White Paper

Understanding Multi-Card Formats: How to Make Sure Your Customers' Cards are Compatible With DMP

The benefits of multi-card format with DMP access control is clear:

For compatibility with what your customers are already using, you have the flexibility to program up to seven different card formats in addition to the DMP format.

With that, there's no need for customers to replace their existing cards.
But how do you know for sure if their cards are compatible with DMP access control?

DMP can program many custom formats as one of the seven custom formats. But to answer that question, DMP's Adam Kinder explains why it's equally important to also confirm the card technology, as well as reader output modes your customers are using. When you need to make an existing card work with a new platform, you'll need to make sure there's compatibility with all three of those components.

"You need a card format that our panel can support, but you also need the correct card technology; otherwise the reader can't communicate the data that's on the card." And when the reader retrieves that information, he adds, "it then has to be able to pass it to the door controller."

Kinder is the regional training manager for the Central States/Lower Mississippi territory. He also has been instrumental in developing DMP's ability to work with multi-card formats. This white paper outlines the three primary components that determine compatibility.

Card Format: It's What Allows the Reader to Decode a Card's Data

The purpose of every access control credential is to store a unique numeric code that can be read and processed by the system. In order to work, a card reader must be able to recognize the data format. A format refers to the way numerical information is structured.

To ensure compatibility with DMP access control, the credential, card reader and door controller are the three primary components to consider. In this illustration, a 26-bit credential uses the 125-kHz frequency to transmit its data to the card reader, which relies on the Wiegand output module to communicate with the door controller.

“It’s all about decoding data,” Kinder says. “The system needs to know how to decode that information, and that’s what the card format determines.”

Basically, it’s comprised of a set of binary “bits," put together a certain way to create a binary number, which is converted into a credential number by an access control system.

“A format describes what a number means, or how it’s used,” Kinder says. For instance, if you see this string of numbers: 4178319362, it may mean nothing. But if you describe it as a phone number in the United States, then it is immediately understood that 417 is the area code, etc. In a similar way, a card and reader need to use the same formats in order to communicate.

The Standard 26-Bit Format

The format in which a card is programmed is determined by the data pattern that will be compatible with the access control panel — almost all access control systems accept the standard 26-bit format public credential, which anyone can buy in a specific number range.

Even though your customer may use the same format and card number range as another business, a second number, known as a facility or site code is encoded into each card to identify the card’s valid authentication. “Your customer’s door controller can be programmed to only accept cards with a matching facility code,” Kinder says.

As you might expect, each group of bits has a function. On a 26-bit card, for instance, the leading parity bit and trailing parity bit are used for starting and ending a stream of data. The first eight bits following the leading parity bit designates the site code also known as a facility code. On a 26-bit card, the facility code range can be anywhere from a value of 1 – 255.

PUBLIC CARD FORMATS

CARD FORMAT	WIEGAND CODE LENGTH	SITE CODE POSITION	SITE CODE LENGTH
H10301 26 BIT	26	1	8
FARPOINTE 39 BIT	39	1	17
CORPORATE 1000 35 BIT	35	2	12
CORPORATE 1000 48 BIT	48	2	22

In addition to the readily available 26-bit card format, there are also additional public formats that can be utilized. However, unlike the standard HID 26-bit format, many newer public formats allow a greater card number range. Some public formats can also offer additional security features, such as the manufacturer tracking issuance to ensure that there is no chance for duplication of card numbers. Corporate 1000 formats are registered to an end-user directly, however, Farpointe 39-bit and HID can be ordered directly by the alarm dealer.

Proprietary Cards

In addition to the 26-bit open format, there are higher bit formats, considered “proprietary” because they’re manufactured specifically for individual companies. We can also work with these, Kinder explains, but it’s important to remember that within a given bit length (34-bit, etc.), the size and location of each data element may change. Therefore, he adds, “The programmer or technician would need to research that card format from the supplier. As long as we know what the card format is and how it’s decoded, we should be able to work with it.”

DMP can work with any range up to a total length of 255 bits. That’s the maximum Wiegand length. Within that 255 bits, we can support up to 24 bits for the facility code and up to 64 bits for the card number length.

How to Confirm Your Customer’s Card Format

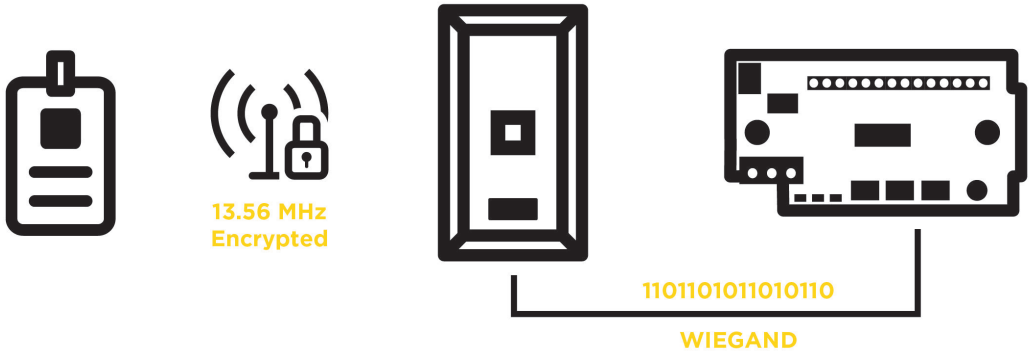
To confirm your customer’s card format, you’ll have the best luck getting that information from their employee who typically purchases the cards. “That person would know what card format and number range they’re using,” Kinder offers. Also, HID prints a serial number on its cards. "If you contact HID and provide that serial number, they can identify what the card format is.”

What Card Technology are Your Customers Using?

You've confirmed what your customer's card format is. It's also important to find out what frequency those cards use for transmitting data to the readers and door controllers. Cards differentiate by low-range or high range, that's when you see the "kHz" measure.

Low-Frequency Technology

What delivers the longest read range is the lower-frequency 125 kHz formatted cards. Popular low-frequency formats include HID Proximity, Indala, EM® and AWID.



High-Frequency Technology

The low-frequency cards are the most commonly used card type, although Mifare DESFire EV1 is becoming more popular for its increased security features. Namely, explains Kinder, "These devices communicate at 13.56 MHz, not 125 kHz, which reduces the ability to copy a credential. Also, the data on the card is secured across multiple sectors that must authenticate with the correct encryption keys before any data is exchanged."

For details on the low-frequency proximity readers and credentials that DMP offers, click here. For information on our high-security readers and credentials, click here.

DMP can work with both types of technology, "as long as the technology a card uses to transmit data is compatible with what the reader can receive," Kinder explains. "If, for example, your customer uses a 13.5 MHz HID iClass® style card, the reader has to be able to understand that."

Reader Outputs

Currently DMP supports Wiegand output card readers. It's by far the most common communication method, although there are other protocols, including Open Security Device Protocol (OSDP), RS485, Clock and Data, to name a few.

Understanding what makes access control work may seem complex, but in its most basic form, it's a matter of being able to properly exchange information. Like the way we communicate with one another, Kinder adds, "If you're going to relay a message, you have to use a language the other person understands." Likewise, he says, "The card format, card technology and reader output have to be able to communicate."

And when they do, your opportunities to take over existing access control panels continues to expand.

866-266-2826
DMP.com
INTRUSION • FIRE • ACCESS • NETWORKS
2500 North Partnership Boulevard
Springfield, Missouri 65803-8877