



# COLORID WHITE PAPER

## Migration and Conversion to HID iCLASS Cards

**Prepared by:** David Stallsmith

[david@colorid.com](mailto:david@colorid.com)

704-897-1156 (phone)

704-987-2240 (fax)

**Paper #:** TTX5360\_ Migration and Conversion to HID  
iCLASS Cards

[www.colorid.com](http://www.colorid.com)

## PURPOSE OF PAPER

At ColorID we are frequently asked by universities if they should consider moving to HID iCLASS cards from their current Magnetic Stripe or HID Proximity card systems. Though a straightforward question, the answer is not always so simple. Often it depends on multiple factors, such as your current investment in cards and infrastructure. In some situations, the move to iCLASS may not be financially justifiable, but in many cases there is no extra cost to either move directly to iCLASS or to at least start a migration to iCLASS that will give your university more options in the future. This white paper was created by ColorID in an attempt to address some of these concerns in a Frequently Asked Questions format. After you have reviewed this document, you may have additional questions. We encourage you to contact us at ColorID to further explore your options.

## FREQUENTY ASKED QUESTIONS

### 1. What is iCLASS?

After nearly 20 years of success with access control systems based on Proximity technology, HID introduced iCLASS in 2002. iCLASS, known as a “contactless smart card,” looks and functions like a Prox card for physical access. Both iCLASS and Prox cards are designed specifically for access control applications. Each card has some kind of unique facility code and card number. However, iCLASS offers two additional benefits:

- 1) Much more memory built in to the chip in the card;
- 2) Much better security.

In addition to the portion of memory which stores the access control data for opening doors, iCLASS cards have 2k or 32k of available, usable memory. This memory is part of the contactless iCLASS chip which is built into the card and it can store data in much the same way as a memory card for a digital camera does. iCLASS card readers can read and, optionally, write to this available memory space on the iCLASS card. iCLASS technology also provides a method for securely reading from, or writing to this memory, so it cannot be accessed by unauthorized users or applications. The power of iCLASS technology enables the simple form of a “Prox card” to have secure memory embedded inside it. This concept opens possibilities for dozens of applications that can take advantage of this memory in the future without having to make any changes to the iCLASS cards themselves. The applications could be as simple as storing additional ID numbers in the memory on the card, e.g., those that do not fit on your current magnetic stripe or Prox format, or as sophisticated as

storing a biometric description of your iris. The important concept is that the specific application does not reside in the iCLASS card and one or more applications can be added later with no change to the iCLASS cards that are being issued today.

The second major advantage of an iCLASS card is that it is much more secure than a Magnetic Stripe or Prox card.

## 2. Why would we want to use iCLASS cards at our University?

- **Security** - iCLASS technology provides much greater security than Prox cards, magnetic stripe cards or key systems.
- **Applications** – The embedded memory inside the iCLASS card provides opportunities for many additional uses of the cards, beyond just securing and opening doors.
- **Cost** – Base model iCLASS cards and readers cost no more than Prox cards and readers.

## 3. What is the difference between iCLASS and HID Prox?

### ***How iCLASS is like Prox:***

- Both technologies involve the reading of internal numbers from the card (Facility Code and ID), when it is presented to a reader.
- Both can use the same card number formats (26 bit, Corporate 1000, many others).
- From the perspective of the Access Control System, the data transmissions from the back of iCLASS readers and Prox card readers look the same. This means that your control panel cannot tell the difference between a Corporate 1000 Prox card and a Corporate 1000 iCLASS card, if the Facility Code and Card ID Number are the same in both cards.
- 2k iCLASS cards and readers cost no more than Prox cards and readers.

### ***How iCLASS is different than Prox:***

- iCLASS and Prox each use different radio frequencies to communicate between the card and the reader. Prox uses 125 KHz (12,500 cycles per second) and iCLASS uses 13.56 MHz (13.65 million cycles per second). A Prox card reader cannot read an iCLASS card and an iCLASS reader cannot read a Prox card, unless you are using an HID *multiCLASS* reader, which is able to read cards at both frequencies.

- iCLASS provides much better security between the card and reader. Prox cards are vulnerable to sniffing (reading the data transmission in the air) and fraudulent duplication. These are nearly impossible with iCLASS cards.
- iCLASS cards have additional, user-specific memory, currently available in 2k and 32k bits, which can be used for many different applications.
- Prox will continue to only open doors, while iCLASS, with its security and memory, will open possibilities for additional future uses.

#### 4. What iCLASS-specific applications are available today?

- **Point-of-Sale** -- *ViVOpay* is an adapter for **POS** terminals, which enables them to read iCLASS cards -- made by *ViVOtech*.
- **Vending, parking, laundry, photocopying, printing** -- *QiWave*, by QI Systems, is a cashless payment device for iCLASS Cards which can be easily fitted to almost all unattended point-of-sale and vending machines. It can be used in online or offline mode.
- **Food service** -- *FreedomPay* is a turnkey, customizable cashless payment program, based on iCLASS.
- **Logical access** -- There are a number of applications that enable the use of iCLASS cards to logon to Windows, websites, and applications on your PC. A contact smart chip can be added to the card, for strong authentication using PKI.
- **Mobile** -- The *DSVII-SC* is a handheld mobile device by Datastrip, specifically designed to provide identity verification by reading iCLASS and other smart cards. It has a 500 DPI fingerprint sensor for instant matching to a biometric templates, and supports wireless communication with a server. There are also other mobile devices that can read iCLASS cards, for offline verification and recording of attendance at events.
- **Biometrics** -- There are many biometric access control devices that are designed to work with iCLASS Cards, made by companies such as *Bioscrypt* (Fingerprint), *LG Electronics* (Iris) and *Ingersoll-Rand* (Hand Geometry). In many cases, the biometric template is stored only on the card and never in a database.

#### 5. We are interested in the advantages of using iCLASS technology on our campus, but we have a Prox Access Control System. How could we migrate to iCLASS?

This is an important question for a university, with significant financial ramifications. Let's consider 3 different situations:

*1) Prox Cards are used by a few of the executives, to gain access to a small number of important doors. The rest of the cardholders are using Magnetic Stripe cards for door access. We also use Magnetic Stripes for all of our POS transactions and meals.*

iCLASS cards are available with magnetic stripes, so that they can be used with any existing Magnetic Stripe system. For door access, it may make sense to remove the Prox readers and replace them with iCLASS readers. The access control system will usually not know the difference. Cardholders could be issued iCLASS cards with the same numbers as their former Prox cards or with new ID numbers. As more doors are secured with iCLASS readers, Magnetic Stripe cards could be replaced with iCLASS cards with Magnetic Stripes.

*2) Prox cards are used by a significant number of our cardholders and about half of our doors are secured by Prox readers.*

In order to migrate to a system which uses only iCLASS for physical access, HID offers Multi-Technology (Prox and iCLASS) cards and readers. The RP40 Multi-Technology reader costs only slightly more than a Prox reader and can be used for new installations with little impact. For existing doors with Prox readers, it may make sense to issue cards containing both Prox and iCLASS technology, for a period of time, until all the readers can be replaced with iCLASS readers. Some Universities have decided to issue multi-technology Prox/iCLASS cards to all their cardholders.

*3) Prox cards and readers are used by our entire university, but we would like to convert to iCLASS.*

While this situation could be addressed with a combination of Multi-Technology cards and readers, it is likely that a replacement of all cards and readers with iCLASS cards and readers would be the most cost effective.

## **6. We use Mag Stripe cards for opening doors and for transactions. Can we convert to iCLASS?**

This may be a very good time to move to iCLASS. Magnetic Stripe readers at doors can usually be replaced easily with iCLASS readers. Issuing new iCLASS cards with Magnetic Stripes offers the following advantages:

- iCLASS cards, with their contactless interface, verify quickly at doors and do not cause wear and tear on the readers.
- Mag Stripe cards have virtually no inherent security – iCLASS has superb security.
- The Application Areas in the memory of an iCLASS card can be individually protected by unique keys, allowing far more uses than those available for magnetic stripes. For example, the data encoded and read for library usage can be isolated from that used by the dormitory system. The keys to protect each area are transparent to the user.

## 7. How does iCLASS work?

### **The Card - Reader Interface – Mutual Authentication and Encryption**

When an iCLASS card is placed within 1” to 4” inches of an iCLASS Reader, the radio signal (13.56 MHz) transmitted by the reader powers up the chip on the card. This initiates the process of Mutual Authentication, because the reader needs to make sure that the card is legitimate, and the card needs to “know” that the reader is authorized to read its information.

Each iCLASS card has a 64 bit security key, which is stored in encrypted form on the card at the time the card is programmed. This key, called a Diversified Key, is formed by using an algorithm to combine each card’s unique Card Serial Number with a secret key provided by HID. The Diversified Key is stored on the card, but not the secret key. The reader, which contains the secret key, sends out a signal that is received by a card entering its field, which then sends its Card Serial Number to the reader. The reader uses the Card Serial Number and the secret key to form a Diversified Key which is the same as the one stored on the card. The reader then sends out a 64 bit random number and the card sends a 16 bit random number as a challenge and response. The card and reader each use the Diversified Key and the random numbers in a Hash algorithm and each should obtain the same result. When each has compared the results and verified the other, the HID Access Control data can be extracted by the reader, converted to Wiegand protocol and sent to the Access Control system.

All of this takes place in a fraction of a second and is invisible to the user. All data on the card is stored in encrypted form. If the card and reader simply transmitted the keys to each other for comparison, anyone with technical skills and a reader could capture the information

and make their own smart card to obtain access. Therefore, iClass cards and readers contain complex cryptographic algorithms which can scramble the transmitted data and make it unintelligible. The process uses random number generators, so that each time the card is read the data is transmitted differently.

### **Application Keys and Elite Custom Keys Program**

Each application area on the iCLASS card can be protected by a unique diversified key. Applications written for iCLASS cards use the default secret key for authentication, and then replace it with their own unique secret keys, in the cards and readers. For even greater security, HID provides the Elite program (this is similar to the Corporate 1000 program for Prox), which issues and manages unique keys for a university's cards and readers. Card data may also be protected with DES or triple DES encryption.

### **Readers**

iCLASS readers are designed to be installed in the same manner as Prox and mag stripe readers. They use Wiegand protocol output, which is the industry standard for access control wiring and card data transmission to the access control panel. This means that when a Prox or mag stripe reader is removed from the wall, the new iCLASS reader will, in most cases, connect in the same manner and interface with the system without any additional adjustments. The same access control format that was used previously can be programmed into the new iCLASS cards. Some features of the reader's operation can be adjusted at any time with the use of special programming cards. R10 and R40 readers are very similar in size to their predecessors, the MiniProx and the ProxPro, respectively.

In order to write data to iCLASS cards, read-write "readers" should be used. (In the world of smart cards, *readers*, *writers*, *encoders* and *scanners* are all referred to as "readers"). These are designated by the "RW" prefix. Most of the applications named above require read and write functions. At a door or entryway, the RW400 would be the appropriate reader. For interior applications which are running on a PC with a USB or serial interface, AirID readers and writers provide a compact, powerful and easy-to-use solution. They can be used to read access control numbers from the cards and enter them into a database, and they can read and write to the application areas of the cards.

HID recently introduced the multiCLASS RP40 reader. It contains two separate antennae and chipsets, one which reads Prox cards in the

125 KHz range and one which reads iCLASS cards in the 13.56 MHz range. Whichever type of card is presented, the reader reads the card data and outputs it to the system in the same manner, regardless of technology.

Another exciting introduction by HID is a new line of IP-based readers known as EDGE. These connect to the network and are powered over ethernet. They can be controlled through a web browser instead of a control panel. Each EDGE reader stores up to 44,000 credential records with 65,000 schedules and will buffer up to 5000 transactions, in the event of a communication disruption. Edge readers are available for iCLASS and Prox card populations.

In addition to reading the data from iCLASS cards, iCLASS Readers can also read data from cards compliant with the following standards:

- ISO 15693 - read/write; 2kbits (256 Bytes) and 16kbits (2K Bytes)
- ISO 14443, Type A - read only; MIFARE® (card serial number)
- ISO 14443, Type B2 - read/write; 16kbits (2kBytes)

## **ADDITIONAL READING MATERIAL**

Additional materials are available on the HID Website:

Frequently Asked Questions and Answers for iCLASS  
[http://www.hidcorp.com/page.php?page\\_id=24](http://www.hidcorp.com/page.php?page_id=24)

Online Training:  
<http://www.hidtraining.com/>

iCLASS Introduction white paper:  
[http://www.hidcorp.com/pdfs/products/introducing\\_iclass.pdf](http://www.hidcorp.com/pdfs/products/introducing_iclass.pdf)

iCLASS Glossary of Terms:  
[http://www.hidcorp.com/pdfs/iclass\\_glossary.pdf](http://www.hidcorp.com/pdfs/iclass_glossary.pdf)

Listing of available documentation:  
[http://www.hidcorp.com/page.php?page\\_id=27](http://www.hidcorp.com/page.php?page_id=27)

The EDGE Readers Home Page:  
<http://www.hidcorp.com/edge/edgehome.php>