



Using SIFER readers



Introduction

The SIFER card reader is a new smart card reader designed and manufactured by Inner Range. It is a multi-drop RS-485 based reader that employs 128 bit AES encryption from the card through to the door module, providing a far superior level of security than that of traditional Wiegand based card readers. SIFER readers utilise the MIFARE DESfire EV1 card format.

It is important to note that the first release version of the SIFER reader will be restricted and specifically configured to support the Inner Range SIFER DESfire EV1 cards only. It is anticipated that subsequent versions of the SIFER reader will support the ability to read the CSN of other 13.56Mhz MIFARE based cards.

It is expected that SIFER readers and cards will be predominately deployed on new sites. For SIFER readers to be installed within an existing site, new Inner Range SIFER cards would need to be issued to all users.

This document explains how to configure SIFER readers connected to an Integrity controller.

The Open Supervised Device Protocol (OSDP) provides a bi-directional communication link to the SIFER reader. Compared to Wiegand, OSDP is more secure, uses fewer wires, can be wired over a longer range and supports a multi-drop topology.

Please read the hardware installation manual for the SIFER readers.

Reader serial numbers

SIFER readers have their own unique serial number. This number is factory configured and cannot be changed. Please refer to the hardware installation manual for information on where to locate the serial number on the reader.

As SIFER readers are attached to an Integrity RS485 reader port, the readers will automatically appear in Integrity System Designer software.

SIFER reader models

Customers have the option to deploy one of the following 3 models:

1. Standard secure
The default configuration
2. Custom secure
A secure configuration with a custom site encryption key
3. Registered secure
A secure configuration with a reserved custom site encryption key

SIFER Programmer



Installers will be able to purchase an Inner Range SIFER Programmer. The SIFER Programmer comes with a standard USB connection and a small Windows® based application to enable card programming.

The SIFER Programmer shall allow the installer to delete the factory configuration on a card and encode card details of their own choosing, namely:

- Card Number
- Site Code
- Encryption Key (32 HEX Digits)

Whilst it is technically possible, it is not recommended that the installer change the card number because the card number is already unique when leaving the Inner Range factory and the card number is also printed onto the card. Changing the default site code to a site specific site code would be the usual practice.

If desired, the installer may change the card number to any number between 1 – 4.3 billion. The site code may be any number from 1 – 16.7 million. SIFER cards are 56 bits in length with 24 bits dedicated to the site code and 32 bits to the card number.

Whenever any change is made to a card by the installer using the SIFER Programmer, a custom encryption key must also be applied. The custom encryption key is generated from a 32 digit

hexadecimal string that the installer assigns. The SIFER Programmer will not allow the installer program cards with the default Inner Range SIFER Global Key. Therefore, when a custom encryption key is used on a range of cards, the SIFER readers at the site must be updated to decrypt the new custom encryption key. A special configuration card can also be created by the SIFER Programmer to program the SIFER readers to operate with the new custom encryption key.

The SIFER Programmer is available to integrators and end users for the creation of User and Config cards.

Configuration Card

By default, SIFER readers are configured to only read cards with the Inner Range SIFER Global Key. Sites that wish to change the default SIFER Global Key to a custom encryption key may do so via the SIFER Programmer. A special configuration card can be created by the installer using the SIFER Programmer. This configuration card can then be used to reprogram the SIFER readers so that each reader on a site will be able to operate with the corresponding new cards produced by the installer for that site. In this way, the installer may maintain their own secret and custom encryption key(s), effectively mandating that all new SIFER cards and readers intended for use on their customer's site be programmed through their own installation company.

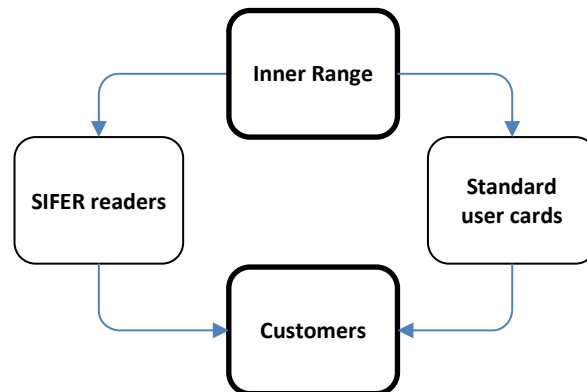
Readers are receptive to configuration cards for 5 mins after power up. After this period any configuration cards (with the correct key) presented will cause 3 seconds of continuous tone and red flashing main LED indicating that use of the configuration card is not allowed. The practice of presenting the configuration card twice within 5 seconds at each SIFER reader will program the reader with the updated custom encryption key. Repeating the process will toggle the SIFER reader back into its default state for use with the default Inner Range SIFER Global Key instead of the installer's custom encryption key.

If this type of card is presented to an unsecured reader in the 5 minute receptive period, the reader will beep, the main LED will turn purple and the small led will flash purple for 5 seconds. If the card is not presented again within the 5 seconds the reader will simply revert to normal operation. If the card is presented again within the 5 second period the reader will change site encryption key to the encryption key on the configuration card, the reader will beep and flash the main LED green for a second to confirm it is now secured.

Once a reader has been secured in this way, it can be un-secured with the same configuration card. If the correct configuration card is presented to a secured reader within the 5 minute receptive period, the reader will beep, the main LED will turn purple and the small LED will flash green (instead of purple) for 5 seconds. If the card is not presented again within 5 seconds, the reader will return to normal (secured) operation. If the card is presented again within the 5 seconds, the reader encryption key shall be converted back to the standard SIFER Global Key, the reader will beep and both LEDs will display green for a second to confirm it is now un-secured.

1. Standard secure

Inner Range sells SIFER readers and standard user cards to customers.



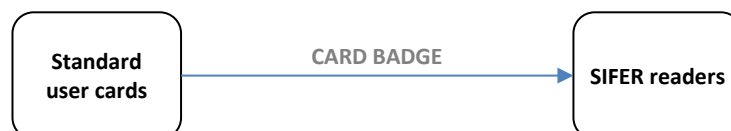
SIFER cards shall be encrypted using the Inner Range SIFER Global Key.

SIFER readers are preprogramed to decrypt the Inner Range SIFER Global Key.

All SIFER cards shall be programmed by Inner Range with the Inner Range SIFER Global Key, a common site code and a unique card number. Inner Range guarantees uniqueness of card numbers so that no two card numbers that leave the Inner Range factory shall ever be duplicated.

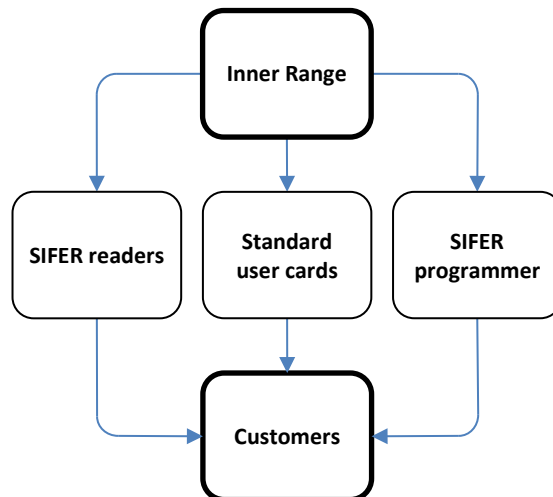
All SIFER cards shall have the card number laser etched onto the card.

SIFER cards have a 7 Byte (56 bit) Card Serial Number (CSN) that can be used and read by other MIFARE based readers.



2. Secure model

Inner Range sells SIFER readers, standard user cards and a SIFER programmer to the customer.



In this configuration, the installer will enter their custom site encryption key into the SIFER programmer using the provided software. The installer will then:

- Create configuration cards out of standard user cards to configure the SIFER readers on site with the custom site encryption key



- Secure the readers (with a custom site encryption key) using configuration cards

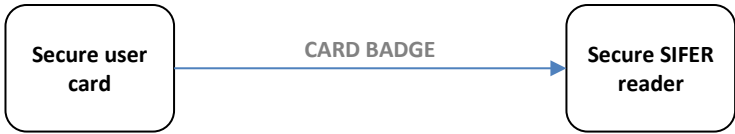


- Secure the standard user cards by programming them with the custom site encryption key using the SIFER programmer



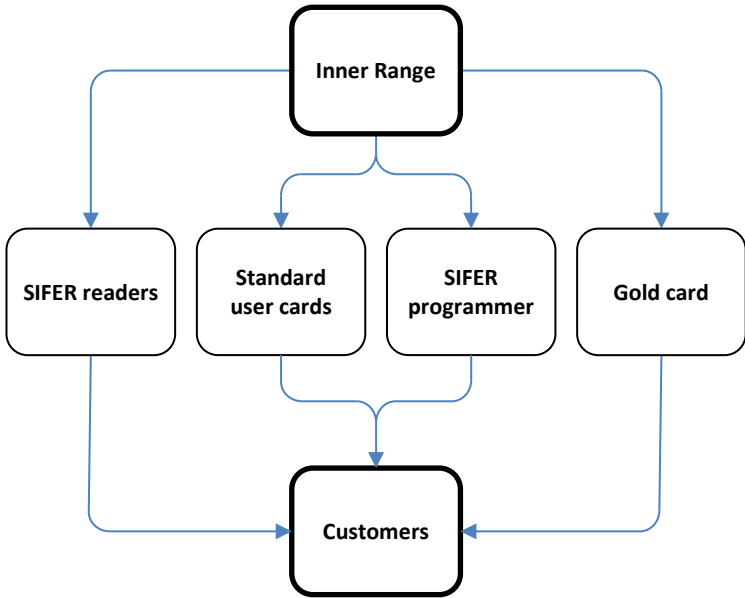
Once the SIFER readers have been configured with the custom site encryption key, the SIFER readers will not be able to read a standard SIFER card, only secured SIFER cards that have had additional secured data added using the same custom site encryption key. This configuration allows the installer to have vertical market lock in if they desire.

Cardholders use secured user cards to gain access.



3. Registered secure

Inner Range sells SIFER readers, SIFER cards, a SIFER programmer and a Gold card to the customer.



Installers:

- Use the Gold card to input the reserved site encryption key into the SIFER programmer



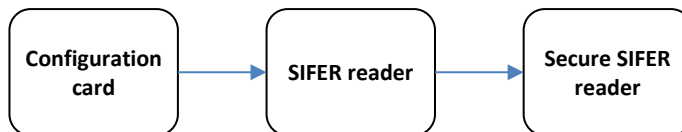
The Gold Key Configuration Card provides a guaranteed unique custom encryption key to the customer or installer. The custom encryption key provided by Inner Range under this service shall be registered and protected such that each custom encryption key CANNOT be accidentally or purposely programmed by an installer using the SIFER Programmer.

An authorised installer who has purchased a Gold Key Configuration Card must present this special configuration card to their SIFER Programmer when programming SIFER cards or reader configuration cards for use on the registered site.

- Use the SIFER programmer to create configuration cards to set the reserved encryption key into the SIFER readers



- Secure readers (with the reserved encryption key) using configuration cards



- Secure the standard user cards by programming them with the reserved encryption key using the SIFER programmer



This method is the same as the custom secure model with the additional guarantee of a unique site encryption key. The Gold card, SIFER card programmer and any configuration cards created should be kept in a secure location because they hold the reserved encryption key. This especially applies to the Gold card, as that may be used to program another SIFER programmer with the reserved encryption key.

Adding a SIFER reader to a door

When SIFER readers are attached to an Integriti module, the readers will automatically address and come online if the following conditions are met:

- The reader module has at least one spare slot (a reader slot set to 'None').
- The total number of SIFER readers supported by the reader has not been exceeded.
- The [OSDP Options](#) » [OSDP_DisableAutoAddressing](#) option is not ticked.
- None of the readers belonging to the reader module are configured to:
 - Salto
 - Aperio

Check the hardware manual for the reader module to determine the total number of SIFER readers supported.

SIFER reader configuration options

Allow roughly 10 seconds for SIFER reader programming changes to take effect.

Reader 1	SIFER
Serial Number	7
Volume	255
Maximum Brightness	255
Feedback Mode	Show the open/locked state of the do...
Main Led Colour	CYAN
Small Led Colour	MAGENTA
Show Area Status Entry Delay	☒
Show Area Status Exit Delay	☒
Show Area Status Armed / Disarmed	☒
Show Area Status Isolated	☐
Show Area Status Had Alarm	☐

Option

Description

Serial Number

The serial number of the SIFER reader.

Please refer to the hardware installation manual for information on where to locate the serial number on the reader.

Volume

Configurable between 0 (off) and 255 (loudest).

Maximum brightness

Configurable between 0 (off) and 255 (brightest).

Feedback Mode

The five options available are:

- (None)
- Show the area state of the area specified by 'Keypad Area' item.
- Show the area state of the area on the same side of the door as this reader.
- Show the area state on the other side of the door to this reader.
- Show the open/locked state of the door associated with this reader.

Main LED colour

Select from 1 of 23 colours (including black / off)

Small LED colour

Select from 1 of 23 colours (including black / off)

Show area status entry delay (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will slow flash green and play a slow chime sound.
Show area status exit delay (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will slow flash green and play a slow chime sound.
Show area status armed / disarmed (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will show green for disarmed and red for armed.
Show area status isolated (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will show amber when an input is isolated.
Show area status had alarm (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will fast flash red and play a repeating two tone chime sound.

SIFER programming software

At the time of writing the SIFER programming software is not available to integrators. This section of the document will be updated closer to the release of the SIFER programmer and software.

SIFER card format

Card numbers are configurable to any number between 1 – 4.3 billion (4,294,967,295).
Site code numbers are configurable to any number between 1 – 16.7 million (16,777,215).

SIFER cards are 56 bits in length with 24 bits dedicated to the site code and 32 bits to the card number.

Bits:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Site Code:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Card Number:																				

Bits:	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Site Code:	21	22	23	24																
Card Number:					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Bits:	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
Site Code:																
Card Number:	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

SIFER reader states

State	Description
Powered on.	• Reader Beep. • Single green flash.
Powered, waiting for address / unaddressed / unable to communicate with the controller.	• The main LED will alternate between White and Grey. • The small LED will fade in and out blue.
Powered, online.	• The reader will play an ascending 'online' tone. • The main LED will be cyan. <i>Note: This value can be changed.</i> • The small LED will be magenta. <i>Note: This value can be changed.</i>

Common problems

Begin by reviewing the hardware installation manual.

- Ensure the readers have been installed correctly according to the hardware manual.
- Make sure the readers have been connected to the correct port on the reader module.

Make sure the Integriti software, module firmware and SIFER firmware are up to date. Please refer to section 10.3 – ‘Maintaining Firmware’ of the ‘System Configuration Handbook’ for more details.

Problem	Resolution
SIFER reader does not appear in the Inside / Outside Reader drop down options. SIFER reader is not getting an address / has not played ‘online’ tone.	• Ensure the Door record you are configuring belongs to the controller that the reader is attached to. • Check the reader is attached to a reader RS485 port. • Make sure you have not exceeded the total number of readers the module supports. • The ‘OSDP_DisableAutoAddressing’ option should be un-ticked. • Ensure the firmware on the controller and readers are up to date. • Cycle power to the SIFER reader.
SIFER reader is not updating when I change settings.	• Make sure your controller, module and software versions are all up to date. • Check the supported number of readers for the module has not been exceeded. • Changes can take roughly 10 seconds.
Enrolment fails.	• Confirm the controller firmware revision is compatible with the Integriti version you are using.
Reader is not responding to SIFER cards.	• Ensure the cards and readers are configured to use the same security key.