

**tSec Multi-Technology Card Reader
Installation Manual**

ICT[®]eSecurity.

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited. Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2015. All rights reserved.

Publication Date: May 2016

Contents

1	Welcome	5
1.1	Document Conventions	5
2	tSec Editions	6
3	Mifare Technology	7
3.1	About Mifare	7
3.2	Mifare Modules	7
	Readers	7
	Cards	7
3.3	About ICT Secured Mifare Card Format	8
	Readers	8
3.4	About Mifare DESFire EV1	8
	Readers	8
	Cards	8
4	Mounting	9
4.1	Mounting Instructions	9
5	Wiegand Connection	10
6	RS-485 Connection	11
7	Installer Programming	12
7.1	Entering RS-485 Programming Mode	12
7.2	Entering 125kHz Programming Mode	12
7.3	125kHz Reading Mode	13
7.4	DESFire Reading Mode	14
7.5	Mifare Reading Mode	14
7.6	Interface	15
7.7	LED Function	15
7.8	Backlight	16
7.9	Default Sector	16
7.10	Encryption Keys	16
7.11	Custom Format	17
7.12	Intelligent Tamper	18
7.13	Factory Reset	18
7.14	Output Mode	18
7.15	Clone Card Notify	18
7.16	Clone Card Reading	18

7.17	Clone Card Destroy	19
7.18	Custom RS-485 Format	19
7.19	Save and Restart	20
8	Technical Diagram	21
9	Technical Specifications	22
10	New Zealand and Australia	23
11	European CE and EN 50131	24
12	UL and ULC Installation Requirements	25
12.1	CAN/ULC-S319-05.....	25
12.2	UL294	25
13	FCC Compliance Statements	26
14	Industry Canada Statement	27
15	Ordering Information	28
16	Warranty	29
17	Contact	30

1 Welcome

Thank you for choosing the tSec Card Reader from Integrated Control Technology. The tSec Reader is an advanced technology high frequency smart card radio frequency identification device (RFID) specifically designed to enhance the functionality of security, building automation and access control by providing multiple format compatibility, high speed data transmission and sabotage protection.

The tSec Reader is designed to operate as a Wiegand Proximity Reader or using Intelligent RS-485 Communications, and can be programmed to read and output different card formats.

Before installing this product, we highly recommend you read this manual carefully and ensure that the data formats you program will operate with the configured access control or security product.

Current features include:

- Multi card technology provides support for DESFire, Mifare, and 125KHz cards
- Encrypted RS-485, un-encrypted configurable RS-485 or standard Wiegand connection
- Keep alive transmission every 30 seconds for intelligent tamper management
- Fully encapsulated design with environment IP Rating of IP65 for outdoor and indoor operation
- Bi color LED (blue and green) with independent or single LED control
- Programmable via programming cards with a range of Wiegand formats including 26 bit and 34 bit
- Keypad output on Wiegand data using ARK501 format (keypad versions only)
- Read range up to 60mm (2.36") with proximity ISO cards

For more information on the tSec Card Reader range and other Integrated Control Technology products please visit the ICT website (<http://www.ict.co>).

1.1 Document Conventions

This document uses the following conventions:



Important warnings or cautionary messages to prevent equipment damage, data loss, or other similar conditions



Notes with additional information such as an explanation, a comment, or a clarification about the subject



Tips containing practical information that may help you solve a problem or describing actions that may save you time



Information relating to UL and ULC compliance



Bold text enclosed in brackets is used to show a section number or address of a programmable option or information on programming shortcut sequences

2 tSec Editions

The tSec Reader comes in three main editions (Standard, Extra, and Mini) and with a range of optional features. Each edition supports either 125KHz, Mifare/DESFire cards or both. The Standard and Extra have the option of a keypad. All models are available in either black or white.

	Keypad	125KHz	Mifare/DESFire
Standard			
PRX-TSEC-STD tSec Standard Card Reader		✓	✓
PRX-TSEC-STD-KP tSec Standard Card Reader with Keypad	✓	✓	✓
PRX-TSEC-STD-125 tSec Standard 125KHz Card Reader		✓	
PRX-TSEC-STD-125-KP tSec Standard 125KHz Card Reader with Keypad	✓	✓	
PRX-TSEC-STD-DF tSec Standard DESFire Card Reader			✓
PRX-TSEC-STD-DF-KP tSec Standard DESFire Card Reader with Keypad	✓		✓
Extra			
PRX-TSEC-EXTRA tSec Extra Card Reader		✓	✓
PRX-TSEC-EXTRA-KP tSec Extra Card Reader with Keypad	✓	✓	✓
PRX-TSEC-EXTRA-125 tSec Extra 125KHz Card Reader		✓	
PRX-TSEC-EXTRA-125-KP tSec Extra 125KHz Card Reader with Keypad	✓	✓	
PRX-TSEC-EXTRA-DF tSec Extra DESFire Card Reader			✓
PRX-TSEC-EXTRA-DF-KP tSec Extra DESFire Card Reader with Keypad	✓		✓
Mini			
PRX-TSEC-MINI tSec Mini Card Reader		✓	✓
PRX-TSEC-MINI-125 tSec Mini 125KHz Card Reader		✓	
PRX-TSEC-MINI-DF tSec Mini DESFire Card Reader			✓

3 Mifare Technology

3.1 About Mifare

Based on the international standard ISO/IEC 14443 Type A, Mifare is a technology used for contactless RFID smart card systems consisting of card and reader components.

The most widely deployed RFID technology in the world and used in thousands of diverse applications, Mifare has established an excellent reputation as a technology that delivers convenience and flexibility for contactless RFID.

- Fully compliant with the international standard ISO/IEC 14443 Type A
- Proven and reliable, with more than 1 billion smart card ICs and 7 million reader components sold Mifare has a market share of 80% in the automatic fare collection industry (Source: Frost & Sullivan 2001)
- Future-proof product portfolio covering reader components as well as contactless and dual interface smart card ICs
- Multi-application memory to store several services on the same card allowing many integration possibilities
- Fast transaction speed
- High security and fraud protection

3.2 Mifare Modules

The Mifare products can be expanded to accommodate large numbers of modules using the encrypted RS-485 Network. Modules that are currently available are listed below. Integrated Control Technology provides a number of reader and tag/card options in the Mifare range. You can take advantage of the ICT Mifare product range while transitioning from legacy equipment using our dual technology cards which feature both low security formats and Mifare. For more information, please contact our support team (see page 30).

Readers

- Mifare Desfire Nano Proximity Card Reader (PRX-NPROX-DF)
- tSec Multi-Technology Standard Card Reader (PRX-TSEC-STD)
- tSec Multi-Technology Standard Card and PIN Reader (PRX-TSEC-STD-KP)
- tSec Multi-Technology Extra Card Reader (PRX-TSEC-EXTRA)
- tSec Multi-Technology Extra Card and PIN Reader (PRX-TSEC-EXTRA-KP)
- tSec Multi-Technology Mini Card Reader (PRX-TSEC-MINI)

Cards

- Mifare 1K (S50) Proximity Clamshell Card (PRX-CLAM-MF)
- Mifare 1K (S50) Proximity Card ISO (PRX-ISO-MF)
- Mifare 1K (S50) Proximity Card ISO Mag (PRX-ISO-MAG-MF)
- Mifare 1K (S50) Proximity Standard Key Tag (PRX-TAG-MF)
- Mifare 1K (S50) Proximity Blue Key Tag (PRX-TAG-MF-BLU)
- Mifare Desfire EV1 Proximity Card ISO 2K (PRX-ISO-DF)
- Mifare Desfire EV1 Proximity Blue Key Tag 2K (PRX-TAG-DF-BLU)

3.3 About ICT Secured Mifare Card Format

ICT Secured Mifare is the compromise between secured card and cost. Card data is protected with a diversified authentication key and encrypted with an AES256 algorithm. These cards are not as secure as DESFire EV1 but still provide high security against cloning. This card mode can be used on all Mifare 1K (S50) cards and tags.

Readers

- Mifare Desfire Nano Proximity Card Reader (PRX-NPROX-DF)
- tSec Multi-Technology Standard Card Reader (PRX-TSEC-STD)
- tSec Multi-Technology Standard Card and PIN Reader (PRX-TSEC-STD-KP)
- tSec Multi-Technology Extra Card Reader (PRX-TSEC-EXTRA)
- tSec Multi-Technology Extra Card and PIN Reader (PRX-TSEC-EXTRA-KP)
- tSec Multi-Technology Mini Card Reader (PRX-TSEC-MINI)

3.4 About Mifare DESFire EV1

Mifare DESFire EV1 is an ideal solution for service providers wanting to use multi-application smart cards in transport schemes, e-government or identity applications. It complies fully with the requirements for fast and highly secure data transmission, flexible memory organization, and interoperability with existing infrastructure.

- Fully compliant with the international standard ISO/IEC 14443 Type A 1-4
- Available in 2, 4 and 8 Kbytes EEPROM version with fast programming
- Secure, high speed command set
- Unique 7-byte serial number
- Open DES/3DES crypto algorithm in hardware
- Open AES 128 bits crypto algorithm in hardware

Mifare DESFire EV1 provides many benefits to end users. Cardholders can experience convenient contactless ticketing while also having the possibility to use the same device for related applications such as payment at vending machines, access control, or event ticketing. In other words, the Mifare DESFire EV1 solution offers enhanced consumer-friendly system design, in combination with security and reliability.

Readers

- Mifare Desfire Nano Proximity Card Reader (PRX-NPROX-DF)
- tSec Multi-Technology Standard Card Reader (PRX-TSEC-STD)
- tSec Multi-Technology Standard Card and PIN Reader (PRX-TSEC-STD-KP)
- tSec Multi-Technology Extra Card Reader (PRX-TSEC-EXTRA)
- tSec Multi-Technology Extra Card and PIN Reader (PRX-TSEC-EXTRA-KP)
- tSec Multi-Technology Mini Card Reader (PRX-TSEC-MINI)

Cards

- Mifare DESFire EV1 Proximity Card ISO 2K (PRX-ISO-DF)
- Mifare DESFire EV1 Proximity Blue Key Tag 2K (PRX-TAG-DF-BLU)

4 Mounting

The TSEC Reader is intended to provide the reading component of access control, time and attendance and alarm systems. It is intended to be mounted on a wall with adequate air flow around and through it.

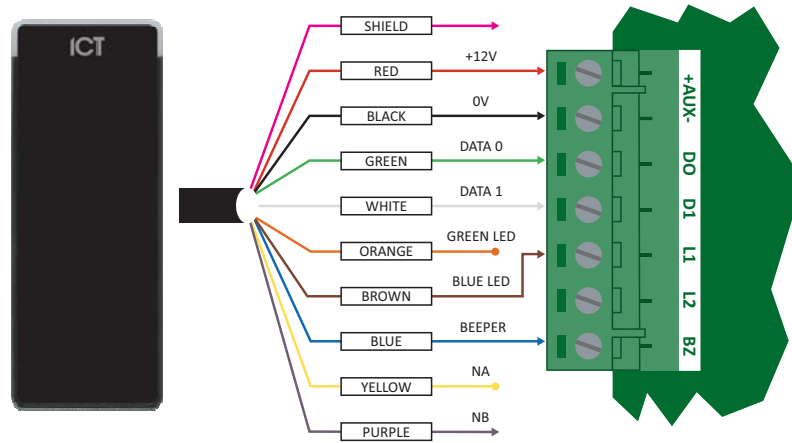
4.1 Mounting Instructions

1. Select where to mount the reader, ensuring it is mounted a minimum of 1.1m (3.5ft) away from other wiring, such as ACM power, computer data wiring, telephone wiring and wiring to electric lock devices. Use the template sticker provided in the kit as a guide to correctly position the unit.
2. Hold the rear case half against the wall and mark the mounting holes and cable entry area. The cable entry area should align with a hole cut through the plaster wall-board. Cables are intended to be run inside the wall. Use appropriate screws (not supplied) to affix the case to the wall.
3. Run the wiring. Refer to later sections of this manual for the electrical connections. Leave about 20cm (8") of wire protruding through the center of the mounted half of the case.
4. Connect the wiring to the reader electronics, then use the top case to press gently on the bottom mounted case until the screw hole for securing the top and bottom case together lines up.
5. To complete the installation, use the M3 x 8mm Plastite screw provided in the kit to secure and fasten the top case to the bottom mounted case.

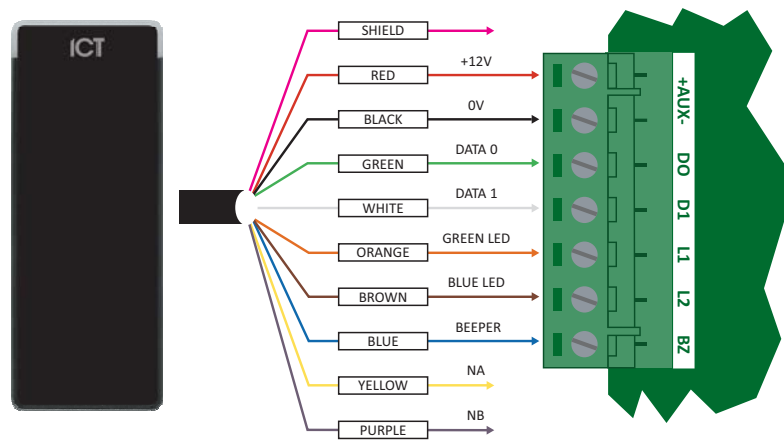
5 Wiegand Connection

Readers are shipped in Single LED mode by default.

When using the standard Wiegand Interface to the access controller or reader expander two wiring methods can be used. Dual LED operation allows the signalling of both LEDs independently using the LED control lines and is ideal to show the status of alarm or other integrated signals. Single LED allows a single LED line to control both LED colors.



Single LED Connection (Default)



Dual LED Connection

Using the recommended cables as listed under the Technical Specifications, splice these cables together with the pigtail of the reader and seal the splice. Route the cable from the reader to the host controller. Connect the cables as shown in the diagrams above for either Dual LED Operation or Single LED Operation.



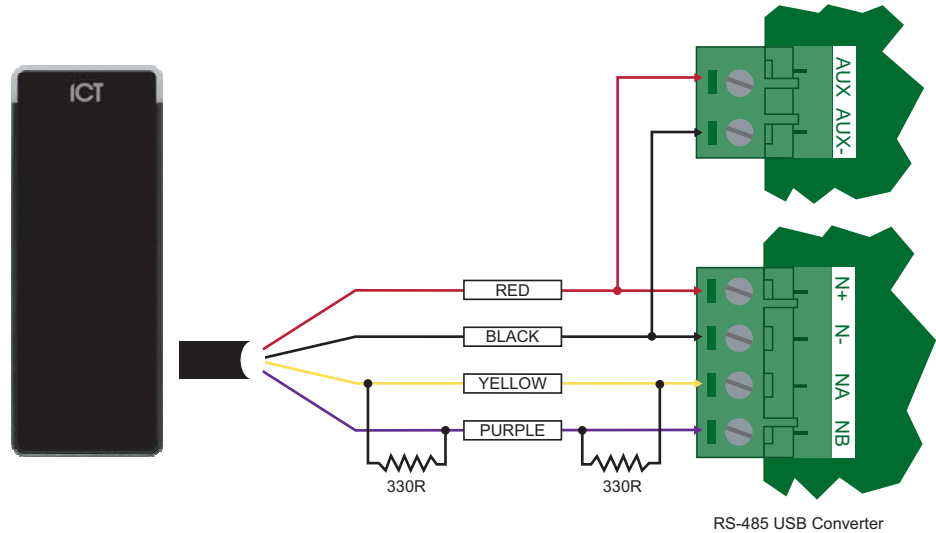
Connect the reader shield to a suitable earth point. DO NOT connect the shield to a ground or AUX connection. DO NOT connect the shield wires together at the reader cable splice. With the shield wire already terminated at the reader terminate the shield at the controller.



Compatible access control card reader communication formats are: 26-, 34-, and 37-Bit Wiegand.

6 RS-485 Connection

Connection of an RS-485 Interface allows the TSEC Reader to communicate using an intelligent protocol or to send data to an ASCII capable terminal. The connection diagram below shows the interface requirements. When connected in this way, the other wires should not be connected to ground and be appropriately isolated.



RS-485 Interface



Connect the reader shield to a suitable earth point. DO NOT connect the shield to a ground or AUX connection.



Warning: When connecting the Reader in RS-485 Mode you must isolate all unused wiring. DO NOT terminate any unused connections to ground or a voltage or to another connection. Doing so may damage the unit and will void any warranty.



A 330 Ohm EOL (End of Line) resistor MUST be inserted between the NA and NB terminals of the Reader and a second 330 ohm EOL resistor must be inserted between the NA and NB terminals at the other end of the wiring.



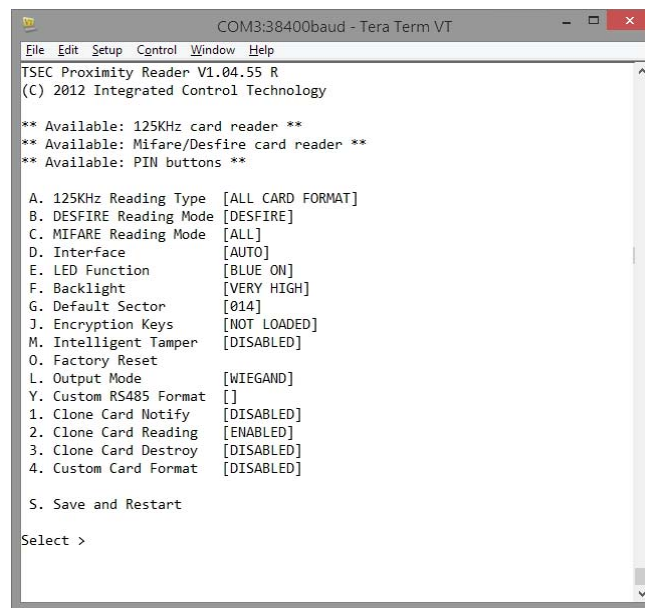
The RS-485 Connection has not been evaluated for UL/ULC installations.

7 Installer Programming

The tSec readers utilize built in programming functions that enable options to be configured via an RS-485 Serial Interface. 125kHz capable tSec readers can also be programmed using a Nano/Vario 125kHz programming card. These cards cannot be used to program the 13.56MHz series of tSec readers.

7.1 Entering RS-485 Programming Mode

1. Complete the wiring connections as shown for using an RS-485 USB Converter (see page 11).
Ensure that the unconnected wires are not shorting to each other or any other connection point. You can still configure the units if they are terminated to a reader interface you will require the +, - and NA, NB connections to be connected to the RS-485 USB Converter.
2. Power up the card reader and RS-485 USB Converter.
3. Open Hyper Terminal or a similar serial terminal program, set the communications port to the RS-485 USB Converter and set the parameters to 38400, N, 8, 1 and VT100 terminal emulation.
4. Make a short between the brown and white wires together and power up the reader. A configuration menu will appear.



Data entry and the menu will time out after 40 seconds of no activity and restart the reader, any programming changes will be lost.

7.2 Entering 125kHz Programming Mode

Applies to the 125kHz series of tSec readers only.

125kHz programming mode is entered by presenting a PRX-PROG-LF (Programming Card - Nano/Vario 125kHz) to the unit within the first 2 minutes of power being applied. The reader beeps twice to indicate 125kHz programming mode has been entered.



Data entry and the menu times out after 2 minutes of no activity and reverts back to normal activity, any programming changes will be lost.

To program the reader using 125kHz mode:

1. Present the card to the reader the number of times matching the data value option for the selected address.
2. Wait for the reader to beep twice.
3. Present the card the required number of times to set the desired option (as outlined by the 125kHz setting column in the tables below).
4. Wait for the reader to beep twice indicating the data has been programmed correctly. At this stage the reader is waiting for a new address to program.
5. If additional settings are required, repeat the above steps.

An invalid entry will result in a long tone being generated. The data can be entered again or allow the reader to timeout to select another address.

6. Once complete, leave the programming interface to time out.

Example: To program Address 1 (Card/Tag Format), present the programming card to the reader once. The card reader will respond by beeping twice to indicate data entry mode has been entered and that you can present the card the required number of times to set the desired option.

Address	Programming Options
1	Card Reading Format
2	Data Output Format
4	Intelligent Tamper Mode
6	PIN Data Interface
12	Restart Only

7.3 125kHz Reading Mode

Reading mode determines how the data on the 125kHz card is processed by the reader.

- In RS-485 programming mode, the following options are available by pressing the **A** key with the main menu displayed. To change the programmed reading mode, press the **A** key and the available modes will toggle on the screen.
- In 125kHz programming mode, the following options are available by badging a programming card once to enter **Address 1**.

Function	125kHz Setting	Description
All Card Format	1	All 125KHz cards will be read (no filtering)
ICT	2	Can only read ICT programmed cards
POSTECH	3	Can only read POSTECH programmed cards
HID	4	Can only read HID programmed cards
ICT & HID	5	Can only read ICT and HID programmed cards
ICT & POSTECH	6	Can only read ICT and POSTECH programmed cards
POSTECH & HID	7	Can only read POSTECH and HID programmed cards
Disable	-	No 125KHz cards will be read

7.4 DESFire Reading Mode

Applies to RS-485 programming mode only.

Reading mode determines how the data on the DESFire card will be processed by the Reader. The following options are available by pressing the **B** key with the main menu displayed. To change the programmed reading mode press the **B** key and the available modes will toggle on the screen.

Setting	Description
CSN	Card serial number (CSN) or electronic serial number (ESN) reading converts the serial number of the card to a site code and card number.
CSN Reverse	Reverse card serial number reading converts the serial number of the card to a site code and card number. The data sent is the binary reverse order of the CSN.
DESfire	DESFire is the most secure reading mode. All card access is secured with a different AES 128 bits encryption key. The ICT DESFire card data is also protected with another AES 256 bit encryption key.
Disable	No DESFire cards will be read.

7.5 Mifare Reading Mode

Applies to RS-485 programming mode only.

Reading mode determines how the data on the Mifare card will be processed by the Reader. The following options are available by pressing the **C** key with the main menu displayed. To change the programmed reading mode press the **C** key and the available modes will toggle on the screen.

Setting	Description
CSN	Card serial number (CSN) or electronic serial number (ESN) reading converts the serial number of the card to a site code and card number.
CSN Reverse	Reverse card serial number reading converts the serial number of the card to a site code and card number. The data sent is the binary reverse order of the CSN.
Secured Mifare	Secured Mifare provides medium protection access. This mode can read only ICT Secured Mifare cards. Each card has a diversified access key and the data is protected with a unique AES 256 bit encryption key.
ICT Card	Setting the reading mode to ICT Card, allows the reader to read the standard Mifare ICT cards.
Sector	Sector based reading is used to read custom sector and allows the data from the Mifare sector to be read and then converted to Wiegand data. Using ICT Mifare format cards, custom key can also be used to increase the card security.
HOTEL	These cards are used for Ving Card integration. Please refer to the Application Note AN-138: Protege Vingcard Mifare Integration.
All	This mode allows the reader to read Secured Mifare and ICT Card format.
Disable	No Mifare cards will be read.



CSN and CSN Reverse modes of operation are not secure. The CSN and ESN numbers found in ISO compliant RFID devices are transmitted without encryption and can be fraudulently generated. The CSN modes are made available for legacy system compatibility and not recommended for new installations.

7.6 Interface

When the Output Mode of the reader is set to Wiegand, interface programming configures how the reader send information to the connected system. When the Output Mode of the reader is set to Custom485 the interface programming defines the data format used with the raw format specifier.

The interface programming configures how the Reader sends information to the connected system.

- In RS-485 programming mode, press the **D** key to cycle through the available options.
- In 125kHz programming mode, the following options are available by badging the programming card twice to enter **Address 2**.

Setting	125kHz Setting	Description
26 Bit Wiegand	1	Standard 26 Bit Wiegand data sent on the D0 and D1 data lines. Truncation of site/facility codes will occur for any card or tag programmed with a site code above 255.
27 Bit Tecom Wiegand	6	Tecom formatted 27 Bit Wiegand sent on the D0 and D1 data lines. Truncation of site/facility codes will occur for any card or tag programmed with a site code above 2048.
32 Bit Wiegand	-	Standard 32 Bit Wiegand data sent on the D0 and D1 data lines. No truncation will typically occur however it is recommended to use industry standard 34 Bit. 32 Bit Wiegand has no parity or other error checking.
34 Bit Wiegand	2	Standard 34 Bit Wiegand data sent on the D0 and D1 data lines.
HOTEL	-	Send card information in HOTEL format.
37 Bit Wiegand	3	Standard 37 Bit Wiegand data sent on the D0 and D1 data lines.
37 Bit Wiegand Alternate Format	4	Alternate 37 Bit Wiegand data sent on the D0 and D1 data lines.
64 Bit Wiegand	-	Standard 64 Bit Wiegand data sent on the D0 and D1 data lines.
Auto	-	When a card is badged, the number of bits sent is determined by the information encoded on the card.

7.7 LED Function

Applies to RS-485 programming mode only.

The LED function allows the configuration of dual or single line led operation. The default is single LED mode, Blue On.

- In RS-485 programming mode, press the **E** key to cycle through the available options.
- In 125kHz programming mode, the following options are available by badging the programming card three times to enter **Address 3**.

Setting	125kHz Setting	Description
Dual	1	Grounding the orange wire will enable the green LED. Grounding the brown wire will enable the blue LED.
Blue On	2	The blue LED is on by default. Grounding the brown wire turns off the blue LED and turns on the green LED.
Green On	3	The green LED is on by default. Grounding the brown wire turns off the green LED and turns on the blue LED.

7.8 Backlight

Applies to RS-485 programming mode only.

The backlight function allows the configuration of the backlight intensity. To change the backlight operation level press the **F** key and the backlight display will change intensity levels.

7.9 Default Sector

Applies to RS-485 programming mode only.

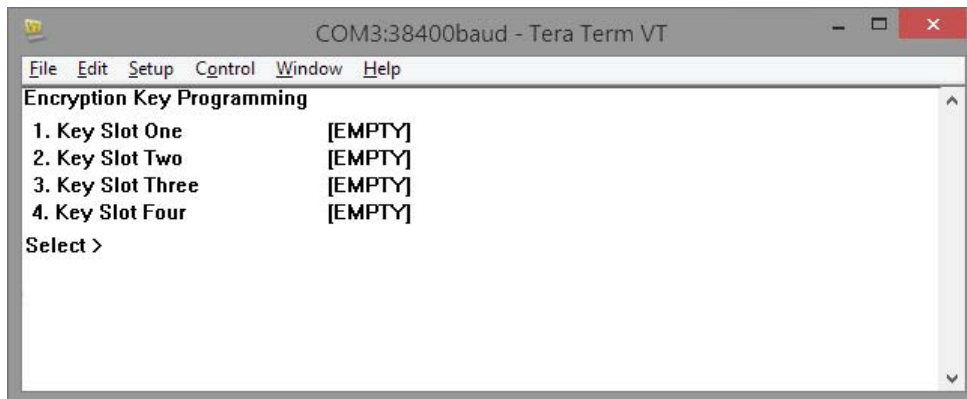
When the Default Sector reading mode is selected, the sector number where the reader will read cards data can be defined. It can be used with custom encryption keys. The default value is 14. To change the Default Sector, press the **G** key from the main menu.

7.10 Encryption Keys

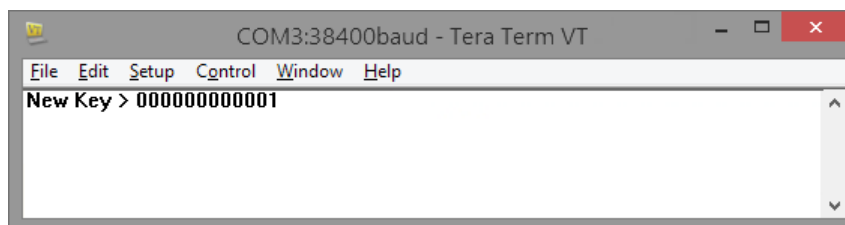
Applies to RS-485 programming mode only.

You are able to program custom keys in to the Reader by selecting the encryption option program the key required in to the location that is available. You can delete encryption keys by programming a key location with all **FFFFFFFFFFFF** however you are not able to view programmed keys.

To change the encryption keys select **J** from the menu, you will be shown the key selection screen below. Select the key slot to program the key in to. Press **ESC** to cancel your entry.



Once you have selected the desired key slot you will be prompted to enter the 6 byte hexadecimal encryption key. This key cannot be read out of the reader and to erase a key program **FFFFFFFFFFFF** in to a key slot.



7.11 Custom Format

To read third party Mifare cards the following settings should be configured as required:

- Encryption Keys: The Mifare Key A used to access the sector the data is encoded on.
- Default Sector: The sector the data is encoded on.
- Custom Card Format: A format string describing how to extract the data on the sector.

To set the custom Mifare format, press the **4** key with the main menu displayed and enter a format string of up to 64 characters. Press **ENTER** to accept entry or **ESC** to cancel entry.

The format string is made up of multiple format specifiers which follow this format (Square brackets denote the field is optional.):

%[count][modifier]specifier

The format string extracts data starting from the most significant bit of the first byte in the Mifare card's sector.

The following modifiers can currently be used.

Modifier	Description
b	BCD (4 bits, decimal)

The reader loads data as either site or card data as defined by the specifier:

Modifier	Description
s	Load site
c	Load card
u	Unused

Example

We have a Mifare card which has been encoded with data in sector 3. The data has a start marker **0xAABBCCDDEEFF** at the start of the sector, 3 packed decimal BCD encoded site values and ends with 5 unpacked decimal BCD card values. It is then filled with binary 1's. For a particular card this may mean the data is **0xAABBCCDDEEFF12300403020100FFFFFF**.

The start marker needs to be ignored. The marker length is 6 bytes which is 48 bits. To ignore this we use the following format specifier: **%48u**.

The site code data is packed BCD. This means we need the 'b' modifier. We want to load this data as site data so we use the 's' specifier. This means we need our format specifier to be **%bs**. As there are 3 site code bytes we repeat this 3 times giving **%bs%bs%bs**.

The card code is unpacked decimal BCD. This means we need the 'b' modifier. We want to load this data as card data so we use the 'c' specifier. This means the format specifier is **%bc**. Note that the BCD data is unpacked, ie for each byte we have 4bits which are 0 and 4bits which are the BCD value. This means we must ignore the first 4bits each time as we did for the start marker, then read the BCD data. So for each unpacked BCD value we use **%4u%bc**. We repeat this 5 times to read the whole set.

The trailing data doesn't need to be read so it can be ignored.

This gives the complete format string: **%48u%bs%bs%bs%4u%bc%4u%bc%4u%bc%4u%bc%4u%bc**.

7.12 Intelligent Tamper

Enabling the intelligent reader tamper mode will force the card reader to check in to the device it is connected to every 30 seconds.

- In RS-485 programming mode, the following options are available by pressing the **M** key from the main menu.
- In 125kHz programming mode, the following options are available by badging the programming card **four** times to enter **Address 4**.

Function	125kHz Setting	RS-485 Setting
Disabled	1	1
Enabled	2	2



Only enable Intelligent Reader Tamper Mode if the access control system or reader interface supports intelligent tamper operation.

7.13 Factory Reset

Applies to RS-485 programming mode only.

This resets all settings in the device excluding custom encryption keys. To reset the reader, press the **O** key from the main menu.

7.14 Output Mode

Applies to RS-485 programming mode only.

The Output Mode defines the output format of the reader. Three formats are available - Wiegand, ICT Smart or Custom RS-485. To change the Output Mode, press the **L** key from the main menu.

7.15 Clone Card Notify

Clone Card Notify enables the reader to notify the reader expander if a card presented is a non-standard Mifare compatible card. This setting is only supported when using RS-485 configuration and requires the Clone Card Reading option to be enabled.

To toggle the Clone Card Notify option, press the **1** key.

7.16 Clone Card Reading

The Clone Card Reading option determines whether non-standard Mifare compatible cards are read by the reader.

To toggle the Clone Card Reading option, press the **2** key.

7.17 Clone Card Destroy

If this setting is enabled and a non-standard Mifare compatible card is presented, the reader modifies the card so it cannot be read.

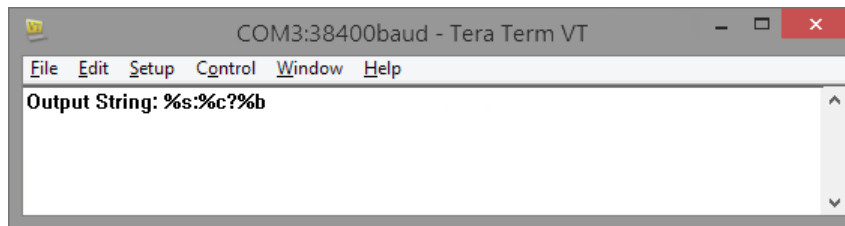
To toggle Clone Card Destroy, press the **3** key.

7.18 Custom RS-485 Format

Applies to RS-485 programming mode only.

To set the custom RS-485 format select **Y** from the menu. You will be prompted to enter a format string. This format string can be up to 64 characters. Press **ESC** to cancel your entry.

The format specifiers are all preceded by a **%** character.



This example shows a format configured to output the site code then a colon. This is followed by the card number then a question mark. This is concluded with the Wiegand data in the currently configured Wiegand format.

The example shown above will output something similar to:

00034463 :00003242?6A987CB0C

Where:

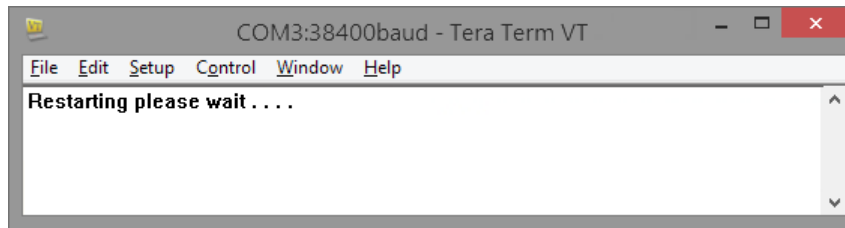
- **00034463** is the site code of the card read
- **00003242** is the card number of the card read
- **6A987CB0C** is the raw Wiegand data of the card read in the currently configured Wiegand format.

The **b** specifier outputs in hexadecimal format. In all other cases uppercase means hexadecimal format and lowercase means decimal format. The definitions of each specifier is listed in the table below:

Specifier	Definition
b	Raw Wiegand hexadecimal data
s or S	Decimal or hexadecimal site code
c or C	Decimal or hexadecimal card number
n	New line
e or E	Decimal or hexadecimal card serial number
p or P	Padded version of the decimal or hexadecimal card serial number. This is padded to 17 characters in decimal and 10 characters in hexadecimal.
%	Two % in a row will place a % in the output

7.19 Save and Restart

You must select the **Save and Restart** option to save your programming changes and restart the device by pressing the **S** key. Failing to select this option and powering the unit down will result in a loss of your programming changes.



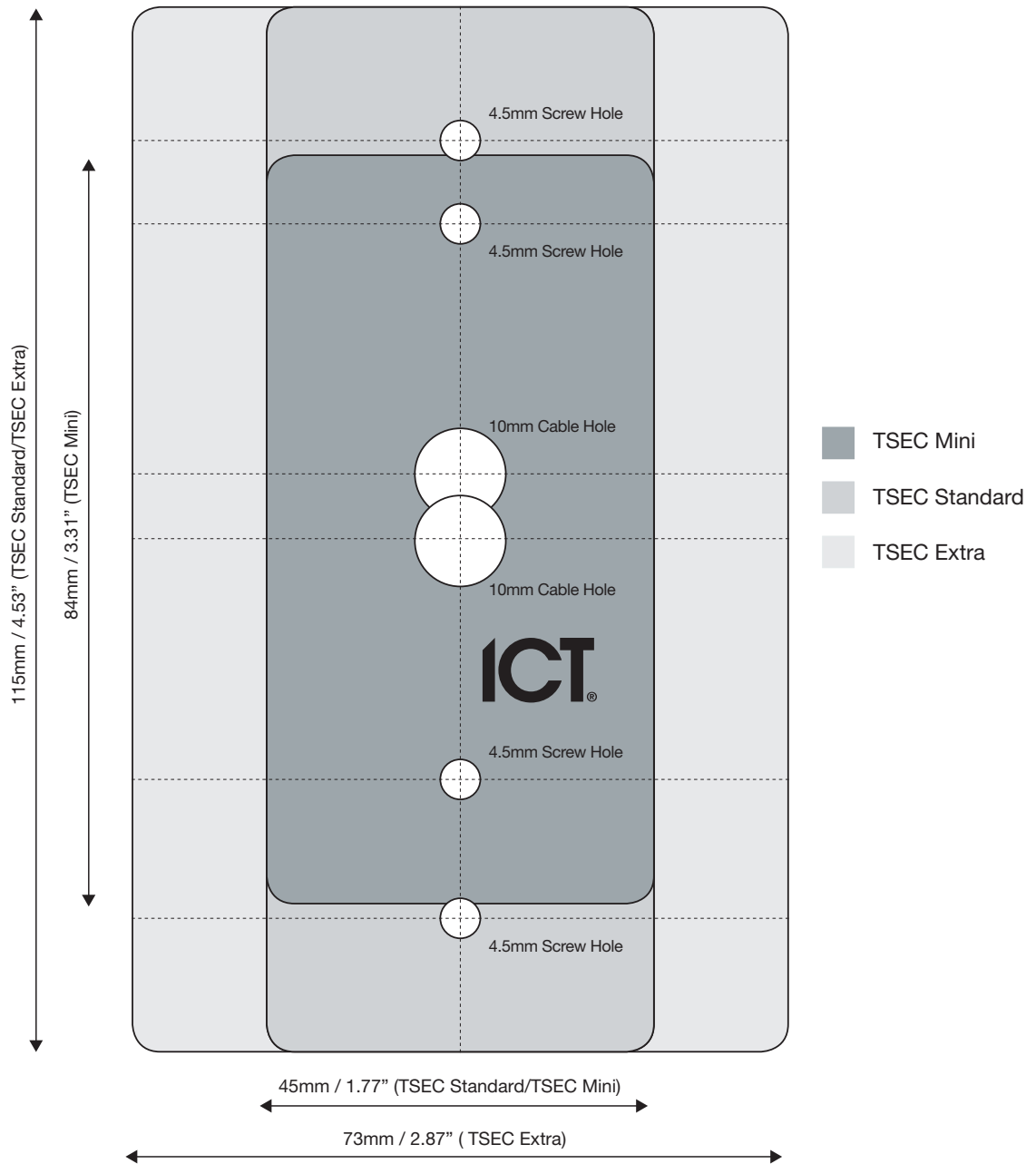
In 125kHz programming mode, badge the programming card **12** times to restart the card reader.



The Restart function immediately causes the card reader to exit programming mode and restart.

8 Technical Diagram

The dimensions shown below outline the essential details needed to help ensure the correct installation of the tSec Reader.



9 Technical Specifications

The following technical specifications are important and vital to the correct operation of the tSec Reader. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

Integrated Control Technology continually strives to increase the performance of its products. As a result these specifications may change without notice. We recommend consulting the ICT website (<http://www.ict.co>) for the latest documentation and product information.

Operating Voltage	12VDC (9.5 to 14VDC)
Operating Current	Standard: 140mA (peak, reading) Extra: 162mA (peak, reading) Mini: 118mA (peak, reading)
Card Read Range	Mifare 60mm (2.36")* DESFire EV1 ISO 15mm (0.6")* 125kHz Clamshell 40mm (1.57")
Tag Read Range	Mifare 35mm (1.18")* DESFire EV1 ISO 6mm (0.23")* 125kHz 25mm (0.98")
Wiegand Interface	Multiple format 26 or 34 Bit data 0 and data 1, card defined.
Max Cable Distance	150m (492ft)
Frequency	13.56 MHz ISO/IEC 14443 Type A* 125KHz pulse width modulated
Multi Conductor Cable	22Awg alpha 5196, 5198, 18Awg alpha 5386, 5388
Environment IP Rating	IP65
Operating Temperature	-35° to 65°C (-31° to 149°F)
Storage Temperature	-10° to 85°C (14° to 185°F)
Dimensions (H x W x D)	Standard: 115 x 45 x 18mm (4.53 x 1.77 x 0.71") Extra: 115 x 73 x 18mm (4.53 x 2.87 x 0.71") Mini: 84 x 45 x 17mm (3.31 x 1.77 x 0.67")
Weight	Standard: 110g (3.89oz) Extra: 155.8g (5.5oz) Mini: 80g (2.82oz)

*Mifare/DESFire and Combo models only

The size of conductor used for the supply of power to the unit should be adequate to prevent voltage drop at the terminals of no more than 5% of the rated supply voltage. Specifications are subject to change without notice, please visit www.ict.co for updated information.

10 New Zealand and Australia

The compliance label indicates that the supplier of the device asserts that it complies with all applicable standards.

R-NZ

11 European CE and EN 50131

European Standards **CE**

Conforms to European Union (EU) Low Voltage Directive (LVD) 73/23/EEC (amended by 93/68/EEC) and Electro-Magnetic Compatibility (EMC) Directive 89/336/EEC (amended by 92/31/EEC and 93/68/EEC). The CE mark indicates that this product complies with the European requirements for safety, health, environmental and customer protection.

This component was tested by the accredited testing laboratory No. 1172 of the company TESTALARM Praha s.r.o. and met the requirements and conditions for full compliance with EN50131 series of standards for equipment classification;

Security Grade 3

Environmental Class IV

Impact: IK06

Equipment Class: Fixed

EN 50131-1:2006, EN 50131-3:2009, EN 50131-6:2008

Recognition class 2 (for readers without a keypad)

Recognition class 3 (for readers with a keypad)

Access class B

EN 50133-1:1998

12 UL and ULC Installation Requirements



Only UL / ULC listed compatible products are intended to be connected to a UL / ULC listed access control system.

12.1 CAN/ULC-S319-05

- This card reader is CAN/ULC-S319 Listed for Class I applications only.
- Exit devices and wiring must be installed within the protected area.
- The card reader must be connected with shielded, grounded cable.
- Fail secure locking mechanism shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to ULC-S533 and CAN/ULC-S104.
- Must be installed with CAN/ULC-S319 Listed portal locking device(s) for ULC installations.
- Input power must be supplied by a Class 2 or power limited device.

12.2 UL294

- This card reader is UL 294 Listed for Class 1 applications only.
- Exit devices and wiring must be installed within the protected area.
- The card reader must be connected with shielded, grounded cable.
- Fail secure locking mechanism shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to UL10B or UL10C.
- Must be installed with UL 1034 Listed electronic locks for UL installations.
- Input power must be supplied by a Class 2 or power limited device.

13 FCC Compliance Statements

FCC PART 15, WARNINGS: INFORMATION TO USER

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Changes or modifications not authorized by the party responsible for compliance could void the user's authority to operate this product.

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

14 Industry Canada Statement

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

15 Ordering Information

Please use the following product codes when placing an order from the tSec Card Reader range.

Standard Range:

- PRX-TSEC-STD - tSec Standard Card Reader
- PRX-TSEC-STD-KP - tSec Standard Card Reader with Keypad
- PRX-TSEC-STD-125 - tSec Standard 125KHz Card Reader
- PRX-TSEC-STD-125-KP - tSec Standard 125KHz Card Reader with Keypad
- PRX-TSEC-STD-DF - tSec Standard DESFire Card Reader
- PRX-TSEC-STD-DF-KP - tSec Standard DESFire Card Reader with Keypad

Extra Range:

- PRX-TSEC-EXTRA - tSec Extra Card Reader
- PRX-TSEC-EXTRA-KP - tSec Extra Card Reader with Keypad
- PRX-TSEC-EXTRA-125 - tSec Extra 125KHz Card Reader
- PRX-TSEC-EXTRA-125-KP - tSec Extra 125KHz Card Reader with Keypad
- PRX-TSEC-EXTRA-DF - tSec Extra DESFire Card Reader
- PRX-TSEC-EXTRA-DF-KP - tSec Extra DESFire Card Reader with Keypad

Mini Range:

- PRX-TSEC-MINI - tSec Mini Card Reader
- PRX-TSEC-MINI-125 - tSec Mini 125KHz Card Reader
- PRX-TSEC-MINI-DF - tSec Mini DESFire Card Reader

Manuals and additional literature are available on the ICT Website (<http://www.ict.co>).

16 Warranty

Integrated Control Technology (ICT) warrants its products to be free from defects in materials and workmanship under normal use for a period of two years. Except as specifically stated herein, all express or implied warranties whatsoever, statutory or otherwise, including without limitation, any implied warranty of merchantability and fitness for a particular purpose, are expressly excluded. ICT does not install or connect the products and because the products may be used in conjunction with products not manufactured by ICT, ICT cannot guarantee the performance of the security system. ICT's obligation and liability under this warranty is expressly limited to repairing or replacing, at ICT's option, any product not meeting the specifications. In no event shall ICT be liable to the buyer or any other person for any loss or damages whether direct or indirect or consequential or incidental, including without limitation, any damages for lost profits, stolen goods, or claims by any other party caused by defective goods or otherwise arising from the improper, incorrect or otherwise faulty installation or use of the merchandise sold.

17 Contact

Integrated Control Technology welcomes all feedback.

Please visit our website (<http://www.ict.co>) or use the contact information below.

Integrated Control Technology

P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

4 John Glenn Ave
Rosedale
North Shore City 0632
Auckland
New Zealand

Phone: +64-9-476-7124

Toll Free Numbers:

0800 ICT 111 (0800 428 111) - New Zealand

1800 ICT 111 (1800 428 111) - Australia

1855 ICT 9111 (1855 428 9111) - USA/Canada

Email: sales@incontrol.co.nz or support@incontrol.co.nz

Web: www.ict.co

NEW ZEALAND

Integrated Control Technology Limited
4 John Glenn Avenue, Rosedale, Auckland 0632
PO Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: sales@incontrol.co.nz Toll Free: (0800) 428 111 Phone: 64 (9) 476 7124

USA

Integrated Control Technology (USA) LLC.
5265 S Rio Grande Street, Suite 201, Littleton, CO 80120
Email: ussales@incontrol.co.nz Toll Free: (855) 428 9111 Phone: 720 442 0767

Designers & manufacturers of integrated electronic access control, security and automation products.

Designed & manufactured by Integrated Control Technology Ltd.

Copyright © Integrated Control Technology Limited 2003-2015. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of these products, 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 Integrated Control Technology policy of enhanced development, design and specifications are subject to change without notice

227-4310-000

www.ict.co

