

X-Tag User Manual

Version 1.0



Union
biometrics

< Revision History >

Version	Date	Description	Firmware Version
1.00	2025-09-01	Initial Release	



< Terminology >

- Administrator

- A user who can modify the device settings and change the operating environment.
- If no administrator is assigned for the device, anyone may change the settings. It is recommended to register at least one administrator in such cases.
- Since the administrator has the authority to modify the device's configuration, careful attention is required during registration and operation.

- Authentication Method

- Refers to various methods, including mobile key authentication, password authentication, RF (card) authentication, or a combination of these methods.
- Example: Card or Password – Authentication using either a card or a password

Table of Contents

< Revision History >	2
< Terminology >	3
< Table of Contents >	4
1. Before Use	5
1.1. Precautions.....	5
1.2. Names of Terminal Parts.....	7
1.3. LED and Buzzer Signals During Operation	8
2. Product Overview.....	11
2.1. Product Features.....	11
2.2. Product Components	12
2.3. Product Specifications.....	13
3. Configuration.....	14
3.1. Terminal Configuration Settings.....	14
3.2. Firmware Update Procedure	14
3.3. RS485 Settings.....	14
4. Terminal Operation	15
4.1. Connection Procedure.....	15
4.2. Using the Keypad (Keypad Model Only)	15
4.3. TNA Function Keys (Keypad Model Only)	15
4.4. Meal Function Keys (Keypad Model Only)	16
5. Compliance Information.....	17

1. Before Use

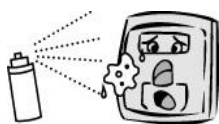
1.1. Precautions

● Warning

Do not handle the Terminal with wet hands or allow liquids to enter the device. ➤ This may cause electric shock or damage to the Terminal.		Do not place any sources of ignition near the Terminal. ➤ This may cause a fire	
Do not disassemble, repair, or modify the Terminal arbitrarily. ➤ This may cause electric shock, fire, or damage to the Terminal.		Keep the Terminal out of reach of children. ➤ This may cause injury or damage.	

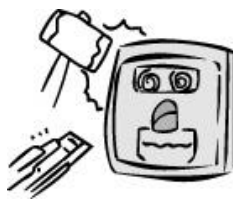
- Failure to follow the above warnings may result in death or serious injury.

● Caution

Keep it away from direct sunlight. ➤ This may cause warping or discoloration.		Avoid humidity or dust. ➤ The device may be damaged.	
Do not use water, benzene, thinner, or alcohol for cleaning. ➤ This may cause electric shock or fire.		Do not place magnets near the device. ➤ The device may stop working or malfunction..	
Do not contaminate the fingerprint sensor. ➤ The fingerprint may not be recognized properly.		Do not spray insecticides or flammable substances on the device. ➤ This may cause warping or discoloration.	

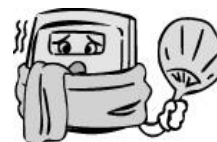
Avoid impacts or using sharp objects on the device.

- The device may be damaged or broken.



Avoid extreme temperature changes.

- The device may be damaged.



- Ignoring the above precautions may result in property damage or personal injury.

※ Under no circumstances shall UNION Biometrics be held responsible for any accidents or damages resulting from improper use of the product without referring to the user manual.

1.2. Names of Terminal Parts



1.3. LED and Buzzer Signals During Operation

1) Buzzer volume adjustable

➔ Key button, standby sound (card, PIN), authentication success and failure

Operation Type	Buzzer and LED
Authentication Success	A "beep-beep" sound plays, and the blue LED flashes
Authentication Failure	A "beeeep" sound plays, and the red LED flashes
Cancel During ID/PIN Input	A "beep-beep-beep" sound plays, and the white LED flashes
Card Standby	A continuous "beep-beep-beep-beep-beep" sound plays, and the blue LED flashes at 0.2-second intervals (times out after 10 seconds)
PIN Standby	A continuous "beep-beep-beep-beep-beep" sound plays, and the key LED flashes at 0.2-second intervals (times out after 10 seconds)
Key Button	When a key button is pressed, a "beep" sound is played

- In card standby mode, only the card is recognized.
- In password (PW) standby mode, only the password can be entered.
- Any attempt to use another authentication method is ignored.
- Volume can be adjusted through the Link App, and no sound is produced when the volume is set to 0.

2) Buzzer volume is fixed at MAX

- ➔ For cover open (tamper) and door open warning sounds, if the buzzer volume is set to 0, it is silent.
- ➔ If the volume is set between 1–3, the buzzer always operates at MAX level 3, regardless of the set value.

Operation Type	Buzzer & LED
Tamper	When the cover is opened, a "beep-beep-beep" sound plays at 5-second intervals
Door Open Warning	A "beep-beep-beep-beep-beep" sound plays at 5-second intervals

1.4. Status LED

1) LAN Connection Status

Status Type	LED Status
Normal (Server not connected)	Red LED blinking
Server connected	Blue LED on
Server connected, RS485 connected	Blue LED on
Server connected, RS485 not connected	White LED blinking
Server not connected, RS485 connected	Red LED blinking
Server not connected, RS485 not connected	Red and White LEDs blinking alternately

2) LAN Disconnected

Status Type	LED Status
Normal	Blue LED blinking
RS485 connected only	Blue LED blinking
RS485 not connected	Blue and White LEDs blinking alternately

3) Terminal Network Setting OFF

Status Type	LED Status
Normal	White LED on
RS485 connected	Blue LED on
RS485 not connected	White LED blinking

4) Others

Status Type	LED Status
Using TNA / Meal Function Key	White LED stays on while the function key is in use (however, Card or ID/PW standby LED takes priority)

BOOT	Red LED + Keypad LED on (may turn off and on during BOOT)
Connecting to Setup App	Pink LED blinking
Firmware Update	Pink LED blinking (during download and update)

- 1) After the internet is connected, the device checks the server connection status.
- 2) RS485 status can only be checked if "LC10/LC15" or "OSDP" is selected in the settings.
- 3) The terminal network settings can be turned ON or OFF via the UBio Link app.
- 4) TNA and Meal functions will operate only if set as TNA/Meal on the server or in the settings app.
- 5) Authentication is not possible while connected to the UBio Link app.

2. Product Overview

2.1. Product Features

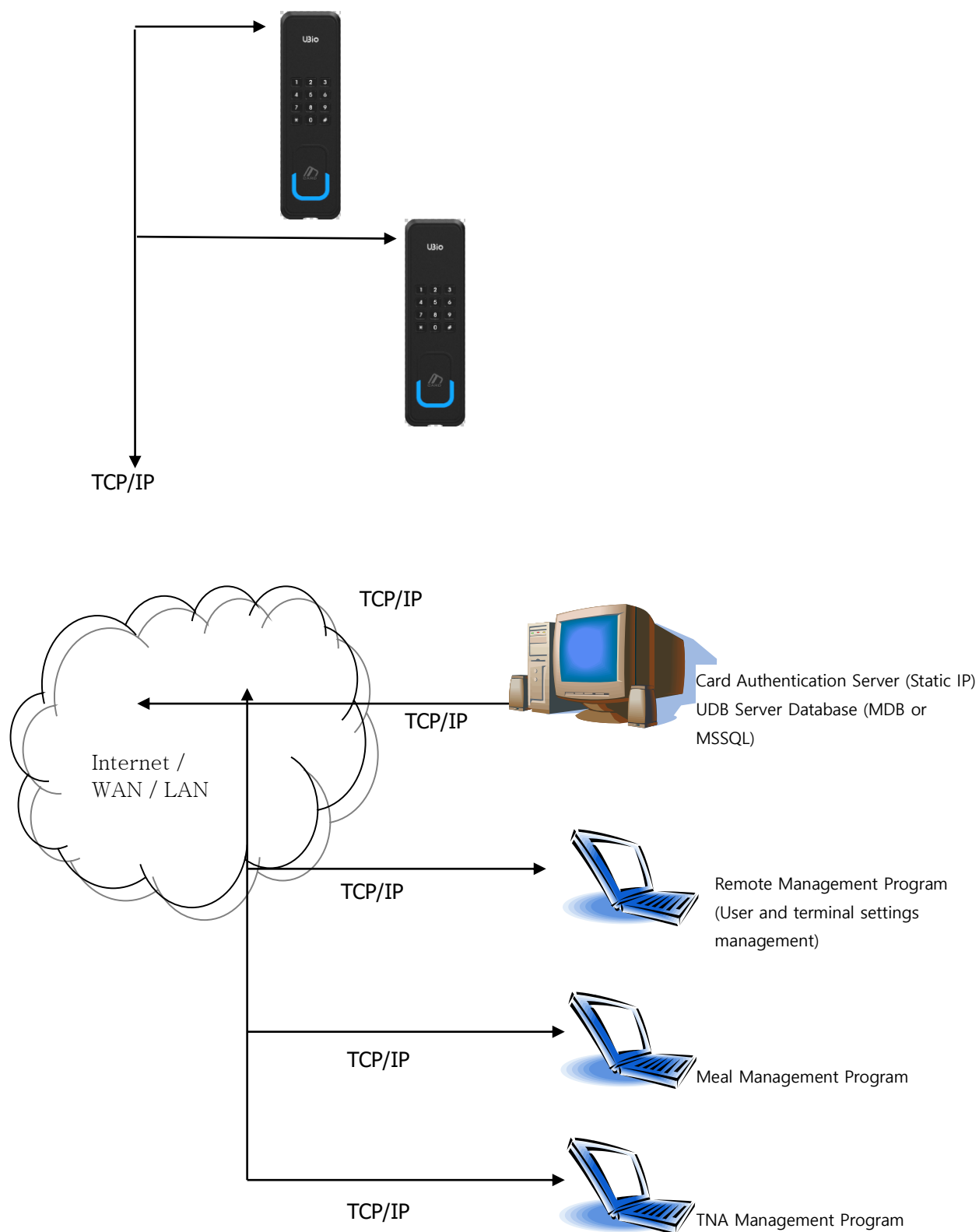
- Multi-modal authentication product supporting user card or password (keypad model only)
- RF (125 kHz) method
- Smart card (13.56 MHz) method
- Supports TCP/IP communication connected to the server database
- User addition and management via UBio Link setup app

- **Various registration and authentication methods**

Card	Register card Card authentication
Password	Register password Password authentication
Mobile Key	Register temporary key (server only) Register user key (server only)
Card OR Password	Register card or password Authenticate with card or password *If an ID is entered, password authentication is required. *Card authentication does not require password entry.
Card AND Password	Register card and password Authenticate with card and password *If an ID is entered, card authentication must be done first, then password entry. *If card authentication is performed first, password can be entered afterward.

2.2. Product Components

(Access, TNA, Meal Management)



2.3. Product Specifications

Category	Specification	Remarks
CPU	RISC-V CPU, Dual-core ARM Cortex-A7	
Memory	eMMC 4GB	
	256MB RAM	
External USB Support	For firmware upgrade only	
Users	400,000 users / 400,000 cards 1,000,000 logs	
Temperature / Humidity	-20 ~ 60°C / <90% RH	
AC / DC Adapter	Input: Universal AC 100 ~ 250V	
	Output: DC 12V	
PoE	Input: 48 Vdc / Output: 12 Vdc	Optional
Lock Control	EM, Strike, Motor Lock (optional), Auto Door	
I/O	2 inputs (1 exit button, 1 monitor), 1 output	
Communication Port	TCP/IP (10/100Mbps)	
	RS-485	
	Wiegand input/output	
Card Reader	13.56 MHz Smart Card Reader (ISO14443A/B, MIFARE, FeliCa, ISO15693, SE iClass optional), 125 kHz RF Card Reader (EM, HiD Prox optional)	
Keypad	12key	(K),(KP) model
Status LED	3 Color (White, Blue, Red)	
Current Consumption	Max 1.5A/DC12V & 0.75A/DC24V	
Dimensions	45*157*27	

3. Configuration

3.1. Terminal Configuration Settings

- Change the terminal settings through the UBio Link App.
- It is recommended to use a device with Android 10 or higher when installing UBio Link.
(Download from the App Store)
- The card format setting is a setting that determines how card data is stored. If the card format is changed, it may be necessary to re-register all card users in the device, so the format to use should be carefully selected.
(Default is recommended)
- When registering users from the server, the card format stored on the server must exactly match the card format of the terminal.

< Refer to the UBio Link App User Manual >

3.2. Firmware Update Procedure

- FW update function is supported via the UBio Link App.
- FW update function is supported from the server.

3.3. RS485 Settings

- RS485 settings can be configured via the Ubio Link App, and the device will reset after configuration.
- Monitoring should not be used when RS485 is in use. (Depends on the situation)
- Lock function should not be used when RS485 is in use. (Depends on the situation)

4. Terminal Operation

4.1. Connection Procedure

- Connect the power.
- Set up the internet via the configuration app.
- Connect the internet cable to establish a server connection.
- Register administrators and users via the configuration app or server.
- When using DHCP, the configuration app will display the default IP 255.255.255.255 until the device obtains an IP address.
- Time synchronization is performed with the server.
- If Bluetooth (BT) settings are changed in the configuration app, the BT connection will be disconnected and must be reconnected.
- → BT RSSI, BT TxPower settings

4.2. Using the Keypad (Keypad Model Only)

- The default format is Number + # (the '#' key is used for input confirmation).
- To cancel input, press '*'.
- Canceling input will cancel the ID and PW entry, and the process must be started from the beginning.
- Admin authentication is also canceled if input is canceled, and must be restarted from the beginning.
- To enter credentials: first input ID + # to enter the ID, then PW + # to enter the password.
- Example: 2 + # (ID "2" entered), 1234 + # (PW "1234" entered)

4.3. TNA Function Keys (Keypad Model Only)

- Operates when the mode is set to TNA via the configuration app or server.
- Pressing '*' sets Check-in mode and a beep sound is heard. (▲▲▲ sound gradually rises)
- Pressing '#' sets Check-out mode and a beep sound is heard. (▼▼▼ sound gradually falls)
- Holding '*' until a beep sounds and then releasing it sets Out mode, and a beep is heard. (▲▲▼ sound rises then falls)
- Holding '#' until a beep sounds and then releasing it sets Return mode, and a beep is heard. (▼▼▲ sound falls then rises)
- When a function key is set, the LED changes to white. If there is no authentication attempt during the 5-second wait, the device returns to normal mode.
- In function key mode (white LED on), pressing '*' cancels the mode.

4.4. Meal Function Keys (Keypad Model Only)

- Operates when the mode is set to Meal via the configuration app or server (initially set to Menu 1).
- Pressing '#1#' sets Menu 1, and a beep is heard. (▲▲▲ sound gradually rises)
- Pressing '#2#' sets Menu 2, and a beep is heard. (▼▼▼ sound gradually falls)
- Pressing '#3#' sets Menu 3, and a beep is heard. (▲▲▼ sound rises then falls)
- Pressing '#4#' sets Menu 4, and a beep is heard. (▼▼▲ sound falls then rises)
- When a function key is set, the white LED blinks once.
- Menu setting must generally be performed before use, but the previous menu setting is retained, so if no new menu is selected, authentication uses the previous menu..

5. Compliance Information

	Equipment Name: UBio-X Tag
	Model Name: UBio-X Tag (KP)
	Certified Company: Union Biometrics Co., Ltd.
	Manufacture Date: Specified separately
	Manufacturer & Country of Origin: Union Biometrics Co., Ltd. / Korea
	Certification Number: R-R-UCC-UBio-XTag
	Certified Module Number: R-C-ULX-NORA-W401