# X-Tag User Manual

Ver 1.0

# <Revision History >

| Version | Date | Description | Firm |
|---|---|---|---|
| 1.00 | 2025-07-18 | Initial release | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# < Terminology >

● Admin, Administrator

- A user who can change device settings and modify the operational environment.
- If there’s no administrator, anyone can modify settings. It is recommended to register at least one administrator
- Admins have the privilege to change device system settings, so caution is needed when registering or managing them.

● Authentication Method

- Includes mobile key, password, RF card authentication, or combinations of the authentication methods.

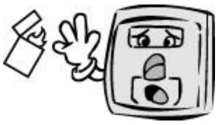
  e.g., Card or Password: Authenticated using either method.

# Table of Contents

# 1. Before Use

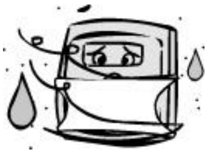
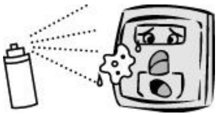
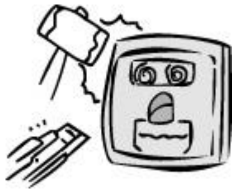
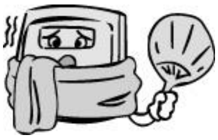
## 1.1. Safety Precautions

- Warning

| | |
|---|---|
| Do not operate with wet hands or allow liquids inside<br>->It may cause an electric shock or damage. | Do not place any ignition source near the terminal.<br>-> It may trigger a fire.  |
| Do not disassemble, repair, or modify the terminal.<br>->It may cause an electric shock, fire, or damage. | Keep out of reach of children.<br>->It may cause an accident or damage |

- Ignoring warnings can cause serious injury or death.

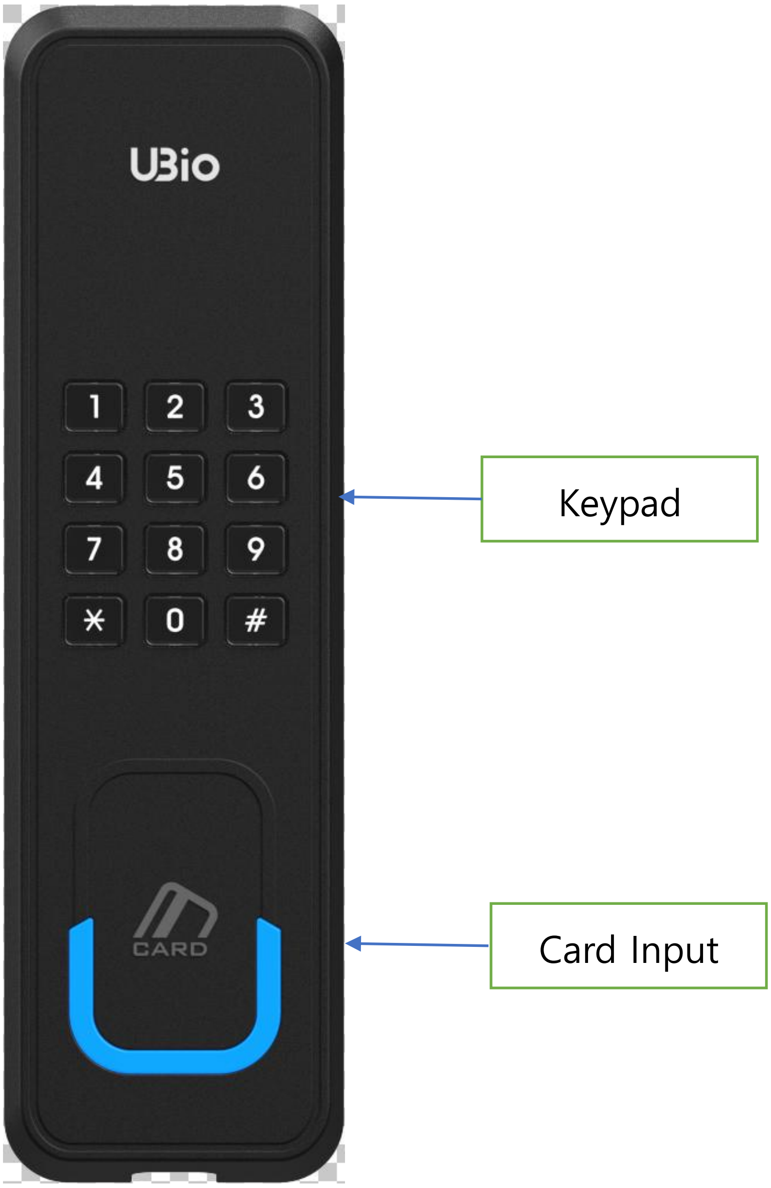
- Warning

| | |
|---|---|
| Avoid direct sunlight.<br>->It may cause a deformation or discoloration. | Avoid humidity or dust<br>->It may damage the device.  |
| Do not clean with water, benzene, thinner, or alcohol -> It may cause fire/electric shock. | Do not place magnets near the device.<br>-> It may cause a malfunction |
| Do not smudge the fingerprint scanner.<br>-> Fingerprints may not be recognized properly. | Do not spray insecticide or flammable substances<br>-> It may cause deformation or discoloration  |
| Avoid impact or sharp objects on terminals.<br>-> It may cause damage or breakage  | Avoid drastic temperature changes<br>-> It may cause damage  |

- Ignoring precautions may cause property damage or personal injury.

※ Disclaimer: UNION Biometrics is not liable for accidents caused by misuse due to ignoring the manual.

## 1.2. Name of Terminal Components


UBio
1 2 3
4 5 6
7 8 9
* 0 #
CARD
Keypad
Card Input

## 1.3. LED and Voice Sound During Event

| Event | Voice and LED |
|---|---|
| Authentication Success | "Ding-dong" sound + blue LED blinking |
| Authentication Failure | Beeping sound + red LED blinking |
| Waiting for the Card | Repeated beep + blue LED blinks (0.2s interval, 10s timeout) |
| Waiting for PW | Repeated beep + keypad LED blinks (0.2s, 10s timeout) |
| Temper | Beep every 3 seconds when opening the cover. |

## 1.3. Status LED

| Condition | Status |
|---|---|
| Normal | White LED |
| Server Connected | Blue LED |
| Server Connected, RS485 Connected | Blue LED |
| Server Connected, RS485 Disconnected | Blue LED blinks every 1s |
| Server Disconnected, RS485 Connected | Red LED + Blue LED blink every 1s |
| Server Disconnected, RS485 Disconnected | Red LED + White LED blink every 1s |
| | |

1) Server connection status is checked after the internet is connected.
2) RS485 status check requires proper configuration (LC10/LC15 or OSDP setting)

# 2. Product Introduction

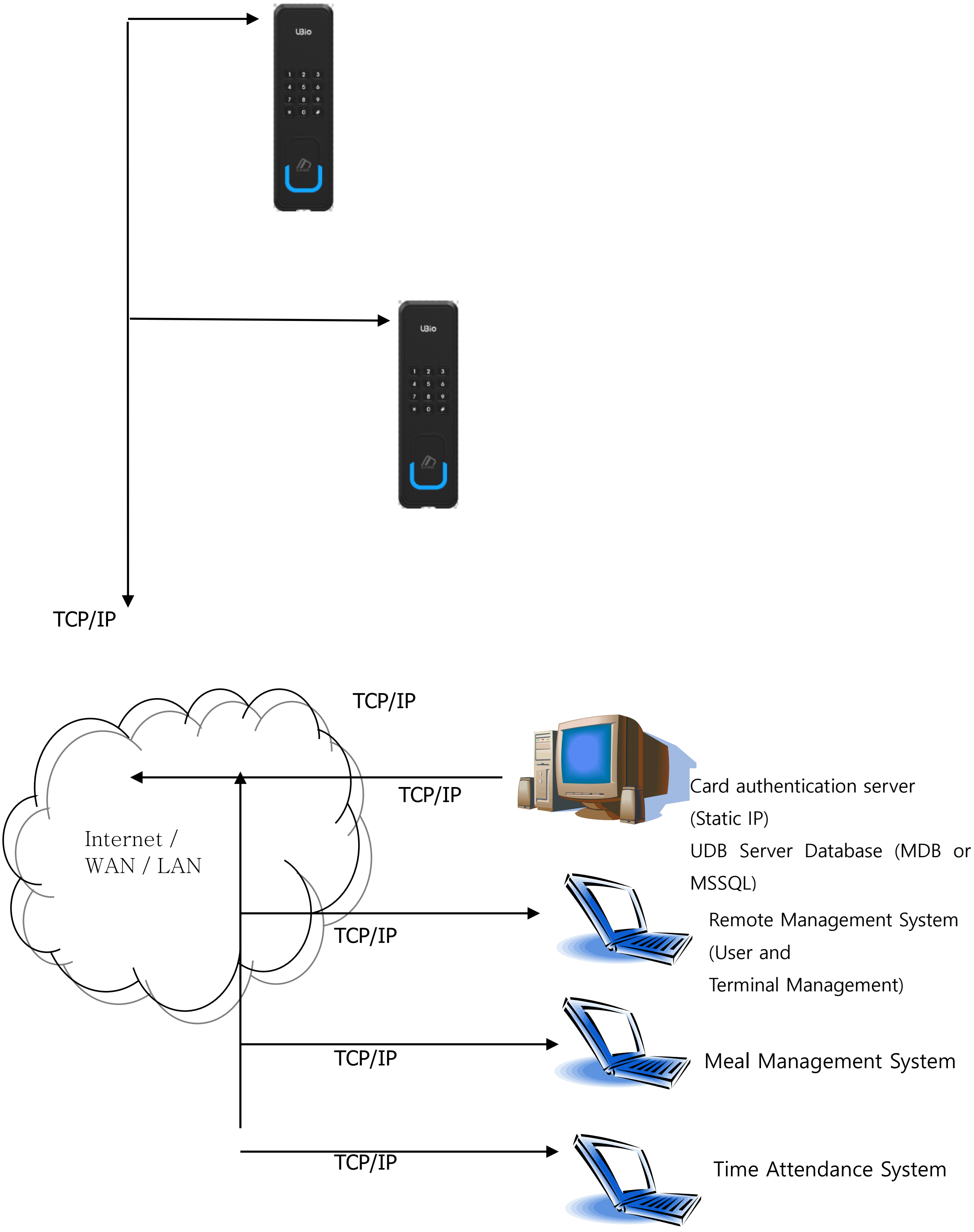
## 2.1. Product Features

- Multi-modal products that can use user cards or passwords
- RF (125 kHz) Card supported
- Smart Card (13.56MHz) supported
- TCP/IP communication supported with server database connection

- Various Registration/Authentication Methods

| | |
|---|---|
| Card | Card registration (Available on the server)<br>Card authentication |
| Password | Password registration (Available in the Server)<br>Password authentication |
| Mobile Key | Temporary mobile key registration (Available in the Server)<br>Mobile key user-key registration (Available in the Server) |
| Card<br>OR Password | Card, Password registration (Available on the Server)<br>Card OR Password authentication<br>⁎ ID & password input required for password authentication |
| Card<br>and Password | Card, Password Registration (Available on the Server)<br>Card AND Password authentication<br>⁎ ID & password input required for password authentication |

## 2.2. Product Components
(Access, Time Attendance, Meal Management)



## 2.3. Product Specification

| Category | Specification | Note |
|---|---|---|
| CPU | RISC-V CPU, Dual-core ARM Coretex-A7 | |
| Memory | eMMc 4GB | |
| | 256MB RAM | |
| USB Support | FW Upgrade Only | |
| Capacity | 400,000 Users / 400,000 Cards<br>1,000,000 Logs | |
| Temperature / Humidity | -20 ~ 60 /<br>< 90% RH | |
| AC / DC Adapter | Input: (Universal) AC100 ~ 250V | |
| | Output: DC 12V | |
| | | |
| PoE | Input: 48 Vdc / Output: 12 Vdc | |
| Lock Control | EM, Strike, Motor Lock, Auto Door | |
| I/O | 2 Input(1 Exit Button, 1 Monitoring)<br>1 Output | |
| Communication Port | TCP/IP (10/100Mbps) | |
| | RS-485 | |
| | Wiegand Input/Output | |
| | | |
| Card Reader | 13.56MHz Smart Card Reader, ISO14443A/B, MiFare, Felica, ISO15693 SE iClass(Option), 125KHz RF Card Reader, EM, HiD Prox(Option) | |
| Dimension | 45*157*27 | |

# 3. Environment Setting

## 3.1. Environment Setting

Use the Settings App to modify terminal configuration.
< Refer to Settings App Manual >

## 3.2. How to Update FW

Firmware updates are supported via the Alpeta Server.
<Refer to Alpeta Manual >

# 4. How to Use Terminal

## 4.1. How to Connect

- Connect power
- Use the Settings App to configure the internet setting
- If you change BT-related settings in the Settings app, BT connection will be disconnected and the device will be reset.
  -> BT rssi, BT txpower

- Connect the network cable to connect to the server
- Register the admins/users on the server
- If using DHCP, the default IP 255.255.255.255 is shown in the Settings App until an IP is assigned from the router

## 4.2. How to Use the Keyboard

- Default format: Number + # (# used as input key )
- Cancel the Input: Input '*'
- When you first enter ID + #, your ID will be entered, and then if you enter PW +#, your password will be entered.
  e.g., 2 + # (enter ID '2'), 1234 + # (enter PW '1234')

# 5. FCC Information

**FCC Information to User**

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.

**Caution**

THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS
NOTEXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE.
SUCH MODIFICATIONS COULD VOID.
THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

**IMPORTANT NOTE : FCC RF Radiation Exposure Statement**

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
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 interference, and
(2) this device must accept anyinterference received, including interference that may cause undesired operation.