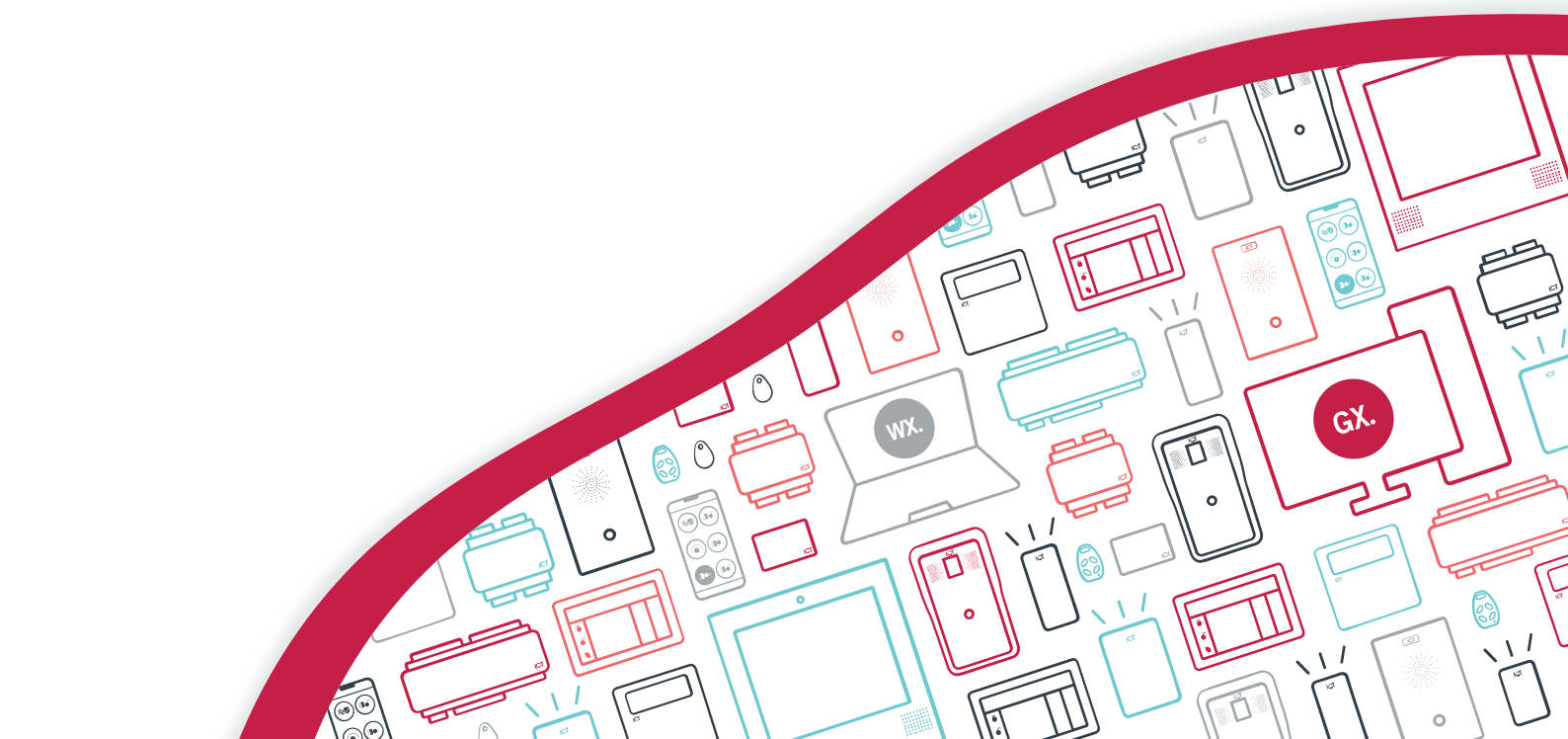
tSec Reader Range

tSec Multi-Technology Card Reader with Bluetooth® Wireless Technology

Installation Manual



Last Published: 02-Feb-23 4:48 PM

Contents

Introduction

This installation manual provides instructions and technical specifications for physical installation of the ICT tSec Multi-Technology Card Reader. For programming information, see the ICT Card Reader Configuration Guide, available from the ICT website.

About This Module

The tSec Multi-Technology Card 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 card reader can operate using Wiegand, intelligent RS-485 or OSDP 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 intend to program will operate with the configured access control or security product.

Current features of the tSec reader range include:

- Multi-card technology provides support for 125KHz, MIFARE and DESFire cards
- Encrypted RS-485, un-encrypted configurable RS-485 or standard Wiegand connection
- Support for OSDP (Open Supervised Device Protocol) version 2.2 communication with secure channel protocol
- 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 GX function codes and other features (programming requires RS-485 connection or Protege Config App)
- Keep alive transmission every 30 seconds for intelligent tamper management
- Programmable via programming cards and the Protege Config App
- Keypad output on Wiegand data lines (keypad versions only)
- Fully encapsulated design with environmental IP rating of IP65 for outdoor and indoor operation
- tSec readers are shipped in Wiegand configuration by default

Reader Editions

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

Standard	117 x 46 x 18mm (4.61 x 1.81 x 0.71″)				
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology	Vandal Resistant Cover*
PRX-TSEC-STD-B tSec Standard Multi-Technology Card Reader		✓	✓		
PRX-TSEC-STD-KP-B tSec Standard Multi-Technology Card Reader with Keypad	✓	✓	✓		
PRX-TSEC-STD-125-B tSec Standard 125kHz Card Reader		✓			
PRX-TSEC-STD-DF-B tSec Standard 13.56MHz Card Reader			✓		
PRX-TSEC-STD-DF-KP-B tSec Standard 13.56MHz Card Reader with Keypad	✓		✓		
PRX-TSEC-STD-BT-B **PRX-TSEC-STD-BT-W** tSec Standard Multi-Technology Card Reader with Bluetooth® Wireless Technology		✓	✓	✓	
PRX-TSEC-STD-KP-BT-B **PRX-TSEC-STD-KP-BT-W** tSec Standard Multi-Technology Card Reader with Keypad and Bluetooth® Wireless Technology	✓	✓	✓	✓	
PRX-TSEC-STD-KP-BT-B-VRC tSec Standard Multi-Technology Card Reader with Keypad, Vandal Resistant Cover and Bluetooth® Wireless Technology	✓	✓	✓	✓	✓
PRX-TSEC-STD-DF-BT-B tSec Standard 13.56MHz Card Reader with Bluetooth® Wireless Technology			✓	✓	
PRX-TSEC-STD-DF-KP-BT-B 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.

Extra	117 x 75x 18mm (4.61 x 2.95 x 0.71")				
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology	Vandal Resistant Cover*
PRX-TSEC-EXTRA-KP-B tSec Extra Multi-Technology Card Reader with Keypad	✓	✓	✓		
PRX-TSEC-EXTRA-125-B tSec Extra 125kHz Card Reader		✓			
PRX-TSEC-EXTRA-DF-B tSec Extra 13.56MHz Card Reader			✓		
PRX-TSEC-EXTRA-DF-KP-B tSec Extra 13.56MHz Card Reader with Keypad	✓		✓		
PRX-TSEC-EXTRA-BT-B **PRX-TSEC-EXTRA-BT-W** tSec Extra Multi-Technology Card Reader with Bluetooth® Wireless Technology		✓	✓	✓	
PRX-TSEC-EXTRA-KP-BT-B **PRX-TSEC-EXTRA-KP-BT-W** tSec Extra Multi-Technology Card Reader with Keypad and Bluetooth® Wireless Technology	✓	✓	✓	✓	
PRX-TSEC-EXTRA-KP-BT-B-VRC tSec Extra Multi-Technology Card Reader with Keypad, Vandal Resistant Cover and Bluetooth® Wireless Technology	✓	✓	✓	✓	✓
PRX-TSEC-EXTRA-DF-BT-B 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.

Mini	85 x 46 x 17mm (3.35 x 1.81 x 0.67”)				
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology	Vandal Resistant Cover*
PRX-TSEC-MINI-B tSec Mini Multi-Technology Card Reader		✓	✓		
PRX-TSEC-MINI-125-B tSec Mini 125kHz Card Reader		✓			
PRX-TSEC-MINI-DF-B tSec Mini 13.56MHz Card Reader			✓		
PRX-TSEC-MINI-BT-B **PRX-TSEC-MINI-BT-W** tSec Mini Multi-Technology Card Reader with Bluetooth® Wireless Technology		✓	✓	✓	
PRX-TSEC-MINI-DF-BT-B 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

Secured MIFARE Card Format

Secured MIFARE is the compromise between secured cards 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 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
- 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. For a truly convenient touch-and-go experience, MIFARE DESFire EV2 offers increased operating distance.

Based on global open standards for both air interface and cryptographic methods, it complies with all requirements for fast and highly secure data transmission and flexible application management.

- Fully compliant with all levels of the international standard ISO/IEC 14443A
- Common Criteria EAL5+ security certified
- 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
- Backwards compatible with all previous MIFARE DESFire generations

About MIFARE DESFire EV3

The latest addition to the MIFARE DESFire product family, MIFARE DESFire EV3 offers even more advanced hardware and software implementation on a brand new internal chip, and combines enhanced performance with a greater operating distance and improved transaction speed compared to its predecessors.

Based on global open standards for both air interface and cryptographic methods, it uses the same security certification level as IC products used for banking cards and electronic passports. Featuring an on-chip backup management system and mutual three-pass authentication, EV3 supports confidential and integrity-protected communication with secure dynamic messaging and mirroring.

- Fully compliant with the international standard ISO/IEC 14443 Type A 1-4 and ISO/IEC 7816-4
- Common Criteria EAL5+ security certified for IC hardware and software
- NFC Forum Tag Type 4 certified
- Secure, high speed command set
- Unique 7-byte serial number
- Choice of open DES/2K3DES/3K3DES/AES crypto algorithms
- Open AES 128 bits crypto algorithm in hardware
- Fully interoperable with existing NFC reader infrastructure
- Transaction timer mitigates risk of man-in-the-middle attacks
- Backwards compatible with all previous MIFARE DESFire generations

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 physical credential options in the MIFARE/DESFire range, including MIFARE Classic and MIFARE DESFire EV1, EV2 and EV3.

Physical Credentials

- Proximity clamshell card
- Proximity ISO card
- Proximity ISO dual technology card
- Proximity standard key tag
- Proximity adhesive disc
- Proximity silicone wristband

Physical credentials are available in an extensive range of technology and EEPROM size configurations. Visit the ICT website to view the full range of proximity products.

For more information on configuration options and ordering, contact ICT Customer Services.

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 provides 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

Cables are intended to be run inside the wall. If cables are to be run through external conduits you must use the surface mount box accessory (see page 14).

1. Select where to mount the card 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 card reader as a guide to correctly position the unit.
2. Hold the rear case section against the wall and mark the mounting holes and cable entry area. The cable entry area should align with a hole cut through the wall.
3. Use appropriate screws (not supplied) to affix the case to the wall.
4. Run the wiring. Leave about 20cm (8") of wire protruding through the center of the mounted half of the case.
5. Connect the wiring to the reader electronics. Refer to later sections of this manual for the wiring connections.
6. Clip the upper rim of the front case over the upper rim of the rear case, then press gently on the front case until the lower rim slots over the lower rim of the rear case, lining up the screw hole at the bottom.
7. To complete the installation, use the M3 x 8mm Plastite screw provided with the card reader to secure and fasten the front case to the rear mounted case.

Mounting with Vandal Resistant Cover Accessory

The optional vandal resistant cover (VRC) accessory provides durability and protection against vandalism and malicious damage. The flush design also serves as an anti-ligature measure for an additional level of safety.

The vandal resistant cover accessory has not been evaluated for UL/ULC applications.

Sealing Gasket

The gasket included with the VRC provides a sealing layer between the mounting surface and the reader/cover to help ensure a sealed vandal-proof installation. The gasket is provided in two distinct pieces, allowing for easy alignment with the hardware and mounting holes. The smaller inner piece is shaped to fit the reader, while the larger outer piece is shaped to fit the vandal resistant cover. The adhesive side of the gasket may be applied to either the mounting surface or the hardware, to suit installation conditions and preference.

Mounting the Reader with Vandal Resistant Cover

1. Select where to mount the card 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 card reader as a guide to correctly position the unit.
2. Hold the rear case section against the wall and mark the mounting holes and cable entry area. The cable entry area should align with a hole cut through the wall.
3. Remove the backing tape from the smaller (reader) gasket and place it carefully in position with the mounting holes and cable entry aligned, then apply pressure to ensure the gasket is securely adhered in place.

It may be preferable to adhere the gasket to the back of the reader case, aligned with the mounting holes and cable entry, and affix the reader case to the wall with the gasket attached.

4. Use appropriate screws (not supplied) to affix the rear case to the wall, aligned over the gasket.
5. Run the wiring. Leave about 20cm (8") of wire protruding through the center of the mounted half of the case.
6. Connect the wiring to the reader electronics. Refer to later sections of this manual for the wiring connections.
7. Clip the upper rim of the front case over the upper rim of the rear case, then press gently on the front case until the lower rim slots over the lower rim of the rear case, lining up the screw hole at the bottom.
8. To complete the reader installation, use the M3 x 8mm Plastite screw provided with the card reader to secure and fasten the front case to the rear mounted case.
9. Apply a silicone seal around the **top and sides** of the reader (see below).
10. Remove the backing tape from the larger (VRC) gasket and place it carefully in position around the reader, then apply pressure to ensure the gasket is securely adhered in place.

    It may be preferable to adhere the gasket to the back of the vandal resistant cover, aligned with the mounting holes, and affix the cover to the wall with the gasket attached.

11. Use appropriate screws (not supplied) to affix the vandal resistant cover to the wall, aligned over the gasket.

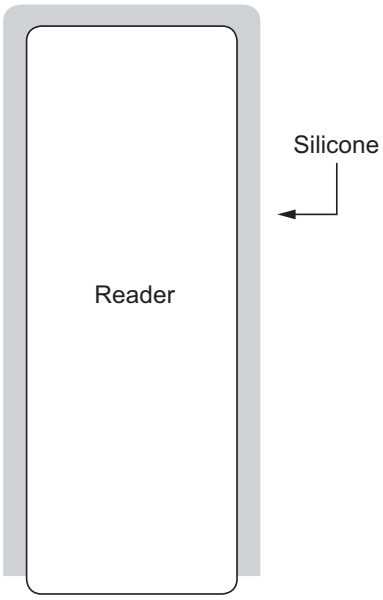
Vandal-proof Silicone Seal

Before installing the vandal resistant cover, silicone is applied along the top and side edges of the card reader to ensure a sealed vandal-proof installation and maintain the impact protection rating.

The silicone is applied after the reader has been mounted, forming an exact fit at the mounting location.

- Ensure that the bottom of the reader is not sealed, so that the faceplate can still be removed.
- Be careful not to leave excess silicone which may impede the VRC mounting.
- To ensure an exact seal, the VRC should ideally be mounted before the silicone sets.

The diagram below demonstrates the placement of the silicone seal.



Mounting with Surface Mount Box Accessory

The optional surface mount box (SMB) accessory enables you to mount the card reader projected from the wall, allowing space for cabling from external conduits. The surface mount box has the same height and width as the card reader rear case, with additional depth.

The processes for mounting Standard and Extra readers with the surface mount box are slightly different.

The surface mount box accessory has not been evaluated for UL/ULC applications.

Mounting the Standard Reader with Surface Mount Box

1. Select where to mount the card 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 card reader as a guide to correctly position the unit.
2. Hold the surface mount box against the wall and mark the mounting holes.
3. Mark the intended entry point for the external conduit on the top, bottom or side of the surface mount box. This must be aligned in the **center** of the box side wall. Drill a hole to accommodate cable entry.

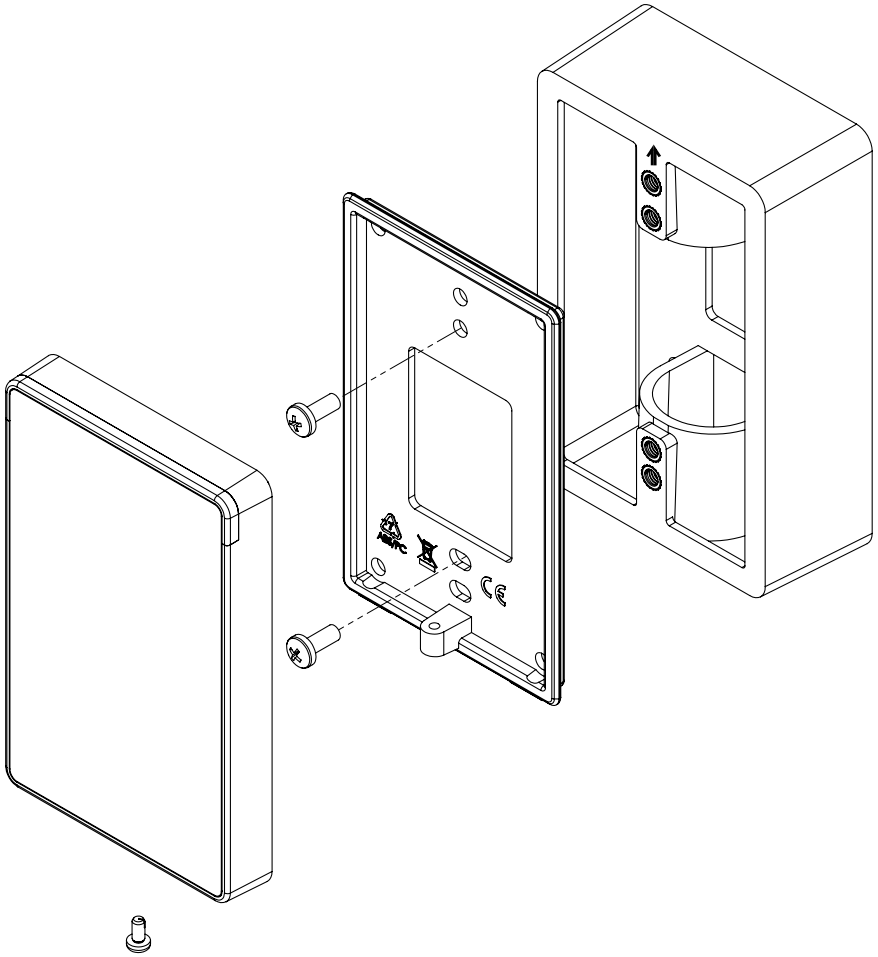
   Warning: Do not drill a hole with a diameter greater than **20mm (0.8")** in the surface mount box. Do not drill off-center. Drilling too close to the edge of the surface mount box may cause structural damage.
4. Use appropriate screws (not supplied) to affix the surface mount box to the wall.
5. Connect the wiring to the reader electronics through the conduit hole. Refer to later sections of this manual for the wiring connections.
6. Clip the upper rim of the front case over the upper rim of the surface mount box, then press gently on the front case until the lower rim slots over the lower rim of the surface mount box, lining up the screw hole at the bottom.
7. To complete the installation, use the M3 x 8mm Plastite screw provided with the card reader to secure and fasten the front case to the surface mount box.

Mounting the Extra Reader with Surface Mount Box

1. Select where to mount the card 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 card reader as a guide to correctly position the unit.
2. Hold the surface mount box against the wall and mark the mounting holes.
3. Mark the intended entry point for the external conduit on the top, bottom or side of the surface mount box. This must be aligned in the **center** of the box side wall. Drill a hole to accommodate cable entry.

   Warning: Do not drill a hole with a diameter greater than **20mm (0.8")** in the surface mount box. Do not drill off-center. Drilling too close to the edge of the surface mount box may cause structural damage.
4. Use appropriate screws (not supplied) to affix the surface mount box to the wall.

   Important: Ensure that you mount the surface mount box in the correct orientation, positioned with the embossed **arrow** at the **top**, pointing up. The mounting holes are offset from the reader case center, so if the surface mount box is upside down the edge of the reader will not align with the edge of the mounting box.
5. Hold the rear case of the card reader against the surface mount box in the correct orientation. Line up the holes on the rear case with the threaded inserts closest to the center of the surface mount box, as shown in the image below.



6. Affix the rear case to the surface mount box using the two M4 x 10mm screws provided.
7. Connect the wiring to the reader electronics through the conduit hole. Refer to later sections of this manual for the wiring connections.
8. Clip the upper rim of the front case over the upper rim of the rear case, then press gently on the front case until the lower rim slots over the lower rim of the rear case, lining up the screw hole at the bottom.
9. To complete the installation, use the M3 x 8mm Plastite screw provided with the card reader to secure and fasten the front case to the rear mounted case.

Reader Connection

Using the recommended cables, splice the cable together with the pigtail of the reader and seal the splice. Route the cable from the reader to the host module. Connect the cable to the module port according to the required operation, as shown in the connection diagrams that follow.

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.

Shield Connection

Connect the reader pigtail shield and cable shield wires together at the reader pigtail splice. Connect the cable shield to a suitable earth point. **Do not** connect the cable shield to a ground or AUX connection. The reader pigtail shield wire is **not** terminated inside the reader.

Important:

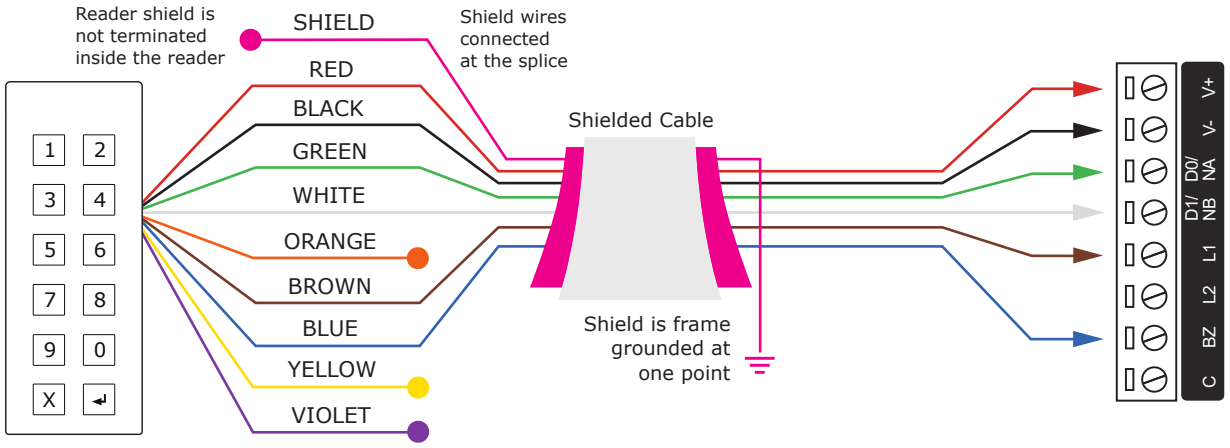
- The card reader must be connected to the module port using a shielded cable.
- The shield must only be connected at one end of the cable in the metallic enclosure (frame grounded).
- Do not connect the cable shield to an AUX-, 0V or V- connection on the module.
- Do not connect the cable shield to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

Wiegand Reader Connection

When using the standard Wiegand interface to access a reader expander, two wiring methods can be used.

Single LED allows a single LED line to control both LED colors.

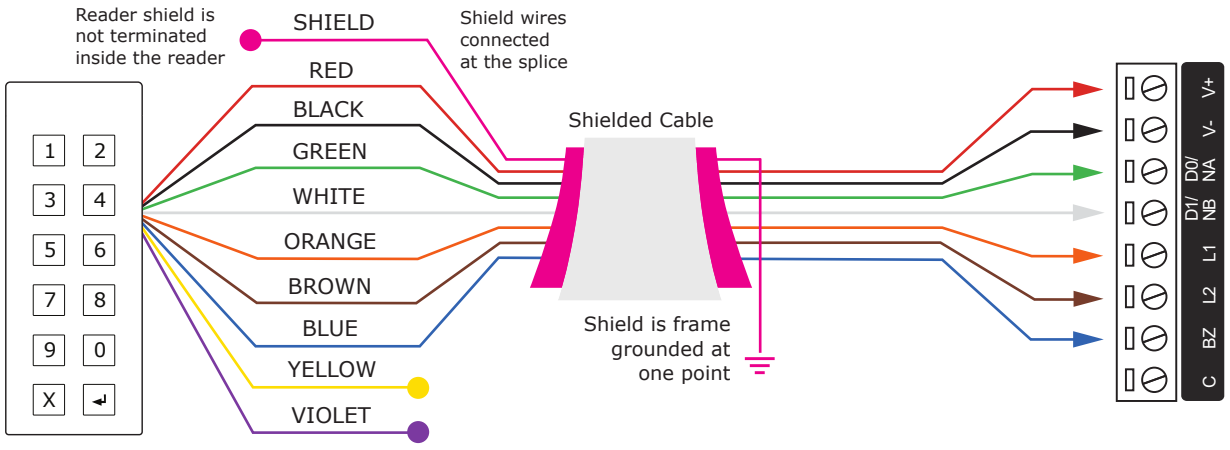
Single LED Connection



Readers are shipped in single LED mode by default.

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.

Dual LED Connection



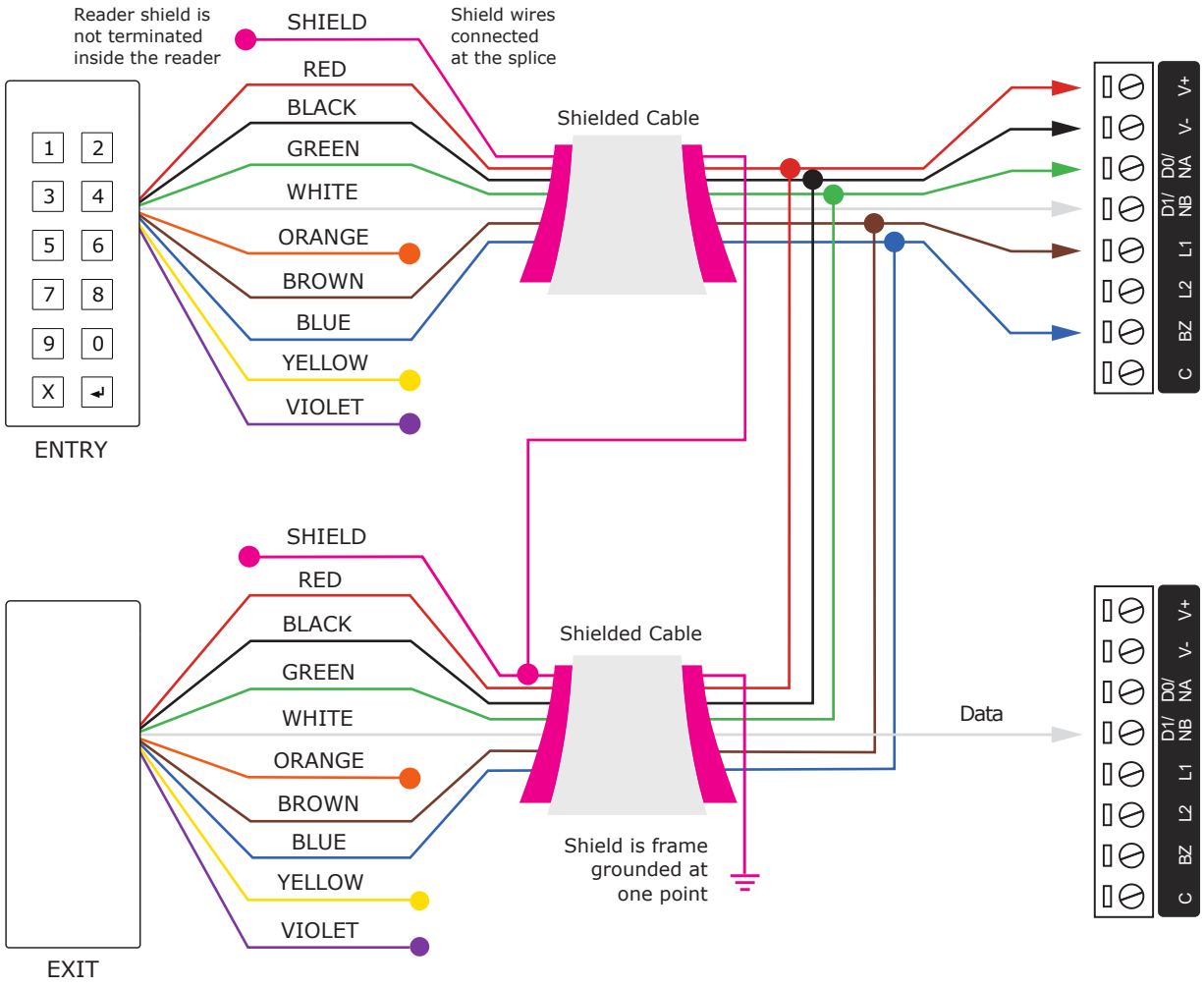
Readers also need to be programmed to operate in dual LED mode. For programming instructions, see the ICT Card Reader Configuration Guide, available from the ICT website.

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 card reader has all connections wired to the same reader port as the primary reader, except the Data 1 connection which is wired to the Data 1 input on the alternate reader port.

The normal primary reader connection operates as the **entry** reader, and the secondary reader that is multiplexed into the alternate reader port will operate as the **exit** reader.



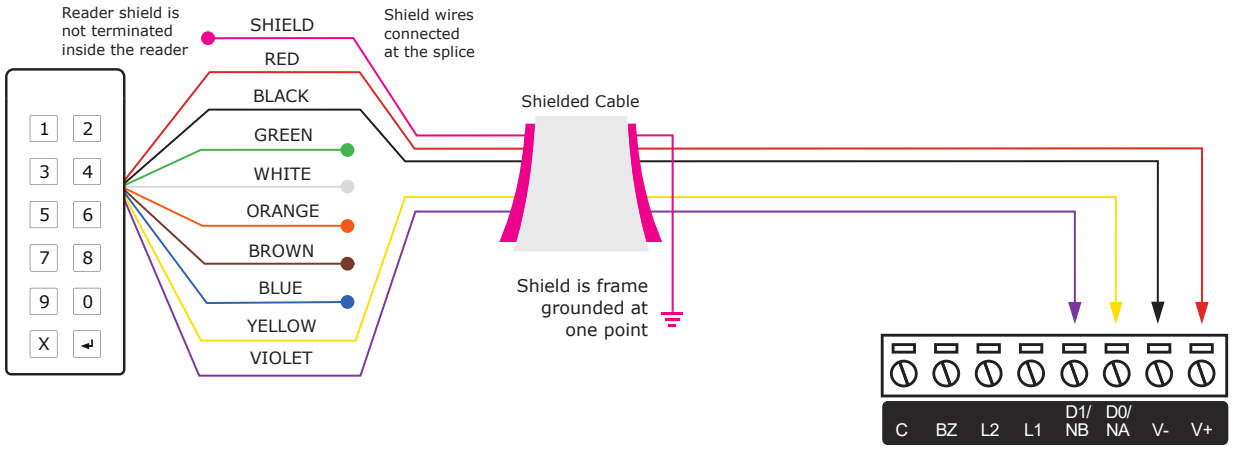
RS-485 Reader Locations

As two RS-485 readers can be connected to the same RS-485 reader port, configuration of the **green** and **orange** wires uniquely identifies the reader, and determines 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.

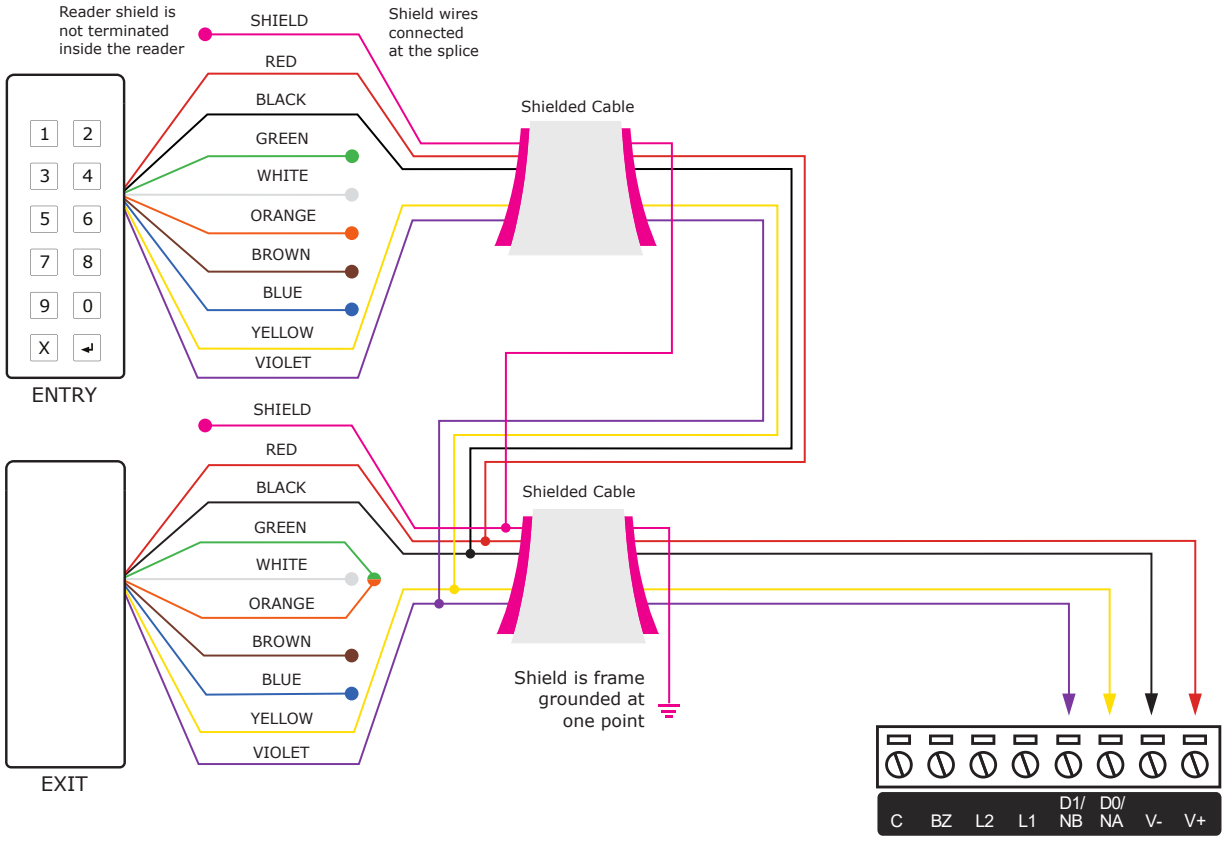
RS-485 Reader Connection

The connection of a single RS-485 reader to a reader expander.



RS-485 Reader Connection (Entry/Exit)

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



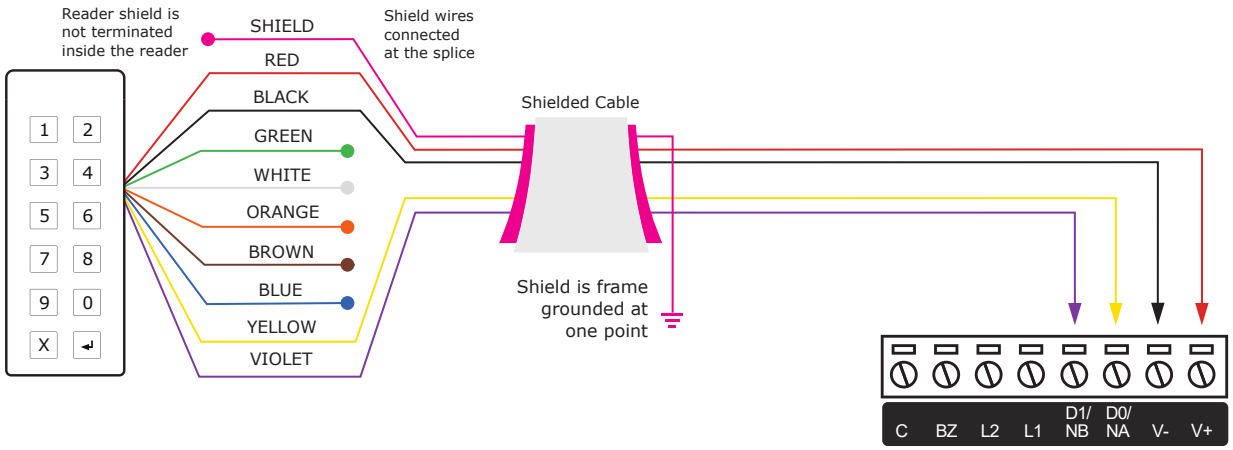
The exit reader has the **green** and **orange** wires connected together.

A 330 ohm EOL (End of Line) resistor may be required to be inserted between the yellow and violet wires after the join.

OSDP Reader Connection

OSDP reader mode is only available for card readers with firmware version 1.04.277 or higher. Readers that only support 125kHz reading and readers with PSK hardware **do not** support OSDP.

Connecting a card reader in OSDP mode is the same as the connection for standard RS-485 configuration.



Readers must also be programmed to operate in OSDP mode. For more information, see Programming the Card Reader (page 22).

For more information about OSDP support on ICT card readers, including configuring readers for secure channel communications, see Application Note 321: Configuring ICT Readers for OSDP Communication.

OSDP Baud Rate Requirement

For a card reader operating in OSDP mode to communicate with an OSDP server, the reader must have the same baud rate setting as the reader port it is connected to. The default reader baud rate is 38400.

ICT card readers support the following baud rates:

Supported Baud Rates
4800 baud
9600 baud
19200 baud
38400 baud (default)
57600 baud
115200 baud

The card reader baud rate can be programmed using:

- A mobile device running the Protege Config App
- A correctly encoded MIFARE config card

A suitably configured MIFARE config card can be ordered from the ICT customer services team.

For detailed information on programming ICT card readers, see the ICT Card Reader Configuration Guide, available from the ICT website.

Reader Addressing

For a card reader operating in OSDP mode to be recognized on a third-party system, the reader address may need to be configured to meet the third-party system's addressing requirements.

For the tSec range of card readers the address and addressing options are determined by the reader's wiring configuration. When the reader is powered up it checks the configuration to determine its address.

1. If the reader's green and orange wires are **not** connected together it uses address 0 as its default address, unless it has been programmed with a specific address.

   The reader's address can be programmed using a mobile device running the Protege Config App.

   The Config App **Reader Configuration** will need a config with the **Reader Address** TLV selected, with the address set as required for the third-party system.

2. If the reader's green and orange wires are connected together it is hardwired to **always** use 1 as its address. The address is not programmable.

Programming the Card Reader

ICT card readers can be programmed for a wide range of functionality to suit your site's requirements.

Card reader programming is configured by applying specific TLV (Type Length Value) settings to the reader to enable, disable and configure reader options. ICT reader configuration can be programmed using:

- A mobile device running the Protege Config App
- An encoded MIFARE config card
- A 125kHz programming card

Programming options are dependent on hardware compatibility and firmware versions.

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

For detailed programming instructions, see the ICT Card Reader Configuration Guide, available from the ICT website.

Protege Config App

The Protege Config App provides a secure, convenient and flexible method for programming a Bluetooth® enabled ICT card reader.

To use the Config App you will need:

- An app account
- A mobile credential

To use the Config App to program a card reader, the reader must meet the following requirements:

- Firmware version 1.04.254 or higher
- Bluetooth® capability

Programming Summary

To program a card reader using the Config App:

1. Log in to the app using your app account.
2. Select your **Credential Profile**.

   Your credential profile is automatically assigned to your app account with your mobile credential, and is based on the credential issuer and the site the credential was allocated to.
3. Create a **Reader Configuration** (config) comprising the required TLV settings.
4. Activate Bluetooth® on your device (if not already activated).
5. Power cycle the reader you want to program.
6. Select the **config** to program the reader with.
7. Apply the configuration to the reader, within two minutes of startup. Hold your mobile device close to the reader and tap **Scan Closest** to apply the configuration.

When programming is successful the reader will beep 4 times quickly, then restart.

For information on using the Config App, see the Protege Config App User Guide, available from the ICT website.

MIFARE Config Card

A MIFARE config card provides a quick and secure method for programming a card reader, by simply placing and holding the card close to the reader.

To use a config card to program a card reader, the reader must meet the following requirements:

- Firmware version 1.04.229 or higher

Using a config card to program a card reader requires a suitably configured MIFARE card. These can be ordered from the ICT customer services team (Ordering code: PRX-ISO-CONFIG).

Alternatively, config cards can be configured using the ICT Encoder Client (see below).

For details on available programming configurations, see the ICT Card Reader Configuration Guide, available from the ICT website.

Programming Summary

To program a card reader using a config card:

1. Power cycle the reader you want to program.
2. Within two minutes, place and hold the config card close to the reader.

When programming is successful, the reader will beep 5 times quickly then restart.

ICT Encoder Client

The ICT Encoder Client is a software application that allows users to encode credentials for use with their ICT card readers, Protege access control system, and optionally other third-party systems.

It also provides the ability to create customized config cards that can be used to program the functions of a card reader. This provides a flexible and convenient method for programming readers as and when needed.

To use the Encoder Client to program a config card you will need:

- A secure operator login
- A correctly configured desktop encoder: PRX-ENC-DT - Desktop USB ISO14443-A and B Proximity Card Encoder
- A blank MIFARE Classic card to encode (Ordering code: PRX-ISO-MF-BLANK)
- Sufficient encoding credits

Programming Summary

To encode a config card that will be used to program ICT card readers:

1. Log in to the Encoder Client using your secure operator login.
2. Select the required **Customer** (this will typically be the site).
3. Create a **Reader Configuration** (config) comprising the required TLV settings.
4. Place the blank MIFARE card on the desktop encoder and click **Write Config** to write the config to the card.

For information on the encoding process and requirements, see the ICT Encoder Client User Manual, available on the ICT Website.

125kHz Programming Card

125kHz capable card readers can be programmed using a 125kHz programming card, by presenting the card to the reader in a specified programming sequence.

To use a 125kHz card to program a card reader, the reader must meet the following requirements:

- Firmware version 1.04.229 or higher
- The card reader must have the capability to read 125KHz cards

Using a 125kHz programming card to program a card reader requires a suitably configured 125kHz programming card. These can be ordered from the ICT customer services team (Ordering code: PRX-PROG-LF).

Programming Summary

To program a card reader using a 125kHz programming card:

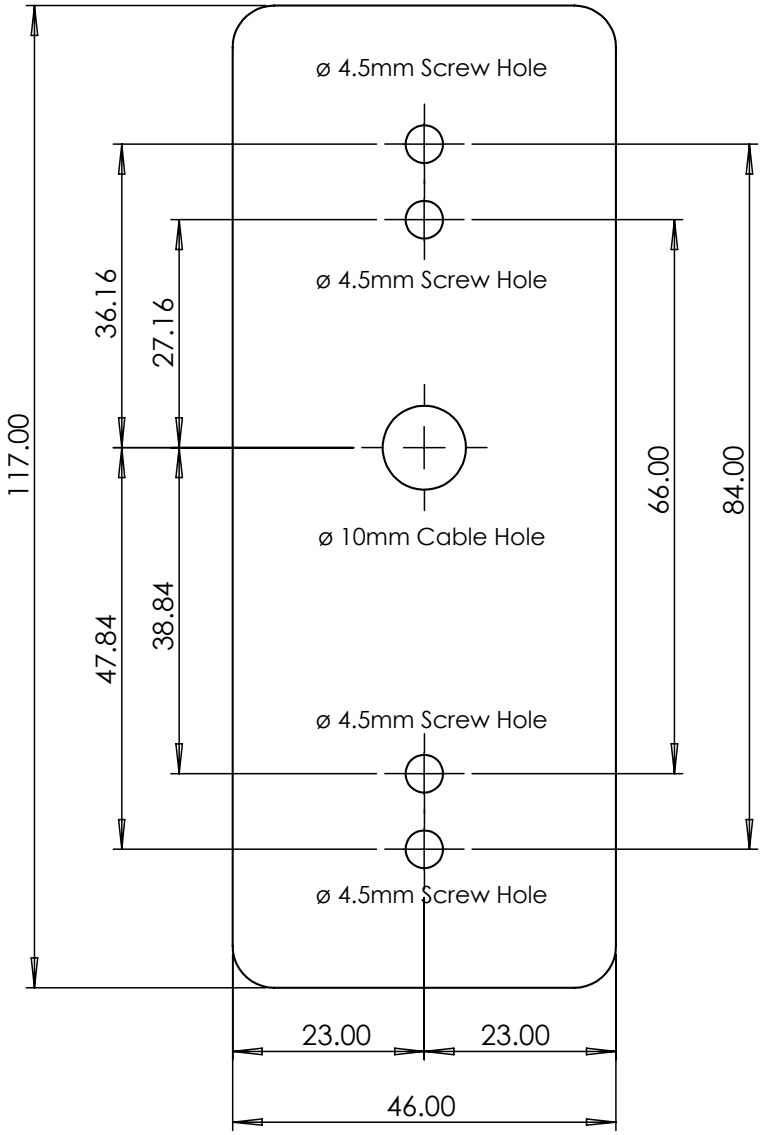
1. You will first need to power cycle the reader you want to program.
2. Within two minutes of startup, present the programming card to the reader to enter **Programming Mode**.
3. Wait for the reader to beep twice to indicate that it has entered 125kHz programming mode.
4. Present the card to the reader the required number of times in the required sequence to apply the desired programming.
5. Once complete, allow the programming interface to time out and return to normal operation.

For detailed information on programming ICT card readers using a 125kHz programming card, including the available programming options and badging sequences, see the ICT Card Reader Configuration Guide, available from the ICT website.

Technical Diagrams

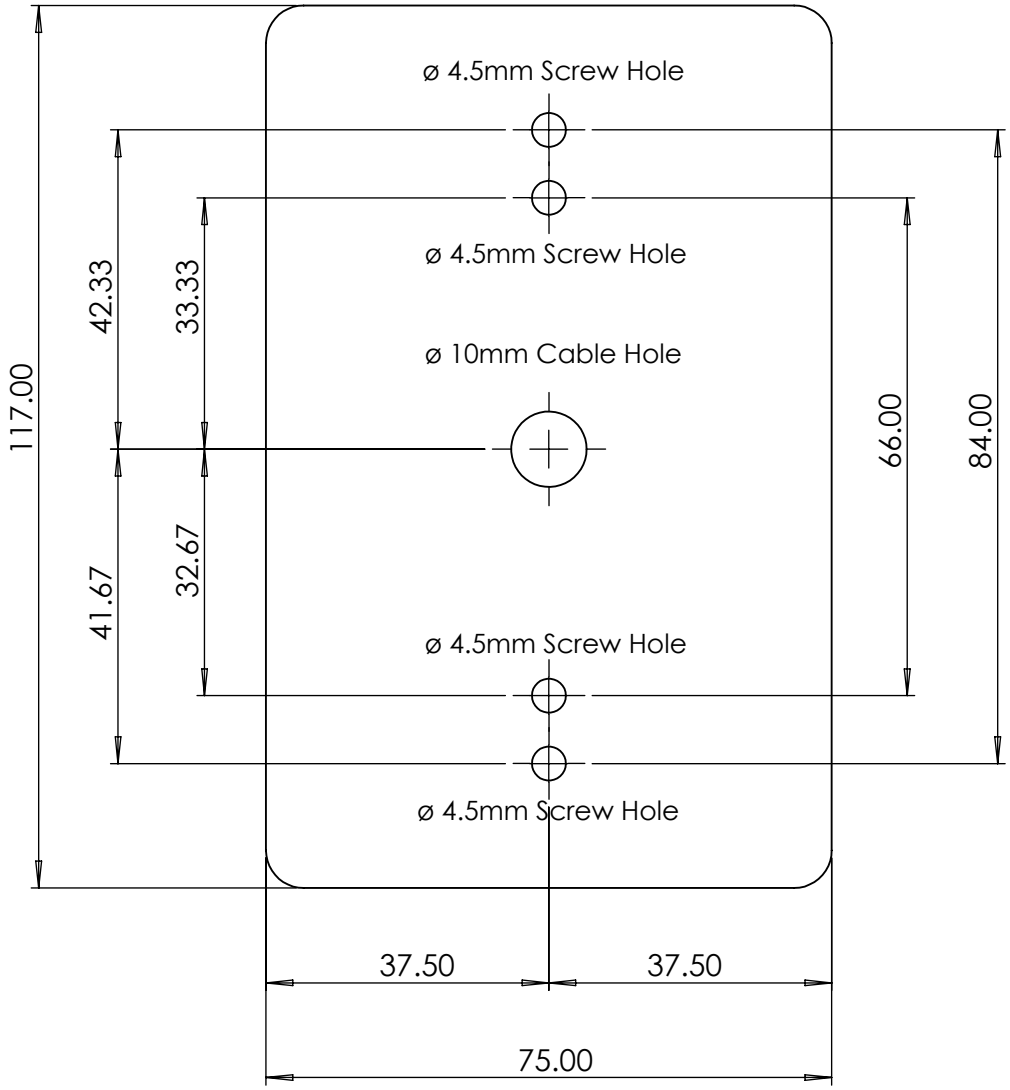
tSec Standard Reader

The dimensions shown below outline the essential details needed to help ensure the correct installation of the ICT tSec Standard reader. All measurements are shown in millimeters.



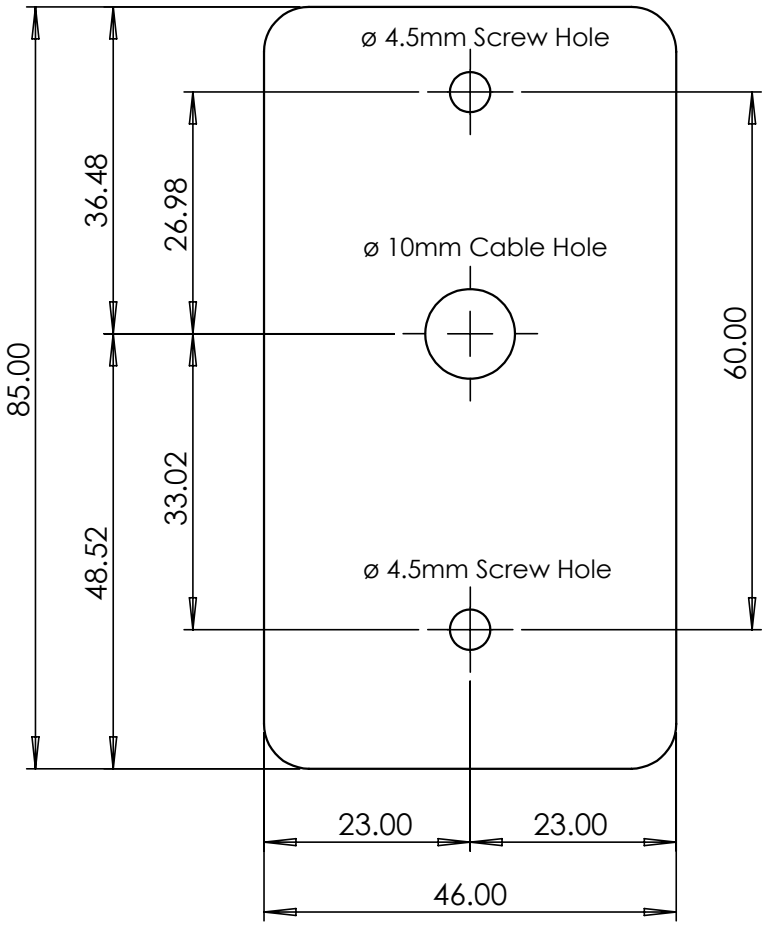
tSec Extra Reader

The dimensions shown below outline the essential details needed to help ensure the correct installation of the ICT tSec Extra Reader. All measurements are shown in millimeters.



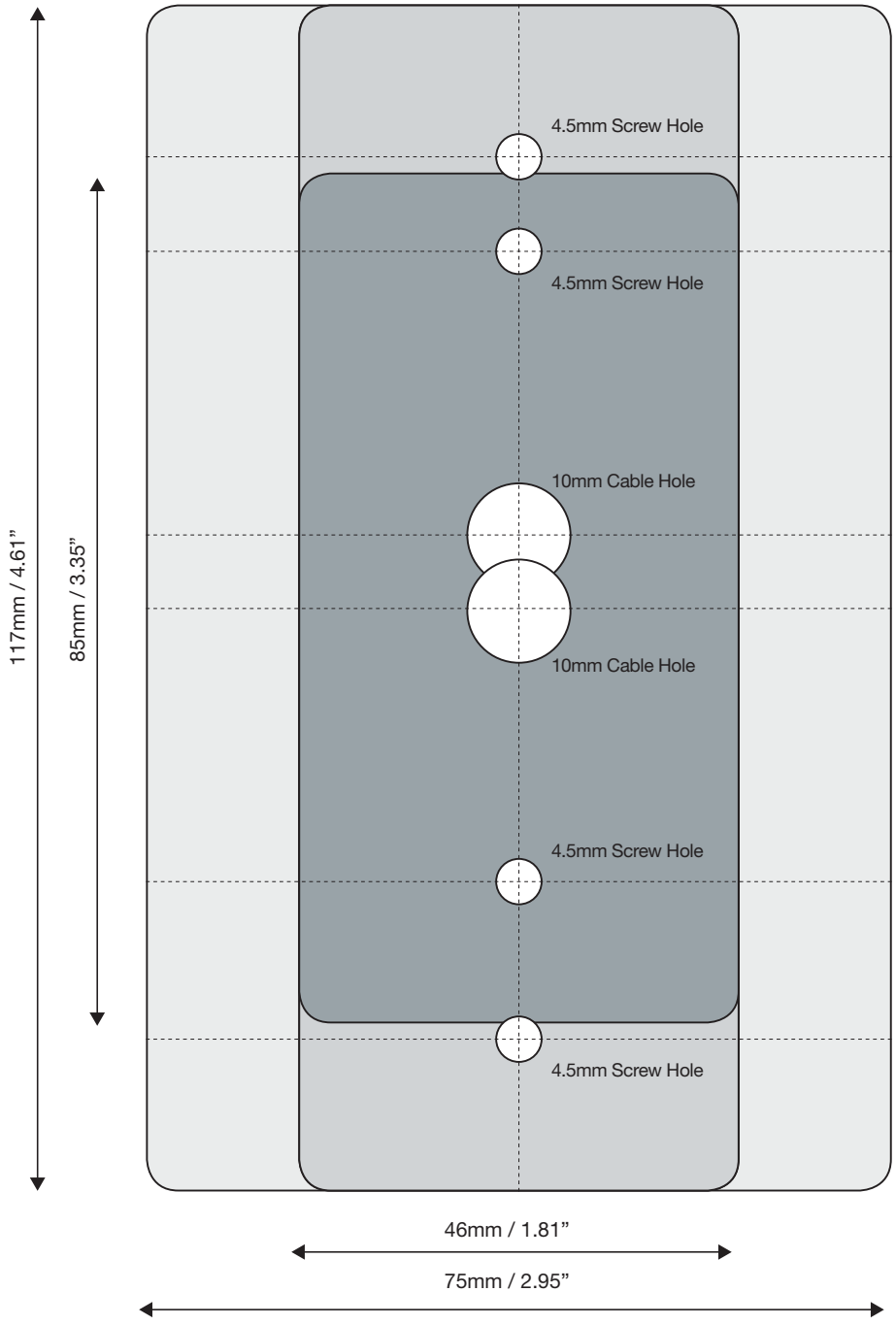
tSec Mini Reader

The dimensions shown below outline the essential details needed to help ensure the correct installation of the ICT tSec Mini reader. All measurements are shown in millimeters.



Reader Comparison

The dimensions shown below provide a direct comparison of the reader models.



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 Reader Editions.
Power Supply	
Operating Voltage	12VDC (9.5 to 14VDC)
Operating Current	Standard Reader: 254mA (Peak, Reading) Extra Reader: 298mA (Peak, Reading) Mini Reader: 203mA (Peak, Reading)
Communications	
Card Read Range	MIFARE 60mm (2.36") * DESFire EV1 ISO 15mm (0.6") * 125kHz Clamshell 40mm (1.57") †
Tag Read Range	MIFARE 30mm (1.2") * DESFire EV1 6mm (0.23") * 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 * 125KHz pulse width modulated †
Multi Conductor Cable	Wiegand: 22Awg alpha 5196, 5198, 18Awg alpha 5386, 5388. Max Distance 150m (492ft) Module comms/RS485: Belden 9842 or equivalent. Max distance 900m (3000ft)
OSDP Communication	OSDP standard 2.2 with Secure Channel Protocol ** / ***
Bluetooth® Wireless Technology	
Bluetooth® Read Range	Proximity mode: up to 0.5m (1.6ft) Configurable ** Action unlock (shake): up to 5m (16.4ft) Configurable **
Bluetooth® Electronic Credential Transmission Technology	NRF8001 Bluetooth® version 4.0 compliant Proprietary data exchange protocol. AES128 Encrypted Reader App Version: 1.04.175 and above 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 Proprietary Secured DESFire credential Credential is AES-256 (NIST certified AES algorithm) Reader App Version: 1.04.175 and above 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 (H x W x D)	Standard Reader: 117 x 46 x 18mm (4.61 x 1.81 x 0.71″) Extra Reader: 117 x 75 x 18mm (4.61 x 2.95 x 0.71″) Mini Reader: 85 x 46 x 17mm (3.35 x 1.81 x 0.67″)
Vandal Resistant Cover (H x W x D)	PRX-SVRC Standard Reader Cover: 162 x 91 x 22.6mm (6.37 x 3.58 x 0.88″) PRX-XVRC Extra Reader Cover: 162 x 120 x 22.6mm (6.37 x 4.72 x 0.88″) PRX-MVRC Mini Reader Cover: 127 x 88 x 20mm (5.0 x 3.46 x 0.78″)
Reader with Surface Mount Box (H x W x D)	Standard Reader: 117 x 46 x 51mm (4.61 x 1.81 x 2.00″) Extra Reader 119 x 77 x 52mm (4.69 x 3.05 x 2.05″)

Reader Weights	Net Weight	Gross Weight
Standard Reader Standard Reader with Vandal Resistant Cover	110g (3.9oz) 190g (6.7oz)	130g (4.6oz) 280g (9.9oz)
Extra Reader Extra Reader with Vandal Resistant Cover	160g (5.6oz) 270g (9.5oz)	190g (6.7oz) 360g (12.7oz)
Mini Reader	80g (2.8oz)	100g (3.5oz)
Standard Reader Surface Mount Box Extra Reader Surface Mount Box	40g (1.4oz) 70g (2.5oz)	60g (2.1oz) 100g (3.5oz)

* 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.

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)
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + USB-4G modem)

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

UK Conformity Assessment Mark

General Product Statement

The UKCA Compliance Label indicates that the supplier of the device asserts that it complies with all applicable standards.

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-60839-11-1

- This card reader is CAN/ULC-60839-11-1 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-60839-11-1 Listed portal locking device(s) for ULC installations.
- Input power must be supplied by a Class 2 or power limited device.

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

ICT Standard Reader	Level I	Level I when wired with Wiegand Level IV when wired with RS485	Level IV	Level I
ICT Mini Reader	Level I	Level I when wired with Wiegand Level IV when wired with RS485	Level IV	Level I
ICT Extra Reader	Level I	Level I when wired with Wiegand 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)

OSDP Verified Logo

Open Supervised Device Protocol (OSDP) Verified Certification

The OSDP Verified logo indicates that this device is compliant with the OSDP 2.2 PD Secure profile and all applicable standards.

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.

Submitted to UL 28-Nov-22

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