

# AY-T6350

**MIFARE® Contactless Smart Card / PIN Readers**

Installation and Programming Manual



**ROSSLARE**  
SECURITY PRODUCTS

## **Copyright © 2018 by Rosslare. All rights reserved.**

This manual and the information contained herein are proprietary to ROSSLARE ENTERPRISES LIMITED and/or its related companies and/or subsidiaries' (hereafter: "ROSSLARE"). Only ROSSLARE and its customers have the right to use the information.

No part of this manual may be re-produced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of ROSSLARE.

ROSSLARE owns patents and patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this manual.

TEXTS, IMAGES, AND ILLUSTRATIONS INCLUDING THEIR ARRANGEMENT IN THIS DOCUMENT ARE SUBJECT TO THE PROTECTION OF COPYRIGHT LAWS AND OTHER LEGAL RIGHTS WORLDWIDE. THEIR USE, REPRODUCTION, AND TRANSMITTAL TO THIRD PARTIES WITHOUT EXPRESS WRITTEN PERMISSION MAY RESULT IN LEGAL PROCEEDINGS.

The furnishing of this manual to any party does not give that party or any third party any license to these patents, trademarks, copyrights or other intellectual property rights, except as expressly provided in any written agreement of ROSSLARE.

ROSSLARE reserves the right to revise and change this document at any time, without being obliged to announce such revisions or changes beforehand or after the fact.

# Table of Contents

<b>1. Introduction .....</b>	<b>8</b>
1.1 Supported RFID Transponders .....	8
1.2 Box Content .....	8
<b>2. Technical Specifications .....</b>	<b>9</b>
<b>3. Installation .....</b>	<b>10</b>
3.1 Mounting .....	10
3.2 Wiring .....	11
<b>4. How to Use the Reader .....</b>	<b>13</b>
4.1 Normal Operation .....	13
4.2 Optical Back Tamper .....	14
4.3 LED Control .....	14
<b>5. Keypad Programming Instructions .....</b>	<b>15</b>
5.1 Programming Menu .....	15
5.2 Entering Programming Mode .....	16
5.3 Exiting Programming Mode .....	16
5.4 Selecting Keypad Transmission Format .....	17
5.4.1 Single Key, Wiegand 6-Bit (Rosslare Format) .....	18
5.4.2 Single Key, Wiegand 6-Bit, Nibble & Parities .....	18
5.4.3 Single Key, Wiegand 8-Bit, Nibbles Complemented .....	18
5.4.4 4 Keys Binary + Facility Code, Wiegand 26-Bit .....	19
5.4.5 1 to 5 Keys + Facility Code, Wiegand 26-Bit .....	19
5.4.6 6 Keys BCD and Parity Bits, Wiegand 26-Bit .....	20
5.4.7 Single Key, 3x4 Matrix Keypad (MD-P64) .....	21
5.4.8 1 to 8 Keys BCD, Clock & Data .....	21

## Table of Contents

---

5.5	Selecting the Proximity Card Transmission Format .....	22
5.5.1	Wiegand 26-Bit .....	23
5.5.2	Clock and Data .....	23
5.5.3	Wiegand Card + PIN Transmission Format .....	23
5.5.4	Wiegand 26-Bit and Facility Code .....	24
5.5.5	Wiegand 32-Bit .....	24
5.5.6	Wiegand 32-Bit Reversed .....	24
5.5.7	Wiegand 34-Bit .....	25
5.5.8	Wiegand 40-Bit and Checksum .....	25
5.6	Changing the Programming Code .....	26
5.7	Changing the Facility Code .....	26
5.8	Return to Factory Default Settings .....	27
5.9	Replacing a lost Programming Code .....	27
<b>A.</b>	<b>Limited Warranty .....</b>	<b>28</b>

# List of Figures

Figure 1: Removing the Top Cover .....	10
--	----

# List of Tables

Table 1: Wiring Colors.....	11
Table 2: Programming Menu.....	15

# Notice and Disclaimer

This manual's sole purpose is to assist installers and/or users in the safe and efficient installation and usage of the system and/or product, and/or software described herein.

**BEFORE ATTEMPTING TO INSTALL AND/OR USE THE SYSTEM, THE INSTALLER AND THE USER MUST READ THIS MANUAL AND BECOME FAMILIAR WITH ALL SAFETY REQUIREMENTS AND OPERATING PROCEDURES.**

- The system must not be used for purposes other than those for which it was designed.
- The use of the software associated with the system and/or product, if applicable, is subject to the terms of the license provided as part of the purchase documents.
- ROSSLARE exclusive warranty and liability is limited to the warranty and liability statement provided in an appendix at the end of this document.
- This manual describes the maximum configuration of the system with the maximum number of functions, including future options. Therefore, not all functions described in this manual may be available in the specific system and/or product configuration you purchased.
- Incorrect operation or installation, or failure of the user to effectively maintain the system, relieves the manufacturer (and seller) from all or any responsibility for consequent noncompliance, damage, or injury.
- The text, images and graphics contained in the manual are for the purpose of illustration and reference only.
- All data contained herein subject to change without prior notice.
- In no event shall manufacturer be liable for any special, direct, indirect, incidental, consequential, exemplary or punitive damages (including, without limitation, any and all damages from business interruption, loss of profits or revenue, cost of capital or loss of use of any property or capital or injury).
- All graphics in this manual are for reference only, some deviation between the image(s) and the actual product may occur.
- All wiring diagrams are intended for reference only, the photograph or graphic of the PCB(s) are intended for clearer illustration and understanding of the product and may differ from the actual PCB(s).

# 1. Introduction

The AY-T6350 is MIFARE® contactless smart card and PIN reader for indoor and outdoor use. The unit reads the MIFARE card serial number (CSN) and transmits in Wiegand, Clock & Data, or Wiegand Card + PIN formats.

In addition, the AY-T6350 comes with a backlit keypad that can be programmed to output eight data formats. The AY-T6350 supports MIFARE Classic and MIFARE Ultralight cards that allow multiple card and keypad transmission formats, thus providing a high level of compatibility and connectivity with host controllers.

## 1.1 Supported RFID Transponders

The AY-T6350 reads the following transponders:

- MIFARE Ultralight 512-bit EEPROM
- MIFARE Classic 1K bytes memory
- MIFARE Classic 4K bytes memory



MIFARE Ultralight 512-bit EEPROM is only partly supported; only 32 bits out of the 64 bits can be transmitted.

## 1.2 Box Content

Before beginning, verify that all of the following is in the box; if anything is missing, please contact your nearest Rosslare office.

- One AY-T6350 reader
- Installation kit including:
  - One drilling template (label/sticker)
  - One security spline key
  - One security hex screw
  - Two mounting screws and wall plugs
- Installation and Programming Manual



## 2. Technical Specifications

### Electrical Characteristics

<b>Power Supply Type</b>	Linear (recommended)
<b>Input Voltage</b>	8–16 VDC
<b>Absolute Maximum Voltage (non-operating)</b>	18 VDC
<b>Maximum Input Current</b>	Standby: 180 mA, Read: 235 mA
<b>LED Control Input</b>	Dry Contact N.O.
<b>Tamper Output</b>	Open collector, active low, max. sink current 32 mA
<b>Max. Controller Cable Distance</b>	150 m (500 ft)
<b>Max. Proximity Read Range*</b>	70 mm (2.8 in.)
<b>Frequency</b>	13.56 MHz
<b>Transmission Formats</b>	Wiegand and Clock & Data
<b>Card Compatibility</b>	MIFARE Classic and MIFARE Ultralight cards

### Environmental Characteristics

<b>Operating Temp. Range</b>	-31°C to 63°C (-25°F to 145°F)
<b>Operating Humidity</b>	0 to 95% (non-condensing) Suitable for outdoor use (meets IP65)

### Physical Characteristics

<b>Height x Width x Depth</b>	110 x 80 x 17.5 mm (4.3 x 3.2 x 0.7 in.)
<b>Weight</b>	170 g (6 oz)

\* Measured using a Rosslare proximity card or equivalent. Range also depends on electrical environment and proximity to metal.

### 3. Installation



Installation of an RFID reader adjacent to metallic surfaces might alter the reader's specifications. To diminish this interference, use a plastic spacer when mounting the reader.

The AY-T6350 pack includes everything needed to install and operate the smart card sector readers. Mount the reader on the required surface and connect it to the access control system.

#### 3.1 Mounting

1. Peel off the back of the self-adhesive mounting label template and place it at the required mounting location.
2. Using the template as a guide, drill two holes (sizes indicated on the template) used for mounting the back plate onto the surface.
3. Insert a suitable wall plug into each screw hole.
4. Drill a 10-mm (7/16") hole for the cable. If mounting on metal, place a grommet or electrical tape around the edge of the hole.
5. At the bottom of the unit's case, remove the screw.
6. Remove the reader's snap-off front cover to reveal the two screw holes (Figure 1).

**Figure 1: Removing the Top Cover**



## Installation

---

7. Insert the unit's cable wire into the cable hole and wire the unit as described in Section 3.2.
8. Screw the back cover to its mounting location.
9. Carefully re-attach the front cover of the unit.
10. Secure the front cover by using the supplied security Torx screw. A Torx security screw tool is provided to tighten the security Torx screw.



The reader can also be mounted using strong epoxy glue. After application, the reader should be firmly held in place until the glue dries.

### 3.2 Wiring

The reader is supplied with an 18" pigtail, comprising six wires.

#### *To connect the reader to the controller:*

1. Prepare the unit's cable by cutting the cable jacket back 3.2 cm (1¼") and stripping the wire 1.3 cm (½").
2. Prepare the controller cable by cutting the cable jacket back 3.2 cm (1¼") and stripping the wire 1.3 cm (½").
3. Splice the reader's pigtail wires to the corresponding controller wires (as listed in Table 1) and cover each joint with insulating tape.

**Table 1: Wiring Colors**

<b>Reader</b>	<b>Color</b>	<b>Function</b>
5~16 VDC	Red	+DC input
Shield/Ground	Black	Ground
Data 1	White	Data 1
Data 0	Green	Data 0
LEDCTL	Brown	LED/buzzer control
Tamper	Purple	Tamper

## Installation

---

4. If the tamper output is being utilized, connect the purple wire to the correct input on the controller.
5. Trim and cover all unused conductors.



- The individual wires from the reader are color-coded according to the Wiegand standard.
- When using a separate power supply for the reader, this supply and that of the controller must have a common ground.
- The reader's cable shield wire should be preferably attached to an earth ground, or a signal ground connection at the panel, or a power supply end of the cable. This configuration is best for shielding the reader cable from external interference.

# 4. How to Use the Reader

After the reader has been mounted, connected to an access control system, and configured, it is ready for use.

## 4.1 Normal Operation

The default mode of the reader is Standby mode. In Standby mode, the unit is ready to receive data from a presented proximity card or an entered PIN code. When a card is presented, the reader scans the card and sends each card's serial number to the access control system. This CSN is unique for each card.



If the CSN is not fully transmitted, only the LSB portion of the serial number is transmitted. This depends on the reader transmit format of the selected reader and the length of the CSN. For example, when the Wiegand 26-bit transmit format is selected; the MSB byte of the MIFARE 1K card's serial number is not transmitted.

Programming the reader is done via the unit's keypad driven programming menu system (Chapter 5).

Keyboard data can be sent via one of several different keypad transmission formats (see Section 5.4).

MIFARE cards presented to the reader are always sent in Wiegand, Clock & Data, or Card + PIN Wiegand format (see Section 5.5).

When the reader is in Standby mode, the LED is white.



When a card or PIN entry is being transmitted, the LED flashes green.



When the reader is in Programming mode, the LED is off.



### **4.2 Optical Back Tamper**

The reader includes an optical back tampering mechanism which detects all attempts to dismantle the unit or remove it from the wall.

The status of the tamper mechanism is indicated by the purple Tamper control wire.

When the back tamper optical sensor is in "darkness" status, the internal tamper output transistor is pulled to low.

When the back tamper optical sensor is in its "lit" status, the internal tamper output transistor's collector is open. A tamper signal is detected by the host control panel.

### **4.3 LED Control**

To cause the LED to remain green continuously, pull the LED control wire (brown) to ground (black wire). If the LED control wire (brown) is left open, the LED behaves as described above.

Connecting the LED control input to the access control unit's LED control output allows control of the LED color; for example, it may turn it green then back to white on access granted by a valid card.

# 5. Keypad Programming Instructions

## 5.1 Programming Menu

Programming the reader is done via the unit's keypad driven programming menu system. Table 2 shows the names of all the programming menus. Default factory settings (certain pre-programmed codes and settings) are marked by an asterisk (\*).

**Table 2: Programming Menu**

	<b>Menu Description</b>	<b>Default</b>
<b>1</b>	<b>Selecting Keypad Transmission Format</b> 1 – Single Key, Wiegand 6-Bit (Rosslare Format, Default) 2 – Single Key, Wiegand 6-Bit with Nibble + Parity Bits 3 – Single Key, Wiegand 8-Bit, Nibbles Complemented 4 – 4 Keys Binary + Facility Code, Wiegand 26-Bit 5 – 1 to 5 Keys + Facility Code, Wiegand 26-Bit 6 – 6 Keys BCD and Parity Bits, Wiegand 26-Bit 7 – Single Key, 3x4 Matrix Keypad 8 – 1 to 8 Keys BCD, Clock & Data Single Key	*
<b>2</b>	<b>Selecting MIFARE Card Transmission Format</b> 1 – Wiegand 26-Bit (default) 2 – Clock & Data 3 – Wiegand Card + PIN 4 – Wiegand 26-Bit with Facility Code Output 5 – Wiegand 32-Bit 6 – Wiegand 32-Bit Reverse Output 7 – Wiegand 34-Bit 8 – Wiegand 40-Bit	*
<b>3</b>	<b>Changing the Programming Code</b>	1234
<b>4</b>	<b>Changing the Facility Code</b>	001
<b>0</b>	<b>Return to Factory Default Settings</b>	

### 5.2 Entering Programming Mode

To reach the Programming Menu System, the unit must first be placed into Programming mode.



- The factory default Programming code is 1234.
- If a Programming code is not entered within 30 seconds, the reader returns to Transmit mode.

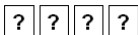
#### *To enter Programming mode:*

1. Press # four times.

The LED flashes white.



2. Enter your 4-digit Programming code.



3. If the Programming code is valid, the program LED turns off and the reader enters Programming mode.



Wrong entries may reset the reader back to Standby mode. If no key is pressed for 30 seconds while in Programming mode, the unit exits Programming mode and returns to Standby mode

### 5.3 Exiting Programming Mode

#### *To exit Programming mode:*

1. Press # to exit Programming mode at any time.

You hear a long beep and the LED turns white.



This indicates that the unit has returned to Standby mode.



### 5.4 Selecting Keypad Transmission Format

There are eight keypad transmission formats.



Only one keypad transmission format can be active at any one time.

*To select the keypad transmission format:*

1. Enter Programming mode.



2. Press **1** to enter Menu 1.



The LED flashes green.



3. Enter one of the following codes:
  - **1** – Single Key, Wiegand 6-Bit (Rosslare Format) (default)
  - **2** – Single Key, Wiegand 6-Bit with Nibble + Parity Bits
  - **3** – Single Key, Wiegand 8-Bit, Nibbles Complemented
  - **4** – 4 Keys Binary + Facility Code, Wiegand 26-Bit
  - **5** – 1 to 5 Keys + Facility Code, Wiegand 26-Bit
  - **6** – 6 Keys BCD and Parity Bits, Wiegand 26-Bit
  - **7** – Single Key, 3x4 Matrix Keypad
  - **8** – 1 to 8 Keys BCD, Clock & Data Single Key
  - **9** – Single Key, Wiegand 4-Bit



When selecting Option 8, the Program LED turns green, awaiting an additional key input to select the number of keys.

You hear three beeps.



The system returns to Standby mode.

If an incorrect option number is entered, a long beep is heard and the reader returns to Standby mode. The keypad transmission format remains unchanged.

### 5.4.1 Single Key, Wiegand 6-Bit (Rosslare Format)

Each key press immediately sends 4 bits with 2 parity bits added – even parity for the first 3 bits and odd parity for the last 3 bits.

0 = 1 1010 0	6 = 1 0110 0
1 = 0 0001 0	7 = 1 0111 1
2 = 0 0010 0	8 = 1 1000 1
3 = 0 0011 1	9 = 1 1001 0
4 = 1 0100 1	* = 1 1011 1 = "B" in Hexadecimal
5 = 1 0101 0	# = 0 1100 1 = "C" in Hexadecimal

### 5.4.2 Single Key, Wiegand 6-Bit, Nibble & Parities

Each key press immediately sends 4 bits with 2 parity bits added – even parity for the first 3 bits and odd parity for the last 3 bits.

0 = 0 0000 1	6 = 1 0110 0
1 = 0 0001 0	7 = 1 0111 1
2 = 0 0010 0	8 = 1 1000 1
3 = 0 0011 1	9 = 1 1001 0
4 = 1 0100 1	* = 1 1010 0 = "A" in Hexadecimal
5 = 1 0101 0	# = 1 1011 1 = "B" in Hexadecimal

### 5.4.3 Single Key, Wiegand 8-Bit, Nibbles Complemented

This options inverts the most significant bits in the message leaving the least 4 significant bits as BCD representation of the key. The host system receives an 8-bit message.

0 = 11110000	6 = 10010110
1 = 11100001	7 = 10000111
2 = 11010010	8 = 01111000
3 = 11000011	9 = 01101001
4 = 10110100	* = 01011010 = "A" in Hexadecimal
5 = 10100101	# = 01001011 = "B" in Hexadecimal

### 5.4.4 4 Keys Binary + Facility Code, Wiegand 26-Bit

This option buffers 4 keys and outputs keypad data with a 3-digit facility code like a standard 26-bit card output.

The Facility code is set in Programming Menu 4 four and can be in the range 000 to 255. The factory default setting for the facility code is 001 (see Section 5.7 for more information).

The keypad PIN code must be 4 digits in length and can range between 0000 and 9999. On the fourth key press of the 4-digit PIN code, the data is sent across the Wiegand Data lines as binary data in the same format as a 26-Bit card.

If \* or # is pressed during PIN code entry, the keypad clears the PIN code entry buffer, generates a beep and is ready to receive a new 4-digit keypad PIN code.

If the entry of the 4-digit keypad PIN code is disrupted and no number key is pressed within 5 seconds, the keypad clears the PIN code entry buffer, generates a beep and is ready to receive a new 4-digit keypad PIN code.

(EP) FFFF FFFF AAAA AAAA AAAA AAAA (OP)

Where: EP = Even parity for first 12 bits

OP = Odd parity for last 12 bits

F = 8-Bit Facility code

A = 24-Bit code generated from keyboard

### 5.4.5 1 to 5 Keys + Facility Code, Wiegand 26-Bit

This option buffers up to 5 keys and outputs keypad data with a facility code like a 26-bit card output.

The Facility code is set in Programming Menu 4 and can be in the range 000 to 255. The factory default setting for the Facility code is 001 (see Section 5.7).

The keypad PIN code can be one to five digits in length and can range between 0 and 65,535. When entering a keypad PIN code that is less than 5 digits in length, # must be pressed to signify the end of PIN code entry. For keypad PIN codes that are 5 digits in length, on the

fifth key press of the 5-digit PIN code, the data is sent across the Wiegand Data lines as binary data in the same format as a 26-bit card.

If \* is pressed during PIN code entry or a PIN code greater than 65,535 is entered, the keypad clears the PIN code entry buffer, generates a beep and is ready to receive a new 4-digit keypad PIN code.

If the entry of the 1- to 5-digit keypad PIN code is disrupted and no number key is pressed within 5 seconds, the keypad clears the PIN code entry buffer, generates a medium length beep and is ready to receive a new 1- to 5-digit keypad PIN code.

(EP) FFFF FFFF AAAA AAAA AAAA AAAA (OP)

Where: EP = Even parity for first 12 bits

OP = Odd parity for last 12 bits

F = 8-Bit Facility code

A = 24-Bit code generated from keyboard

### 5.4.6 6 Keys BCD and Parity Bits, Wiegand 26-Bit

This option sends a buffer of 6 keys, adds parity, and sends a 26-bit BCD message. Each key is a four bit equivalent of the decimal number.

The keypad PIN code must be 6 key presses long. On the sixth key press of the 6-digit PIN code, (# and \* keys are valid), the data is sent across the Wiegand Data lines as a BCD message.

If the entry of the 6-digit keypad PIN code is disrupted and no number key is pressed within 5 seconds, the keypad clears the PIN code entry buffer, generates a medium length beep and is ready to receive a new 6-digit keypad PIN code.

(EP) AAAA BBBB CCCC DDDD EEEE FFFF (OP)

Where:

A = The first key entered      D = Fourth key entered

B = Second key entered      E = Fifth key entered

C = Third key entered      F = Sixth key entered

### 5.4.7 Single Key, 3x4 Matrix Keypad (MD-P64)

Each key press immediately sends 4 bits data, no parity bits added.

0 = 0000	6 = 0110
1 = 0001	7 = 0111
2 = 0010	8 = 1000
3 = 0011	9 = 1001
4 = 0100	* = 1010 = "A" in Hexadecimal
5 = 0101	# = 1011 = "B" in Hexadecimal

### 5.4.8 1 to 8 Keys BCD, Clock & Data

This option buffers up to 8 keys and outputs keypad data, much like standard Clock and Data card output.

The keypad PIN code can be one to eight digits in length. The PIN code length is selected while programming the reader for Option 8. The reader transmits the data when it receives the last key press of the PIN code. The data is sent across the two data output lines as binary data in Clock & Data format.

If \* or # is pressed during PIN code entry, the keypad clears the PIN code entry buffer, generates a beep, and is ready to receive a new keypad PIN code.

If the entry of the digit keypad PIN code is disrupted and a number key or # is not pressed within 5 seconds, the keypad clears the PIN code entry buffer, generates a medium length beep and is ready to receive a new keypad PIN code.

### 5.5 Selecting the Proximity Card Transmission Format

There are eight selectable card transmission formats.

*To select the proximity card transmission format:*

1. Enter Programming mode.



2. Press **2** to enter Menu 2.



The LED flashes green.



3. Enter one of the following codes:
  - **1** – Wiegand 26-Bit (default)
  - **2** – Clock & Data
  - **3** – Wiegand Card and PIN
  - **4** – Wiegand 26-Bit with Facility Code
  - **5** – Wiegand 32-Bit
  - **6** – Wiegand 32-Bit Reverse
  - **7** – Wiegand 34-Bit
  - **8** – Wiegand 40-Bit

You hear three beeps.



The system returns to Standby mode.

If an incorrect option number is entered, the reader returns to Transmit mode and the keypad transmission format remains unchanged.

### 5.5.1 Wiegand 26-Bit

In this mode, 3 bytes of the CSN are transmitted in Wiegand 26-Bit format. Two parity bits are added. An even parity bit is sent first, followed by three bytes card data than followed by odd parity bit.



The fourth byte of the cards serial number is not transmitted.

(EP) AAAA AAAA AAAA AAAA AAAA AAAA (OP)

Where:      EP = Even parity for first 12 bits  
              OP = Odd parity for last 12 bits  
              A = 3 bytes code generated from card data

### 5.5.2 Clock and Data

In this mode, 4 bytes of the CSN are transmitted in Clock&Data format.

### 5.5.3 Wiegand Card + PIN Transmission Format

This unique mode is intended to let host controllers get card and keypad data simultaneously. This option overrules the selected Keypad Transmission Format and sends the keypad data as described below.

The output data turns into a virtual Wiegand 52-bit – 26-bit card data followed by a 26-bit keypad data.

After a card is presented to the reader, the LED starts to flash white to indicate that the reader is waiting for the PIN code.

The entered PIN code is buffered up to 5 keys and outputs keypad data with a Facility code much like Option 5 (1 to 5 Keys + Facility Code, Wiegand 26-Bit) (see Section 5.4.5).

### 5.5.4 Wiegand 26-Bit and Facility Code

In this mode, 1 byte Facility code followed by 2 bytes of the card's serial number are transmitted in Wiegand 26-Bit format. Two parity bits are added. An even parity bit is sent first, followed by one facility code byte then followed by a two-byte CSN ending with an odd parity bit.

(EP) FFFF FFFF AAAA AAAA AAAA AAAA (OP)

Where:     EP = Even parity for first 12 bits  
             OP = Odd parity for last 12 bits  
             F = 1 byte Facility code  
             A = 2 bytes code generated from the CSN



The third and fourth bytes of the CSN is not transmitted.

### 5.5.5 Wiegand 32-Bit

In this mode, 4 bytes of the CSN are transmitted in Wiegand 32-bit format. No parity bits are added.

AAAA AAAA BBBB BBBB CCCC CCCC DDDD DDDD

Where:     A = 4<sup>th</sup> (MSB) byte of the CSN  
             B = 3<sup>rd</sup> byte of the CSN  
             C = 2<sup>nd</sup> byte of the CSN  
             D = 1<sup>st</sup> (LSB) byte of the CSN

### 5.5.6 Wiegand 32-Bit Reversed

In this mode, 4 bytes of the CSN are transmitted in Wiegand 32-bit format. Bytes are sent in reversed order. LSB part of the CSN is sent first and MSB byte is sent last. No parity bits are added.

DDDD DDDD BBBB BBBB CCCC CCCC AAAA AAAA



Where:        D = 1<sup>st</sup> (LSB) byte of the CSN  
                  C = 2<sup>nd</sup> byte of the CSN  
                  B = 3<sup>rd</sup> byte of the CSN  
                  A = 4<sup>th</sup> (MSB) byte of the CSN

### 5.5.7     Wiegand 34-Bit

In this mode, 4 bytes of the CSN are transmitted in Wiegand 34-bit format. Bytes are sent in reversed order. LSB part of the CSN is sent first and MSB byte is sent last. An even parity is sent first, followed by 32 bits data followed by odd parity bit.

(EP) AAAA AAAA BBBB BBBB CCCC CCCC DDDD DDDD (OP)

Where:        EP = Even parity for first 16 data bits  
                  OP = Odd parity for last 16 data bits  
                  A = 4<sup>th</sup> (MSB) byte of the CSN  
                  B = 3<sup>rd</sup> byte of the CSN  
                  C = 2<sup>nd</sup> byte of the CSN  
                  D = 1<sup>st</sup> (LSB) byte of the CSN

### 5.5.8     Wiegand 40-Bit and Checksum

In this mode, 4 bytes of the CSN are transmitted in Wiegand 40-Bit format. Bytes are sent in reversed order. LSB part of the CSN is sent first. Last byte sent is Checksum byte generated by adding 4 data bytes and discarding remainder beyond 8 bytes.

AAAA AAAA BBBB BBBB CCCC CCCC DDDD DDDD (CSUM)

Where:        A = 4<sup>th</sup> (MSB) byte of the CSN  
                  B = 3<sup>rd</sup> byte of the CSN  
                  C = 2<sup>nd</sup> byte of the CSN  
                  D = 1<sup>st</sup> (LSB) byte of the CSN  
                  CSUM = Checksum value, 1 byte (A+B+C+D)

### 5.6 Changing the Programming Code

*To change the Programming code:*

1. Enter Programming mode.



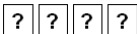
2. Press **3** to enter Menu 3.



The LED flashes green.



3. Enter the new code you wish to set as the Programming code.



You hear three beeps.



The system returns to Standby mode.



Note

- The Default Programming code is 1234.
- The Programming code cannot be erased, meaning the code 0000 is not valid and does not erase the Programming code

### 5.7 Changing the Facility Code

*To change the Facility code:*

1. Enter Programming mode.



2. Press **4** to enter Menu 4.



The LED flashes green.



3. Enter the new 3-digit code you wish to set as the Facility code.



You hear three beeps.



The system returns to Standby mode.



Note

- The default Facility code is 001.
- Facility codes can be in the range between 000 and 255.

### 5.8 Return to Factory Default Settings



You must be very careful before using this command! Doing so erases the entire memory that includes all user and special codes, and returns all codes to their factory default settings.

#### *To return to factory default settings:*

1. Enter Programming mode.



2. Press **0** to enter Menu 0.



The LED flashes green.



3. Enter your Programming code.

If the Programming code is valid, all memory is erased. You hear three beeps and the controller returns to Transmit mode.

If the Programming code is invalid you hear a long beep and the controller returns to Transmit mode without erasing the memory of the controller.

### 5.9 Replacing a lost Programming Code

In the event that the Programming code is forgotten, the unit may be reprogrammed in the field using the following instructions:

1. Remove power from the reader.
2. Activate tamper by removing the reader from the wall or removing the reader's case.
3. Apply power to the reader.
4. You now have 10 seconds to enter Programming mode using the factory default Programming code 1234.

### A. Limited Warranty

The full ROSSLARE Limited Warranty Statement is available in the Quick Links section on the ROSSLARE website at [www.rosslaresecurity.com](http://www.rosslaresecurity.com).

Rosslare considers any use of this product as agreement to the Warranty Terms even if you do not review them.



AY-T6350

## Asia Pacific, Middle East, Africa

Rosslare Enterprises Ltd.

Kowloon Bay, Hong Kong

Tel: +852-2795-5630

Fax: +852-2795-1508

support.apac@rosslaresecurity.com

## United States and Canada

Rosslare Security Products, Inc.

Southlake, TX, USA

Toll Free: +1-866-632-1101

Local: +1-817-305-0006

Fax: +1-817-305-0069

support.na@rosslaresecurity.com

## Europe

Rosslare Israel Ltd.

22 Ha'Melacha St., P.O.B. 11407

Rosh HaAyin, Israel

Tel: +972-3-938-6838

Fax: +972-3-938-6830

support.eu@rosslaresecurity.com

## Latin America

Rosslare Latin America

Buenos Aires, Argentina

support.la@rosslaresecurity.com

## China

Rosslare Electronics (Shenzhen) Ltd.

Shenzhen, China

Tel: +86-755-8610 6842

Fax: +86-755-8610 6101

support.cn@rosslaresecurity.com

## India

Rosslare Electronics India Pvt Ltd.

Tel/Fax: +91-20-40147830

Mobile: +91-9975768824

sales.in@rosslaresecurity.com

**ROSSLARE**  
SECURITY PRODUCTS



• EN ISO 13485



0706-0960659+01