AN-352

Setting Up Custom Credential Encryption

Application Note

Last Published: 10-Feb-23 08:42 AM

Contents

Introduction

When you order cards, tags and mobile credentials from ICTit is important to consider the security of the card encryption. While ICT Secured MIFARE and MIFARE DESFire are encrypted credential standards, using the default encryption key set makes it possible for bad actors to create clone cards which can gain access to your system.

ICT recommends that you mitigate this risk by using credentials with a **custom encryption key set**. These are unique encryption keys which are used for a single customer or site, making it much more difficult for attackers to create clone cards for the site. The key set is shared between the credential and the card reader so that the reader will only accept credentials with the correct encryption.

Custom encryption keys are available for ICT Secured MIFARE, MIFARE DESFire and mobile credentials. The table below outlines the main differences between default and custom encryption keys for credentials:

Default Encryption Keys	Custom Encryption Keys
Generic key set used by readers and cards.	**Custom** key set used by readers and cards.
Encryption keys are **publicly available**.	Encryption keys are **unique** to the customer or site and are **not** publicly available.
Will read on factory defaulted ICT card readers.	Will **not** read on factory defaulted ICT readers. Readers must be programmed with the keys in order to read these credentials.
Restricted to a **Registered Site Code**.	Freedom to choose **custom** site/facility code combinations.
One-off charge for managed site code.	One-off change for managed site code. No additional charge for custom encryption keys, but may be required to order config cards.

This document provides a summary of the process for ordering custom credentials and configuring card readers to use them.

Summary of the Process

To use credentials with custom encryption keys on your site, you must complete the following steps:

1. Order ICT Secured MIFARE, MIFARE DESFire or mobile credentials from ICT, specifying that you require custom encryption keys.

   If you are transitioning an existing site to use custom encryption keys it may be possible to re-encode existing cards which have been issued to users. This has specific requirements - contact ICT Technical Support.

2. Obtain the config for programming the custom keys onto the reader.
3. Program the readers to read the new custom encryption keys using a config card or the Protege config app.
4. Program the credentials into the security system and issue them to users who need access.
5. When you need to order more credentials, contact ICT Customer Services with the **CP number** from your previous order to receive cards with the same format and key set.

Ordering and Managing Custom Credentials

If you order cards, tags or mobile credentials from ICT but do not provide any further requirements, you will receive credentials which use the default ICT encryption keys and formats. However, there is a large amount of customization available upon request, including custom encryption key sets.

The process for ordering and managing credentials with custom encryption keys is different depending on whether you are ordering physical or mobile credentials.

Custom MIFARE and MIFARE DESFire Credentials

Before you order physical credentials for the first time, determine any custom requirements needed for this site. This could be unique encryption keys only, or may include additional features such as specific facility codes, card formats, custom sector data or applications for third-party integrations.

MIFARE DESFire credentials in particular have a wide range of customization options. For more information, see Application Note 315: Understanding MIFARE DESFire Credentials.

Then contact ICT Customer Services to discuss your requirements and request a custom **credential profile** for the customer site.

There are two options for managing custom MIFARE and MIFARE DESFire credentials:

- **Credentials are managed by ICT**: When the customer orders credentials, ICT will encode the credentials with their credential profile at the factory.

  For this option you will need to order:

  - One Managed Site Code license: **PRX-ENC-MSC**
  - Cards or tags that have been encoded using your credential profile
- **Credentials are managed by the integrator/customer**: The customer's credential profile is managed by the integrator or customer using the ICT Encoder Client. They can order blank cards/tags and encoding credits from ICT and encode them with the ICT Desktop Encoder.

  For this option you will need to order:

  - One Managed Site Code license: **PRX-ENC-MSC**
  - The ICT Encoder Client software
  - At least one ICT Desktop Encoder
  - Blank cards or tags
  - The same number of encoding credits

  This document will focus on credentials managed by ICT. For more information about managing and encoding credentials, see the ICT Encoder Client User Guide.

Once your credential profile is set up with ICT it is simple to order more credentials with the same encryption keys and format. Simply order credentials and reference the **CP number** (credential profile number) which was provided with the previous order. If this is not available, provide the site name, site/facility code and information about previous orders to help Customer Services identify your profile.

Custom Mobile Credentials

When you order mobile credentials you can specify that you need custom mobile credentials with a unique encryption key. This will be applied to your mobile credential profile so that all credentials added to that profile will use that encryption key. There is no additional charge for this feature.

The encryption key used for your mobile credentials will typically be different from the keys used for your MIFARE or MIFARE DESFire credentials.

Obtaining the Card Reader Config

The card readers on the site must be programmed with the same encryption keys as the credentials in order to read the right credentials. To program the readers you will need a special reader config (hex code used to program readers) that will achieve that following:

- Add the new encryption keys for MIFARE / MIFARE DESFire credentials
- Add the new encryption keys for mobile credentials (if these are being used)
- Disable the default key set

  If you are transitioning a site from default encryption to custom encryption you may need to leave the default key set active until all cards have been replaced.

- Lock down the reader so that it will not accept further configs

In this case the configs can become very complicated, so you will likely need help from ICT Technical Support to create the correct config. However, once it has been created you can use this config for all card readers installed on the site.

In addition to the config described above, you may also need a **reset config**. This unlocks the reader so that it will accept configs again, allowing you to apply further programming. Then you must lock the reader again using the first config.

There are two methods for programming card readers, depending on the type of card readers you have and what is most convenient for your installation:

- MIFARE Config Cards (can be used for any MIFARE / MIFARE DESFire card readers)
- The Protege Config App (can only be used for readers that support **Bluetooth**® Wireless Technology)

Below are more details about how to obtain the correct config for programming your readers with either of these methods.

For more information about using these programming methods and how to confirm your readers are compatible, see the ICT Card Reader Configuration Guide.

Config Cards

There are two methods for acquiring the correct config card for your credential profile.

Ordering Cards from ICT

You can order one or more config cards from ICT using the order code: **PRX-ISO-CONFIG**

Make sure that you specify the programming that you need on the card, including whether you need mobile credential encryption as well. In addition to the card with the custom credential profile, we recommend that you also order a reset card so that you can unlock the card readers for further programming if required.

Encoding Config Cards

If the credential profile is being managed by the integrator or customer it is possible to encode your own config cards. Several reader configuration records are created by ICT when you order the custom credential profile and will be available in the encoder client.

- You can encode one or more config cards with the **V2 Config** record, which contains the programming for the custom encryption keys.
- It is also recommended that you encode at least one card with the **V2 Config Reset** record so that you can unlock the card readers for further programming if required.

To encode the config card, right click on the reader configuration record and select **Encode**. Place a blank card on the desktop encoder, then click **Write Config**.

You will need to contact ICT Technical Support for assistance in these cases:

- If you are also using mobile credentials with custom encryption (you will need a config which also includes the encryption keys for the mobile credentials)
- If you have created a new custom credential profile and it does not yet have a configuration record available.

Protege Config App

Due to the complexity of the configuration required, you will need to contact ICT Technical Support for assistance with creating the config for the readers. This may require a remote session.

It is recommended that you also request a **reset config** so that you can unlock the card readers for further programming if required.

Programming Card Readers

Finally, you will need to apply the config to all readers on the site.

Before you begin, be aware that using a credential profile config will 'lock down' the reader so that it will no longer accept configuration. If you have any other configs that need to be applied to the reader (e.g. changing the LED colors or output mode), it is recommended that you apply these **before** the custom encryption config.

If you need to program the card readers after they have been locked down, you can unlock the reader by applying the **reset config**. Then you can apply any additional programming and relock the reader by using the original credential profile config.

Programming with a Config Card

Once the required Config Card is available, it can be used to easily program readers.

ICT card readers can only be programmed within 2 minutes of startup. In order to program the reader you will need to disconnect power and complete programming within 2 minutes of powering up.

To program a Card Reader using a Config Card

1. Power cycle the reader to be programmed. The configuration must be completed in the next 2 minutes.
2. To apply the new configuration to the reader, place and hold the config card close to the reader.
3. When programming is successful, the reader will beep 4 times quickly and then restart.

   If the reader beeps 3 times slowly the configuration has failed. Wait for the reader to restart and try again.

Programming with the Config App

Once the required reader config is available in the Config App, it can be applied to individual readers via Bluetooth® communication.

ICT card readers can only be programmed within 2 minutes of startup. In order to program the reader you will need to disconnect power and complete programming within 2 minutes of powering up.

To program a Card Reader using the Protege Config App

1. Activate Bluetooth® on your device.
2. In the Config App, navigate to the **Reader Configuration** page and select the appropriate **Credential Profile**.
3. Tap the required config to apply to the reader. The selected config will be marked as ACTIVE.
4. Power cycle the reader that requires programming. The following steps must be completed in the next 2 minutes.
5. To apply the selected config to the nearest reader, place the device with the app close to the reader and tap **Scan Closest**.
   - The app should display Connecting to reader _R<SERIALNUMBER>. If there is no response, the device may need to be closer to the reader.
   - When programming is successful, the app will display the message Configuration of _R<SERIALNUMBER> successful and the reader will beep several times quickly and then restart.
   - If a power cycle is required, the app will display the message Failed to configure _R<SERIALNUMBER>. Configuration timeout. Please restart the reader.
6. To view and select from a list of nearby readers, tap **Select Reader**.

- If the reader is compatible, its **Broadcast Address** (_R<SERIALNUMBER>) will be displayed in the list.
- If only the reader model is displayed, this reader cannot be configured using the app.
- The number to the right identifies the decibel response. The smaller the value (i.e. the closer to zero), the nearer the reader is to the device.

  The **Bluetooth Proximity** setting in **Mobile Credential Settings** can be adjusted to exclude readers that are further away.

7. Identify the appropriate reader and tap **Apply**.
   - The app should display Connecting to reader _R<SERIALNUMBER>.
   - When programming is successful, the app will display the message Configuration of _R<SERIALNUMBER> successful and the reader will beep several times quickly and then restart.
   - If a power cycle is required, the app will display the message Failed to configure _R<SERIALNUMBER>. Configuration timeout. Please restart the reader.
   - If the reader is not compatible, the app will display the message Failed to configure <READER>. Reader disconnected.

Failed Programming

Sometimes reader programming can fail. This may occur because of Bluetooth® connection interference, such as from the Mobile App, invalid config programming, or incorrect reader firmware.

If programming is unsuccessful the reader will respond with **3 long beeps** (as opposed to the 4 short beeps when programming is completed successfully), and then restart.

If reader programming fails you should attempt to apply the config to the reader again, as the failure may have been caused by temporary interference.

If the reader continues to reject the programming, attempt to apply a previously applied config. Depending on the outcome, the new config may need to be checked or firmware may need to be updated. Previous programming may also need to be reapplied if there is a chance that earlier programming was unsuccessful.

Further Reading

This document is intended only to provide a summary of the process for ordering and using credentials with custom key sets. ICT has a wealth of documentation available covering technical details and additional options for credentials and ICT card readers.

- The ICT Blog includes a number of articles to help you understand the difference between the various credential standards and options.
- ICT Card Reader Configuration Guide
- Protege Config App User Guide
- ICT Encoder Client User Guide
- Application Note 315: Understanding Protege MIFARE DESFire Credentials

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.