

Fingerprint Identification System

Owner's Manual



Model : LAFP10-R
LAFP10-S



This lightning flash with arrowhead symbol within an equilateral triangle is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.



The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.

FCC WARNING: This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the

instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.

REGULATORY INFORMATION: FCC Part 15

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 provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

- A suitable conduit entries, knock-outs or glands shall be provided in the cable entries of this product in the end user.
- **Caution:** Danger of explosion if battery is incorrectly replaced. Replaced only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

- Holes in metal, through which insulated wires pass, shall have smooth well rounded surfaces or shall be provided with brushings.

Warning: Do not install this equipment in a confined space such as a bookcase or similar unit.

Warning: Wiring methods shall be in accordance with the National Electric Code, ANSI/NFPA 70.

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Warning: To reduce a risk of fire or electric shock, do not expose this product to rain or moisture.

Caution: This installation should be made by a qualified service person and should conform to all local codes.

Caution: To avoid electrical shock, do not open the cabinet. Refer servicing to qualified personnel only.

Caution: The apparatus should not be exposed to water (dripping or splashing) and no objects filled with liquids, such as vases, should be placed on the apparatus.

To disconnect power from the mains, pull out the mains cord plug. When install the product, ensure that the plug is easily accessible.



Disposal of your old appliance

1. When this crossed-out wheeled bin symbol is attached to a product it means the product is covered by the European Directive 2002/96/EC.
2. All electrical and electronic products should be disposed of separately from municipal waste stream via designated collection facilities appointed by the government or the local authorities.
3. The correct disposal of your old appliance will help prevent potential negative consequences for the environment and human health.
4. For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service or the shop where you purchased the product.
5. EEE Compliance with Directive.



This product is manufactured to comply with EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC.

European representative :

This class [B] digital apparatus complies with Canadian ICES-003
 Cet appareil numérique de la classe [B] est conforme à la norme
 NMB-003 du Canada

Important Safety Instructions

1. **Read these instructions.** - All these safety and operating instructions should be read before the product is operated.
2. **Keep these instructions.** - The safety, operating and use instructions should be retained for future reference.
3. **Heed all warnings.** - All warnings on the product and in the operating instructions should be adhered to.
4. **Follow all instructions.** - All operating and use instructions should be followed.
5. **Do not use this apparatus near water.** - For example: near a bath tub, wash bowl, kitchen sink, laundry tub, in a wet basement; near a swimming pool; etc.
6. **Clean only with dry cloth.** - Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners.
7. **Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.** - Slots and openings in the cabinet are provided for ventilation, to ensure reliable operation of the product, and to protect it from overheating. The openings should never be blocked by placing the product on a bed, sofa, rug or other similar surface. This product should not be placed in a built-in installation such as a bookcase or rack unless proper ventilation is provided and the manufacturer's instructions have been adhered to.
8. **Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.**

Important Safety Instructions

9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.
13. Unplug this apparatus during lightning storms or when unused for long periods of time.
14. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.



Glossary



LAFP10
Fingerprint Identification System

■ Admin, Administrator

- As a user who can enter into the terminal menu mode, he can register/modify/delete terminal users and change the operating environment by changing settings.
- If there is no administrator for a terminal, anyone can change the settings. In this regard, it is recommended to register at least one administrator.
- Caution is required with registration and operation because an administrator has the right to change critical environmental settings of the terminal.

■ 1 to 1 Verification

- A user's verification fingerprint (template) is compared to the user's enrollment fingerprint (template) previously registered. The terminal performs 1:1 matches against the user's enrolled template until a match is found.
- It is called 1 to 1 Verification because only the fingerprint registered in the user's ID or card is used for comparison.

■ 1 to N Identification

- The terminal performs matches against multiple fingerprints (templates) based solely on fingerprint information.
- Without the user's ID or card, the user's fingerprint is compared to fingerprints previously registered.

■ I-Capture (Intelligent Capture)

- Reinforces detection capability for residual fingerprints (fingerprints left on a sensor window due to sweat or contaminants on a finger) and automatically adjusts sensor settings to detect good-quality fingerprints regardless of the conditions (dry or wet) of the fingerprints.

■ Authentication level

- Depending on the fingerprint match rate, it is displayed from 1 to 9. Authentication is successful only if the match rate is higher than the set level.
- The higher the Authentication level, the higher the security. However, it requires a relatively high match rate, so Authentication is vulnerable to failure.
- 1:1 Level: Authentication level used for 1:1 verification.
- 1:N Level: Authentication level used for 1:N identification.

■ Authentication method

- Various kinds of authentication including FP (fingerprint) authentication, PW (password) authentication, RF (card) authentication, or a combination of these methods.
- Ex) FP/PW: fingerprint or password authentication; password is used for authentication if fingerprint authentication fails.

■ Function keys

- [F1], [F2], [F3], [F4], [ENTER] are used, and they are used for direct authentication and each key represents each authentication mode.

1. Before using

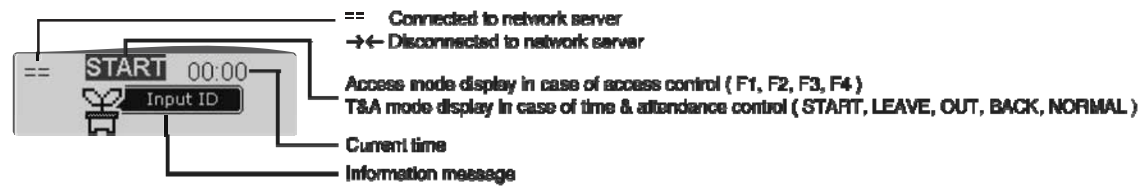
Terminal description



		Terminal
●	LCD	Display character message for all the operations
●	Key pad	[F1] : Start, [F2] : Leave, [F3] : Outside work, [F4] : Come back
		Input digits (1-9)
		Enter '0' or LCD menu scroll
		Terminal menu setting (Enter info menu mode for terminal menu setting when pressed over 2 seconds)
●	Enter, Call	- Clear typo when entering settings - Move up to higher menu - Use when escaping from menu setting
		Use after entering the settings when configuring the terminal environment. Visitors use this to ring the interphone bell
●	Micro phone	Convey visitor's voice to door phone
●	LED Lamp	Show operation status like power supply, Lock status and card contact
●	Fingerprint input window	Fingerprint input
●	IRLED sensor	Person's approach makes it automatically turn on button LED and LCD window with ID input screen
●	Card input area	Card input
●	Speaker	Voice output

1. Before using

Screen description



- Initial screen.



- Waiting for a user's ID to be input.



- Fingerprint input.



- When a non-registered user ID is entered.
- When connection mode is 3:N and 1:N identification is tried even though there is no user allowed for 1:N identification.



- Password input.



- Successful authentication.



- Authentication failed.



- Terminal program is in upgrade.
(Power must not turn off when this message is displayed.)



- There is no user registered on the terminal or no connection to the server, so it is trying to connect.



- Waiting for a reply from the server for authentication.



- A registered user tried authentication at that time when access is not allowed.



- There is no response from the server during the authentication process.
- Network to server is disconnected during the authentication process.



- Terminal is locked.
- It is not mealtime in case of meal control mode.

2. Introduction

2.1. Features

- Access control system using LAN**
 - Communication between the unit and authentication server is done through a UTP cable and TCP/IP protocol, so an existing LAN can be used as it is. It guarantees network-based administration and monitoring as well as easy expansion, high reliability, and higher speed.
- Convenient auto sensing function**
 - Simple authentication process without any key input simple fingerprint touching is sufficient.
- Simple authentication using fingerprints**
 - Fingerprint authentication technology prevents users from forgotten password or card, stolen key or card, etc., which is one of good ways to improve security level.
- High processing capacity of terminal and server**
 - There is not any limit on management of user's access information in case that access server is used. Even in standalone operation by using local terminal, it is possible to manage fingerprint authentication of more than 8,000 users (in optional case).
- Various information messages**
 - It ensures easy fingerprint recognition because voice and LCD window information are provided during the authentication process. In addition, the backlight installed in the LCD window helps with easy key operation in the dark.
- Door phone**
 - Easy visitor identification and convenient response.
- Various and flexible access controls**
 - No risk of rent, forgery, or loss of keys or cards.
 - Perfect control by assigning different security clearances to each user or group.
 - Flexibility provided by allowing limited time for entry/exit.
 - Low maintenance.
 - No need to issue visitor card for visitor.

2. Introduction

2.1. Features

- Various applications including access control, time & attendance, etc.**
 - Various operation modes depending on the terminal menu settings.
- Enhanced security with detection of fake finger**
 - Adopted detection technology of fake finger enhances security level.
- Various registration and authentication methods**
 - There are a total of 11 registration and authentication methods (4 methods if the card reader is not installed), so you are required to select one method before registering users and an administrator.

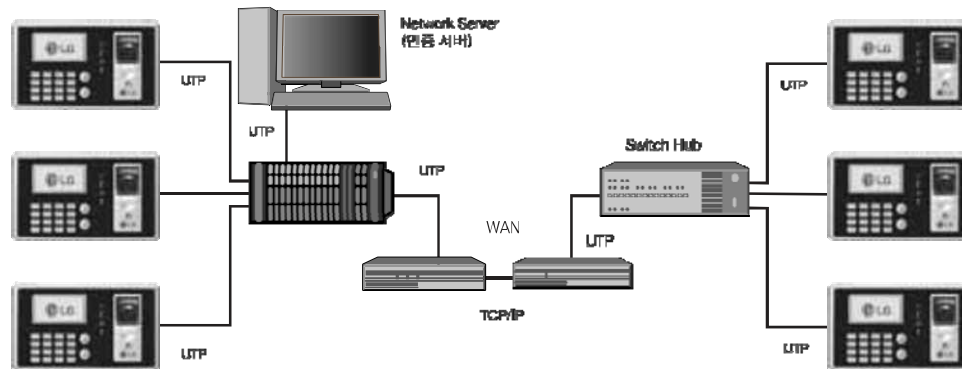
registration	
FP	Fingerprint registration. Fingerprint authentication.
ID&PW	Password registration. Password authentication after ID input.
FP&PW	Fingerprint and password registration. Fingerprint or password authentication.
FP&PW	Fingerprint and password registration. Password authentication after fingerprint authentication.
RF	Card registration. Card authentication
RF&FP	Card and fingerprint registration. Card or fingerprint authentication
RF&FP	Card and fingerprint registration. Fingerprint authentication after card authentication.
RF&PW	Card and password registration. Card or password authentication.
RF&PW	Card and password registration. Password authentication after card authentication.
ID&FP&RF&FP	Card and fingerprint registration. Fingerprint authentication after ID input or fingerprint authentication after card authentication.
ID&PW&RF&PW	Card and password registration. Password authentication after ID input or password authentication after card authentication.

* RF defines '125KHz Proximity Card' or '13.56MHz Smart Card'.

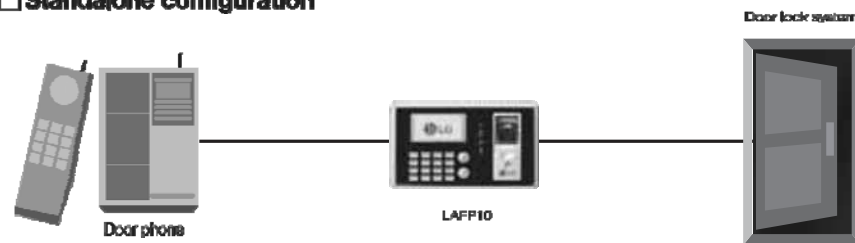
2. Introduction

2.2, Configuration

Network configuration



Standalone configuration



3. Configuration settings

3.1. Check items before device configuration settings

3.1.1. Entering menu

The following screen appears when [-] is pressed for over 2 sec.



1. User
2. Network
3. Option
4. Terminal Info
5. Ext Function
6. Device

- Press [0] to view menus not shown in the LCD window.
- Press a number key in order to go submenu. The following administrator authentication allows for entry of submenu.



<Input Admin ID>
ID : 0001

- Press [ENTER] after entering the administrator's ID, and the administrator authentication is processed according to the previous setting such as fingerprint authentication or password authentication. If the authentication succeeds, submenu screen appears.

※ Administrator authentication is required only once for all in main menu, so all other menus are accessible until he/she completely exits from the main menu.

3. Configuration settings

3.1.2. Changing setting parameters

To change setting parameters, press [#] to delete old values and input new values.



Press [0] to see menus not shown in the LCD window, and press the corresponding number to select a menu.



Press [ENTER] for confirmation of setting parameter or to move to the next setting, and press [#] to move to upper menus.



Hold [#] for over 2 sec. to cancel the current setting and move to the upper menu.

3. Configuration settings

3.1.3. Saving device configuration settings

Press [#] in the main menu to save device configuration settings.
The following screen appears:



Save?
[Y=1/N=2] : _

Press [1] to save changes.
If not, press [2].



If there are no changes in device configuration settings, it goes out of this setting mode without going through the above screen.

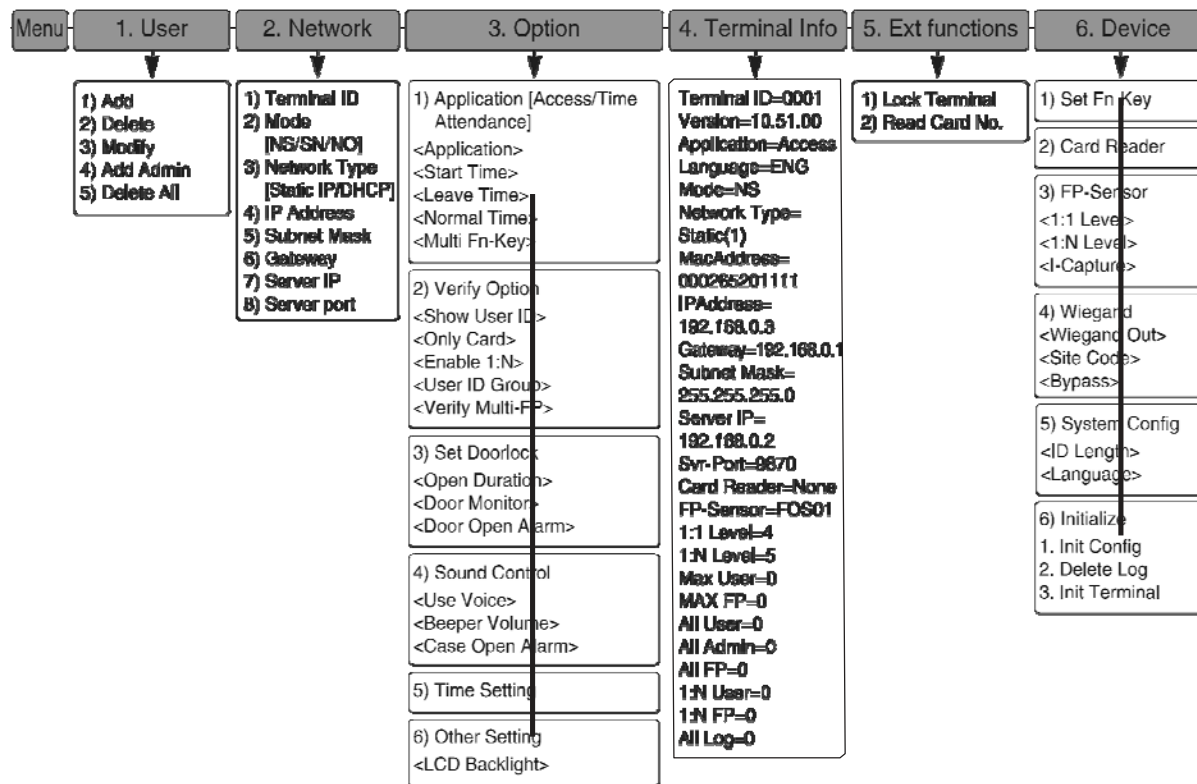


If there is no input for a certain period of time while changing the device configuration settings, the setting process finishes. If there are changes in device configuration settings, the above screen "Save?" appears. If not, it goes out of this setting mode and the initial screen appears.

3. Configuration settings

3.2. Menu configuration

□ Press [*] for over 2 sec. to enter the menu.



4. How to use

4.1. Access control application

Default screen [*] [3] Option [1] Application [0] for access control application

4.1.1. Authentication mode



• Fingerprint authentication

- Fingerprint authentication in the corresponding mode by pressing a relevant function key; [Enter], [F1], [F2], [F3] and [F4]. Fingerprint authentication through auto sensing without pressing any keys. This authentication is performed in the current mode displayed in the screen.

• Password authentication

- After inputting the user ID and changing the authentication mode by pressing the corresponding function key, input the password for authentication.

• Card authentication after the following settings are done : menu

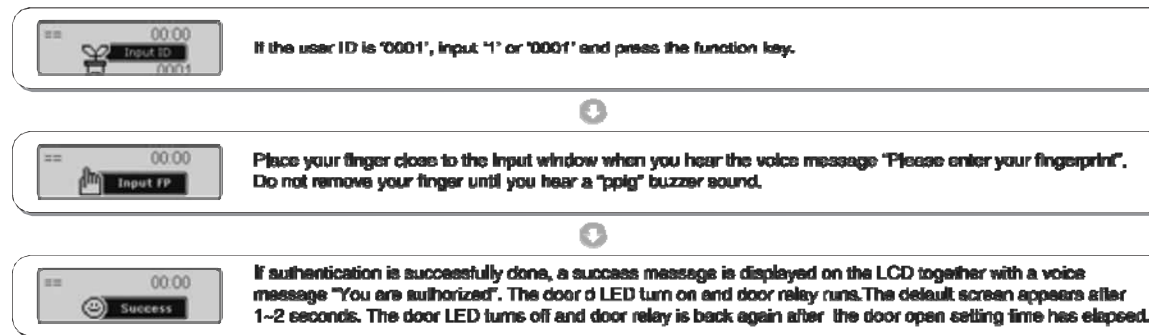
'6.Device' settings '2.Card reader' <Card Reader> is set to [1] or over

- Pressing the function key changes just authentication mode. For card authentication, press the corresponding function key and then place the card close to the terminal.

4. How to use

4.1.2. [1:1] fingerprint authentication

- When auto sensing is running, input '0001' if the user ID is '0001' and then place your finger close to the fingerprint sensor. The light on the fingerprint input window turns on to detect the fingerprint and the authentication result is displayed on the LCD window.
- If the user ID is '0001', input '0001' and press the function key. Voice information like "please enter your fingerprint" follows. When a fingerprint is inputted, the authentication result is displayed on the LCD window. is entered, the authentication result will be displayed on the LCD window.



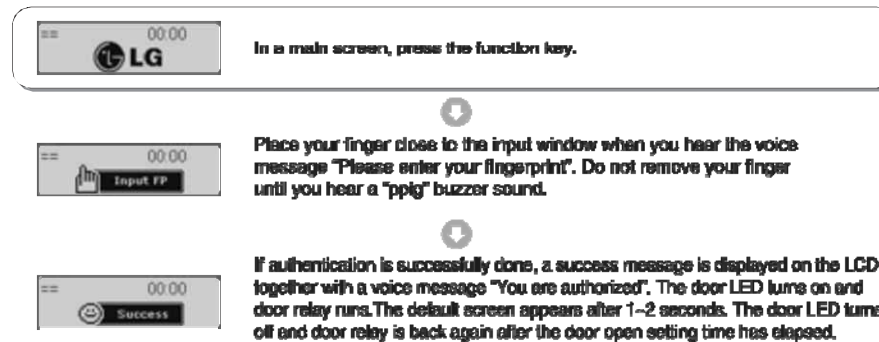
- The following error message appears together with a voice message "Please try again".



4. How to use

4.1.3. [1:N] fingerprint authentication

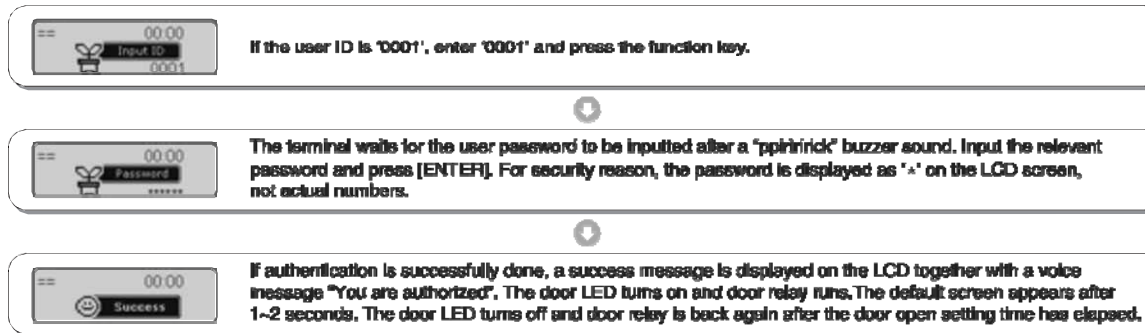
- This authentication is allowed only for users who are registered as 1:N authentication setting.
- If a user places his/her finger close to the fingerprint sensor when auto sensing is running, the light on the fingerprint input window turns on to detect the fingerprint and the authentication result is displayed on the LCD window.
- When you press the function key, voice information like "please enter your fingerprint" follows. When a fingerprint is inputted, the authentication result is displayed on the LCD window.



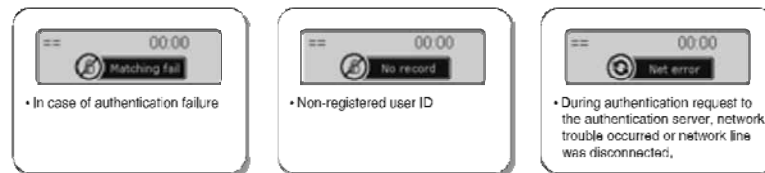
4. How to use

4.1.4. Password authentication

- If the user ID is '0001', input '0001' and press the function key. The terminal waits for the user password to be inputted after a "ppiririck" buzzer sound. Input the relevant password and press [ENTER]. The authentication result appears on the LCD.




- Error message:** An error message appears together with the voice message "Please try again"




4. How to use

4.1.5. Card authentication

- In case of a user who is registered as [RF], [RFIFP] or [RFIPW], place the card close to the terminal in main screen. After a "ppig" buzzer sound, the authentication result appears on the LCD.

 Place your card close to the terminal. It makes a "ppig" buzzer sound.


 If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs. The default screen appears after 1-2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

- Error message : An error message appears together with the voice message "Please try again"

 Non-registered card

 During authentication request to the authentication server, network trouble occurred or network line was disconnected.

- In case of a user who is registered as [RF&FP] or [ID&FP | RF&FP], place the card close to the terminal in main screen. After a "ppig" buzzer sound, the following fingerprint authentication screen appears:

 When the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint", enter your fingerprint and hold it there until you hear a "ppig" buzzer sound.

- In case of a user who is registered as [RF&PW] or [ID&PW | RF&PW], place the card close to the terminal in main screen. After a "ppig" buzzer sound, the following fingerprint authentication screen appears:

 After a "ppirirrick" buzzer sound, the terminal waits for the user password to be inputted. Enter password and press [ENTER].

4. How to use

4.1.6. User ID group authentication

- User ID group authentication is performed just among users grouped with same first digit and/or above of user ID - at least one digit. This authentication can conveniently be used if there are too many users and the matching time for 1:N authentication takes too long. In the menu, set as below: 3. Option 2. Verify option Enable 1:N <User ID Group>=1.
- For your information, refer to the followings on how to use this authentication in more details, If the relevant ID for a user is '1234', enter only '12' for this authentication. This matching is performed just among users having IDs of from '1200' to '1299', starting with '12'. If the ID is '0012', enter '0012' or '00' for authentication.



If the user ID is '1234', enter '1', '12' or '123' and then press the function key.



When the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint", enter your fingerprint and hold it there until you hear a "ppig" buzzer sound.



If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs. The default screen appears after 1-2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

4. How to use

4.1.7. Multiple fingerprint authentication

- For a door where higher security is required, multiple fingerprints captured from more than two persons are assigned to a single ID for access to the specific door. The door opens only when all the registered fingerprints are successfully authenticated. In the menu, set as below: 3. Option 2. Verify option <Enable 1:N>=0 <Verify Multi-FP>=1.
- For example, if the ID '0001' is registered with three different fingerprints, all three fingerprints must be authenticated for access after ID input. A single authentication failure in mid course results in overall failure and the whole authentication process should be restarted. This iterative process continues until all three fingerprints are authenticated.

