APPLICATION NOTE # 25

Using the Model 6055B HID MIFARE Reader

The Model 6055B HID MIFARE Reader is a multi-purpose contactless card reader/writer, with both Wiegand and RS232 ports, as well as external control lines for LED and Beeper control.

Compatible Cards

The 6055B is designed for use with the following MIFARE contactless smart cards:

HID Model 1430 with Philips S50 Standard card IC.
HID Model 1431 with 125 kHz proximity and Philips S50 Standard card IC.
Cards using Philips S50 or compatible Infineon Card IC
Card using Philips Mifare Pro IC, emulating the S50 in contactless mode
Card using Philips Mifare Lite (reads Card Serial Number only)

These cards operate at 13.56 MHz and meet the ISO 14443-A standard for contactless smart cards.

Operational Modes

The 6055B HID MIFARE Reader has two operational modes**:**

Security Mode - Wiegand reader function. The reader defaults to this mode, intended for use with an access control panel. The reader will output OEM card data or the Mifare 32-bit Card Serial Number in Wiegand format. This data is also transmitted in Hexadecimal format on the RS232 port.

Transaction Mode – Non-access control function. The reader responds to external commands received at the RS-232 port, typically connected to a host PC or micro-controller. The software developer or system integrator must incorporate HID's communications protocol into the host software or firmware to communicate with the reader.

USING THE 6055 IN SECURITY MODE

In security mode, the 6055B typically transmits OEM card data in Wiegand format data exactly as it is encoded onto the card. The only exception to this is when the reader is configured to transmit the 32-bit Card Serial Number (CSN), in which case there are several configurable options for data output formats.

HID Factory Encoded MIFARE Cards

HID can encode OEM Wiegand card data onto new MIFARE cards at the factory into the same formats provided on 125 kHz cards, including the new Long Format. The customer simply orders MIFARE cards with Wiegand encoding by specifying:

HID format number
Facility Code
ID range
Additional fields, such as Issue Level, OEM Code, etc.
Ink jetting

The OEM card data bears no relationship to the unique random 32-bit CSN.

HID normally encodes the Wiegand OEM card data into Sector 1 of the MIFARE card and protects the data with an HID proprietary key, which is not published. The HID proprietary key is also securely stored in each HID MIFARE reader.

On HID factory encoded cards, all sectors including the MIFARE Applications Directory are protected with Philips default keys (except for sector 1, which contains access control data, Figure 1). These keys are published, and are present in most generic MIFARE readers. Only HID readers have the HID keys, which enable the readers to read HID access control data. (HID keys also have Philips default keys for use in transaction mode.)

Fig 1 - HID Factory Encoded MIFARE Card – Standard Sector Allocation

Sector 0 – CSN, MIFARE Applications Directory – Default A & B Keys	Sector 8 – Empty Sector – Default A & B Keys
Sector 1 – HID Wiegand OEM Card Data – HID Secret Keys	Sector 9 – Empty Sector – Default A & B Keys
Sector 2 – Empty Sector – Default A & B Keys	Sector 10 – Empty Sector – Default A & B Keys
Sector 3 – Empty Sector – Default A & B Keys	Sector 11 – Empty Sector – Default A & B Keys
Sector 4 – Empty Sector – Default A & B Keys	Sector 12 – Empty Sector – Default A & B Keys
Sector 5 – Empty Sector – Default A & B Keys	Sector 13 – Empty Sector – Default A & B Keys
Sector 6 – Empty Sector – Default A & B Keys	Sector 14 – Empty Sector – Default A & B Keys
Sector 7 – Empty Sector – Default A & B Keys	Sector 15 – Empty Sector – Default A & B Keys

Once customers have purchased HID Factory Encoded MIFARE cards, they (or other application providers) can program additional data into other sectors on the card. See the section on Transaction Mode for more details.

Keys – A Brief Explanation

A Key is basically a password. The Mifare card uses 48-bit keys (typically expressed as 12 Hex characters). There is one pair of keys, called the A key and B key, used to protect each of the 16 card data sectors. Each key in a pair can be used to protect a certain function. For example, the A key could be required to read data in a sector, while the B key could be required to write data to a sector; or the A key could be required to deduct stored value from a sector, while the B key could be required to add stored value. To access data in a protected card sector, the reader must have a matching key.

Keys are used to protect data from being read or changed without authorization. Because each sector has its own separate key pair, a Mifare card can be used to store information encoded on the cards by separate vendors for separate applications, and each vendor would be prevented from modifying the other vendor's data accidentally or otherwise, simply by keeping the keys secret. For this to work, the keys to the card's Mifare Applications Directory need to be known to all parties. Separate sets of readers would be used to control each application – each reader would have only the appropriate keys for its own application.

Non-Factory Encoded Cards

Many customers already own MIFARE cards that are encoded with transit, vending, campus or other applications, and they wish to add access control functionality to those cards. This can be accomplished by connecting model 6055B HID MIFARE Readers to standard access control panels.

The easiest approach is to configure the HID MIFARE reader to output the MIFARE card's 32-bit Card Serial Number (CSN) as Wiegand data. The HID MIFARE Reader can be pre-configured to do this at the factory, or it can field-configured with a configuration card. Unfortunately, most access control panels require data formats with a fixed facility code and sequential numbering, and therefore cannot accept the 32-bit data. A common workaround is to cut off (or *truncate*) some of the data from the 32-bit CSN and adding a fixed facility code to synthesize 26-bit Wiegand format data. However, this still may result in duplication of numbers, and will provide random rather than sequential card numbering. This type of modification of CSN output can be configured on the 6055B.

Note that if the existing cards are Mifare Lite or Mifare Pro cards, outputting the CSN in Wiegand format is the ONLY method of using these cards for access control. There is no means available to encode HID OEM formatted data on these cards.

HID MIFARE Card Encoder

The cleanest solution for the customer who already has cards and cannot use the 32-bit CSN is to purchase an HID MIFARE Card Encoder and encode the cards on site.

The HID MIFARE Card Encoder is a special version of the reader that connects to a PC, running Windows software (similar to the HID ProxProgrammer).

The Card Encoder can encode HID OEM Wiegand data on any available sector of the MIFARE card, and analyze the card to see which sectors are available. It can also print the Wiegand Card ID number on the card when used with a dye sublimation printer (or it can print the card numbers on standard adhesive labels).

Whenever the Card Encoder writes data to the card it:

- Locks the encoded sector with HID Proprietary Keys
- Writes the HID Applications ID (AID) into the MIFARE Applications Directory

The MIFARE Applications Directory (MAD) is a table of contents stored on each card. Philips (the developer of MIFARE technology) assigns unique applications ID numbers to various suppliers and integrators. The reader scans the MAD, looks for a certain AID, and then goes directly to that sector to read the data. This is much faster than searching the entire card for data.

Philips recommends that MIFARE cards be encoded with the MAD in Sector 0, which HID does, but this is not required for the card to function.

Reader Configuration Options

The HID MIFARE Reader may be ordered pre-configured (or field programmed) to look for HID data in various places on the MIFARE card and output it in various formats. In the reader's model numbering scheme – the last two digits allow various configurations, explained in the tables below (Figs 2 and 3):

6055B - base model
X - Color (**G**-Grey, **W**-White, **B**-Beige, **K**-black)
X - Hardware Option (**N** – none)
00 - Beeper/LED Config Options (**00-07**, same as MiniProx)
0 - Card Read Mode (**0** - HID Data Only, **1** - HID+MIFARE CSN, **2** - CSN Only)
0 - CSN Output Mode (0 - 32 bit, 1 - 32-bit reverse (6055A), 2 - 26 bit, 3 - 34 bit, 4 - 40 bit)

Fig 2 - Card Read Mode Options

Card Read Mode	Description	Comments
0	HID Data Only	Reader looks in Sector 1 (or user-configured sector) first, then scans MAD for the HID AID. If HID data is found, it is output in Wiegand format as programmed, or if HID data is not found, the card read fails.
1	HID+MIFARE CSN	Reader looks in Sector 1 (or user-configured sector) first, then scans MAD for the HID AID. If HID data is found, it is output in Wiegand format as programmed, or if HID data is not found, the reader outputs the CSN in the configured Wiegand output mode.
2	CSN Only	Reader outputs CSN in the configured Wiegand output mode.

Fig 3- Card Serial Number Output Mode Options

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 previous 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 000, 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

Contact HID Technical Support for information on ordering configuration cards, or for information on card formats.

Existing Cards – Possible Scenarios

Because cards in an existing MIFARE card population have likely been encoded by one or more application providers, HID has carefully designed its MIFARE Readers and MIFARE Card Encoder to be adaptable to many different scenarios.

Scenario	Method	Comments
Customer has blank cards with Philips default keys	Use MIFARE encoder – encode HID data in sector 1	Encoder will set up MIFARE Applications Directory and indicate HID data in sector 1.
Customer has encoded cards with available sector 1 and Philips default keys	Use MIFARE encoder – encode HID data in sector 1	Encoder will modify existing MIFARE Applications directory, indicating HID data in sector 1

Scenario	Method	Comments
Customer has encoded cards with available sector 1, but no MAD (or MAD is locked, or sector 0 is used for some other purpose)	Use MIFARE encoder – encode HID data in sector 1	Encoder will not modify MAD / Sector 0
Customer has encoded cards, sector 1 is not available, MAD is available and Philips default keys are used for available sectors	Use MIFARE encoder – encode HID data in available sector X	Encoder will modify existing MIFARE Applications directory, indicating HID data in sector X
Customer has encoded cards, sector 1 is not available, MAD is not available and Philips default keys are used for available sectors	Use MIFARE encoder – encode HID data in available sector X	Configure HID readers by changing default sector to sector X. Order configuration card from factory, or create with MIFARE programmer.
Customer has encoded cards, MAD is available and non-default keys are used for available sectors	Use MIFARE encoder – encode HID data in available sector. Configure HID readers to look in MAD for HID data Obtain non-default keys and enter them into the MIFARE encoder software to access the available sector	Encoder will modify existing MIFARE Applications directory, indicating HID data in sector X. Keys for sector X will be changed to HID Proprietary.
Customer has encoded cards, and non-default keys are used for MAD and available sectors	Obtain non-default keys and enter them into the MIFARE encoder software to access the MAD and the available sector. Use MIFARE encoder to encode HID data in available sector. Configure HID readers to look in MAD for HID data	Keys for sector X with HID access control data will be changed to HID Proprietary. Configure HID readers by changing default sector to sector X. Order configuration card from factory, or create with MIFARE programmer.
Customer has encoded cards and does not know how they are encoded	Read cards on MIFARE encoder – it will try Philips default keys, or any known A & B keys which customer enters into the software. Or, obtain encoding information and keys from whoever originally encoded the cards. Once open sectors and keys are determined, use HID MIFARE Card programmer to encode	If keys are unknown and are not defaults, data protected by those keys cannot be read or modified. If the customer does not have a MIFARE encoder, they may send sample cards to HID Technical Support for analysis.

Scenario	Method	Comments
Customer has combined two groups of cards, and some cards have a different available sector than others for HID data – MAD is available	Use MIFARE encoder – encode HID data in available sector X on one group and Y on the other group	Encoder will modify existing MIFARE Applications directory, indicating HID data in sector X or Y. Reader will search all cards for HID AID and will read the data from the appropriate sector
Customer has combined two groups of cards, and some cards have a different available sector than others for HID data – MAD is NOT available	Set readers to CSN only mode.	There is no way for the readers to find OEM data in various sectors without using the MAD.

Using the 6055B in Transaction Mode

Transaction Mode allows developers and integrators to create their own software or firmware programs that can use the HID MIFARE Reader to read or write to a MIFARE card. The actual application program (vending, debit, transit, etc.) resides in the host computer or micro-controller – it does not reside on the reader.

Transaction Mode requires a connection to the reader's RS-232 port. The reader is set to Transaction Mode by a command from the host computer – no command card or factory pre-configuration is required.

The HID reader performs three important functions:

- Manages the RF interface with the card
- Manages the communications and encryption
- Reads and writes to the card

Because there is no standard for communicating with a MIFARE reader, each manufacturer has its own unique protocol.

HID has made its complete protocol available to developers as part of the **HID MIFARE Developer's Resource Kit**, containing a protocol document and programming guide, some example software, a sales demo program, and a reader with power supply and desktop stand.

By using this protocol, the connected PC or controller can:

- Read or write to any sector on the card (except HID Wiegand data)
- Load or rewrite keys
- Increment or decrement a stored value sector
- Scan or modify the MIFARE Applications Directory
- Control the beeper and LED

In transaction mode, every function of the reader is under the complete control of the connected PC or controller.

The reader will assert the DTR control line when it successfully reads a card. This alerts the host that a card has been read, and can be used to trigger the customer's application program. The reader continuously re-transmits the CSN until an acknowledgement is received from the host. The reader also sends a "break" signal when it powers up. If the developer is using non-standard keys for his application, this allows the application to resend the keys (only the default keys are stored in Flash memory).