NOTICE TECHNIQUE N° 28

Lecteurs et cartes *iCLASS* HID

Les lecteurs et cartes sans contact ***iCLASS*** de HID sont intégrés par de nombreux fournisseurs d'applications. Ils permettent de réaliser diverses applications, telles que la biométrie, la gestion horaire, la monétique, la gestion des processus de production et des immeubles, l'accès logique aux ordinateurs, la gestion des rondes, la gestion des parkings, les cartes d'abonnement, etc.

Les lecteurs ***iCLASS*** HID communiquent avec les cartes ***iCLASS*** par liaison radio 13,56 MHz. La norme ISO 15693 autorise une distance de lecture plus longue, tout en restant conforme aux normes en vigueur en matière de rayonnement électromagnétique. Grâce à un système d'authentification mutuelle, à des clés d'authentification plus longues et à un cryptage plus performant, la technologie ***iCLASS*** offre une meilleure sécurité que les technologiques 13,56 MHz comparables, telles que MIFARE. De plus, ***iCLASS*** utilise des clés diversifiées et est en mesure de crypter les données enregistrées sur la carte en utilisant les normes de chiffrage de données DES ou triple DES, là ou MIFARE enregistre les clés et les données en clair.

L'objectif du présent document est vous familiariser avec les fonctionnalités de la gamme ***iCLASS***. Le développement d'une nouvelle application nécessitera une formation ainsi qu'un kit de développement logiciel.

Les lecteurs *iCLASS*

Les lecteurs ***iCLASS*** sont actuellement disponibles en trois couleurs différentes : noir, gris ou blanc. Ils sont aussi disponibles en trois différentes tailles pour différentes applications. Toutes les options de configuration, telles que le mode de fonctionnement des LEDs et du beeper peuvent être présélectionnées en usine ou modifiées sur site au moyen de cartes de configuration spéciales disponibles auprès de votre agence HID.

Les lecteurs ***iCLASS*** peuvent être classés en 3 groupes : modèles à lecture seule, modèles à lecture/écriture, et modules OEM.

Modèles à lecture seule (sortie Wiegand)

R10 – pour les montants de portes et les espaces restreints
R30 – pour les boîtes d'encastrement européennes
R40 – pour les boîtes d'encastrement américaines (possède également des trous de fixation pour l'Europe/Asie)
RK40 – pour les boîtes d'encastrement américaines (possède également des trous de fixation pour l'Europe/Asie)

Ces lecteurs possèdent une interface Wiegand standard qui peut être utilisée par la plupart des systèmes de contrôle d'accès. Ils peuvent lire les données encodées (p. ex. au format Wiegand HID) dans les cartes, porte-clés et tags ***iCLASS*** ou les numéros de série des cartes MIFARE utilisant des circuits intégrés Philips S50 ou compatibles, en les convertissant en données Wiegand.

Modèles à lecture/écriture

RW300 – pour les boîtes d'encastrement européennes et applications nécessitant une interface Wiegand et/ou RS232
RW400 – pour les boîtes d'encastrement américaines (possède également des trous de fixation pour l'Europe/Asie) et applications nécessitant une interface Wiegand et/ou RS232
RWK400 – pour les boîtes d'encastrement américaines (possède également des trous de fixation pour l'Europe/Asie) et applications nécessitant une interface Wiegand et/ou RS232/485

En plus d'une interface Wiegand, ces lecteurs possèdent également une interface RS-232 leur permettant d'être connectés à un système de contrôle (un PC ou un contrôleur local). En utilisant le protocole série ***iCLASS***, les fournisseurs d'applications ont la possibilité de lire, d'écrire ou de modifier les informations enregistrées dans les secteurs d'application des cartes ***iCLASS***.

Modules OEM

OEM100/TTL – pour l'intégration dans des équipements de tiers disposant d'un volume réduit et nécessitant une interface Wiegand et/ou TTL.
OEM100/RS232 – pour l'intégration dans des équipements de tiers disposant d'un volume réduit et nécessitant une interface RS232
OEM300 – pour l'intégration dans des équipements de tiers nécessitant une interface Wiegand ou RS232

Ces modules sont constitués d'un circuit imprimé pouvant être intégré dans les boîtiers d'autres produits tels que des lecteurs biométriques ou des terminaux de gestion de temps de présence. Le lecteur OEM100/TTL dispose d'une interface TTL bidirectionnelle, le lecteur OEM300 et le lecteur OEM100/RS232 disposent d'une interface RS232. L'ensemble des modèles disposent de fonctions de lecture/écriture et permettent de contrôler une sortie collecteur ouvert. Ces circuits imprimés intègrent antenne et LEDs (pouvant être désolidarisées). Le beeper n'est pas fourni.

Les identifiants *iCLASS*

Les identifiants ***iCLASS*** peuvent être programmées en usine au format Corporate 1000 ou dans la quasi totalité des formats existants. Ces cartes sont disponibles en version 2 kbits (256 octets) ou 16 kbits (2koctets), la version 16 kbits étant disponible avec 2 ou 16 secteurs d'application (cf. paragraphe Organisation de la mémoire des cartes ***iCLASS***).

Il existe trois catégories d'identifiants ***iCLASS*** : les cartes, les porte-clés et les tags.

Les cartes *iCLASS* (réf. 200X – 204X) : cartes en PVC d'aspect blanc et brillant, dont les dimensions et l'épaisseur sont conformes aux normes CR80 et ISO 7810, ce qui permet de les utiliser dans tout type d'imprimante à badges. Elles peuvent être perforées en usine pour une utilisation verticale. Un numéro externe peut y être imprimé ou gravé au laser. Elles ne peuvent PAS être estampées.

Les cartes ***iCLASS*** sont également disponibles en combinaison avec d'autres technologies, p. ex. Piste magnétique, puce à contact, proximité HID ou Wiegand (cf. notre Guide de commande).
Nota : les cartes associant les technologies ***iCLASS*** et Wiegand ne peuvent pas être également combinées à une puce à contact pour des raisons d'épaisseur (0,94 mm).

Les porte-clés *iCLASS* (réf. 205X) : porte-clés en polycarbonate moulé possédant une fente afin de pouvoir être accrochés à un anneau. Un numéro externe peut y être imprimé.

Les tags *iCLASS* (réf. 206X) : disques autocollants fins et plats de 32 mm de diamètre et de 1,78 mm d'épaisseur qui, une fois collés, ne peuvent plus être décollés sans être détériorés. Ils peuvent être collés sur les surfaces non métalliques des assistants numériques, téléphones mobiles, porte documents ou autres. Vous pouvez également les coller sur la face arrière des cartes de contrôle d'accès utilisant d'autres technologies (par exemple : proximité, Wiegand, ferrite de baryum ou piste magnétique), ceci afin de permettre une transition aisée vers la technologie ***iCLASS***, sans pour autant avoir à changer vos badges existants. Etant donné que ces tags entraînent une surépaisseur du badge, nous vous recommandons de vous procurer des échantillons auprès de votre agence HID, afin de vérifier leur compatibilité avec des lecteurs à insertion, à défilement ou motorisés.

Les cartes MIFARE

Les lecteurs ***iCLASS*** permettent en outre de lire le numéro de série des cartes MIFARE de type :

- MIFARE HID, modèle 1430
- MIFARE HID et proximité à 125 kHz, modèle 1431
- Cartes équipées d'une puce Philips S50 ou compatible Infineon Card
- Cartes équipées d'une puce Philips Mifare Pro

Mode de sortie du CSN	Description	Commentaires
0	32 bits	Fournit comme sortie le numéro de série 32 bits de la carte, sous forme de donnée Wiegand (bit de poids fort (MSB) d'abord)
1	32 bits inversé (6055A)	Fournit comme sortie le numéro de série 32 bits de la carte, sous forme de donnée Wiegand en ordre inversé (pour être compatible avec le lecteur HID MIFARE, modèle 6055A)
2	26 bits	Fournit comme sortie une donnée Wiegand 26 bits formée des 16 bits (de poids faible) des 32 bits du numéro de série de la carte, de 8 bits fixes pour le code site, commencant et se terminant par des bits de parité. Le code site par défaut est égal à 001, mais vous pouvez le modifier au moyen d'une carte de configuration.
3	34 bits	Fournit comme sortie le numéro de série 32 bits de la carte, plus les bits de parité de début et de fin sous forme de donnée Wiegand
4	40 bits	Fournit comme sortie le numéro de série 32 bits de la carte, plus 8 bits de total de contrôle sous forme de donnée Wiegand

Figure 1 –Modes de sortie CSN des cartes MIFARE

Cette fonctionnalité convient tout particulièrement aux applications pour lesquelles l'utilisateur possède déjà des cartes MIFARE et désire utiliser ces mêmes cartes pour le contrôle d'accès. Bien qu'un lecteur MIFARE tel que le HID 6055B serait en mesure de réaliser cette tâche, l'utilisation du lecteur ***iCLASS*** offre les avantages suivants :

- un coût très avantageux
- Une distance de lecture supérieure d'environ 25%
- la possibilité de lire ou de passer à la technologie ***iCLASS***

Le lecteur ***iCLASS*** peut mettre à disposition le numéro de série 32 bits de la carte MIFARE, sous forme de donnée Wiegand, ceci dans divers formats (cf. figure 1) pouvant être configurés en usine (cf. notre Guide de commande) ou sur site au moyen de cartes de configuration.

Hormis le numéro de série de la carte, le lecteur ***iCLASS*** n'est PAS en mesure de lire d'autres données enregistrées dans les cartes MIFARE et ne peut pas non plus écrire sur une carte MIFARE.

Nota :
Le numéro de série aléatoire, unique, à 64 bits des cartes ***iCLASS*** est utilisé exclusivement pour l'anti-collision et la diversification des clés. Contrairement au numéro de série des cartes MIFARE, le numéro de série des cartes ***iCLASS*** HID n'est jamais transmis par le lecteur sous forme de donnée Wiegand. Ceci, parce que la plupart des contrôleurs de contrôle d'accès ne peuvent lire des codes sur 64 bits et parce que le CSN n'est pas sécurisé.

Le lecteur *iCLASS* peut également prendre en compte une population mixte de cartes MIFARE et *iCLASS*. Dans ce cas, il lira les données HID encodées dans les cartes *iCLASS* ainsi que le CSN des cartes MIFARE et les transmettra via l'interface Wiegand selon un format standard.

Nota : Les lecteurs RW300 et RW400 peuvent aussi fournir le CSN et les codes cartes iCLASS via liaison RS232.

L'interface des lecteurs iCLASS

Les lecteurs ***iCLASS*** sont munis d'un câble de connexion blindé de 45 cm (22AWG) présentant les couleurs et fonctions indiquées dans le tableau 2. Les modules OEM possèdent des plots à souder percés avec les mêmes connexions.

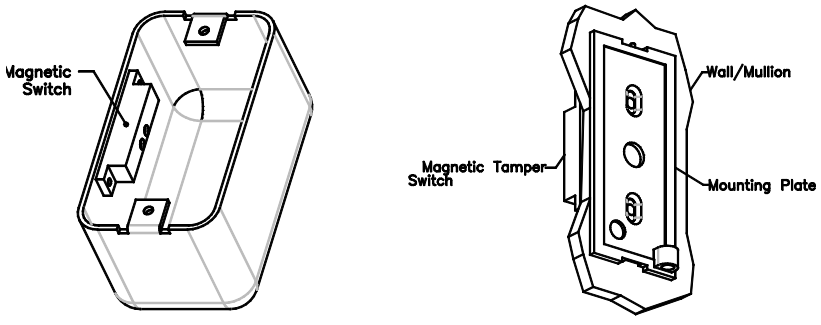
Rouge	+DC (10-16 Volts)
Noir	Masse
Vert	Donnée 0
Blanc	Donnée 1
Drain	** Masse Blindage
Orange	*LED verte
Brun	*LED rouge
Jaune	*Beeper
Bleu	*Hold
Violet	***Collecteur ouvert
Gris	***RX (réception série)
Rouge/vert	***DSR (non utilisé)
Rose	***TX (transmission série)
Rouge/jaune	***DTR (non utilisé)

* Connexions optionnelles
** Peut servir de ligne de retour de données si vous utilisez une alimentation séparée
*** Non utilisé sur les R10, R30, R40

Tableau 2 – Connexions du câble *iCLASS*

Contact d'autoprotection

Un signal d'autoprotection est fourni par un aimant interne lorsque ce dernier est utilisé avec un contact magnétique (ILS) connecté à un système d'alarme (à l'exception du lecteur R10). Positionnez le contact derrière le côté gauche de la plaque de montage, de manière centrée par rapport aux trous de fixation (figure 3). Les contacts magnétiques recommandés sont les suivants : Ademco 945T, Sentrol 1038T, GRI 100T ou 110T ou Aleph DC-2531. Ceci ne concerne pas les modules OEM.



Boîte d'encastrement **Mur**

Figure 3 – Montage du contact d'autoprotection

Alimentation

Les lecteurs ***iCLASS*** nécessitent une alimentation régulée linéaire 12 VDC. Leur plage de fonctionnement est comprise entre 10 et 16 VDC. Comme pour tous les lecteurs utilisant des communications radio, toute présence de parasites sur l'alimentation aurait pour conséquence une diminution des performances et de la distance de lecture. L'utilisation d'alimentations à découpage et de transformateurs couplés à des ponts redresseurs n'est pas recommandée.

La consommation moyenne (65 mA) est plus élevée que pour les lecteurs de proximité. De même, la consommation de crête (260 mA) est également plus élevée en raison du courant supplémentaire nécessaire pour la rangée de LEDs située à l'arrière de la "barre lumineuse".

Connexions Wiegand, LEDs, Beeper

Les connexions Wiegand sont identiques à celles des lecteurs de proximité HID.
La sortie Clock&Data n'est pas disponible. Les LEDs et le beeper peuvent être configurés pour un contrôle interne ou externe, la LED étant normalement verte, rouge ou éteinte. Les entrées des LEDs et du beeper sont activées lorsqu'elles sont au niveau bas (tension inférieur à 2,5 Volts). Vous avez la possibilité de commander le lecteur avec la configuration LEDs / beeper que vous souhaitez (cf. notre Guide de commande).

Lorsque le câble Wiegand est très long, il est conseillé de relier le blindage à la masse.

Le beeper peut produire des sons et des séquences de sons de volume variable. Ceci peut être configuré en usine ou sur site, au moyen de cartes de configuration. L'entrée beeper est du type TOR, la production effective du signal sonore étant contrôlée par le microprocesseur du lecteur. Il n'y a pas d'entrées audio externes.

Entrée Hold

L'entrée Hold, lorsqu'elle est active, inhibe le circuit de transmission radio. Cette entrée peut être, par exemple, pilotée par un détecteur de véhicules, de sorte à ce que le lecteur de carte n'accepte de carte qu'en présence d'un véhicule. Cette entrée peut également être configurée de sorte à ce que le lecteur ne mémorise qu'une seule lecture de carte (ignorant toutes les lectures consécutives) jusqu'à ce qu'elle soit désactivée. Ceci peut être déterminé au moyen d'une carte de configuration.

Sortie Collecteur ouvert

Cette sortie est normalement ouverte et est contrôlée par une commande via la liaison série (n'existe pas sur les modèles R10, R30 et R40). Ceci permet de contrôler tout

dispositif pouvant être commandé au moyen d'une fermeture d'un contact. Ceci s'avère particulièrement utile dans les applications autres que le contrôle d'accès, dans lesquelles aucun relais n'est disponible à l'emplacement où se trouve le lecteur. La sortie peut être fermée, ouverte ou fermée momentanément durant une période de 1 à 255 secondes.
La sortie Collecteur ouvert peut commuter jusqu'à 50 mA à 12 VDC (13,8 VDC max.). Pour des charges plus élevées, vous devez utiliser un relais d'interfaçage. Il est recommandé d'installer un parasurtenseur (MOV) pour toute charge inductive reliée à cette sortie, afin d'empêcher que des impulsions transitoires n'endommagent le lecteur.

Liaison série

Les lecteurs RW300, RW400, et RWK400 possèdent une liaison série RS-232 afin d'être connectés à un système de contrôle. Seules les lignes RX et TX sont utilisées. Le circuit imprimé de l'OEM100/TTL est muni de deux plots pour l'interface TTL.
Nota :le lecteur RWK400 dispose aussi d'une interface RS485.

Les modes de fonctionnement

Les lecteurs sans contact 13,56 MHz ***iCLASS*** (RW400, RW300, RWK400, OEM100 et OEM300) possèdent deux modes de fonctionnement : le **Mode Sécurité** et le **Mode Transparent**. Les lecteurs ***iCLASS*** à lecture seule (R10, R30, R40, RK40) fonctionnent uniquement en mode Sécurité.

Mode Sécurité – Ce mode de fonctionnement est prévu pour être utilisé avec une centrale de contrôle d'accès. Le lecteur peut lire tout type de formats de données programmées sur la carte ***iCLASS*** (ou encore, le CSN 32 bits des cartes Mifare) et transmettre ces données au format Wiegand (et/ou en option, au format hexadécimal via le port série pour les lecteurs à lecture/écriture). Dans ce mode, le lecteur fonctionne de manière autonome lorsqu'une carte lui est présentée. Il répond également à une activation de ses entrées de commandes LEDs, Beeper et Hold.

Le fonctionnement en Mode Sécurité peut être mis en œuvre par les OEM, intégrateurs et installateurs de contrôle d'accès, par simple connexion des sorties Wiegand, de la même manière que pour un lecteur de proximité standard ou un lecteur Wiegand. Les données Wiegand sont programmées dans les cartes ***iCLASS*** en usine ou sur site au moyen d'un programmateur. HID vous propose des formations, afin que vous soyez en mesure d'assister vos clients dans le choix des cartes et lecteurs ***iCLASS*** adaptés à leurs besoins.

Mode Transparent – Ce mode de fonctionnement permet aux développeurs et aux intégrateurs d'effectuer la lecture ou l'écriture des cartes ***iCLASS***.
Le programme d'application proprement dit (distribution automatique, retrait, billetterie, etc.) réside dans l'ordinateur ou le microcontrôleur du système de contrôle et non pas dans le lecteur. Le lecteur fonctionne sous contrôle exclusif du système en répondant aux commandes externes transmises via la liaison série.

Le système centrale contrôle la lecture des cartes, les LEDs, le beeper, la sortie collecteur ouvert, de même que toutes les opérations de lecture/écriture.
Le logiciel ou firmware doit contenir une boucle de programme demandant au lecteur de détecter périodiquement les cartes ayant pénétrées le champ radio. Les lignes de contrôle des LEDs, du beeper et de la fonction Hold continuent à fonctionner dans ce mode.

iCLASS utilise le protocole ISO 7816-4 qui correspond également à la norme en vigueur pour la communication avec les lecteurs de cartes à puce à contact.

Le fonctionnement en mode Transparent peut être mis en œuvre par les fournisseurs d'applications. HID leur propose des kits de développement logiciel, une formation ainsi qu'une assistance technique.

Les standards ISO

Les lecteurs ***iCLASS*** peuvent communiquer avec des cartes à puce sans contact conforment à des normes ISO. Ces normes définissent le protocole utilisé pour la communication entre la carte et le lecteur, la fréquence, le type de modulation ainsi que le débit des données. Les lecteurs ***iCLASS*** sont conforment à la norme ISO 14443A (pour la prise en compte des cartes MIFARE) et aux normes ISO 1443B2 et ISO 15693 pour les cartes ***iCLASS***. L'avantage des normes 14443A ou 14443B2 réside en un débit de données plus important, ceci toutefois au détriment de la distance de lecture. Les lecteurs ***iCLASS*** utilisent typiquement la norme 15693, parce que le débit de données s'adapte parfaitement à la plupart des applications et que la distance de lecture est plus importante (les cartes 2K peuvent uniquement communiquer selon la norme ISO 15693).

Les lecteurs ***iCLASS*** sélectionnent automatiquement la norme ISO 14443A ou ISO 15693, selon que vous leur présentez une carte MIFARE ou une carte ***iCLASS***. En utilisant une carte de configuration, vous pouvez les paramétrer de sorte à ce qu'ils utilisent uniquement la norme ISO 14443B2 pour communiquer avec des cartes ***iCLASS***. Les lecteurs ***iCLASS*** à lecture/écriture peuvent être configurés pour utiliser la norme ISO 14443B2 via une commande du protocole série ***iCLASS***.

La possibilité de communiquer selon une norme ISO particulière ne signifie pas qu'il est possible de communiquer au moyen des méthodes de cryptage propriétaires utilisées par les divers fabricants de puces. Chaque fabricant, comme Philips ou Infineon, propose son propre “jeu de circuit” contenant des algorithmes propriétaires. S'il ne possède pas le jeu de circuits requis, le lecteur ne peut pas lire les données enregistrées dans la carte ; il peut uniquement lire le CSN de la carte.

Utilisation de la technologie *iCLASS* pour des applications autres que le contrôle d'accès

Pour utiliser les lecteurs ***iCLASS*** à lecture/écriture pour des applications telles que la biométrie, la gestion horaire, la distribution automatique, etc., les fournisseurs

d'applications doivent écrire ou adapter leur application afin qu'elle puisse utiliser le protocole ***iCLASS***. Ils peuvent ensuite proposer une solution intégrée consistant soit en un lecteur ***iCLASS*** connecté à un PC ou à un terminal spécialisé, soit en un module OEM ***iCLASS*** intégré dans un terminal spécialisé.

Les fournisseurs d'applications vont également développer un logiciel ou un autre moyen permettant de programmer les données de leur application dans les cartes ***iCLASS***, comme p. ex. un terminal de saisie dans le cas de la biométrie, un distributeur de billets ou un terminal de cartes de crédit dans le cas d'applications de distribution automatique.

Etant donné que ***iCLASS*** utilise le protocole ISO 7816-4, cette intégration sera relativement simple pour les fournisseurs d'applications ayant déjà intégré des cartes à puce à contact dans leurs applications. Plusieurs fabricants de biométrie ont ainsi déjà intégré la technologie ***iCLASS***.

Le SDK (kit de développement logiciel) **iCLASS** comprend une documentation sur le protocole, un guide de programmation ainsi qu'une DLL (Dynamic Link Library), quelques exemples logiciels, un programme de démonstration, ainsi qu'un lecteur avec son alimentation et un support.
Les DLLs nécessitent une plateforme PC. Il est possible d'utiliser des commandes de protocole de bas niveau pour les microcontrôleurs et les plateformes autres que PC.

Les utilisateurs finaux peuvent s'adresser à HID afin d'obtenir une liste de fournisseurs d'applications proposant des solutions clé en main.

L'organisation de la mémoire des cartes *iCLASS*

Il existe trois types de zones de mémoire (figure 4) sur les cartes ***iCLASS*** :

1 – Secteur fabricant/configuration
2 – Secteur 1 (secteur HID)
3 – Secteurs 2 à 16 (fournisseurs d'applications)

Secteur fabricant/configuration

Le secteur de données fabricant/configuration de chaque carte (figure 4) comporte 6 blocs (48 octets) et contient les données suivantes :

- Numéro de série de la carte (numéro unique à 64 bits)
- Données de configuration incluant la limite du secteur d'application et les fusibles
- Champ comprenant des enregistrements sécurisés
- Clés d'authentification pour les secteurs d'application 1 et 2
- Champ créateur d'application (non utilisé)

Secteurs d'application

Les cartes et tags ***iCLASS*** existent en diverses configurations. Selon leur modèle, les cartes ***iCLASS*** peuvent avoir 2 ou 16 secteurs d'application.
Dans la figure 5, la "mémoire disponible" désigne la mémoire qui n'est pas encore utilisée pour les secteurs fabricant/configuration ou pour le secteur d'application 1 (HID).

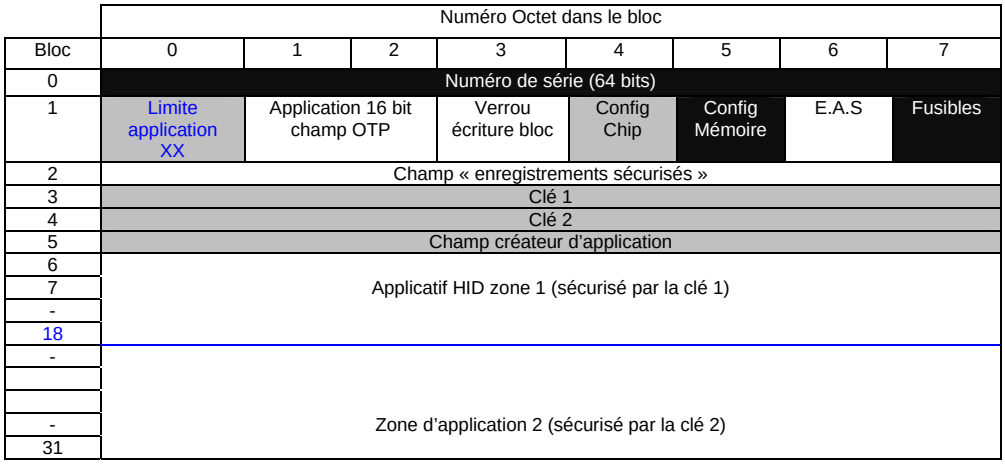


Figure 4 – Topographie de la mémoire des cartes *iCLASS* 2K (ou d'une paire de secteurs des cartes 16K/16)

Type de carte	Secteurs d'application	Mémoire totale de la carte	Secteurs disponibles	Mémoire disponible
2K/2	2	2 kbits (256 octets)	1	104 octets
16K/2	2	16 kbits (2048 octets)	1	1896 octets
16K/16	16	16kbits (2048 octets)	15	1560 octets

Figure 5 – Mémoire disponible pour divers types de cartes

Secteur d'application 1

Le secteur d'application 1 comporte 13 blocs ou 104 octets (figure 6) et est toujours réservé pour l'application HID contenant les données suivantes :

- Répertoire
- Code de contrôle d'accès (donnée au format Wiegand)
- Numéro d'identification personnelle PIN
- Mot de passe (futur)
- Etat APB (futur)
- Contrôle du secteur (futur)
- Champs utilisateur 1 à 4 (16 octets chacun)

Bloc		
6	Répertoire d'application HID	Répertoire d'application étendue HID
7	ID de contrôle d'accès HID	
8	ID de contrôle d'accès HID	
9	ID de contrôle d'accès HID	PIN
10	Mot de passe	
-	RFU	
18	RFU	

Figure 6 - Organisation du secteur d'application 1 des cartes *iCLASS*

Secteur d'application 2

Ce secteur de longueur fixe est prévu pour les applications utilisateur.

- Sur les cartes 2K/2, il comprend 13 blocs, soit 104 octets pouvant contenir des valeurs enregistrées (figure 4).
- Sur les cartes 16K/2, il comprend 237 blocs ou 1896 octets pouvant contenir un plus grand nombre de valeurs enregistrées, comme p. ex. des modèles biométriques ou des enregistrements (figure 7). Il est possible d'enregistrer plusieurs applications dans un même secteur, cependant dans ce cas, chaque fournisseur d'applications doit veiller à ne pas écraser les autres applications et tous doivent partager la même clé d'authentification.

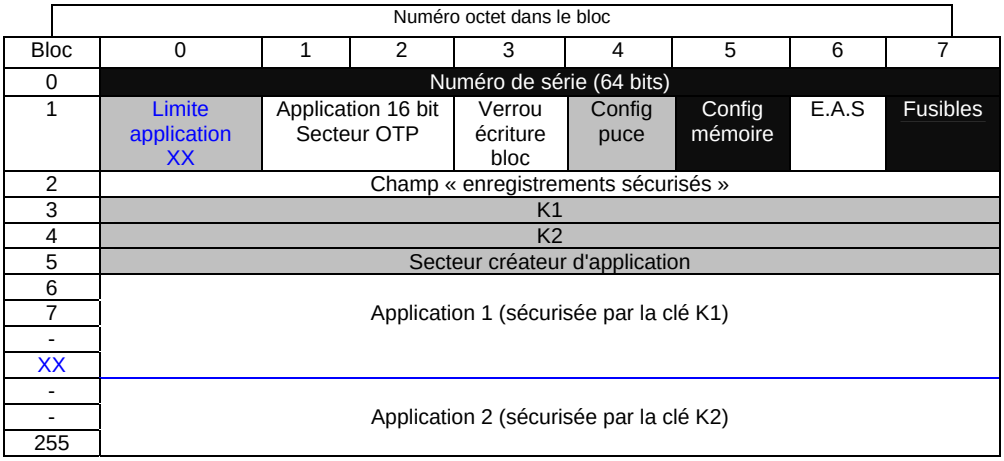


Figure 7- Topographie de la mémoire des cartes *iCLASS* 16K/2

Carte multi-application

La carte 16K/16 possède 16 secteurs d'applications (figure 8). Ils sont organisés en 8 pages, chaque page comportant un secteur fabricant et deux secteurs d'application formatés de manière similaire à ceux de la carte 2K/2 (figure 4). Le secteur fabricant de 6 blocs existe sur chacune des 8 pages, mais le numéro de série de la carte de la page 0 est utilisé pour toutes les clés. Le secteur fabricant de chaque page enregistre les clés appropriées pour ses propres secteurs d'application.

Dans la page 0, le secteur 1 est réservé pour l'application HID et le secteur 2 est fixe, comme pour les cartes 2K/2 et 16K/2. Dans les pages 1 à 7, les secteurs 3 à 16 sont disponibles pour les applications utilisateur et la limite entre chaque paire de secteurs d'application (3&4, 5&6, etc.) peut être définie une fois pour toutes durant la programmation.

Le fournisseur d'applications peut inscrire des données pour chaque application dans des secteurs individuels ou peut répartir des enregistrements plus grands (tels que des modèles biométriques) sur plusieurs secteurs, auquel cas chaque secteur doit être authentifié individuellement pour permettre l'extraction de l'enregistrement complet. Dans le cas de l'utilisation de secteurs multiples, il est recommandé de paramétrer la limite d'application à 31 (1F hexa) pour chaque paire de secteurs d'application, de sorte à ce que le premier secteur soit de taille maximale (208 octets) et le second soit de taille égale à zéro (figure 4). Ceci permet de réduire le nombre d'authentifications nécessaires pour lire les données enregistrées dans les multiples secteurs.

Pour la plupart des modèles biométriques, il existera encore des secteurs d'application disponibles sur la carte 16K/16, une fois le modèle enregistré. La figure 8, compare l'enregistrement d'un modèle biométrique entre une carte 16K/2 et une carte 16K/16.

Carte 16K/2

SECTEUR	CONTENU
1	Application HID
2	Application biométrique
↑	(non utilisé)
↓	

Carte 16K/16

PAGE	SECTEUR	CONTENU
0	1	Application HID
	2	Application biométrique
1	3	
	4	
2	5	
	6	
3	7	
	8	
4	9	Distribution autom.
	10	Parking
5	11	Retrait
	12	Bibliothèque
6	13	Accès logique
	14	Gestion
7	15	Infos personnelles
	16	Infos personnelles

Figure 8 – Enregistrement d'applications dans les cartes 16K/2 et 16K/16

Champ « enregistrements sécurisés » (application de crédit/débit) (bloc 2)

Cette fonction n'existe pas sur les cartes 2K ou 16K/2, mais est disponible dans les pages 1 à 7 de la carte 16K/16. Le champ « enregistrements sécurisés » permet de définir des “portes monnaie” sur la carte ***iCLASS*** pour des applications de distribution automatique, de billetterie ou de porte monnaie électronique.
Lorsque vous utilisez cette fonction dans une page particulière, la première clé sert de clé de débit, et la seconde de clé de crédit. Puisque ces clés sont également utilisées pour sécuriser le premier et le deuxième secteur d'application pour cette page, il n'est pas recommandé d'utiliser ces secteurs pour d'autres applications. Cependant, ces secteurs pourraient être utilisés pour y enregistrer des données en rapport, telles que le numéro de compte, la devise, les unités, les conditions de crédit, le solde du compte et le retrait maximum autorisé.

Programmation d'usine par défaut

Initialement, toutes les cartes sont préprogrammées en usine par HID. Vous pouvez également disposer d'un programmeur pour une programmation sur site.
La programmation par défaut est la suivante :

- ***Numéro de série*** : le bloc 0 correspond à l'ID 64 bits unique de la puce.
  Le numéro de série de la carte ne peut pas être modifié par l'utilisateur (norme ISO).
- ***Limite d'application*** : cet octet correspond à la valeur 18 (12 hexa) et paramètre ainsi la limite supérieure de l'application au bloc 18. L'application HID se trouve toujours dans le secteur d'application 1. Elle est constituée de 13 blocs. Pour la carte 16K/16, l'application HID se trouve toujours dans le secteur d'application 1 de la première paire de secteurs d'application. Les limites d'application des secteurs 3 à 16 de la carte 16K/16 peuvent être changées par le fournisseur d'application. Valeur par défaut : 0xFF
- ***Application 16 bit OTP (programmable une seule fois)*** : non utilisé
- ***Verrou écriture bloc*** : non utilisé – valeur par défaut : 0xFF
- ***Config puce*** : utilisé pour distinguer une carte sécurisée d'une carte non sécurisée. Valeur par défaut : 0xF9
- ***Config mémoire*** : utilisé pour distinguer une carte 16K/16 d'une carte 16K/2. valeur par défaut pour une carte 2K : 0x1F et pour une carte 16K : 0x9F
- ***E.A.S*** : non utilisé. Valeur par défaut : 0xFF
- ***Fusibles*** : s'ils sont "grillés", les clés d'authentification ne peuvent pas être changées sur site. Valeur par défaut pour une carte 2K est 0xB4 et 0xBC pour les cartes 16K
- ***Champ enregistrements sécurisés*** : non utilisé (existe dans les pages 1 à 7 de la carte 16K/16)
- ***K1, K2*** : K1 et K2 sont diversifiées par rapport aux clés standard HID.
  Pour la carte 16K/16, les 14 clés restantes sont également programmées à des valeurs par défaut HID. Chacune de ces clés sera différente. HID autorise des tiers à utiliser divers secteurs d'application en leur fournissant les clés par défaut correspondantes.
  Pour la carte 2K, ces clés ne peuvent plus être modifiées une fois qu'elles ont été programmées en usine. Pour les cartes 16K/2 et 16K/16, elles peuvent être modifiées sur site tant que les fusibles ne sont pas grillés.
- ***Application 1*** : réservé pour l'application HID
- ***Application 2*** : (et 3 à 16 sur des cartes multi applications) réservé pour les fournisseurs d'applications
- ***Répertoire d'application HID*** : définit la longueur et le format du code de contrôle d'accès HID, de même que la taille du code PIN. Précise si le code PIN et le code sont cryptés et, si tel est le cas, indique la clé et le mode de cryptage (DES ou triple DES).
- ***Répertoire d'application étendue HID*** : utilisé pour définir le format du mot de passe du reste du secteur d'application.
- ***Code de contrôle d'accès HID*** : code utilisée pour l'application de contrôle d'accès HID (sortie Wiegand ou RS-232). Sa longueur maximale est de 144 bits.
- ***PIN*** : code PIN à 48 bits réservé pour l'application de contrôle d'accès HID
- ***Mot de passe*** : nombre à 64 bits pouvant être écrit et lu par le programmateur (futur)
- ***RFU*** : zone de mémoire réservée pour une utilisation future

La sécurité *iCLASS*

Authentification mutuelle

L'authentification mutuelle est une procédure couramment utilisée en cas de communications cryptées. En fait, la carte et le lecteur doivent chacun s'assurer que l'autre possède des clés correspondantes, de sorte à ce que le lecteur "sache" que le détenteur de la carte est légitime et que la carte "sache" que le lecteur est autorisé à lire les informations qu'elle contient.

Si la carte et le lecteur se transmettaient simplement leurs clés afin de les comparer, quiconque possédant les connaissances techniques suffisantes ainsi qu'un récepteur réglé à la fréquence du lecteur serait en mesure de saisir cette information. Ceci lui permettrait de faire obtenir l'autorisation d'accès à sa propre carte à puce.

C'est la raison pour laquelle, la carte et le lecteur contiennent chacun des algorithmes cryptographiques complexes capables de brouiller les données transmises, afin qu'elles soient inintelligibles. Afin d'empêcher les "pirates" de désosser l'algorithme, la carte et le lecteur possèdent également des générateurs de numéros aléatoires qui insèrent chacun un numéro aléatoire dans l'algorithme, de sorte que lorsque vous lisez plusieurs fois la même carte, les données transmises sont différentes à chaque fois. Chaque carte contient un numéro de série unique utilisé pour crypter la clé enregistrée dans la carte, ce qui rend la clé unique dans chaque carte.

Lorsqu'elle est sélectionnée par le lecteur, la carte envoie d'abord son numéro de série (CSN) "en clair". Dans l'éventualité où de nombreuses cartes lui sont présentées, le lecteur utilise ces numéros d'identification pour réduire les autres cartes au silence et sélectionner une seule carte avec laquelle communiquer. Ce processus est appelé anti-collision. Ceci explique également pourquoi ***iCLASS*** n'utilise jamais le numéro de série pour le contrôle d'accès. Le numéro de série n'est pas crypté.

A ce stade, en supposant que le lecteur et la carte sont tous deux légitimés, ils ont à présent certaines informations en commun. Tous deux "connaissent" le numéro de série de la carte, tous deux possèdent l'algorithme de cryptage et tous deux possèdent la clé (le lecteur possède la clé actuelle, celle de la carte est diversifiée par le CSN).

Le lecteur utilise le numéro de série de la carte, la clé, un numéro aléatoire, et l'algorithme pour calculer un nombre à 64 bits. Il n'envoie cependant que les 32 premiers bits, appelés challenge. La carte reçoit le challenge à 32 bits, utilise cette donnée, l'algorithme, le numéro de série et la clé pour recréer les derniers 32 bits du nombre à 64 bits, appelés réponse, puis les renvoie au lecteur. Ce dernier compare la réponse de la carte à la réponse enregistrée dans sa mémoire et, si elles sont identiques, authentifie la carte. Une fois l'authentification mutuelle réalisée, la carte et le lecteur peuvent commencer à transmettre des données et le lecteur peut lire ou écrire dans le secteur de la carte ayant été authentifié.

Cryptage des données

Les données enregistrées dans le secteur d'application HID de la carte peuvent être cryptées au moyen du système de chiffrage DES ou triple DES, de sorte à ce que, même dans l'éventualité très peu probable où les clés auraient été "décodées“, les données ne pourraient toujours pas être lues.

Clés

Toutes les données enregistrées dans les cartes ***iCLASS*** sont sécurisées au moyen d’une clé. Une clé correspond à un mot de passe utilisé pour protéger les données contre la lecture ou la modification non autorisées. Les cartes et lecteurs ***iCLASS*** utilisent des clés à 64 bits. Chaque secteur d'application de la carte est protégé par une clé.

HID encode des données au format Wiegand dans le secteur d'application 1 de la carte ***iCLASS*** et protège ces données au moyen d'une clé propriétaire HID unique qui n'est pas divulguée. Une clé compatible est également enregistrée de manière sécurisée dans tout lecteur ***iCLASS*** HID.

Etant donné que chaque secteur d'application possède sa propre clé, une carte ***iCLASS*** peut être utilisée pour y enregistrer des informations de divers fournisseurs d'applications, ces deniers ne pouvant pas modifier, ni accidentellement, ni intentionnellement, les données des autres fournisseurs. Nous recommandons aux fournisseurs d'applications de modifier les clés par défaut de leurs secteurs, car ils sont responsables de leur propre gestion des clés et du cryptage de données.

Les fournisseurs d'applications ***iCLASS*** doivent utiliser des clés diversifiées pour protéger les secteurs d'application qu'ils utilisent. Le lecteur ***iCLASS*** à lecture/écriture facilite ceci en proposant une fonction de diversification des clés.

Le lecteur ***iCLASS*** peut enregistrer jusqu'à 12 clés d'authentification (seules 8 sont disponibles). Même si plus de 8 clés sont utilisées sur un site particulier, chaque lecteur ne doit enregistrer que les clés utilisées pour son application spécifique. Si nécessaire, il est possible de charger de nouvelles clés dans un lecteur.

Gestion des clés

Les principes de base de la gestion des clés sont les suivants :

- Toute clé doit être unique pour chaque carte et chaque client.
- Toute clé doit être cryptée et enregistrée de manière sécurisée.
- Aucune clé ne doit être transmise “en clair” via communication radio ou via RS-232.
- Aucune clé ne doit pouvoir être lue à partir d’un disque dur ou d’une puce mémoire non protégés.

Lorsque la gestion standard des clés est utilisée, les clés utilisées pour protéger le secteur d'application 1 sur toutes les cartes sont diversifiées à partir de la clé maître standard HID par un algorithme de cryptage, le numéro de série unique de la carte et le numéro de secteur de l'application, de façon à les rendre les uniques dans chaque carte et dans chaque secteur d'application. La même clé maître standard est enregistrée de manière sécurisée dans le lecteur et n'est jamais transmise. Etant donné qu'une clé maître est utilisée pour créer les clés de toutes les cartes et de tous les lecteurs, les lecteurs ***iCLASS*** possédant des clés standard sont interchangeables et compatibles les uns avec les autres. Grâce au cryptage et à l'authentification mutuelle utilisés dans les lecteurs ***iCLASS***, cette clé est très sécurisée.

Les clés haute sécurité ajoutent un niveau de sécurité supplémentaire au schéma de diversification et de cryptage de base des clés ***iCLASS.*** Pour les clients ***iCLASS Elite*** une clé haute sécurité client spécifique à un site est attribuée par HID à chaque client pour remplacer la clé standard. Pour le secteur d'application HID, le système de gestion des clés HID utilise un algorithme propriétaire pour générer une matrice de 256 octets à partir de la clé haute sécurité. Le numéro de série de la carte est utilisé pour extraire des octets en 8 endroits différents dans cette matrice afin de créer des clés 64 bits.

Dans toutes les cartes utilisant des clés à haute sécurité HID sécurise le secteur d'application 1 au moyen d'une clé diversifiée à partir de la clé à haute sécurité, et ensuite configure l'ensemble des lecteurs du site en conséquence. Chaque lecteur contient la clé haute sécurité et la base de données des clés. HID conserve les clés haute sécurité générées pour les clients ***iCLASS Elite*** dans une base de données cryptée, stockée dans un endroit sûr de son usine. De plus, une copie de sauvegarde est stockée dans un lieu externe sécurisé. Etant donné qu'une clé haute sécurité est utilisée pour encoder toutes les cartes et tous les lecteurs, les cartes et lecteurs ne sont pas interchangeables avec des cartes et lecteurs d'un autre site Des cartes et lecteurs supplémentaires doivent être commandés avec le même numéro ID ***iCLASS Elite*** .

HID proposera un programmateur de cartes ***iCLASS***. Il s'agit d'une version spéciale du lecteur que vous pouvez connecter à un PC fonctionnant sous Windows (similaire au ProxProgrammeur HID). Ce programmateur permet aux utilisateurs finaux ou aux intégrateurs de systèmes de créer et de sécuriser leurs propres clés haute sécurité sur site et permet également d'encoder et de crypter des données personnelles dans des zones de données spécifiées dans le secteur d'application HID de chaque carte. Ceci nécessite l'utilisation de cartes 16K/2 ou 16K/16. L'utilisateur final ou l'intégrateur de systèmes devra prendre particulièrement soin de la sécurité globale du système mis en place (confidentialité des clés, gestion des clés, …)

Pour de plus amples informations sur la gestion des clés, veuillez consulter le document "***iCLASS*** Security Implementation Plan" sur notre site Internet, à l'adresse www.hidcorp.com /iclass/index.html.