

***Star* FINGER006/EX**
***iPASS* IP-FINGER006**
***IDTECK* FINGER006SR**

Fingerprint Identification
Proximity / PIN Reader



Table of Contents

1. Important Safety Instructions	5
2. General	6
3. Features	6
4. Specifications	7
5. Identifying Supplied Parts	9
6. Product Overview	9
6.1. Functions	9
6.2 Product Explanation	10
6.2.1 Panel Description	10
6.2.2. Color Coded & Wiring Table	11
6.3 Option	12
6.3.1 TCP/IP Module	12
7. Installation Tips & Check Point.....	13
7.1 Check Points before Installation.....	13
7.1.1 Selection of Cable	13
7.1.2 Recommended Cable Type and Permissible Length of Cable	14
7.2 Check Point during Installation	15
7.2.1 Termination Resistor	15
7.2.2 How to Connect Termination Resistors	15
7.2.3 Grounding System for Communication Cable	16
8. Installation of the Product	17
8.1 Template	17
8.2 System Initialization	18
8.3 Wiring	19
8.3.1 Power	19
8.3.2 Output Connections	19
9. Communication	19
9.1 RS232 Communication Port Connection	19
9.2 RS422 Communication Port Connection	20
9.2.1 RS422 Connection (Single FINGER006 Connection)	20
9.2.2 RS422 Connection (Multiple FINGER006 Connections)	20
9.3 TCP/IP Converter (External Version).....	21
10. Basic Setting	22
10.1 Initialization of FINGER006	22
10.2 How to Enter the Setup Menu	22

10.3 Time / Date Setting	23
10.4 Maximum Number of Cardholder IDs	23
10.5 Registering Cardholder IDs	23
11. Operation	24
11.1 Normal Operation	24
11.2 Default Setting	24
12. Setting Changes	25
12.1.1. TIME SETTING	27
12.1.2. COMMUNICATION ADDRESS	27
12.1.3. BAUD RATE	27
12.1.4. READER 1 MODE	28
12.1.5. READER 2 MODE	28
12.1.6. MASTER ID REGISTRATION	29
12.1.7. SYSTEM INITIALIZATION	29
12.1.8. CARD ID CLEAR	30
12.1.9. EVENT CLEAR	30
12.2 SETUP MENU F2	31
12.2.1 LCD DISPLAY	32
12.2.2 BUZZER STATUS	32
12.2.3 OUTPUT MODE	32
12.2.4 LED_BUZZER_CONTROL	32
12.2.5 RF PIN INPUT	33
12.2.6 KEY OUTPUT MODE	33
12.2.7 OUTPUT TYPE	33
12.2.8. STAND ALONE	33
12.2.9 DATA BYTE (FINGER006SR ONLY)	34
12.3 SETUP MENU F3	35
12.3.1 ID REGISTRATION	35
12.3.2 ID DELETE	36
12.3.3 ID LIST	37
12.3.4 REGISTERED ID COUNT	37
12.3.5 ID MEMORY	37
12.4 SETUP MENU F4	38
12.4.1 FIRMWARE VERSION	40
12.4.2 MEMORY TEST	40
12.4.3 OUTPUT TEST	40
12.4.4 LCD TEST	41
12.4.5 KEYPAD TEST	41

12.4.6 READER TEST	42
12.4.7 INPUT / DIP SWITCH TEST	42
12.4.8 COMMUNICATION TEST	43
12.4.9 IDENTIFICATION MODE	43
12.4.10 DUAL FINGERPRINT MODE	43
12.4.11 ADAPTIVE MODE	44
12.4.12 FP STATUS	44
12.4.13 HIGH SECURITY	44
12.4.14 FP QUALITY	45
12.4.15 FP LEVEL	45
12.4.16 FINGERPRINT MODULE VERSION	45
12.4.17 FINGERPRINT COUNT	45
12.4.18 FINGERPRINT MODULE TEST	46
12.4.19 FINGERPRINT DEVICE INFORMATION CHECK	46
13. Appendix	46
13.1 Default Values for Parameters	46
14. FCC Registration Information	47
15. Warranty Policy and Limitation Liability	48
16. Template	49

1. Important Safety Instructions

When using **Fingerprint Identification (Proximity / PIN) Reader**, basic safety precautions should always be followed to reduce the risk of fire, electrical shock, and injury to persons.

In addition, the following safety guides should also be followed:

1. **Fully** read and understand all instructions and follow them completely.
2. **Follow** all warnings and instructions marked on the product.
3. **Do not** use liquid or aerosol cleaners. Use a damp cloth for cleaning. If necessary, use mild soap.
4. **Do not** use this product near water.
5. **Only** operate this product using the type of power source indicated. If you are not sure of the type of power supplied to your installation site, consult your dealer or local power company.
6. **Never** insert objects of any kind into the product or through the cabinet slots as they may touch voltage points and/or short circuit parts possibly resulting in fire or electric shock.

Never spill liquid of any kind on the product.

7. **Never** disassemble this product by yourself; take the unit to a qualified service center whenever service or repair is required. Opening or removing the covers may expose you to dangerous voltages or other risks. Also, incorrect reassembly can cause electric shock when the unit is subsequently used.

8. **Unplug** this product from the Direct Current (DC) power source and refer to qualified service personnel under these conditions:

- a. When the power supply cord or plug is damaged or frayed.
- b. If liquid has been spilled on the product.
- c. If the product does not operate normally after following the operating instructions in this manual.

Adjust only those controls that are covered by the operating instructions in this manual. Improper adjustment of other controls that are not covered by this manual may damage the unit and will often require extensive work by a qualified technician to restore normal operation.

- d. If the product exhibits a distinct change in performance.

2. General

The **Star FINGER006 / iPASS IP-FINGER006 / IDTECK FINGER006SR** is such a highly advanced and intelligent fingerprint reader (with a keypad) with a powerful 32bit and dual 8bit microprocessor to meet the market requirement for a robust integrated solution for access control and time & attendance.

The unit has been designed to be flexible and reliable in providing the ultimate biometrics high security at a reasonable cost.

This user-friendly device allows you to register up to 4,000 fingerprint IDs (optional 1,000/2,000) and 50,000 cards and add / delete user IDs (Cards) conveniently.

With the built-in 4" RF reader, the keypad for Personal Identification Numbers (PIN), and a sophisticated biometric fingerprint module, the **FINGER006** offers up to three levels of ID verification.

Any combination of Proximity, PIN, and Biometric may be used and different verification levels can be customer programmed for each user or user group.

3. Features

- 125KHz Proximity / PIN and Fingerprint Recognition
- 1,000 / 2,000 / 4,000 Fingerprint Users
- 1:1 Verification and 1: N Identification
- 2 Fingerprint Storage Templates
- Identification Method:
 - by PIN Key (default)
 - by Auto Touch Sensor
- ID Only Function for Persons with Unregisterable Fingerprints
- Network Communication via RS232 / RS422 (Max.32ch)
TCP/IP (Internal LAN Converter Required)
- 1 ea of External Reader Port: 26bit Wiegand, 4 / 8bit Burst
- 26bit Wiegand and ABA Track II Output Format
- High Protection from Scratch and ESD (Electro Static Discharge)
- High Quality Optical Sensor
- Dual Tamper Switches
- Options:
 - TCP/IP Communication (FINGER006T, FINGER006PT, IP- FINGER006T)
 - Supervisory Signal
- Compatible Software: STARWATCH DUAL PRO I / II, STARWATCH iTDC PRO I / II, STARWATCH STANDARD
- Compatible Controller: iCON100, iTDC, Third Party Controller, Standalone Controller

* Comparison Table

FINGER006	Built-in 125KHz (4") Proximity Reader
	RF(PIN) Only / Fingerprint Only / RF(PIN)+ Fingerprint RF(PIN)+P/W(4digit) / RF(PIN)+P/W+ Fingerprint
FINGER006P	PIN(4~8digit) Only / Fingerprint Only / PIN + Fingerprint PIN + P/W(4digit) / PIN+ P/W+ Fingerprint
FINGER006A	Auto Touch Sensor for Identification
FINGER006PA	Auto Touch Sensor for Identification

4. Specifications

Model			FINGER006	FINGER006P
CPU			32bit ARM9 and Dual 8bit Microprocessor	
Memory	Fingerprin t Module	Program Memory	Program Flash memory 1Mbytes	
		Data Memory	DB Flash memory 1/2/4 Mbytes	
	Controller	Program Memory	128K Byte Flash Memory	
		Data Memory	1M Byte Flash Memory	
Fingerprint User			1,000 / 2,000 / 4,000 Fingerprint Users	
Fingerprint Template Size			800 Bytes for 2 Fingerprint Templates	
Read Range		Passive Type	IDK50 / IMC125: Up to 2 inch (5cm) IDC80 / IDC170: Up to 4 inch (10cm)	PIN Only
		Active Type	IDA150 / IDA200 Comapatile	
Reading Time (Card)			30ms	
Verification / Identification Time			Less than 1sec. / Less than 2sec.	
Power / Current			DC 12V / Max.300mA	
External Reader Port			1ea(26bit Wiegand, 4/8bit Burst for PIN)	
Communication			RS232 / RS422 (Max.32ch)	
			TCP/IP (Internal LAN Converter Required)	
Baud Rate			9,600bps (Recommended) / 4,800bps, 19,200bps 38,400bps, 57,600bps and 115200bps (Selectable)	
Input Port			2ea (Error-Input, OK-Input)	
Output Port			2ea (Error-Output , OK-Output (Open Collector Output))	
Output Format			26bit Wiegand, ABA Track II	
LCD			Character LCD (2 Lines x 16 Char) / 65.6mm x 13.8mm (2.62" x 0.55") Screen	



Keypad		16 Key Numeric Keypad with Back Lighting
LED Indicator		7 Array LED Indicators (Red, Green and Yellow)
Beeper		Piezo Buzzer
Operating Temperature	Fingerprint Module	-20° to +60°C (-4° to +140°F)
	LCD	0° to +50°C (+32° to +122°F)
	Controller	-15° to +70°C (+5° to +158°F)
	RF Reader	-35° to + 65°C (-31° to +149°F)
Operating Humidity		10% to 90% Relative Humidity Non-Condensing
Color / Material		Dark Pearl Gray / Polycarbonate
Dimension (W x H x T)		161.5mm x 134mm x 48.5mm (6.36" x 5.28" x 1.9")
Weight		547g (1.21lbs)
Certification		MIC

*** Fingerprint Module Specification**

Resolution	500Dpi
Capture Image Size	412 X 302 pixels
Extraction Image Size	260 X 300 pixels
Sensing Area	13mm X 15.2mm
Scanner	High Quality Optical Sensor
FAR(False Acceptance Ratio)	0.001%
FRR(False Reject Ratio)	0.1%
ESD(Electro Static Discharge)	15KV
Verification Time	Less than 1sec.
Identification Time	Less than 2 sec.

5. Identifying Supplied Parts

Please unpack and check the contents of the box.



Main unit

(1 Unit)



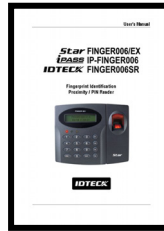
Wall mount

(1 PC)



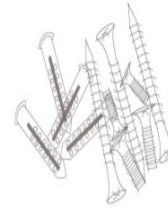
O-ring

(5 PCS)



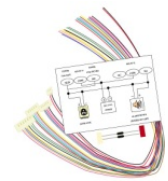
User's manual

(1 Copy)



Screws

(4 PCS)



Cable & Diode

Cable(5 ea)

Diode(2 ea)

6. Product Overview

6.1. Functions

Operation with the Host Computer

ID data transactions can be managed via the host computer. The data transmitted from the controller can be displayed and stored on the host PC.

Data Backup

The controller retains all user information and event data, even in the case of power failure.

Keypad Registration

The built-in keypad and the LCD screen let you perform manual programming without a PC connected.

Dual Finger Mode

Dual Finger Mode is a function that lets a user register two fingers for one ID so that the user can receive authentication with either of the two registered fingers. This is useful when a user's finger is injured.

1:N Identification

A user can gain authentication using the fingerprint alone without RF card or PIN. You can set this function through the <TYPE SELECTION> in SETUP MENU F1. In the IDENTIFICATION MODE, the security level is automatically increased and it causes FRR(False Rejection Ratio) to get higher, which may result in reduction of successful

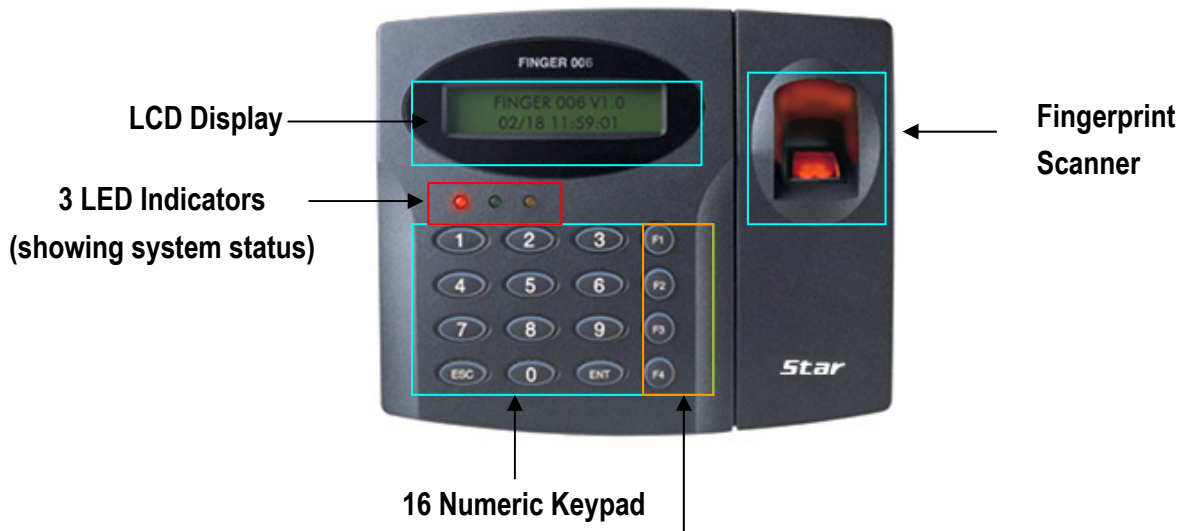
recognition rate. When using this mode, the user has to press the <ENT> key first, and then the fingerprint scanner waits for a fingerprint to be scanned. When the fingerprint-scan is completed, **FINGER006** identifies the user and makes corresponding outputs.

FINGER006 has a sensor. Normally, a user needs to press <ENT> in the identification mode before placing their finger on the sensor. However, if a sensor is installed, **FINGER006** detects the user's finger and scans it automatically.

6.2 Product Explanation

6.2.1 Panel Description

Front View



LCD Display

LCD displays **FINGER006**'s status.

3 LED Indicators (showing system status)

The red LED turns on with power supply.

The green LED turns on with Relay #1 operation.

The yellow LED turns on with Relay #2 operation.

Finger Print Scanner

When users put their finger on the scanner, red light will turn on.

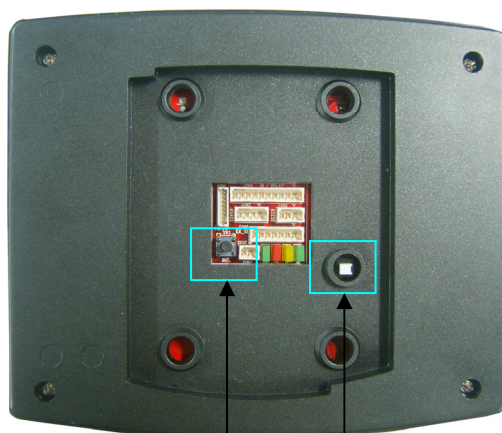
16 Numeric Keypad

Card data registration, deletion and various function settings are possible through keypad input without host computer control.

Function Keypad

There are four function keys: F1, F2, F3 and F4

Rear View



Initialization Switch

Temper Switch

Communication Display LED

3, 4(yellow, green) LED will twinkle during RS232, RS422 and TCP/IP communication.
 If the LAN is connected normally during TCP/IP communication, green LED will turn on.
 But in the collision status, #2 LED (red) will turn on.

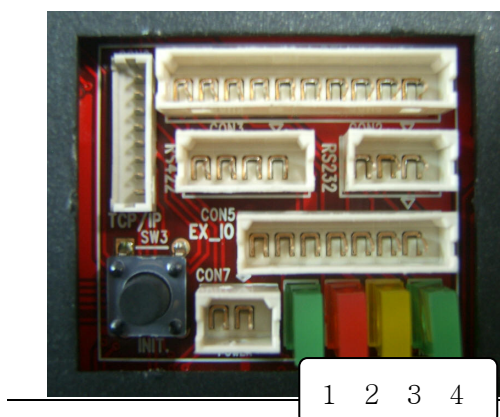


Figure: The Communication Display LED in the Rear View

6.2.2. Color Coded & Wiring Table

I/O PORT NAME	SIGNAL NAME	COLOR CODED
POWER	(CON7)	
Main Power(+12V)	DC +12V	Red
Power Ground	GND	Black
OUTPUT	(CON4)	
Door Relay(COM)	COM(1)	Gray with Red Stripe
Door Relay(NC)	NC(1)	Blue with White Stripe

Door Relay(NO)	NO(1)	White with Red Stripe
Alarm Relay(COM)	COM(2)	White
Alarm Relay(NC)	NC(2)	Purple with White Stripe
Alarm Relay(NO)	NO(2)	Purple
INPUT	(CON4)	
Exit Button	EXIT	Orange
Door Sensor	CONTACT	Yellow with Red Stripe
Aux Input 1	IN1(OK input-Reader Mode)	Green
Aux Input 2	IN2(Error input-Reader Mode)	Green with White Stripe
EXTERNAL READER PORT	(CON5)	
Wiegand Data0	DATA0	Pink
Wiegand Data1	DATA1	Cyan
OUTPUT	(CON5)	
TTL Output1	TTL1/D0	Orange with White
TTL Output2	TTL2/D1	Brown with White Stripe
OK Signal Out	OK Out (Not Use)	Green with Red Stripe
Error Signal Out	Error Out (Not Use)	Blue with Red Stripe
Tamper Switch Out	Tamper Switch Out (Not Use)	Yellow with White Stripe
RS232 INTERFACE	(CON2)	
RS232-TX	TXD	Black with White Stripe
RS232-RX	RXD	Red with White Stripe
Ground	GND	Black
RS422 INTERFACE	(CON3)	
RS422-TX(-)	TX(-)	Yellow
RS422-TX(+)	TX(+)	Gray
RS422-RX(-)	RX(-)	Blue
RS422-RX(+)	RX(+)	Brown
TCP/IP Communication	(CON6)	
	TCP/IP Communication	8PIN connector module

6.3 Option

6.3.1 TCP/IP Module

The **Finger006** is able to use TCP/IP Communication. An optional TCP/IP module is needed for TCP/IP communication to the PC.

7. Installation Tips & Check Point

Installing the **Star FINGER006/P / iPASS IP-FINGER006 / IDTECK FINGER006SR** is an easy task. It can be installed with common hand tools and readily available communications wires.

This section provides information about wiring, wire runs and other information to make the installation quick and easy.

7.1 Check Points before Installation

7.1.1 Selection of Cable

System installation cabling will be configured as follow:.

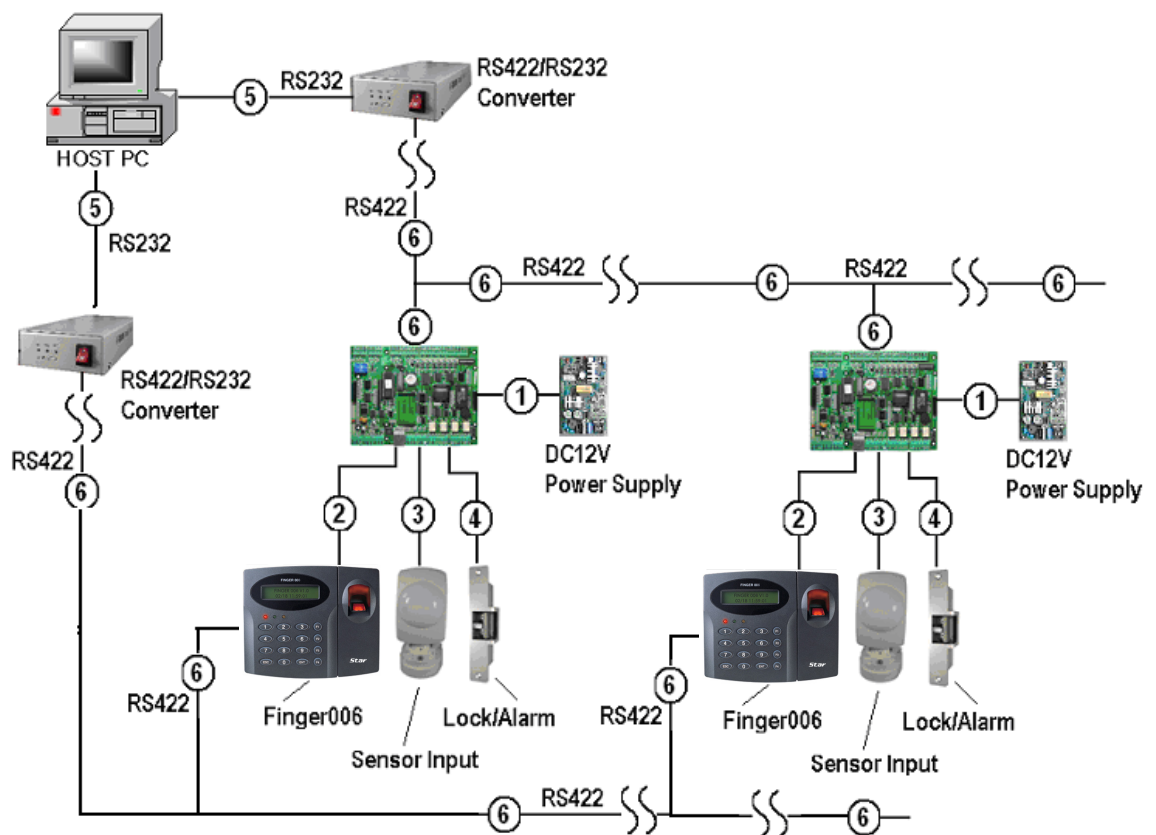


Figure: System Installation Layout

7.1.2 Recommended Cable Type and Permissible Length of Cable

Reference	Description	Cable Specification	Maximum Distance
①	Controller Power (DC12V) DC Power ➡ Controller	Belden #9409, 18 AWG 2 conductor, unshielded	30m
②	Reader (Power and Data) FINGER006 ➡ Controller	Belden #9512, 22 AWG 4 conductor, shielded	150m
		Belden #9514, 22 AWG 8 conductor, shielded	
③	Door Contact Exit Button Sensor Input Input ➡ Controller	Belden #9512, 22 AWG 4 conductor, shielded	300m
		Belden #9514, 22 AWG 8 conductor, shielded	
④	Door Lock, Alarm Device Lock (Alarm) ➡ Controller	Belden #9409, 18AWG 2 conductor, unshielded	300m
⑤	RS232 Cable	Belden #9829, 24 AWG 2-twisted pair, shielded	15m
	Converter ➡ Host P.C.		
⑥	RS485 Cable	Belden #9829, 24 AWG 2-twisted pair, shielded	1,200m
	Controller ➡ Converter		
	Controller ➡ Controller		
	Controller ➡ FINGER006		
	FINGER006 ➡ FINGER006		
	FINGER006 ➡ Converter		
	RS422 Cable	Belden #9830, 24 AWG 3-twisted pair, shielded	
	Controller ➡ Converter		
Controller ➡ Controller			
	Controller ➡ FINGER006		
	FINGER006 ➡ FINGER006		
	FINGER006 ➡ Converter		

* Thicker wires are necessary if the connected reader consumes a higher current.

7.2 Check Point during Installation

7.2.1 Termination Resistor

Termination resistors are used to match impedance of the network to the impedance of the transmission line being used. When impedance is mismatched, the transmitted signal is not completely absorbed by the receiver and a portion of signal is reflected back into the transmission line.

The decision whether or not to use termination resistors should be based on the cable length and data rate used by the communication system.

For example, if you use 9,600 baud rate and 1,200m length of cable, the propagation velocity of cable is 0.66 x speed of light (This value is specified by the cable manufacturer), if we assume the reflections will damp out in three round trip up and down the cable length, the transmitted signal will stabilize 18.6us after the leading edge of a bit. Since the data bit is captured in the middle of the bit which is approximately 52us after the leading edge of a bit. The reflection stabilizing time 18.6us is much before the center of the bit therefore the termination resistors are not required.

However, if you install the cable to maximum length, the impedance of cable and network is mismatched and the transmitted signal is overlapped by the reflected signal. In this case, it is recommended to add termination resistors to the end of the receiver lines. A 120Ω resistor can be used for termination resistor in parallel between the receiver lines “A” and “B” for 2 wires RS485 system or “RX+” and “RX-” for 4 wires RS422 system. A termination resistor of less than 90Ω should not be used and no more than 2 terminations should be used in one networking system.

7.2.2 How to Connect Termination Resistors

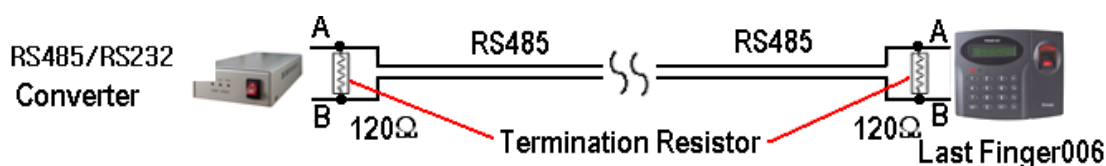


Figure: Termination Resistors for 2-Wire RS485 Communication System

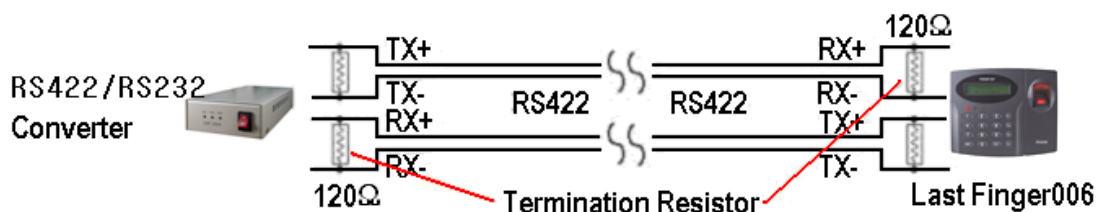


Figure: Termination Resistors for 4-Wire RS422 Communication System

7.2.3 Grounding System for Communication Cable

We recommend using proper grounding system on the communication cable. The best method for grounding system is to put the shield wire of the communication cable to the 1st class earth grounding; however it is not so easy to bring the earth ground to the communication cable and also the installation cost is raised.

There will be three grounding points where you can find during installation;

- 1) Earth Ground
- 2) Chassis Ground
- 3) Power Ground

The most important point for grounding system is not to connect both ends of shield wires to the grounding system; in this case there will be a current flow through the shield wire when the voltage level of both ends of shield wire is not equal and this current flow will create noise and interfere to communications.

For the good grounding, we recommend to connecting ONLY one end of shield wire of communication cable to the grounding system; If you find earth ground nearby, then connect one end of shield wire to earth ground; If you do not have earth ground nearby, then find chassis ground and connect one end of shield wire to chassis ground; If you do not find both earth ground and chassis ground, then connect one end of shield wire to power ground. (GND of FINGER006)

Note that if the chassis ground is not properly connected to the earth and floated from the ground level, then grounding to the chassis ground will give the worst communication; in this case we recommend to using power ground instead of chassis ground.

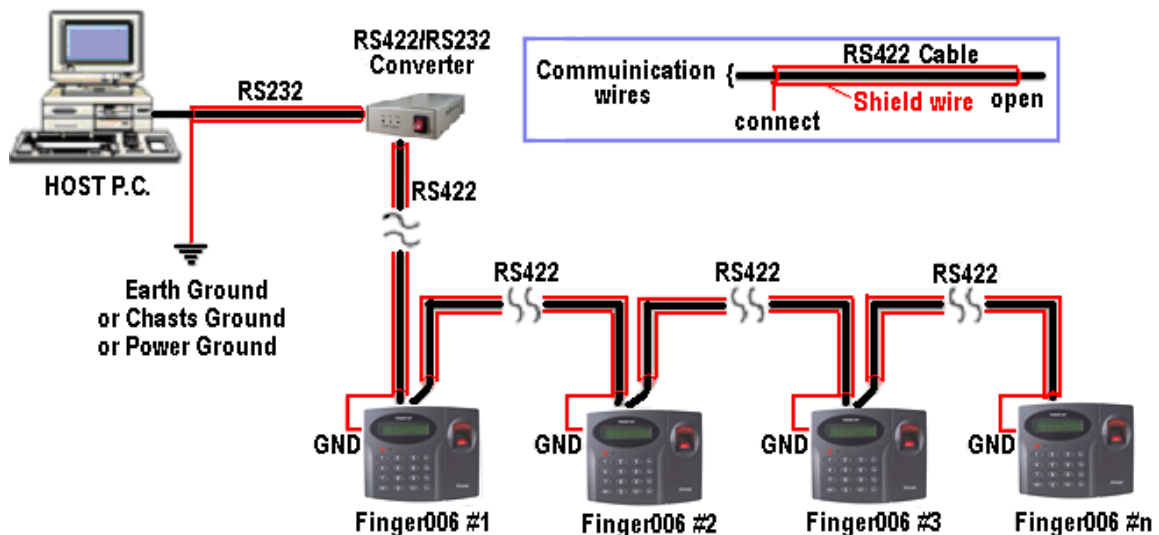


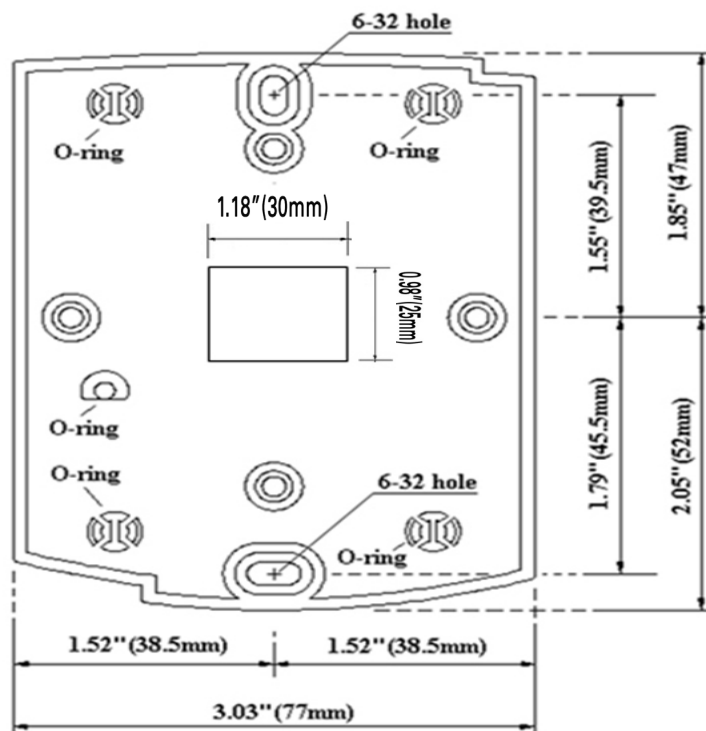
Figure: Grounding System

8. Installation of the Product

8.1 Template

- Tear off the Template page (51p) at the back of this manual and use the Template to drill two 6-32 holes and one 1/2" hole on the proper location of the wall to mount the Wall Mount bracket as shown below.

(If the gang box is installed on the wall, skip this step.)



- Using 2 screws, install wall mount to the wall.

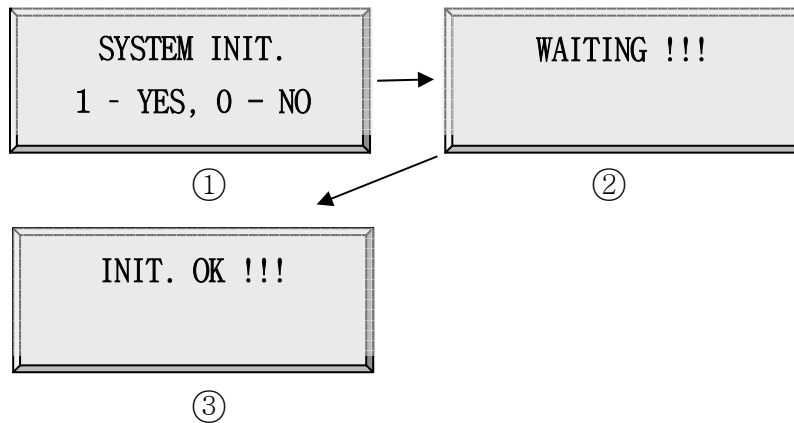
※Caution Before mounting the **Star FINGER006/P / iPASS IP-FINGER006 / IDTECK FINGER006SR** unit to the Wall Mount bracket, an operational test of the unit should be completed, because the locking pins will lock the unit to the Wall Mount. Removing the unit from the Wall Mount bracket after it has been snapped in place may cause damage to the bracket and prevent reattachment.

- Insert 5 O-Rings to the Wall Mount as indicated, then run the cable from the main unit through the center hole and snap in place the main unit to Wall Mount. Make sure that the main unit is secure locked in place with Wall Mount.

8.2 System Initialization

You have to initialize the **FINGER006** unit prior to installation.

Once power is supplied to the **FINGER006**, press the initialization switch in the back of the **FINGER006** unit. If you want hardware initialization, press key <1> otherwise press key <0>.



- ① Press the key <1> if you wish to initialize the **FINGER006**.
- ② Initialization is progressing
- ③ Rebooted automatically after Initialization

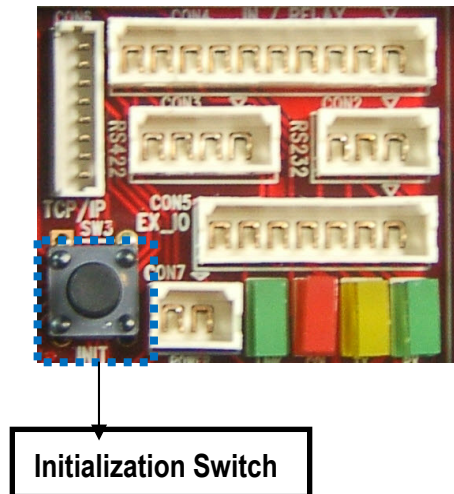


Figure: The Position of Initialization Switch

8.3 Wiring

8.3.1 Power

- Connect the (+) wire of DC 12V power to the +12V port (Red).
- Connect the GND (-) wire of DC 12V power to the GND port (Black).

8.3.2 Output Connections

Wiegand Data Connection

- Connect Data 0 wire of the controller to Wiegand Data 0 Out wire (Orange with White Stripe).
- Connect Data 1 wire of the controller to Wiegand Data 1 Out Wire (Brown with White Stripe).
- If you disconnect the power from the controller, connect the GND port between controllers.

Control Signal Connection

- Connect Error input wire of the controller to Error Signal Out wire (Blue with Red Stripe).
- Connect Ok input wire of the controller to OK Signal Out wire (Green with Red Stripe).
- Connect Error output wire of the controller to Error Signal In wire (Green with White stripe).
- Connect Ok wire output of the controller to OK Signal In wire (Green).
- Connect Tamper input wire of the controller to Tamper Switch Out wire (Yellow with White stripe).

External Reader Connection

[Wiegand Input]

- Connect Data 0 wire of the external reader to Wiegand Data 0 In (EX) wire (Pink).
- Connect Data1 wire of the external reader to Wiegand Data 1 In (EX) wire (Cyan).
- If you disconnect the power from the external reader, connect the GND port between external readers.

9. Communication

9.1 RS232 Communication Port Connection

A 9-pin connector (Serial communication connector, female) is required to connect the **FINGER006** to a host computer via RS232 communication. Please follow the instructions.

- Connect RS232-TX port of **FINGER006** to the pin 2 of the 9-pin connector.
- Connect RS232-RX port of **FINGER006** to the pin 3 of the 9-pin connector.
- Connect RS232-GND of **FINGER006** to the pin 5 of the 9-pin connector.

Plug in the 9-pin connector to COM1 or COM2 Port of the host PC.

Install and run **FINGER006** Application Software.

9.2 RS422 Communication Port Connection

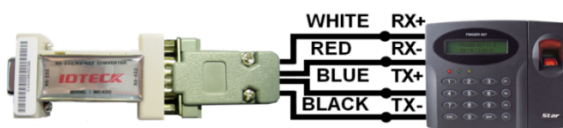
9.2.1 RS422 Connection (Single FINGER006 Connection)

RS422/RS232 converter (INC400) is required to use RS422 communication between the **FINGER006** and a host computer. Please follow the instructions.

- Connect RS422-TX(+) (Gray wire) of the **FINGER006** to RS422-RX(+) port of the converter.
- Connect RS422-TX(-) (Yellow wire) of the **FINGER006** to RS422-RX(-) port of the converter.
- Connect RS422-RX(+) (Brown wire) of the **FINGER006** to RS422-TX(+) port of the converter.
- Connect RS422-RX(-) (Blue wire) of the **FINGER006** to RS422-TX(-) port of the converter.
- Plug in the RS232 9pin connector of the converter to the COM1 or COM2 Port of the PC.
- Install and run the **FINGER006** Application Software.

< A Type >

INC400	Unit(RS422)
WHITE	RX+
RED	RX-
BLUE	TX+
BLACK	TX-



< B Type >

INC400	Unit(RS422)
485-/(T-)	RX+
485+/(T+)	RX-
R+	TX+
R-	TX-

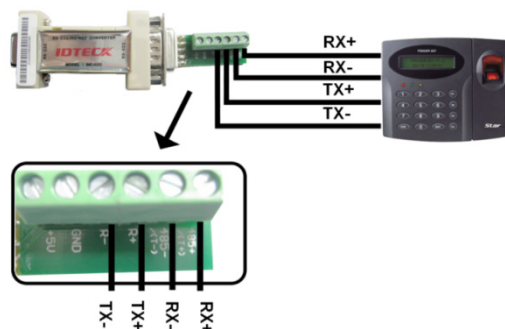


Figure: RS422 Communication between FINGER006 and the PC

9.2.2 RS422 Connection (Multiple FINGER006 Connections)

RS422/RS232 converter is required to use RS422 communication between multiple **FINGER006** units and a host PC. Please follow the next instructions.

First, you have to connect all RS422 port of all **FINGER006s** in parallel.

- Connect RS422-TX(+) of one **FINGER006** to RS422-TX(+) of another **FINGER006**.
- Connect RS422-TX(-) of one **FINGER006** to RS422-TX(-) of another **FINGER006**.
- Connect RS422-RX(+) of one **FINGER006** to RS422-RX(+) of another **FINGER006**.

- Connect RS422-RX(-) of one **FINGER006** to RS422-RX(-) of another **FINGER006**.

Second, you have to connect one of RS422 port of **FINGER006** to RS422/RS232 converter.

- Connect RS422-TX(+) of the one **FINGER006** to RX(+) port of the converter.
- Connect RS422-TX(-) of the one **FINGER006** to RX(-) port of the converter.
- Connect RS422-RX(+) of the one **FINGER006** to TX(+) port of the converter.
- Connect RS422-RX(-) of the one **FINGER006** to TX(-) port of the converter.
- Plug in the RS232 9pin connector of the converter to the COM1 or COM2 port of the PC.
- Install and run **FINGER006** Application Software.

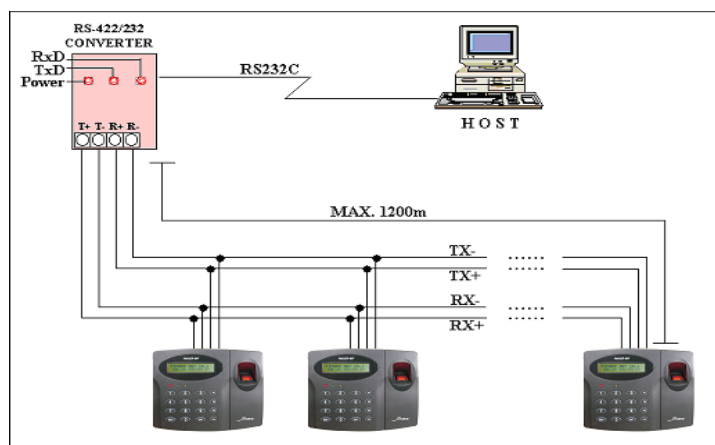


Figure: RS422 Communication between FINGER006s and the Host PC

9.3 TCP/IP Converter (External Version)

When you use the TCP/IP converter, choose only one converter between RS232 and RS422.

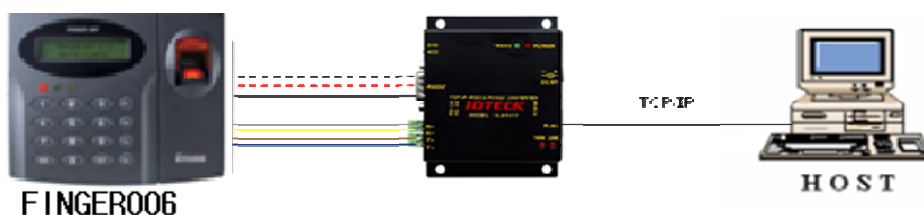


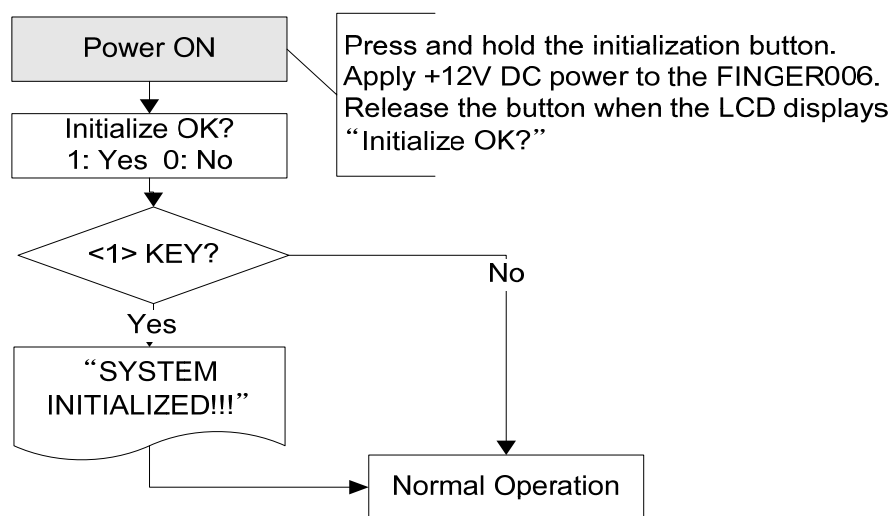
Figure: TCP/IP Converter between FINGER006s and the Host PC

INTERFACE	FINGER006	ILAN422	LINE COLOR
RS232	TX (CON2)	RX (RS232 DSUB9)	BLACK+WHITE
	RX (CON2)	TX (RS232 DSUB9)	RED + WHITE
	GND(CON2)	GND	BLACK
RS422	TX+ (CON3)	RX+ (RS422 CONNECTOR)	GRAY
	TX- (CON3)	RX- (RS422 CONNECTOR)	YELLOW
	RX+ (CON3)	TX+ (RS422 CONNECTOR)	BROWN
	RX- (CON3)	TX- (RS422 CONNECTOR)	BLUE

10. Basic Setting

10.1 Initialization of FINGER006

After installation and cable connections are completed, apply power (DC12V) to the **FINGER006** with the initialization button held down. (The initialization button can be found on the back of the **FINGER006**.) Then, the LCD will first display “**Initialize OK? 1: Yes 0: No**”. Press **<1>** key if you want to initialize the system or **<0>** to cancel the initialization procedure. After all the initialization process is completed, the system will be operating in the normal mode and the LCD will display “**FINGER006 [F1], MM/DD hh : mm : ss**”.



10.2 How to Enter the Setup Menu

For a setup or **FINGER006** setting adjustment, you have to enter the **SETUP MENU**, first. To do so, press the **<0>** key 8 times for **Master ID** (Default “00000000”) and the user can get into the **SETUP MENU**. There are 4 main **SETUP MENU**s and you first get into [SETUP MENU F1]. You can move to other **SETUP MENU**s by pressing **<F1>** key for [SETUP MENU F1], **<F2>** key for [SETUP MENU F2], **<F3>** key for [SETUP MENU F3], and **<F4>** key for [SETUP MENU F4]. There are several **SUB MENU**s for each main **SETUP MENU** and you can scroll up and down the **SUB MENU** by pressing **<4>** and **<6>** key in the main **SETUP MENU**. You can press the **<ESC>** key to exit the **SETUP MENU** and return to the normal operation. You can also change the Master ID in the [SETUP MENU F1]. The Master ID for **FINGER006SR** is a 10-digit number (Default “0000000000”).

10.3 Time / Date Setting

After you enter the Setup Mode, you will see the following screen with the current date and time. To adjust the time / date setting, press **<ENT>**, then enter 15 Digits in a YYYYMMDDhhmmssW format, and then enter **<ENT>** again to confirm.



NOTE: For the days of the week (W), 1 : Sun, 2 : Mon, 3 : Tue, 4 : Wed, 5 : Thu, 6 : Fri, 7 : Sat.
 e.g. To input August 24, 2009, 13:30:15, Monday, enter 200908241330152.

10.4 Maximum Number of Cardholder IDs

By default, the **FINGER006** is set to store up to 10,000 cardholders and 50,000 events and User can't change Maximum Number of Cardholder IDs because FINGER006 doesn't have the controller inside.

10.5 Registering Cardholder IDs

To add new cardholder IDs to the **FINGER006**, enter the Setup Mode (See 10.2 How to Enter Setup Mode), press **<F3>**. Once the 1.ID registration item appears on the LCD, press **<ENT>** to begin the ID registration process.

For detailed information on the ID registration process, please refer to "12.3.1 registration".

NOTE: How to place your finger onto the scanner:

When you register or verify your fingerprint, please place your finger onto the scanner correctly as illustrated below.

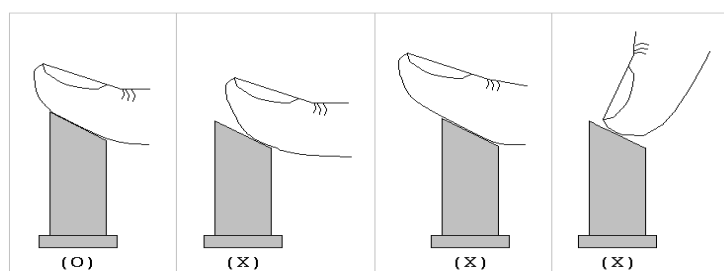


Figure: How to Put Your Finger on the Scanner

11. Operation

11.1 Normal Operation

Power On

When the power is applied to **FINGER006**, the “RED LED” is turned on.

Fingerprint Identification

1. If registered card is read by the unit, red LED of fingerprint sensor is on.
At this time, you should put your finger and then remove your finger if red LED is off.
2. If fingerprint identification is done, card ID or authorization status appears on the LCD.

Registered Card Reading

When a registered card (or PIN) is read, the door (Relay1) will open for 3 seconds (Defaults) with the “GREEN LED” on.

Exit Button

To make a request for exiting from inside, an Exit Button (Or External Reader) can be used.
The Door (Relay1) will open for 3 seconds (Defaults) with the on.

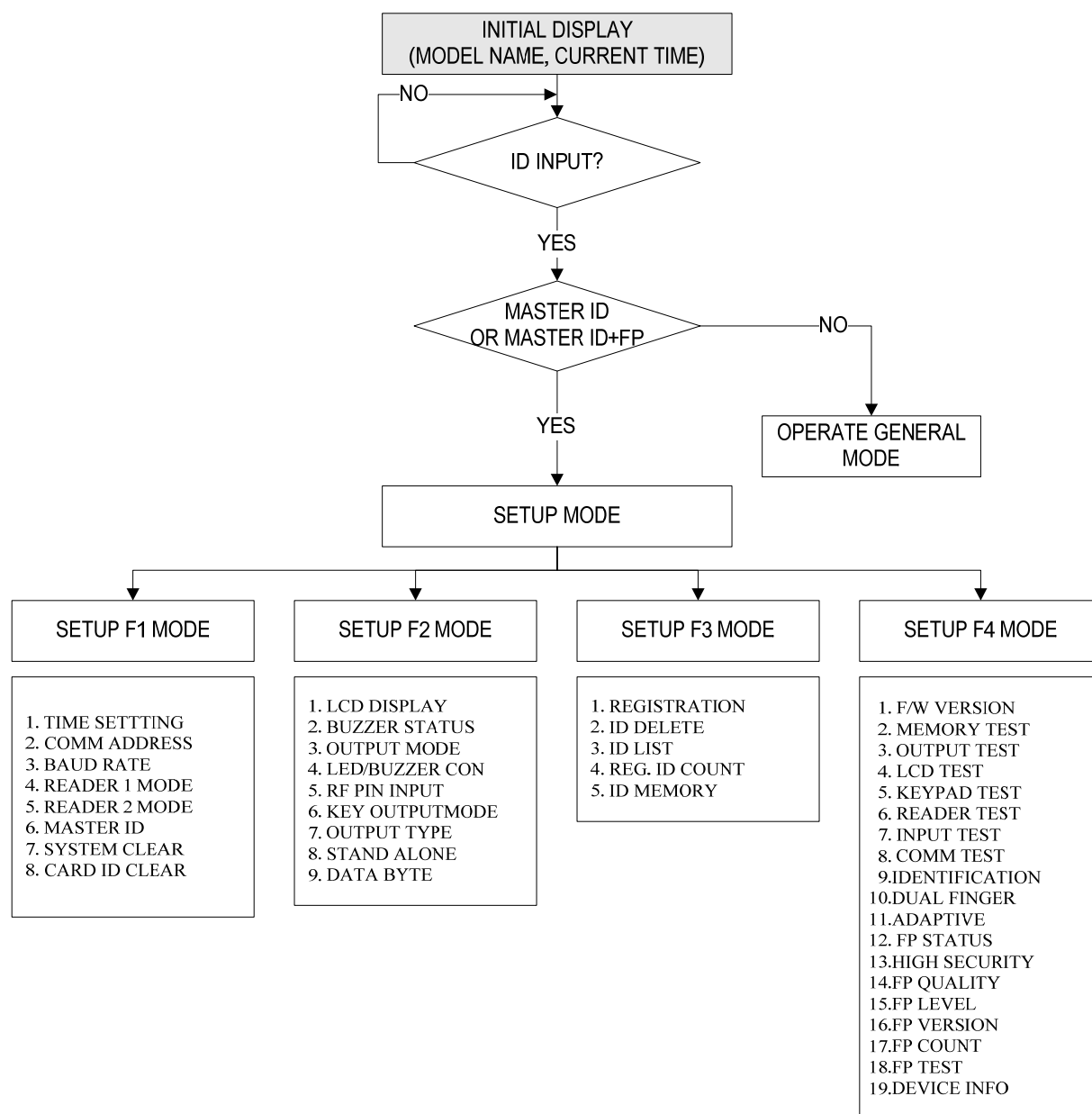
Alarms (Unregistered / Password / Fingerprint)

When an unregistered card is read, wrong password is input, wrong fingerprint is input, the access is denied and the alarm (Relay 2) will be activated for 3 seconds (Defaults) with “RED LED” on.

11.2 Default Setting

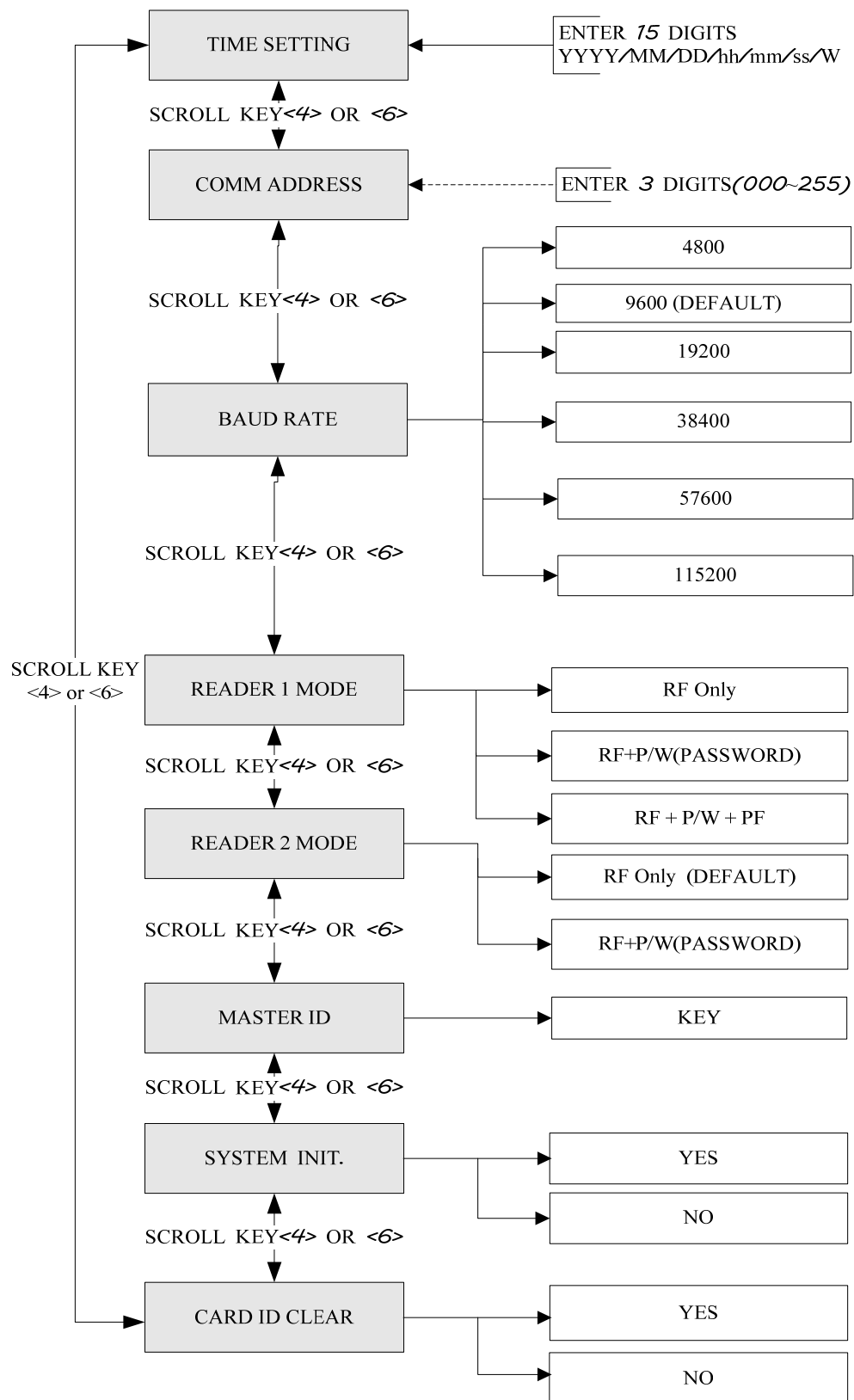
When you operate the **FINGER006** first time or you initialize the **FINGER006**, the **FINGER006** will set up all values to default settings (Factory Settings). You can change the settings for desired application. Please refer to the “APPENDIX” section at the back of this manual for the default setting values.

12. Setting Changes



☞ For a setup or **FINGER006** setting adjustment, you have to enter the SETUP MENU, first. To do so, press the <0> key 8 times for Master ID (Default “00000000”) and the user can get into the SETUP MENU. There are 4 main SETUP MENUs and you first get into **[SETUP MENU F1]**. You can move to other SETUP MENUs by pressing <F1> key for **[SETUP MENU F1]**, <F2> key for **[SETUP MENU F2]**, <F3> key for **[SETUP MENU F3]**, and <F4> key for **[SETUP MENU F4]**. There are several SUB MENUs for each main **SETUP MENU** and you can scroll up and down the SUB MENU by pressing <4> and <6> key in the main **SETUP MENU**. You can press the <ESC> key to exit the **SETUP MENU** and return to the normal operation. You can also change the Master ID in the **[SETUP MENU F1]**. The Master ID for **FINGER006SR** is a 10-digit number. (Default “0000000000”)

12.1 SETUP MENU F1



12.1.1. TIME SETTING

1. TIME SETTING

MM/DD hh:mm:ss

YYYYMMDDhhmmssW

The LCD displays the current time. To change the time, press **<ENT>**, enter 15 Digits in a "YYYYMMDDhhmmssW" format, and then enter **<ENT>** again to confirm.

NOTE: For the days of the week (W),
 1 : Sun, 2 : Mon, 3 : Tue, 4 : Wed, 5 : Thu, 6 : Fri, 7 : Sat.
e.g. To input August 24, 2009, 13:30:15, Monday,
enter 200908241330152.

12.1.2. COMMUNICATION ADDRESS

2. COMM ADDRESS

033

2. COMM ADDRESS

12

A communication address is a unique number assigned to each device for communication. The default address is 033.

For proper communication with the PC, it is important that the value you set here should match the value you set on the application software. It is also important to make sure each device on a loop has a unique address.

To change the communication address of the FINGER006, press **<ENT>**, enter the desired 3-Digit address in the 000-255 range, and then press **<ENT>** again to confirm.

12.1.3. BAUD RATE

3. BAUD RATE

9600

3. BAUD RATE

->9600

Baud Rate is the measurement of the serial communication speed.. As with the communication address, the baud rate you set here should match the value you set on the software.

Baud Rates of 4800bps, 9600bps, 19200bps, 38400bps, 57600bps and 115200bps are supported, and 9600bps is recommended.

To change the Baud Rate, press **<ENT>**, select the desired baud rate by pressing **<4>** or **<6>**, and then press **<ENT>** again to confirm.

NOTE: If a TCP/IP module is being used, the Baud Rate setting must be set the same as the TCP/IP module setting.

Troubleshooting Communication Problems

Step 1. Match the communication address between the device and the Application Software.

Step 2. Match the Baud Rate between the device and the Application Software.

Step 3. Ensure that the COM port setting in the Application Software is correct.

Step 4. Ensure that the communication settings in the Application Software are as follows;

1) Parity Bit: None 2) Data Bit: 8 Bits 3) Stop Bit: 1 Bit

12.1.4. READER 1 MODE

4. READER 1 MODE
RF + FP(PW)

4. READER 1 MODE
->RF + PW + FP

You can decide which combination of RF card, fingerprint and password verification you wish to use on Reader1 (the FINGER006 device itself).

To change the Access Mode for Reader 1, press <ENT>, select the "DESIRED MODE" by pressing <4> or <6>, and then press <ENT> again to confirm.

Access Modes for Reader 1

1. RF ONLY: Users can access the door by presenting their card or entering their ID number.

2. RF+F/P (P/W): Users can access the door by presenting their card or entering their ID number and then verifying their identity by a fingerprint. For users who did not register their fingerprints, password verification is used instead of fingerprint verification.

3. RF+P/W+F/P: Users can access the door by presenting their card or entering their ID number and then verifying their identity by both a fingerprint and a password.

12.1.5. READER 2 MODE

5. READER 2 MODE
RF ONLY

5. READER 2 MODE
->RF + PW

If you have an external reader connected to the FINGER006 (referred to herein as Reader2), you must adjust this setting according to what access mode is used on Reader 2.

To change the Access Mode for Reader2, press <ENT>, select the desired mode by pressing <4> or <6>, and then press <ENT> again to confirm.

Access Modes for Reader 2

1. RF ONLY: Select this option if Reader2 is operating without password verification

2. RF+ P/W: Select this option if Reader2 uses password verification.

NOTE: Proper selection of this setting depends solely on whether Reader2 uses password verification, but it has nothing to do with whether Reader2 uses fingerprint verification or not.

12.1.6. MASTER ID REGISTRATION

6. MASTER ID

ENTER ID NO.
-> 12345678

ID: 12345678
PW: FP:

TO REGISTER F/P
PUT YOUR FINGER!

REGISTRATION OK!

Master ID is the number/card that you use to enter the Setup Mode. For security reasons, it is advisable that you change the default Master ID immediately and keep the new Master ID / card confidential.

CAUTION: Beware that if you forget the Master ID, you cannot access the Setup Mode.

To change the Master ID, press <ENT>, and then either enter the desired 8Digit Master ID or present a card to the reader.

NOTE: For the FINGER006SR, the Master ID is 10Digits long in the range of 0000000000 to 4294967295.

On the next screen, enter the desired 4Digit Master Password in the PW field and, in the FP field, enter <0> if you wish to access Setup Mode without master fingerprint verification or <1> if you wish to use master fingerprint, in which case you will be asked to place your fingerprint on the scanner twice in the next step. When the Master ID/card registration is successfully completed, the LCD displays the "REGISTRATION OK" message.

NOTE: The default Master ID for FINGER006/P and IP-FINGER006 is 00000000 (Eight zeros), but for the FINGER0006SR, it is 0000000000 (Ten zeros).

12.1.7. SYSTEM INITIALIZATION

7. SYSTEM INIT.

7. SYSTEM INIT.
1 – YES, 0 - NO

WAITING ! !

System initialization allows you to initialize the FINGER006. Initialization clears all the user-defined data stored in the device such as card data, input/output setting, Time Schedules, etc.

CAUTION: Prior to system initialization, make sure to check whether or not the data stored in the device is not needed, since it will be deleted after the initialization.

To initialize the FINGER006, press <ENT>, and then press <1> to confirm. If you wish to cancel and exit without initialization, press <0> instead.

12.1.8. CARD ID CLEAR

8. CARD ID CLEAR**8. CARD ID CLEAR****1 – YES, 0 – NO**

Card ID clear allows you to delete all the card data from the FINGER006.

CAUTION: Before you clear the card memory, make sure you do not need the data stored in the device.

To clear the card data stored in the memory, press **<ENT>**, and then press **<1>** to confirm. If you wish to cancel and exit, press **<0>** instead.

12.1.9. EVENT CLEAR

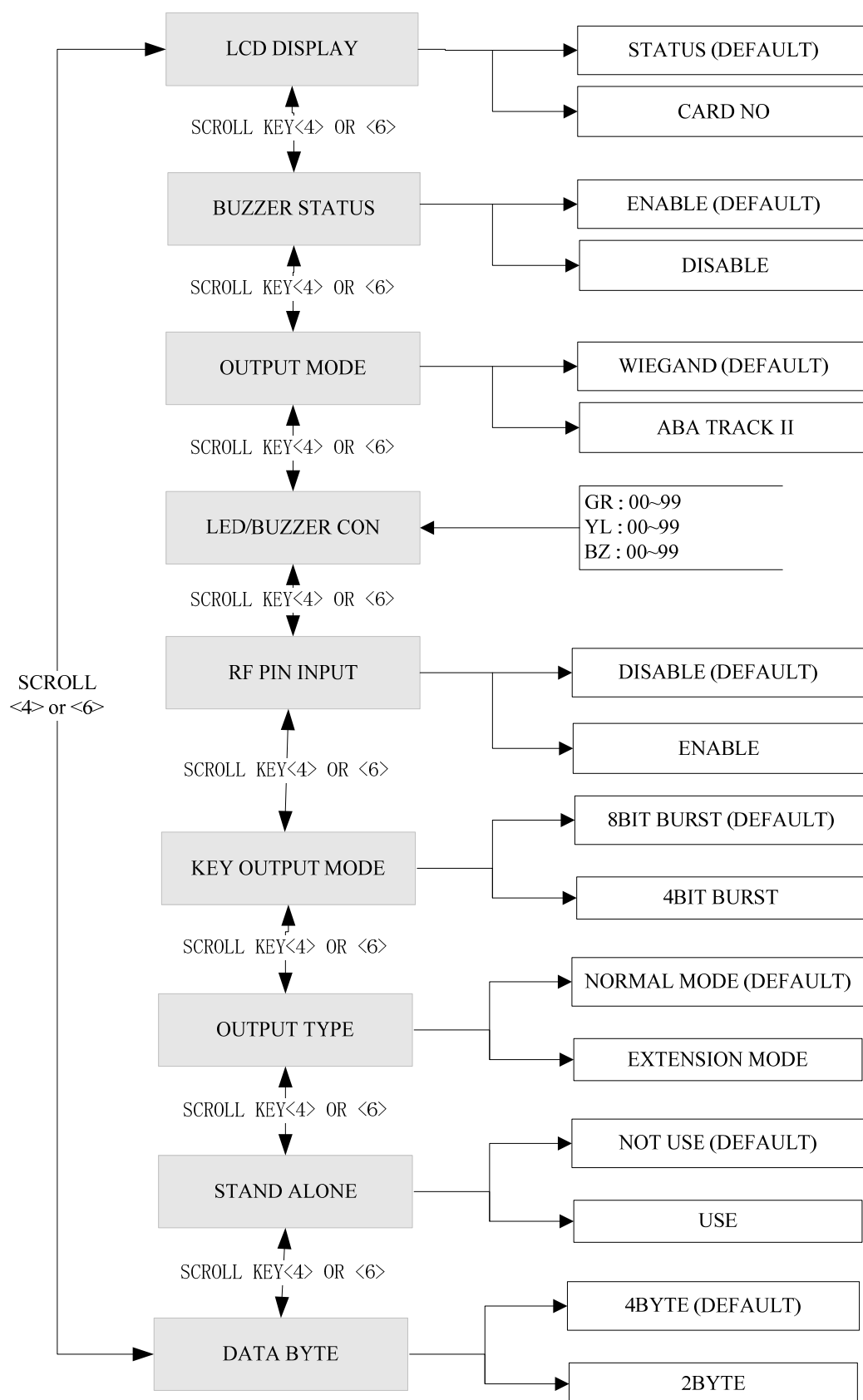
9. EVENT CLEAR**9. EVENT CLEAR****1 – YES, 0 – NO**

Event clear allows you to delete all the event data from the FINGER006.

CAUTION: Before you clear the event memory, make sure you do not need the data stored in the device.

To clear the event data stored in the memory, press **<ENT>**, and then press **<1>** to confirm. If you wish to cancel and exit, press **<0>** instead.

12.2 SETUP MENU F2



12.2.1 LCD DISPLAY

**1. LCD DISPLAY
STATUS**

**1. LCD DISPLAY
- > CARD NO**

LCD DISPLAY allows you to decide whether to display the card number or the status message on the LCD when access is granted or denied.

- **STATUS:** The LCD will display the text message indicating the status, i.e. "ACCESS GRANTED" or "ACCESS DENIED"
- **CARD NO:** Display the number of the card.

To change the setting, press <ENT> and press <4> or <6> to select "STATUS" or "CARD NO" and press <ENT> to confirm.

12.2.2 BUZZER STATUS

**2. BUZZER STATUS
ENABLE**

**2. BUZZER STATUS
- > DISABLE**

The buzzer generates a beep when a button on the keypad is pressed, when a card is read, when an error occurs, etc.

To enable or disable the buzzer sound, press <ENT> and press <4> or <6> to select "ENABLE" or "DISABLE" and press <ENT> to confirm.

NOTE: The buzzer beeps regardless of this setting, when you exit the Setup Mode, when a memory alarm is activated, or when Buzzer Output is defined in "In/Output Define".

12.2.3 OUTPUT MODE

**3. OUTPUT MODE
WIEGAND**

**3. OUTPUT MODE
→ ABA TRACK II**

You can select the output format between WIEGAND or ABA TRACK.

WIEGAND:

Outputs ID data through Wiegand output line.

ABA TRACK II:

Outputs ID data through ABA track output line.(Open collector)

12.2.4 LED_BUZZER_CONTROL

**4. LED_BUZZER_CON
GL03 YL03 BZ01**

This function controls the LED and Buzzer of the reader.

GL (Green LED): controls the card reading status.

YL (Yellow LED): controls the error indication in case the user's card isn't authorized.

BZ (Buzzer): It controls the buzzer sound.

e.g.) GL03 YL03 BZ01 : When card is presented to the unit, green LED indicator is lit for 3sec. If a user card isn't authorized, the yellow LED indicator is lit and the buzzer beeps for 1sec.

12.2.5 RF PIN INPUT

**5. RF PIN INPUT
ENABLE**

**5. RF PIN INPUT
- > DISABLE**

RF Pin Input allows you to decide whether to enable or disable PIN (or RF card number) Input via the keypad. If not configured, PIN Input is enabled by default.

Caution: If you choose "Disable", you cannot gain access via password input when using RF+PW mode.

12.2.6 KEY OUTPUT MODE

**6. KEY OUTPUTMODE
8BIT BURST**

**6. KEY OUTPUTMODE
→ 4BIT BURST**

You can change the Output Mode when you press function keys

4BIT Burst: 4bit burst will be output when you press function keys

8BIT Burst: 8bit burst will be output when you press function key

12.2.7 OUTPUT TYPE

**7. OUTPUT TYPE
NORMAL MODE**

**7. OUTPUT TYPE
→EXTENSION**

You can select the OUTPUT TYPE between NORMAL MODE and EXTENSION MODE.

NORMAL MODE: If a registered ID or/and a fingerprint is entered, FINGER006 outputs ID data only.

EXTENSION MODE: If an ID or/and a fingerprint is entered, FINGER006 outputs OK or ERROR signal and ID data.

12.2.8. STAND ALONE

**8. STAND ALONE
NOT USE**

**8. STAND ALONE
→ USE**

You can choose whether to use a standalone function or not by using <4> or <6> key. After changing set values, press <Enter>key to save the changed values

Caution: When you select "USE", FINGER006 waits for a reply of a controller. But if there is no reply after a lag, verification process is denied. (Default is <NOT USE>)

When the controller is waiting for the verification signal, LCD shows "RD CERTIFYNG" message.

12.2.9 DATA BYTE (FINGER006SR ONLY)

9. DATA BYTE
4BYTE**9. DATA BYTE**
- > 2BYTE**This feature only applies to FINGER006SR.**

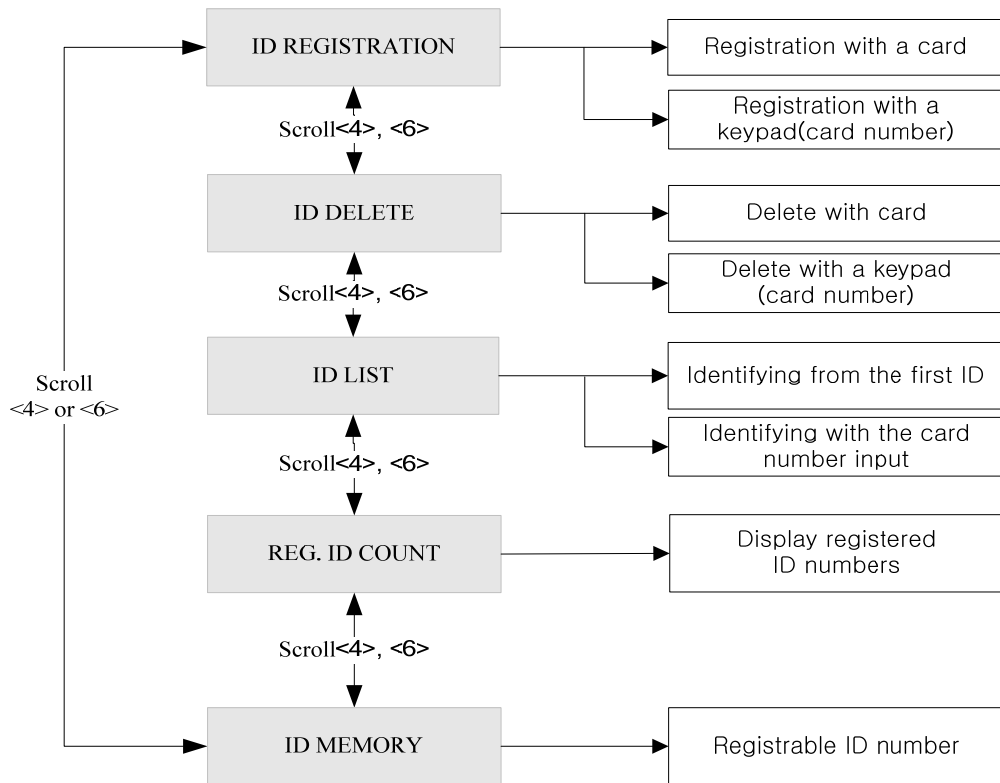
By default, the FINGER006SR can read smart card written in the 4BYTE format, but, for advanced applications, you can use 2BYTE format smart cards. To do so, you must change the Data BYTE setting to "2BYTE". To change the setting, press <ENT> and press <4> or <6> to select "4BYTE" or "2BYTE" and press <ENT> to confirm.

Range of Card Number (FINGER006SR Only)

- **4 Byte (Default):** The Card Number can be in the ranges of 000000000 – 4294967295
- **2 Byte:** The first and last 5 digits can each be in the upper ranges of 00000 ~ 65535
lower ranges of 00000~65535

The total is in the ranges of 0000000000~6553565535

12.3 SETUP MENU F3



12.3.1 ID REGISTRATION

1. ID REGISTRATION	Registration allows you to add new cardholders to the FINGER006. To add a new cardholder ID, press <ENT> .
ENTER ID NO. - >	Either present a card you wish to register to the FINGER006 or enter the card number (ID) via the keypad and press <ENT>. NOTE: A Card Number (ID) can be 4 to 8Digits long. For the FINGER006SR, it can be 4 to 10Digits long. For more information about the Card Number Range on the FINGER006SR, refer to the note under 12.2.9 Data BYTE.
ID: 12345678 PW____ FP_	Once the Card Number is entered, enter the Password (PW), and Use of Fingerprint (FP) and press <ENT>. For more information, see below.

**TO REGISTER F/P
PUT YOUR FINGER!**

If you have entered 1 in the FP field, the fingerprint scanner will be lit up. Then, place the cardholder's fingerprint on the scanner.

**LIFT AND
PUT YOUR FINGER!**

Once the light from the fingerprint scanner is turned off, lift the finger up and put it back on a while later.

**[Q1:3] [Q2:4]
REGISTRATION OK!**

If the registration is successful, the "REGISTRATION OK!" message will be displayed on the LCD. If you have registered the fingerprint, the quality score for the fingerprint will appear as shown on the left. If the registration is not successful, the "REGISTRATION ERR!" Message will be displayed on the LCD.

Description of Fields

- **PW (Password):** Enter the 4Digit password. Password verification can be enabled in 12.1.4. Reader1 Mode. This field is compulsory even if you do not use password verification.
- **FP (Fingerprint):** To register the cardholder's fingerprint, enter 1. If you do not wish to register the cardholder's fingerprint, enter 0.

12.3.2 ID DELETE

2. ID DELETE

ID Delete allows you to delete existing cards from the FINGER006. To delete an existing card (Or ID), press **<ENT>**.

**ENTER ID NO.
- >**

Either present a card you wish to delete to the FINGER006 or enter the card number (ID) via the keypad and press **<ENT>**.

**ID: 12345678
DELETE SUCCESS!**

If the card was successfully deleted, the "DELETE SUCCESS!" message will be displayed on the LCD. If the card you presented or the card number you entered is not found, the "UNREGISTERED ID" message will be displayed.

12.3.3 ID LIST

3. ID LIST	ID List allows you to search for a certain registered card or view the list of all registered cards. To begin, press <ENT>
3. ID LIST 1: CARD 2: FIRST	To search for a certain registered card, press <1> . To view the entire list of all registered cards, press <2> .
ENTER ID NO. - >	If you have entered <1> , enter the Card Number (ID) or present the card you wish to view
ID: 12345678 PW1234FP1	The LCD will show the information of the card you have selected in the previous step or the first card on the list. Press <4> or <6> to view the information of the previous or next card. The "FIRST ID" or "LAST ID" message will appear if you are viewing the first or last ID. If there is no card data, the LCD will display the "MEMORY EMPTY" message.

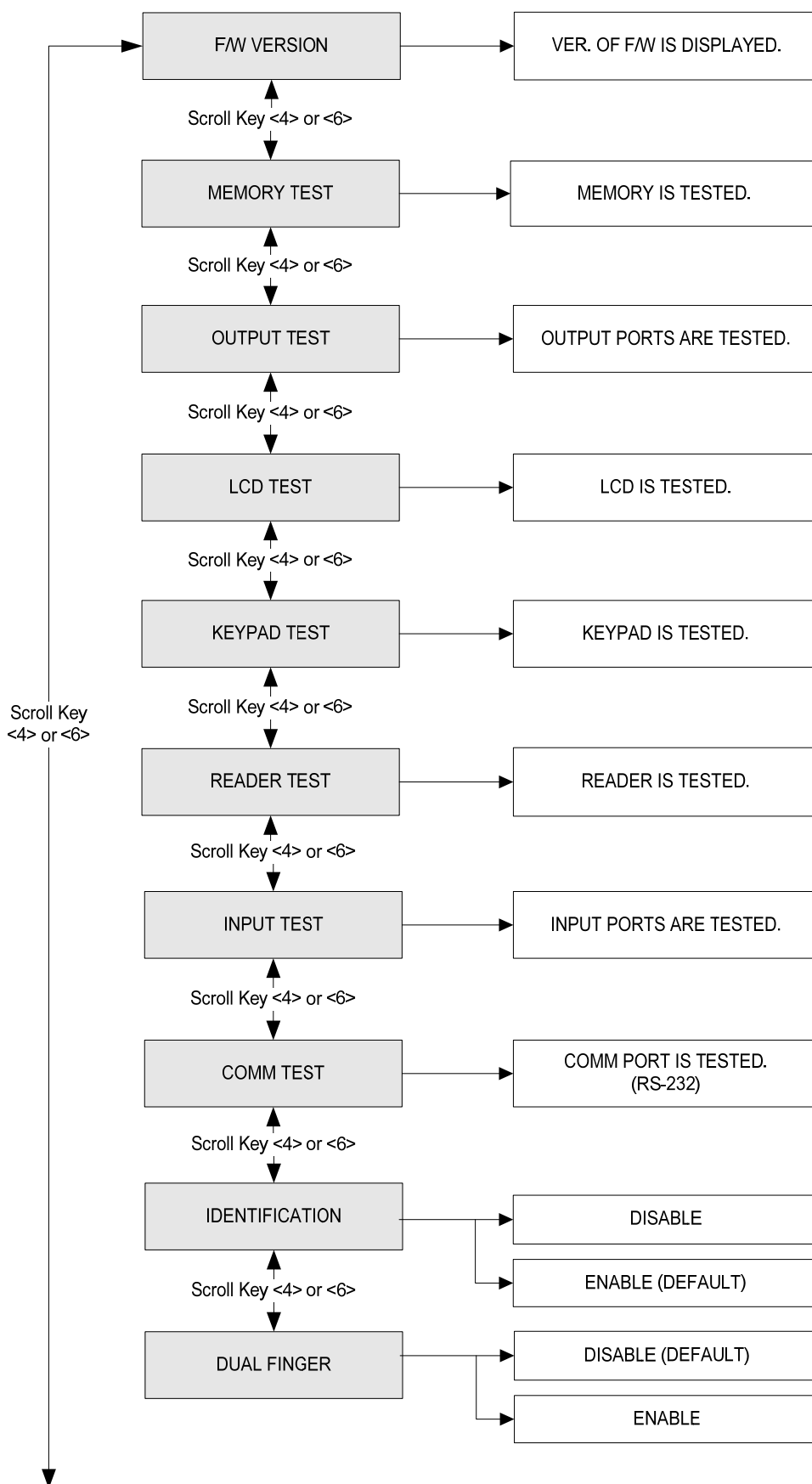
12.3.4 REGISTERED ID COUNT

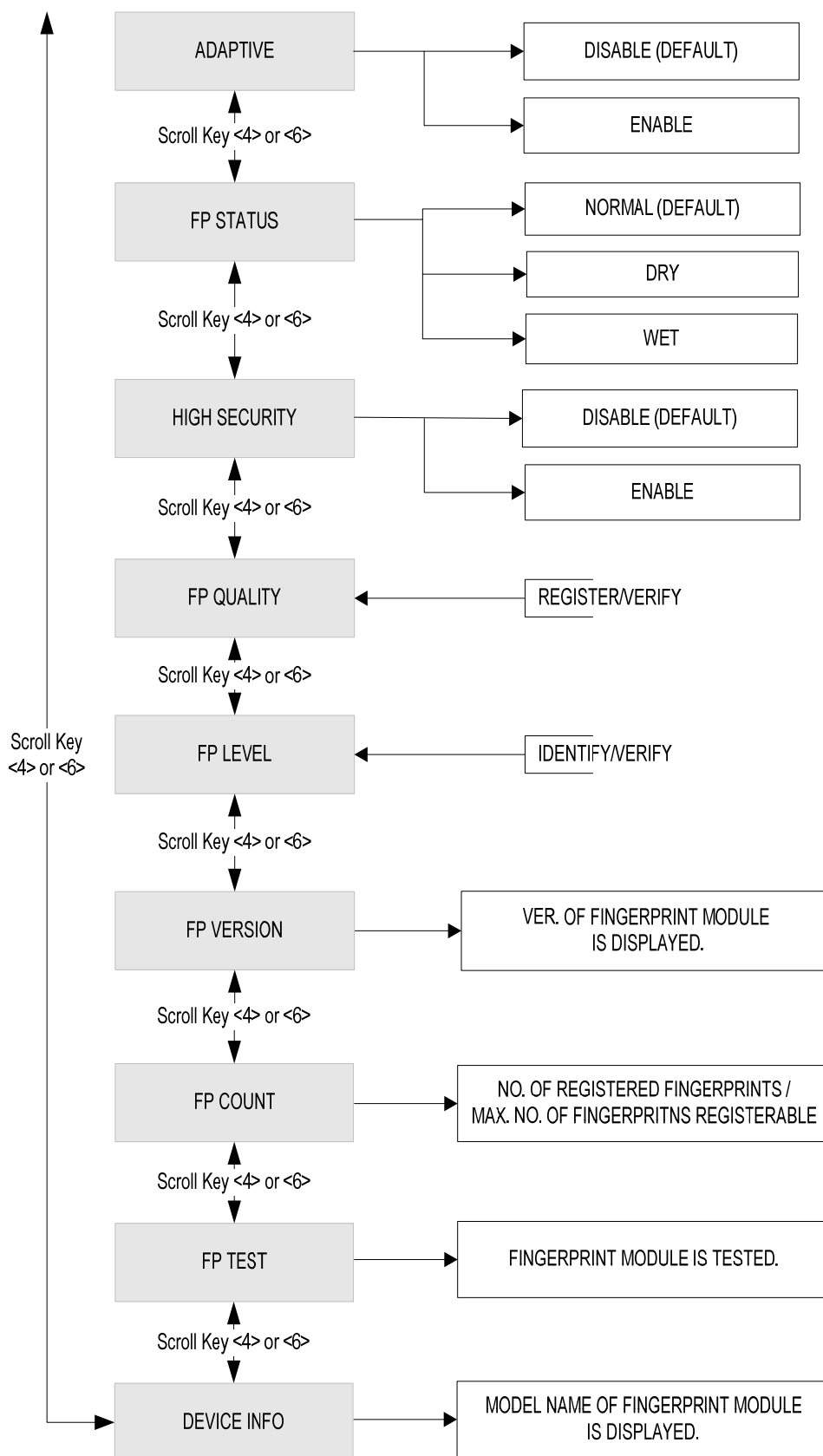
4. REG. ID COUNT 00123	The number of registered user IDs is displayed. This count automatically increases or decreases as IDs are registered or deleted. The LCD on the left shows that the sum totals of 123 user IDs are registered in the memory.
---	---

12.3.5 ID MEMORY

5. ID MEMORY 50000	Show the maximum number of events where you can save.
-------------------------------------	---

12.4 SETUP MENU F4





12.4.1 FIRMWARE VERSION

1. F/W VERSION V A.1.0

The version of the firmware installed in the FINGER006 is displayed on the LCD.

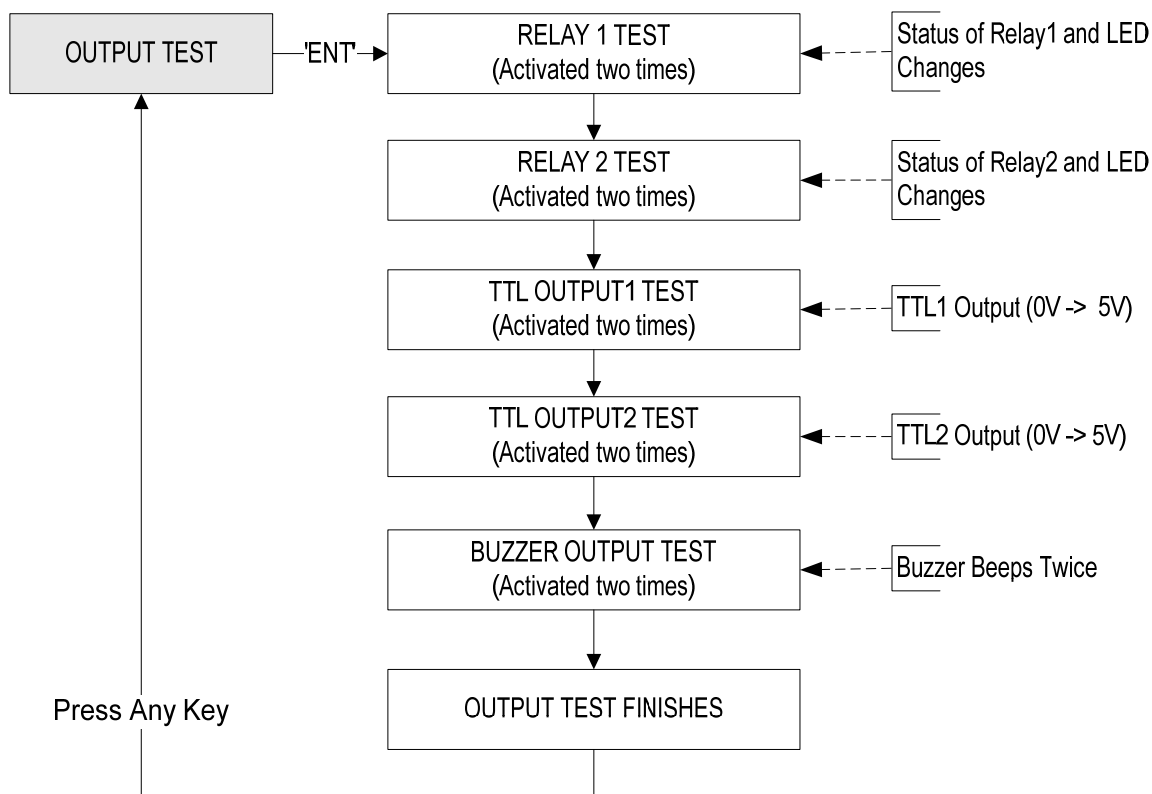
12.4.2 MEMORY TEST

2. MEMORY TEST

**TEST FAILED!!!
PRESS ANY KEY...**

Memory Test allows you to test the memory of the FINGER006. To begin the test, press **<ENT>**. If the test is successful, the LCD will display the "TEST PASSED" message. Press any key to finish the test. If the test is unsuccessful, the LCD will display the "TEST FAILED" message. Press any key to finish the test and try again. If the problem persists, please contact your local IDTECK dealer for assistance or service.

12.4.3 OUTPUT TEST



3. OUTPUT TEST

**OUTPUT 1
OFF**

PRESS ANY KEY...

Output Test allows you to test the output ports of the FINGER006. To begin the test, press **<ENT>**. First, output ports 1 and 2 will be tested. During the test, relay outputs are activated and you will hear Tick-Tack sounds with the green LED blinking twice. Second, output ports 3 and 4 will be tested. During the test, TTL outputs are activated and the yellow LED blinks twice. You can check the voltage level of the TTL outputs with appropriate test equipment. Lastly, output port 5 will be tested. During the test, you will hear 2 beeps. After all the tests are over, press any key to exit.

12.4.4 LCD TEST

4. LCD TEST

**AAAAAAAAAAAAAAAA
CCCCCCCCCCCCCCCC**

LCD Test allows you to test the LCD of the FINGER006. To begin the test, press **<ENT>**. Once the test begins, the LCD will display a series of different screens. Ensure that all the screens on the LCD are properly displayed. The test ends with the display of the firmware update date (YYYY/MM/DD). After the test is finished, press any key to exit.

12.4.5 KEYPAD TEST

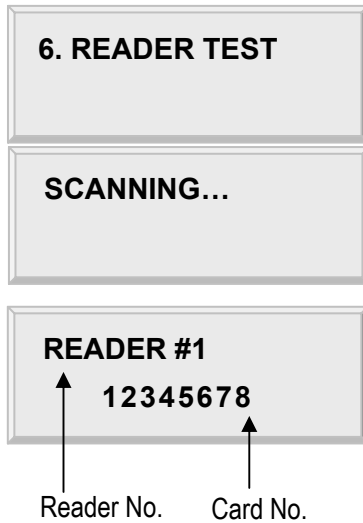
5. KEYPAD TEST

**5. KEYPAD TEST
0123456789ABCDEF**

Keypad Test allows you to test the keys on the keypad. To begin the test, press **<ENT>**. Press each key on the keypad, then the number or letter that corresponds to the key pressed will disappear from the screen. After all the keys are pressed, the LCD displays the "TEST PASSED" message.

NOTE: Letter A corresponds to **<ESC>**, B to **<ENT>**, C to **<F1>**, D to **<F2>**, E to **<F3>**, and F to **<F4>**.

12.4.6 READER TEST

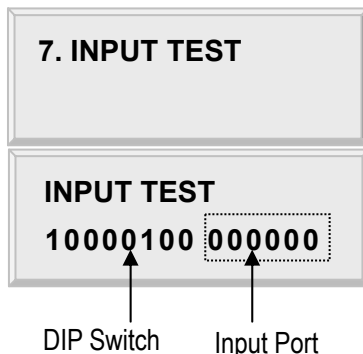


Reader Test allows you to test the reader(s). To begin the test, press **<ENT>**. While the LCD displays “SCANNING”, present a card to the reader you would like to test, and the LCD will display the reader number and the card number. After the test is finished, press **<ESC>** to exit.

NOTE: Reader#1 refers to the built-in reader of the FINGER006, and Reader #2 refers to an external reader.

NOTE: You can also use Reader Test to check the number of a card.

12.4.7 INPUT / DIP SWITCH TEST



Input Test allows you to check the status of Input Ports and DIP switches (Communication Address Setting Switches). To begin the test, press **<ESC>**.

1. **DIP Switch:** 1=ON, 2=OFF (It shows how the DIP switch on the back of the FINGER006 is set.)
2. **Input 1-4:** 0=OFF (Disabled)
1=ON (Enabled)
2=Input Disconnected
3. **Input 5:** The status of the tamper switch inside the FINGER006 (0=OFF (Disabled), 1=ON (Enabled))
4. **Input 6:** The status of the Proximity Sensor (0=OFF (Disabled), 1=ON (Enabled))

If you activate the Cut-Off Check feature for all the input ports in “5.IN/OUT DEFINE” from F2 Setup menu, the result of an input port test will change to 222200 (If termination resistors are not connected) or 000000 (If termination resistors are connected).

12.4.8 COMMUNICATION TEST

8. COMM TEST

TEST PASSED!!!
PRESS ANY KEY...

TEST FAILED!!!
PRESS ANY KEY...

COMM Test allows you to test communication. Prior to the test, connect the RS232-RX wire (Black wire with White stripe) and the RS232-TX wire (Red wire with Black stripe) together. To begin the test, press **<ENT>**. If the test is successful, the LCD will display the "TEST PASSED" message. Press any key to finish the test. If the test is unsuccessful, the LCD will display the "TEST FAILED" message. Press any key to finish the test and try again after powering the FINGER006 off and back on.

12.4.9 IDENTIFICATION MODE

9. IDENTIFICATION

9. IDENTIFICATION
- > ENABLE

Identification Mode is a feature that allows users to use just fingerprint verification without having to present their cards or enter their ID numbers. If this feature is enabled, a user can just place the fingerprint onto the fingerprint scanner, and then the FINGER006 will perform 1: N authentication for all fingerprint templates in the database and grant access if a fingerprint template that matches the user's fingerprint is found.

12.4.10 DUAL FINGERPRINT MODE

10. DUAL FINGER

10. DUAL FINGER
- > DISABLED

The Dual Fingerprint Mode allows one user to register two different fingerprints per ID. This feature is useful when a user's finger is injured and wishes to use the other registered finger in the verification process.

To enable or disable the "Dual Fingerprint Mode", press **<ENT>** and press **<4>** or **<6>** to select "ENABLE" or "DISABLE" and press **<ENT>** to confirm.

DUAL FINGER MODE	Number of Templates and Fingers	Authentication Success Ratio	Recommended Authentication Mode
NOT USE	2 Storage Templates for a single finger.	High	Identification Mode
USE	1 Storage Template each for 2 different fingers.	Low	Verification Mode

12.4.11 ADAPTIVE MODE

11. ADAPTIVE

**11. ADAPTIVE
 - > DISABLED**

The Adaptive Mode is a feature that improves the quality of fingerprint images in the authentication process, guaranteeing a higher likelihood of successful authentication. However, the authentication process may take longer with this feature on. To enable or disable the Adaptive Mode, press **<ENT>** and press **<4>** or **<6>** to select "ENABLE" or "DISABLE" and press **<ENT>** to confirm.

12.4.12 FP STATUS

**12. FP STATUS
 NORMAL**

**12. FP STATUS
 - > DRY**

FP Status is a special feature designed for special environments where the fingers of most employees might be too dry or wet. If you set the FP Status setting to dry or wet, the FINGER006 will adjust the fingerprint images according to the environment to improve the authentication rate. To change the setting, press **<ENT>** and press **<4>** or **<6>** to select "NORMAL", "DRY" or "WET" and press **<ENT>** to confirm.

12.4.13 HIGH SECURITY

13. HIGH SECURITY

**13. HIGH SECURITY
 - > DISABLED**

High Security allows you to enable or disable the latent fingerprint image processing.

CAUTION: *Since the image of a latent fingerprint and that of a dry fingerprint are both equally faint, it is hard to tell dry fingerprints from latent images. Therefore, enabling High Security will lower the recognition success rate of dry fingerprints as they might be mistaken to be latent fingerprints.*

NOTE: *In a place where many users have dry fingerprints, a better recognition success rate can be achieved by adjusting the exposure value higher and/or enabling Adaptive Mode.*

12.4.14 FP QUALITY

14. FP QUALITY**REGISTER / VERIFY****40 / 30**

Register Quality and Verify Quality are the threshold values for fingerprint image capture in the fingerprint registration enrollment process (Register Quality) and verification process (Verify Quality). If the quality value for a capture fingerprint image is below the Register Quality threshold, the authentication (registration or verification) is rejected. By adjusting the threshold value, you can control the desired level of fingerprint image quality.

NOTE: If you want to change this function, please consult with IDTECK. Otherwise the recognition success rate is not guaranteed.

12.4.15 FP LEVEL

15. FP LEVEL**8 / 5****IDENTIFY / VERIFY****8 / 5**

Verify / Identify Security Level is the threshold value for fingerprint authentication. By adjusting the setting value, you can achieve either a higher recognition success rate or a higher security level.

NOTE: If you want to change this function, please consult with IDTECK. Otherwise the recognition success rate is not guaranteed.

12.4.16 FINGERPRINT MODULE VERSION

16. FP VERSION**V1.71**

FP Version allows you to check the version of the fingerprint module on your FINGER006.

12.4.17 FINGERPRINT COUNT

17. FP COUNT**0000/1000**

FP Count allows you to see how many fingerprints are registered in your FINGER006 and how many can be registered in total. Depending on the specification of the fingerprint module in use, the total fingerprint capacity can be 1000, 2000 or 4000 fingerprints.

12.4.18 FINGERPRINT MODULE TEST

18. FP TEST**TEST PASSED!!!**

FP Test allows you to test the fingerprint module on your FINGER006. To begin the test, press <ENT>. If the test is successful, the "TEST PASSED" message will be displayed. If the test is unsuccessful, the LCD will display the "TEST FAILED" message. If that is the case, try again. If the problem persists, please contact your local IDTECK dealer for assistance or service.

12.4.19 FINGERPRINT DEVICE INFORMATION CHECK

19. DEVICE INFO
FIM2030-HD

Device Info shows you the model name of the fingerprint module on your FINGER006.

13. Appendix

13.1 Default Values for Parameters

No	Parameter	Default Value
1	READER #1 Operation Mode	ID(RF), FP(PW)
2	READER #2 Operation Mode	ID ONLY
3	READER #1 Keypad Input Limit	USE
4	READER #2 Keypad Input Limit	USE
5	Output Mode	WEIGAND
6	Key Output Mode	8BIT BURST
7	Output Type	NOMAL MODE
8	LCD Display	STATUS

14. FCC Registration Information

FCC REQUIREMENTS PART 15

Caution: Any changes or modifications in construction of this device which are not expressly approved by the responsible for compliance could void the user's authority to operate the equipment.

NOTE: This device complies with **Part 15 of the FCC Rules**.

Operation is subject to the following two conditions;

1. This device may not cause harmful interface, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A Digital Device, pursuant to **Part 15 of the FCC Rules**. These limits are designed to 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 radio or television off and on, the user is encouraged to try to correct interference by one or more of the following measures.

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on another circuit.
4. Consult the dealer or an experienced radio/TV technician for help.

15. Warranty Policy and Limitation Liability

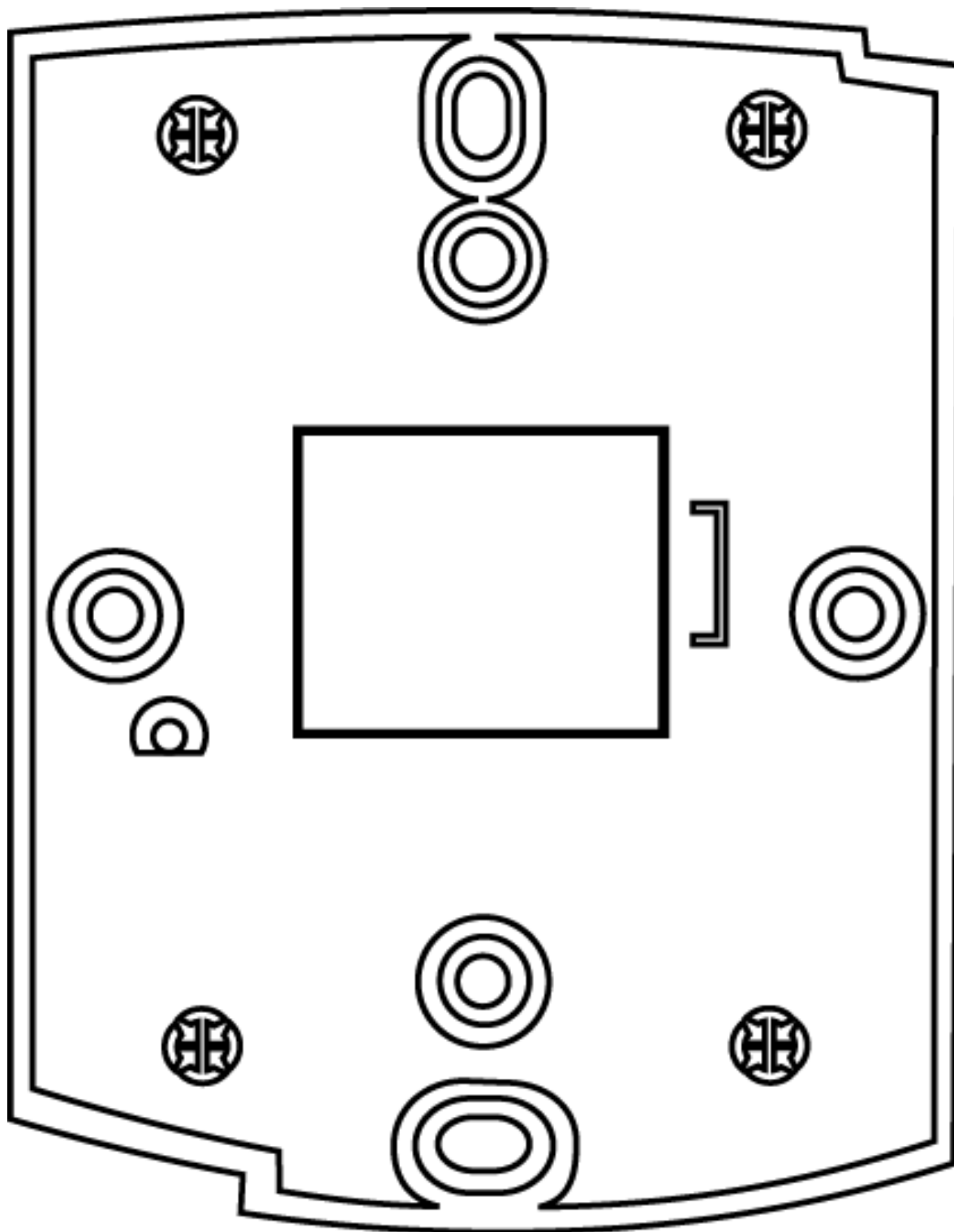
IDTECK warrants this product against defects in material and workmanship for the period specified below from the date of purchase under normal customer use. This Warranty doesn't apply: 1) to any product which has been dismantled without authorization of IDTECK or/and has a damaged or detached QC label on its back side; 2) to any losses, defects, or damages caused by improper testing, operation, installation, maintenance, modification, alteration, or adjustment; 3) to any product with a damaged or faded serial number on it; or 4) to any losses, defects, or damages caused by lightning or other electrical discharge, natural disaster, misuse, accident or neglect.

This Limited Warranty is in lieu of all other warranties, obligations, or liabilities on the part of IDTECK, and IDTECK DISCLAIMS ANY AND ALL WARRANTY, WHETHER EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IDTECK does not, and cannot, know who is present, what property is located, where this product will be used; it would be extremely difficult to determine the actual damages that may result from a failure of the product to perform as anticipated; and the low price of this product is based upon the nature of the product provided and the limited liability that IDTECK assumes. IDTECK IS NOT RESPONSIBLE FOR ANY PERSONAL INJURY, PROPERTY DAMAGE OR LOSS, DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR OTHER LOSS, AND IDTECK'S MAXIMUM LIABILITY SHALL NOT IN ANY CASE EXCEED THE PURCHASE PRICE OF THE PRODUCT.

To obtain repair or replacement under the terms of this warranty, visit IDTECK's Website (<http://www.idteck.com>) and place an online RMA request. After an RMA code is issued, return the product along with the authorization RMA code.

>> Warranty Period

	Product Category	Warranty Period
1	RF CARDS (ACTIVE TYPE)	1 year
	FINGERPRINT MODULE / SENSOR	
2	RF READERS (WITH EPOXY POTTING)	2 years
3	STANDALONE CONTROLLERS	
4	CONTROL PANELS	
5	FINGERPRINT READERS	
6	RF READERS (WITH EPOXY POTTING)	Lifetime
7	RF CARDS (PASSIVE TYPE)	

16. Template

How to Make RMA Request (After Sales Service)

To make the RMA request, the product must be initially registered on IDTECK webpage. Please attach the RMA request form on the product and send it to IDTECK RMA Center.

Please follow the instructions below:

1. Please register the RMA request via IDTECK webpage.
: www.idteck.com → "Support & Download" → "Online RMA" → "RMA REQUEST"
(Please refer to the IDTECK webpage for more details.)
2. RMA Code will be issued after the RMA Center reviews the RMA request form.
3. Fill out the A/S request form (included in the product package) and attach it to the product using the aluminum string.
4. Enclose the product along with the RAM Code and send it to IDTECK RMA Center.
(Product without RMA Code is not accepted.)

If you have any questions or problems regarding the RMA services, please contact us using the following contact information below. Friendly representatives at IDTECK are always standing by to provide the best after sales services.

IDTECK Headquarter

5F, Ace Techno Tower B/D, 684-1, Deungchon-Dong,

Gangseo-Gu, Seoul, 157-030, Korea

Tel: +82-2-2659-0055 (Ext. 158)

Fax: +82(2) 2659-0086

E-mail: webmaster@idteck.com

Website: www.idteck.com

E-Training Center: <http://www.idtecktraining.com>

IDTECK Production Facility and RMA Center

3F, 10/10-1/10-2, Dodang-Dong,

Weonmi-Gu, Bucheon-Si, Gyeonggi-Do 157-030, Korea

Tel: +82-2-2659-0055 (Ext. 158)

Fax: +82(2) 2659-0086

E-mail: webmaster@idteck.com

Website: www.idteck.com

E-Training Center: <http://www.idtecktraining.com>



The specifications contained in this manual are subject to change without notice at any time.

**5F, Ace Techno Tower B/D, 684-1, Deungchon-Dong,
Gangseo-Gu, Seoul, 157-030, Korea**

Tel : +82-2-2659-0055

Fax : +82-2-2659-0086

E-mail : webmaster@idteck.com