



Secure Badges

Transparence

Intuitif

Sécurisé

Efficacité

Convivial

Clair

Simplicité



Secure Badges



Comment sécuriser ses badges de contrôle d'accès?

Dinec apporte une solution conviviale à la sécurisation des badges de contrôle d'accès.

Il faut avant tout prendre conscience que pour copier un badge, il faut que la personne qui le copie se le procure : soit l'utilisateur lui donne, soit le badge est volé ou subtilisé ne fusse que temporairement.

Il appartient donc à chaque détenteur de badge d'être attentif à ne pas permettre ce genre d'opération et de signaler immédiatement la perte de son badge. Normalement on ne laisse pas trainer ses clés ou sa carte de crédit, alors pourquoi le faire avec son badge d'accès ?

Dans la sécurité, il faut toujours faire l'analyse de risque et augmenter les moyens mis en œuvre pour la sécurité si nécessaire.

En règle générale, cet aspect des choses est souvent négligé au profit du budget.

Mais concernant les badges, ce budget est plus que raisonnable Il n'y a donc aucune raison budgétaire pour ne pas augmenter sa sécurité

Majoritairement, il existe différentes technologies de badges qui fonctionnent suivant 2 fréquences :

- Le 125 KHz : permet une lecture de l'ordre de maximum 20-30 cm avec des moyens raisonnables.
- Le 13.56 Mhz : permet une lecture à maximum 3-5 cm. A cette fréquence, une communication bidirectionnelle est initiée entre le badge et le lecteur, ce qui augmente légèrement la sécurité.

Dans les 2 cas ces badges possèdent un numéro de badge accessible 'publiquement'. On l'appelle le CSN (Card Serial number) ou UID (Unique ID). Ce numéro est unique et est produit par le fabricant de la puce.

Lorsqu'il y a un piratage, c'est ce numéro qui est lu et encodé dans une carte programmable de la technologie équivalente.

On obtient ainsi une carte pirate produisant le même numéro de badge et qui permettra au fraudeur de s'identifier comme s'il était le porteur du badge initial.

Cette problématique n'est en rien liée à votre système de contrôle d'accès. Elle est liée à la technologie des badges.

Nous attirons votre attention sur le fait :

- Que la technologie 125 KHz est encore commercialisée actuellement car :
 1. meilleur marché : lecteur et badge
 2. la distance de lecture est plus confortable
 3. encore prescrite par les bureaux d'étude
- La technologie Mifare est de plus en plus répandue, mais reste utilisée sur base de son numéro de série (CSN ou UID)



Augmenter la sécurité des badges, quelle solution ?

Si l'on veut se garantir une protection contre les copies, à ce jour, seule l'utilisation de la technologie Mifare-Desfire avec application sécurisée peut être mise en oeuvre. Toutes les autres technologies sont copiables ou ont été piratées avec des moyens plus ou moins importants.

Les systèmes de contrôle d'accès Dinec apportent une solution sécurisée pour vos badges

Comment ça marche ?

Deux composants de votre système de contrôle d'accès sont impliqués dans cette sécurisation :

- le badge
- le lecteur

Du côté du badge, le numéro d'identification de l'utilisateur est encodé dans une zone du badge protégée par une clé d'authentification et un cryptage de haut niveau (AES 128 bits).

De son côté, le lecteur reçoit, à chaque mise sous tension, la configuration de sécurisation au travers de la communication RS-485 et peut donc accéder au numéro d'identification de l'utilisateur et le transmettre au système de contrôle d'accès.

Une histoire de clé !

Un mot revient régulièrement, c'est le mot 'clé'. En effet les encryptions se font sur base de clés de protection.

Il faut considérer le badge comme une grande armoire dans laquelle on peut avoir différentes boîtes.

Il existe une clé pour ouvrir l'armoire (qui représente le badge Mifare-Desfire) et il existe une clé pour chacune des boîtes rangées dans l'armoire (applications créées dans la mémoire du badge Mifare-Desfire).

En d'autres termes, il existe une clé pour créer ou supprimer des applications dans le badge et une ou plusieurs clés pour accéder au contenu d'applications sur la carte. Chaque application étant définie par un numéro d'identification (AID).

Il faudra donc définir :

- Un numéro d'application (AID).
- Une clé d'accès à cette application.
- Une clé protégeant la carte (optionnel).

Le principe est que le lecteur soit programmé pour aller lire exclusivement le contenu d'une application protégée.

Secure Badges



Dinec a fait le choix de l'ouverture et de la convivialité

Certains fournisseurs peuvent vous proposer des cartes sécurisées. Mais bien souvent ils restent propriétaire de votre sécurité. En effet, ils vous proposent des lecteurs et des cartes dont seuls eux sont propriétaires de la clé de protection ou de la programmation des lecteurs.

Ce qui lie le client avec le fournisseur et l'oblige à acheter les cartes chez un fournisseur unique qui peut dès lors pratiquer le prix qu'il veut.

Dinec a choisi de permettre au client de définir lui-même sa clé de protection et de formater ses cartes à partir d'un encodeur spécialement développé pour sécuriser la carte.

Concrètement

- Il faut encoder un numéro d'identifiant unique dans un badge Mifare-Desfire et plus particulièrement dans une application protégée par une clé.
- Il faut configurer les lecteurs DA-5003/DA-5013 pour qu'ils puissent lire le contenu de cette application protégée.

Du point de vue matériel il faut :

- Un système Dinec mis à jour avec une version logicielle reprenant la sécurité (DA400/DBM6000)
- Des lecteurs Dinec DA-5003/DA-5013
- Des cartes Mifare – Desfire (DA-1897/DA1877/DA-1899)
- L'application Android Smart6000 pour DMB6000 (pour Smartphone avec option NFC)





Du côté système

Dans le menu de configuration des lecteurs, le numéro de l'application et la clé de protection seront définis. Notez que la clé d'accès à la configuration de la carte est laissée libre. En effet, cela permet au client d'ajouter d'autres applications dans la carte afin de l'utiliser aussi pour d'autres solutions (Photocopieur, porte monnaie électronique, etc.).

Naturellement cela permet le formatage de la carte, mais le formatage ne créera pas une faille de sécurité. La carte sera effacée et ne sera tout simplement plus acceptée.

Une fois ces paramètres introduits, les lecteurs DA-5003/DA-5013 seront configurés automatiquement pour pouvoir lire cette zone sécurisée. De même l'application Android recevra ces paramètres pour pouvoir créer cette zone sécurisée dans le badge Mifare-Desfire.

Point de vue lecteur

Il n'y a pas d'action à entreprendre auprès du lecteur. La configuration de sécurisation est automatiquement envoyée au lecteur. Si le lecteur est déconnecté ou mis hors tension, il perd automatiquement sa clé. La sécurisation sera reprogrammée dès le retour du lecteur sur l'installation.

Point de vue de l'application Smartphone

Les paramètres Secure sont transférés dans l'application soit par WiFi soit par transfert des fichiers dans le directory de l'application. Dans la gestion des badges de l'application, le choix de l'option Secure permet le formatage du badge et la création de l'application avec son identifiant.

Comme numéro d'identifiant unique, nous avons choisi d'encoder soit le numéro de série du badge (CSN-UID) soit ce même numéro précédé par le préfixe 10.

Le choix du numéro de série présente les avantages suivant :

- Ne pas devoir réencoder les badges dans le cas d'une installation existante dans laquelle le numéro de série est lu. Le client pourra ainsi formater ses badges et passer en mode sécurisé quand tout est prêt.
- Lecteurs opérateurs LCT-5006 pourront être utilisés sans aucune reconfiguration
- Une garantie de l'unicité du numéro de badge sans risque de doublon.

Secure Badges



Encore plus de sécurité !!

La diversification des clés

Une option pour diversifier les clés existe. Cela permet d'augmenter la sécurité.

En effet, imaginons que quelqu'un parvienne à avoir connaissance de la clé de sécurité. Et ce malgré que ce soit un élément qui doit rester caché et secret.

Il pourrait recréer n'importe quel badge du système puisqu'il connaît la clé.

Le lecteur lirait le contenu de l'application et y trouverait un bon numéro.

Lorsque la diversification est activée, la clé d'accès à l'application est différente pour chacun des badges. Cette clé est le résultat d'un algorithme complexe tenant compte:

- du numéro de série de la carte (CSN-UID)
- de la clé de sécurisation
- d'une clé propre à Dinec

Une carte n'ayant pas été formatée par l'application Dinec ne pourra donc pas être lue !

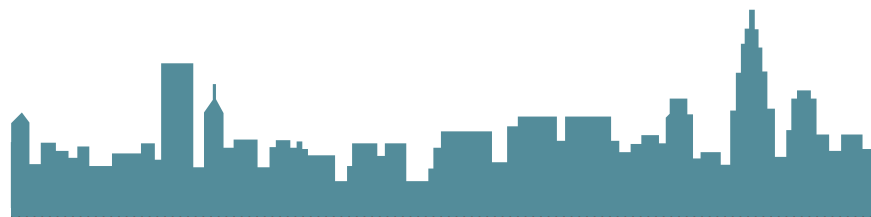


Une histoire, depuis 1981

Innovateur, concepteur et fabricant depuis 1981 Dinec International développe et commercialise ses solutions de sécurité, de gestion de temps et de gestion de bâtiments. Nos équipes travaillent avec l'objectif d'élaborer des systèmes dotés d'une technologie moderne et efficace. Nos développements préservent l'intégrité de votre patrimoine immobilier ou industriel tout en facilitant sa gestion technique et administrative au quotidien.

La proximité de notre bureau de développement et de l'unité de production en Belgique nous assure une symbiose parfaite pour le contrôle et la qualité de nos systèmes.

Notre gamme



 Contrôle d'accès par badges empreintes ou claviers

 Gestion des visiteurs

 Alarme anti - intrusion

 Gestion technique de bâtiments

 Suivi statistique

 Gestion de parking

 Vidéo surveillance

 Gestion de temps de présence

 Gestion énergétique

 Suivi des rondes



DINEC INTERNATIONAL
BELGIUM

Chaussée de Louvain 592
B-1380 Ohain

+32 (0)2 389 16 40  contact@dinec.be
+32 (0)2 387 14 02  www.dinec.be