PRX-ENC

ICT Encoder Client

User Guide

Last Published: 20-Apr-21 12:34 PM

Contents

Introduction

The ICT Encoder Client is a software application that allows users to encode credentials for use with their ICT tSec Readers, Protege access control system, and optionally other third party systems. This manual provides instructions on encoding credentials with the ICT Encoder Client.

Prerequisites

The following prerequisites are required in order to encode credentials for use with your access control system.

ICT Encoder Client

The Encoder Client must be installed and operational, with the necessary credential profiles configured. A secure operator login is required to set up the software for the first time (see page 7).

Internet Connection

The Encoder Client is a secure cloud-connected application, so internet connection is required. The machine with the desktop encoder installed on it needs to have access to connect out to the site where the service is hosted.

Desktop Encoder

It is assumed that the desktop encoder is already installed and configured on the local machine. You must have the following encoder installed in order to encode credentials:

- PRX-ENC-DT - Desktop USB ISO14443-A and B Proximity Card Encoder

System Preferences

As part of the desktop encoder installation, it needs to be configured under the System Preferences menu in the ICT Encoder Client application. It should be confirmed to be operational by your installer.

If you change machines or access the ICT Encoder Client via remote desktop the System Preferences will need to be updated to reflect the settings of the local machine.

Encoding Credits

You will need sufficient encoding credits for the number of credentials you intend to encode. For additional credits please contact ICT.

- PRX-ENC-100 - Floating Card Encoding Pack (100 Units)
- PRX-ENC-1K - Floating Card Encoding Pack (1,000 Units)
- PRX-ENC-10K - Floating Card Encoding Pack (10,000 Units)

Credentials

The term credential is used to describe an RFID device that has been encoded with data. This can be a card, key tag, disc or RF transmitter with an RFID tag inside. These RFID devices are all credentials that are physically different but electrically identical for the purposes of access control.

Supported Credentials

You will need blank credentials to encode. The following options can be encoded with the ICT Encoder Client:

- PRX-ISO-MF-BLANK - ISO Graphic Printable MIFARE Blank Card
- PRX-ISO-DF-BLANK - ISO Graphic Printable MIFARE DESFire EV1 2K Blank Card
- PRX-ISO-DF-EV2-2K-BLANK - ISO Graphic Printable MIFARE DESFire EV2 2K Blank Card
- PRX-ISO-DF-EV2-4K-BLANK - ISO Graphic Printable MIFARE DESFire EV2 4K Blank Card
- PRX-ISO-DF-EV2-8K-BLANK - ISO Graphic Printable MIFARE DESFire EV2 8K Blank Card
- PRX-ISO-DF-HID26-BLANK - ISO Graphic Printable MIFARE DESFire 125kHz (HID26 Format) Blank Card
- PRX-CLAM-MF-BLANK - Clamshell MIFARE Blank Card
- PRX-TAG-MF-BLANK-B - Black MIFARE Blank Tag
- PRX-TAG-MF-BLANK-W - White MIFARE Blank Tag
- PRX-TAG-DF-EV2-B-BLANK - Black MIFARE DESFire Blank Tag

Credential Profiles

To encode a credential you need a credential profile.

Your integrator will configure these based on your company's encoding requirements.

A credential profile stores the site code and card number data that you want to encode onto the card, as well as the credential formats which define how data is loaded onto the physical credential. Depending on the format this might include encryption keys that specify how data is encoded.

- You encode a card with a credential profile.
- The profile holds the information you want to encode.
- Credential profiles are made up of credential formats.
- The format defines how the data will be encoded onto the credential.
- Credential formats may contain encryption keys to encrypt and decrypt the data.

A credential profile can contain a mixture of technologies if the reader you are using is capable of decoding both technologies.

Getting Started

Operator Registration

Operation of the ICT Encoder Client requires a secure Operator Login.

If you have not yet registered with ICT you will need to complete the registration process to obtain your login details. Please contact ICT Technical Support for assistance registering for your secure operator login.

After the initial operator registration has been completed, new users will be provided with a temporary password in an invitation email. You must use this password to log in at least once, at which point you will be prompted to change the password.

Logging In

1. Navigate to **Operator | Login** and enter your **User** and **Password** details.
2. Click **Login**.
3. If this is your first time logging in you will be prompted to change your password.
4. Enter a secure password (see below).

If you want to change your password again in the future, navigate to **Operator | Change Password** and enter your current and new password details, then click **Apply** to update.

Login Error

If you are attempting to log in to the ICT Encoder Client application and receive a Login Error, this could mean the application is being prevented from reaching the external cloud service by a firewall or internal IT policy.

If you are certain that you are entering the correct login credentials please check with your IT provider first, and then contact ICT Technical Support for assistance.

Creating a Secure Password

When creating or changing the operator password it is **highly recommended** that you create a very secure password.

As a guideline, a secure password should include these features:

- Minimum 8 characters in length
- Combination of upper and lower case letters
- Combination of numbers and letters
- Inclusion of special characters

Change Password

1. Navigate to **Operator | Change Password**.
2. Enter your **Current Password**.
3. Enter and confirm your **New Password**, in accordance with the secure password requirements.
4. Click **Apply**.

Password Recovery

If you have lost or cannot remember your password you can use the password recovery process.

1. Navigate to **Operator | Login** and click **Lost Password**.
2. Enter your **E-Mail Address** and **User Login** and click **Reset**. A temporary password will be emailed to you.

If you have changed email address or are having other issues with receiving the password recovery email, please contact ICT Technical Support for assistance.

Updating the Software

When you log in, the ICT Encoder Client automatically checks to ensure you are using the most recent version. If not will prompt you to download the latest release. This is a very simple process. The system will download a zipped file that contains the installers for the software.

If you are prompted to download and update the ICT Encoder Client, you must complete this task before you can finish logging in to the system.

1. Download the installer to a directory on your machine when prompted by the ICT Encoder Client.
2. Once the installer has downloaded, open the file location and extract the contents of the ZIP file.
3. Open the Windows Settings and navigate to **Apps & Features**. Locate the ICT Encoder Client in your installed applications list, click on it and select **Uninstall**.
4. A restart of your computer may be required, and we recommend doing this prior to completing the install.
5. After you have successfully uninstalled the previous version, run the new **MSI** installation file and follow the on-screen instructions.
6. Open the ICT Encoder Client from the start menu and complete the login process.

Logging Out

For security reasons it is recommended that you log out of the ICT Encoder Client when finished. To log out, navigate to **Operator | Logout**.

Basic Navigation and Record Types

Once logged in you will arrive at the **Credential Manager** screen. This is the home screen where you can manage and encode credentials.

Operator Menu

The **Operator** menu allows you to manage your password and log out.

Change Password

To change your password simply enter you current password, then enter and confirm your new password.

Passwords must conform to the minimum complexity requirements.

Logout

Select **Logout** to log out of the Encoder Client. It is recommended that you log out whenever not using the Encoder Client, to preserve security restrictions for other users.

System Menu

The **System** menu provides access to configuration options and card tools.

Access to these features is dependent on your assigned operator security level.

Tools | Card Explorer

The Card Explorer provides useful tools for managing cards and card data.

- **Scan Card**: Read the encoded data on a card.
- **Tools | Format Card**: Allows you to format a DESFire card, if you have the master key for the card.

  This tool is helpful when testing to allow reformatting of cards instead of replacing them.
- **Tools | Diversification**: Allows allows you to configure a symmetric key diversification scheme* so that you can read, encode or validate cards.

  * For more information, refer to https://www.nxp.com/docs/en/application-note/AN10922.pdf

  These tools are useful when trying to decipher a card format in the case of third-party integration.
- **Export**: Generate a report of a scanned card.
- **Setup Keys**: Customize card configuration by adding or removing encryption key sets.

Tools | Card Functions

The Card Explorer provides useful tools for managing cards and card data.

- **Reset Sector**: Reset a single sector on a MIFARE card.
- **Reset Card**: Reset every sector on a MIFARE card.

Preferences

Configure encoding and printing devices.

About

Displays version information.

Organisation

There are three levels of organisation, displayed within the **Organisation** menu tree:

- Company
- Operators within a company
- Customers assigned to a company

If you have access to multiple companies you will be prompted to select the company you want to open when you log in. You can always select another company via the menu once you are logged in.

Company

The first level of the credential manager organization menu tree is the Company. This represents the business or entity that credentials will be encoded for.

Right click on the Company and select **Properties** to view company information, including the remaining available Encoding Credits.

Encoding credits are purchased and consumed at the **company** level, not for a particular **customer** or site.

Operators

The next level of the menu tree displays the Operators who have access to encode credentials for this company. If you have the necessary security access you can view and assign operator access levels from this menu.

Although there is a warning, it is possible for an administrator to create duplicate operators by assigning the same email address to a second operator. This also creates a duplicate company record. This is a known issue.

Customers

Customers are organizational structures within a company, used to configure credential format and profile options at a site level. A company may have only one customer, or may have several customers to represent multiple sites and credential encoding configurations.

Configuration

Within the setup of each customer there are a number of configuration components that must be defined before credentials can be encoded:

Your installer will configure these settings based on your company's encoding requirements.

- **Encryption Keys** are used to encrypt and decrypt the credential data. Keys are available for a variety of encryption methods, including Crypto 1, which is used for NXP MIFARE sector based keys, and AES128 and AES256, used for higher security cards such as DESFire EV1/EV2 and MIFARE Plus EV1.

  An encryption key is used in a credential format to encrypt or decrypt data.

- **Credential Formats** define how data is loaded onto the physical credential. You can specify the RFID technology such as MIFARE, 125 Prox or DESFire. The credential format also defines how the data will be encoded and where it needs to be written to. This could be the sector location for MIFARE, or the file or application location for DESFire.

  The credential format uses encryption keys to encode the data and configure security parameters.

- **Credential Profiles** contain the site code and card number that will be encoded on the credential. The credential profile is used to encode a credential. A credential profile is made up of one or more credential formats. For example, you can encode the ICT format into one sector, open formats into another sector to accommodate third-party applications, and additional custom data into other sectors as needed.

- **Reader Configuration** is used to configure reader settings that may be required to set up card readers. This might include LED colors, controller interface programming, and settings to allow certain cards to be read.

Encoding Credentials

In order to encode a credential you will need:

- An operational **ICT Encoder Client** with configured **Credential Profile**
- A correctly configured **Desktop Encoder**
- Blank **Credentials** to encode
- Sufficient **Encoding Credits**

System Preferences

To view your **Desktop Encoder** and its configuration, navigate to **System | Preferences**.

If you change machines or access the ICT Encoder Client via remote desktop the System Preferences will need to be updated to reflect the settings of the local machine.

Encoding Credits

Encoding credits are required to encode a credential and operate as a form of encoding currency. To view your available credits right click on the Company and navigate to **Properties**.

If you require additional credits please contact ICT.

Encoding Process

To encode a credential you must select a Credential Profile. The credential profile stores the site code and card number that will be encoded on the credential, as well as the credential formats which contain the encryption.

1. To encode a credential, first place it on the **desktop reader**.
2. Double click the **credential profile** to encode it with. You can also right click the credential profile and select **Encode.**
3. The **Encode** screen will display the **Next Card** number. This is the identification number that will be encoded on the credential and you will need to record this number to assign to the **user** the encoded credential is given to.
4. On the encode screen select **Execute**.

   If the card number has previously been issued for this site the **Issue Error** will be displayed. If you think you might have accidentally duplicated a card please contact ICT Technical Support for assistance.

5. As the encoding takes place the progress information is shown on the **Details** screen. The messages Writing passed and Credential Encoding Finish will display when successfully completed.

   When the credential is successfully encoded the card number will increment by 1.

6. The credential can be removed from the encoder once successfully encoded.
7. The **card number** will need to be assigned to the appropriate **user** in your system software. The newly encoded credential will not be recognized by your access control system until it is assigned to a valid user.

If you encounter any problems or errors during the encoding process please contact ICT Technical Support.

Configuration Cards

The ICT Encoder Client provides the ability to create customized configuration cards that can be used to program the functions of a tSec Reader.

The **Reader Configuration** option enables you to encode a single MIFARE Classic card with a configuration setting, and then badge it at any compatible tSec Reader to program that reader.

This allows you to update settings quickly and efficiently to readers on a site without needing to pull each reader off the wall and connect to it directly.

Requirements

To program a reader with a configuration card:

- You will need a blank MIFARE Classic card to encode. These can be ordered from ICT: PRX-ISO-MF-BLANK.
- The tSec Reader to be programmed should be firmware version 1.04.229 or higher .

Config cards can be re-written with a new configuration after use. However, cards encoded as regular credentials cannot be encoded with a reader configuration.

Reader Configurations

To encode a card that will be used to program readers you must first create a Reader Configuration. This configuration contains the settings that will be applied to the reader.

You can add multiple settings to a Reader Configuration, and you can edit the properties of your Reader Configuration to add, remove or change settings when needed.

Creating a Reader Configuration

To create the Reader Configuration that will be encoded on your Configuration Card:

1. Navigate to the **Customer** level of the site you need to create the Configuration Card for.
2. Right click on the **Reader Configuration** option and click **New Config**.
3. Enter a **Name** for your configuration. This should clearly describe the programming function, including specific options and settings.
4. In the **Configuration Properties** click **Add**.
5. From the drop-down menu select the required **Setting** for the function you want to program.
6. Next, select or enter the setting variation option. This will vary depending on the setting you have chosen.
7. Click **OK** to finalize your selection, then **Save** your configuration.

If you are unsure about any of the settings or options you should contact ICT support before continuing.

Basic Settings

The following settings cover the most common configurations for reader programming.

- **LED Mode**: Set the reader to use Blue ON, Green ON, or Dual LED mode.
- **Backlight Setting**: Adjust the keypad backlight brightness level.
- **Output/Interface Mode**: Set the reader to output in Wiegand, ICT Smart Reader (RS-485), or a Custom Serial (RS-485) format.

  OSDP output mode can also be programmed, using a custom format. For information on programming config cards to enable OSDP, refer to the ICT Encoder Client User Guide.

- **Wiegand Format Definition**: Set the data format the reader will use when sending card data over RS-485 or Wiegand.
- **Keypad Format Definition**: Set the data format the reader will use when sending PIN data over Wiegand ONLY.
- **Wiegand Site Code**: The site code to send when using Keypad Formats that can send a site code.
- **Low Frequency Prox Options**: Enable/Disable reading of various low frequency formats.
- **Clone Card Options**: Enable/Disable clone card reading and clone card destroy.
- **Card Serial Number Reading**: Enable/Disable reading of CSN for MIFARE, DESFire, and other NFC cards.

Advanced Settings

The following settings include more advanced configurations that affect critical reader operation.

Important: It is possible to prevent a reader from reading cards, **INCLUDING CONFIGURATION CARDS**, using some of these settings. Only use advanced configuration settings if you have been instructed to do so by ICT Technical Support. If you are not certain please get in touch with the Technical Support team.

- **Bluetooth Power Output**: Manually set the power that the BLE module outputs, effectively controlling the Bluetooth reading range for the reader.

  Changing this setting can cause the Bluetooth on a reader to stop working.

- **Custom RS485 Format**: Specifies the RS-485 format to use if the reader has been set to Custom Serial Output Mode.
- **Custom Card Format**: Allows the entry of a custom format string which describes how to interpret data from the card being read.

  Changing this setting can stop a reader from reading cards. Consult ICT Support before using this setting.

- **Encryption Key Slot**: Used to load custom Encryption Keys onto the reader. Must be used in conjunction with Credential Type and Credential Format Link settings.
- **Credential Type**: Used to configure the details of reading of different types of credentials.

  Changing this setting can stop a reader from reading cards. Consult ICT Support before using this setting.

- **Credential Format Link**: Used to link Credential Types, Custom Card Formats, and Encryption Keys.

  Changing this setting can stop a reader from reading cards. Consult ICT Support before using this setting.

Custom Settings

The following settings relate to obsolete or custom operations and are not applicable to most users.

- **MIFARE Classic Sector** (Legacy): Obsolete firmware only.
- **PSK Decryption**: Custom reader hardware only.
- **UHF Power Output**: Custom reader hardware only.
- **Smart Serial Address**: Custom reader firmware only.

Encoding a Config Card

A blank MIFARE Classic card can be easily encoded with a Reader Configuration from the ICT Encoder Client.

It is assumed that the desktop encoder is already installed and configured on the local machine. You must have the following encoder installed in order to encode a Config Card:

- PRX-ENC-DT - Desktop USB ISO14443-A and B Proximity Card Encoder

Requirements

To encode a Config Card you will need:

- A **Reader Configuration**
- A correctly configured **Desktop Encoder**
- A blank MIFARE Classic **Card** to encode. These can be ordered from ICT: PRX-ISO-MF-BLANK.

  Config Cards are re-writable, so you can overwrite an existing Config Card with a new configuration.
- Sufficient **Encoding Credits**. Each card encoded consumes one encoding credit.

System Preferences

To view your **Desktop Encoder** and its configuration, navigate to **System | Preferences**.

If you change machines or access the ICT Encoder Client via remote desktop the System Preferences will need to be updated to reflect the settings of the local machine.

Encoding a Config Card

To encode a Config Card with your customized Reader Configuration:

1. Navigate to the **Customer** level for the site that you need to create the Config Card for.
2. Right click on the **Reader Configuration** option and select **Encode**.
3. Place your MIFARE Classic card on the **Encoder**.
4. Click **Write Config**.
5. Wait for the dialog to display "Reader configuration programming success".

Programming a tSec Reader

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

tSec 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 tSec 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 5 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.

Reader Configuration Examples

The following examples illustrate programming a config card with some common tSec Reader configuration requirements, using the ICT Encoder Client.

Enable OSDP

The following programming example demonstrates how to create a config card that enables the tSec Reader to use the OSDP communication protocol.

1. Log in to the ICT Encoder Client using your secure operator login.
2. Select the required **Customer**.
3. Right click the **Reader Configuration** component and create a **New Config** called OSDP Output Mode.
4. Click the **Import** button to create a custom format.
5. In the **Custom Format** field, enter the OSDP Output Mode Hex code **`0B0104`**.
6. **Save** the custom format, then **Save** your configuration.
7. Right click your new OSDP Output Mode config and click **Encode**.
8. Place your blank MIFARE Classic card on the desktop encoder.
9. Click **Write Config** and wait for the 'programming success' message.

You can now apply the configuration to the required reader(s). Power cycle the reader, and within two minutes place and hold the OSDP Output Mode config card close to the reader.

For more information on configuring OSDP, see AN-321: Configuring tSec Readers for OSDP Communication.

ISO14443 Gain for DESFire EV2 Tags

To read DESFire EV2 tags, the ISO14443 gain should be set to 6. Some tSec Reader firmware versions do not contain the required ISO14443 gain configuration by default, so it is necessary to program the configuration.

1. Log in to the ICT Encoder Client using your secure operator login.
2. Select the required **Customer**.
3. Right click the **Reader Configuration** component and create a **New Config** called ISO14443 Gain for EV2 Tags.
4. Click the **Import** button to create a custom format.
5. In the **Custom Format** field, enter the ISO14443 Gain 6 Hex code **`180106`**.
6. **Save** the custom format, then **Save** your configuration.
7. Right click your new ISO14443 Gain for EV2 Tags config and click **Encode**.
8. Place your blank MIFARE Classic card on the desktop encoder.
9. Click **Write Config** and wait for the 'programming success' message.

You can now apply the configuration to the required reader(s). Power cycle the reader, and within two minutes place and hold the ISO14443 Gain for EV2 Tags config card close to the reader.

Enable Dual LED Mode

By default tSec Readers are operate in single LED mode (when wired in Wiegand configuration). To enable dual LED mode, you need to change its configuration. For more information, see Wiegand Connection (page 1).

1. Log in to the ICT Encoder Client using your secure operator login.
2. Select the required **Customer**.
3. Right click the **Reader Configuration** component and create a **New Config** called Dual LED Mode.
4. Click **Add** and select the **LED Mode** option.
5. Set the **LED Mode** to Dual LED Operation, then click **Ok**.
6. **Save** your configuration.
7. Right click your new Dual LED Mode config and click **Encode**.
8. Place your blank MIFARE Classic card on the desktop encoder.
9. Click **Write Config** and wait for the 'programming success' message.

You can now apply the configuration to the required reader(s). Power cycle the reader, and within two minutes place and hold the Dual LED Mode config card close to the reader.

Set Wiegand Output Mode

By default, tSec Readers are configured to output Wiegand data. However, if the reader is ever connected to a reader expander configured to use RS-485, the reader will switch into RS-485 communication mode. If you want to use the reader's Wiegand output again, you need to change its configuration.

1. Log in to the ICT Encoder Client using your secure operator login.
2. Select the required **Customer**.
3. Right click the **Reader Configuration** component and create a **New Config** called Wiegand Output Mode.
4. Click **Add** and select the **Output/Interface Mode** option.
5. Set the **Interface Mode** to Wiegand Output, then click **Ok**.
6. **Save** your configuration.
7. Right click your new Wiegand Output Mode config and click **Encode**.
8. Place your blank MIFARE Classic card on the desktop encoder.
9. Click **Write Config** and wait for the 'programming success' message.

You can now apply the configuration to the required reader(s). Power cycle the reader, and within two minutes place and hold the Wiegand Output Mode config card close to the reader.

Enable CSN Reading Mode

By default, tSec Readers will read ICT secured formats from high frequency cards. However, for lower security sites using third-party cards it can be useful to read and send the Card Serial Number (CSN) instead.

WARNING: The CSN of your MIFARE card can be read and duplicated by anyone with access to the card. It is not recommended to use CSN reading on high security sites.

1. Log in to the ICT Encoder Client using your secure operator login.
2. Select the required **Customer**.
3. Right click the **Reader Configuration** component and create a **New Config** called CSN Reading Mode.
4. Click **Add** and select the **Card Serial Number Reading** option.
5. Select all the appropriate CSN Reading options to enable, then click **Ok**.
6. **Save** your configuration.
7. Right click your new CSN Reading Mode config and click **Encode**.
8. Place your blank MIFARE Classic card on the desktop encoder.
9. Click **Write Config** and wait for the 'programming success' message.

You can now apply the configuration to the required reader(s). Power cycle the reader, and within two minutes place and hold the CSN Reading Mode config card close to the reader.

Appendix: Operator Security Levels

Security levels determine the features and functions that an operator has access to. Operators are assigned a security level of User, Manager or Administrator. The functions they can perform are listed below.

Action	User	Manager	Administrator
Encode Credentials	✓	✓	✓
Edit Card Numbers when Encoding Credentials *	✓	✓	✓
Encode Reader Configurations	✓	✓	✓
Card Explorer	✓	✓	✓
System Preferences (Configure Card Encoder)	✓	✓	✓
Generate Credential Profile Encoding Audit Reports	✗	✓	✓
Add/Edit Customers	✗	✓	✓
Add/Edit Credential Formats	✗	✓	✓
Add/Edit Credential Profiles	✗	✓	✓
Add/Edit Reader Configurations	✗	✓	✓
Register Credential Profiles	✗	✓	✓
Assign Operator Security Levels	✗	✗	✓
Generate Company Encoding Audit Reports	✗	✗	✓
Card Explorer Tools	✗	✗	✓
Card Functions	✗	✗	✓
Delete Customers	✗	✗	✓
Delete Credential Formats	✗	✗	✓
Delete Credential Profiles	✗	✗	✓
Delete Reader Configurations	✗	✗	✓
Add/Edit/Delete Encryption Keys	✗	✗	✓

An operator can be assigned to multiple companies and have different security levels in each company.

* Card numbers can only be edited if this option has been enabled in the corresponding configuration profile.

Disclaimer and Warranty

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.

For warranty information, see our Standard Product Warranty.

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