HID Indala FlexSecur® Technology

Introduction

The popularity of proximity access control and 26-bit open format cards, combined with interchangeable proximity readers has resulted in a situation where different customers can receive identical cards, and cards from one facility can obtain access to another facility.

HID's Indala Proximity access control cards and readers offer an exclusive security technology called FlexSecur® whereby cards and readers are programmed as a unique set for each customer. Therefore, cards belonging to one customer cannot be read by another customer's readers. FlexSecur® provides a dramatic improvement in access control system security at no additional cost, and it works with any access control system.

The Problem

Most proximity card readers will transmit proximity card data to the access control panel without verifying that the card is authorized for that facility. Most proximity cards cannot be configured to operate at only one specific facility. The readers are fully interchangeable and the cards will read on any reader of the same brand. Local distributors usually have interchangeable readers and 26-bit open format cards in stock.

While this is convenient for the security dealer, it can also represent a significant security risk for the customer. It means that it is possible for customers to receive cards that are identical to those of others. A few customers have accidentally discovered that their cards can gain entry to another customer's facility; and they are concerned that someone from another facility could gain unauthorized entry to their facility.

Additionally, most proximity access control cards contain unencrypted data. This means that if a person with some technical knowledge obtains a card from a particular site, even if the card is voided in the access control system database, the facility code and ID number could be determined using a card reader purchased from any distributor. Additional cards in the same ID number range could then be purchased, enabling unauthorized entry.

The Solution

FlexSecur® multi-layer security prevents accidental or fraudulent entry attempts by creating unique formats for individual customers, which include a unique password to be specified, and unique encryption of the card data so that it cannot be interpreted by potential intruders. These security measures are programmed into both the cards and readers, so that the reader will output data to the access control system only when matching cards are used.

FlexSecur® Formats Consist of the Following Components:

- Indala Format Number - A unique reference number is assigned to each format. New formats are assigned the next available number in sequence. The format number has no direct relation to the card data format. The format number is entered into the Indala database, and it links to a "project file" with the following components used to program cards and readers:
  - Password – This 10-digit (30-bit) numeric value is stored in both cards and readers. Passwords are optional, but highly recommended.
  - Encryption Key – A randomly generated string of bits assigned to each new format number, it is used during the card encoding process to encrypt card data and it is used by the reader to decrypt the data before it is output to the access

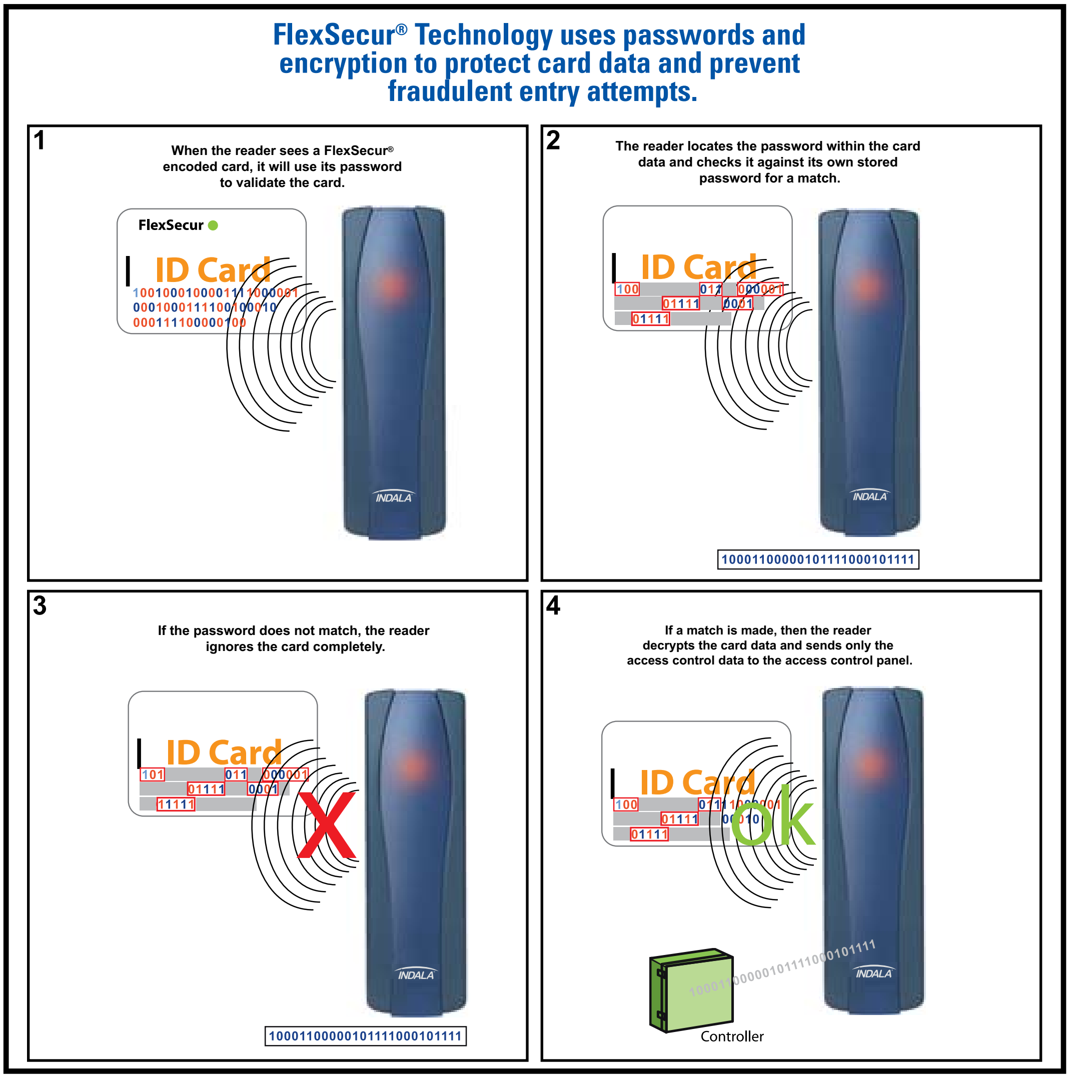
control system. The key is stored in the reader but not on the card.

- Card and Reader Data Format – This format describes how access control data is encoded on the cards, including number of bits, field lengths, types and positions, data order and parity scheme. It also tells the reader how many bits are encoded on the card and how many bits to transmit to the access control system.
- Reader Parameters – The format project file also includes any special reader configuration that the customer requires such as beeper on/off, LEDs on/off, single or dual LED control, Wiegand pulse width, etc. Reader parameters can also be modified by using "Option Cards."

How Does FlexSecur® Work?

When a card is presented to the reader:

1. The reader compares its password to the password in the card.
2. The reader applies its data structure to the card data, using its internal table.
3. If the passwords do not match, the reader does not output data to the control panel.
4. If the passwords match, the reader uses its own encryption key to decrypt the card data. If the data structure is correct, decrypted data is output from the reader to the access control panel. The correct data structure indicates successful decryption, meaning that the key used to encrypt the card matches the key in the reader.



FlexSecur® Technology uses passwords and encryption to protect card data and prevent fraudulent entry attempts.

1 When the reader sees a FlexSecur® encoded card, it will use its password to validate the card.

2 The reader locates the password within the card data and checks it against its own stored password for a match.

3 If the password does not match, the reader ignores the card completely.

4 If a match is made, then the reader decrypts the card data and sends only the access control data to the access control panel.

FlexSecur® works with any card data format, including the generic 26-bit Wiegand format . By adding a FlexSecur® password and encryption to 26-bit format cards (or cards with any data format), they become unique and secure. Because security is handled between the card and reader, it is transparent to the access control system, which sees only plain (unencrypted) card data.

What is an Encryption Key?

FlexSecur® uses an encryption algorithm (a mathematical formula) to convert plain card data into a secret code (encrypted data) prior to encoding. The corresponding decryption algorithm is programmed into each reader, allowing it to convert the secret code back into plain card data before sending it to the access control panel.

The encryption key is a string of bits used as part of the algorithm. By creating a unique encryption key for each Indala format number, Indala FlexSecur® ensures that each format is encrypted differently than other formats. Readers ordered with one Indala format number cannot decrypt cards ordered with a different Indala format number.

Encryption converts the data to entirely different values than the original plain card data, so that there is no apparent relationship between the encoded data and the plain data. (Example: plain data = 1234, encrypted data = 0876). Encryption is used on all Indala ASP+ cards and readers. It is more secure than scrambling technology used on legacy Indala ASP cards and readers, which takes the plain data and moves it to different locations in the string. (Example: plain data = 1234, scrambled data = 4132).

Customers do not need to be concerned about encryption keys. These are all automatically generated by the programming software—whether cards and readers are programmed at the factory or the customer purchases a ProxSmith® Programmer Kit and programs cards and readers on site. It is unnecessary for the customer to know the key, and he should not worry about losing it.

26-bit Format with Default Key

Some dealers prefer the ability to purchase cards and readers from any distributor and use them on any system. For this reason, Indala cards and readers sold through distribution are programmed with the 26-bit Wiegand format, using the Indala default encryption key. Additionally, the password feature is not used. Because these readers and cards are programmed with the same encryption key, they are interchangeable, and it is possible for a card from one facility to gain entry at another facility if the facility codes and ID ranges are the same.

How Formats are Assigned to Customers

When a customer wishes to request a new format, he contacts HID Indala Technical Support. A project file is created. The next available Indala format number is assigned to the customer. An encryption key is randomly generated by the programming software and assigned exclusively to that format. The customer specifies the card data format, describing the format length in bits, data fields, minimum/maximum ranges, parity, etc. He is given the option of using a password, which can be randomly assigned by the programming software or entered manually. The customer may specify desired reader configuration parameters such as LED and beeper operation or Wiegand pulse timing. The project file is linked to the format number in HID Indala's database, and all this information is used to program the customer's cards and readers.

When the customer wants to order additional cards or readers, he simply provides the Indala format number, facility code, and card ID range. He does not have to specify any other details such as encryption keys, passwords or reader configuration parameters.

If the customer has a control panel which accepts custom formats, he can have a totally unique Indala format, with a unique password, unique encryption key, and a unique card data structure.

In some cases the access control panel will not accept custom formats, only allowing 26-bit, or perhaps the panel manufacturer's own registered format. With FlexSecur®, this is not a problem. The customer can contact HID Indala and request a new Indala format number, including the common card data structure, but with unique encryption and a unique password, making the cards and readers unique and secure.

HID Indala customers, who are frequently OEM manufacturers or large integrators with many customers (rather than individual end users), typically order cards and readers programmed with their own registered Wiegand format. If the OEM or integrator always orders cards and readers with the same Indala format number, their readers and cards will be interchangeable with one another. This allows OEMs to stock and exchange readers, while preventing competitors from ordering compatible cards and readers or taking over systems. While the OEM's customers will not have totally unique cards and readers, the proprietary OEM format combined with careful management of facility codes and ID numbers by the OEM, and FlexSecur® data encryption provides the end user with a much higher level of security than most access control cards and readers.

Are There Different Levels of FlexSecur® Security Formats?

FlexSecur® is not offered in specific levels, but customers can get more or less security depending on how they order their cards and readers.

	Low Security	Medium Security	High Security
Password	Not Implemented	OEM Password	Unique Password
Card Data Format	Default 26-bit	OEM Data Format	Unique Data Format

Every customer can have the highest level of security with FlexSecur®, by requesting a unique password and a unique card data format. Most panels will allow customers to define their own card data format. By contrast, some older or less expensive panels only allow OEM or default card data formats. However, if cards and readers are ordered with a unique password, the readers will still reject any unauthorized cards.

ProxSmith® Programmer Kit

For the ultimate level of security, the customer can order a ProxSmith® Programmer Kit, program all cards and readers onsite, and keep the unique password completely confidential.

The Indala ProxSmith® Programmer Kit is a card and reader programming system consisting of a programming unit (a special reader/writer) and a Windows® software application. ProxSmith® allows customers to purchase generic format cards and readers from HID Indala and reprogram them onsite to match existing cards and readers with custom formats.

ProxSmith® also allows customers to purchase a supply of unencoded cards in advance, and then program cards one at a time on demand, rather than wait for the factory to encode and ship a minimum order of cards.

It also enables customers to define their own custom card data formats and unique passwords, such that no one else in the world will know them, including HID Indala. The encryption keys are automatically created by the software, and the password can either be randomly generated or manually input by the customer as (up to) a 10-digit number.

ProxSmith® allows customers, such as OEMs or system integrators, to create multiple formats for cards and readers. This gives the OEM ultimate flexibility, and allows the OEM to program cards and readers for any system, while making those cards and readers secure and unique.

The ProxSmith® user is responsible for keeping accurate records of card data formats, passwords, ID numbers and facility codes of cards that have been issued, as HID Indala cannot be responsible for them. If no records are kept, and the ProxSmith® is lost or damaged, HID Indala will not be able to re-create the customer's formats by reading the cards.

What is FlexEnterprise®?

FlexEnterprise® is an Indala product line program offered by HID that assigns corporate end-user customers their own unique Indala FlexSecur® format, and they designate the access control hardware/software platform provider and system integrator of their choice. Format security is controlled by a closely monitored authorization process. Individuals must be authorized by the customer to order cards and readers, and each new order must be accompanied by a new authorization form.

The FlexEnterprise® program offers two main benefits. First, it gives the customer full control over who is authorized to order cards and readers programmed with their unique format. Second, it avoids locking the customer into one system supplier (because the card format is registered to the OEM). The customer is free to use multiple system vendors, or to change vendors at any time without having to replace cards and readers.

Conclusion

FlexSecur® provides customers with the highest level of security available for 125 kHz Proximity Access Control cards and readers. FlexSecur® can be used with any access control panel because the security is between the card and reader, and is transparent to the panel. FlexSecur® converts even common and frequently duplicated formats such as 26-bit Wiegand, into customer-specific, unique, secure formats where readers and cards are non-interchangeable with those from other systems.

Ordering additional cards and readers for a system is easy. Customers only need their Indala format number when ordering for their systems. They do not have to remember passwords, encryption keys or reader configuration. FlexSecur® does this automatically for the customer.

FlexSecur®, along with the ProxSmith® Programmer Kit that allows customers to program cards and readers onsite, and FlexEnterprise®, which allows the customer to "own" their own HID Indala format and choose or change their access control suppliers at any time, offers customers the ultimate in flexibility.

Questions/Comments

For more information about HID Indala FlexSecur® technology, please visit the HID website at www.hidcorp.com.