Ultimate Range.
Ultimate Choice.

tSec.

ICT® eSecurity.

tSec: Because one size does not fit all.

tSec.

Introducing the tSec Series

Sleek and stylish, and with a range of optional features, the TSEC series has a solution for everyone. Available in three sizes, multiple card capabilities, with an optional keypad, and in a choice of black or white, you can select the model to fit your needs and your decor.

Because one size does not fit all.

Multi Card Technology

Available with either 125kHz proximity or 13.56MHz smart card capability, or as a multi technology reader that combines both capabilities in a single unit delivering maximum compatibility while providing a path forward to the latest technology.

The Multi Technology Reader is ideal for organizations that wish to transition to smart technology at their own pace, as it means they don't need to replace all their cards upfront.

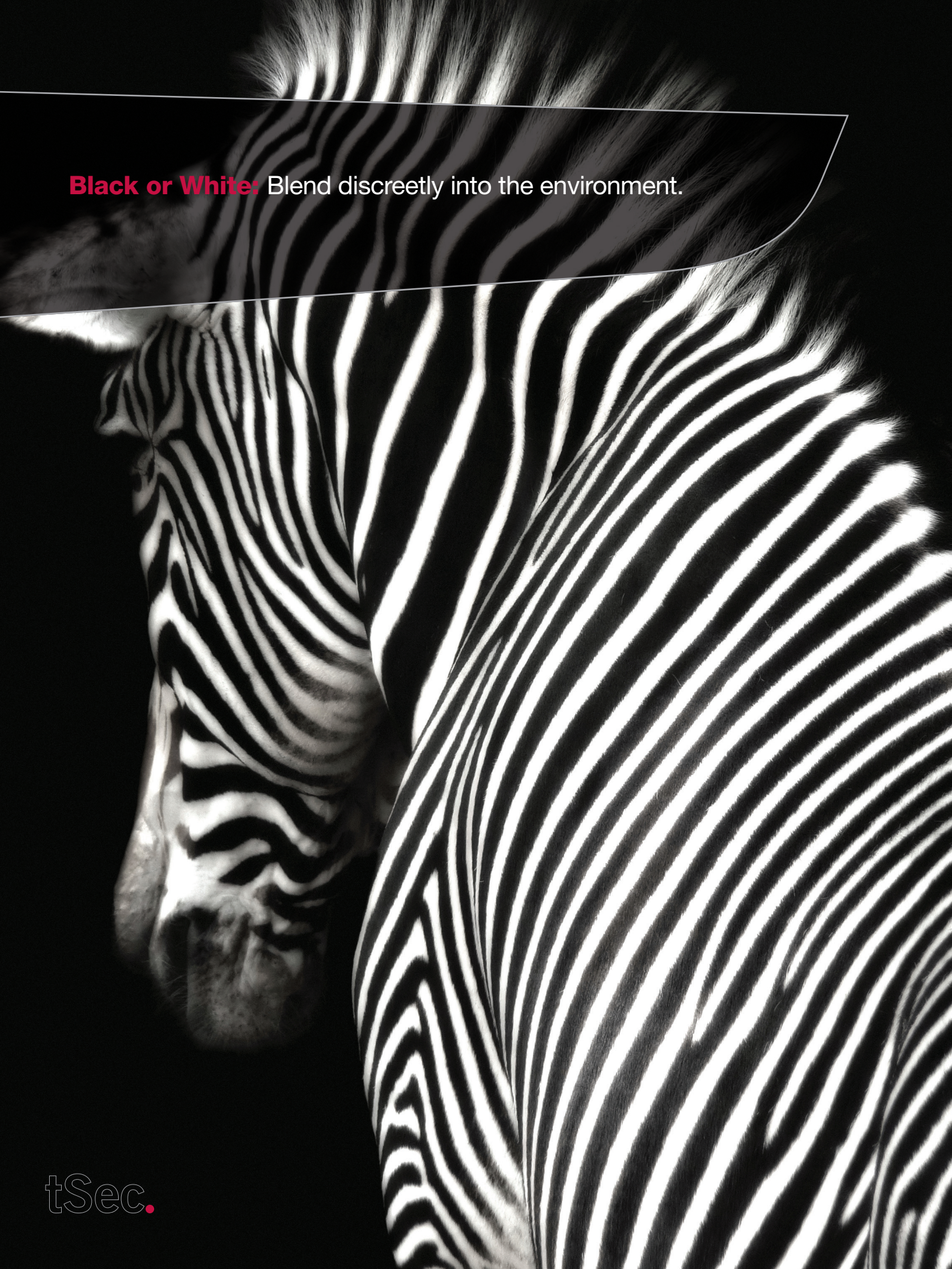
Flexible Communication

Choose between the intelligent RS-485 connection for fast, flexible, secure communication, or Wiegand for compatibility with all standard access control systems. RS-485 provides the added benefits of being easier and more cost effective to wire and deploy, and allows for direct integration with Protege systems enabling you to make changes on the fly once readers are installed. RS-485 also allows for longer cable runs and offers a simpler firmware update process.

IP65 Protection

The IP65 environmental rating provides a high degree of protection from the elements, making the TSEC Reader suitable for harsh environments. Readers can be mounted indoors or outdoors, located anywhere from the car park gate to the office door.

ICT® eSecurity.


Black or White: Blend discreetly into the environment.
tSec.

Models and Features

The TSEC Reader comes in three models (Standard, Extra, and Mini) and with a range of optional features. Each model is available with support for either 125kHz or Mifare/DESFire cards. The Standard and Extra are also available in a Multi Technology model combining support for Mifare, DESFire and 125kHz cards from a single reader, and with an optional capacitive touch keypad. **All models are available in either black or white.**

TSEC Standard

With a slim attractive design and the versatile mullion mount, the TSEC Standard is ideal for almost any location, including aluminium framed doors where larger readers are not an option.

		Keypad	125kHz	Mifare	DESFire
PRX-TSEC-STD	TSEC Standard Card Reader		•	•	•
PRX-TSEC-STD-KP	TSEC Standard Card Reader with Keypad	•	•	•	•
PRX-TSEC-STD-125	TSEC Standard 125kHz Card Reader		•		
PRX-TSEC-STD-125-KP	TSEC Standard 125kHz Card Reader with Keypad	•	•		
PRX-TSEC-STD-DF	TSEC Standard DESFire Card Reader			•	•
PRX-TSEC-STD-DF-KP	TSEC Standard DESFire Card Reader with Keypad	•		•	•

ICT® eSecurity.

Models and Features

TSEC Extra

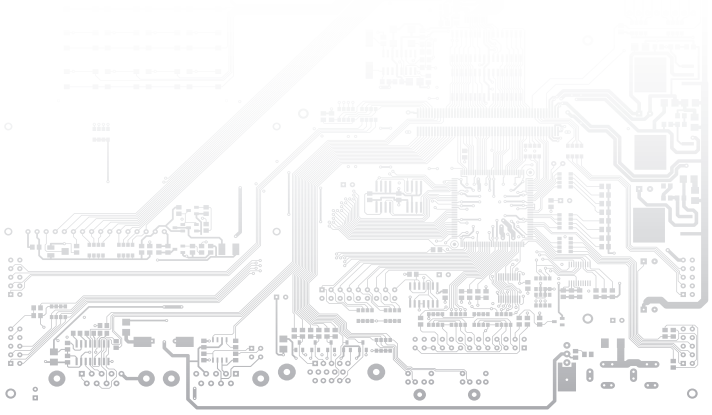
The full wall plate/lightswitch size makes the TSEC Extra the ideal choice when replacing existing readers with a larger footprint.

		Keypad	125kHz	Mifare	DESFire
PRX-TSEC-EXTRA	TSEC Extra Card Reader		•	•	•
PRX-TSEC-EXTRA-KP	TSEC Extra Card Reader with Keypad	•	•	•	•
PRX-TSEC-EXTRA-125	TSEC Extra 125kHz Card Reader		•		
PRX-TSEC-EXTRA-125-KP	TSEC Extra 125kHz Card Reader with Keypad	•	•		
PRX-TSEC-EXTRA-DF	TSEC Extra DESFire Card Reader			•	•
PRX-TSEC-EXTRA-DF-KP	TSEC Extra DESFire Card Reader with Keypad	•		•	•

TSEC Mini

The smallest of the TSEC family, the Mini is both unobtrusive and cost effective.

		Keypad	125kHz	Mifare	DESFire
PRX-TSEC-MINI-125	TSEC Mini 125kHz Card Reader		•		
PRX-TSEC-MINI-DF	TSEC Mini DESFire Card Reader			•	•



ICTeSecurity®

Choosing Card Technology

125kHz or 13.56MHz? When it comes to the end user, there is little visible difference between a 125kHz card and a 13.56MHz card. They present a card to a reader and access is either granted or denied. What happens behind the scenes is quite different however. Apart from the frequency that is used to transmit data, there are key differences in security and the card read range.

Card Technology Security Comparison

Historically, card based access control systems were built around a card with a magnetic stripe. These cards required a swipe action through a magnetic card reader to gain access to a door. This technology had a number of disadvantages, including an inconvenience factor, a high wear rate, and very low security. It was these disadvantages that led to the development of a new contactless proximity technology, allowing cards to be read without physically contacting the reader.

Proximity readers work by constantly emitting a short range RF field. When a proximity card comes within range of this field, an integrated chip within the card is powered up and the chip transmits a card number back to the reader. Not all proximity cards are born equal however, and it is important that the differences are weighed up before making a decision about which technology to adopt.

125kHz

The first of the proximity technologies was 125kHz. When a 125kHz card is powered up, it immediately begins to transmit its card number. In effect, this is very similar to the way the old mag-stripe readers worked. The problem is that being a proximity system, it is possible to create a device that will 'power up' a card from a distance, then read the data that is being transmitted. Once you have this, you can easily reproduce the card, making as many copies as you like. In many cases, you can even create cards in the same series with different numbers.

The one advantage of 125kHz is that due to the lower power requirements and small amount of data being transmitted, it offers a good read range (of around 110cm or 3.9") and a short read time, allowing users to present, swipe, or wave their card in the general direction of the reader to get a successful read.

While 125kHz is still commonly used, the widely publicized security flaws are something that require serious consideration.

Mifare / 13.56MHz

The Mifare standard was originally created as a ticketing solution for transport systems, and at the same time addressed the security issues in 125kHz technology by enabling two way communication between the card and reader. This saw the introduction of card encryption and the ability to store data on the card.

Most Mifare technologies store the card number in one of the storage areas on the card, known as sectors. When the card approaches the RF field of the reader, the card and reader begin a secure communication session using shared encryption keys. Once this is established, the card number is transmitted and the communication session is closed off. This process happens very quickly, however it does take slightly longer than a 125kHz based system and means that generally, a Mifare card cannot be simply swiped or waved at a card reader, but must be presented. Also, the two way process requires more energy than 125kHz, meaning a slightly reduced read range of around 7cm or 2.75".

Along with the added security, the additional storage space on the card can be used for many applications, such as offline locking systems or the storage of credit for pay as you go systems.

Mifare comes in many forms, each with their own advantages and disadvantages.

Mifare CSN

All Mifare cards come with a built-in CSN or card serial number. This electronic number is presented in much the same way as 125kHz in that it is not encrypted and can be read by a larger range of devices easily purchased on the open market. For instance, many smart phones are able to read this information, making it an even less secure method than most 125kHz systems. CSN is generally used where there is a requirement to read Mifare cards from a number of different access control systems, or from third party cards such as pay as you go cards. While it offers great flexibility, it is very insecure.

Mifare Classic

Mifare Classic was the first version of the Mifare standard. It stores the card number on one of its sectors, then encrypts the communication between the card and reader, theoretically making it impossible, or at least very difficult to copy a card. Unfortunately, a security flaw was discovered in the Mifare Classic standard which meant that with the right knowledge and hardware, a card could still be copied or another card in the series created.

ICT Secured Mifare

This is ICT's implementation of the Mifare standard. Card data is protected with a diversified authentication key and encrypted with an AES256 algorithm, effectively plugging the known security flaw in the Mifare standard. These cards are not as secure as DESFire but still provide high security against cloning.

ICT® eSecurity.

Mifare DESFire

The newest of the Mifare standards, Mifare DESFire includes a cryptographic module on the card itself to add an additional layer of Triple DES encryption to the card / reader transaction. This is the highest standard of card security currently available, however it does come with some disadvantages. The additional cryptographic module requires more energy to operate, resulting in a further reduced read range of 1-2cm or 0.4-0.8”. This means that when implementing DESFire technology, it is critical that it is done with some simple user education in order to avoid frustration. A DESFire card must be firmly presented to the reader and held in place until access is granted. Waving or swiping a DESFire card will not result in a successful read. Educate users to think of the card reader as a security guard – when requesting access, the reader needs to be shown your credentials, much like a security guard might inspect an ID card.

Site Codes

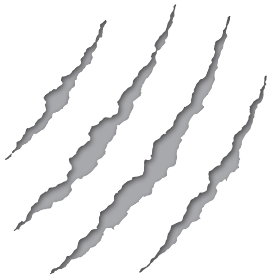
All cards are made up of a site code and a card number. The site code is designed to be unique to a particular site or building, meaning that a card from one building would not allow access at another building, even if the card number was the same.

With 125kHz, there are so many producers of cards worldwide and a relatively small number of site codes available, that it is possible - or even likely - that many legitimate versions of the same card exist.

With ICT Secured Mifare and Mifare DESFire cards, every site is registered with its own globally unique site code, and every card produced is recorded in our secure database. This ensures that duplicate cards are never created.

Encryption keys

ICT also offers the ability for an integrator or end user to purchase a reserved set of encryption keys. This effectively gives the organization its own entire set of globally unique site codes and card numbers. Optionally, the integrator or end user can encode their own cards at their site as they require them. This is still a managed system, ensuring that duplicates cannot be made.



ICT® eSecurity.

Integrated Control Technology Limited

11 Canaveral Drive, Albany, Auckland 0632
P.O. Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: support@incontrol.co.nz **Phone:** +64 (9) 476 7124 **Fax:** +64 (9) 476 7128
Designers & manufacturers of integrated electronic access control, security & automation products.
Designed & manufactured by Integrated Control Technology Limited.

www.ict.co