# How an HID Card is "Read"

The purpose of this paper is to briefly explain the nature of the data on an HID card and the steps required to get that data to the controller and unlock a door. This information applies to both 125 kHz Prox cards and to 13.56 MHz iCLASS® cards.

## Four Elements of a Card Access System

Any card access system will consist of four basic elements. Depending on the size and purpose of the system, there may be many additional types of devices however the four basic elements are:

1. Cards
2. Readers (possibly equipped with keypads)
3. Access control panels (controllers)
4. An operator interface or "Host" PC

Let's look at these individually and determine their place in the access control system. We will use the scenario of an individual carrying a card and wanting to be granted access.

## The Card

Any access card simply carries a set of binary numbers (ones and zeros) that are used to identify the cardholder. HID makes cards that are capable of carrying this kind of binary data including:

- Magnetic Stripe
- Wiegand (swipe)
- 125 kHz Prox
- MIFARE™ contactless smart cards
- 13.56 MHz iCLASS contactless smart cards

NOTE: HID makes many cards that combine two or more of the above technologies on a single card. Most notable is the 13.56 MHz iCLASS/125 kHz Prox/Magnetic stripe combination.

There are special characteristics of both MIFARE and iCLASS cards and readers that will be briefly addressed at the end of this document.

The means of encoding data on the card and conveying the data to the reader varies according to the technology involved. In every case, however, the data on the card is a string of binary numbers of some fixed configuration and length.

- In the vast majority of cases, the data on the card is comprised only of the "format" that will eventually be received by the controller.
- In extremely rare cases, an additional code will be carried on the card that is linked to a specific group of readers. This ID code will be stripped off by the reader and only the format sent to the controller.

The card itself has no awareness of the makeup of its format, nor is it aware of any access privileges for the cardholder. That information exists only at the controller, and possibly the host (if present).

## The Reader

HID makes readers that are compatible with each of the five types of cards listed above. In every case, each reader can only talk to its corresponding card type since each of the technologies is unique.

NOTE: HID makes a combination Magnetic Stripe and 125 kHz Prox reader intended for transition applications.
Each type of reader uses its own technology to read the data from the card. All of the readers are able to convert that data to the "Wiegand Protocol" for transmission to the controller. (Some readers can also communicate to the controller by other means such as RS232 or Clock & Data.)

- All standard readers using any listed technology simply convert the binary card data to Wiegand (or other) Protocol and send it without changes to the controller.
- Certain proprietary readers will receive the site-specific ID code from matching proprietary cards. Those readers will strip away the ID code and send only the remaining binary data to their controller.

The reader itself has no awareness of the makeup of the card data format, nor is it aware of any access privileges for the cardholder. That information exists only at the controller, and possibly the host (if present).

## The Access Control Panel (Controller)

When the controller receives the data from the reader, its software begins the process of deciding whether or not to grant access. This is usually done in several stages.

- Does the length of the data format match what the controller is expecting? Some controllers are designed to only accept a certain length of data (34 bits for example.) If the data from the card is too long or too short, the controller may ignore it completely. Other controllers may have a special "access denied" for a non-matching format length.
- Does the format structure make sense to the controller? If the length is acceptable, the controller then breaks the binary string down into its component parts. These might include:
    - o Facility Code
    - o Site Code
    - o Card Number
- Does the Facility Code match? The controller will examine the data to determine if the Facility Code portion matches the one that has been programmed into the controller. Some controllers can support many different Facility Codes, possibly even multiple formats. If the Facility Code doesn't match, access will be denied and a log message generated.
- Does the Site Code match? If the format contains a Site Code or other secondary identifier, it will be handled just like the Facility Code above.
- Is the Card Number within the allotted range? If yes, the decision process will continue. If no, access will be denied and a log is generated.
- Is the Card Number in memory? If yes, the process continues. If no, access is denied and a "card not in memory" log is generated.
- Is the card valid at the reader at this day and time? If yes, access will be granted and the lock relay will be activated. If no, a log message will be generated that will identify the reason for denial.

The controller is the only device in the system where the binary card data format can be decoded and acted upon. Only the controller (and possibly, the host) is aware of the makeup of the format and whether the received data makes sense. Different brands of controllers react in many ways to incorrect card data formats. Some have a log message for every conceivable type of "access denied." Simple controllers may have only one generic log. Still others might completely ignore an incompatible format and give no reaction at all.

You must understand your controller's capabilities to fully debug any apparent problem with card and reader performance.

## User Interface (Host software)

Every access control system has some form of terminal or PC program for operators to use. This is where an operator or administrator can:

- Add and delete cardholders
- Assign, modify or delete access privileges
- Create and modify time schedules, holiday lists, etc.
- Configure system hardware for doors, alarm points, etc.
- Monitor system events in real time
- Generate historical reports on all types of system activity

Only in extremely rare cases in large, complex systems does the host ever make access decisions. In 99.9% of the existing systems, that task is always performed by the controller.

## iCLASS and MIFARE Authentication

Both iCLASS and MIFARE are "contactless smart cards" by definition. When either of the cards is read in their normal functional mode, there is an additional security step. The reader and the card go through a complex mathematic process where they compare security keys carried within both the card and reader. This process is called Mutual Authentication. It ensures that the communication between the card and reader can never be copied and repeated back to the reader.
If the key in the reader matches the key in the card, then the reader will extract the binary data format from the card and send it on to the controller. If the keys DO NOT match, the mutual authentication process is terminated and the reader shows no reaction at all.