TSL Reader Range

TSL Multi-Technology Card Reader

Installation Manual

Last Published: 22-Feb-24 10:46 AM

Contents

Introduction

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

About This Module

The TSL 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 TSL card reader can operate using intelligent RS-485, OSDP or Wiegand 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 TSL reader range include:

- Multi card technology provides support for DESFire, MIFARE and 125kHz cards from a single reader
- Bluetooth® / NFC credential reading
- 125kHz PSK and G-Prox II support
- Encrypted RS-485, OSDP or standard Wiegand connection
- Supports OSDP communication protocol with Secure Channel
- Secure Access Module (SAM) for robust protection of encryption keys
- Custom encryption keys for MIFARE and DESFire credentials
- Programmable using the Protege Config App
- Operates as an update point in the ICT offline wireless locking system
- Signed firmware updates
- Three convenient sizes, making it suitable for any situation
- 16-color LED strip for configurable status display
- Read range up to 50mm (1.97") with proximity ISO cards
- Keep alive transmission for intelligent tamper management
- Fully encapsulated design with environmental IP Rating of IP65 for outdoor and indoor operation

Note: TSL readers are shipped in RS-485 configuration by default.

Reader Editions

The TSL Multi-Technology Card Reader comes in multiple sizes and with a range of optional features.

Standard	117 x 43 x 9.5mm (4.61 x 1.69 x 0.37")			
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology
TSL-STD-RR-HL TSL Standard Multi-Technology Card Reader with Bluetooth® Wireless Technology		✅	✅	✅
TSL-STD-RK-HL TSL Standard Multi-Technology Card Reader with Bluetooth® Wireless Technology and Keypad	✅	✅	✅	✅
TSL-STD-RR-H TSL Standard 13.56MHz Card Reader with Bluetooth® Wireless Technology			✅	✅
TSL-STD-RK-H TSL Standard 13.56MHz Card Reader with Bluetooth® Wireless Technology and Keypad	✅		✅	✅

Extra	117 x 75 x 9.5mm (4.61 x 2.95 x 0.37")			
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology
TSL-EXTRA-RR-HL TSL Extra Multi-Technology Card Reader with Bluetooth® Wireless Technology		✅	✅	✅
TSL-EXTRA-RK-HL TSL Extra Multi-Technology Card Reader with Bluetooth® Wireless Technology and Keypad	✅	✅	✅	✅
TSL-EXTRA-RR-H TSL Extra 13.56MHz Card Reader with Bluetooth® Wireless Technology			✅	✅
TSL-EXTRA-RK-H TSL Extra 13.56MHz Card Reader with Bluetooth® Wireless Technology and Keypad	✅		✅	✅

Mini	87 x 43 x 9.5mm (3.43 x 1.69 x 0.37")			
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology
TSL-MINI-RR-HL TSL Mini Multi-Technology Card Reader with Bluetooth® Wireless Technology		✅	✅	✅
TSL-MINI-RR-H TSL Mini 13.56MHz Card Reader with Bluetooth® Wireless Technology			✅	✅

Reader Accessories

A number of optional accessories are available to complement your TSL reader installation.

Faceplates

All TSL readers are shipped with a black faceplate. To switch to a white reader simply order a white faceplate.

Whether you're looking for a color change or need to replace a damaged cover, replacement white and black faceplates are available to suit all TSL reader sizes and configurations.

Ordering Codes

Standard Reader Faceplates	
TSL Standard Reader Faceplate - Black	TSL-FP-STD-B
TSL Standard Reader Faceplate - White	TSL-FP-STD-W
TSL Standard Reader with Keypad Faceplate - Black	TSL-FP-STD-KP-B
TSL Standard Reader with Keypad Faceplate - White	TSL-FP-STD-KP-W
Extra Reader Faceplates	
TSL Extra Reader Faceplate - Black	TSL-FP-EXTRA-B
TSL Extra Reader Faceplate - White	TSL-FP-EXTRA-W
TSL Extra Reader with Keypad Faceplate - Black	TSL-FP-EXTRA-KP-B
TSL Extra Reader with Keypad Faceplate - White	TSL-FP-EXTRA-KP-W
Mini Reader Faceplates	
TSL Mini Reader Faceplate - Black	TSL-FP-MINI-B
TSL Mini Reader Faceplate - White	TSL-FP-MINI-W

Fitting Instructions

1. To replace the faceplate, first remove the screw from the hole at the bottom of the reader.
2. Lift the front cover out and up from the reader body.
3. Position the new faceplate over the reader body, ensuring the top clip snaps into place.
4. Using the M3(G4)x4 Plastite self-tapping screw removed earlier, secure the cover via the hole at the bottom.

Vandal Resistant Cover

The vandal resistant cover (VRC) accessory is ideal for locations where a card reader may be exposed to damage, including corridors, parking buildings, correctional facilities, and other public places.

Highly resistant to impact, such as from the swing of a hammer or baseball bat, its robust construction provides greater durability and protection against vandalism and malicious damage.

The flush design also serves as an anti-ligature measure for an additional level of safety.

Mounted correctly the vandal resistant cover is compliant to **DHF TS 001:2013** Enhanced Requirements & Test Methods For Anti-Ligature Hardware to Grade B4 for vertical direction devices, and to impact level **IK10**.

For installation instructions, see Mounting with Vandal Resistant Cover Accessory (see page 16).

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

Ordering Codes

Accessory	Ordering Code
TSL Standard Reader VRC	TSL-VRC-STD-B
TSL Standard Reader with Keypad VRC	TSL-VRC-STD-KP-B
TSL Extra Reader VRC	TSL-VRC-EXTRA-B
TSL Extra Reader with Keypad VRC	TSL-VRC-EXTRA-KP-B

Surface Mount Box

The surface mount box (SMB) accessory is ideal for locations where cables cannot run inside the wall and must instead be run through external conduits. The surface mount box allows you to mount the card reader projected from the wall and provides a protected cavity where external cabling can be securely connected to the reader.

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

Ordering Codes

Accessory	Ordering Code
TSL Standard Reader SMB - Black	TSL-SMB-STD-B
TSL Standard Reader SMB - White	TSL-SMB-STD-W
TSL Extra Reader SMB - Black	TSL-SMB-EXTRA-B
TSL Extra Reader SMB - White	TSL-SMB-EXTRA-W

For installation instructions, see Mounting with Surface Mount Box Accessory (see page 17).

Pigtail Cables

TSL readers use a shielded 8-wire pigtail wiring loom with a Hirose socket plug for connection to the reader. A standard 34cm cable is supplied with the reader. Additional 34cm or 3.5m cables can be ordered separately.

The 3.5m pigtail cable is not compliant for UL/cUL installations.

Ordering Codes

Accessory	Ordering Code
Standard 34cm TSL Reader Pigtail Cable	TSL-CABLE-34CM
3.5m TSL Reader Pigtail Cable	TSL-CABLE-3.5M

Ferrite Shield

A ferrite shield, also known as a noise suppression sheet, is designed to reduce electromagnetic interference and may help to improve read range for readers mounted on a metal surface. The shield is placed between the reader and the mounting surface to suppress interference caused by the reader's proximity to the metal surface.

All TSL Standard and Mini readers come with a ferrite shield fitted. For TSL Extra readers ferrite shields are available as an optional accessory.

Ordering Codes

Accessory	Ordering Code
TSL Extra Reader Ferrite Shield 10pk	TSL-FS-EXTRA

The effectiveness of using a ferrite shield to improve read range is determined by many factors, including the mounting surface material and installation environment, and may not necessarily produce the desired result. Testing should be performed to assess effectiveness before planning installation on multiple readers.

ICT recommends using a **surface mount box** as the preferred solution for interference caused by metal mounting surfaces. A surface mount box is generally more effective at reducing interference and improving read range as it distances the reader from direct contact with the mounting surface, breaking the 'path of transfer'.

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 MIFARE DESFire 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 bit 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 bit 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 bit 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.

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.

Compatible Card Formats

Compatible access control card reader communication formats for UL/cUL installations are 26-, 34- and 37-bit Wiegand.

Installation Requirements

This equipment is to be installed in accordance with:

* The product installation instructions
* UL 294 - Access Control System Units
* 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
* CAN/ULC-60839-11-1, Alarm and Electronic Security Systems – Part 11-1: Electronic Access Control Systems – System and Components Requirements
* 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 17).

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 locking devices.

2. Use the drill template sticker provided with the card reader as a guide to correctly position the unit and drill the necessary holes as instructed.
   You can also print the drill templates from the ICT website:
   - www.ict.co/tsl-std-template
   - www.ict.co/tsl-extra-template
   - www.ict.co/tsl-mini-template

3. The reader's cable connection socket should align with the 'connector' hole cut through the wall. Cables are intended to be run inside the wall.

4. If using cavity anchors, affix the anchors (not supplied) into the wall.

5. If you are mounting an Extra reader with the optional ferrite shield, position the ferrite shield on the back of the reader using the pre-cut holes.

   This is not required for Standard and Mini readers because the ferrite shield is glued in place.

6. Run the module network wiring and connect to the reader wiring loom provided. Refer to the Connections section (see page 19) for the electrical connections.

7. Connect the wiring loom Hirose socket plug to the connection socket on the back of the reader.

8. Use appropriate screws (not supplied) to securely fasten the reader body to the wall or cavity anchors.

   It is strongly recommended to fasten screws by hand to avoid potential damage to the reader.

9. To complete the installation, position the faceplate over the reader body, ensuring the top clip snaps into place.

10. Using the M3(G4)x4 Plastite self-tapping screw provided, secure the faceplate via the hole at the bottom.

Important Notes

It is not advisable to use countersunk screws as they may embed into the body and damage the reader.

Screws must be firmly fastened to ensure the reader is mounted flush and securely against the wall.

It is strongly recommended to tighten screws by hand, as excess force from an electric driver may embed the screw head into the reader or crack the reader body if the mounting holes are not properly aligned.

Screw heads must not protrude above the mounting hole cavity, otherwise the reader cover will not fit correctly over the reader body. Cheese head (Fillister head) screws are recommended.

Screw heads must not protrude above the mounting hole cavity

Mounting screws

Connection socket
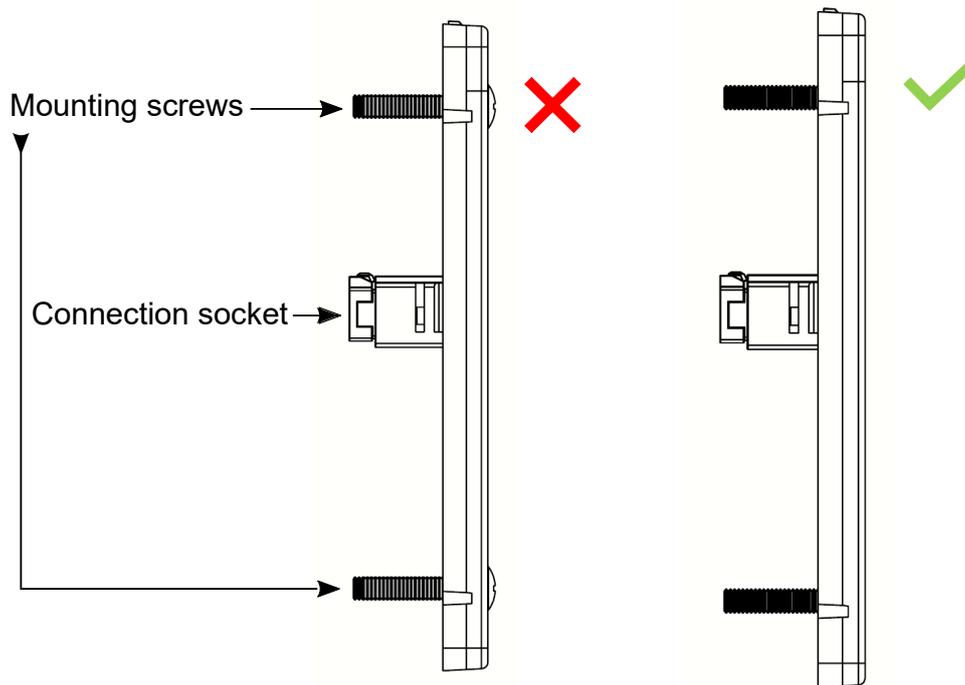
Accessories Provided

- 1 x shielded 8-wire wiring loom with waterproof Hirose socket plug
- 1 x M3(G4)x4 PanPozi Plastite SS316 stainless steel self-tapping screw

Accessories Not Included

- Cavity anchors. 4M fixings are recommended.
- Fastening screws. 6g screws should be used when fixing the reader directly to the wall (mounting holes are 4.5mm). Cheese head (Fillister) screws are recommended. Countersunk screws are not advised.

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 replaces the normal faceplate of the reader.

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

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 locking devices.

2. Use the drill template sticker provided with the card reader as a guide to correctly position the unit and drill the necessary holes as instructed.

   You can also print the drill templates from the ICT website:

   - www.ict.co/tsl-std-vrc-template
   - www.ict.co/tsl-extra-vrc-template

3. The reader's cable connection socket should align with the 'connector' hole cut through the wall. Cables are intended to be run inside the wall.

4. If using cavity anchors, affix the anchors (not supplied) into the wall.

5. Run the module network wiring and connect to the reader wiring loom provided. Refer to the Connections section (see page 19) for the electrical connections.

6. Connect the wiring loom Hirose socket plug to the connection socket on the back of the reader.

7. Use appropriate screws (not supplied) to securely fasten the reader body to the wall or cavity anchors.

   > It is strongly recommended to fasten screws by hand to avoid potential damage to the reader.

8. Use appropriate screws (not supplied) to affix the vandal resistant cover to the wall.

Accessories Not Included

- Cavity anchors. 4M fixings are recommended.
- Fastening screws. 10g screws should be used when fixing the surface mount box to the wall (mounting holes are 5.3mm). Pan head security screws are recommended. Countersunk screws are not advised.

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 is the same height and width as the card reader rear case, with a protected cavity to allow external cabling to be securely connected to the reader.

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

Mounting a 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 with the embossed arrow pointing upwards and mark the mounting holes.

   You can also print the drill templates from the ICT website:

   - www.ict.co/tsl-std-smb-template
   - www.ict.co/tsl-extra-smb-template

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. Run the reader wiring loom through the conduit hole and connect to the module network wiring. Refer to the Connections section (see page 19) for the electrical connections.

6. Connect the wiring loom Hirose socket plug to the connection socket on the back of the reader.

7. Remove the reader faceplate. Hold the reader body against the surface mount box in the correct orientation. Line up the holes on the rear case with the threaded inserts, as shown in the image below.
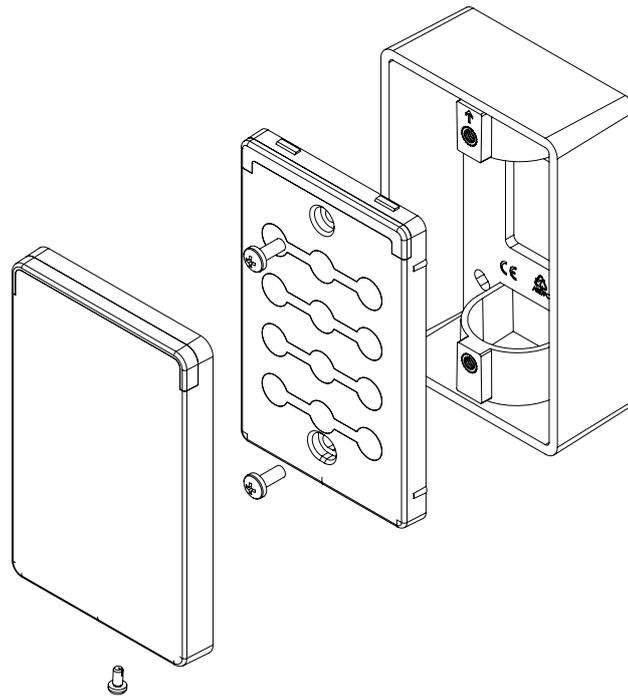
8. Affix the reader body to the surface mount box using the two M4 x 10mm screws provided.

9. Position the faceplate over the reader body, ensuring the top clip snaps into place.

10. To complete the installation, use the M3 x 8mm Plastite screw provided with the card reader to secure and fasten the faceplate to the reader body.

Accessories Not Included

- Cavity anchors. 4M fixings are recommended.
- Fastening screws. 8g screws should be used when fixing the surface mount box to the wall (mounting holes are 4.5mm). Cheese head (Fillister) screws are recommended. Countersunk screws are not advised.

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

Maximum distance: 900m (3000ft)

The recommended cable types for Wiegand are:

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

Maximum distance: 150m (492ft)

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.

Reader Pigtail

TSL readers have a shielded 8-wire pigtail wiring loom with a Hirose socket plug for connection to the reader.
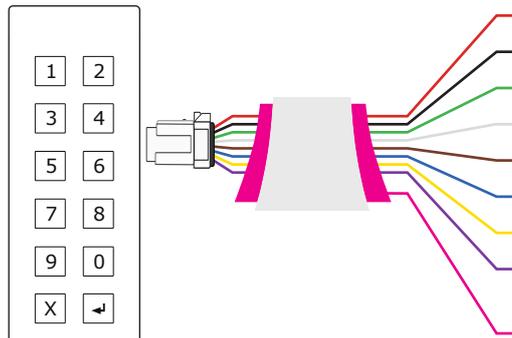
Color	Wire	Description
🔴	Red	**12VDC+** positive
⚫	Black	**12VDC-** negative
🟢	Green	Wiegand **D0** (Data 0)
⚪	White	Wiegand **D1** (Data 1)
🟤	Brown	Wiegand LED control
🔵	Blue	Wiegand beeper control
🟡	Yellow	RS-485 **A**
🟣	Violet	RS-485 **B**
🟣	Shield	Shield (drain) wire

Shield Connection

1. Connect the reader pigtail shield and cable shield wires together at the reader pigtail splice.
2. Connect the cable shield to a suitable earth point. **Do not** connect the shield to a ground or AUX connection.

The reader pigtail shield wire is **not** terminated inside the reader.
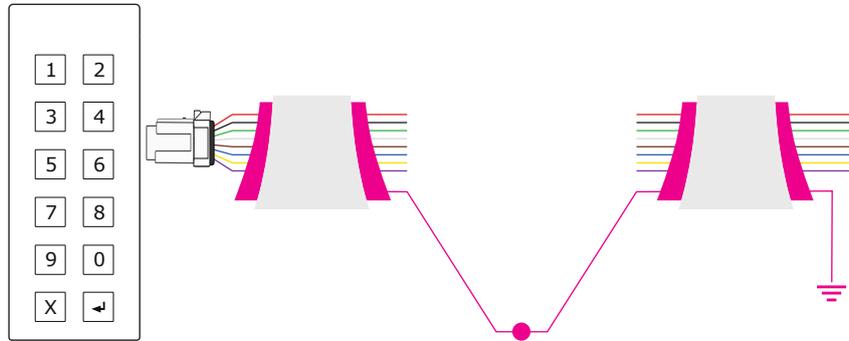
Important:

- 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.

RS-485 Reader Connection

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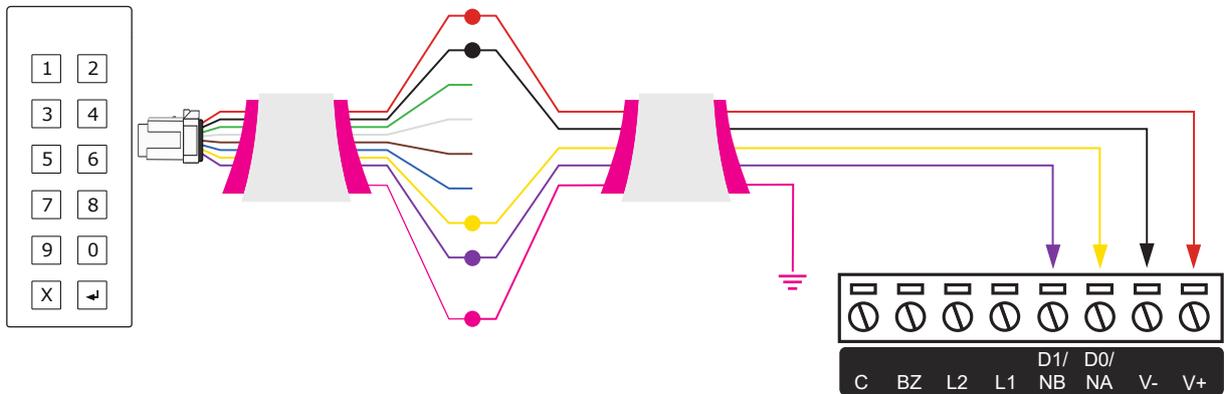
Reader Connections

Color	Wire	Connection
	Red	**V+** 12VDC positive
	Black	**V-** 12VDC negative
	Yellow	**D0/NA** RS-485 A
	Violet	**D1/NB** RS-485 B
	Shield	Shield (drain) wire. Frame grounded at one point only

RS-485 Reader Connection (Entry/Exit)

The connection of two RS-485 readers to a reader expander providing an entry/exit configuration.
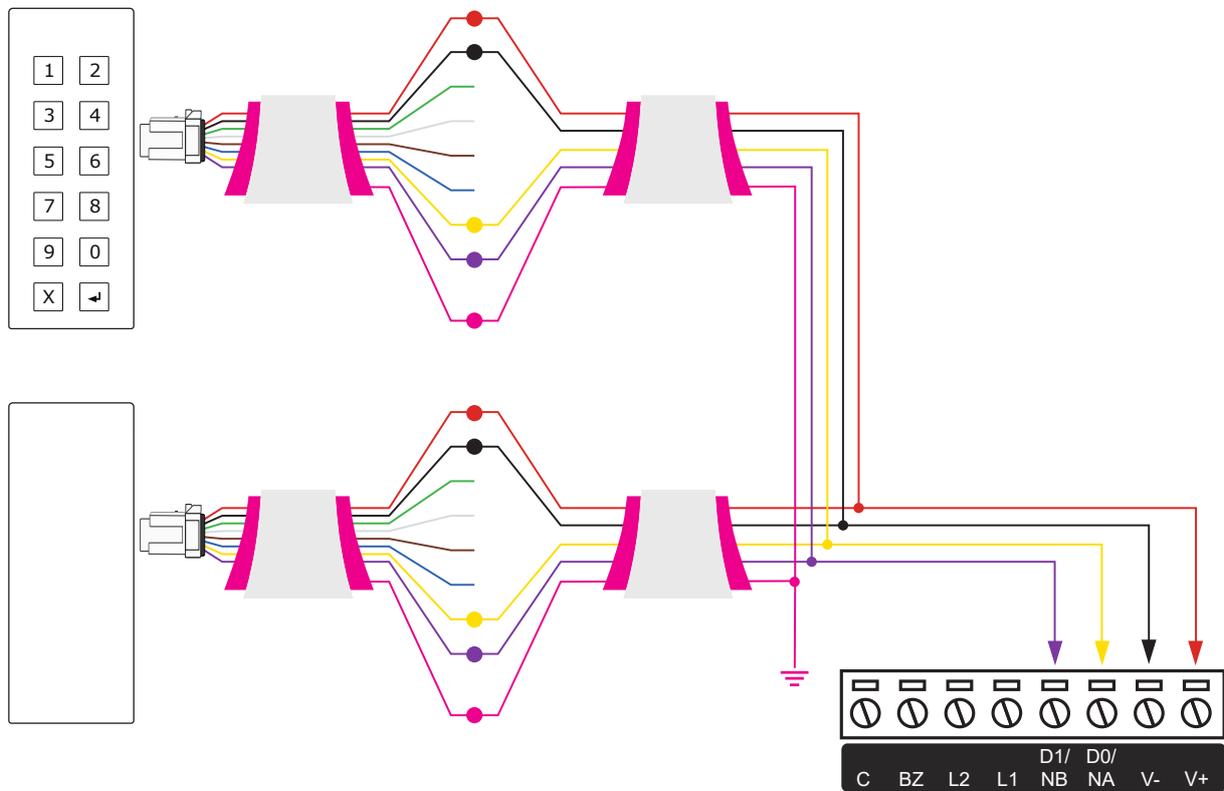
A 330 ohm EOL (End of Line) resistor may be required, inserted between the yellow and violet wires after the join.

When connecting two TSL readers for RS-485 entry/exit configuration, the reader address determines which is the entry reader and which is the exit reader, so it does not matter which reader is the 'secondary' connection.

Primary Reader Connections

Color	Wire	Connection
🔴	Red	**V+** 12VDC positive
⚫	Black	**V-** 12VDC negative
🟡	Yellow	**D0/NA** RS-485 A
🟣	Violet	**D1/NB** RS-485 B
🟣	Shield	Join the shield (drain) wires together. Frame grounded at one point only

Secondary Reader Connections

Color	Wire	Connection
🔴	Red	Join to primary reader **red** wire (12VDC positive)
⚫	Black	Join to primary reader **black** wire (12VDC negative)
🟡	Yellow	Join to primary reader **yellow** wire (RS-485 A)
🟣	Violet	Join to primary reader **violet** wire (RS-485 B)
🟣	Shield	Join the shield (drain) wires together. Frame grounded at one point only

RS-485 Reader Address

As two RS-485 readers can be connected to the same RS-485 reader port, the **reader address** uniquely identifies each reader and determines the entry and exit locations.

Configuration	Location
Reader address = **0**	Entry (default setting)
Reader address = **1**	Exit

The reader address can be programmed using the Protege Config App. For more information, see Programming the Card Reader (page 29).

The address and location of TSL card readers are **not** determined by the reader's wiring configuration.

OSDP Reader Connection

Connecting TSL readers in OSDP mode is the same as the connection for standard RS-485 configuration.
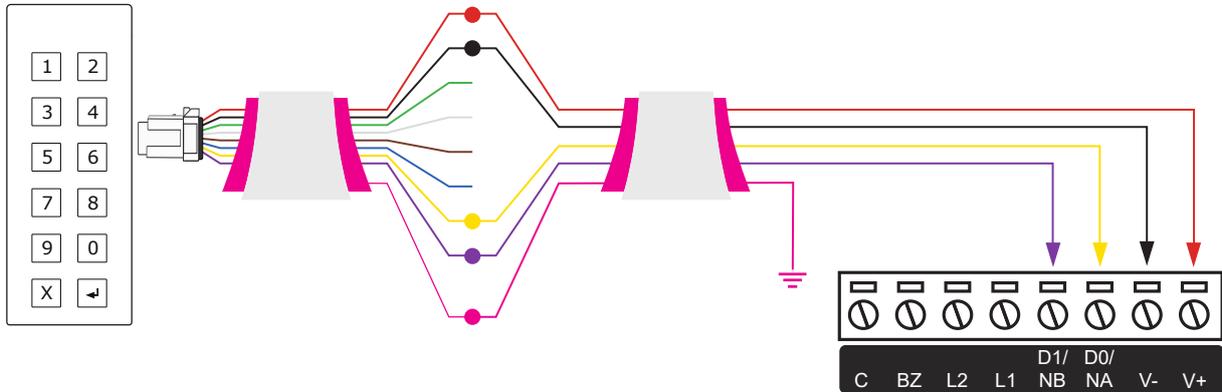
Reader Connections

Color	Wire	Connection
🔴	Red	**V+** 12VDC positive
⚫	Black	**V-** 12VDC negative
🟡	Yellow	**D0/NA** RS-485 A
🟣	Violet	**D1/NB** RS-485 B
🩷	Shield	Shield (drain) wire. Frame grounded at one point only

Readers must also be programmed to operate in OSDP mode. For more information, see Programming the Card Reader (page 29).

Connecting OSDP readers to Protege modules requires additional hardware configuration and system programming. For more information, see Application Note 254: Configuring OSDP Readers in Protege.

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

OSDP Reader Address

When multiple OSDP readers are connected to the same reader port, each reader needs a **unique address**. The default address is 0.

- For Protege systems, the entry and exit readers can have any unique address. This must be used when programming the smart reader record in the software:
    - The **Configured address** of the smart reader is the reader address plus 1.
    - The **Reader location** of the smart reader determines whether the reader is an entry or exit reader.
- For third-party systems, consult the user documentation to determine the required address settings. Typically this is 0 for entry and 1 for exit.

The reader address can be programmed using the Protege Config App. For more information, see Programming the Card Reader (page 29).

OSDP Baud Rate

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 baud rate can be programmed using the Protege Config App. For more information, see Programming the Card Reader (page 29).

OSDP Installation Mode

TSL readers are in installation mode by default, allowing them to establish a secure channel with the module they are connected to. To establish a secure channel, enable installation mode in the module (e.g. using manual commands in the Protege software). This causes the reader and module to share encryption keys and pair with each other.

If the encryption keys are lost (e.g. the module is defaulted) or the reader is connected to a new module, you will need to put the card reader into installation mode again. To do this, create a config in the Protege Config App with the **Device Mode** TLV set to OSDP Install Mode. For more information, see Programming the Card Reader (page 29).

> **Communications are not secure during the installation mode process.** Until this process is complete, the installer is responsible for ensuring that no unauthorized person or device has access to the wiring between the card reader and module.

Wiegand Reader Connection

When connected using the Wiegand interface, TSL readers operate in single LED mode, which allows a single LED line to control the two reader LED colors.

TSL readers do not support dual LED operation for Wiegand interfaces.

Reader Connections

Color	Wire	Connection
🔴	Red	**V+** 12VDC positive
⚫	Black	**V-** 12VDC negative
🟢	Green	**D0/NA** Wiegand Data 0
⚪	White	**D1/NB** Wiegand Data 1
🟤	Brown	**L1** LED control
🔵	Blue	**BZ** beeper control
🟣	Shield	Shield (drain) wire. Frame grounded at one point only

Readers must also be programmed to operate in Wiegand mode. For more information, see Programming the Card Reader (page 29).

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.

Entry Reader Connections

Color	Wire	Connection
🔴	Red	**V+** 12VDC positive
⚫	Black	**V-** 12VDC negative
🟢	Green	**D0/NA** Wiegand Data 0
⚪	White	**D1/NB** Wiegand Data 1
🟤	Brown	**L1** LED control
🔵	Blue	**BZ** beeper control
🟣	Shield	Join the shield (drain) wires together. Frame grounded at one point only

Exit Reader Connections

Color	Wire	Connection
🔴	Red	Join to entry reader **red** wire (12VDC positive)
⚫	Black	Join to entry reader **black** wire (12VDC negative)
🟢	Green	Join to entry reader **green** wire (Wiegand Data 0)
⚪	White	**D1/NB** Wiegand Data 1 (alternate reader port to entry reader)
🟤	Brown	Join to entry reader **brown** wire (LED control)
🔵	Blue	Join to entry reader **blue** wire (beeper control)
🟣	Shield	Join the shield (drain) wires together. Frame grounded at one point only

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

Connecting 4 Wiegand Readers

Multiple reader mode allows the connection of 4 Wiegand readers controlling 2 doors, each with entry/exit readers. To connect 4 Wiegand reading devices to a Protege module:

- Door 1 entry reader is connected to reader **port 1**
- Door 1 exit reader has its Wiegand Data 1 wire connected to the reader **port 2** D1 connection
- Door 2 entry reader is connected to reader **port 2**
- Door 2 exit reader has its Wiegand Data 1 wire connected to the reader **port 1** D1 connection
- The **Multiple reader input port 1** option is enabled in the reader expander programming (General | Options)
- The **Multiple reader input port 2** option is enabled in the reader expander programming (General | Options)

To connect two Wiegand readers to a reader port the **Multiple reader input port 1/2** option must be enabled in the reader expander programming. When this option is disabled the reader port will only process a single reader.

Programming the Card Reader

ICT readers have a wide range of functionality available to suit your site's requirements.

TSL readers are programmed using the Protege Config App, which applies specific TLV (Type Length Value) settings to the reader to enable, disable and configure reader options. The app can be used by any Android or iOS mobile device with Bluetooth® capability.

This section covers the basic operation of the config app and the most common settings you will need to get the reader up and running. For detailed programming instructions and information about all available settings, see the ICT Card Reader Configuration Guide, available from the ICT website.

TSL readers do not support programming via config card.

Protege Config App

The Protege Config App provides a secure, convenient and flexible method for programming TSL card readers.

To use the config app you will need:

- An app account
- A mobile credential

Programming Summary

To program a 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. You must apply the config **within two minutes of startup**.
6. Select the **config** to program the reader with.
7. 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.

Initial TSL Reader Setup

TSL readers have some important settings that may need to be configured before the reader will function:

- Output mode
- Reader address
- MIFARE/DESFire encryption keys

Before you begin, install the Protege Config App on an Android or iOS device and sign in. Switch on Bluetooth® communication.

Setting the Output Mode

The output mode determines how the TSL reader communicates with the controller or reader expander it is connected to.

The default output mode is **ICT RS-485**. If you are using a different output mode such as Wiegand or OSDP, you must configure the reader:

1. Log in to the Protege Config App.
2. Navigate to the **Reader Configuration** section.
3. Select the appropriate **Credential Profile**.
4. Tap **+** to add a new config.
5. Enter a relevant **Config name**, e.g. Enable OSDP Output Mode.
6. Tap **Add TLV** and select **Output Mode**.
7. Set the **Output Mode** to the required mode.
8. If you are using OSDP with a third-party system, you may also need to program the baud rate (see page 25). To program the baud rate, add a new TLV with the **Uart Configuration** type and set the **Baud** as required.
9. Tap **Save**.
10. Power cycle the reader you wish to program.
11. Tap the new config to activate it.
12. Hold your mobile device close to the reader and tap **Scan Closest** to apply the configuration.

Setting the Reader Address

There are two situations where you may have to program the reader address:

- In ICT RS-485 mode, the default address is 0 (entry). For an exit reader, set the address to 1 (see page 23).
- In OSDP mode, the readers used for entry and exit on the same door must have different addresses. These are typically 0 (default) for entry and 1 for exit (see page 24).

To set the reader address:

1. In the config app, tap **+** to add a new config.
2. Enter a relevant **Config name**, e.g. Exit Reader.
3. Tap **Add TLV** and select **Reader Address**.
4. Toggle the slider to **Dec** to set the address in decimal.
5. Enter the required reader address.
6. Tap **Save**.
7. Power cycle the reader you wish to program.
8. Tap the new config to activate it.
9. Hold your mobile device close to the reader and tap **Scan Closest** to apply the configuration.

MIFARE/DESFire Encryption Keys

By default, TSL readers use standard ICT encryption keys for MIFARE/DESFire cards and mobile credentials. If your site uses unique custom encryption keys (recommended), you must program the keys into each reader.

When you order cards and mobile credentials with custom encryption keys from ICT, you will be provided with a custom TLV for programming the card readers.

This TLV also locks down the card readers so that they will accept no further configuration without a special reset config. Ensure that you configure all other required settings **before** applying this config.

1. In the config app, tap **+** to add a new config.

2. Enter a relevant **Config name**, e.g. Company X Custom Encryption Keys.

3. Tap **Add TLV** and select **Hex**.

4. Enter the custom TLV provided by ICT.

5. Tap **Save**.

6. Power cycle the reader you wish to program.

7. Tap the new config to activate it.

8. Hold your mobile device close to the reader and tap **Scan Closest** to apply the configuration.

To unlock the reader and perform further configuration, program a config with the reset TLV provided by ICT.

For more information about ordering and setting up custom encryption keys, see Application Note 352: Setting Up Custom Credential Encryption.

Mechanical Diagrams

TSL Standard Reader

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

This template is included for information only and may not be to scale. For a version of this template that can be printed to scale, go to www.ict.co/tsl-std-template

ø 4.5mm Screw Hole

ø 18mm
Connector Hole (Min)

ø 4.5mm Screw Hole

51.9

36.4

117.0

84.0

47.6

65.12

21.5

21.5

43.0
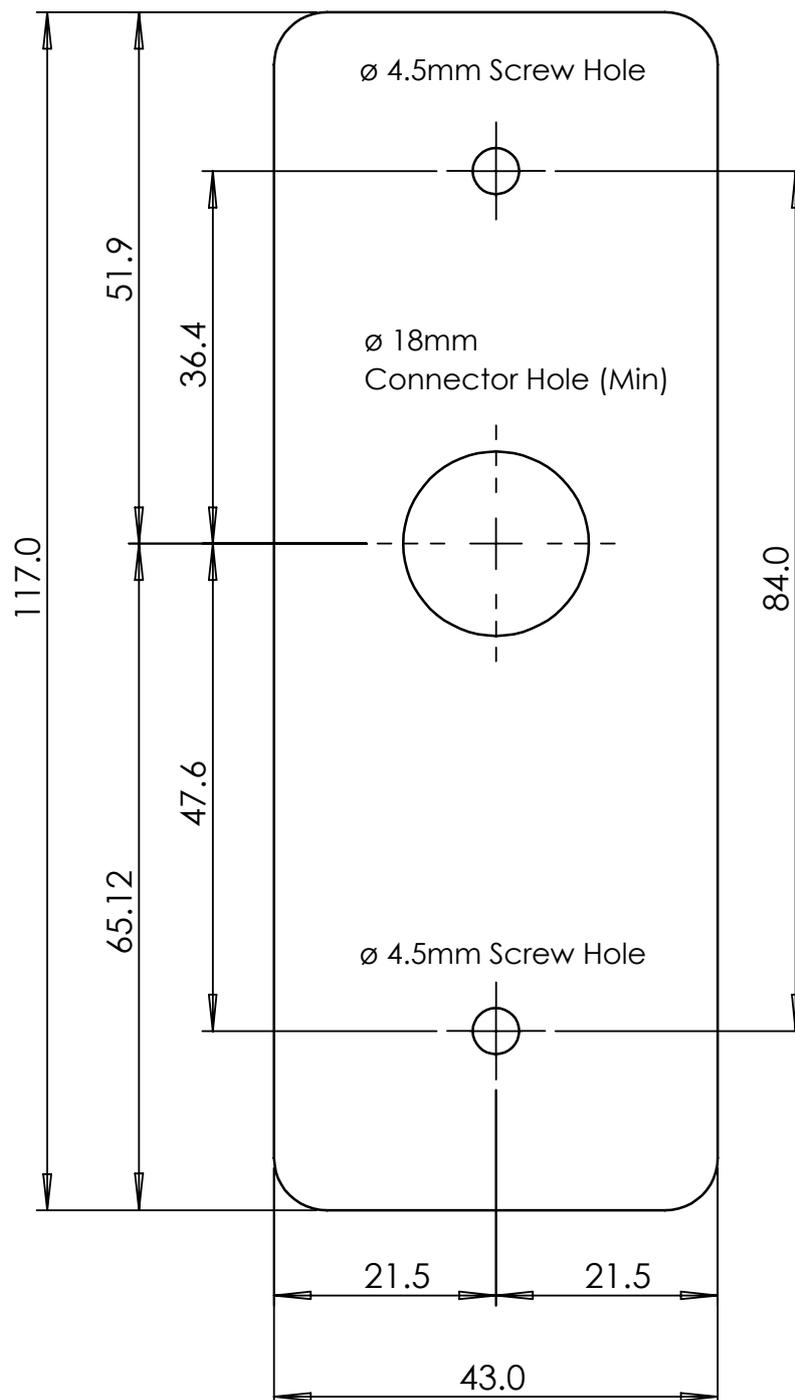
TSL Extra Reader

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

This template is included for information only and may not be to scale. For a version of this template that can be printed to scale, go to www.ict.co/tsl-extra-template

ø 4.5mm Screw Hole

ø 18mm
Connector Hole (Min)

ø 4.5mm Screw Hole

60.0

44.5

117.0

39.5

57.0

84.0

37.5

37.5

75.0

TSL Mini Reader

The dimensions shown below outline the essential details needed to help ensure the correct installation of the ICT TSL Mini Reader. All measurements are shown in millimeters.
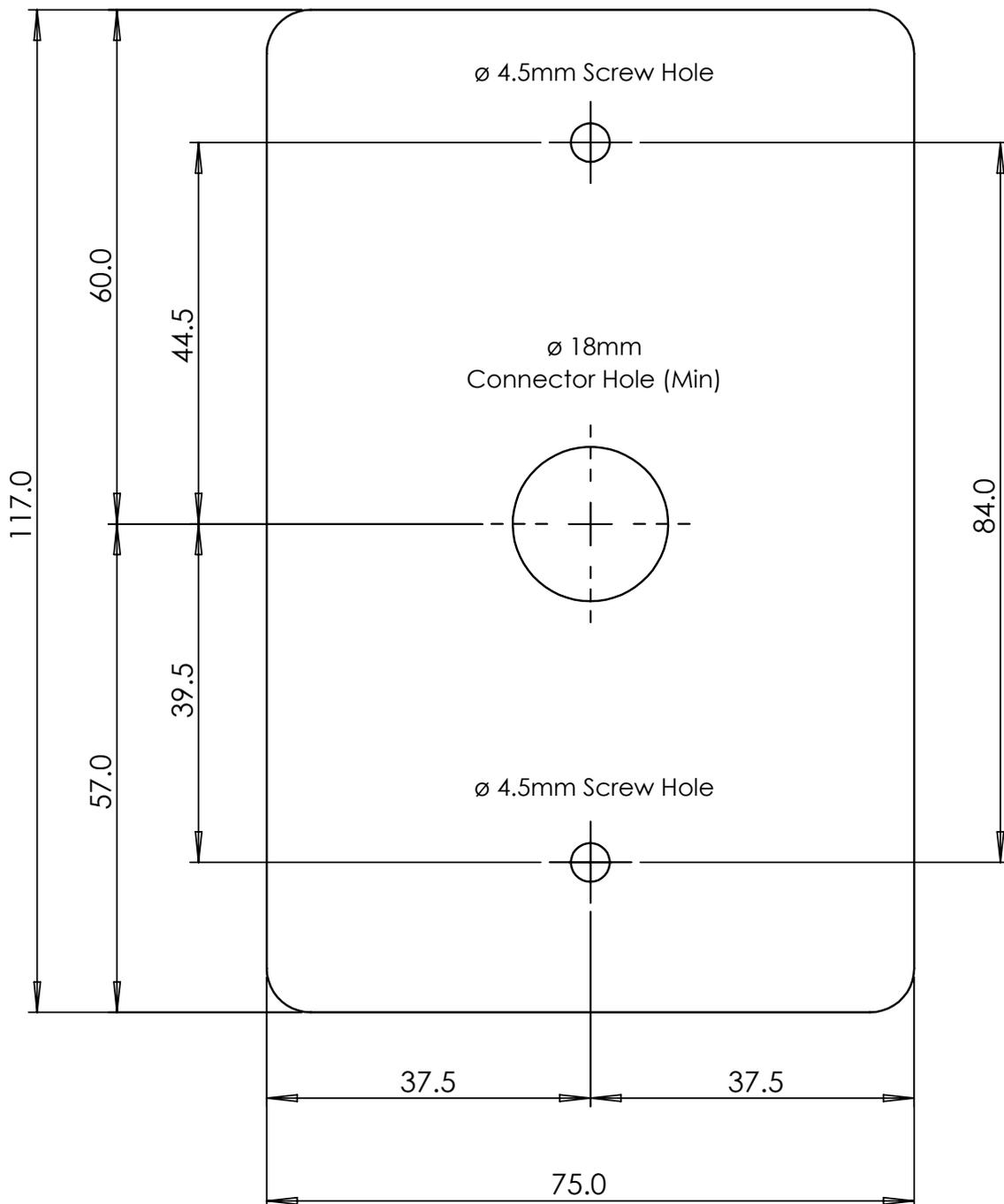
This template is included for information only and may not be to scale. For a version of this template that can be printed to scale, go to www.ict.co/tsl-mini-template

TSL Standard Vandal Resistant Cover

This template is included for information only and may not be to scale. For a version of this template that can be printed to scale, go to www.ict.co/tsl-std-vrc-template

89mm (3.5")

∅5.3mm (0.21")
Mounting Holes

29mm (1.14")

41.5mm (1.63")

41.5mm (1.63")

29mm (1.14")

162mm (6.38")

69mm (2.72")

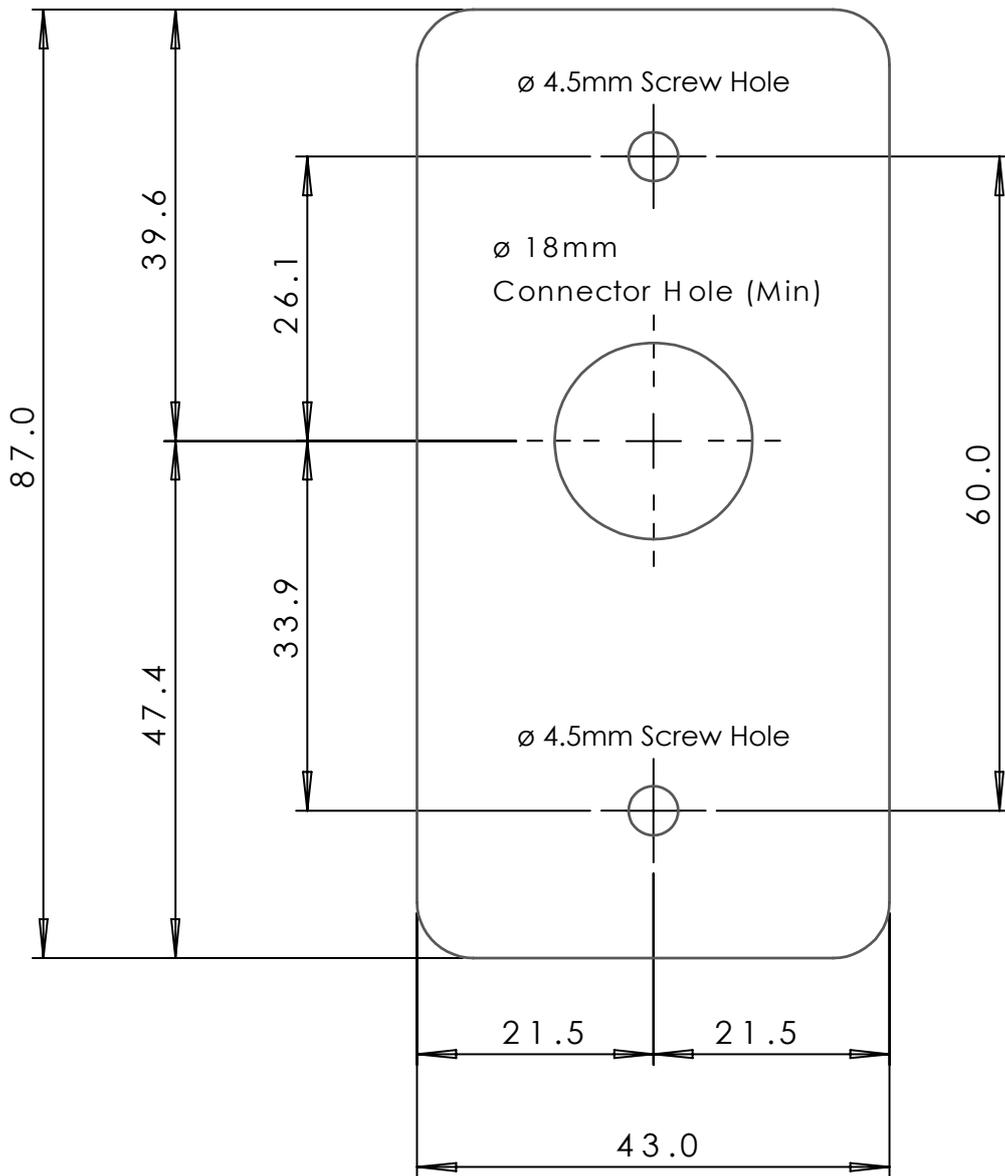11.5mm (0.45")

TSL Extra Vandal Resistant Cover

This template is included for information only and may not be to scale. For a version of this template that can be printed to scale, go to www.ict.co/tsl-extra-vrc-template

121mm (4.76")

11.5mm (0.45")

∅5.3mm (0.21")
Mounting Holes

29mm (1.14")

41.5mm (1.63")

41.5mm (1.63")

29mm (1.14)

162mm (6.38")

99mm (3.9")

TSL Standard Surface Mount Box

This template is included for information only and may not be to scale. For a version of this template that can be printed to scale, go to www.ict.co/tsl-std-smb-template
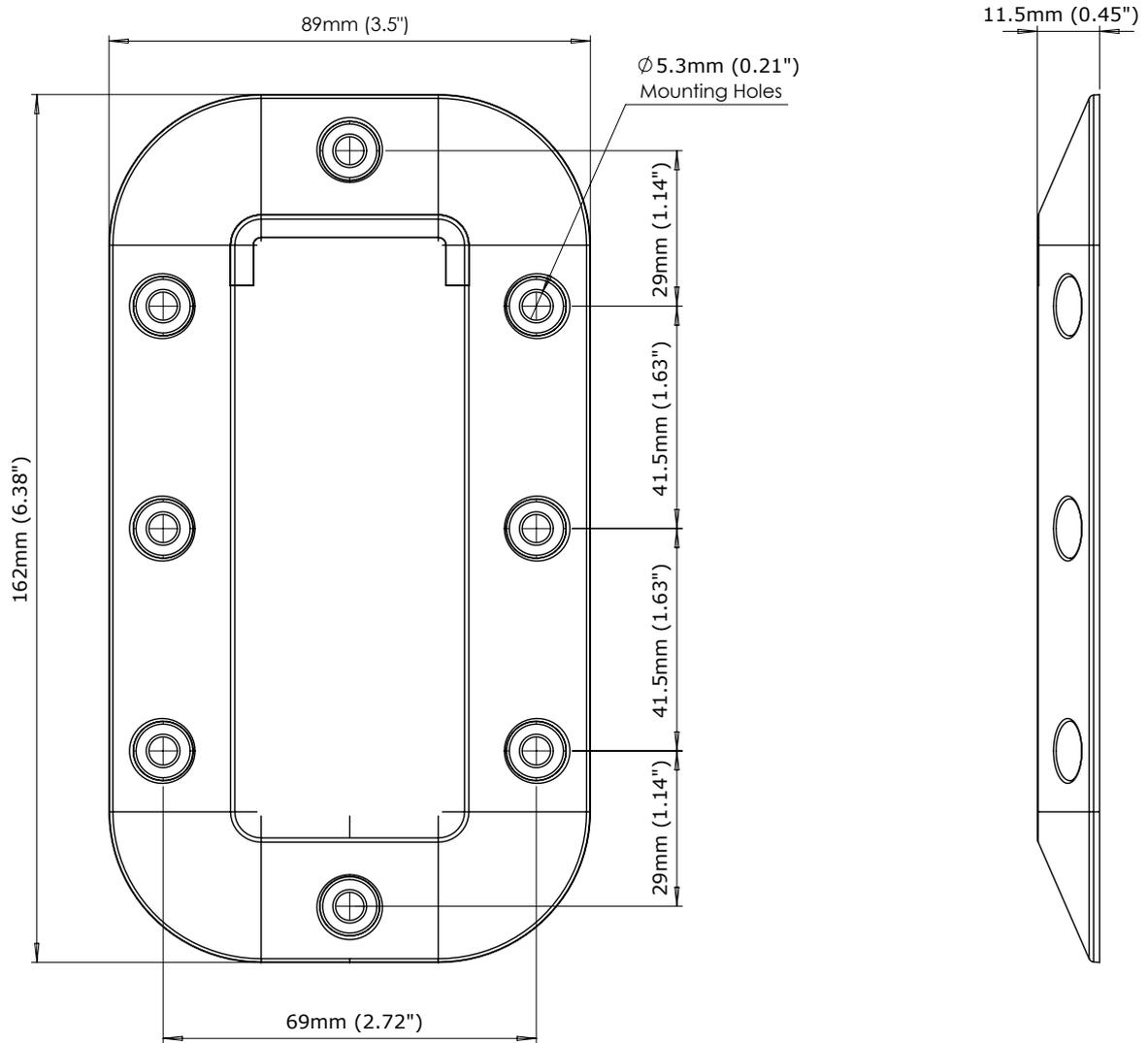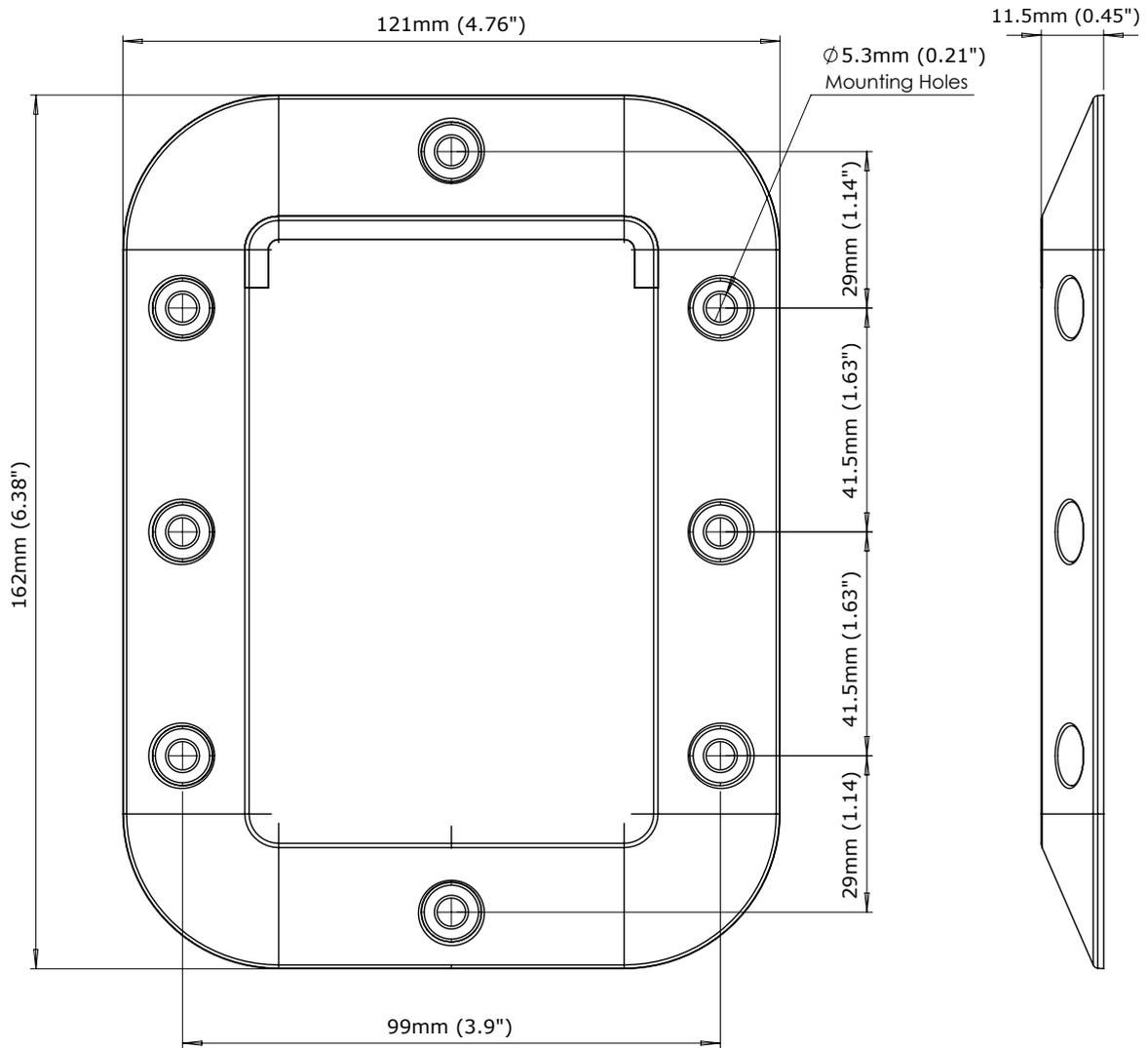

(2x) M4x0.7 Mounting Holes

22.00 [0.866in]

⌀4.50mm[0.177in]

84.00mm[3.307in]

66.00mm[2.598in]

60.00mm[2.362in]

60.00mm[2.362in]

22.00 [0.866in]

(5x) 7mm [0.276in] x 4.5mm [0.177in] Mounting Slots

34.00mm[1.339in]

117.00mm[4.606in]

114.63mm[4.513in]

TSL Extra Surface Mount Box

This template is included for information only and may not be to scale. For a version of this template that can be printed to scale, go to www.ict.co/tsl-extra-smb-template
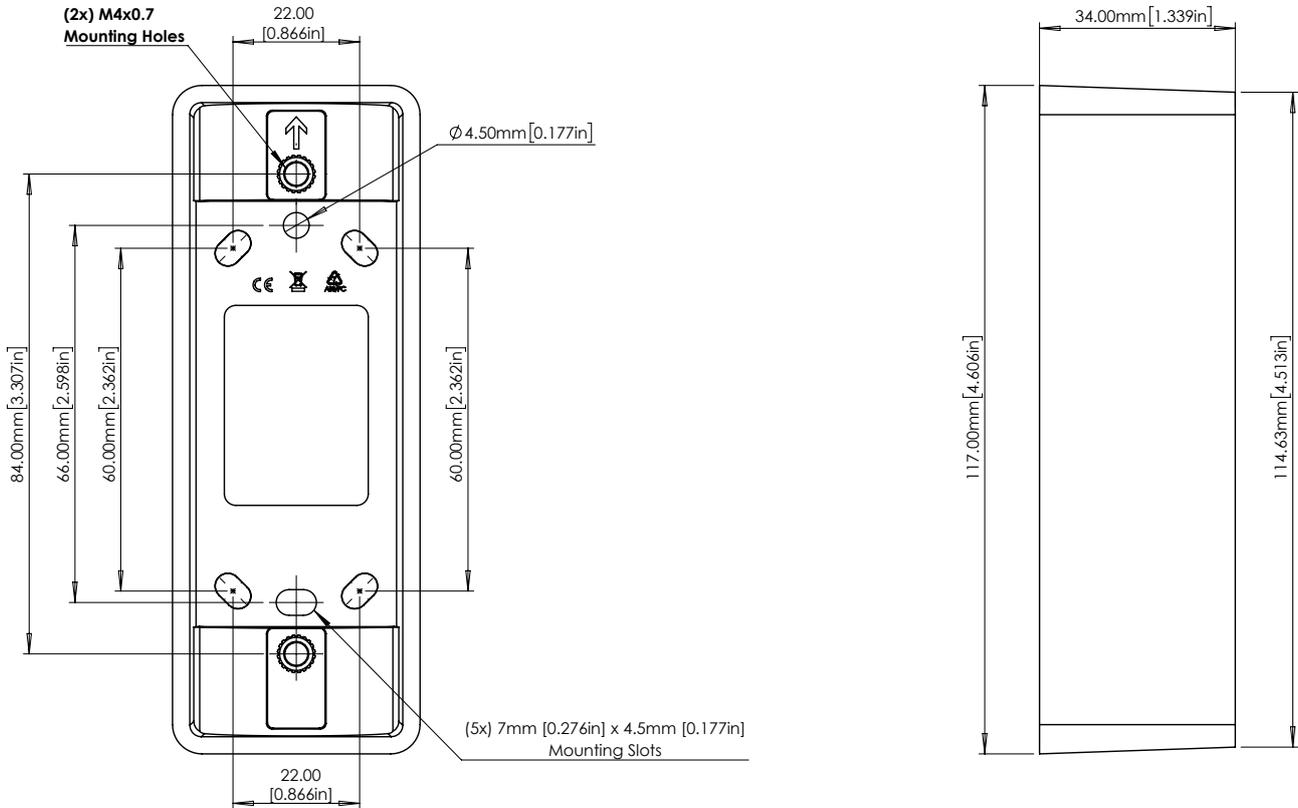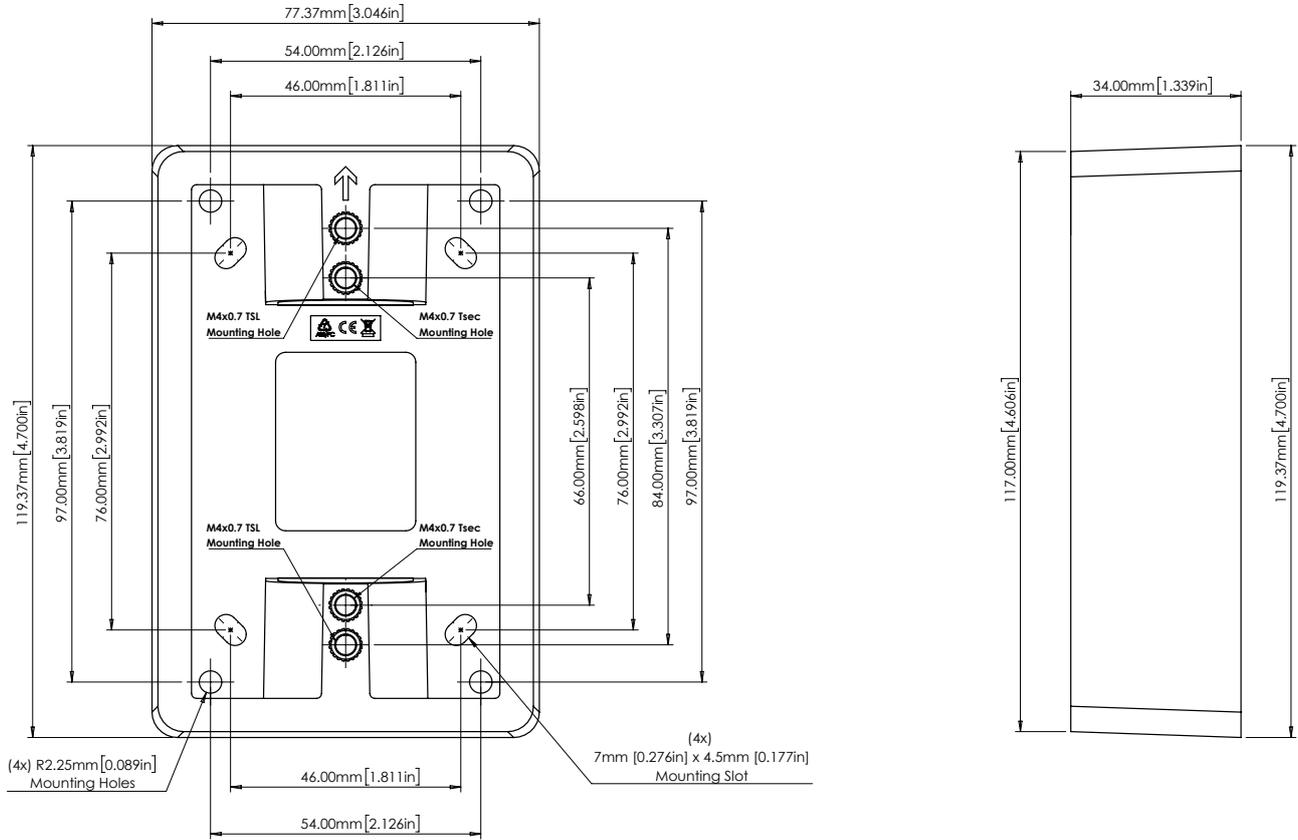

Dimensions shown on the front view:
- 77.37mm [3.046in]
- 54.00mm [2.126in]
- 46.00mm [1.811in]
- M4x0.7 TSL Mounting Hole
- M4x0.7 Tsec Mounting Hole
- 119.37mm [4.700in]
- 97.00mm [3.819in]
- 76.00mm [2.992in]
- 66.00mm [2.598in]
- 76.00mm [2.992in]
- 84.00mm [3.307in]
- 97.00mm [3.819in]
- (4x) R2.25mm [0.089in] Mounting Holes
- 46.00mm [1.811in]
- 54.00mm [2.126in]
- (4x) 7mm [0.276in] x 4.5mm [0.177in] Mounting Slot

Side view dimensions:
- 34.00mm [1.339in]
- 117.00mm [4.606in]
- 119.37mm [4.700in]

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	165mA (Peak, Reading)
Communications	
Card Read Range	MIFARE: 50mm (1.97″) DESFire EV1 ISO: 5mm (0.2″) DESFire EV2 ISO: 25mm (0.98″) DESFire EV3 ISO: 20mm (0.79″) 125kHz Clamshell: 45mm (1.78″) *
Tag Read Range	MIFARE: 25mm (0.98″) DESFire EV1: 5mm (0.2″) DESFire EV2: 5mm (0.2″) DESFire EV3: 10mm (0.39″) 125kHz: 25mm (0.98″) *
Wiegand Interface	Multiple format 26, 34 or 37, customizable; Bit data 0 and data 1 sent at 1kHz
Frequency	13.56 MHz ISO/IEC 14443 Type A 125KHz carrier. Several modulation formats are supported. *
Multi Conductor Cable	Module comms / RS-485: Belden 9842 or equivalent Max distance 900m (3000ft) Wiegand: 22 AWG alpha 5196, 5198, 18 AWG alpha 5386, 5388 Max Distance 150m (492ft)
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	Bluetooth® version 5.1 compliant Proprietary data exchange protocol. AES-128 encrypted 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) 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/cUL -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 RDF 2000 (UTE C 80-810) Standard)
Dimensions (H x W x D)	
Standard Reader	117 x 43 x 9.5mm (4.6 x 1.7 x 0.37")
Extra Reader	117 x 75 x 11.5mm (4.6 x 3.0 x 0.45")
Mini Reader	87 x 43 x 9.5mm (3.4 x 1.7 x 0.37")
Vandal Resistant Cover Dimensions	
Standard Reader VRC	160 x 90 x 13mm (6.3 x 3.5 x 0.51")
Extra Reader VRC	160 x 120 x 13mm (6.3 x 4.7 x 0.51")
Surface Mount Box Dimensions	
Standard Reader SMB	43 x 55 x 135mm (1.7 x 2.2 x 5.3")
Extra Reader SMB	43 x 83 x 135mm (1.7 x 3.3 x 5.3")

Weights	**Net Weight**	**Gross Weight**
Standard Reader	60g (2.1oz)	100g (3.5oz)
Extra Reader	120g (4.2oz)	130g (4.6oz)
Mini Reader	40g (1.4oz)	90g (3.2oz)
Vandal Resistant Cover Weights	**Net Weight**	**Gross Weight**
Standard Reader VRC	60g (2.1oz)	70g (2.5oz)
Extra Reader VRC	80g (2.8oz)	90g (3.2oz)
Surface Mount Box Weights	**Net Weight**	**Gross Weight**
Standard Reader SMB	50g (1.8oz)	70g (2.5oz)
Extra Reader SMB	80g (2.8oz)	110g (3.9oz)
Faceplate Weights	**Net Weight**	**Gross Weight**
Standard Reader Faceplate	10g (0.4oz)	20g (0.7oz)
Extra Reader Faceplate	30g (1.1oz)	40g (1.4oz)

Mini Reader Faceplate	10g (0.4oz)	20g (0.7oz)
Pigtail Cable Weights	**Net Weight**	**Gross Weight**
34cm Pigtail Cable	20g (0.71oz)	20g (0.71oz)
3.5m Pigtail Cable	190g (6.7oz)	230g (8.1oz)
Ferrite Shield Weights	**Net Weight**	**Gross Weight**
Extra Reader Ferrite Shield (10pc)	60g (2.1oz)	60g (2.1oz)

* Applies to multi technology models only

The size of conductor used for the supply of power to the unit should be adequate to prevent voltage drop at the terminals of no more than 5% of the rated supply voltage.

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

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

New Zealand and Australia

Intentional Transmitter Product Statement

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

R-NZ

European Standards

CE Statement CE

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

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

WEEE

Information on Disposal for Users of Waste Electrical & Electronic Equipment

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

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

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

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

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

For business users in the European Union

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

Information on Disposal in other Countries outside the European Union

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

EN50131 Standards

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

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

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

UKCA

UL and cUL Installation Requirements

Only UL / cUL listed compatible products are intended to be connected to a UL / cUL 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 cUL 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:

- Reorient or relocate 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.
- Consult the dealer or an experienced radio/TV technician for help.

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.