PRX-TSEC Range

# tSec Multi-Technology Card Reader with Bluetooth® Wireless Technology

## Installation Manual

Last Published: 11-Jun-20 10:35 AM

# Contents

# Introduction

The Protege tSec Multi-Technology Card Reader with Bluetooth® Wireless Technology 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 125KHz, MIFARE and DESFire cards
- Encrypted RS-485, un-encrypted configurable RS-485 or standard Wiegand connection
- NFC Credential Reading
- Optional **Bluetooth®** Wireless Technology for reading mobile credentials
- Configurable LED strip: 2 color control via external LED wiring, 16 color selectable for Protege Function Codes (RS-485 connection only)
- Keep alive transmission every 30 seconds for intelligent tamper management
- Fully encapsulated design with environmental IP Rating of IP65 for outdoor and indoor operation
- Programmable via programming cards
- Keypad output on Wiegand data lines (keypad versions only)

# tSec Reader Editions

The tSec Reader comes in three main sizes and with a range of optional features.

| tSec Standard Reader | 115 x 45 x 18mm (4.53 x 1.77 x 0.71”) | | | | |
|---|---|---|---|---|---|
| | Keypad | 125kHz | MIFARE/ DESFire/ NFC | Bluetooth® Technology | Vandal Resistant Cover* |
| PRX-TSEC-STD-B<br>tSec Standard Multi-Technology Card Reader | | ✓ | ✓ | | |
| PRX-TSEC-STD-KP-B<br>tSec Standard Multi-Technology Card Reader with Keypad | ✓ | ✓ | ✓ | | |
| PRX-TSEC-STD-125-B<br>tSec Standard 125kHz Card Reader | | ✓ | | | |
| PRX-TSEC-STD-DF-B<br>tSec Standard 13.56MHz Card Reader | | | ✓ | | |
| PRX-TSEC-STD-DF-KP-B<br>tSec Standard 13.56MHz Card Reader with Keypad | ✓ | | ✓ | | |
| PRX-TSEC-STD-BT-B<br>PRX-TSEC-STD-BT-W<br>tSec Standard Multi-Technology Card Reader with Bluetooth® Wireless Technology | | ✓ | ✓ | ✓ | |
| PRX-TSEC-STD-KP-BT-B<br>PRX-TSEC-STD-KP-BT-W<br>tSec Standard Multi-Technology Card Reader with Keypad and Bluetooth® Wireless Technology | ✓ | ✓ | ✓ | ✓ | |
| PRX-TSEC-STD-KP-BT-B-VRC<br>tSec Standard Multi-Technology Card Reader with Keypad, Vandal Resistant Cover and Bluetooth® Wireless Technology | ✓ | ✓ | ✓ | ✓ | ✓ |
| PRX-TSEC-STD-DF-BT-B<br>tSec Standard 13.56MHz Card Reader with Bluetooth® Wireless Technology | | | ✓ | ✓ | |
| PRX-TSEC-STD-DF-KP-BT-B<br>tSec Standard 13.56MHz Card Reader with Keypad and Bluetooth® Wireless Technology | ✓ | | ✓ | ✓ | |

* Keypad editions with vandal resistant cover included. Covers may be purchased separately for readers without keypads, but regular keypad editions do not support vandal resistant covers.

| tSec Extra Reader | 115 x 73 x 18mm (4.53 x 2.87 x 0.71”) | | | | |
|---|---|---|---|---|---|
| | Keypad | 125kHz | MIFARE/ DESFire/ NFC | Bluetooth® Technology | Vandal Resistant Cover* |
| PRX-TSEC-EXTRA-KP-B<br>tSec Extra Multi-Technology Card Reader with Keypad | ✓ | ✓ | ✓ | | |

| tSec Extra Reader | 115 x 73 x 18mm (4.53 x 2.87 x 0.71”) | | | | |
|---|---|---|---|---|---|
| | Keypad | 125kHz | MIFARE/ DESFire/ NFC | Bluetooth® Technology | Vandal Resistant Cover* |
| PRX-TSEC-EXTRA-125-B<br>tSec Extra 125kHz Card Reader | | ✓ | | | |
| PRX-TSEC-EXTRA-DF-B<br>tSec Extra 13.56MHz Card Reader | | | ✓ | | |
| PRX-TSEC-EXTRA-DF-KP-B<br>tSec Extra 13.56MHz Card Reader with Keypad | ✓ | | ✓ | | |
| PRX-TSEC-EXTRA-BT-B<br>PRX-TSEC-EXTRA-BT-W<br>tSec Extra Multi-Technology Card Reader with Bluetooth® Wireless Technology | | ✓ | ✓ | ✓ | |
| PRX-TSEC-EXTRA-KP-BT-B<br>PRX-TSEC-EXTRA-KP-BT-W<br>tSec Extra Multi-Technology Card Reader with Keypad and Bluetooth® Wireless Technology | ✓ | ✓ | ✓ | ✓ | |
| PRX-TSEC-EXTRA-KP-BT-B-VRC<br>tSec Extra Multi-Technology Card Reader with Keypad, Vandal Resistant Cover and Bluetooth® Wireless Technology | ✓ | ✓ | ✓ | ✓ | ✓ |
| PRX-TSEC-EXTRA-DF-BT-B<br>tSec Extra 13.56MHz Card Reader with Bluetooth® Wireless Technology | | | ✓ | ✓ | |

* Keypad editions with vandal resistant cover included. Covers may be purchased separately for readers without keypads, but regular keypad editions do not support vandal resistant covers.

| tSec Mini Reader | 84 x 45 x 17mm (3.31 x 1.77 x 0.67”) | | | | |
|---|---|---|---|---|---|
| | Keypad | 125kHz | MIFARE/ DESFire/ NFC | Bluetooth® Technology | Vandal Resistant Cover* |
| PRX-TSEC-MINI-B<br>tSec Mini Multi-Technology Card Reader | | ✓ | ✓ | | |
| PRX-TSEC-MINI-125-B<br>tSec Mini 125kHz Card Reader | | ✓ | | | |
| PRX-TSEC-MINI-DF-B<br>tSec Mini 13.56MHz Card Reader | | | ✓ | | |
| PRX-TSEC-MINI-BT-B<br>PRX-TSEC-MINI-BT-W<br>tSec Mini Multi-Technology Card Reader with Bluetooth® Wireless Technology | | ✓ | ✓ | ✓ | |
| PRX-TSEC-MINI-DF-BT-B<br>tSec Mini 13.56MHz Card Reader with Bluetooth® Wireless Technology | | | ✓ | ✓ | |

***** Keypad editions with vandal resistant cover included. Covers may be purchased separately for readers without keypads, but regular keypad editions do not support vandal resistant covers.

# MIFARE Technology

## 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.

- Fully compliant with the international standard ISO/IEC 14443 Type A
- Multi-application memory to store several services on the same card, allowing for many integration possibilities
- Fast transaction speed
- High security and fraud protection

## MIFARE/DESFire Products

The MIFARE/DESFire products can be expanded to accommodate large numbers of modules using the encrypted RS-485 Network. ICT provides a number of reader and tag/card options in the MIFARE/DESFire range.

### Cards

- MIFARE 1K (S50) Proximity Clamshell Card
- MIFARE 1K (S50) Proximity Card ISO
- MIFARE 1K (S50) Proximity Card ISO Mag
- MIFARE 1K (S50) Proximity Standard Key Tag

### MIFARE/DESFire Cards

- MIFARE/DESFire EV1 Proximity Card ISO2K
- MIFARE/DESFire EV2 Proximity Card ISO2K

## Secured MIFARE Card Format

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.

## 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
- Common Criteria EAL4+ security certified
- 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

# About MIFARE DESFire EV2

MIFARE DESFire EV2 delivers the perfect balance of speed, performance and cost-efficiency. The latest addition to the MIFARE DESFire product family introduces new features along with enhanced performance for the best user experience. For a truly convenient touch-and-go experience, MIFARE DESFire EV2 offers increased operating distance compared to previous versions. Based on global open standards for both air interface and cryptographic methods, it fully complies with the requirements for fast and highly secure data transmission and flexible application management.

- Fully compliant to all levels of the international standard ISO/IEC 14443A
- Common Criteria EAL5+ security certified
- Available in 2, 4, 8, 16 or 32 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
- Fully interoperable with existing NFC reader infrastructure
- Operating distance up to 100 mm

# Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- UL 681 - Installation and Classification of Burglar and Holdup Systems
- UL 827 - Central-Station Alarm Services
- CAN/ULC-S301, Central and Monitoring Station Burglar Alarm Systems
- CAN/ULC-S302, Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults
- CAN/ULC-S561, Installation and Services for Fire Signal Receiving Centres and Systems
- The National Electrical Code, ANSI/NFPA 70
- The Canadian Electrical Code, Part I, CSA C22.1
- AS/NZS 2201.1 Intruder alarm systems
- The Local Authority Having Jurisdiction (AHJ)

# Mounting

The card 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.

## Mounting Instructions

1. Select where to mount the tSec 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 with the tSec Reader 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 with the tSec Reader to secure and fasten the top case to the bottom mounted case.

# Reader Connection

The recommended cable types for RS-485 are:

- Belden 9842 or equivalent
- 24 AWG twisted pair with characteristic impedance of 120ohm

The recommended cable types for Wiegand are:

- 22 AWG alpha 5196, 5198, 18 AWG alpha 5386, 5388

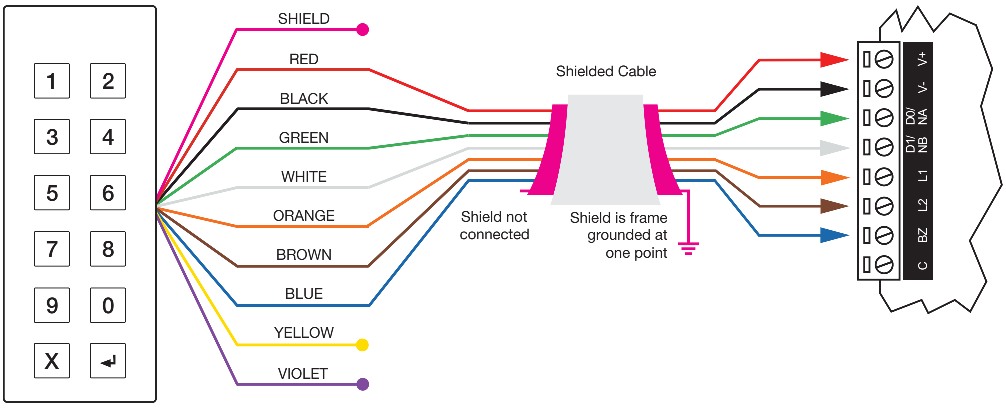
**Warning:** The reader outputs D0 (green wire) and D1 (white wire) can switch to a maximum capacity of 50mA. Exceeding this amount will damage the output.

## Wiegand Connection

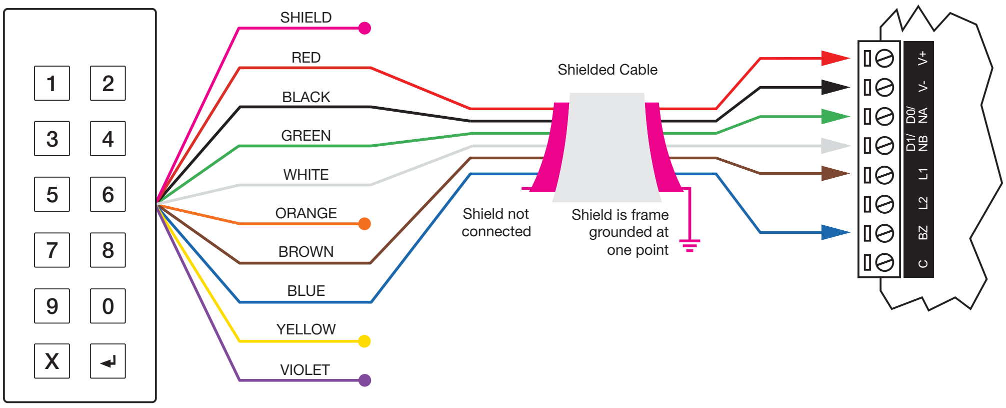
Readers are shipped in Single LED mode by default.

When using the standard Wiegand Interface to access a Reader Expander, two wiring methods can be used. Dual LED operation allows the signaling 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.

Dual LED Connection



Single 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.

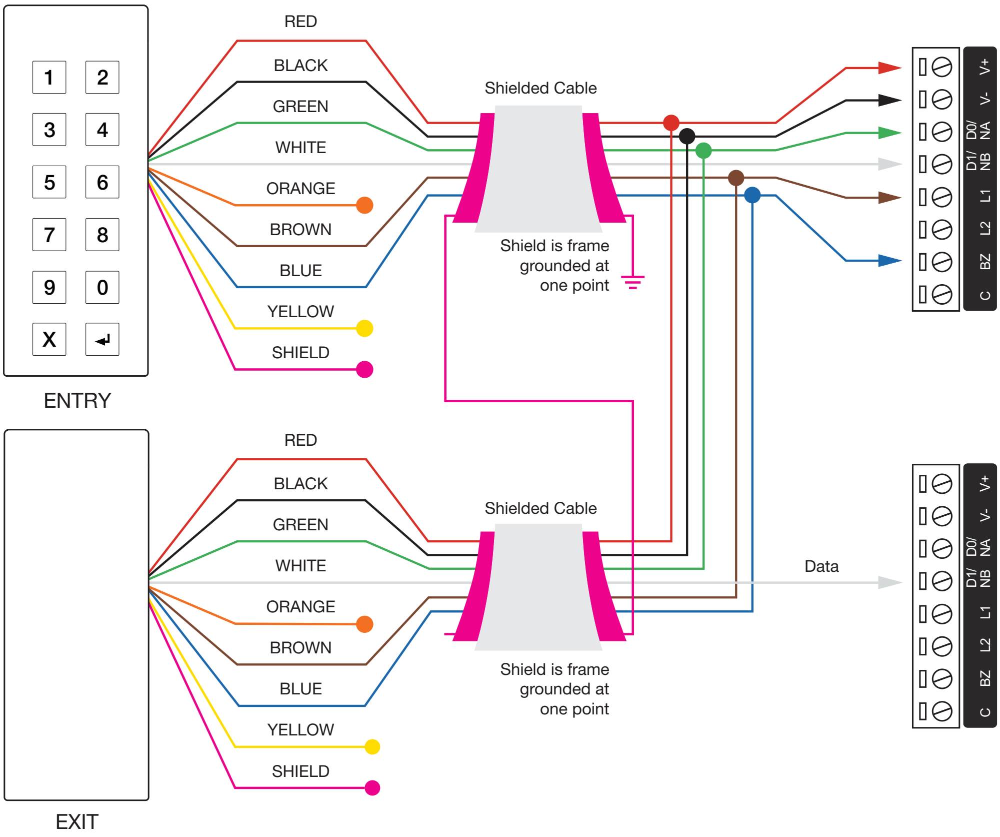
Connect the reader shield to a suitable earth point. **DO NOT** connect the shield to a ground or AUX connection. **DO NOT** connect the shield wires together at the reader cable splice. With the shield wire already terminated at the reader terminate the shield at the controller.

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

# Wiegand Reader Connection (Entry / Exit)

In multiple reader mode, the secondary reader has all connections wired to the same port as the primary card reader with the DATA 1 connection wired to the opposite reader connection DATA 1 input.

The reader that is multiplexed in to the alternate reader port will operate as the exit reader and the normal reader connection shall be programmed to operate as the Entry Reader.



**Important:**

- The card reader must be connected to the module port using a shielded cable.
- Do not connect the shield to an AUX-, 0V or V- connection on the module.
- Do not join the shield and black wires at the reading device.
- Do not connect the shield to any shield used for isolated communication.
- The shield connection must only be connected at one end of the cable in the metallic enclosure (frame grounded).

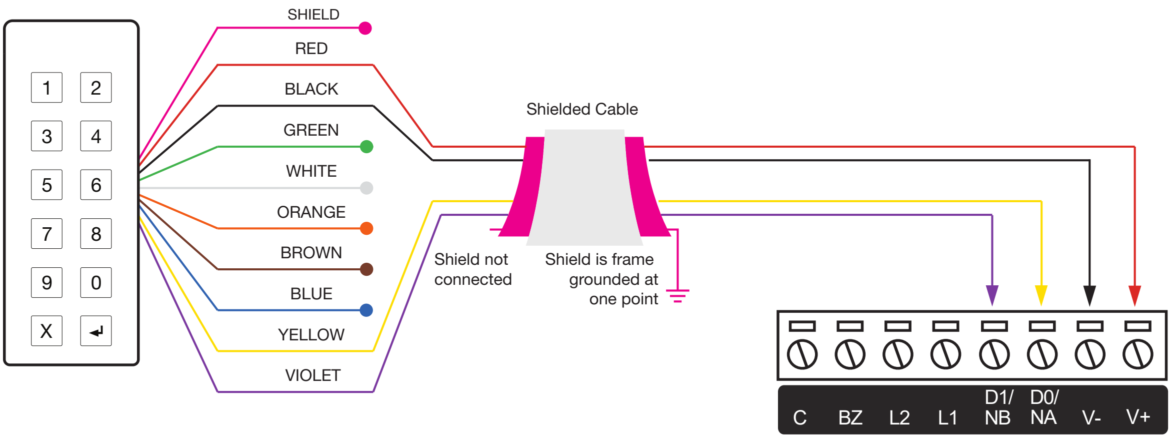
# RS-485 Reader Locations

As two RS-485 readers can be connected to the same RS-485 reader port, the configuration of the **green** and **orange** wires is used to uniquely identify the reader and determine which is the entry reader, and which is the exit reader.

| Location | Configuration |
|---|---|
| Entry | Green and orange wires **not** connected. |
| Exit | Green and orange wires connected together. |

# RS-485 Reader Connection

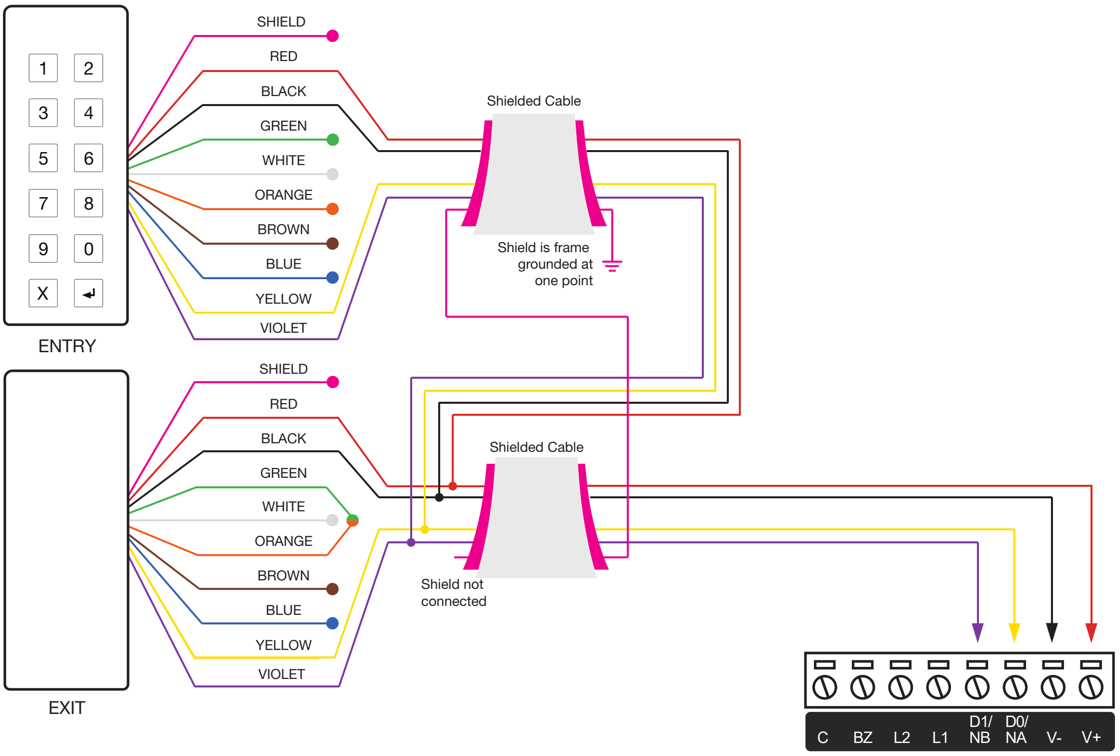
The connection of a single RS-485 reader to a Reader Expander in entry only mode.



When the green and orange wires are not connected together, the reader defaults to an entry reader.

# RS-485 Connection (Entry/Exit)

The connection of two RS-485 readers to a Reader Expander providing an entry/exit configuration.



The exit reader has the **green** and **orange** wires connected together.

A 330 Ohm EOL (End of Line) resistor MAY be required to be inserted between the NA and NB terminals of the reader and a second 330 Ohm EOL resistor must then be inserted between the source NA and NB terminals at the other end of the wiring.

# 125kHz Installer Programming

125kHz capable tSec Readers can be programmed using a 125kHz programming card. These cards cannot be used to program the 13.56MHz series of tSec Readers.

## Entering 125kHz Programming Mode

125kHz programming mode is entered by presenting a 125kHz programming card to the unit within the first 2 minutes of power being applied. The reader beeps twice to indicate that it has entered 125kHz programming mode.

Data entry and the programming menu will time out after 2 minutes of no activity and reverts back to normal activity. Any incomplete programming changes will be lost.

### To program the reader using 125kHz mode:

1. Present the 125kHz programming card to the reader to enter **Programming Mode**.
2. Wait for the reader to beep twice.
3. Present the same card to the reader a number of times in quick succession to indicate the **Address** of the required **Programming Option**. See the Programming Option Addresses table below.
4. Wait for the reader to beep twice.
5. Present the same card a number of times in quick succession to indicate the required **125kHz Setting**. The settings for each programming option are outlined in the tables below.
6. 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.
7. 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 you can allow the reader to timeout to select another address.

8. Once complete, allow the programming interface to time out and return to normal operation.

## Example

### Programming the Interface to output 26 Bit Wiegand:

1. Present the programming card to the reader once to initiate **Programming Mode**. The card reader will respond by beeping twice to indicate that Programming Mode has been entered.
2. Once Programming Mode has been entered, present the programming card twice to enter **Address 2**, the **Programming Option** for Wiegand Output Format. The card reader will respond by beeping twice to indicate that it has entered the Wiegand Output Format menu.
3. Next, present the programming card twice, corresponding with the **125kHz Setting** (2) for 26 Bit Wiegand. Wait for the reader to beep twice, indicating the data has been programmed correctly.
4. Continue programming additional settings, or leave the programming interface to time out.

## Programming Option Addresses

| Address | Programming Options |
|---|---|
| 1 | 125kHz Reading Mode |

| | |
|---|---|
| 2 | Wiegand Output Format |
| 3 | LED Function |
| 4 | Intelligent Tamper Mode |
| 5 | Enable ASK (EM) Cards |
| 6 | PIN Data Interface |
| 7 | PSK Unscramble |
| 8 | PSK Enable |
| 12 | Factory Default |

## 125kHz Reading Mode

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

The following options are available by badging a programming card **once** to enter **Address 1**.

| Function | 125kHz Setting | Description |
|---|---|---|
| | 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. Selecting this option disables the programming card. |
| HID | 4 | Can only read HID programmed cards. Selecting this option disables the programming card. |
| 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. Selecting this option disables the programming card. |

## Wiegand Output Format

When the Output Mode of the reader is set to Wiegand, the interface programming configures how the reader sends information to the connected system.

The following options are available by badging the programming card **twice** to enter **Address 2**.

| Setting | 125kHz Setting | Description |
|---|---|---|
| **Auto** | **1** | When a card is badged, the number of bits sent is determined by the information encoded on the card. |
| 26 Bit Wiegand | 2 | 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 | 3 | 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 | 4 | Standard 32 Bit Wiegand data sent on the D0 and D1 data lines. No truncation will typically occur; however, it is recommended that you use industry standard 34 Bit. 32 Bit Wiegand has no parity or other error checking. |
| 34 Bit Wiegand | 5 | Standard 34 Bit Wiegand data sent on the D0 and D1 data lines. |
| 66 Bit Wiegand | 6 | Standard 66 Bit Wiegand data sent on the D0 and D1 data lines. |
| 37 Bit Wiegand | 7 | Standard 37 Bit Wiegand data sent on the D0 and D1 data lines. |
| 64 Bit Wiegand | 8 | Standard 64 Bit Wiegand data sent on the D0 and D1 data lines. |
| Kantech KSF | 9 | Kantech formatted 26 Bit Wiegand sent on the D0 and D1 data lines. |

# LED Function

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

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. |

# Intelligent Tamper Mode

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

The following options are available by badging the programming card **four** times to enter **Address 4**.

| Function | Setting |
|---|---|
| **Disabled** | **1** |
| Enabled | 2 |

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

# Enable ASK (EM) Cards

This enables the card reader to read ASK (EM) formatted cards. By default, this feature is enabled only if the PSK/EM hardware is fitted.

The following options are available by badging the programming card **five** times to enter **Address 5**.

| Function | Setting |
|---|---|
| Disabled | 1 |
| **Enabled** | **2** |

## PIN Data Interface

The PIN data interface format defines how the PIN data is sent using the D0 and D1 data interface.

The following options are available by badging the programming card **six** times to enter **Address 6**.

| Setting | Function | Max PIN (when using a reader module) |
|---|---|---|
| **1** | **ARK-501** | 99999999 |
| 2 | 26 Bit Wiegand Format | 65535 |
| 3 | 4 Bit | 99999999 |
| 4 | 4 Bit with Parity | 99999999 |
| 5 | 4 Bit Buffered | 99999999 |
| 6 | 4 Bit Buffered with Parity | 99999999 |
| 7 | 36 Bit Wiegand Format | 1048575 |

ARK-501, 4 bit, and 4 bit with parity send every button press instantly down the data interface. 26 bit Wiegand, 36 Bit Wiegand, 4 bit buffered, and 4 bit buffered with parity buffer the key presses and send them when the user presses ENTER. Pressing the CLEAR key wipes the buffer. If the max PIN is exceeded a long beep is generated and no data is sent.

When using the format 4 bit buffered with parity a Reader Expander set with the card format of 26 bit will decode PINs that are 6 digits long as card numbers and handle it as a card. This is the same for HID 34 Bit with 8 digit PINs. Where possible, these combinations should be avoided.

## PSK Unscramble

PSK Unscramble enables the reader to read Kantech, Tecom and Motorola cards.

The following options are available by badging the programming card **seven** times to enter **Address 7**. This option is only available if the PSK hardware is present.

| Function | Setting |
|---|---|
| Raw | 1 |
| **Kantech** | **2** |
| Tecom | 3 |
| Motorola | 4 |

## PSK Enable

This enables the card reader to read PSK formatted cards. By default, this feature is enabled and is only available if the PSK hardware is present.

The following options are available by badging the programming card **eight** times to enter **Address 8**.

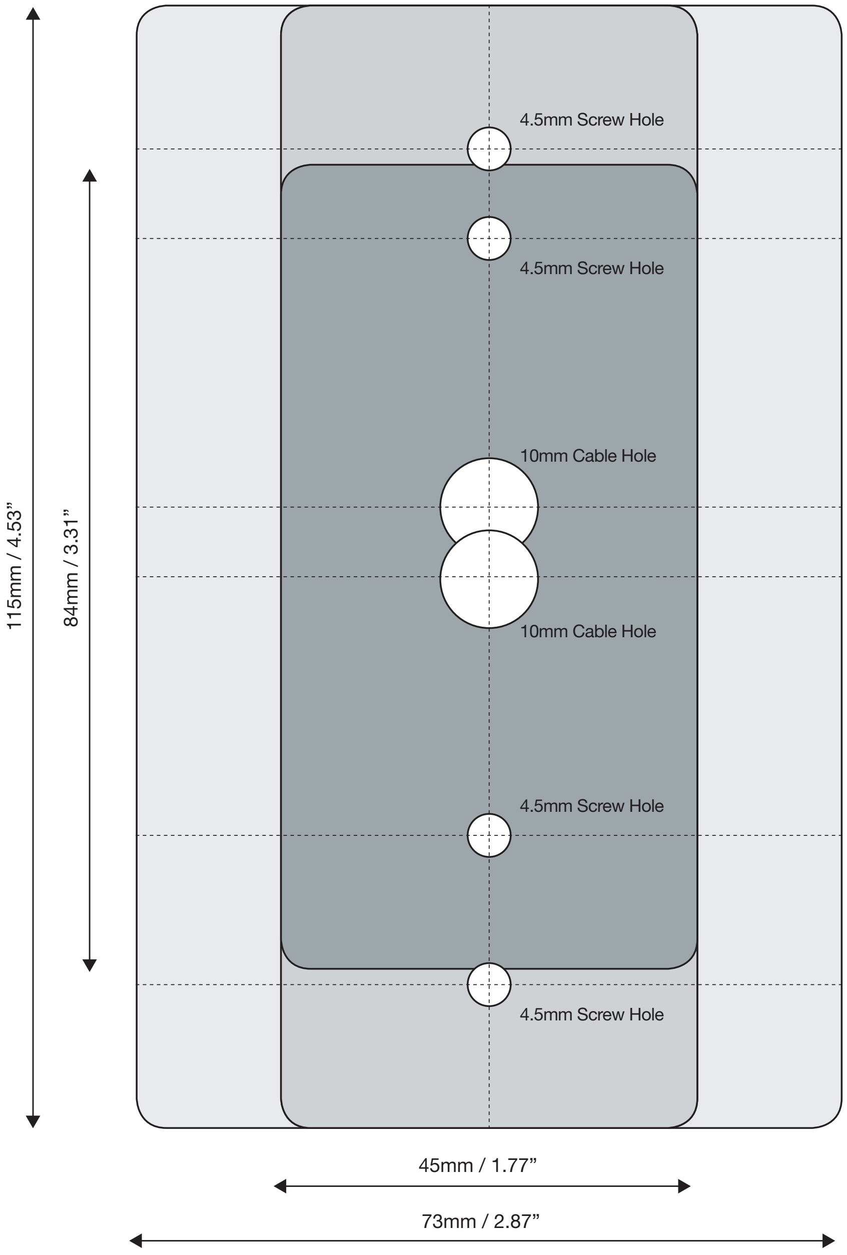
| Function | Setting |
|---|---|
| Disabled | 1 |
| **Enabled** | **2** |

# Factory Default

This resets all of the device's settings. To reset the reader, badge the 125kHz programming card **twelve** times to enter **Address 12**.

# Technical Diagram

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



# Technical Specifications

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

| | |
|---|---|
| **Ordering Information** | |
| Order Codes | See tSec Reader editions. |
| **Power Supply** | |
| Operating Voltage | 12VDC (9.5 to 14VDC) |
| Operating Current | tSec Standard Reader: 254mA (peak, reading)<br>tSec Extra Reader: 298mA (peak, reading)<br>tSec Mini Reader: 203mA (peak, reading) |
| **Communications** | |
| Card Read Range | MIFARE 60mm (2.36″) *<br>DESFire EV1 ISO 15mm (0.6″) *<br>125kHz Clamshell 40mm (1.57”) † |
| Tag Read Range | MIFARE 30mm (1.2″) *<br>DESFire EV1 6mm (0.23″) *<br>125kHz 25mm (0.98”) † |
| Wiegand Interface | Multiple format 26 or 34 Bit data 0 and data 1, card defined. |
| Frequency | 13.56 MHz ISO/IEC 14443 Type A*<br>125KHz pulse width modulated† |
| Multi Conductor Cable | Wiegand: 22Awg alpha 5196, 5198, 18Awg alpha 5386, 5388. Max Distance 150m (492ft)<br>Module comms/RS485: Belden 9842 or equivalent. Max distance 900m (3000ft) |
| **Bluetooth® Wireless Technology** | |
| Bluetooth® Read Range | Proximity mode: up to 0.5m (1.6ft) Configurable**<br>Action unlock (shake): up to 5m (16.4ft) Configurable** |
| Bluetooth® Electronic Credential Transmission Technology | NRF8001 Bluetooth® version 4.0 compliant<br>Proprietary data exchange protocol. AES128 Encrypted<br>Reader App Version: 1.04.175 and above<br>Credentials can be distinguished by unique site code and card number |
| Bluetooth® Wireless Device | Protege Mobile 1.0.x |
| **NFC** | |
| NFC Read Range | Up to 60mm*** |
| NFC (Near-field communication) electronic credential transmission technology | Android 4.4 or above, with phones which support ISO7816-4<br>Proprietary Secured DESFire credential<br>Credential is AES-256 (NIST certified AES algorithm)<br>Reader App Version: 1.04.175 and above<br>Credentials can be distinguished by unique site code and card number |

| | |
|---|---|
| NFC Wireless Device | Protege Mobile 1.0.x |
| **Operating Conditions** | |
| Environment IP Rating | IP65 |
| Operating Temperature | UL/ULC -35° to 66°C (-31° to 151°F) : EU EN -40° to 70°C (-40° to 158°F) |
| Storage Temperature | -10˚ to 85˚C (14˚ to 185˚F) |
| Mean Time Between Failures (MTBF) | 520,834 hours (calculated using RFD 2000 (UTE C 80-810) Standard) |
| **Dimensions** | |
| Reader Dimensions<br>(H x W x D) | tSec Standard Reader: 115 x 45 x 18mm (4.53 x 1.77 x 0.71″)<br>tSec Extra Reader: 115 x 73 x 18mm (4.53 x 2.87 x 0.71”)<br>tSec Mini Reader: 84 x 45 x 17mm (3.31 x 1.77 x 0.67”) |
| Weight | tSec Standard Reader: 110g (3.89oz)<br>tSec Extra Reader: 155.8g (5.5oz)<br>tSec Mini Reader: 80g (2.82oz) |

* Applies to MIFARE/DESFire and Multi-Technology models only

† Applies to 125kHz and Multi-Technology models only

** Applies to Bluetooth® wireless technology enabled models only

*** Applies to NFC capable 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.

The **Bluetooth®** word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Integrated Control Technology is under license. Other trademarks and trade names are those of their respective owners.

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

# New Zealand and Australia

## Intentional Transmitter Product Statement

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

**R-NZ**

# European Standards

## CE Statement CE

Conforms where applicable to European Union (EU) Low Voltage Directive (LVD) 2014/35/EU, Electromagnetic Compatibility (EMC) Directive 2014/30/EU, Radio Equipment Directive (RED)2014/53/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU + Amendment Directive (EU) 2015/863.

This equipment complies with the rules, of the Official Journal of the European Union, for governing the Self Declaration of the CE Marking for the European Union as specified in the above directive(s).

## WEEE

**Information on Disposal for Users of Waste Electrical & Electronic Equipment**

This symbol on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, please take this product(s) to designated collection points where it will be accepted free of charge.

Alternatively, in some countries you may be able to return your products to your local retailer upon purchase of an equivalent new product.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Please contact your local authority for further details of your nearest designated collection point.

Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

**For business users in the European Union**

If you wish to discard electrical and electronic equipment, please contact your dealer or supplier for further information.

**Information on Disposal in other Countries outside the European Union**

This symbol is only valid in the European Union. If you wish to discard this product please contact your local authorities or dealer and ask for the correct method of disposal.

## EN50131 Standards

This component meets the requirements and conditions for full compliance with EN50131 series of standards for equipment classification.

EN 50131-1:2006+A2:2017, EN 50131-3:2009, EN 50131-6:2008+A1:2014, EN 50131-10:2014, EN 50136-1:2012, EN 50136-2:2013, EN 60839-11-1:2013

**Security Grade 4**
**Environmental Class II**
Equipment Class: Fixed
Readers Environmental Class: IVA, IK07
SP1 (PSTN – voice protocol)
SP2 (PSTN – digital protocol),
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + PSTN)

**Tests EMC (operational**) according to EN 55032:2015
**Radiated disturbance** EN 55032:2015
**Power frequency Magnetic field immunity tests** (EN 61000-4-8)

# UL and ULC Installation Requirements

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

## CAN/ULC-S319

- 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.

## UL 294

- 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.
- A means of verification shall be employed by the user to enable access to the wireless electronic device such as a PIN or biometric feature, which subsequently provides access to the credential application software present on the wireless electronic device.
- The access control system shall have the means to distinguish between the type of credential used via code or description (e.g. authentication/digital signature keys received from a physical card vs. authentication/digital signature keys received from a wireless electronic credential.)

### Performance Levels

| | Destructive Attack | Line Security | Endurance | Standby Power |
|---|---|---|---|---|
| tSec Standard Reader | Level I | Level I when wired with Wiegand<br>Level IV when wired with RS485 | Level IV | Level I |
| tSec Mini Reader | Level I | Level I when wired with Wiegand<br>Level IV when wired with RS485 | Level IV | Level I |
| tSec Extra Reader | Level I | Level I when wired with Wiegand<br>Level IV when wired with RS485 | Level IV | Level I |

# FCC Compliance Statements

## FCC PART 15, WARNINGS: INFORMATION TO USER

This equipment complies 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.

# 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.

CAN ICES-3 (A)/NMB-3(A)

# 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.

**New Zealand**
4 John Glenn Ave
Rosedale
Auckland 0632
Email: sales@ict.co
Toll free: (0800) 428 111
Ph: +64 9 476 7124

**USA**
5265 S Rio Grande Street
Suite 201
Littleton, CO 80120
Email: ussales@ict.co
Toll free: (855) 428 911
Ph: +1 720 442 0767

**Canada**
6201 Highway 7
Unit 7
Vaughan, Ontario, L4H 0K
Email: cansales@ict.co
Ph: +1 647 724 3428

**Australia**
Building 4
39-43 Duerdin Street
Notting Hill, VIC 3168
Email: ausales@ict.co
Ph: +61 426 145 907

**EMEA**
Email: emeasales@ict.co
Ph: +44 1625 800078

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.