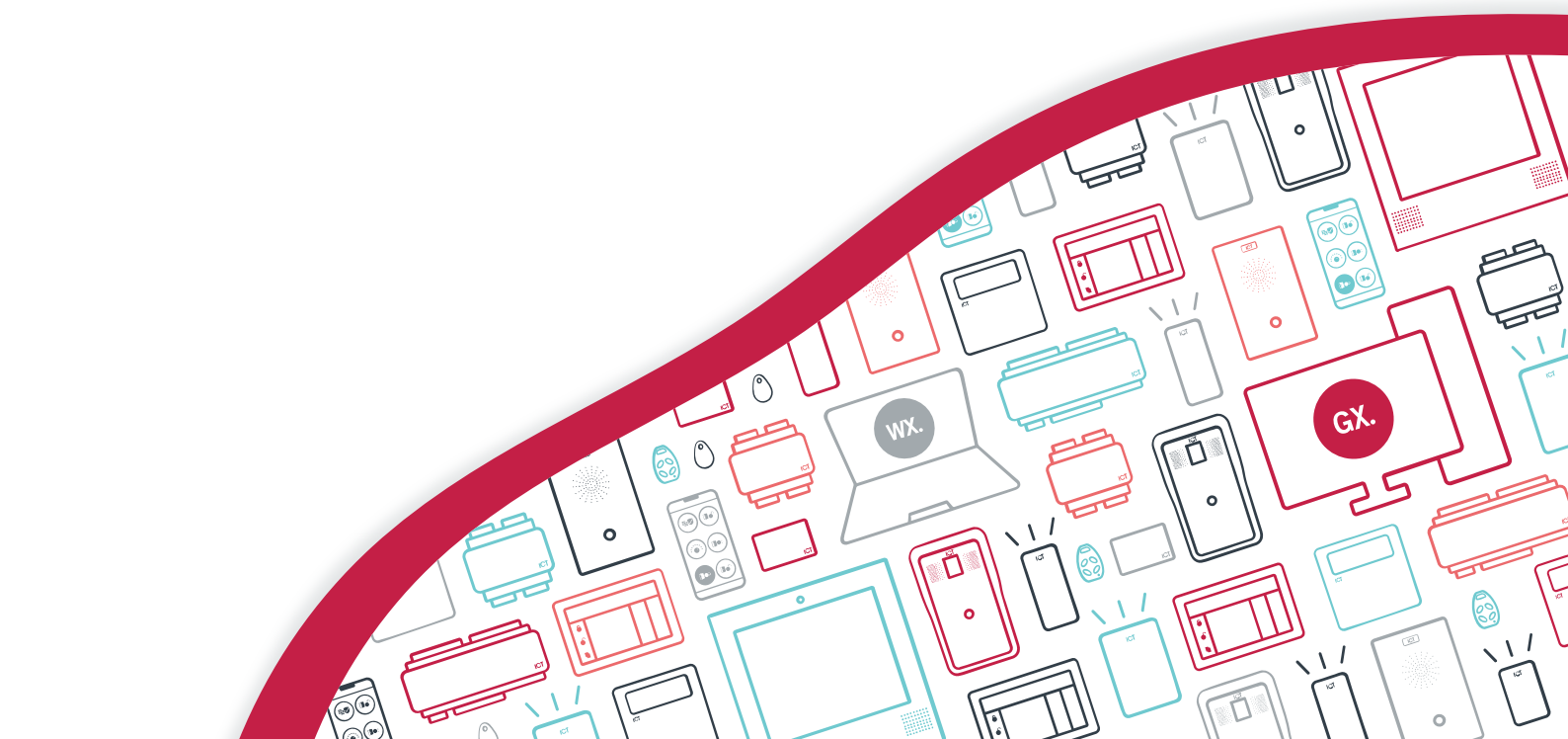
PRX-TSEC Range

tSec Multi-Technology Card Reader with Bluetooth® Wireless Technology

Installation Manual



Last Published: 25-May-21 4:56 PM

Contents

Introduction

The ICT 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 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 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) 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 (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	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.

tSec Extra Reader	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.

tSec Mini Reader	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

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 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 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 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 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

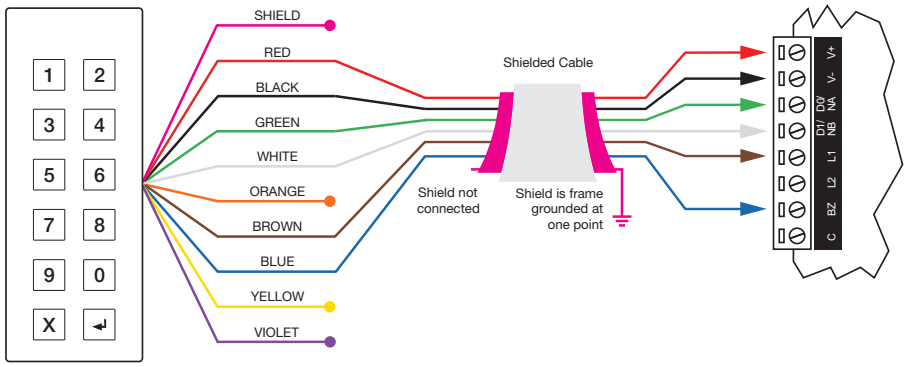
Warning: The reader outputs D0 (green wire) and D1 (white wire) can switch to a maximum capacity of 50mA. Exceeding this amount will damage the output.

Wiegand 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.

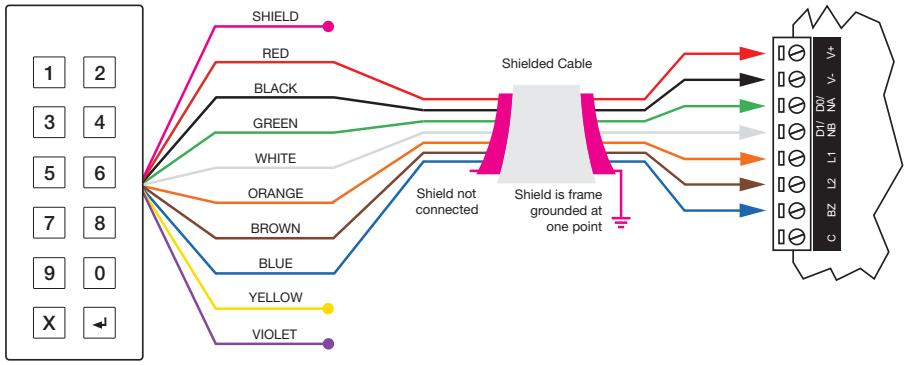
Single LED Connection



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 must be programmed to operate in dual LED mode. For more information, see Programming the Card Reader (page 18).

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 single or dual LED operation.

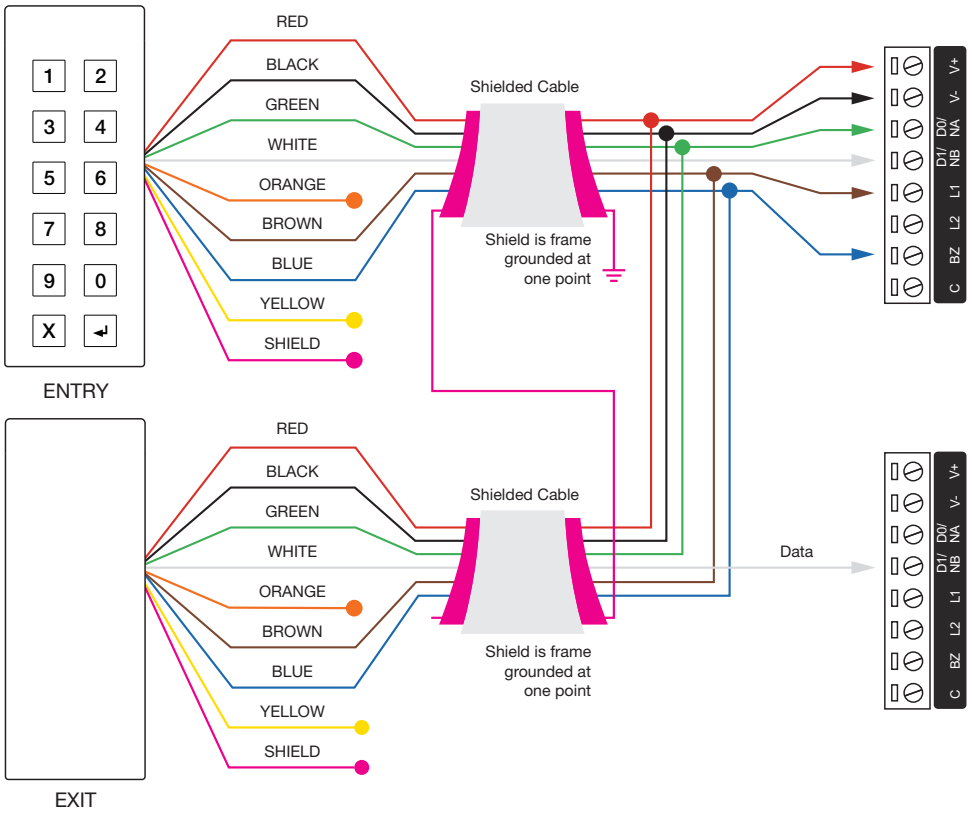
Connect the reader shield to a suitable earth point. **Do not** connect the shield to a ground or AUX connection. **Do not** connect the shield wires together at the reader cable splice. With the shield wire already terminated at the reader, terminate the shield at the controller.

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 into the alternate reader port will operate as the **exit** reader, and the normal reader connection shall 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).

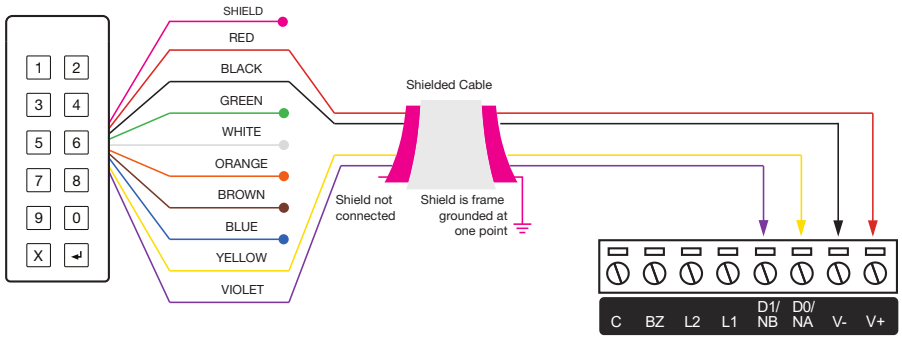
RS-485 Reader Locations

As two RS-485 readers can be connected to the same RS-485 reader port, 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

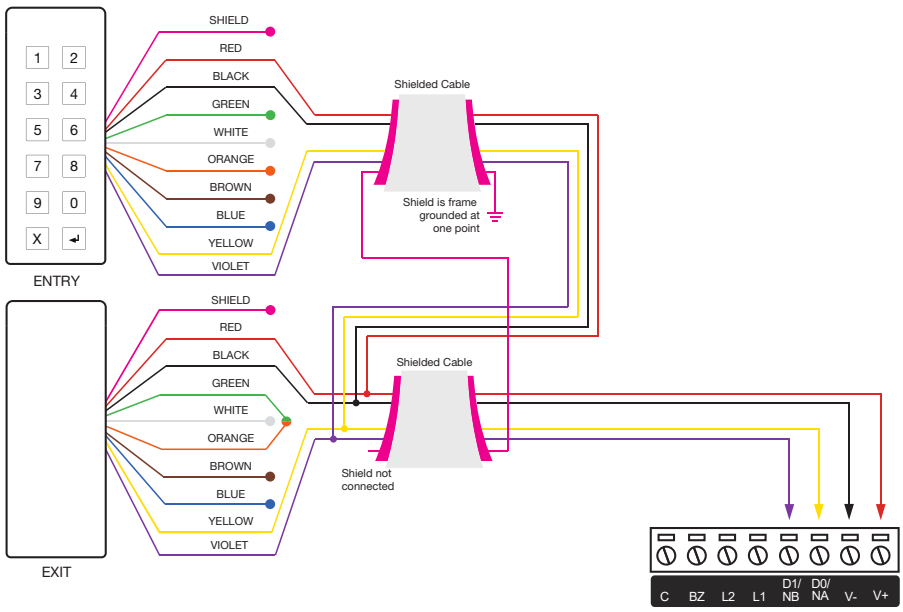
The connection of a single RS-485 reader to a reader expander in entry only mode.



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

RS-485 Reader Connection (Entry/Exit)

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



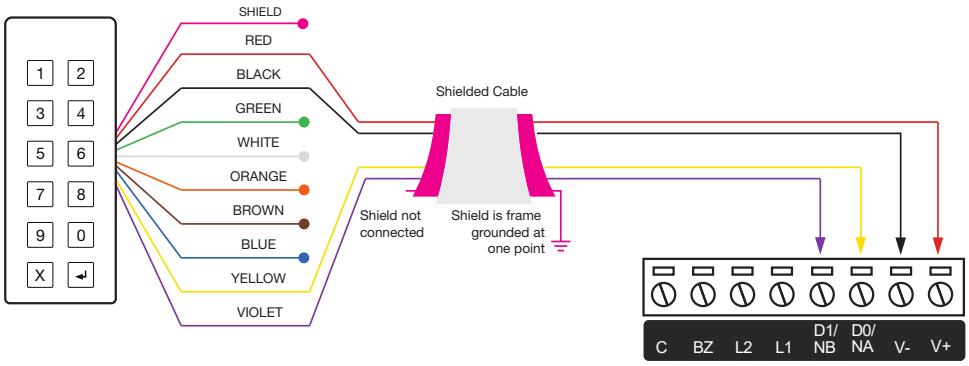
The exit reader has the **green** and **orange** wires connected together.

A 330 ohm EOL (End of Line) resistor may be required to be inserted between the 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.

OSDP Reader Connection

OSDP reader mode is only available for tSec Readers with firmware version 1.04.267 or higher. Readers that only support 125kHz reading and readers with PSK hardware **do not** support OSDP.

Connecting a tSec 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 (next page).

For more information about OSDP support on tSec Readers, including configuring readers for secure channel communications, see Application Note 321: Configuring tSec Multi-Technology Card Readers for OSDP Communication.

OSDP Baud Rate Requirement

For a tSec Reader operating in OSDP mode to communicate with an OSDP Server, it must have the same baud rate as the reader port it is connected to.

- The default tSec Reader baud rate is 38400
- The typical default reader port baud rate is 9600

The tSec 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.

To program the reader using the Config App select the **Uart Configuration** TLV and set the **Baud** to 9600.

For detailed information on programming tSec Readers, refer to AN-283: Programming tSec Reader Functions.

Programming the Card Reader

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

For detailed information on programming tSec Readers, refer to AN-283: Programming tSec Reader Functions.

Protege Config App

The Protege Config App provides a secure, convenient and flexible method for programming a Bluetooth® enabled tSec Reader.

To use the Config App you will need:

- An app account
- A mobile credential

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

- Firmware version 1.04.254 or higher
- Bluetooth® capability

Programming Summary

To program a tSec Reader using the Config App:

1. You will first need to 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 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 5 times quickly then restart.

Config App Programming Examples

The following examples illustrate programming some common tSec Reader configuration requirements, using the Config App.

Enable OSDP Output Mode

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

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called OSDP Output Mode.
4. Tap the **Add TLV** dropdown and select the **Hex** option.
5. In the **Hex** field, enter the OSDP Output Mode Hex code **`0B0104`**, then tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new OSDP Output Mode config within two minutes of startup.

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

ISO14443 Gain for DESFire EV2 Tags

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

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called ISO14443 Gain for EV2 Tags.
4. Tap the **Add TLV** dropdown and select the **Hex** option.
5. In the **Hex** field, enter the ISO14443 Gain 6 Hex code **`180106`**, then tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new ISO14443 Gain for EV2 Tags config within two minutes of startup.

Enable Dual LED Mode

By default tSec Readers are operate in single LED mode (when wired in Wiegand configuration). To enable dual LED mode, you need to change its configuration. For more information, see Wiegand Reader Connection (page 14).

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called Dual LED Mode.
4. Tap the **Add TLV** dropdown and select the **LED Mode** option.
5. Set the **LED Mode** to Dual, then tap **Save**.

Set Wiegand Output Mode

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

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called Wiegand Output Mode.
4. Tap the **Add TLV** dropdown and select the **Output Mode** option.
5. Set the **Output Mode** to Wiegand Output, then tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new Wiegand Output Mode config within two minutes of startup.

Enable CSN Reading Mode

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

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

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called CSN Reading Mode.
4. Tap the **Add TLV** dropdown and select the **CSN Reading Mode** option.
5. Tap the dropdown and select all the appropriate CSN reading options to enable, then tap **OK**.
6. Tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new CSN Reading Mode config within two minutes of startup.

For detailed information on programming tSec Readers using the Protege Config App, refer to AN-283: Programming tSec Reader Functions.

MIFARE Config Card

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

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

- Firmware version 1.04.229 or higher

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

For details on available programming configurations, refer to AN-283: Programming tSec Reader Functions.

Alternatively, config cards can be configured using the ICT Encoder Client. This provides a flexible and convenient method for programming readers as and when needed. For information on the encoding process and requirements, refer to the PRX-ENC ICT Encoder Client User Manual, available on the ICT Website.

Programming Summary

To program a tSec 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 tSec 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 tSec Reader.

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 tSec 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.

Encoder Client Programming Examples

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

Enable OSDP

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

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

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

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

ISO14443 Gain for DESFire EV2 Tags

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

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

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

For detailed information on programming config cards using the Encoder Client, including the available configuration settings, refer to the ICT Encoder Client User Guide.

Enable Dual LED Mode

By default tSec Readers are operate in single LED mode (when wired in Wiegand configuration). To enable dual LED mode, you need to change its configuration. For more information, see Wiegand Reader Connection (page 14).

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

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

Set Wiegand Output Mode

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

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

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

Enable CSN Reading Mode

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

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

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

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

125kHz Programming Card

125kHz capable tSec 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 tSec Reader, the reader must meet the following requirements:

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

Using a 125kHz programming card to program a tSec 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

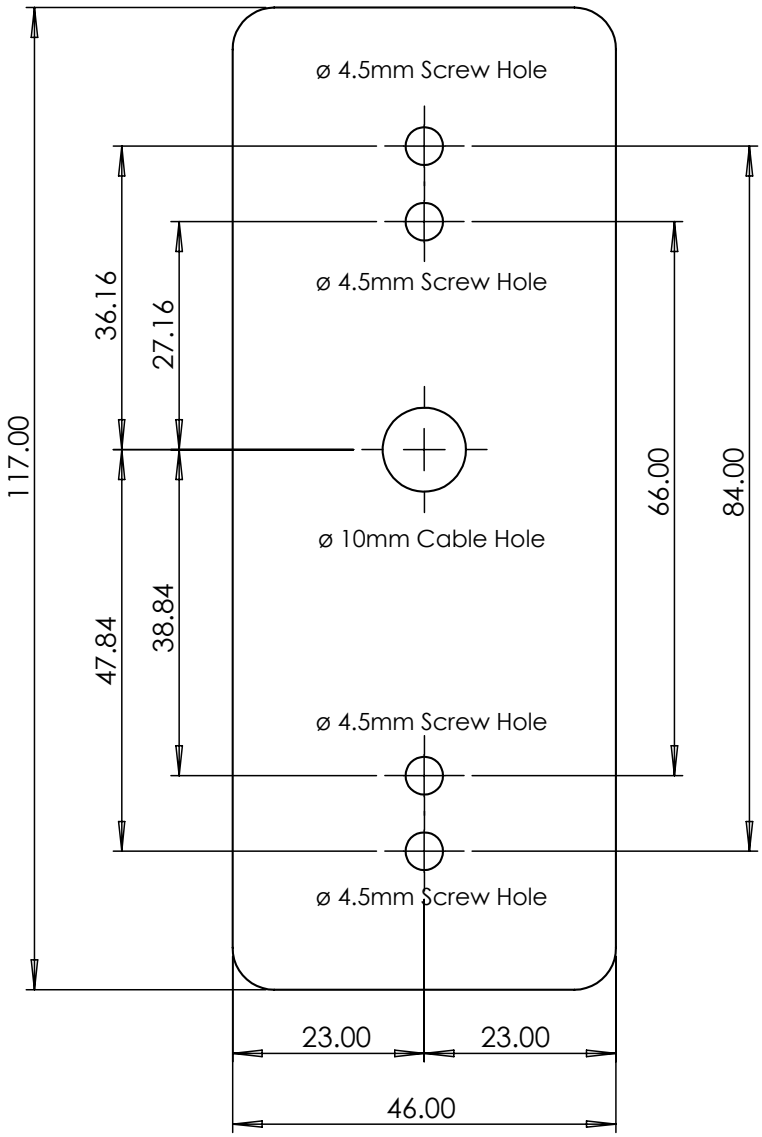
To program a tSec Reader using a 125kHz programming card:

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 tSec Readers using a 125kHz programming card, including the available programming options and badging sequences, refer to AN-283: Programming tSec Reader Functions.

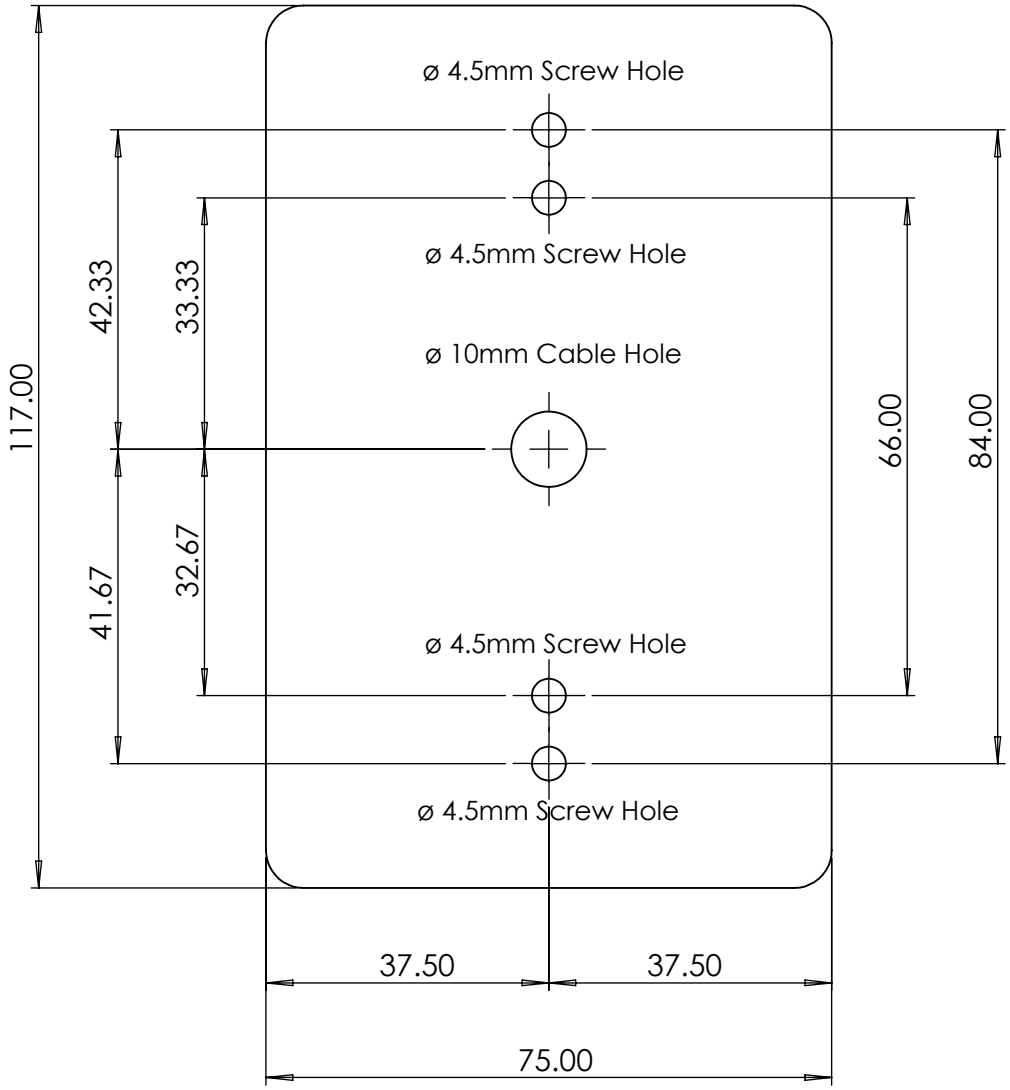
Technical Diagram - tSec Standard Reader

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



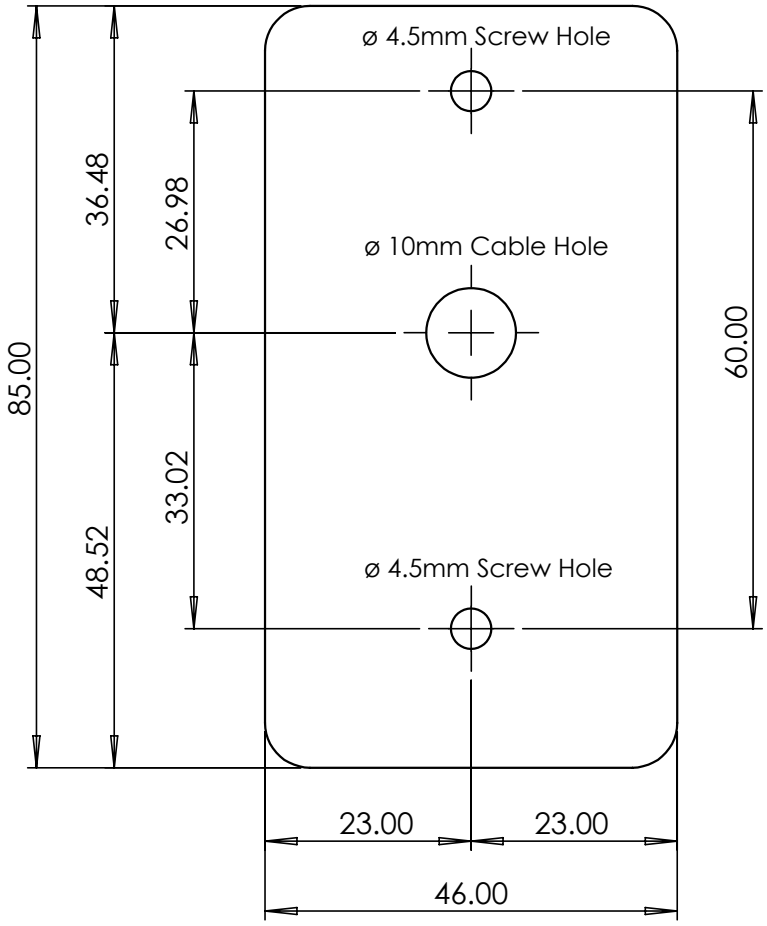
Technical Diagram - tSec Extra Reader

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



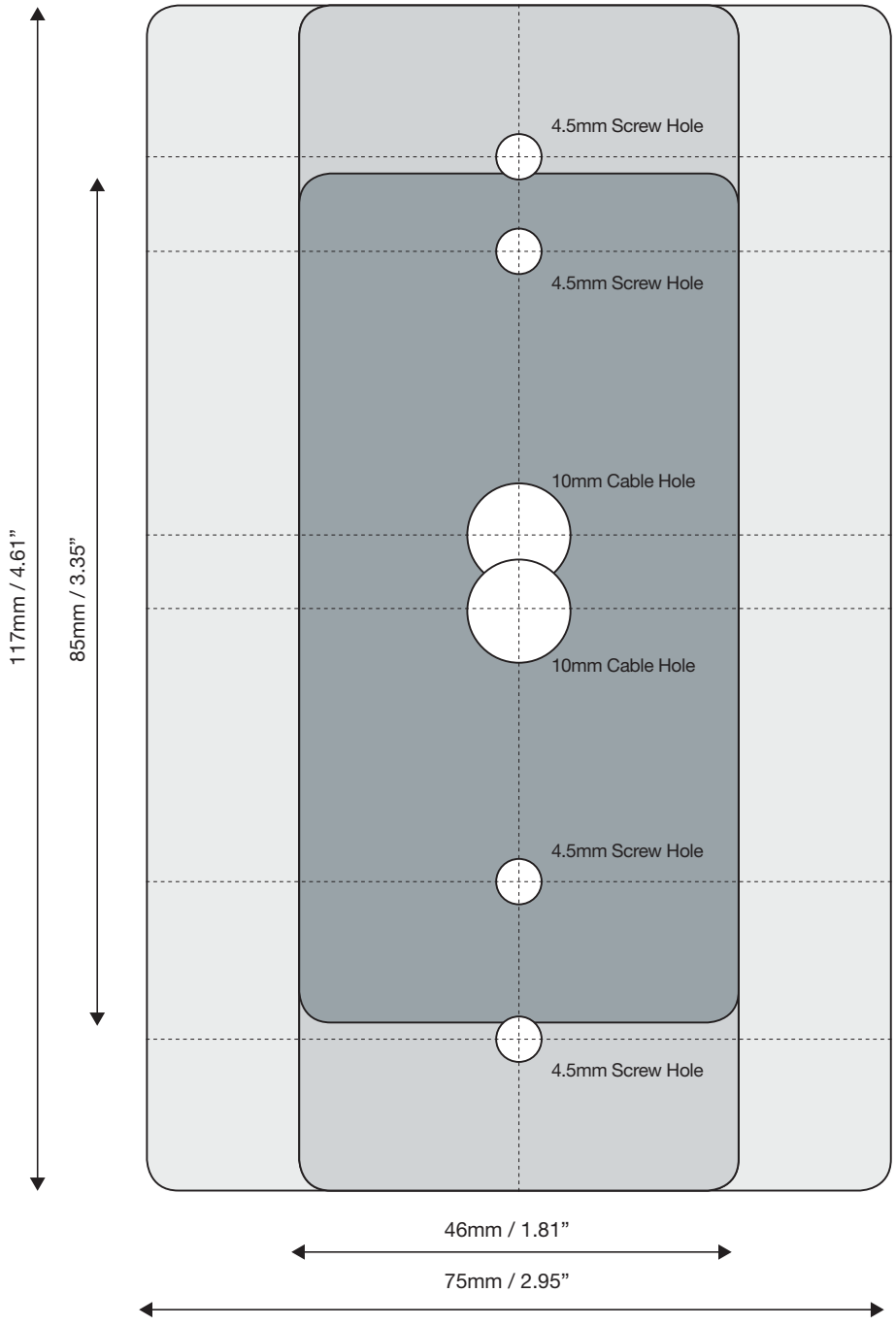
Technical Diagram - tSec Mini Reader

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



Technical Diagram - Comparison

The dimensions shown below provide a direct comparison of the dimensions of the tSec 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 tSec Reader editions.
Power Supply	
Operating Voltage	12VDC (9.5 to 14VDC)
Operating Current	tSec Standard Reader: 254mA (peak, reading) tSec Extra Reader: 298mA (peak, reading) tSec 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 2.1.5 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)	tSec Standard Reader: 117 x 46 x 18mm (4.61 x 1.81 x 0.71") tSec Extra Reader: 117 x 75x 18mm (4.61 x 2.95 x 0.71") tSec Mini Reader: 85 x 46 x 17mm (3.35 x 1.81 x 0.67")
Weight	tSec Standard Reader: 110g (3.89oz) tSec Extra Reader: 155.8g (5.5oz) 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.

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 Level IV when wired with RS485	Level IV	Level I
tSec Mini Reader	Level I	Level I when wired with Wiegand Level IV when wired with RS485	Level IV	Level I
tSec 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)

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 20-Apr-21

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