SVA-SHP-FV-00113-1

SecuaVeinAttestor

セキュアベインアテスター

FVTC720 series
Finger Vein Access Control System
Manual (Authentication Operation part)

Hitachi Information & Control Solutions, Ltd.

NOTICE

FCC Regulatory Information(§15.105)

Note: 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.

FCC WARNING

Change or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

Properly shielded and grounded cables and connectors must be used for connection to peripherals in order to meet FCC emission limits.

Precautions

○ Before you use the Finger Vein Access Control System, please read this guide carefully and gain thorough understanding of the instructions and cautions.

○ Please keep this guide handy (but keep away from being seen by normal users) for your quick reference as needed.

○ If you have questions about the descriptions in this guide, please contact the vendor from whom you purchased this product.

○ We are not responsible for any accidents or damage caused by improper operation.

○ If you find any malfunctions or abnormal state such as unusual odor or heat, please shut down the device and contact the vendor from whom you purchased the product.

○ Do not use the device in the places where it is exposed to extreme high/low temperatures, large temperature fluctuations, direct sunlight, high humidity, much dust, noise, water, and/or chemicals.

○ If the finger vein scanner gets dirty, it may not work properly. Please keep the scanner clean for secure authentication.

○ Depending on how the finger is placed on the finger-vein scanner, the success rate of the authentication may deteriorate. Practice scanning before registering your finger vein pattern.

○ To use the "1:N" type authentication, the finger vein pattern must be registered correctly and its quality checked and verified after registration. To improve identification reliability, it is recommended that you use the "1:1" authentication type ("ID plus Finger Vein" or "Card plus Finger Vein" authentication type).

○ A door failure indicates that the door is left open. Check that the door is closed.

○ A key failure indicates that the key did not work properly. Check that the lock is engaged.

○ An unhealthy user may not be properly identified because the device employs biometric authentication technology. If the system is in operation with no administrator who has the master key to the door, the door must also be able to be unlocked with a key (mechanical key).

○ An unhealthy user may not be properly identified because the device employs biometric authentication technology. If you want to use the device for exit control, install an electric thumb-turn key for evacuation in case of an emergency.

○ The door does not close after the alarm-box-sync test. This is normal. The door resumes normal operation after DI signals from the fire alarm are restored.

○ In case of an emergency such as a fire, the point to which power will be supplied is not known in advance. There could be a power loss to this device or disconnection of cables. An appropriately safe electrical lock should be selected by SIer, Inc., and the distributor, at system design. If the door is set to be locked with power on, it will unlock in case of a power failure, and vice versa.

○ Personal information such as the registered data may be lost due to malfunctions, etc Back up the data periodically to secure your data. If personal data is lost, you need to register it again for the standalone type vein authentication system.

○ Duplicating or copying all or any part of this guide, without consent, is strictly prohibited.

○ This guide is subject to change without notice in accordance with device upgrades, etc.

○ Especially for the use under the circumstances in which a malfunction cause a life-threatening condition, this product is not assumed to be installed with other devices/systems. Do not use this product under the circumstances mentioned above.

○ Implantable medical appliance carries should always keep more than 22 cm between the insertion site from the authentication terminal.

Disclaimer

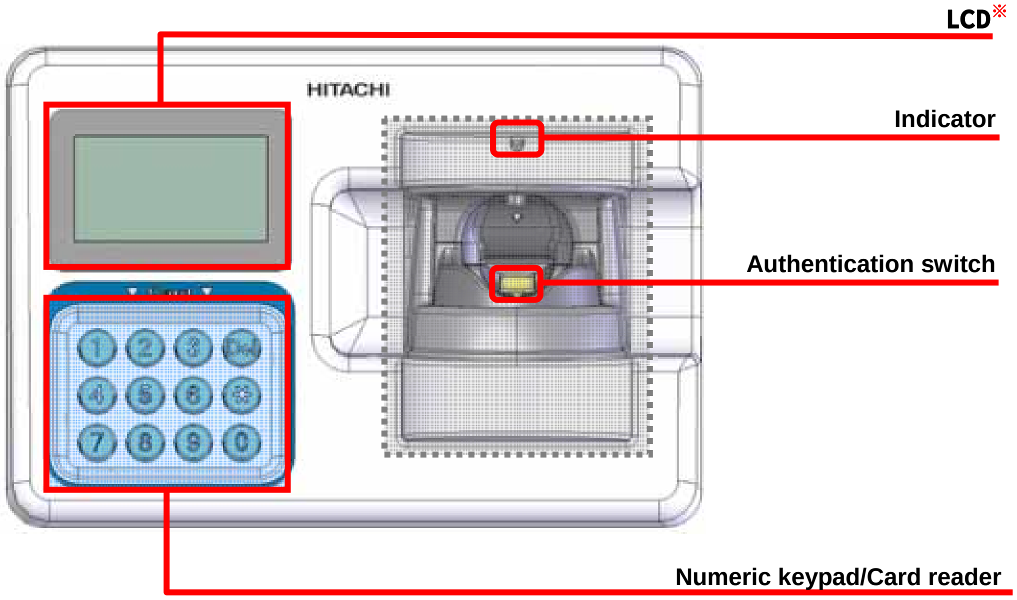
This product is intended for authenticating a person by matching finger veins. Thus, we do not guarantee that the product itself prevents criminal offenses, such as theft.
We are not responsible in the following cases:

1) Accidental, unusual, or inevitable injury or damage caused directly or indirectly by the product
2) Accidental or willful damage or malfunction caused by user's improper use or inattention
3) If the device is modified or altered by a party other than us after it is delivered, damage caused by this modification or alteration, or all malfunctions or damage caused by failure of the device regardless of the cause
4) Damage caused by software that is developed or modified by others
5) Damage or malfunction caused by lack of periodic maintenance, or improper maintenance
6) Damage or malfunction caused by using other than the genuine parts defined as the expendable supplies or replacement parts
7) Hardware defects that are not reported within the warranty period or damage caused by your contract delinquency
8) Damage or malfunction caused by poor maintenance
9) Inconvenience or damage that arises when the system fails to authenticate a registered user due to a problem including device failure or malfunctions
10) Malfunctions caused by a system configured with a third-party optional device that you purchased, or consequent inconvenience, loss, or damage
11) Damage or complaints caused by loss or leak of finger vein data stored in the ID management server, IC card or memory (Finger vein information is personal data. User has responsibility for controlling finger vein data stored in the ID management server, IC card or memory. You have responsibility for managing finger vein data stored in the ID management server, IC card or memory.)
12) Any software or hardware products that you purchased or obtained as well as damage caused by them.
13) Damage caused by operating beyond the scope of the contract specifications
14) Damage caused by hardware and/or software products which we delivered, under your approval, without customization for fitting to the client’s existing system.
15) Damage caused by software and/or data that you provided
16) Damage caused by the actions that you are responsible for.
17) Damage caused by configuration faults or operation delays caused by incomplete materials, data or information that you provided
18) Damage caused by natural disasters, or similar events
19) Hardware defects that are not reported within the warranty period or damage caused by your contract delinquency

Table of Contents

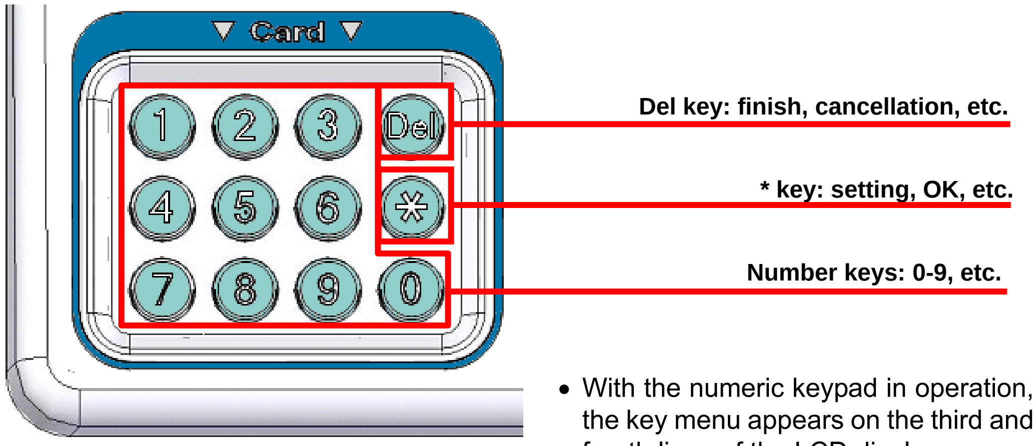
1 Authentication Terminal Interface

■Authentication Terminal



A card reader is installed in the interior of the numeric keypad. Hold the card here to scan.

■Numeric Keypad



- With the numeric keypad in operation, the key menu appears on the third and fourth lines of the LCD display.
  The location of the key menu varies depending on the display.

※ In this guide, the horizontal lines are used on the LCD display for better view.
The horizontal lines do not appear on the LCD display actually.

2 Authentication Mode Type and Operation

The authentication modes are as follows:
Each authentication mode has its own operation method. Check with the administrator for authentication.

■**Card Authentication**

Hold the card over the authentication device (with the card only).

■**Card + Finger vein authentication**

Hold the card over the authentication device and scan the finger vein.

■**Card + PIN authentication**

Hold the card over the authentication device and enter the PIN with the numeric keypad.

PIN: a password that you can arbitrarily set

■**ID + Finger vein authentication**

Using the numeric keypad, enter the user ID is not the authentication device, and then scan the finger vein.

■**ID + PIN authentication**

Using the numeric keypad, enter the PIN into the authentication device..

■**Finger Vein Authentication**

Scan the finger vein.

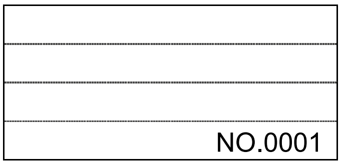
■**Authentication group NO + Finger vein authentication**

Using the numeric keypad, input the group number into the authentication device, then scan the finger vein.

This item is not available with the stand-alone type.

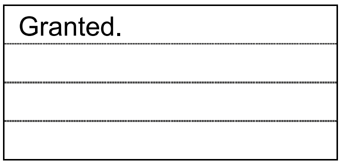
2.1 Card Authentication

1 Hold your card over the numeric keypad during the stand-by mode.


NO.0001

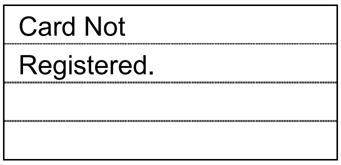
■**When granted successfully**

A successful message is displayed and the door is unlocked.


Granted.

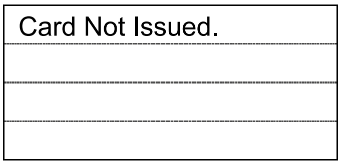
■**When the card is not registered**

"Card Not Registered" message is displayed.
The user is not registered to the auth. terminal.
Please contact an administrator to use the card.


Card Not
Registered.

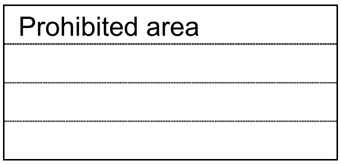
■**When the card is not granted for the terminal**

"Card Not Issued" message is displayed.
You do not have the permission to use the anth. terminal.
Please contact an administrator to use the card.
(This message is not displayed for the stand-alone type.)


Card Not Issued.

■**When entry/exit is not permitted**

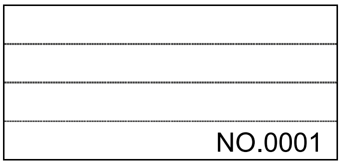
Prohibited area screen is displayed.
Entry/exit is not permitted for this room.
Please contact an administrator to enter/exit.
(This message is not displayed for the stand-alone type.)


Prohibited area

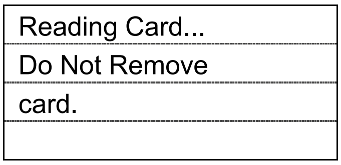
2.2 Card + Finger vein authentication

1 Hold your card over the numeric keypad during the stand-by mode.

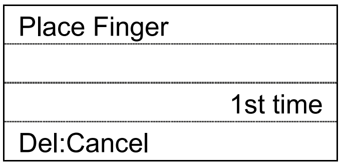
"Reading Card" message is displayed after the card is recognized. After the card reading is completed, a vein authentication message appears.


NO.0001

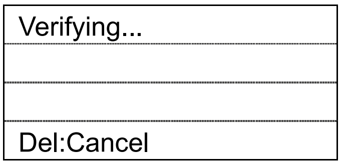
*When you have already registered finger vein information in the card, the window on the right appears during scanning.
Do not remove the card before the operation guide LED starts flickering green.


Reading Card...
Do Not Remove
card.

2 Insert a finger into the terminal device ► Press the auth. button inside the device with the inserted finger.
When also using Card + PIN authentication, entering PIN with numeric keypad switches to Card + PIN authentication.

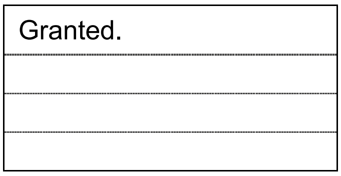

Place Finger
1st time
Del:Cancel

Press the authentication button


Verifying...
Del:Cancel

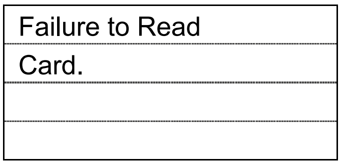
■When the card reading and the finger vein authentication have succeeded

A successful message is displayed and the door is unlocked.


Granted.

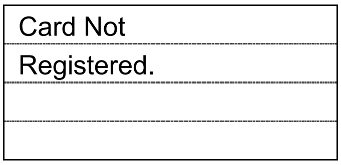
■When the card is unreadable

"Failure to Read Card" message is displayed.
Confirm that the card is absolutely yours, then hold it over the auth. terminal again.
Do not remove the card before the reading is completed.


Failure to Read
Card.

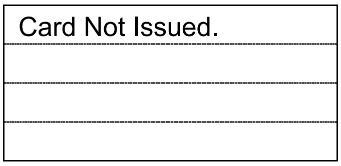
■When the card is not registered

"Card Not Registered" message is displayed.
The user is not registered to the auth. terminal.
Please contact an administrator to use the card.


Card Not
Registered.

■When the card is not granted for the terminal

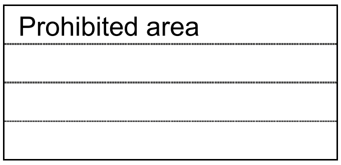
"Card Not Issued" message is displayed.
You do not have the permission to use the anth. terminal.
Please contact an administrator to use the card.
(This message is not displayed for the stand-alone type.)



Card Not Issued.

■When entry/exit is not permitted

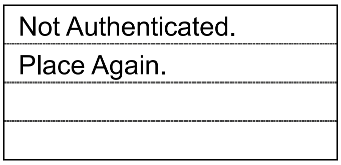
Prohibited area screen is displayed.
Entry/exit is not permitted for this room.
Please contact an administrator to enter/exit.
(This message is not displayed for the stand-alone type.)



Prohibited area

■When the finger-vein authentication failed

A message prompts you to try again.
Again, insert the finger into the terminal device, then press the auth. button inside the device with the inserted finger.



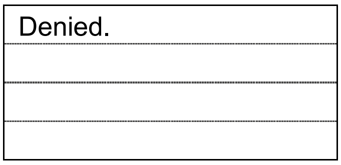
Not Authenticated.
Place Again.

■When authentication failed 4 times

An error message is displayed.
Please follow the steps below.

- Confirm whether the finger is registered one or not
- Try another finger that is already registered
- Please note the descriptions in "4 Finger-Vein Authentication" to retry authentication operation.

If you are still denied, contact an administrator.

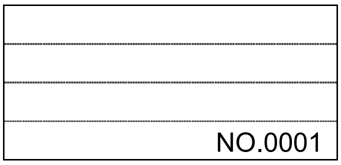


Denied.

2.3 Card + PIN authentication

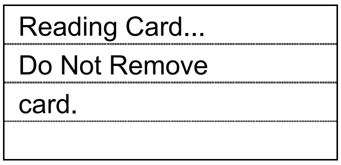
1 Hold your card over the numeric keypad during the stand-by mode.

"Reading Card" message is displayed after the card is recognized. After the card reading is completed, a PIN authentication message appears.



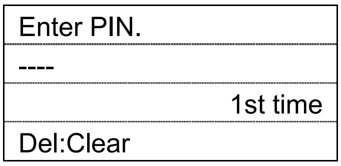
NO.0001

*When you have already registered finger vein information in the card, the window on the right appears during scanning.



Reading Card...
Do Not Remove
card.

2 Enter all digits of a PIN with the numeric keypad.

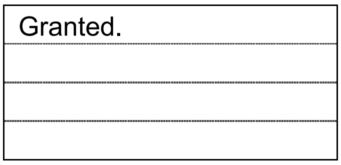


Enter PIN.

1st time
Del:Clear

■**When granted successfully**

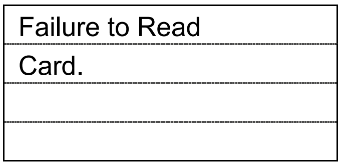
A successful message is displayed and the door is unlocked.



Granted.

■**When the card is unreadable**

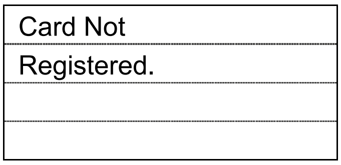
"Failure to Read Card" message is displayed. Confirm that the card is absolutely yours, then hold it over the auth. terminal again.



Failure to Read
Card.

■**When the card is not registered**

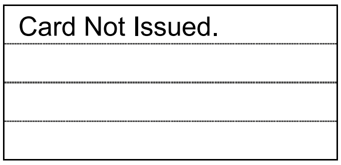
"Card Not Registered" message is displayed.
The user is not registered to the auth. terminal.
Please contact an administrator to use the card.



Card Not
Registered.

■**When the card is not granted for the terminal**

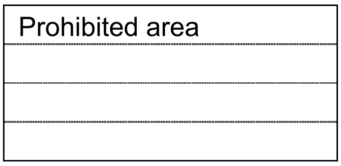
"Card Not Issued" message is displayed.
You do not have the permission to use the anth. terminal.
Please contact an administrator to use the card.
(This message is not displayed for the stand-alone type.)



Card Not Issued.

■When entry/exit is not permitted

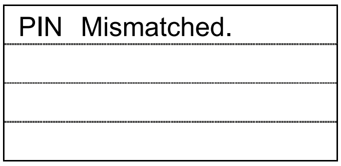
Prohibited area screen is displayed.
Entry/exit is not permitted for this room.
Please contact an administrator to enter/exit.
(This message is not displayed for the stand-alone type.)



Prohibited area

■When PIN is mismatched

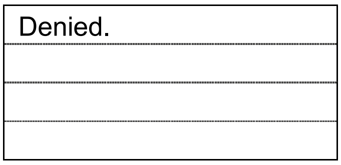
"PIN Mismatched" message is displayed.
The PIN entry dialog automatically reappears, then enter PIN again.



PIN Mismatched.

■When authentication failed 4 times (with the number of authentication retries set to 3 times)

An error message is displayed.
The PIN number might be incorrectly memorized.
The card may be damaged, or the user information may not be registered correctly.
Please contact an administrator.



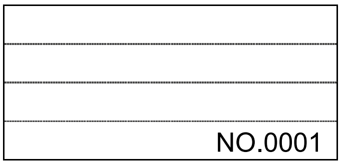
Denied.

2.4 ID + Finger vein authentication

1 Enter your user ID with the numeric keypad during the stand-by mode ► [*].

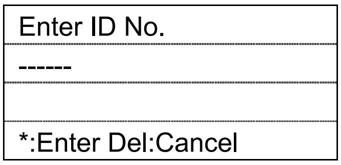
After pressing the first digit, you will be prompted to push the others. Make sure to enter an asterisk "*" at the end.
After your ID is granted, proceed to the finger-vein authentication process.

When you enter all the digits of the user ID including first "0", the last "" can be omitted.



```
                 NO.0001
```

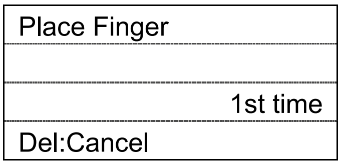
Enter your user ID



```
Enter ID No.
------

*:Enter Del:Cancel
```

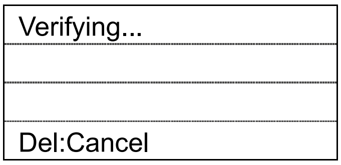
2 Insert a finger into the terminal device ► Press the auth. button inside the device with the inserted finger.
When also using ID + PIN authentication, entering PIN with numeric keypad switches to ID + PIN authentication.



```
Place Finger

                1st time
Del:Cancel
```

Press the authentication button

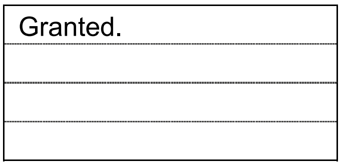


```
Verifying...


Del:Cancel
```

■**When granted successfully**

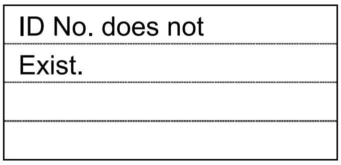
A successful message is displayed and the door is unlocked.



```
Granted.
```

■**When user ID has not been registered (error)**

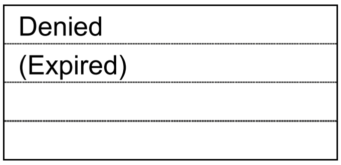
A user ID input error message appears.
Confirm whether the user ID is correct or not.



```
ID No. does not
Exist.
```

■**When user ID expired (validity date expired)**

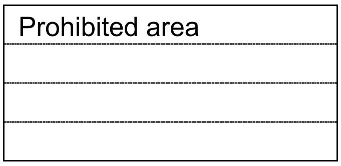
A user ID invalidity message appears.
Your user ID is invalid. Check with the administrator.
(This message is not displayed for the stand-alone type.)



```
Denied
(Expired)
```

■**When entry/exit is not permitted**

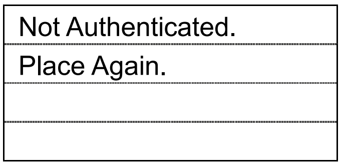
Prohibited area screen is displayed.
Entry/exit is not permitted for this room.
Please contact an administrator to enter/exit.
(This message is not displayed for the stand-alone type.)



Prohibited area

■**When the finger-vein authentication failed**

A message prompts you to try again.
Again, insert the finger into the terminal device, then press the auth. button inside the device with the inserted finger.



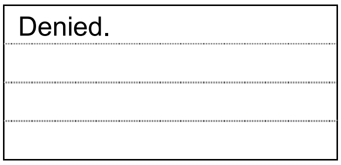
Not Authenticated.
Place Again.

■**When authentication failed 4 times (with the number of authentication retries set to 3 times)**

An error message is displayed.
Please follow the steps below.

- Confirm whether the user ID is correct or not.
- Confirm whether the finger is registered one or not
- Try another finger that is already registered
- Please note the descriptions in "4 Finger Vein Authentication" to retry authentication operation.

If you are still denied, contact an administrator.



Denied.

2.5 ID + PIN authentication

1 Enter your user ID with the numeric keypad during the stand-by mode ▶ [*].

After pressing the first digit, you will be prompted to push the others. Make sure to enter an asterisk "*" at the end.
After your ID is granted, proceed to the PIN authentication process.

When you enter all the digits of the user ID including first "0", the last "" can be omitted.

```



                    NO.0001
```

Enter your user ID

```
Enter ID No.
------

*:Enter Del:Cancel
```

2 Enter all digits of a PIN with the numeric keypad.

```
Enter PIN.

                   1st time
Del:Clear
```

A successful message is displayed and the door is unlocked.

```
Granted.



```

■When user ID has not been registered (error)

A user ID input error message appears.
Confirm whether the user ID is correct or not.

```
ID No. does not
Exist.


```

■When user ID expired (validity date expired)

A user ID invalidity message appears.
Your user ID is invalid. Check with the administrator.
(This message is not displayed for the stand-alone type.)

```
Denied
(Expired)


```

■When entry/exit is not permitted

Prohibited area screen is displayed.
Entry/exit is not permitted for this room.
Please contact an administrator to enter/exit.
(This message is not displayed for the stand-alone type.)

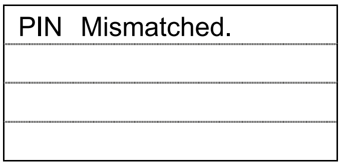
```
Prohibited area



```

■**When PIN is mismatched**

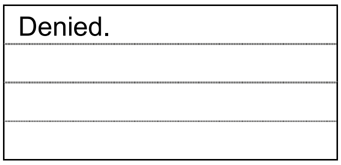
"PIN Mismatched" message is displayed.
The PIN entry dialog automatically reappears, then enter PIN again.



PIN Mismatched.

■**When authentication failed 4 times (with the number of authentication retries set to 3 times)**

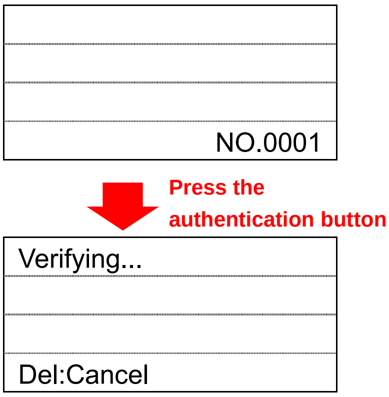
An error message is displayed.
The PIN number might be incorrectly memorized.
The user information may not be registered correctly.
Please contact an administrator.



Denied.

2.6 Finger Vein Authentication

1 In stand-by mode, insert a finger into the terminal device ▶ Press the auth. button inside the device with the inserted finger.


NO.0001

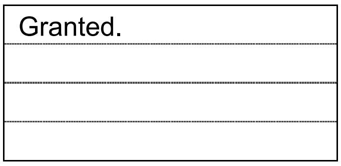
Verifying...

Del:Cancel

■**When granted successfully**

A successful message is displayed and the door is unlocked.

The more finger veins you have registered, the longer the authentication operation takes.


Granted.

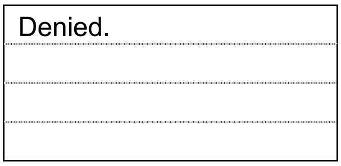
■**When authentication failed**

An error message is displayed.

Please follow the steps below.

- Confirm whether the finger is registered one or not
- Try another finger that is already registered

If you are still denied, contact an administrator.


Denied.

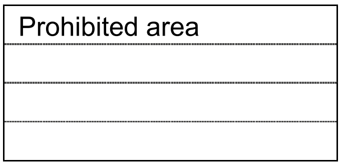
■**When entry/exit is not permitted**

Prohibited area screen is displayed.

Entry/exit is not permitted for this room.

Please contact an administrator to enter/exit.

(This message is not displayed for the stand-alone type.)


Prohibited area

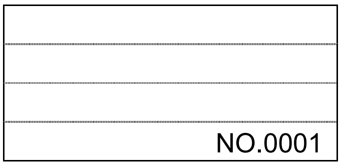
2.7 Authentication group NO + Finger vein authentication

***This function is not available with the stand-alone type.**

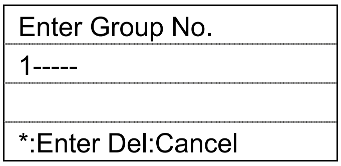
1 Enter your authentication group No with the numeric keypad during the stand-by mode ► [*].

After pressing the first digit, you will be prompted to push the others. Make sure to enter an asterisk "*" at the end.
After your ID is granted, proceed to the finger-vein authentication process.

When you enter all the digits of the user ID including first "0", the last "" can be omitted.

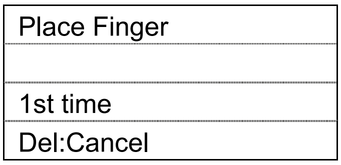

NO.0001

Enter Authentication group No


Enter Group No.
1-----

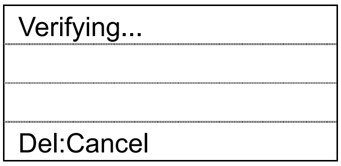
*:Enter Del:Cancel

2 Insert a finger into the terminal device ► Press the auth. button inside the device with the inserted finger.


Place Finger

1st time
Del:Cancel

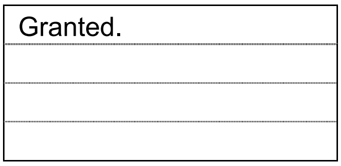
Press the authentication button


Verifying...

Del:Cancel

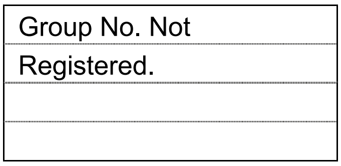
■When granted successfully

A successful message is displayed and the door is unlocked.


Granted.

■When authentication group No has not been registered

An authentication group entry error message appears.
The entry window automatically opens again. Specify the authentication group No again.


Group No. Not
Registered.

■When entry/exit is not permitted

Prohibited area screen is displayed.
Entry/exit is not permitted for this room.
Please contact an administrator to enter/exit.
(This message is not displayed for the stand-alone type.)

Prohibited area

■When the finger-vein authentication failed

A message prompts you to try again.
Again, insert the finger into the terminal device, then press the auth. button inside the device with the inserted finger.

Not Recognized.
Place Again.

■When authentication failed 4 times (with the number of authentication retries set to 3 times)

An error message is displayed.
Please follow the steps below.

- Confirm whether the finger is registered one or not
- Try another finger that is already registered
- Please note the descriptions in "4 Finger Vein Authentication" to retry authentication operation.

If you are still denied, contact an administrator.

Denied.

3 Clocking Authentication Operation

The following explains an authentication method of clocking.

***This function is not available with the stand-alone type.**

3.1 Clocking Definition

Clocking is to log and output the authentication time stamps.

When the authentication operation of clocking is enabled, CLK is displayed on the left bottom of the authentication terminal screen.

Setting the clocking schedule allows you to record the authentication time, such as "Clock-in" and "Clock-out" in the same way as in timecard.

Setting method ⇒ "8.3 Setting Clocking Schedule" in "Manual (Operation)"

Any number that you can set is "Clocking Operation No".

There are two types of authentication of clocking. They are:

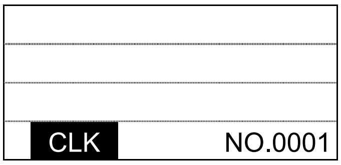
- Inputting clocking operation No
- Not inputting clocking operation No

3.2 Authentication Method

■Inputting clocking operation No

1 Enter [*] and clocking operation No (any number from [0] to [9]) with the numeric keypad during the stand-by mode.

The clocking schedule menu opens.

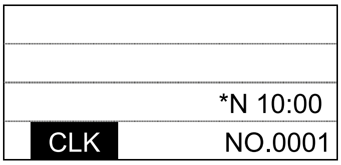


CLK NO.0001

2 Perform normal authentication operation.

About a clocking mode’s display

*N ：Clocking No



*N 10:00

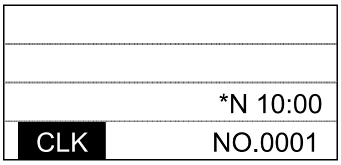
CLK NO.0001

*Before the authentication operation, always check the clocking operation No is correct.

If the entered clocking operation No is incorrect, log output fails.

■Not inputting clocking operation No

For the time frame during which a clocking schedule is set, a clocking operation No and time are displayed on the bottom left of the terminal screen.

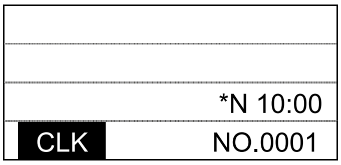


*N 10:00

CLK NO.0001

Entering a clocking operation No is not required.

1 Perform normal authentication operation.



*N 10:00

CLK NO.0001

About a clocking mode’s display

*N ：clocking operation No (the number set in the clocking schedule of the ID Management Server)

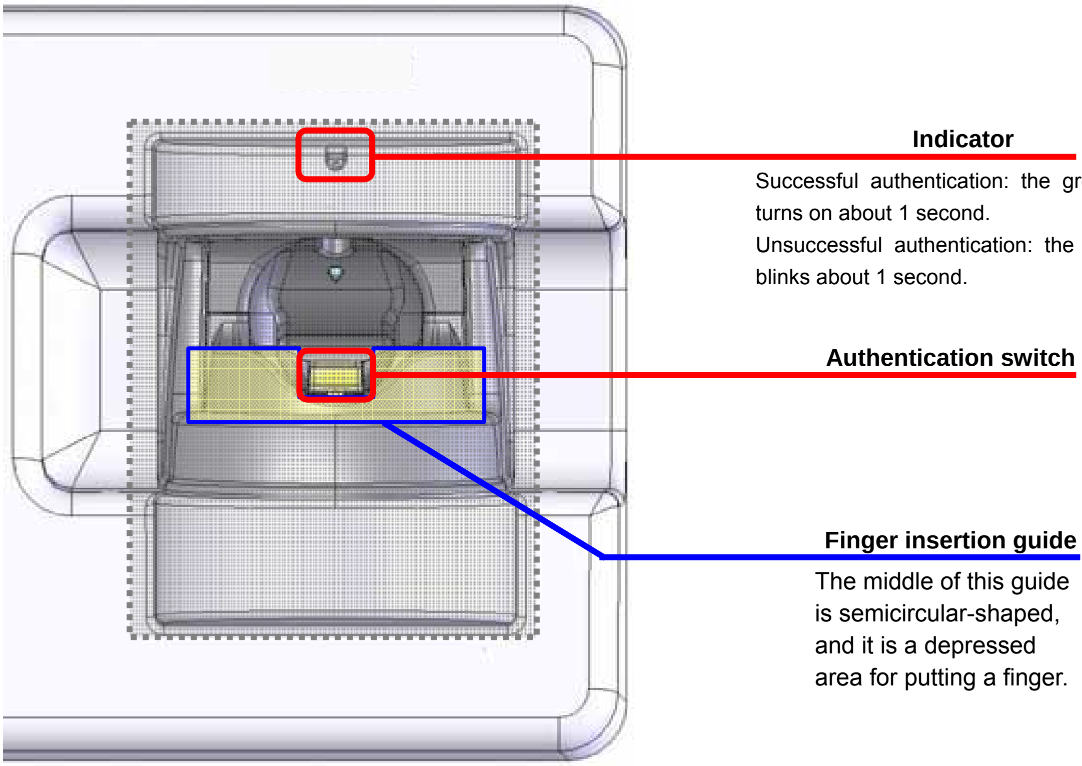
*For the authentication type not inputting clocking operation No, some system settings allow "clocking operation No" entry using numeric keypad. In this case, "clocking operation No" entry using numeric keypad takes priority.

Check with the administrator regarding the system setting.

4 Finger-Vein Authentication

The following shows how to insert the finger and how the authentication function works.

4.1 Finger Vein Scanner Description



Indicator

Successful authentication: the green light turns on about 1 second.
Unsuccessful authentication: the red light blinks about 1 second.

Authentication switch

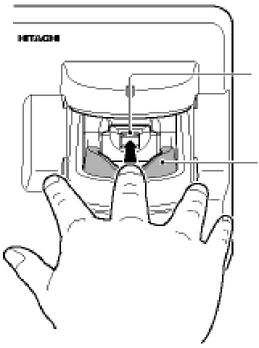
Finger insertion guide

The middle of this guide is semicircular-shaped, and it is a depressed area for putting a finger.

4.2 How to Scan Finger Vein

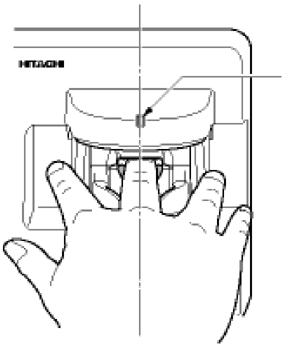
1 Put the finger properly on the depressed area of the finger insertion guide.

- Do not make the finger tight.
- Insert the finger as far as to the authentication switch so that the finger tip can touch it.
- Straighten the finger.



2 Touch the authentication switch ▶ Put the finger cushion lightly on the finger authentication guide.

- Align the center of the finger back with the center of the operation guide LED.



3 Press the authentication switch lightly with the finger tip.

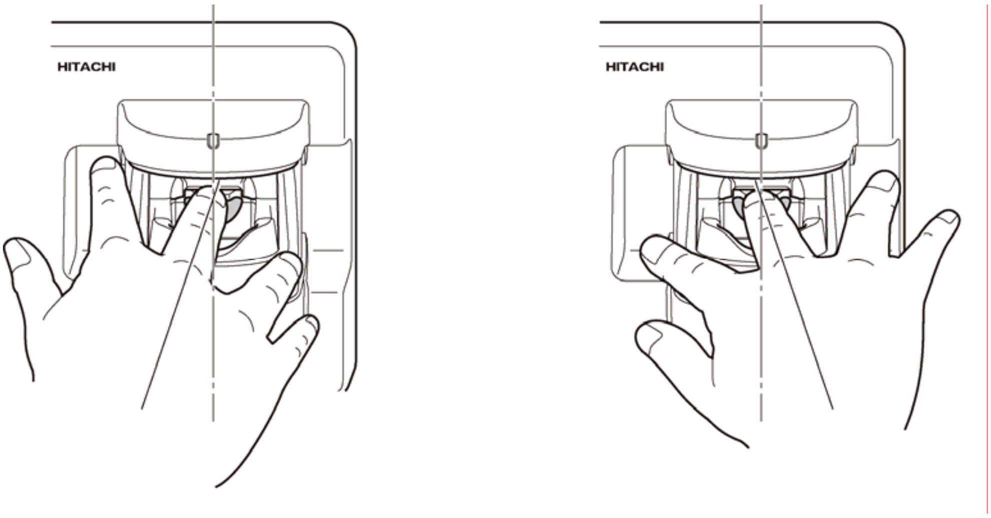
The beeper sounds when the authentication is successfully completed.

***Do not move the finger until the authentication is completed.**

4.3 Notes for Scanning Finger Vein

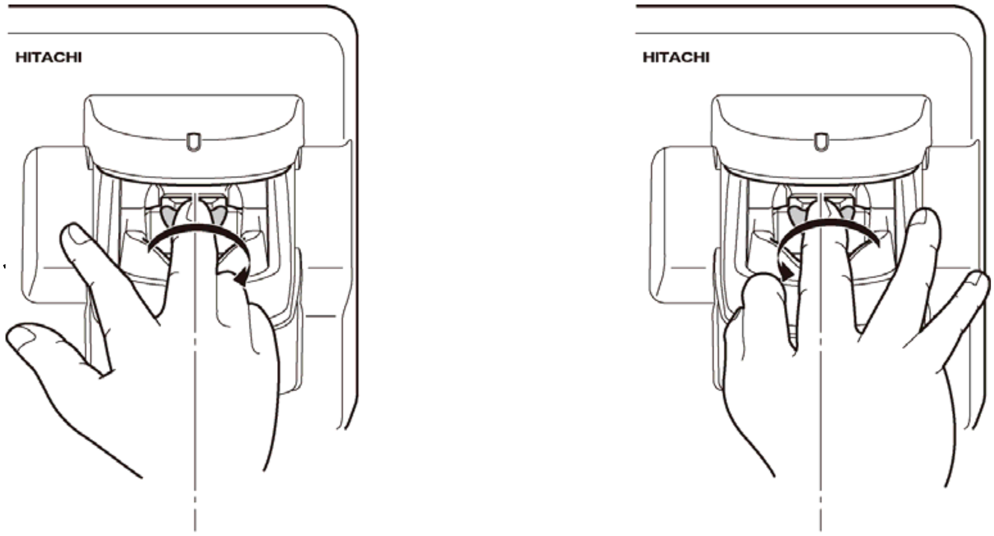
The authentication function may not work in any of the following cases.

- If the finger is tight or stiff
- If the finger is not straight forward
- If the finger is wet
- If you are wearing a glove
- If the finger is chapped
- If the finger is scarred (If the finger has a band-aid on it)
- If the finger is cold
- If the finger is stained with ink
- If the finger is dirty
- If the finger is affected due to some kind of work
- If you move the finger before authentication is completed and the beeper sounds
- If you are pressing the finger onto the finger plate
- If the finger is not in the proper position



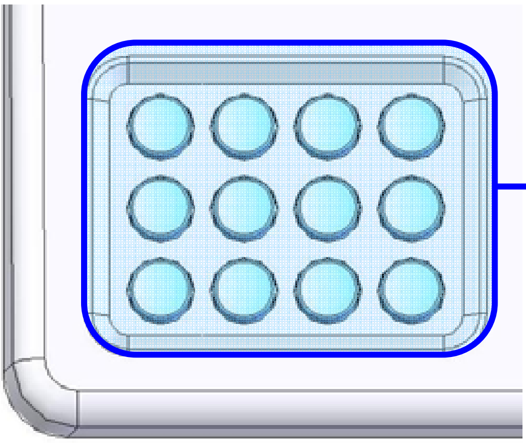
- If the finger is rotating

  *For a better visibility of the whole device, the other fingers in each of the illustrations below are not straight forward.



5 Card Authentication

5.1 Card Reader Description



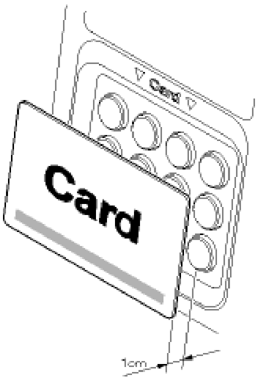
Card reader

The whole blue section in this illustration is called the card reader.

5.2 How to Scan Card

1 Hold the card close to the card reader

- · Do not press the card onto the card reader. The numeric keypad may be accidentally pressed
- · Making the card and the card reader parallel, move them closer.
- · The most preferable distance between the card and the card reader is approximately 1 cm.



5.3 Precautions for Card Use

The authentication function may not work in any of the following cases.

- ● If the card is deformed or damaged
- ● If the card has been soaked in water
- ● If you hold the card 3 or more cm over the card reader
- ● If you move the card before the card reading is completed
- ● If the card is placed under the other card
- ● With the card stored in a card case which contains metal objects such as coins