UP-Series

Manual

Version	0.1
Autor	cschardt
Datum	20.12.2018
Log	v0.1

Table of contents

1 Scope of functions

The UP devices are IP-capable access terminals designed for installation in a standard flush-mount box indoors.

Access is possible via face recognition (FaceUP only), RFID card [1], and PIN code. Access control can be selected from 1-tier up to 3-tier access control. While only one of the credentials is required for 1-tier access control (PIN, RFID or face), at least two credentials are required for multi-tier access control before access is granted.

The UP terminal has a relay (e.g. door opener) and a wiegand interface for connection to external access controllers. Functions of the terminal can also be controlled via two trigger inputs. It has a sensor which detects the removal o the frame and in this case can sound an alarm and switch off the access function.

The terminal is configured via WEB interface. With the EventHandler, the control functions of the inputs, the relay and the detection can be configured in a variety of ways [2].

The enrollment of face and PIN on the FaceUP is possible as soon as persons are created in the personnel database and these persons have been assigned PIN numbers in the WEB-GUI. The enrollment of PIN numbers on the UP keypad is not intended, these are assigned via the device's web pages.

2 Operating concept - keypad

The UP terminal has a keypad which signals requests and states via different lighting states.

The keys are backlit in color. The brightness of the keypad can be configured via the WEB interface. The background color indicates the operating status of the terminal:

- blue - standard operation
- green - enrollment
- red - special status (Firmware Upload, Personnel Database Upload, Tamper Alarm)

The operation of the keys is confirmed by a key click. In addition, events such as "Access Granted", "Access Denied" or "Tamperalarm" are signaled with various tones. The volume of the key clicks and the tones can be set separately. General meaning of the signal tones:

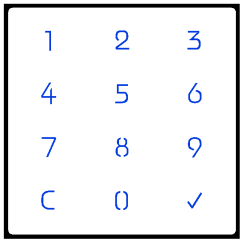
- short high-pitched tone - successful
- short medium-high tone - further action required
- sound with descending interval - not successful

The previous screen can generally be accessed with the C-key.

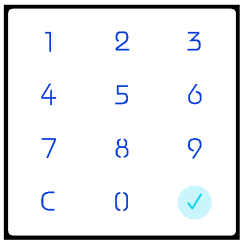
2.1 Standard operation

In normal recognition mode, the background of the keypad is highlighted in blue.

2.1.1 Main Screen



In the main screen, PIN entry, RFID card recognition and face recognition (FaceUP only) are active. As soon as any face is found, the OK button will light up.

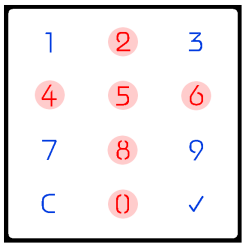


An entered PIN can be deleted by pressing the C key. The complete PIN is deleted. The entry of a PIN is confirmed with the OK button.

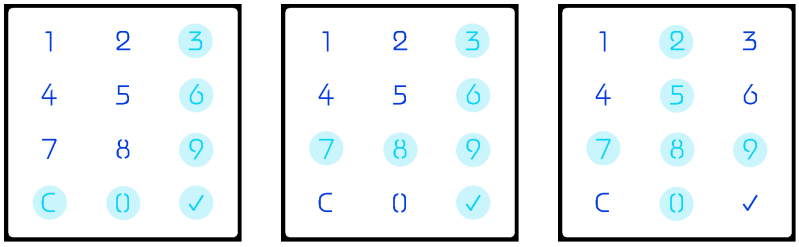
By pressing the OK key without PIN you reach the positioning screen.

2.1.2 Positioning screen (only for face recognition FaceUP)

The positioning screen helps to position the face for recognition correctly. If no pair of eyes is found, a red cross is displayed.



As soon as a pair of eyes is detected by the system, a blue glowing crosshair is displayed, which symbolizes the position of the face in the camera image.

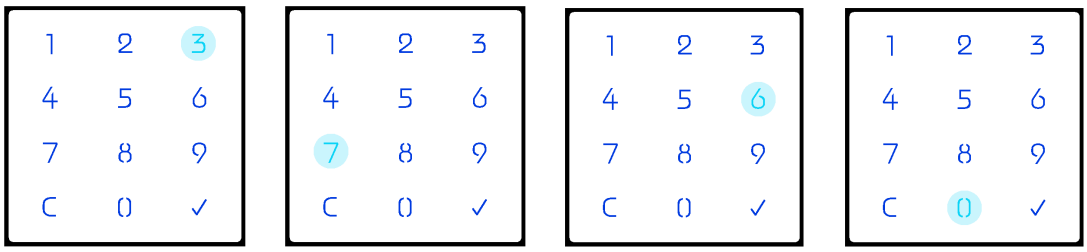


This screen is also shown if, in the case of multi-tier access control, the face verification should be performed.

When switching to the positioning screen, a short medium-high signal tone sounds.

2.1.3 Request for PIN entry

If the PIN entry is expected for multi-tier access control the keys are lighting up blue in a random pattern.



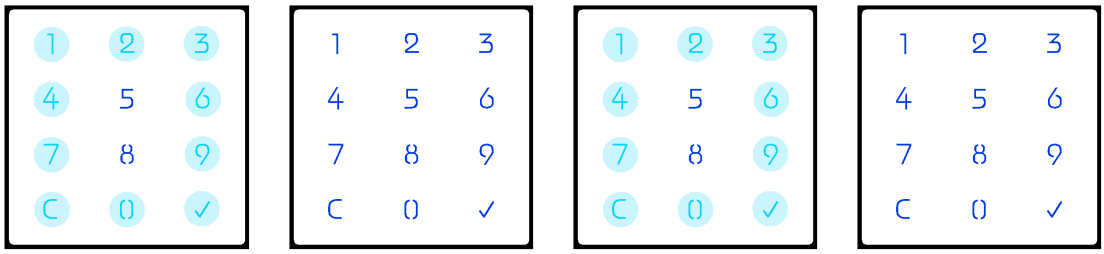
As soon as the PIN is entered, the light will stop flashing. The PIN is confirmed with OK.

The recognition can be aborted with the C-key. Then the main screen is active again.

When switching to the PIN input screen, a short medium-high signal tone sounds.

2.1.4 Request to present an RFID card

If the RFID card is expected for multi-tier access control, this is signaled by a rectangle flashing blue.

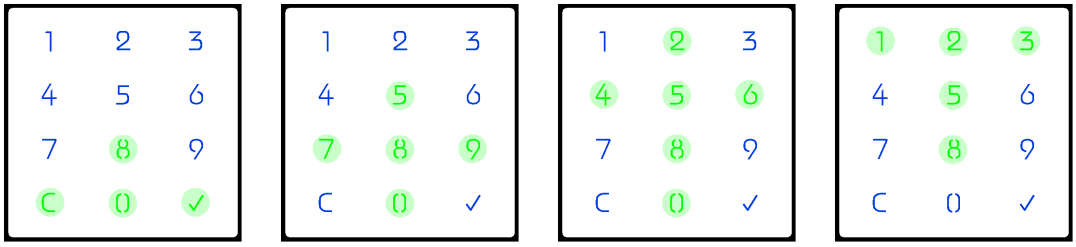


The recognition can be aborted with the C-key. Then the main screen is active again.

When switching to the RFID screen, a short medium-high signal tone sounds.

2.1.5 Access granted

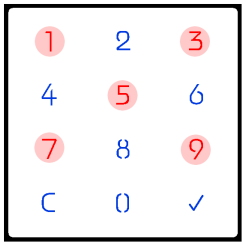
Once a person has been correctly identified, the Access Grant screen is displayed. Here, a green arrow is displayed that scrolls upwards.



In addition, access is signaled by a short high-pitched signal tone.

2.1.6 Access denied

If a wrong PIN or a wrong card is held in front of the reader, the access refusal screen is displayed. A red cross is displayed here.



Furthermore, a descending signal tone sounds.

2.2 Enrollment

In the enrollment area, the keys are backlit green.

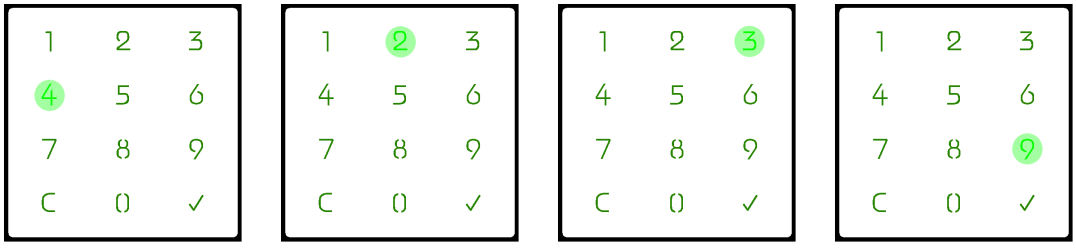
The enrollment for face recognition (FaceUP only) can be started with the green enrollment card while the enrollment for an RFID card can be reached with the red enrollment card.

To enroll a person, it must first be created via the WEB interface and at least one PIN or RFID card number must have been assigned.

Before each enrollment, the PIN of the person to be enrolled on the device is requested.

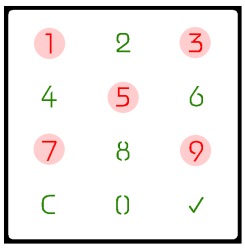
2.2.1 Request to enter a PIN code

After the respective enrollment card has been presented, the request to enter a PIN is signaled by the keys lighting up green in a random pattern. The PIN is used to select the person to whom this PIN is assigned by the corresponding entry in the WEB interface. It is also possible to use an RFID card, if one already exists.



2.2.2 PIN for enrollment incorrect

If a wrong PIN or card is held in front of the reader, the enrollment refused screen is switched on. A red cross on a green background is displayed here.



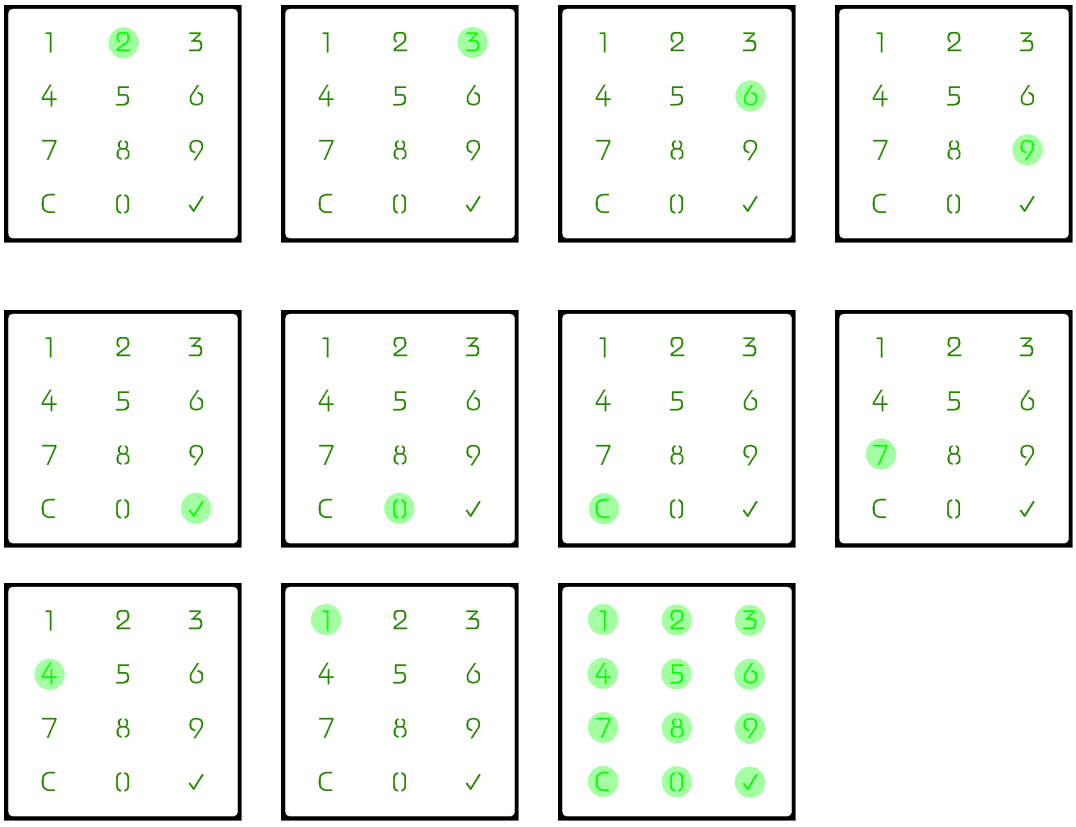
Furthermore, a descending signal tone sounds.

2.2.3 Face enrollment (only for face recognition FaceUP)

To enroll a face, the person should stand in front of the terminal and move the head in **minimal** circles.

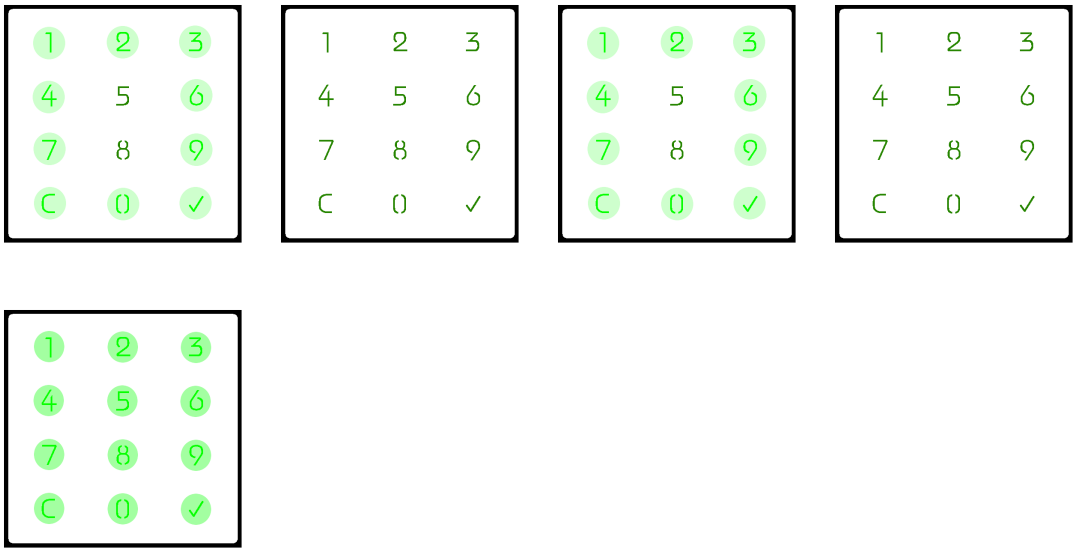
The progress of enrollment is symbolized by the buttons lighting up in a circle. After successful enrollment, all keys light up green briefly and a short high-pitched signal tone sounds.

Normally the enrollment is finished after the keys are illuminated once in a circle (starting from 2, ending at 1). In a few cases it may happen that further recordings are necessary. Then the circle moves a little further.



2.2.4 RFID enrollment

The RFID enrollment status is indicated by a green flashing rectangle.



The enrollment can be aborted with the C-key. Then the main screen is active again.

2.3 Special status

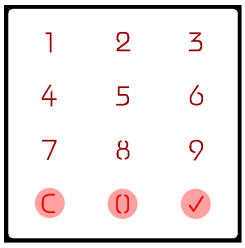
In situations where the terminal does not have its normal function, the LED basic color is red.

This is the case in the following situations

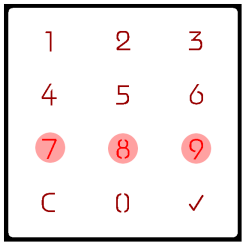
- Boot up
- Firmware/File Upload
- Upload of a personnel database
- Tamper alarm

2.3.1 Boot up

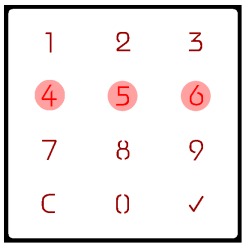
During the boot up, the screen displays the current status:



Ethernet link is established



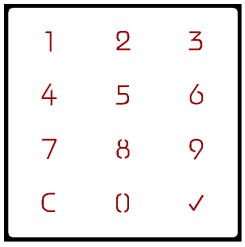
Waiting for DHCP address



System is initialized

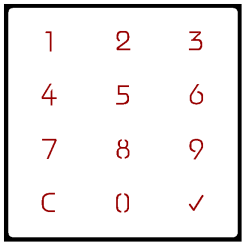
2.3.2 Firmware- or personnel database update

No access function is active during firmware updates and personnel database updates.



2.3.3 Tamper

If the frame is removed from the housing and the terminal is opened, the tamper screen is displayed. The access function is switched off.



Furthermore, a continuous alarm tone sounds.

3 Related documents

[1] Short manual RFID
https://adatis.com/wp-content/uploads/Short_manual_RFID.pdf

[2] Manual EventHandler
https://adatis.com/wp-content/uploads/Manual_EventHandler.pdf