

ИСО 9001



**STANDALONE
ACCESS CONTROLLERS
WITH KEYPAD AND PROXIMITY READER**

**Proxy-KeyAV, Proxy-KeyAH,
Proxy-KeyMV, Proxy-KeyMH**

User's Manual

TABLE OF CONTENTS

1	Description.....	4
1.1	Purpose.....	4
1.2	Specifications.....	4
1.3	Standard Delivery	5
1.4	Operation.....	5
1.5	Measuring Equipment, Tools, and Accessories	5
1.6	Marking and Sealing	6
1.7	Packing.....	6
2	Intended Usage	6
2.1	Operation Restrictions	6
2.2	Preparations for Use.....	6
2.3	Operating the Product	12
3	Maintenance.....	14
3.1	General.....	14
3.2	Safety Precautions.....	14
3.3	Maintenance Works	14
3.4	Testing Operability of the Device	14
3.5	Technical Inspection	14
3.6	Preservation (Depreservation, Represervation)	14
4	Running Repair.....	14
5	Storage.....	15
6	Transportation.....	15
7	Disposal	15
8	Manufacturer Warranty.....	15
9	Certificates.....	15

This User's Manual is intended for studying principles of functioning and operation of standalone access controllers with built-in proximity reader and keypad Proxy-KeyAV, Proxy-KeyAH, Proxy-KeyMV, Proxy-KeyMH.

Only the personnel can be allowed to maintain the controller who examined this User's Manual. All installation, start-up, adjustment, and commissioning works must be carried out in compliance with the regulatory documents in force at the site of operation.

1 Description

1.1 Purpose

1.1.1 Proxy-KeyAV, Proxy-KeyAH, Proxy-KeyMV, Proxy-KeyMH standalone access controllers with built-in proximity reader and keypad (hereinafter referred to as the controllers) are designed for entering passcodes and reading unique codes of proximity cards.

Possible applications: security systems, access control systems.

1.1.2 The controller can operate both in the standalone mode and in the mode of transferring codes to a control and indicating equipment or access controller over the Wiegand interface (the reader mode).

1.1.3 The controller is equipped with an optical tamper switch to detect tearing from the wall.

1.1.4 The controller is intended for round-the-clock operation.

1.1.5 The controller relates to non-recoverable, periodically serviced products.

1.2 Specifications

Table 1.2.1

No.	Characteristic	Value
1.2.1	Power Voltage	- 10 through 15 VDC
1.2.2	Average Consumed Current	- 200 mA
1.2.3	Power Input	- 1
1.2.4	Pre-operation Time	- 1 s
1.2.5	Card Capacity	- 1000 cards
1.2.6	Passcode Capacity	- 8 codes
1.2.7	Relays	- 2
1.2.8	Relay Switched Voltage	- 24 VDC
1.2.9	Relay Switched Current	- 2 A
1.2.10	Ingress Protection Rating as per GOST 14254-2015	- IP65
1.2.11	Resistance to mechanical stress as per OST 25 1099-83	- Category 3
1.2.12	Vibration loads: - Frequency - Max acceleration	- 1-35 Hz (for Category 3); - 0.5 g (for Category 3)
1.2.13	Climatic Category as per OST 25 1099-83	- O3
1.2.14	Operating Temperature	- Minus 35 through +50°C
1.2.15	Relative Humidity	- 0 to 95%
1.2.16	Weight	- 0.5 kg
1.2.17	Overall Dimensions: Proxy-KeyAV, Proxy-KeyMV Proxy-KeyAH, Proxy-KeyMH	- 50.2 × 160.2 × 21 mm - 86.2 × 120.2 × 21 mm

No.	Characteristic	Value
1.2.18	Non-stop Operation	- 24/7
1.2.19	MTBF in quiescent mode	- 80000 hours
1.2.20	Non-failure Operation Probability	- 0.98758
1.2.21	Average Lifetime	- 8 years

1.2.22 The device meets the requirements of man-made noise standards for the equipment of Class “B” as per GOST R 51318.22.

1.2.23 As to immunity to man-made radio disturbance the device meets the requirements of the third test level as per GOST R 50009.

1.3 Standard Delivery

1.3.1 Find the following unpacking the controller (see Table 1.3.1).

Table 1.3.1

Item	Q-ty
Proxy-KeyAV Proxy-KeyAH Proxy-KeyMV Proxy-KeyMH	1 pc.
Accessory Kit:	
Proximity card	1 pc.
Diode FR-107	1 pc.
Mounting bracket	1 pc.
Torx screw T10 for fastening on the bracket	1 pc.
Torx T10 L-wrench	1 pc.
Screw with Wall Plug:	
Proxy-KeyAV, Proxy-KeyMV	2 pcs.
Proxy-KeyAV, Proxy-KeyMV	4 pcs.
Documentation	
Instruction Manual	1 copy

1.4 Operation

Controllers *Proxy-KeyAV* and *Proxy-KeyAH* supports operation with identification cards and keyfobs of EM-Marin standard.

Controllers *Proxy-KeyMV* and *Proxy-KeyMH* supports operation with identification cards and keyfobs of the following MIFARE® standards: MIFARE® Ultralight, MIFARE® Classic, MIFARE® Plus.

The controller operating as a reader, a card code can be transferred in one of the formats Wiegand-26, Wiegand-34, Wiegand-44. Codes of keys are sent in Wiegand-8 when every key press results in sending 8 bits of the key code with 4 direct bits and 4 inverted bits.

1.5 Measuring Equipment, Tools, and Accessories

While mounting, commissioning, and maintaining the controller the tools shown in Table 1.5.1 should be used.

Table 1.5.1

Tools	Features
Digital Multimeter	Measuring AC and DC voltage up to 500 V, current up to 5 A, resistance up to 2 Mohm
Flat head screw driver	3.0×50 mm
Cross head screw driver	2×100 mm
Side cutter	160 mm
Pliers	160 mm

1.6 Marking and Sealing

1.6.1 Each controller has a marking made on its rear side.

1.6.2 The marking covers the following information: the name of the device, its decimal number, factory number, year and quarter of production, and conformity mark.

1.6.3 The controller is sealed by manufacturer.

1.6.4 The fixing screw of the printed circuit board of the controller is sealed by paint at the factory.

1.6.5 Violation of sealing automatically cancels the possibility of warranty service.

1.7 Packing

The device along with its accessory kit and Instruction Manual is packed into an individual carton box.

2 Intended Usage

2.1 Operation Restrictions

The design of the controller doesn't imply its using in aggressive and dusty environments as well as in explosion-hazardous premises.

2.2 Preparations for Use

2.2.1 Safety Precautions

- The design of the controller meets the requirements of electric and fire safety including emergency operation in accordance with Russian standards GOST 12.2.007.0-75 and GOST 12.1.004-91;

- There are no potential hazard circuits within the controller;

- Do SHUT OFF power from the controller before mounting, installing, and maintaining this one;

- Mounting and maintenance of the controller should be carried out by persons with the second or higher electric safety qualification level.

2.2.2 Design

Appearance and overall dimensions of the controllers are shown in Figure 1 (with Proxy-KeyAV, Proxy-KeyMV at the left and Proxy-KeyAH, Proxy-KeyMH at the right).

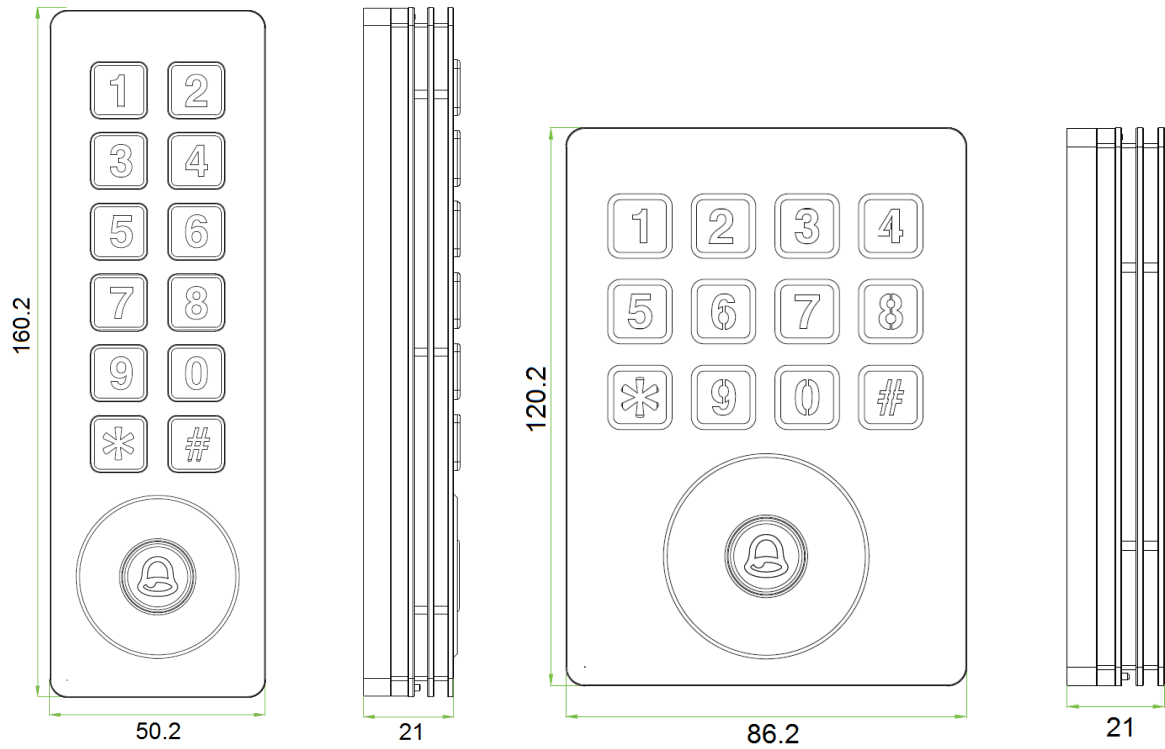


Figure 1. Appearance and Overall Dimensions

2.2.3 Mounting

To attach the controller to a wall please use the metal mounting bracket provided. Putting the bracket to the wall you can use it for marking the mounting holes.

For attaching Proxy-KeyAV or Proxy-KeyMV to a wall drill two holes for the screws and one opening to pass the cable.

For attaching Proxy-KeyAH or Proxy-KeyMH to a wall drill four holes for the screws and one opening to pass the cable.

The controller is fastened on the bracket by a torx screw with T10 head. These screw and torx wrench T10 comes with the controller.

While mounting the controller please take into account that its reading range reduces on exposure to electromagnetic interference or if the controller is installed on a metal surface.

2.2.4 Connecting

2.2.4.1 Connecting the Controller for Standalone Operation Mode

The diagrams for connecting external circuits to the controller in standalone mode are shown in Figure 2.

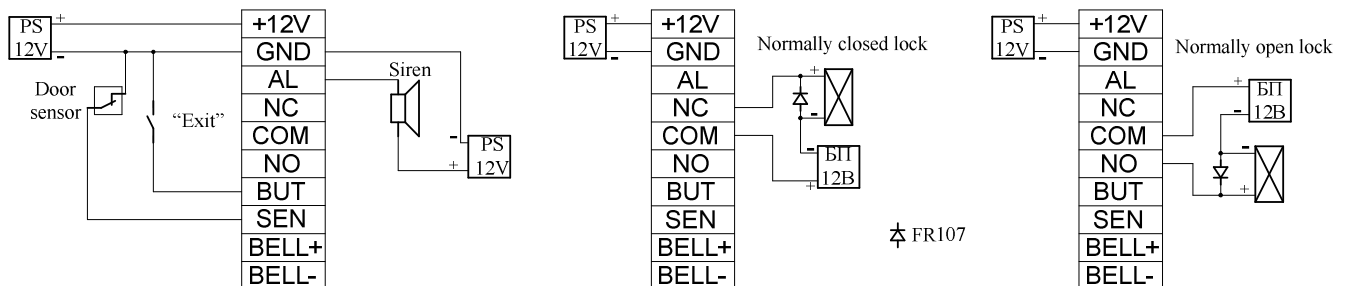


Figure 2. Diagrams for Connecting the Controller in Standalone Mode

The purpose and colors of wires for connecting the controller for standalone mode are shown in Table 2.2.4.1.1.

Table 2.2.4.1.1

Lettering	Color	Description
+12V	Red	Power Voltage
GND	Black	0 V
NC	Yellow	Lock relay, normally closed contact
COM	Pink	Lock relay, common contact
NO	Blue	Lock relay, normally open contact
SEN	Cyan	Door sensor
BUT	Grey	EXIT button
AL	Orange	Siren
BELL+	Lilac	Bell «+»
BELL-	Brown	Bell «-»

The output for connecting a door bell is a dry contact type one. We advise to use bells with working supply voltage 12 VDC. Bells with working voltage 220 VAC should be connected via switching units UK-VK. **Switching high voltage (220V) alternating current on the “BELL+” and “BELL-” contacts is prohibited!**

It is strongly recommended not to power the lock and the controller by a single power supply. **It is advised to power electric locks from a separate power supply.** If the lock is not equipped with a circuit for suppression of high-voltage pulses generated during commutation then the provided reverse switched diode must be connected at the lock terminals in parallel with the lock’s winding (the admissible direct current of the diode must not be less than 1A). **The diode must be installed even if the lock is powered by a separate power supply.**

2.2.4.2 Connecting the Controller to Operate as a Reader

The purpose and colors of wires for connecting the controller used as a reader to a control and indicating equipment or access controller are shown in Table 2.2.4.2.1

Table 2.2.4.2.1

Lettering	Color	Description
+12V	Red	Power voltage
GND	Black	0 V
WD0	Green	Wiegand data «0»
WD1	White	Wiegand data «1»
LED	Cyan	Blue LED Control
BEEP	Grey	Sounder Control
BELL+	Lilac	Bell «+»
BELL-	Brown	Bell «-»

Control polarity for the blue LED and the sounder is inverse (active “0”).

Figure 3 shows the examples of connecting the controller to control and indicator equipment and access controllers manufactured by the Bolid Company.

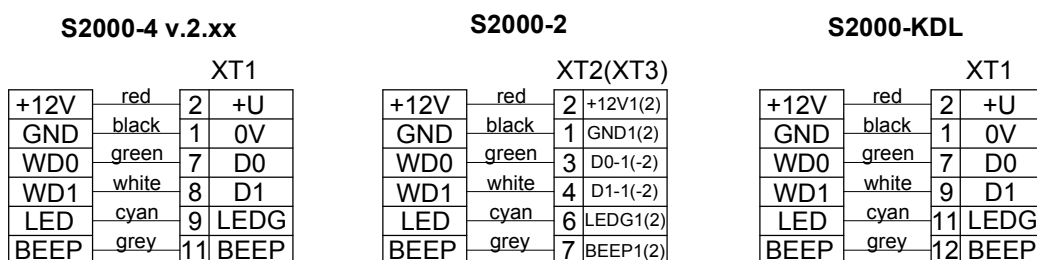


Figure 3. Diagrams for Connecting to CIE and Access Controllers (the controller is always shown at the left)

In the **standalone mode** the built-in siren is activated if one of the following has been detected:

- Brute force guessing of the administrator PIN;
- Unauthorized opening of the door (forcing open);
- Holding the door open after passing for more than a given time;
- Dismantling (tearing) the controller from the wall.


In the **reader mode** the built-in siren is activated if one of the following has been detected:



- Brute force guessing of the administrator PIN;
- Dismantling (tearing) the controller from the wall.

Alarms can be disabled – please see the relevant settings in Section 2.2.5 of this manual.

2.2.5 Settings

Settings of the controller are performed using its keypad. For changing parameters it is necessary to enter Administrator PIN (to enter to the menu of the controller).

The controller can be in one of the two operation modes, namely the standalone mode and the reader mode. The current mode of the controller is indicated by the key “” (bell).

If the standalone mode is active, the LED of the key “” flashes with blue. If the reader mode is active then the LED of the key “” is lit steady with red (if there is high logic level at the LED contact of the controller).

2.2.5.1 Entering Administrator PIN (Entering to Menu)

The default administrator PIN is 1234. It is advised to change this passcode prior to putting the controller into operation.

To enter the administrator passcode in the **standalone mode**, press the key “*”. The controller shall emit a long sound. Then press “#” and enter the passcode. Successive input is confirmed by controller’s emitting a long sound.

To enter the administrator passcode in the **reader mode**, press and hold “*” for about 5 s until the controller emits a long sound. Then press “#” and enter the passcode. Successive input is confirmed by controller’s emitting a long sound.

If the administrator passcode contains less the four digits then press “#” after entering the passcode.

If nothing is done for longer than 20 s the controller automatically exits the menu.

2.2.5.2 Switching Between Operation Modes

To switch the operation mode of the controller enter the menu (see 2.2.5.1), press “0” (the controller shall emit a long sound), then press “6” (the controller shall emit a long sound), and enter the code of the required operation mode (0 for the standalone mode or 1 for the reader mode). Successive switching is indicated by a long sound. Then the controller automatically exits the menu.

2.2.5.3 Changing Administrator PIN

To change the administrator passcode enter the menu (see Section 2.2.5.1), press “8”, and then enter a new administrator passcode. Then after a long sound enter the new passcode once more. Successive changing of the PIN is confirmed by emitting a long sound.

The maximum length of an administrator passcode is four digits. If there are fewer digits in the passcode then every entering of the PIN should be terminated by pressing “#”.

2.2.5.4 Resetting Administrator PIN

If the administrator PIN is missed, you should reset it. In this case controller settings and the user descriptors will not be removed from the controller memory. Resetting is performed using the optic tamper switch.


To reset the administrator PIN, remove the controller from the wall keeping it powered. Wait for about 30 s until the controller emits a long sound. Then within 30 seconds press three times on the optic tamper switch located at the rear side of the controller. Each press should be 2 to 5 s long. Each press shall be confirmed by a beep. In case of successive reset after the third press the controller emits a long sound. The administrator PIN returns to its factory value 1234.

If reset failed or 30 seconds have elapsed, then power off the controller. Then press the optic tamper switch down and hold it pressed. Holding the tamper switch, apply power to the controller, then release the tamper switch, wait for 30 seconds, and try to reset the administrator PIN again.

2.2.5.5 Opening the Door by Administrator PIN (Standalone Mode)

To open the door using the administrator PIN, enter the menu of the controller (see Section 2.2.5.1), then press the key “0” twice (the controller shall beep after each press). Then the door will be open.

2.2.5.6 Enrolling User Cards (Standalone Mode)

To enroll user cards enter the controller menu (see Section 2.2.5.1) and press “1”. The controller shall emit a long sound. Bring the card to the controller (to the black area around the key “”), the controller shall emit a long sound that means that the card is enrolled. Then you can bring the next card or exit the menu using the key “*”.

2.2.5.7 Enrolling User Passcodes (Standalone Mode)

The controller can store up to eight user passcodes each containing up to four digits. To add / change a user passcode enter the controller menu (see Section 2.2.5.1), press “3”, then enter the sequential number of the passcode (1 to 8), and enter the new passcode twice. If the passcode includes less than four digits then every passcode entering should be terminated by pressing “#”.

Then the next passcode can be enrolled by entering its sequential number and the passcode itself twice. Or you can exit from the menu by pressing “*”.

If a passcode should be deleted, then after selecting the passcode number enter zero twice just as if you enroll an ordinary passcode. By default all the passcodes are equal to zero, that is they are absent.

2.2.5.8 Deleting User Cards (Standalone Mode)

To delete a card from the controller memory, enter the menu (see Section 2.2.5.1), press “2” (the controller shall emit a long sound), and bring the card to be deleted to the controller. Successive deleting of the card is indicated by a long sound. Then you can bring the next card or exit the menu using “*”.

2.2.5.9 Deleting All User Cards Together (Standalone Mode)

To delete all the user cards from the controller memory enter to the menu (see Section 2.2.5.1), press “9” (the controller shall emit a long sound), and then press “9” once more. Successive deleting of all user cards is indicated by a long sound. Then the controller automatically quits the menu.

2.2.5.10 Setting Relay Activation Time (Standalone Mode)

To set the time for which the relay is to be activated, enter the menu (see Section 2.2.5.1), press “4” (the controller shall emit a long sound), and then enter the relay activation time (1 to 254 s) using the keypad. If the value is less than 100 then complete entering by pressing “#”. Successive setting of the time is indicated by a long sound. Then the controller automatically quits the menu.

2.2.5.11 Switching Between User Authorization Modes (Standalone Mode)

In the standalone mode the controller supports the following user authorization modes:

- 1) Authorization by passcode only;
- 2) Authorization by card only;
- 3) By entering the passcode or presenting the card (default mode);
- 4) By entering the passcode and presenting the card.

To switch between authorization modes, enter the menu (see Section 2.2.5.1), press “5” (the controller shall emit a long sound), and then enter the required number of authorization mode (1 to 4). Successive setting is indicated by a long sound. Then the controller automatically quits the menu.

2.2.5.12 Setting Door Sensor Mode (Standalone Operation Mode)

There can be three modes to operate the door sensor:

- 0) Normally open door sensor;
- 1) Normally closed door sensor;
- 2) No door sensor is in use (disabled).

To switch between operation modes of door sensor, enter in the menu of the controller (see Section 2.2.5.1), press “0” (the controller shall emit a long sound), then press “5” (the controller shall emit a long sound again), and finally enter the number of the mode (0 to 2). Successive setting of the door sensor mode is indicated by a long sound. Then the controller automatically quits the menu.

2.2.5.13 Setting Alarms

This parameter enables alarms on guessing of administrator PIN, on holding the door open for more than given time, or on forcing the door open. The parameter has no effect on alarms in case of tearing the controller from the wall. Two alarm modes are provided:

- 0) Alarms enabled (by default);
- 1) Alarms disabled;

To enable/disable alarms, enter the menu of the controller (see Section 2.2.5.1) and press “0” (the controller shall emit a long sound), then press “1” (the controller shall emit a long sound) and enter the number of the alarm mode (0 or 1). Successive changing of the alarm mode is indicated by a long sound. Then the controller automatically quits the menu.

2.2.5.14 Setting Alarms on Guessing Administrator PIN

By default this alarm is activated. If the PIN has been entered incorrectly three times running the controller emits an alarm and within next 20 seconds possibility of entering a PIN will be locked.

To activate/disable emitting this alarm, enter the menu of the controller (see Section 2.2.5.1), press “0” (the controller shall emit a long sound), then press “2” (the controller shall emit a long sound), and enter the number of the mode (0 for enabling alarms or 1 for disabling guessing alarms). Successive setting will be indicated by a long sound. Then the controller automatically quits the menu.

2.2.5.15 Setting Tamper Alarms

By default these alarms are enabled. The alarms are activated by the optical tamper switch when the controller has been teared from the wall.

To enable/disable these alarms, enter the controller menu (see Section 2.2.5.1), press “7” (the controller shall emit a long sound), and then press the number of mode (0 if the alarms are enabled or 1 if the alarms are disabled). Successive enabling/disabling of the alarms is indicated by a long sound. Then the controller automatically quits the menu.

2.2.5.16 Setting Door Open Timeout (Standalone Mode)

If the door has not yet closed after expiration of this timeout then the controller emits an alarm.

To set the door open timeout, enter the controller's menu (see Section 2.2.5.1) and press "0" (the controller shall emit a long sound), then press "4" (the controller shall emit a long sound), and then enter the timeout value using the keypad (1 to 254 seconds). If the value is less than 100 s then complete entering by pressing #. Successive setting of the timeout is indicated by a long sound. Then the controller automatically quits the menu.

2.2.5.17 Restore Factory Settings

Resetting the controller settings to default values doesn't involve cards and passcodes stored in the memory. Factory settings to be returned are shown in Table 2.2.5.17.1.

Table 2.2.5.17.1

Authorization mode	By card OR by passcode
Door sensor mode	Missed (disabled)
Alarms (2.2.13, 2.2.14, 2.2.15)	Enabled
Relay activation time	5 s
Door open timeout	15 s

To return the controller to factory settings, enter the controller's menu (see Section 2.2.5.1), press "0" (the controller shall emit a long sound), then press "9" (the controller shall emit a long sound), and press "9" once more. Successive resetting to factory values is indicated by a long sound. Then the controller automatically quits the menu.

2.2.5.18 Setting Data Output Format (Reader Mode)

The controller supports the following output formats:

- 0) Wiegand-26;
- 1) Wiegand-34;
- 2) Wiegand-44;

To select a required output format, enter the menu of the controller (see Section 2.2.5.1), press the "0" button (the controller shall emit a long sound), then press the "7" button (the controller shall emit a long sound again) and enter the number of the output format (0, 1, or 2). Successful changing of the output format will be indicated by a long sound. Then the controller automatically quits the menu.

2.3 Operating the Product

Only the personnel can be allowed to operate the controller who studied the current and is certified for safety regulations.

If the controller in the **reader mode** is used for operating partitions (or alarm loops) of the security alarm system then for correct indication of partition status the devices should be configured as follows:

- For S2000-2 and S2000-4 direct LED control polarity (active "1") should be selected;
- For S2000-KDL and S2000-KDL-2I controlling two LEDs and inverse control polarity (active "0") should be selected.


The maximum length of PIN should be set to a value equal to the length of codes which are supposed to be used in the system. If PIN codes of various lengths can be used in the system then after entering a code which is shorter than the ones of maximum length complete entering by pressing "#".

In case of centralized operating of the partitions after the first entering of the code operating the partition the controller LED indicates the partition status: blue color means the partition is disarmed and red color means that the partition is armed. After the second entering of the code the partition status will be inverted. To exit the partition operation mode, press "#" or wait for 30 s.

In case of local operating of alarm loops, if the device supports flipping alarm loop status “by a single touch” then the status of an alarm loop will be changed after the first code entering.

When the controller is used in the **standalone mode** users are authorized by the following way:

1) *Authorization by card (authorization modes by card only and by card or passcode)*


For opening the door a card should be touched to the controller (to black area around the key “”).

If the card is enrolled into the memory of the controller then the blue LED turns off for a short time, the sounder beeps, and then the door opens. If the card is not written in the memory then the red LED turns on twice for a short time while the sounder emits two beeps.

2) *Authorization by Passcode (authorization modes by passcode only and by passcode or card)*

For opening the door a passcode followed by “#” should be entered. If the passcode complies with that one which is written in the controller’s memory then the blue LED turns off for a short time, the sounder beeps, and then the door opens. If the passcode differs from the one written in the controller's memory then the red LED turns on for a short time two times and the sounder beeps doubly.


3) *Authorization by Passcode and Card*

To open the door, primarily put a card to the controller (to the black area around the key “”). If the card is enrolled in the controller’s memory then the blue LED starts flashing. If the card is not written in the memory then the red LED turns on twice for a short time and the sounder emits two beeps.

After successive reading, when the blue LED is flashing enter the passcode and complete entering by pressing “#”.

If the entered passcode is the same as the one written to the memory then the blue LED turns off for a short time, the sounder beeps, and the door opens. If the passcode differs from the one written to the memory then the red LED turns on twice for a short time and the sounder issues two beeps.

2.3.1 Testing Operability

On applying power the controller emits a long sound. Performance of the indicator on the key “” depends on the current operation mode.

To check operation in the **standalone mode**, a card or passcode has to be written in the memory of the controller. Present a card to the controller or enter a user passcode. The controller shall beep and grant access.

To test operation of the controller in the **reader mode**, enter the passcode or present the card to the controller. Further performance of the LEDs and the sounder depends on how the system access controller responds to the presented credential.

2.3.2 Emergency Action



CAUTION

If sparking, fire, smoke, or smell of burning is detected near the controller it shall be de-energized and submitted for repair.

2.3.3 Troubleshooting

Table 2.3.3.1

Trouble	Possible Cause	Solution
The controller being in the reader mode, the connected access controller beeps continuously	The access controller is adjusted incorrectly	Check settings of the access controller for indication control polarity which is to be inverse, with active “0”
The controller being in the standalone mode, the door does not open	The lock is connected improperly	Check the lock for proper connecting

3 Maintenance

3.1 General

The controller is to be maintained according to a scheduled-preventive system which provides annual maintenance.

3.2 Safety Precautions

Maintenance works shall be carried out at by electricians with safety qualification level II or higher.

3.3 Maintenance Works

Scheduled maintenance works include:

- Checking the exterior conditions of the controller;
- Inspection for secure mounting of the controller and good conditions of wires as well as terminal tightening;
- Testing operability in line with Section 3.4 of this manual.

3.4 Testing Operability of the Device

On applying power to the controller it shall emit a long sound. Performance of the LED on the key “🔔” depends on the current operation mode of the controller.

To test operation of the controller in the **standalone mode**, a card or a passcode should be written in the controller memory. Touch the controller with the card or enter the user the passcode. The controller shall emit a sound and grant access.

To test operation of the controller in the **reader mode**, enter the passcode or present the card to the controller. Further performance of the LEDs and the sounder depends on how the system access controller responds to the presented credential.

3.5 Technical Inspection

Not applicable.

3.6 Preservation (Depreservation, Represervation)

Not applicable.

4 Running Repair

4.1 Current repair of a defective product shall be carried out by the manufacturer or at authorized repair centers. The product shall be sent for repair in line with established procedures.



WARNING

The equipment shall be submitted for repair being assembled and clean along with all the parts listed in the documentation.

Claims are accepted if only a reclamation report describing the failure is applied.

4.2 A product's failure resulted from consumer's not observing mounting or operation rules is not a reason for claims and warranty repair.

4.3 Claims shall be submitted to the following address:

NVP BOLID CJSC, 4 Pionerskaya Str., Korolyov city, Moscow region, 141070, Russia

Tel./Fax: +7 (495) 775-71-55 (multiline). E-mail: info@bolid.ru.

4.4 In case of any issue related to operating the product, please contact with the technical support: +7 (495) 775-71-55 or e-mail: support@bolid.ru.

5 Storage

5.1 The controller in transportation packing can be stored at ambient temperatures minus 50 to +50 °C and relative humidity up to 95% at +35 °C.

5.2 The controller in the consumer packing shall be stored in heated warehouses at temperatures +5 to +40 °C and relative humidity up to 80% at +20 °C.

6 Transportation

6.1 The devices can be transported in transportation packing at ambient temperatures minus 50 to +50°C and relative humidity up to 95% at +35°C.

7 Disposal

7.1. While disposing the device please take into account that there are no toxic components within it.

7.2. Precious material content: not subject to inventory accounting in case of storage, disposal and recycling (Article 1.2 of GOST 2.608-78).

7.3. The content of non-ferrous metals: does not require accountability for retirement and further disposal.

8 Manufacturer Warranty

8.1. The manufacturer guarantees that the product meets technical requirements if the user follows the instructions for transportation, storage, installation, and usage.

8.2. Warranty period is 18 months since putting the controller into operation but no more than 24 months from the manufacturer's date of issue.

9 Certificates

9.1. Proxy-KeyAV, Proxy-KeyAH, Proxy-KeyMV, Proxy-KeyMH standalone access controllers with built-in proximity reader and keypad meet the requirements of Technical Regulations of Custom Union TR CU 020/2011 and approved by Conformity Certificate No. RU C-RU.ME61.B.01753.

9.2. Proxy-KeyAV, Proxy-KeyAH, Proxy-KeyMV, Proxy-KeyMH standalone access controllers with built-in proximity reader and keypad are approved by the certificate of conformity of transportation security technical arrangement with their functional properties No. МБД ПФ.03.000037 issued by Federal State Institution "Special Equipment and Communications" Scientific and Manufacturing Association of the Ministry of Internal Affairs of the Russian Federation.

9.3. The production of Proxy-KeyAV, Proxy-KeyAH, Proxy-KeyMV, Proxy-KeyMH standalone access controllers with built-in proximity reader and keypad is certified according to GOST ISO 9001-2015 by certificate No. ROSS RU.AB66.K00003.