accorder l'accès au système du site en entier.

L'application Ajax vous permet de gérer les autorisations d'accès en temps réel. Vous pouvez limiter, étendre, ou bloquer ces autorisations instantanément.

- Code d'accès personnel
- Journal d'événements
- Blocage d'accès instantané

Ajouter des utilisateurs. Rapide et simple.

Les systèmes Ajax prennent en charge jusqu'à **200 Tags ou Pass**[2]. Il est inutile de créer un compte Ajax pour les nouveaux utilisateurs, il suffit d'attribuer un nom à l'appareil et de définir les autorisations d'accès. De cette façon il est plus facile de déléguer l'accès à la gestion du système à des employés temporaires ou nouvellement embauchés.

Indicateur du mode de sécurité

KeyPad Plus dispose d'indicateurs lumineux et sonores qui permettent de gérer l'état du système sans l'application Ajax. Le volume de l'appareil et la luminosité du rétroéclairage sont réglables.

Système anti-sabotage à plusieurs niveaux

Anti-sabotage	Blocage en cas de code erroné	Authentification	Intervalles d'interrogation
Les utilisateurs et le centre de télésurveillance reçoivent une notification lorsque quelqu'un retire le clavier de son support	Si 3 codes erronés consécutifs sont saisis, le clavier est bloqué et une alarme se déclenche	Si quelqu'un tente d'utiliser une carte ou un porte-clés non-valide, une alarme se déclenche.	Le système détecte une perte de connexion avec le clavier en moins d'une minute[3]

Transmission d'alarmes silencieuses vers une centre de télésurveillance

Si des intrus forcent un utilisateur à désarmer le système

Le code de contrainte vous permet de simuler le désarmement du système via KeyPad Plus. La présence de l'utilisateur ne déclenche pas de sirène, ni dans l'application ni via le clavier, mais une alarme est transmise instantanément au centre de télésurveillance[4].

Transmission des alarmes garantie

Nous avons développé le protocole radio Jeweller pour assurer le fonctionnement ininterrompu de tous les appareils du système. Le protocole radio utilise des intervalles de temps pour synchroniser la communication des appareils connectés, l'authentification pour éliminer les contrefaçons et le cryptage pour se protéger contre le piratage.

- Communication bidirectionnelle avec une portée de 1700 mètres
- 5 ReX au système
- Intervalle ping réglable de 12 secondes

Interface de gestion intelligente du système de sécurité

Utilisez des scénarios pour que vos procédures quotidiennes soient gérées automatiquement. Lors de l'armement, le système éteint les lumières, coupe l'arrivée d'eau, désactive les appareils électriques, ferme les volets roulants, le tout en un seul clic sur KeyPad Plus.

Installation simple

KeyPad Plus est connecté et paramétré dans l'application Ajax. Inutile de démonter le boîtier ni d'insérer des piles. L'appareil est ajouté au système grâce à son code QR. Il suffit au technicien de tester l'appareil, d'ajouter des cartes et de gérer les autorisations d'accès.

Spécifications techniques

Type de clavier	Clavier tactile capacitif
Installation	Intérieur seulement
Compatibilité	Hub Plus, Hub 2, Hub 2 Plus, ReX avec OS Malevich 2.11 et version supérieure
Code d'accès personnel	Oui
Protection contre les mots de passe erronés	Oui
Code de contrainte	Oui
Accès sans contact	DESFire® EV1, EV2 ISO14443-A (13,56MHz)
Alimentation	Piles : 4 lithium AA (FR6) Tension 1,5 V Autonomie des piles : jusqu'à 4,5 ans
Capteur de température	Disponible

Technologie radio Jeweller	Portée de communication avec l'unité centrale : jusqu'à 1700 m Communication bidirectionnelle entre les appareils Fréquences de fonctionnement : 868,0–868,6 MHz[5] Puissance de sortie RF auto-réglable : jusqu'à 20 mW Cryptage par blocs avec clé dynamique Intervalle Ping : 12 - 300 secondes En savoir plus sur Jeweller
Anti-sabotage	Authentification Détection de brouillage Alarme anti-sabotage
Plage de températures de fonctionnement	De - 10° C à + 40° C
Humidité de fonctionnement	Jusqu'à 75 %
Dimensions	165 × 113 × 20 mm
Poids	267 g
Certification	EN 50131, conforme aux exigences des règlements techniques régissant les équipements radio
Garantie	24 mois En savoir plus
Kit complet	KeyPad Plus Panneau de montage SmartBracket 4 piles AA (préinstallées) Kit d'installation Manuel d'utilisateur

[1] Les cartes et les porte-clés sont vendus séparément.
[2] Selon le modèle du hub : Hub 2 – jusqu'à 50 utilisateurs, Hub Plus – jusqu'à 99, Hub 2 Plus – jusqu'à 200.
[3] *Avec hub - période d'interrogation du détecteur de 12 secondes*
[4] À la condition que le système de sécurité soit connecté à un centre de télésurveillance.
[5] Selon la région de commercialisation