

Glossaire *iCLASS*TM

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Annexe A – Glossaire des clés

16K/16 – Carte mémoire 16 kbits (2 ko) avec jusqu'à 16 secteurs d'application. La zone lecture/écriture s'étend du bloc 6 au bloc 31 sur chacune des 8 pages. Cette carte permet les communications ISO dans les modes 15693 et 14443B, de même qu'un nombre infini de mises à jour des clés.

16K/2 – Carte mémoire 16 kbits (2 ko) avec 2 secteurs d'application. La zone lecture/écriture s'étend du bloc 6 au bloc 255. Cette carte permet les communications ISO dans les modes 15693 et 14443B, de même qu'un nombre infini de mises à jour des clés.

2K/2 – Carte mémoire 2 kbits (256 octets) avec 2 secteurs d'application. La zone lecture/écriture s'étend du bloc 6 au bloc 31. Cette carte ne permet ni les communications ISO 14443B, ni la mise à jour des clés une fois que le fusible est grillé.

Accès logique (*Logical Access*) -- (voir Connexion sécurisée).

AES -- Advanced Encryption Standard. Algorithme de cryptage de blocs symétriques pouvant utiliser des longueurs de clé de 128, 192 ou 256 bits. Depuis juillet 2002, la norme AES remplace les normes DES dans les applications du gouvernement américain. Elle est documentée dans la norme NIST FIPS 197. L'algorithme AES peut être utilisé avec la technologie *iCLASS* pour crypter les clés générées par le programmeur *iCLASS* avant que celles-ci ne soient enregistrées dans la base de données (voir aussi Cryptage).

Aimant pour alarme d'autoprotection (*Tamper Magnet*) – HID intègre un aimant dans le boîtier de ses lecteurs. Vous pouvez le combiner à un contact magnétique (non fourni) monté dans un boîtier d'encastrement, afin de générer une alarme d'autoprotection. Uniquement disponible sur les modèles R30, R40, RW300, RW400, RK40 et RKW400 (pas sur le R10).

Algorithme (*Algorithm*) – Suite d'opérations mathématiques permettant le traitement de données (voir aussi Algorithme de hachage, Cryptage).

Algorithme de hachage (*Hash Algorithm*) – Algorithme qui fournit toujours une sortie unique de longueur fixe lorsqu'on lui fournit une entrée unique de longueur variable. Il s'agit d'un algorithme à sens unique qui, une fois la sortie calculée, rend pratiquement impossible de régénérer l'entrée. NIST prend en charge des algorithmes de hachage avec SHA-1 conformes à la norme FIPS 180.

Anti-contrefaçon (*Anti-counterfeiting*) – Caractéristiques physiques ajoutées sur la surface de la carte afin d'en rendre la copie plus difficile, comme p. ex. les hologrammes, les encres fluorescentes ultraviolettes, les dispositifs à variabilité optique et la micro-implosion.

Anti-passback (*Anti-Passback*) – Paramètre configurable du lecteur permettant de définir la durée entre deux lectures consécutives de la même carte.

APDU -- Application Protocol Data Unit, selon ISO 7816-4. Protocole de communication simple (Commande/Réponse), développé pour l'industrie des puces à contact. L'utilisation de ce protocole dans les produits *iCLASS* permet une transition aisée des applications anciennement développées vers la technologie des cartes à puce sans contact.

Application de contrôle d'accès HID (application HID) (*HID Access Control Application (HID Application)*) – Réside toujours dans l'application 1 des cartes *iCLASS* programmées. HID réserve 13 blocs (6 à 18) pour l'application HID contenant le répertoire HID, le format de carte HID, le numéro d'identification personnelle (PIN), le mot de passe et 4 secteurs définis par l'utilisateur.

ASCII – American Standard Code for Information Interchange.

Rédigé par : Nathan Cummings – Responsable Marketing

Attaque frontale (*Brute Force Attack*) – Tentative de décryptage des clés dans laquelle il s'agit de tester, l'une après l'autre, toutes les combinaisons de clés possibles. Cette technique est irréaliste, car même s'il était possible de tester des milliers de clés par minute, il faudrait des années pour trouver la clé recherchée.

Attaque par répétition d'un enregistrement (*Replay Attack*) -- Mise en défaut de la sécurité consistant à enregistrer les communications entre la carte et le lecteur, puis à les répéter ultérieurement dans le lecteur (voir aussi Sniffer et Clonage).

Authentification mutuelle (*Mutual Authentication*) -- Procédé permettant à deux entités de s'authentifier l'une l'autre avant de transférer des données. Dans **iCLASS**, l'authentification mutuelle est réalisée au moyen d'un Challenge et d'une réponse générés à partir d'un algorithme secret résidant à la fois dans les lecteurs et les cartes. Les clés ne sont jamais transmises durant l'authentification mutuelle.

Binaire (*Binary*) – Système numérique utilisant la base 2, dans lequel les deux seules valeurs possibles sont 0 et 1 (voir aussi Bit).

Biométrie (*Biometrics*) – Technologie de vérification d'identité utilisant les caractéristiques physiques du corps humain.

Bit (*Bit*) – Chiffre binaire pouvant prendre la valeur un (1) ou zéro (0) (voir aussi Binaire).

Bloc de configuration (*Configuration Block*) – Bloc 1 de toutes les cartes **iCLASS**.

Boîtier d'encastrement (*Back Box*) – Egalement appelé boîte de jonction, il s'agit d'un boîtier pour interrupteur électrique mural classique dans lequel il est également possible de monter un lecteur. Les dimensions de ce boîtier varient selon les pays.

BWL -- Block Write Lock. Champ fixe de 8 bits dans le bloc de configuration (octet 6) pouvant être paramétré pour protéger les blocs 6 à 12 contre l'écriture.

Carte (*Card*) – Support de données en PVC conforme à la norme ISO 7810. Il existe également des cartes répondant à des normes plus rigoureuses (voir aussi Carte permettant d'intégrer une puce) ou ne répondant à aucune norme (voir aussi **iCLASS**/Wiegand).

Carte (*Credential*) – Désignation générique des supports de données **iCLASS** (carte, tag et porte-clés).

Carte configurée (*Configured Credential*) – Carte ayant été configurée (c'est-à-dire dans laquelle la configuration de la mémoire a été paramétrée) et dont le fusible a été activé.

Carte de configuration – Carte **iCLASS** spéciale permettant de reconfigurer les paramètres des lecteurs **iCLASS** (fonctionnement des LED et du beeper, caractéristiques des impulsions Wiegand, ...).

Carte multitechnologie (*Multi-Technology Credential*) -- Une même carte intégrant plusieurs technologies (p. ex. **iCLASS** Prox ou **iCLASS** Wiegand).

Carte permettant d'intégrer une puce (*Embeddable*) – Carte fabriquée conformément à la norme ISO 7816 afin de permettre l'intégration d'une puce à contact.

Carte programmée (*Programmed Credential*) -- Toute carte ayant été configurée et dont le secteur d'application 1 a été programmé pour le contrôle d'accès utilisant un format HID quelconque existant.

CE (*CE*)– Le marquage CE est le certificat officiel exigé par la Communauté Européenne pour tout équipement électronique mis en vente ou utilisé pour la première fois dans l'un des pays de la Communauté Européenne.

Challenge (*Challenge*) – Résultat fourni par l'algorithme d'authentification mutuelle et utilisé par la carte pour authentifier le lecteur (voir aussi Authentification mutuelle).

Champ créateur d'application (*Application Issuer Area*) -- Bloc 5 dans toutes les cartes **iCLASS**. Zone permettant d'enregistrer l'identification et la version de l'application.

Champ enregistrement sécurisé (*Stored Value Area*) – Bloc 2 dans toutes les pages des cartes **iCLASS**. Requiert l'accès à la fois à la clé 1 (débit) et à la clé 2 (crédit). Non disponible sur les cartes possédant 2 secteurs d'application. Valeur maximale : 65535.

CHK – Checksum : caractère de contrôle utilisé pour valider des données.

Clonage (*Cloning*) – Tentative de duplication d'une carte afin de mettre en défaut un système de cartes à puce (voir aussi Attaque par répétition d'un enregistrement).

Rédigé par : Nathan Cummings – Responsable Marketing

Code source (*Source Code*) -- Fichiers de texte, générés par des développeurs de logiciels, que vous pouvez compiler en applications exécutables. Le code source est habituellement généré dans des langages de programmation tels que Visual Basic (VB) ou C++ (voir aussi SDK).

Commande double des LED (*Dual-LED Control*) – Paramètre pouvant être configuré dans le lecteur, de sorte à permettre la commande matérielle à la fois de la LED rouge et de la LED verte.

Complément à un (*Ones Complement*) -- Permutation de données binaires, où chaque 1 devient 0 et chaque 0 devient 1.

Configuration de la puce (*Chip Configuration*) – Champ fixe de 8 bits dans le bloc de configuration (octet 3) permettant de définir les cartes sécurisées et non sécurisées.

Connexion sécurisée (*Secure Logon*) – Application permettant de vous connecter en toute sécurité à votre PC. Outre un mot de passe, vous devez généralement utiliser un badge ou une identification biométrique.

Contrôleur (*Host*) -- PC ou microcontrôleur qui commande les communications d'un lecteur/écriture *iCLASS* (esclave), fonctionnant généralement en mode transparent.

Cryptage (*Encryption*) – Traitement des données via un algorithme, afin de les rendre indéchiffrables.

CSN – Card Serial Number : numéro de série de la carte, également appelé identificateur unique (Unique Identifier, UID). Ce numéro est unique pour chacune des cartes à puce à contact existant dans le monde entier. Il permet d'éviter les collisions, une seule carte pouvant être sélectionnée à la fois dans le champ d'excitation.

Décryptage (*Decryption*) – Traitement des données cryptées par un algorithme, afin de leur rendre leur forme initiale.

DES -- Data Encryption Standard. Algorithme de cryptage via blocs symétriques utilisant une clé unique de 56 bits. La même clé est utilisée pour le cryptage et le décryptage. La norme DES est documentée dans la norme NIST FIPS 46.

Distance de lecture (*Read Range*) -- Distance maximale entre la carte et le lecteur, à laquelle une communication satisfaisante peut être réalisée. Elle peut être influencée par le facteur de forme de la carte, les dimensions du lecteur et les conditions d'installation.

Diversification (*Diversification*) – Algorithme de hachage qui crypte le numéro de série de la carte (CSN) au moyen d'une clé spécifique.

DLL -- Dynamic Link Library. Cette bibliothèque fournit aux développeurs de logiciels une interface de programmation évoluée, grâce à laquelle l'intégration est plus rapide et plus simple.

EAS -- Electronic Article Surveillance : surveillance électronique des articles.

EEPROM -- Electrically Erasable Programmable Read Only Memory : mémoire morte effaçable électriquement.

Elite (*Elite*) -- Programme développé par HID qui se charge de générer, gérer et programmer des clés de haute sécurité spécifiques à un site dans les cartes et lecteurs *iCLASS*, avant d'expédier ces derniers au client. Ceci permet d'obtenir un niveau de sécurité encore supérieur à celui des clés de sécurité standard et de diminuer les responsabilités du client quant à la gestion des clés.

Esclave (*Slave*) – Etat d'un lecteur/écriture totalement commandé par un contrôleur (voir aussi Mode Pass-thru).

FCC -- Federal Communications Commission.

FIPS -- Federal Information Processing Standards (documents normalisés publiés par NIST).

Firmware (*Firmware*) – Programme exécutable résidant dans un microcontrôleur. Le firmware de *iCLASS* réside dans un microcontrôleur PIC18F et définit la mise en route, les paramètres par défaut, le fonctionnement et les fonctionnalités du lecteur/écriture.

Fusible (*Fuse*) – Champ fixe de 8 bits dans le bloc de configuration (octet 0). Une fois que ce champ est activé, il ne sera plus possible de modifier le bloc de configuration.

Gabarit (*Template*) -- Représentation mathématique d'une caractéristique physique utilisée pour l'enregistrement et la vérification biométriques (voir aussi Biométrie).

Rédigé par : Nathan Cummings – Responsable Marketing

Gestion des clés (*Key Management*) – Manière dont les clés sont générées, transférées et enregistrées en toute sécurité.

Haut-parleur (*Speaker*) -- Utilisé à la place d'un beeper dans les lecteurs **iCLASS**, afin d'émettre des sons de fréquence et de durée variables.

Hexa (*Hex*) -- hexadécimal. Système numérique utilisant la base 16, dans lequel les valeurs vont de 0 à F.

iCLASS/Wiegand (*iCLASS/ Wiegand*) – Carte multitechnologie combinant les technologies **iCLASS** et Wiegand. Plus épaisse que la plupart des autres cartes, elle ne répond pas aux normes ISO.

Impulsion Wiegand (*Wiegand Pulse*) -- Paramètre configurable du lecteur permettant de définir la durée d'une impulsion Wiegand.

Interopérabilité (*Interoperability*) – Aptitude des produits de multiples fabricants à se reconnaître et à fonctionner les uns avec les autres.

Intervalle entre deux impulsions Wiegand (*Wiegand Spacing*) -- Paramètre configurable du lecteur permettant de définir la durée minimale entre deux impulsions Wiegand.

ISO -- International Standards Organisation.

ISO 10373 – Norme relative aux méthodes de test des cartes d'identification.

ISO 10536 – Norme relative aux cartes à puces sans contact - Couplage direct. Peu répandue.

ISO 14443 – Norme relative aux cartes à puces sans contact - Proximité. Inclut les versions de Type A (initialement MIFARE®) et de Type B.

ISO 15693 – Norme relative aux cartes à puces sans contact - Mains-libres. Norme initiale utilisée dans **iCLASS**.

ISO 7810 – Norme relative aux caractéristiques physiques des cartes d'identification.

ISO 7811 – Norme relative aux spécifications des techniques d'enregistrement de données, telles que la gravure et les pistes magnétiques.

ISO 7816 – Norme relative au positionnement et à la communication des cartes à puce à contact.

Lecteur (*Reader*) -- Lecteur **iCLASS** utilisé pour des applications de contrôle d'accès en mode sécurisé. Les lecteurs ne permettent pas la communication série.

Lecteur/écriture (*Reader/Writer*) -- Lecteur/écriture **iCLASS** possédant toutes les fonctionnalités d'un lecteur **iCLASS** avec en plus la possibilité de réaliser des communications série.

LED -- Light Emitting Diode : diode électroluminescente. Les lecteurs HID sont équipés d'une rangée de LED ou d'une barre lumineuse pour améliorer la signalisation visuelle.

Ligne HOLD (*Hold Line*) – Entrée de commande du lecteur dont la fonction est définie par un paramètre EEPROM configurable dans tous les lecteurs **iCLASS**. Lorsqu'elle est activée, elle permet soit d'enregistrer une lecture unique de carte, soit de désactiver totalement le champ d'excitation des radiofréquences.

Limite d'application (*Application Limit*) – Champ fixe de 8 bits dans le bloc de configuration (octet 7), qui définit le dernier bloc du premier secteur d'application sur chaque page.

LSB -- Least Significant Byte : octet de poids faible.

mA -- Milliampère

MHz -- Mégahertz

Microcontrôleur (*Microcontroller*) – Composant sur carte qui gère le fonctionnement et les communications d'un système spécifique sur la base de son firmware. Il peut également servir d'hôte pour l'intégration de modules OEM **iCLASS** dans d'autres équipements.

Mode Pass-thru (*Pass-thru Mode*) -- Etat dans lequel un lecteur/écriture peut répondre à des commandes de communication série (voir aussi Esclave).

Mode sécurisé (*Security Mode*) – Etat de fonctionnement du lecteur/écriture pendant lequel celui-ci recherche les informations sur le format de carte de l'application HID, puis les transmet sous forme de données Wiegand et/ou RS-232 (voir aussi Application de contrôle d'accès HID).

Module OEM (*OEM Module*) -- Module de lecture/écriture sous forme de carte de circuit imprimé destiné à être intégré à des produits d'autres fabricants. Fonctionne généralement en mode esclave.

Rédigé par : Nathan Cummings – Responsable Marketing

Mot de passe (*Password*) -- Champ de 64 bits réservé dans l'application HID (bloc 10) pour mémoriser le mot de passe (voir aussi Connexion sécurisée et Accès logique).

MSB -- Most Significant Byte : octet de poids fort.

NIST -- National Institute of Standards and Technology, fondé en 1901. Il s'agit d'une agence fédérale au sein de la Commerce Department's Technology Administration américaine. Elle n'a aucun pouvoir de réglementation, mais est chargée du développement et de la promotion des méthodes de test, des normes et de la technologie en vue d'augmenter la productivité, de faciliter le commerce et d'améliorer la qualité de vie.

Octet (*Byte*) – Huit bits.

OEM -- Original Equipment Manufacturer.

OTP -- One-time Programmable : programmable une seule fois. Champ fixe de 16 bits dans le bloc de configuration (octets 5 et 6), qui ne peut pas être actualisé. Son paramétrage par défaut est "FFFF". Chaque bit peut être mis une seule fois de un (1) à zéro (0).

Page (*Page*) -- Section de 2 kbits (256 octets) dans les cartes 16K/16. Il existe donc huit pages. Chaque page dispose de jusqu'à 2 secteurs d'application protégés par leur propre clé diversifiée de 64 bits. La capacité mémoire des données de lecture/écriture est de 208 octets au maximum.

PC -- Personal Computer : ordinateur personnel. Ordinateur de bureau ou ordinateur portable pouvant être connecté à tout lecteur/écriture **iCLASS** (voir aussi Contrôleur).

PCB -- Printed Circuit Board : carte de circuit imprimé

PDA -- Personal Digital Assistant : assistant numérique personnel. Processeur mobile généralement utilisé comme agenda. Lorsque vous lui ajouterez un module **iCLASS**, il deviendra un lecteur/écriture mobile.

Permuter (*Permute*) – Changer l'ordre ou la disposition.

PIN -- Personal Identification Number : numéro d'identification personnel. Autre moyen de vérification nécessitant un lecteur/clavier. Champ de 48 bits réservé dans l'application HID (bloc 9) pour mémoriser le code PIN.

Porte-clé (*Keyfob*) – Identifiant en plastique dur, conçu pour être accroché à un anneau ou suspendu à un clip de badge classique.

Programmeur (*Field Programmer*) – Produit **iCLASS** de HID permettant au client de programmer des cartes **iCLASS** avec des clés soit de sécurité standard, soit de haute sécurité. Grâce au Programmeur, le client pourra également réaliser le codage de l'Application HID, l'enregistrement et la mise à jour des numéros d'identification personnelle (PIN) et des mots de passe, l'enregistrement et la mise à jour des secteurs définis par l'utilisateur et la génération sur site de clés de haute sécurité.

Protocole série (*Serial Protocol*) -- Liste de commandes utilisées par les développeurs de logiciels pour communiquer avec les lecteurs/écriture et les cartes **iCLASS** (voir aussi DLL).

Réponse (*Response*) -- Résultat de l'algorithme d'authentification mutuelle utilisé par le lecteur pour authentifier la carte (voir aussi Authentification mutuelle).

RES (*RES*) -- Chaîne de caractères enregistrée de manière temporaire pendant le calcul du caractère de contrôle, lors du processus de génération de la clé.

RFU -- Reserved for Future Use : réservé pour une utilisation future.

RND -- Random Number : numéro aléatoire. Numéro aléatoire de 64 bits généré par le lecteur/écriture et utilisé lors du processus de génération de la clé.

RS-232 -- Protocole de communication série courant pour une distance de câble jusqu'à 45 m.

RS-485 -- Protocole de communication série courant pour une distance de câble jusqu'à 1219 m.

SDK -- Software Developers Kit. Ensemble complet d'outils permettant aux développeurs de logiciels d'intégrer aisément **iCLASS** à leur application. Il comprend généralement un lecteur/écriture, une alimentation, un câble pour interface série ainsi qu'un CD-ROM incluant un exemple d'application, le code source et la documentation.

Secteur d'application (*Application Area*) – Zone de mémoire dynamique à lecture/écriture.

Sniffer (*Sniffer*) -- Dispositif utilisé pour analyser, enregistrer et répéter des communications par radiofréquence. Des sociétés telles que IFR fabriquent des analyseurs de spectre capables d'analyser des fréquences comprises entre 9 kHz et 26,5 GHz (voir aussi Clonage et Attaque par répétition d'un enregistrement).

Sortie collecteur ouvert (*Open Collector Output*) -- Permet de commander tout dispositif fonctionnant par fermeture d'un contact. Celui-ci est utilisé dans les applications autres que le contrôle d'accès, lorsque le lecteur n'est pas équipé d'un relais. Il existe uniquement dans les lecteur/écriture.

Spécifique au site (*Site-specific*) -- Seules des cartes programmées pour un site spécifique peuvent fonctionner avec des lecteurs configurés pour ce même site (voir aussi Elite).

Tag (*Tag*) -- Identifiant adhésif pouvant être collé sur tout dispositif non métallique afin de le rendre compatible à **iCLASS** (voir aussi Carte).

Triple DES (*Triple-DES*) -- Algorithme de cryptage de blocs symétriques utilisant deux clés de 56 bits. Les mêmes clés sont utilisées pour le cryptage et le décryptage. La norme DES est documentée dans la norme NIST FIPS 46.

TTL – Transistor-Transistor-Logik. Communication série binaire dans laquelle le niveau logique haut (>2 V) = 1 et le niveau logique bas (<0,8 V) = 0.

UL – Underwriters Laboratory. Organisme indépendant à but non lucratif chargé du test et des certifications de sécurité.

VDC – Volts Direct Current : courant continu exprimé en Volts.

Vierge (*Blank*) – Carte n'ayant été ni configurée, ni programmée.

Wiegand (*Wiegand*) -- Protocole de transmission de données standard utilisé dans le contrôle d'accès, dans lequel deux conducteurs, un blanc et un vert, servent à envoyer des données binaires, respectivement des 1 et des 0. Le niveau normal d'un conducteur Wiegand est de +5 VDC. Lorsque la tension descend en-dessous +1,7 VDC, le bit est mis à 1. Lorsqu'elle dépasse de nouveau +2,8 VDC, le bit est remis à 0 et le conducteur reprend son état initial (voir aussi Impulsion Wiegand et Pause Wiegand).

XOR -- Table de vérité

Entrée		Sortie
0	0	0
0	1	1
1	0	1
1	1	0

Annexe A – Glossaire des clés

Clé (Key) -- Une clé correspond à un "mot de passe" destiné à protéger le contenu d'un secteur d'application spécifique sur la carte à puce sans contact. Toute carte possède une clé diversifiée, qu'il s'agisse d'une clé secrète que personne ne connaît ou d'une clé non sécurisée connue par de nombreuses personnes.

Clés enregistrées dans la carte :

- Clé 1 (Key 1)** -- Clé diversifiée résidant dans le bloc 3 de la carte destinée à protéger le premier secteur d'application de la page correspondante.
- Clé 2 (Key 2)** -- Clé diversifiée résidant dans le bloc 4 de la carte destinée à protéger le premier secteur d'application de la page correspondante.
- Clé de crédit (Credit Key)** -- Identique à la clé 2, elle est requise pour incrémenter le montant inscrit dans le champ enregistrement sécurisé (bloc 2).
- Clé de débit (Debit Key)** -- Identique à la clé 1, elle est requise pour décrémente le montant inscrit dans le champ enregistrement sécurisé (bloc 2).
- Clé diversifiée (Diversified key)** -- Toutes les clés enregistrées sur la carte sont diversifiées au moyen du numéro de série de la carte (CNS), afin de garantir l'unicité de chaque clé sur chaque carte.

Clés enregistrées dans le lecteur :

- Clé de sécurité standard (Standard Security Key)** -- Clé développée par HID et enregistrée dans tous les lecteurs et lecteur/écriture *iCLASS*. Elle garantit une compatibilité instantanée entre les lecteurs de sécurité standard et les cartes de sécurité standard.
- Clé d'échange (Exchange Key)** -- Vous devez connaître cette clé afin de pouvoir charger d'autres clés dans le lecteur. Cette clé est enregistrée dans la zone de mémoire 0 des clés.
- Clé haute sécurité actuelle (High Security Current Key)** -- Clé du mode haute sécurité destinée à protéger l'application HID. Vous pouvez la mettre à jour au moyen d'une carte de configuration spéciale. Celle-ci décale la clé actuelle dans la zone de mémoire de la clé précédente et met à jour la clé actuelle avec celle enregistrée dans la carte. Existe uniquement sur les cartes 16K.
- Clé haute sécurité précédente (High Security Previous Key)** -- Clé du mode haute sécurité destinée à protéger l'application HID. Elle est utilisée pour l'authentification mutuelle, si la clé actuelle fait défaut. Si l'authentification réussit avec la clé précédente, la clé actuelle sera mise à jour sur la carte. Existe uniquement sur les cartes 16K.
- Clés de cryptage (Encryption Keys)** -- Deux clés, enregistrées de manière sécurisée dans le lecteur, utilisées pour le cryptage de données DES ou triple DES dans l'application HID.
- Clés par défaut (Default Keys)** -- Durant la fabrication du lecteur, des clés par défaut sont affectées aux zones de mémoire prévues pour les clés 1 et 2. Ces clés par défaut correspondent à la clé 1 et à la clé 2 dans les cartes vierges (clé par défaut 1 = F0E1D2C3B4A59687 et clé par défaut 2 = 7665544332211000).
- Clés par défaut HID (HID Default Keys)** -- Clés "publiques" générées par HID pour protéger les secteurs d'application 2 à 16 sur toutes les cartes *iCLASS* configurées ou programmées. Ces clés sont mises à disposition de vos partenaires de développement logiciel, dans le document dénommé "Key Distribution".
- Zone de mémoire 0 à 11 des clés (Key locations 0 – 11)** -- Douze zones de mémoire dans le lecteur, dans lesquelles sont enregistrées les clés utilisées en mode Pass-Thru. Il s'agit des seules clés accessibles via le port série (à l'heure actuelle, seules les zones de mémoire 0 à 7 des clés sont accessibles).