AN-315

Understanding MIFARE DESFire Credentials

Application Note

Last Published: 11-May-22 10:33 AM

Contents

Introduction

MIFARE DESFire credentials can be programmed with **standard application** configuration or **custom application** configuration. Credential encoding must match your reader configuration, so it is critical that the appropriate configuration is ordered for the site to prevent incorrect credential encoding.

The purpose of this application note is to clarify the differences between cards that have been programmed with custom application keys and standard application keys, primarily to simplify the process of ordering cards and ensure the right end result for the site.

This application note will cover the various types of applications stored on the card, what they mean, and how they can apply to use in a customer facility. This will help you to better understand the options and provide your customers with the most secure interoperable system without compromise.

The information in this application note should allow you to confidently identify whether your site requires credentials programmed with a **standard application** configuration or a **custom application** configuration.

Terms

Throughout this document, 'Card' will be used as a uniform term to define any card, key tag, disc or other physical credential device.

About MIFARE DESFire

This application note applies to MIFARE DESFire EV1 and MIFARE DESFire EV2 (2K/4K/8K) credentials when encoded for ICT card readers and interoperability applications.

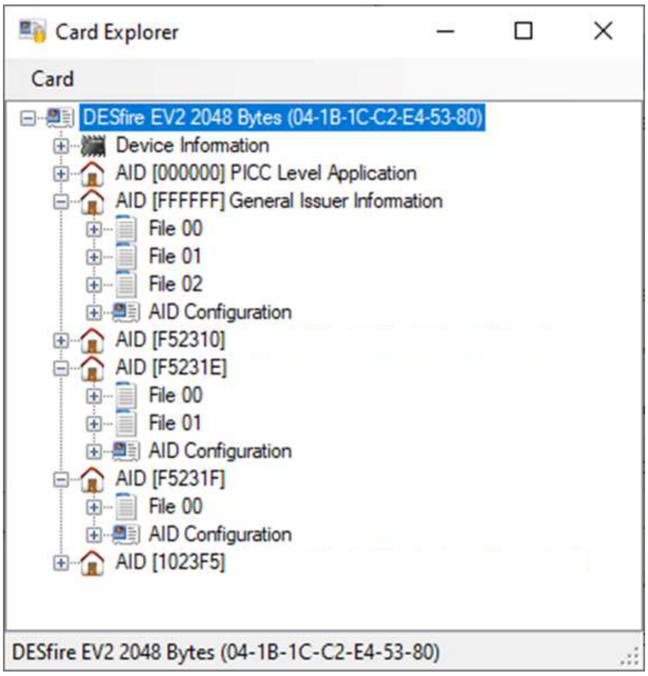
The full MIFARE DESFire specification and in-depth information on the technology and capability is available at https://www.mifare.net/en/products/chip-card-ics/mifare-desfire/.

Applications and Files

You can imagine the memory of a MIFARE DESFire card as a USB drive you would plug into your computer.

- The card can have applications which have certain properties, similar to a directory on your drive.
- Within each application you have files which store the data. An application can contain multiple files.
- Applications can have multiple keys assigned to them, and each application can have different keys.
- A file can have different keys to read the file, write the file, or read and write the file.
- Files stored on the card can be of variable length.

The ICT Encoder Client software is laid out in this manner, and the relationship can be seen in the example below which shows the structure of a scanned MIFARE DESFire card.



```
DESfire EV2 2048 Bytes (04-1B-1C-C2-E4-53-80)
    Device Information
    AID [000000] PICC Level Application
    AID [FFFFFF] General Issuer Information
        File 00
        File 01
        File 02
        AID Configuration
    AID [F52310]
    AID [F5231E]
        File 00
        File 01
        AID Configuration
    AID [F5231F]
        File 00
        AID Configuration
    AID [1023F5]
```

DESfire EV2 2048 Bytes (04-1B-1C-C2-E4-53-80)

When viewed like this, each application displays [in brackets] its unique **application ID**. This application ID can be used to identify each application and confirm the card programming configuration.

Standard Application vs Custom Application

MIFARE DESFire encoded cards are shipped with a standard application configuration by default.

Important: If a custom application configuration is not explicitly specified, orders will be processed using the standard application configuration.

Standard Application	Custom Application
Generic key set used by readers and cards.	**Custom** key set used by readers and cards.
Diversified keys.	Diversified keys.
Will read on factory defaulted ICT card readers.	Will **not** read on factory defaulted ICT readers.*****
	Requires a **configuration card** to load the keys into a defaulted card reader.
Restricted to a **Registered Site Code**.	Freedom to choose **custom** site/facility code combinations.

* The reader must be presented with a customized configuration card that will allow it to read the custom cards.

If required a credential card can contain both standard and custom keys, so that it can be read at readers configured with standard keys as well as readers configured with custom keys. This must be explicitly specified at the time of ordering.

Customers may elect to have readers factory keyed if required. Additional charges may apply.

Standard Application

- Cards will read on any ICT reader that is factory defaulted and has not been configured to either read only a custom key or have MIFARE DESFire disabled.
- Standard application is restricted to registered site codes. You cannot select your own site code.
- Allows for interoperable reading of cards. Default format is 34 bit: 16 bit for card and 16 bit for facility code.
- The keys used to read the file from the application are diversified using the serial number of the card and other seed information, meaning every key is different for each card.
- A standard application and associated keys can also be encoded on a card that is encoded with a custom application and keys. This is possible because they use different application IDs.*****

* The standard application and keys are **not** loaded by default on custom applications and **MUST** be requested at the time of ordering. The standard application encoding may not be able to have the same site/facility code as the custom application encoding.

Custom Application

- Cards will only read on ICT readers that have been configured with the application ID and custom keys.*****
- You can specify a custom site code or combination of site codes and card numbers. When configured, the card reader will not read other cards, and as such the site code selection can be managed by the customer.
- There is no restriction on the format type (number of bits or structure) with custom formats. However, cards are typically encoded with a 34 bit format allowing 16 bits of card number and 16 bits of facility code.
- All interoperability is available, with no restriction on other uses and integration.

  This is a key benefit to using the MIFARE DESFire technology.

* The reader must be programmed, using the config app or a configuration card, to allow it to read the cards.

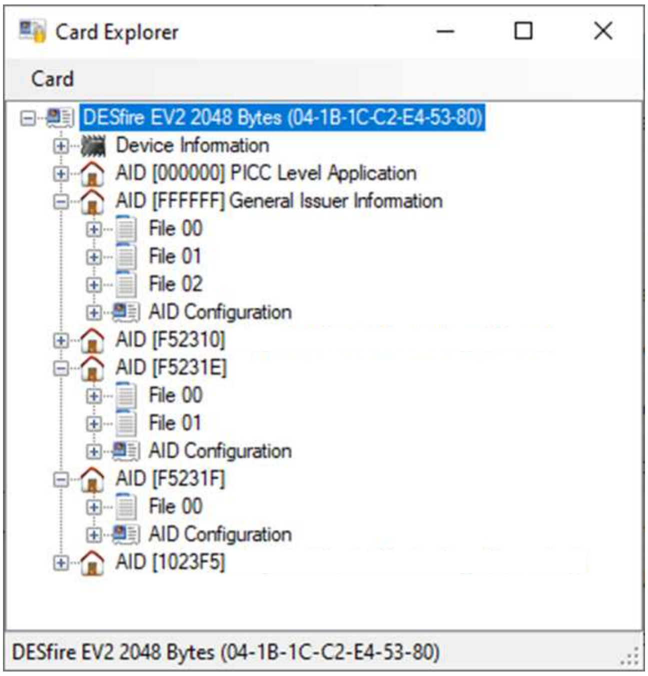
If you require a config card to configure readers it must be requested at the time of ordering credentials.

Card Directory Structure

Cards are loaded with more than one application and these are used for traceability, interoperability and integration with some third party locking systems.

Cards may contain a mixture of applications comprising the standard application or a custom application, as well as the General Issuer Information.

A typical card layout will look similar to the example below, which shows the structure of a MIFARE DESFire card scanned in the ICT Encoder Client.



```
DESfire EV2 2048 Bytes (04-1B-1C-C2-E4-53-80)
    Device Information
    AID [000000] PICC Level Application
    AID [FFFFFF] General Issuer Information
        File 00
        File 01
        File 02
        AID Configuration
    AID [F52310]
    AID [F5231E]
        File 00
        File 01
        AID Configuration
    AID [F5231F]
        File 00
        AID Configuration
    AID [1023F5]
DESfire EV2 2048 Bytes (04-1B-1C-C2-E4-53-80)
```

Default Primary Application

The default primary application is programmed as standard, with an application ID of **F52310**.

This will be programmed unless a custom application is specifically requested.

- 16, 32 or 128 byte file length.
- Diversified keys.
- Designed to be read by ICT card readers.
- Readers do not require configuration to read these credentials.

Default Secondary Application

The default secondary application is programmed as standard, with an application ID of **1023F5**.

This will be programmed unless a custom application is specifically requested.

- 16, 32 or 128 byte file length.
- Diversified keys.
- Designed to be read by ICT card readers.
- Readers do not require configuration to read these credentials.

Default Custom Application

The default custom application is programmed when you select a custom application. The default application ID is **F52318**, however if required this can be changed at the time of ordering. Customization charges may apply.

This configuration must be specified at the time of ordering.

- 32 byte file length.
- Diversified keys.
- Designed to be read by ICT card readers **that have the appropriate configuration card presented**.*

The reader must be configured to allow it to read the cards. A config card must be ordered if required.

Interoperability Application

One of the benefits of the MIFARE DESFire technology is the ability to provide an interoperable solution, whereby a single card can be recognized by multiple systems. This removes the need for users to fish through their pile of similar-looking cards to find the one that they currently need.

Interoperability can be achieved with both standard and custom keys by use of the third-party application, which by default is loaded with 2 files - one ASCII file and one WIEGAND file. Its application ID is **F5231E**.

The file can be read for validation using the ICT Encoder Client.

There are two encoded options:

- **ASCII** (text based) format allowing any system to read the formatted data. The data comprises two decimal numbers separated by a colon and terminated with a carriage return 0x0D char and a null 0x00 terminator.
- **WIEGAND** (bit based) format that emulates the encoded format from a tSec Multi-Technology Card Reader, allowing third parties to read the card information and output the standard Wiegand format.

Any combination of third party applications can be encoded (or not) as required.

By default only two files are loaded to the application. You can request a further two files that use OPEN reading, although **this is not recommended**.

Third-Party Locking Application

An application used for the integration to third party locks, with an application ID of **F5231F**.

- When integrating with third-party locking solutions such as Aperio®, Salto Sallis™ and others, a specific application ID is created.*
- The application comprises a single file that contains an encrypted data blob.
- Programming the information into the locking device configuration will require:
  - The AES128 bit read key
  - The key number
  - The application ID
  - The file number
  - The length of the data to read

  This is necessary to allow the third party lock to read the blob and send it to the controller.
- Programming the information into the controller will require the AES256 bit blob key to be entered into the key location in the reader configuration properties of the reader expander.

*Refer to the relevant lock integration application notes for configuration of the keys and reading settings.

Credential Ordering Summary

So, do you need the standard application configuration or a custom application configuration?

1. You need to order the **standard application configuration** if:
   - your readers use the default factory configuration with no explicit after-factory programming
   - your credentials have a registered allocated site code
   - your credentials use a generic key set

   MIFARE DESFire encoded cards are shipped with the standard application configuration by default.

2. You need to order the **custom application configuration** if:
   - your readers use a custom configuration programmed with a config card or the config app
   - your credentials have a custom site or facility code that you choose yourself
   - your credentials use a custom key set

   Remember to request a reader config card, if required, at the time of ordering credentials.

3. If you have readers that use the default factory configuration, as well as readers that use a custom configuration:

   You need a custom application configuration with the standard application configuration included.

   This must be explicitly specified at the time of ordering.

Important: If a custom application configuration is not explicitly specified, orders will be processed using the standard application configuration.

Still not sure?

Ask ICT Customer Services. If you have ordered previously we have records of your previous configuration, or we can identify the configuration from the application IDs and other information on the card. If you haven't ordered yet, we can help you figure out what you need.

FAQ

Q. Can I revert my reader back from reading cards with custom keys to reading cards that have standard keys?

A. Yes. You can present a config card that has the reader default option encoded and this will set the reader to factory default.

Q. Can a reader be programmed to read more than one custom key? For example, if I have two companies with custom keys and they are in a building that has a common set of doors, how would I set up the readers?

A. You would not alter the custom configuration of the readers. You would either encode all cards with another application that is used for the common building access, or you would use readers configured with standard keys on the common access doors.

Q. We have ordered cards previously. What is the best way to order the same encoding again?

A. All orders are provided with a **reference number** and in particular a **CP number**. This is the credential profile (CP) and is a unique profile used for you.

If you do not have this available the site name, site/facility code and any previous order information will help to identify your profile, but the preferred and most accurate method to avoid potential errors is the **CP number**.

Q. You mention diversified keys for both the standard and custom applications. What does that mean?

A. Diversification is a method whereby a unique piece of information such as the card serial number, application ID or file number is used as a seed with a key to derive a key that is unique to the card itself. For more information refer to https://www.nxp.com/docs/en/application-note/AN10922.pdf.

Q. How can I tell what has been encoded on the card?

A. Each encoded card has traceability information that will hold the manufacturing information and profile number that it was encoded with.

This can be viewed by looking at the issuer **AID 0xFFFFFF** which holds 3 files:

- The version (3)
- The holder details (encoded profile)
- and the issuing company

These are free to read text and value files. You will find the CP reference in the holder details.

Q. Is there documentation on what configuration parameters can be set in a tSec Multi-Technology Card Reader?

A. Yes. This is available in application note AN-283: Programming tSec Reader Functions, which includes all options for programming tSec Multi-Technology Card Reader configuration.

Q. Can I overwrite a config card?

A. Yes. You can re-use a config card any number of times, to add to an existing configuration or overwrite the card entirely with a new one.

Q. When a config card is made to read a custom application, what does the configuration change in the reader?

A. The configuration changes the encryption key, key number, application ID and file number being used to read the file. This is stored in the config card and read by the reader. A configuration can also be configured and stored in the Protege Config App.

Credential Tools

NFC Tag Info provides good information on what is in the card and can be used to read the traceability information.

- https://play.google.com/store/apps/details?id=com.nxp.taginfolite&hl=en
- https://apps.apple.com/us/app/nfc-taginfo-by-nxp/id1246143596

The **Protege Config App** allows you to configure a Bluetooth® reader using the configuration tool and application available on your phone.

- https://play.google.com/store/apps/details?id=com.ict.ProtegeMobileConfig&hl=en
- https://apps.apple.com/us/app/protege-config/id1441256253

For information on configuring readers using the Protege Config App, refer to AN-283: Programming tSec Reader Functions, available on the ICT website.

The **ICT Encoder Client** allows you to scan a card, encode cards and read back programmed information, and view configured applications.

Interoperability Encoding

Following is the bit/encoding structure and key settings encoded in the interoperability application. This can be provided to a third-party reader manufacturer to specify exactly how to read the data from the file.

Application Keys: 3

Application Files: 2

Key 00: Master

Key 01: Read Only (for Read Secured Files)

Key 02: Write Only (for all Files)

File 00: 32 Bytes. Secured read, Secured write.

- Format: ASCII. 5 Bytes facility code, 5 Bytes card number, ':' delimiter.
  e.g. 00001:00001

File 01: 32 Bytes. Secured read, Secured write.

- Format: 34 Bit Wiegand (S=Site Code; C=Card Number) with 8 bits Length (L) and Parity (P).
  LLLLLLLLPSSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCP
  e.g. 001000101000000000000000100000000000000010

The first parity is calculated as Even Parity on the 'S' Bits.
The second parity is calculated as Odd Parity on the 'C' Bits.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.