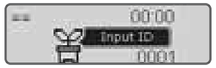
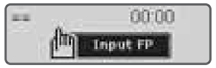
4.1.2. [1:1] fingerprint authentication

□ 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.

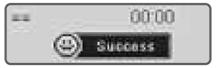
□ If the user ID is ‘0001’, input ‘0001’ and press the function key. Voice information like “please enter your fingerprint” follows. When a fingerprint is inputted, the authentication result is displayed on the LCD window. is entered, the authentication result will be displayed on the LCD window.



If the user ID is ‘0001’, input ‘1’ or ‘0001’ and press the function key.

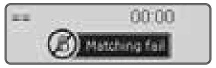


Place your finger close to the input window when you hear the voice message “Please enter your fingerprint”. Do not remove your finger until you hear a “ppig” buzzer sound.

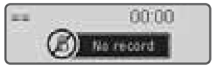


If authentication is successfully done, a success message is displayed on the LCD together with a voice message “You are authorized”. The door d LED turn on and door relay runs.The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting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

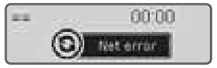
□ The following error message appears together with a voice message “Please try again”.



- In case of authentication failure



- Non-registered user ID



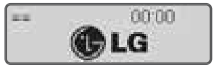
- During the authentication request to the authentication server, network trouble occurred or network line was disconnected.

4.1.3. [1:N] fingerprint authentication

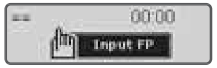
□ This authentication is allowed only for users who are registered as 1:N authentication setting.

□ 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.

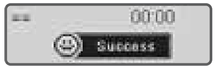
□ When you press the function key, voice information like “please enter your fingerprint” follows. When a fingerprint is inputted, the authentication result is displayed on the LCD window.



In a main screen, press the function key.

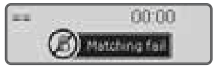


Place your finger close to the input window when you hear the voice message “Please enter your fingerprint”. Do not remove your finger until you hear a “ppig” buzzer sound.

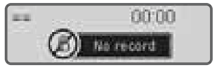


If authentication is successfully done, a success message is displayed on the LCD together with a voice message “You are authorized”. The door LED turns on and door relay runs.The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting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

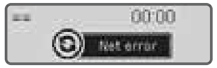
□ Error message : The following error message appears together with a voice message “Please try again”



- In case of authentication failure



- If the connection method is SN - refer to 3.4.2. Connection [NS / SN / NO] mode settings - and there is no user to whom 1:N authentication is allowed in the terminal



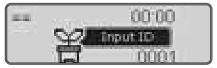
- During authentication request to the authentication server, network trouble occurred or network line was disconnected.

- In case of a user who is registered as [fingerprint & password], correct password input is required after successful fingerprint authentication.

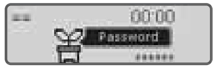
4. How to use

4.1.4. Password authentication

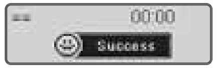
□ If the user ID is ‘0001’, input ‘0001’ and press the function key. The terminal waits for the user password to be inputted after a “ppiriririck” buzzer sound. Input the relevant password and press [ENTER]. The authentication result appears on the LCD.



If the user ID is ‘0001’, enter ‘0001’ and press the function key.

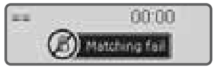


The terminal waits for the user password to be inputted after a “ppiriririck” buzzer sound. Input the relevant password and press [ENTER]. For security reason, the password is displayed as ‘*’ on the LCD screen, not actual numbers.

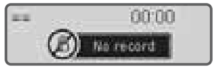


If authentication is successfully done, a success message is displayed on the LCD together with a voice message “You are authorized”. The door LED turns on and door relay runs.The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting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

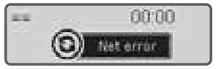
□ Error message: An error message appears together with the voice message “Please try again”



- In case of authentication failure



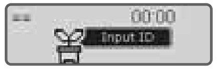
- Non-registered user ID



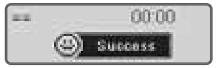
- During authentication request to the authentication server, network trouble occurred or network line was disconnected.

4.1.5. Card authentication

□ In case of a user who is registered as [RF], [RF|FP] or [RF|PW], place the card close to the terminal in main screen. After a “ppig” buzzer sound, the authentication result appears on the LCD.

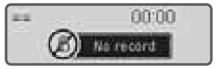


Place your card close to the terminal. It makes a “ppig” buzzer sound.

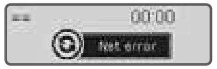


If authentication is successfully done, a success message is displayed on the LCD together with a voice message “You are authorized”. The door LED turns on and door relay runs.The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting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

□ Error message : An error message appears together with the voice message “Please try again”

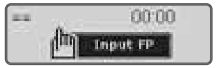


Non-registered card



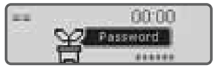
During authentication request to the authentication server, network trouble occurred or network line was disconnected.

□ 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:

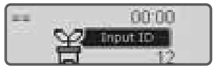


After a “ppiriririck” buzzer sound, the terminal waits for the user password to be inputted. Enter password and press [ENTER].

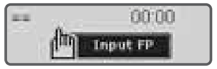
4.1.6. User ID group authentication

□ 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.

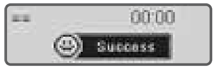
□ For your information, refer to the followings on how to use this authentication in more details, If the relevant ID for a user is ‘1234’, enter only ‘12’ for this authentication. This matching is performed just among users having IDs of from ‘1200’ to ‘1299’ , starting with ‘12’. If the ID is ‘0012’, 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.

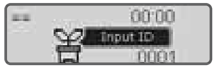


If authentication is successfully done, a success message is displayed on the LCD together with a voice message “You are authorized”. The door LED turns on and door relay runs.
The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting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

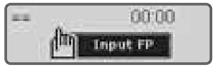
4.1.7. Multiple fingerprint authentication

□ 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.

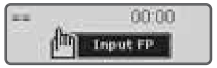
□ For example, if the ID ‘0001’ is registered with three different fingerprints, all three fingerprints must be authenticated for access after ID input. A single authentication failure in mid course results in overall failure and the whole authentication process should be restarted. This iterative process continues until all three fingerprints are authenticated.



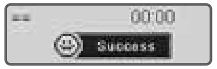
If the user ID is ‘0001’, input ‘0001’ and press the function key.



Place your finger close to the input window when you hear the voice message “Please enter your fingerprint”. Do not remove your finger until you hear a “ppig” buzzer sound.



If authentication is successfully done, a “ppiririck” buzzer sounds and the light on the fingerprint input window turns on together with the voice message “Please enter your fingerprint”. This iterative process continues until all inputted fingerprints have been authenticated.



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.

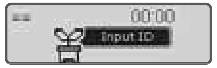
□ Error message is same as that of [1:1] authentication.

4.2. Time & Attendance control

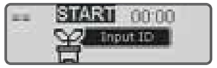
□ Default screen ➔ [*] ➔ [3] Option ➔ [1] Application ➔ [1] T&A (Time Attendance) settings

□ If start and leave time for employees are fixed, set <start time>, <leave time> and <normal time> to reduce user input errors.

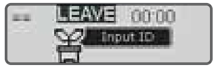
4.2.1. Authentication mode



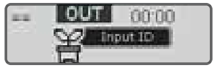
- Normal mode; authentication with [ENTER]



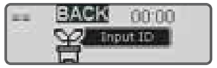
- Start mode; authentication with [F1]



- Leave mode; authentication with [F2]



- Outside work mode; authentication with [F3]



- Return mode; authentication with [F4]

- Fingerprint authentication
  - Press the function key which is related to specific T & A mode.If the function key is not used and authentication process is done in auto sensing, the current mode on the screen is working for authentication.
- 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.
  - After authentication is done, working mode returns to the mode - start, leave or normal - previously set as time frames but if no mode is set for the specific time period, the previous authentication mode is maintained.
- [1:1] fingerprint authentication : Same as ‘4.1.2.’. [1:N] fingerprint authentication : Same as ‘4.1.3.’. Password authentication : Same as ‘4.1.4.’ Card authentication : Same as ‘4.1.5.’. User ID group authentication : Same as ‘4.1.6.’

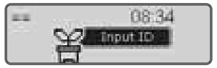
4.2.2. Expansion of working mode by multi-key function

□ If more than 5 working modes - start, leave, outside work (out), return (back) and normal - are required, it can be expanded up to 41 modes.

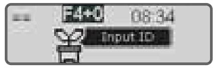
□ After setting Menu ➔ 3.Option ➔ 1.Application ➔ [1] T&A, set more than one key to ‘O’ in <Multi Fn-key> setting. The keys set to ‘X’ are not applied in this multi-key function.

□ As a mode is defined as a function key plus a number key, press a number key after pressing the function key for authentication. In the server program, authentication mode is displayed as a function key plus a number key like ‘F3+1’.

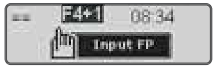
□ For example, when [F4] is set to [O] and <start time> is set to ‘07:00~09:30’, if a fingerprint user tries for authentication in ‘F4+1’mode,



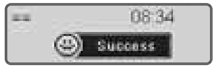
• In main screen, press [F4].



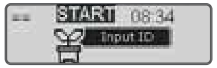
• The mode is changed to ‘F4+0’.



• When the mode is changed to ‘F4+1’, enter the fingerprint.



• When authentication is successfully done, a success message appears.



• The current time is 08:34, so it returns to the start mode.

4.3. For using as meal management system

□ Default screen ➔ [*] ➔ [3] Option ➔ [1] Application ➔ [2] Setting up to meal

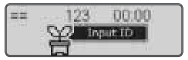
□ When setting up meal management, a user must input at least one mealtime because the terminal is locked except for mealtime.

□ Each user can authenticate only once for each meal and multiple authentications are not allowed, but multiple authentications by using [ENTER] key are allowed.

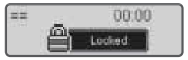
□ If multiple authentications should not be allowed under any circumstances, go to
Default screen ➔ [*] ➔ [6] Device settings ➔ [1] Function key ➔ Setting up to Ent=[X] at <KeyOn/Off>.

4.3.1. Meal Classification

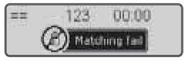
□ Function key is used as manipulating key for authentication and can only classify meal based on mealtime without mode classification. The number placed in the upper center of screen displays the number of authentications for each mealtime.



- Total successful authentications for each mealtime.



- When it is not mealtime



- When user attempts to try duplicate authentication in the same mealtime

- In case of authentication by fingerprint, authentication is available by auto sensing function without pressing Enter or function key.
- For password authentication Input user ID and function key and press password
- For card authentication
  (ex:Default screen ➔ [*] ➔ [6] Device settings ➔ [3] Card reader ➔ <Card Reader>= more than 1)
  Punch card for authentication

4.3.2. [1:1] Fingerprint authentication

□ Same as 4.1.2. but [ENTER] key is not available

4.3.3. [1:N] Fingerprint authentication

□ Same as 4.1.3. but [ENTER]

4.3.4. Password authentication

□ Same as 4.1.4. but [ENTER] key is not available

4.3.5. Card authentication

□ Same as 4.1.5. but [ENTER] key is not available

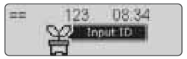
4.3.6. User ID group authentication

□ Same as 4.1.6. but [ENTER] key is not available

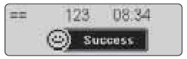
4.3.7. Allowing multiple authentications

□ Default screen ➡ [ENTER] ➡ [6] Device settings ➡ [1] Function key ➡ Must be setting as Ent=[O] on <Key On/Off>
(For initializing, edit is not needed since default setting value is [O], but it needs to be checked if it is not working.)

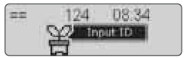
□ For multiple fingerprint authentications


123 08:34 Input ID

- Input fingerprint while pressing [ENTER] button from the default screen

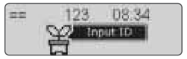

123 08:34 Success

- Displaying a success message when authentication is successful

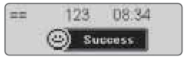

124 08:34 Input ID

- The number of meal times increases once the screen returns to the default

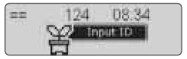
□ For multiple card user authentications


123 08:34 Input ID

- Input card with pushing [ENTER] key on the basic screen

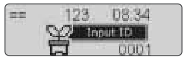

123 08:34 Success

- Displaying a success message when authentication is successful

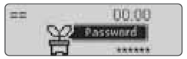

124 08:34 Input ID

- The number of meal times increases once the screen returns to the default

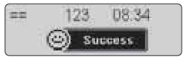
□ For multiple password authentications


123 08:34 Input ID 0001

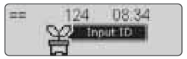
- Input a function key (one of [F1], [F2], [F3], [F4]) with pushing [ENTER] key after inputting user ID on the basic screen


00:00 Password ******

- It is a screen to wait for inputting user's password with a beep sound. Push [ENTER] key after inputting password.


123 08:34 Success

- Displaying a success message when authentication is successful


124 08:34 Input ID

- The number of meal times increases once the screen returns to the default

LG

P/N : MFL62730801