

APPLICATION NOTE # 28 (Preliminary)

HID *iCLASS*™ Readers and Cards

HID *iCLASS* Readers, Reader/Writers and Contactless Smart Cards are compatible with existing access control systems, and through integrations by various Application Providers, will perform additional applications such as Biometrics, Time and Attendance, Digital Cash and Vending, HVAC Automation and Billing, IT Secure Authentication, Guard Tour, Parking, and Medical or Service Record Storage.

HID *iCLASS* readers transmit 13.56MHz RF energy to power and communicate with passive *iCLASS* contactless smart cards. The ISO 15693 standard allows a longer read range while still meeting FCC power output limits. *iCLASS* offers better security than comparable 13.56MHz technologies, such as MIFARE®¹, due to its larger authentication keys and stronger encryption. *iCLASS* uses 64-bit keys, compared with MIFARE's 48-bit keys, and *iCLASS* uses diversified keys and can encrypt stored data on the cards using DES or Triple DES, whereas MIFARE stores its keys and data "in the clear."

This document is an overview intended to familiarize Applications Providers, Consultants, Resellers and End Users with the capabilities of *iCLASS*. To implement a new application, a Software Development Kit and factory training and certification will be required.

iCLASS Readers

iCLASS readers are available in three colors: black, gray and white. They are also available in three different sizes for various applications, as described below. In addition to various modes of LED and Beeper operation, they have many other configurable options, which can be pre-set at the factory or modified in the field with special configuration cards available from HID Technical Support.

iCLASS reader products can be classified in three groups, read-only models, read/write models and OEM modules.

Read-Only Models (Wiegand Output)

- R10** – use on doorframes, mullions, limited space applications
- R30** – use on 80mm square European or Asian back boxes
- R40** – use on US j-boxes; also has Euro / Asian mounting holes

These readers feature a standard Wiegand interface for use with most access control systems. They can read HID Wiegand format data which is

¹ MIFARE is a registered trademark of Royal Philips Electronics, N.V.

factory-encoded on *iCLASS* cards, key fobs and tags, or they can read the CSN (Card Serial Number) from MIFARE® cards using Philips S50 or compatible ICs, converting it to Wiegand data.

Reader/Write Models (Wiegand + RS232)

RW300 - use on 80mm square European or Asian back boxes

RW400 - use on US J-boxes; also has Euro/Asian mounting holes

In addition to the Wiegand interface, these readers feature an RS-232 interface, for connection to a Host system (a PC or microcontroller). By using the *iCLASS* Serial Protocol, Application Providers can read, write or modify information stored in the application areas of the *iCLASS* card.

OEM Modules (Wiegand + RS232 or TTL)

OEM100 – for integration into third-party equipment with limited space and applications requiring Wiegand or TTL²

OEM300 - for integration into third party equipment with applications requiring Wiegand or RS-232

These modules consist of conformal-coated circuit boards, which can be integrated into the enclosures of other products such as biometric readers or time and attendance terminals. Both models feature a standard Wiegand interface. Additionally, the OEM100 features a bi-directional TTL interface, and the OEM 300 includes an RS232 interface. Both models support host-controlled read/write capability, and host control of the open-collector logic output. These circuit boards contain an integrated antenna, and LEDs (which can be de-populated). The speaker is available separately.

***iCLASS* Credentials**

These can be factory programmed with HID Corporate 1000 or any Wiegand formatted data for use with access control systems. Credentials are available with either 2K bits (256 bytes) or 16K (2K bytes) bits of memory, and the 16K bit version is available with either 2 or 16 Application Areas (see section on Card Memory Organization).

² TTL: Transistor-Transistor Logic, binary serial communications where logic high (>2V) = 1 and logic low <0.8V) = 0.

iCLASS contactless credentials can be classified in three categories: ID Cards, Key Fobs, and Tags.

***iCLASS* 200X – 204X – Card** These white, glossy, laminated PVC cards meet CR80 and ISO 7810 standards for size and thickness, and can be printed on both sides, using a dye-sublimation or thermal transfer card printer, or they may be custom printed by the factory. They can also be slot punched for vertical orientation only. The access control ID number may be ink-jet printed or laser engraved on the card. They are NOT embossable.

iCLASS cards are available with *iCLASS* technology only, or with multiple technologies allowing transition from (or use with) legacy systems, including magnetic stripe, contact chip, HID Proximity, and Wiegand (see How to Order Guide). *iCLASS* with Wiegand technology cannot be used simultaneously with contact chip or Proximity, and requires a thicker card (0.037" or 0.94mm).

***iCLASS* 205X – Key Fob** These rugged molded polycarbonate key fobs include a slot for use with most key rings or badge clips. The access control ID number may be ink jet printed on the tag.

***iCLASS* 206X – Tag** These thin, flat polycarbonate discs are 1.285" (32mm) in diameter, and 0.070" (1.78mm) thick, and have an industrial adhesive backing. The tags are non-removable (removal of the tag will destroy it). They can be affixed to non-metallic surfaces of PDA's, cellular phones, briefcases, and other personal items or assets. They can also be affixed to the back of existing ID or Access Control cards using other technologies such as Proximity, Wiegand, Barium Ferrite, or Magstripe, allowing transition to *iCLASS* technology without costly re-badging. The tags may not be compatible with all insert, swipe or motorized tractor-feed readers – it is strongly recommended to request a non-functional or functional sample tag to test the desired application.

MIFARE Cards

iCLASS Readers offer the additional capability of reading the Card Serial Number (CSN) only from the following types of MIFARE cards:

- HID Model 1430 MIFARE
- HID Model 1431 MIFARE with HID 125 kHz proximity
- Cards using Philips S50 or compatible Infineon Card IC
- Cards using Philips Mifare Pro IC
- Cards using Philips Mifare Lite

This capability is useful for applications where the customer already has a large MIFARE card population and wishes also to use the cards for access control. While a MIFARE reader such as the HID 6055B could also be used to accomplish this, the advantages to using the *iCLASS* reader are:

- Lower cost (*iCLASS* does not require the Philips decoding chip)
- Improved read range (by about 25%)
- Ability to read or transition to *iCLASS* technology

CSN Output Mode	Description	Comments
0	32 bit,	Outputs 32-bit CSN as Wiegand data (MSB first)
1	32-bit reverse (6055A)	Outputs 32-bit CSN as Wiegand data in reverse order (to match HID MIFARE reader model 6055A)
2	26 bit	Outputs 26-bit Wiegand data comprised of 16 lower bits of 32-bit CSN, fixed 8-bit facility code, and beginning and ending parity bits. Facility code defaults to 001, but can be changed with a configuration card.
3	34 bit	Outputs 32-bit CSN plus beginning and ending parity bits as Wiegand data
4	40 bit	Outputs 32-bit CSN plus 8-bit checksum as Wiegand data

Fig 1- MIFARE Card Serial Number Output Mode Options

The *iCLASS* reader can output the MIFARE card's 32-bit Card Serial Number (CSN) as Wiegand data in various formats (Figure 1), which are configurable from the factory (see the How To Order Guide) or in the field using configuration cards.

Other than the CSN, the *iCLASS* reader is NOT capable of reading any of the stored data on MIFARE Cards, and it cannot write to a MIFARE Card.

The *iCLASS* card's unique, random 64-bit CSN is used exclusively for anti-collision and key diversification. Unlike the MIFARE CSN, the HID *iCLASS* CSN is never transmitted by the reader as Wiegand data. This is primarily because most access control panels cannot accept 64-bit numbers, and also because the CSN is not secure.

The *iCLASS* reader is also capable of reading a mixed population of MIFARE and *iCLASS* Cards. The *iCLASS* reader will output the HID encoded data from the *iCLASS* cards, and will output the MIFARE CSN as configured. This may require that the access panel is capable of accepting Wiegand data in multiple formats. This capability is **not** available for cards and readers with Custom keys.

Hardware Interface

The *iCLASS* readers are equipped with an 18” shielded 22AWG wire pigtail, with wire colors and functions shown in Figure 2, below. OEM Modules provide solder pads with through-holes with the same connections.

Red	+DC (10-16 VDC)
Black	Ground
Green	Data 0
White	Data 1
Drain	**Shield Ground
Orange	*Green LED
Brown	*Red LED
Yellow	*Speaker
Blue	*Hold
Violet	***Open Collector
Gray	***RX (Serial Receive)
Red/Green	***DSR (Not Used)
Pink	***TX (Serial Transmit)
Red/Yellow	***DTR (Not Used)

* Optional Connections. ** Drain wire can be data return line when a separate power supply is used. *** Not used on R10, R30, R40

Figure 2 – *iCLASS* Wiring Connections

Tamper Switch

An internal magnet provides tamper indication when used with a magnetic reed switch connected to an external alarm system (except R10). Locate the switch behind the left side of the mounting plate, centered between the mounting holes (Figure 3). Recommended Magnetic switches are: Ademco 945T, Sentrol 1038T, GRI 100T or 110T or Aleph DC-2531. This does not apply to OEM Modules.

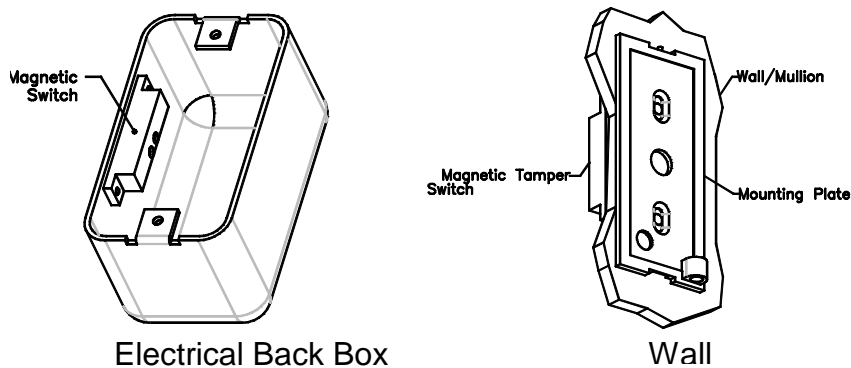


Figure 3 - Tamper Switch Mounting

Power

iCLASS readers require a 12 VDC linear power supply, and can operate over a range of 10-16VDC. As with all RFID readers, any noise on the DC input power would affect performance and read range. Switching supplies or transformers with rectifiers are not recommended.

Average power consumption (75mA) is higher than proximity. Peak power consumption (300-350 mA) is also higher due to the power required for the LED array behind the “light bar.”

Wiegand, LED, Speaker Connections

Wiegand connections are identical to HID proximity readers. Clock and Data output is not available. LED and speaker operation is configurable for internal or external control, single or dual line operation, with the LED normally green, red or off. The LED and speaker inputs are activated when asserted (grounded, or held to logic low, below 2.5VDC). The reader can be pre-ordered with the desired LED / Speaker configuration (see How to Order Guide).

Note that when the Wiegand cable is extremely long, it may be necessary to ground both ends of the cable shield (or earth-ground the reader and panel) to provide a common reference point for the reader and its power supply (or panel).

The speaker is capable of producing tones and tone sequences, and at a high or low level. This is configurable at the factory, or in the field, using configuration cards. The input is a logic control line, with the actual tone production controlled by the reader’s microprocessor. There are no external audio inputs.

Hold Input

The Hold Input is a control line which when asserted³ will turn off the RF transceiver circuit, until the line is released. This input can be connected to the contact or logic output of a vehicle loop detector, so that the card reader will not accept a card unless a vehicle is present. Alternatively, when this line is asserted, the reader will buffer one card read (ignoring subsequent reads) until the line is released. This can be selected with a configuration card.

Open Collector Output

This output is a normally open logic output controlled by a serial command via the RS232 or TTL input. (Not available on R10, R30, and R40 models.) This solid-state switch provides a means of controlling any device or logic input that

³ Assertion of a control line is accomplished by grounding, or “pulling” it to logic low with a transistor circuit.

can be operated by a switch closure, and is useful for non-access control applications, where a relay may not be available at the reader location. The output can be latched, unlatched, or momentarily latched for 1 – 255 seconds.

The open collector output can switch up to 50mA at 12VDC (13.8VDC max). For larger loads, an interposing relay must be used. A surge suppressor (MOV) should be installed across any inductive load attached to this output, to prevent transient pulses from damaging the reader.

Serial Inputs

The RW300/400 have serial RS-232 receive and transmit inputs for connection to a host system. There are no handshaking lines provided. The host serial cable ground can be connected to the reader's power ground input. The OEM100/TTL has two pins on the PCB which provide a TTL interface.

Operational Modes

The HID *iCLASS* Reader/Writers (RW400, RW300, OEM100 and OEM300) have two operational modes: **Security Mode** and **Host Mode**. The *iCLASS* readers (R10, R30, R40) operate only in Security Mode.

Security Mode - This mode is for use with an access control panel. The reader will output factory-programmed HID Corporate 1000 or any Wiegand formatted card data (or the Mifare 32-bit Card Serial Number) in Wiegand format (and/or optionally in hexadecimal format from the serial port). In this mode the reader operates under its own control when a card is presented. It will also respond to assertion of its LED, speaker and Hold control lines.

Security Mode operation can be implemented by traditional access control OEMs, integrators, and installers, by connecting the Wiegand outputs just as they would a standard proximity or Wiegand reader. Wiegand data is programmed into *iCLASS* cards at the factory or with a field programmer. Access Control dealers should obtain training and support from HID, to help customers to select the appropriate *iCLASS* cards and readers.

Host Mode – This mode is typically for non-access control applications. It allows developers and integrators to read or write to *iCLASS* cards. The actual application program (vending, debit, transit, etc) resides in the Host computer or microcontroller – it does not reside in the reader. The reader operates under the exclusive control of the Host device, responding to external commands received at the RS-232 or TTL port.

The host will control card reading, LED, speaker, open collector, and all read-write operations. The software or firmware must include a program

loop that causes the reader to periodically look for cards that have entered the RF field. The control lines for the LED, speaker and Hold functions will also continue to function in this mode.

iCLASS uses the ISO 7816-4 protocol, also the standard for contact Smart Card reader communications.

Host Mode operation can be implemented by Application Providers, who can obtain Software Developer Kits, training and support from HID.

ISO Standards

iCLASS readers can communicate with contactless smart cards using various ISO standards. These standards define the RF protocol used to communicate between the card and reader, and specify frequency, modulation depth and data rate. *iCLASS* readers are capable of using ISO 14443A (with MIFARE cards) or ISO 1443B2 and ISO 15693 with *iCLASS* Cards. The advantage of 14443A or 14443B2 is a faster data rate, but much of the read range is sacrificed. *iCLASS* readers typically use 15693, because the data rate is more than adequate for most applications, and because the longer read range is more convenient. (Also note that 2K cards can only communicate using ISO 15693).

iCLASS readers will automatically switch between 14443A and 15693, depending on whether a MIFARE or *iCLASS* card is presented. *iCLASS* readers can be set to only use ISO 14443B2 when communicating with *iCLASS* cards by using a configuration card. *iCLASS* reader/writers can be set to use ISO 14443B2 on a “per-command” basis, using the *iCLASS* serial protocol.

Note that capability of communicating in a particular ISO standard does not include proprietary encryption methods used by various chip manufacturers to protect data stored on the card. Each vendor, such as Philips or Infineon offers its own reader “chip set” which includes the proprietary decryption algorithms. Unless the reader has the required chip set, it cannot read the stored data on the card; it can only read the Card Serial Number.

Using *iCLASS* for Non-Access Control Applications

To use *iCLASS* Reader/Writers for non-access control applications such as biometrics, time and attendance, vending, etc., the Application Provider must write or adapt their application to use the *iCLASS* protocol. Once this is done, the Application Provider will have an integrated offering consisting either of an *iCLASS* reader connected to a PC or specialized terminal, or an *iCLASS* OEM module embedded inside a specialized terminal.

The Application Provider will also develop software or some other means of programming their application data into *iCLASS* cards, such as an enrollment

station in the case of biometrics, a cash acceptor or credit card terminal in the case of cashless vending applications, or a software program in the case of time and attendance applications. Most Application Providers can adapt their equipment to the *iCLASS* Reader/Writers' RS-232 interface.

Because *iCLASS* uses the ISO 7816-4 protocol, this integration will be relatively simple for Application Providers who have already integrated their applications with contact smart cards. At the time of the initial *iCLASS* product launch, several biometrics vendors had already completed successful integrations with *iCLASS*.

The *iCLASS* Software Developer's Kit contains a protocol document, programming guide, Dynamic Link Libraries (DLL's), an Active-X control, some example software, a sales demo program, and a reader with power supply and desktop stand. Note that the DLLs and Active X program require a Windows platform – low level protocol commands can be used for microcontrollers and non-Windows software platforms. These applications can be written in C or Assembly language.

End users may contact HID for a referral to one of its Application Providers who can provide a turnkey solution.

***iCLASS* Card Memory Organization**

There are three classifications for memory areas (Figure 4) on the *iCLASS* cards:

- 1 - Manufacturing/Configuration Area
- 2 - Area 1 (HID Area)
- 3 - Areas 2 - 16 (Application Providers)

Manufacturer/Configuration Area

The manufacturer/configuration data area of each card (Figure 4) is 6 blocks long (48 bytes) and includes:

- Card Serial Number (64 bit unique number)
- Configuration Data, Application Area Limit
- Secure Stored Value Area (not used)
- Authentication Keys for Area 1, Area 2
- Application Issuer Area

Application Areas

iCLASS cards and tags are available in various configurations. Depending on the model of card ordered, *iCLASS* cards might have either two or sixteen application areas. In Figure 5, "Available Memory" indicates memory not already used for the Manufacturing/Configuration Areas or for Application Area 1 (HID).

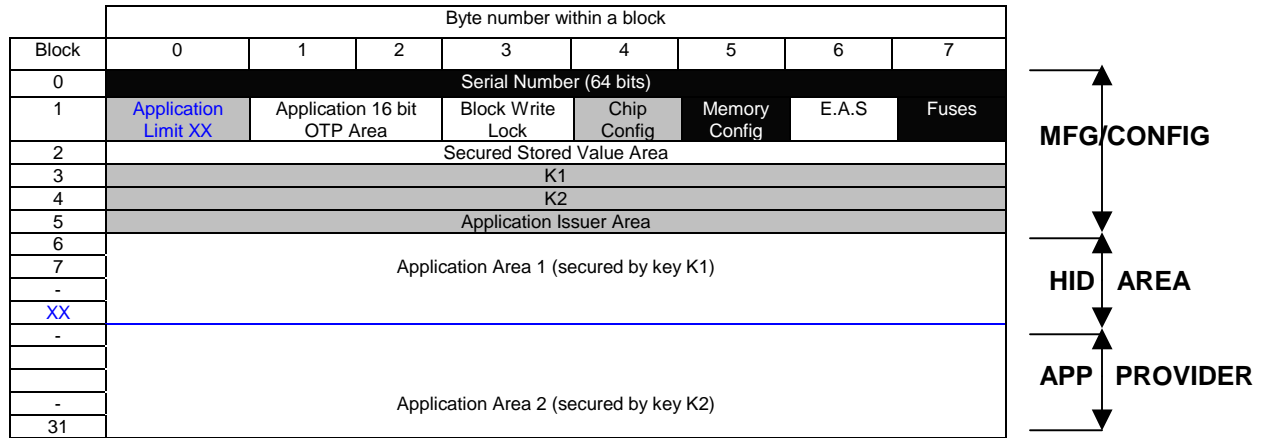


Figure 4 - Memory Mapping for the *iCLASS* 2K (or one pair of Areas on the 16K/16)

Card Type	Application Areas	Total Card Memory	Available Areas	Available Memory
2K/2	2	2k bits (256 bytes)	1	104 bytes
16K/2	2	16k bits (2048 bytes)	1	1888 bytes
16K/16	16	16k bits (2048 bytes)	15	1560 bytes

Figure 5 – Available Memory for Various Card Types

Application Area 1

Application Area 1 is 13 blocks or 104 bytes (Figure 6), and is always reserved for the HID application which includes the following data:

- Directory
- Access Control ID (Wiegand format data)
- PIN (future)
- Password (future)
- APB Status (future)
- Area Control (future)
- User fields 1 – 4 (16 bytes, each)

Block	Data	
6	HID Application Directory	HID Extended Application Directory
7	HID Access Control ID	
8	HID Access Control ID	
9	HID AccessControl ID	PIN
10	Password	
-	RFU	
18	RFU	

Figure 6 - *iCLASS* Memory Organization for the HID Application Area 1

Application Area 2

This area is for user applications, and is fixed in length.

- On 2K/2 cards it is 13 blocks, 104 bytes, which can contain stored value applications (Figure 4).
-
- On 16K/2 cards it is 236 blocks or 1888 bytes, which can contain large stored value applications, such as biometric templates, medical history or service records (Figure 7). Multiple applications could be stored in a single area, but each Application Provider must be careful not to overwrite others, and all must share the same Authentication Key.

Block	Byte number within a block							
	0	1	2	3	4	5	6	7
0	Serial Number (64 bits)							
1	Application Limit XX	Application 16 bit OTP Area	Block Write Lock	Chip Config	Memory Config	E.A.S	Fuses	
2	Secured Stored Value Area							
3	K1							
4	K2							
5	Application Issuer Area							
6	Application 1 (secured by key K1)							
7								
-								
XX	Application 2 (secured by key K2)							
-								
-								
255								

Figure 7- Memory Mapping for the *iCLASS* 16K/2

Multi-Application Card

The 16K/16 card has 16 Application Areas (Figure 8). They are arranged in 8 pages, with each page consisting of one Manufacturing and two Application Areas formatted similarly to the 2K/2 card (Figure 4). The 6-block manufacturing area exists on all 8 pages, but the card serial number from Page 1 is used for all key diversification. The manufacturing area on each page stores the appropriate keys for its own Application Areas.

On Page 1, Area 1 is reserved for the HID Application, and Area 2 is fixed, just as on the 2K/2 and 16K/2 cards. On Pages 2 – 8, Areas 3 -16 are available for user applications, and the boundary between each pair of Application Areas (3&4, 5&6, etc) can be set one time during programming.

The Application Providers can write data for each application in individual Areas, or they can distribute larger records (such as biometric templates) across multiple Areas, in which case, each area must be individually authenticated by the reader to extract the entire record. When using multiple Areas, it is advisable

to set the application boundary at 31 blocks for each pair of Application Areas so that first area is maximized (208 bytes) and the other is zero (Figure 4). This will reduce the number of authentications required to read data is stored in multiple areas.

For most biometric templates, the 16K/16 card will still have available Application Areas after the template has been stored. Figure 8, below, shows how a biometric template might be stored on 16K/2 vs 16K/16 cards.

16K/2 Card		16K/16 Card		
AREA	CONTENT	PAGE	AREA	CONTENT
1	HID Application	1 {	1	HID Application
2	Biometric Application		2 {	2
		3 {		3
			4 {	4
		5 {		5
6 {	6			
	7 {	7		
8 {		8		
	5 {	9	Vending	
6 {		10	Parking	
	7 {	11	Debit	
8 {		12	Library	
	7 {	13	Logical Access	
8 {		14	HVAC	
	8 {	15	Personnel Info	
8 {		16	Personnel Info	

(unused)	↑	↓
----------	---	---

Figure 8 – Storing Applications on 16K2 and 16K2 Cards

Secure Storage Area (Credit/Debit Application)

While this feature is not available on the 2K or 16K/2 cards, it may be used on Pages 2-8 of the 16K/16 card. The Secure Stored Value area allows “purses” to be defined on the *iCLASS* card for vending, transit, or other digital cash applications. Note that when using this feature in a particular Page, the first key acts as a debit key, and the second acts as a credit key. Since these keys are also used to secure the first and second application areas for that page, it is not advisable to use those areas for unrelated applications. However, those areas could be used for storing relevant data, such as account number, currency, units, credit line, account balance and maximum purchase allowed.

Factory Default Programming

Initially, all cards will be pre-programmed by HID Manufacturing. In Q4 2002 a field programmer will be available. The factory default programming is described as follows:

- **Serial Number:** Block 0 is the 8-Byte unique ID for the chip. The Serial Number cannot be changed by the user (ISO standard).
- **Application Limit:** This Byte will be set to the value 18 (0x12), setting the application limit below block 18. The HID application will always reside in Application area 1. Application Area 1 (HID App) consists of 13 blocks. For the 16K/16 card, the HID Application will always reside in Application Area 1 in the first pair of Application Areas. Application limits for Areas 3-16 of the 16K/16 card can be changed once by the Application Provider.
- **Application 16 bit OTP (one time programmable) Area:** Unused
- **Block Write Lock:** Unused - Default value 0xFF
- **Chip Config:** Used to distinguish between a 2K and a 16K card.
- **Memory Config:** Used to distinguish between a 16K/16 and a 16K/2 card
- **E.A.S:** Unused
- **Fuses:** if these are “blown” the authentication keys cannot be changed in the field.
- **Secured Stored Value Area:** Unused (Available on pages 2-8 of 16K/16 card)
- **K1, K2:** K1 and K2 are diversified from HID Standard master keys. In the case of the 16K/16 the 14 remaining keys will also be programmed to default values also diversified from the HID Standard. Each of the keys will be different. HID will allow third parties to use various application areas by divulging the corresponding default keys to them.

In the case of the 2K card, once these keys are programmed at the factory, they cannot be changed later. In the 16K/2 and 16K/16 cards, these can be changed in the field, as long as the fuses are not blown.

- **Application 1:** Reserved for the HID Application
- **Application 2:** (and 3-16 on multiapplication cards) Reserved for Application Providers
- **HID Application Directory:** Defines the length and format of the HID Access Control ID, the size of the PIN. Indicates if PIN and ID are encrypted and if so with what key and what encryption scheme (DES or triple-DES).
- **HID Extended Application Directory:** Used to define the format of the Password and the rest of the Application area.
- **HID Access Control ID:** ID used for the HID access control Application (to be output via Wiegand or RS-232). Its maximum length is 144 bits.
- **PIN:** 48-bit PIN reserved for the HID Access Control Application (future)
- **Password:** 64-bit number which can be written and read by the programmer (future)
- **RFU:** memory area reserved for future use.

iCLASS Security

Mutual Authentication

Mutual authentication is a common practice in key-based encrypted communications. Simply put, the card and the reader each need to make sure that the other has matching keys, so that the reader "knows" that the cardholder is legitimate, and so the card "knows" that the reader is authorized to read its information.

If the card and the reader simply transmitted the keys to each other for comparison, anyone with technical skills and a receiver tuned to the reader's frequency could capture the information, and make his own smart card to obtain access.

For this reason, the card and reader each contain complex cryptographic algorithms, which can scramble the transmitted data so that it is unintelligible. (An algorithm is a mathematical formula used to encrypt numbers.) To prevent "hackers" from reverse-engineering the algorithm, the card and reader also have random number generators, and each one factors a random number into the algorithm, so that if you were to read the same card multiple times, the data transmitted would be different every time. Each card contains a unique serial number, which is used to encrypt the key that is stored on the card, making the key appear to be unique.

When selected by the reader, the card begins by sending its card serial number (CSN) "in the clear." In the event that multiple cards are presented, the reader uses these ID numbers to silence other cards and select one card to transmit. This process is called anti-collision. (This also explains why *iCLASS* never uses the serial number for access control – the serial number is not encrypted.)

At this point, assuming the reader and the card are both legitimate, they now have some information in common. Both "know" the card serial number, both have the encryption algorithm, and both have the key (the reader has the actual key, the card's is diversified from the CSN).

The reader uses the CSN, Key, random number and algorithm to calculate a 64-bit number. However, it only sends the first 32 bits, called a Challenge. The Card receives the 32-bit Challenge number, and it uses the number, the algorithm, CSN and key to recreate the last 32 bits of the 64-bit number, called a Response, and sends it back to the reader. The reader compares the response from the card to the response it has stored in memory and if they match, it authenticates the card. The Card then reverses the process by sending a Challenge to the reader, which sends a Response back to the Card.

Once Mutual Authentication has occurred, then the card and reader can begin to transmit data, and the reader can read or write to the sector of the card that has been authenticated.

Data Encryption

The data stored on the card in the HID Application Area can be encrypted with DES or triple DES, so that even in the highly unlikely event that the keys were “broken,” the data would still be unreadable.

Authentication Keys

All data stored on *iCLASS* cards is secured by Authentication Keys. A Key is basically a password used to protect data from being read or changed without authorization. The *iCLASS* cards and readers use 64-bit keys. One key is used to protect each of the card’s Application Areas.

HID encodes Wiegand formatted card data into Application Area 1 of the *iCLASS* card and protects the data with a unique, diversified HID proprietary key, which is not published. A compatible key is also securely stored in each HID *iCLASS* reader.

Because each Application Area has its own key, an *iCLASS* card can be used to store information from multiple Application Providers, and each Application Provider would be prevented from modifying the other provider’s data accidentally or otherwise. Application Providers are advised to change the keys for their areas from the default, and they are responsible for their own key management and data encryption.

iCLASS Application Providers must use diversified keys to protect the Applications Areas that they will use. The *iCLASS* reader/writer makes this easy by performing the key diversification function.

The *iCLASS* reader can store up to 8 Authentication Keys. Even if more than 8 keys are in use at a particular site, a reader will only need to store the keys used for its particular application. New keys can be loaded on-the-fly when necessary.

Key Management

The basics principles of key management are:

- Keys must be unique per card, and per customer.
- Keys must be securely stored and encrypted
- Keys must never be transmitted “in the clear” via RF or RS232
- Keys must never be readable from an unprotected hard drive or memory chip

When Standard Key Management is used, the keys used to protect Application Area 1 on all cards are diversified from the HID Standard Master Key, using an encryption algorithm, the unique card serial number, and the Area Number, such that keys on each card and in each Application Area are unique. The same Standard Master Key is securely stored in the reader, and is never transmitted. Because one Master key is used to create keys for all cards and readers, *iCLASS* readers with Standard keys are interchangeable and compatible with one another. Because of the encryption and mutual authentication used in *iCLASS* readers, this key is extremely secure.

HID Custom Keys add an additional layer of security to the basic *iCLASS* key diversification and encryption scheme. A site-specific Custom Key is assigned by HID to each customer, replacing the Standard Key. For the HID Application Area, HID's key management system uses a proprietary algorithm to generate a 256 key matrix from the Custom Master key. The CSN is used to extract bytes from 8 different locations in the key matrix to create 64-bit keys.

On all cards at Custom Key sites, HID secures Application Area 1 with keys diversified from the Custom Key, and then keys all readers to match. The Custom Key and key database resides in each reader. HID maintains Custom Keys in an encrypted database, which is stored at the factory in a secure location, and a backup copy is stored in a secure offsite location. Because a site specific Master key is used to key all cards and readers, Custom-keyed cards and readers are not interchangeable with cards or readers from another site, and additional cards and readers must be ordered with the same key ID number.

In Q4, 2002, HID will offer an *iCLASS* card programmer, which is a special version of the reader that connects to a PC, running Windows software (similar to the HID ProxProgrammer). The programmer will allow end users or system integrators to create and secure their own Custom Keys on-site, and will also allow personalization data to be encoded and encrypted into designated data fields in the HID Application Area of each card. Note that 16K/2 or 16K/16 cards are required. The end user or system integrator assumes full responsibility for system security when they purchase their own programmer.

For more information on key management see the document, "*iCLASS* Security Implementation Plan"