DATASHEET

Universal standalone reader-controller "Privratnik-03A"

Product overview.

Universal reader-controller **Privratnik-03A** is designed for use in standalone systems for control of access into the ATM lobbies. The reader-controller accepts as cards for access into the facility any bank cards of all payment systems, both with a magnetic stripe (according to ISO 7813) and a microprocessor (according to ISO 7816).

The structural design of the universal controller-reader allows to use it both in "cut-in" and attachable versions (through a special wallmount box).

Specifications of the device.

1	Supply voltage, V	12±10%
2	Power supply current of the device, mA*	max. 100
3	Load current at the output of the device, A	max. 2
4	Impulse feed time for the lock, sec.	from 1 (programmable)
5	Operating temperature range, °C	from –30° to +35°

* - power supply current of lock/latch not considered

Component parts of the product

1	Reader-controller	1 pc.
2	Mounting set (antivandal)	1 pc.
3	Front panel, antivandal	1 pc.
4	Exit button, attachable	1 pc.
5	Information labels	1 set
6	Datasheet for the product	1 pc.
Components (optionally)		
7	Box for attachable installation version	1 pc.
8	Reader for proximity NFC cards	1 pc.
9	Skimming presence sensor	1 pc.

Notes on installation of the universal reader-controller "Privratnik-03A"

Structurally, the universal reader of plastic cards is designed as a device for cut-in (hidden) installation. The device is installed on the surface adjacent to the blocked doorway. The reader is attached to the surface through special mounting holes located on its face front antivandal panel. The external view of the reader-controller assembly is presented in **Fig. 1**. In cases where the door unit is framed by metal-glass windows, it is possible to install the reader-controller in a special attachment box. This box is an optional position and is ordered separately.

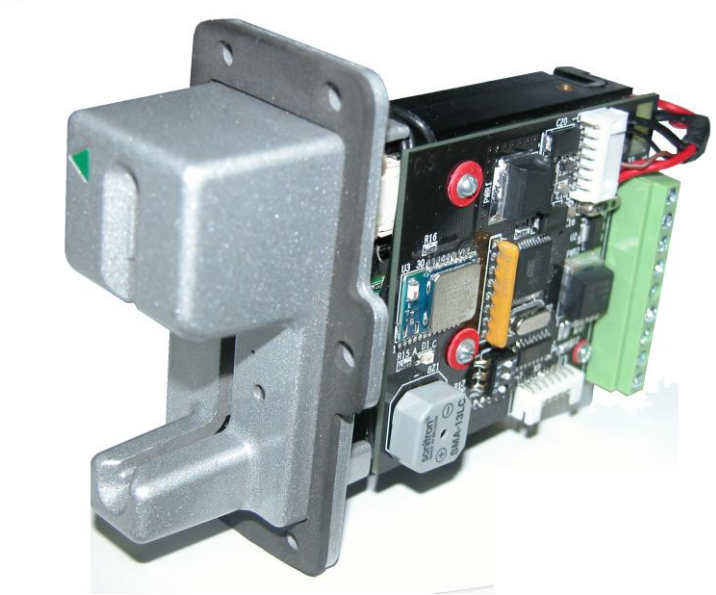

Fig. 1

Description of operation of the universal reader-controller Privratnik-03A

The device "Privratnik-03A" includes a universal reader of plastic cards and a controller. The controller receives and processes the data from the cardreader, from external sensors (exit button, blocking, presence detector) and controls the operation of the door locking device (electromagnetic lock, door latch).

Upon voltage (+12 VDC) supply the device is switched in a standby mode. Depending on the initial settings with reference to the time of day the door goes into a blocking mode (by lock, by latch) or remains unlocked (free passage). If the door, as per settings, remains unlocked - the colour of the LED located on the front panel of the reader remains "green". If the door is locked, the LED switches to the mode of alternating blinking in green and red colour. When the card of a standard form that allows the passage is installed into the reader the door is unlocked for the time determined by the controller settings, an audio signal sounds to indicate that the passage is allowed, the indication of the light-emitting diode changes to continuous green. The countdown for unlocking the door is marked from the moment of extraction of the credit card by the user from the reader.

After this time period the door is locked, and the device is put in a standby mode. The unlocking of the door from inside the facility is done by pressing the exit button connected to the controller.

The device allows to implement a number of additional features that enhance system performance:

A) complete blocking of the entrance door - in the event of collection of ATM or facility locking in case of obvious questioned transactions or manifestations of vandalism. This blocking is performed by connecting a limit switch with fixation (toggle switch) or the relay contacts of the video recorder to the corresponding terminals of the controller. When this mode is activated, the system does not respond to the exit button and does not read the cards.

B) blocking entry through the entrance door - this function prevents the passage into the ATM facility, if a card holder is already being served here. This function is implemented by connecting the alarm line of the IR sensor installed at the ATM.

C) detection of abnormal external devices – this optional function allows to detect skimming covers on the system reader. When the corresponding sensor is triggered, the door is unlocked, at the same time light and sound indications are switched into the appropriate mode. At a certain contact of the terminal block (**E**) there is a control voltage allowing to implement the devices and algorithms that meet the situation (mode).

On the front panel of the reader there is a service port that allows to urgently remove the jammed plastic card (for example, the card installed in the turned power-off reader). This will require to use either a needle, or a fragment of a paper clip.

Description of board components of the universal reader-controller "Privratnik-03A"

The controller board of the product contains a number of switching elements used for the device operation and activated when installing the product. Clicking the **Read Logs** button starts uploading on the application screen the data presented in the form of a table in **Fig.19**. This data can be viewed, and the user can also upload it to a mobile device by clicking the **Save** button. The board also includes interface connector **X4** (to communicate with the reader of the product). The connector **XT1** located on the opposite side of the controller board is a service one, and it is not used for operation. The connector **X5** is designed for connecting an optional reader of proximity bank cards, as well as for the sensor for detecting skimming covers on the device reader.

The location of the connectors on the controller board is shown in **Fig.2**. The external supply and control lines are connected to the controller through terminal block **X3**.

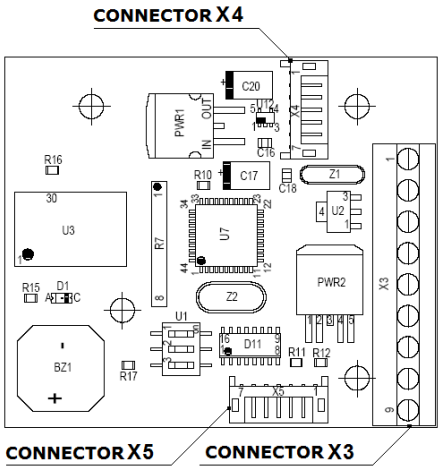

Fig. 2

Connecting the universal reader-controller "Privratnik-03A"

The controller is initially programmed and is ready for operation. The settings screens are filled with typical values of variables and constants that the controller uses during its operation. The external supply and control lines are connected to the controller through terminal block **X3**, the pin assignment of this block is shown in **Fig. 3**.

G	GROUND
+	+12 V., SUPPLY VOLTAGE
R	ANTISKIMMING INPUT
E	ANTISKIMMING OUTPUT
D	DRIVE LOCK
C	PRESENCE SENSOR
B	BLOCKING
A	EXIT BUTTON
G	GROUND

Fig. 3

A typical wiring diagram of the reader-controller is shown in **Fig. 4**. The diagram also shows the names of external switching devices (coil for electromagnetic lock, exit button, blocking (with fixation) and NC contacts of presence detector). As the external circuits are also specified the following devices: the sensor for detecting the skimming cover and the device running the operation algorithm based on the detection of abnormal external device.

The protection against skimming attack is optional and is disabled in software by default. The service for controlling the sensor for client presence detection is also disabled in software.

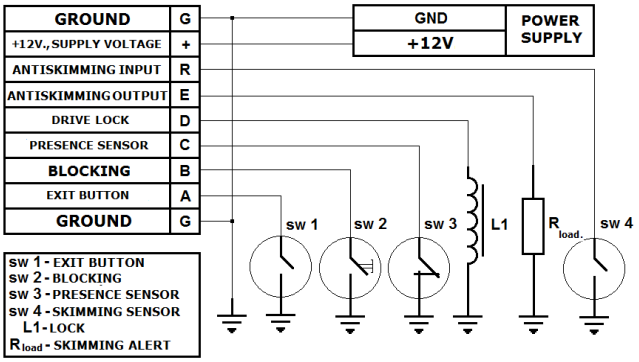

Fig. 4

The controller is initially programmed and is ready for operation. After the device is turned on, depending on the time of day, it is switched in 2 different versions of the standby mode. If the controller was turned on within the interval from 20-00 to 8-00 (MSC), the doorlock goes into the blocking mode, the LED switches to the mode of alternating blinking in green and red colour. If the controller was turned on within another time interval, the doorlock remains unlocked and the colour of the LED located on the front panel of the reader remains "dark".

To change the settings, to synchronize with the local time, and if necessary, to organize the viewing and uploading of the logs based on the passages, you shall install on your mobile device a free software **PRIVRATNIK 03**. To install the application, you shall ensure that your smartphone supports the following:

- installed ANDROID OS version 4.3 or higher;
- Bluetooth 4.0, including low energy support (eng. Bluetooth Low Energy, Bluetooth LE);

Then, using the QR-code on the last page of the Manual, you need to download Privratnik.apk file and to install the Application. After installing the application, the following icon (**Fig. 5**) appears on the desktop:

Fig. 5

In the main menu of the device you should activate wireless communication interface BLUETOOTH to connect with the reader-controller "Privratnik-03A". After starting the application, a service window for searching the device will appear on the smartphone screen (**Fig. 6**). After the device is found, you shall select in the resulting menu the window with the name of the found device BLUEGIGA PRIVRATNIK (**Fig.7**):

Fig. 6

Fig. 7

Then, the window will open with the data for the unknown device to be selected (**Fig. 8**),

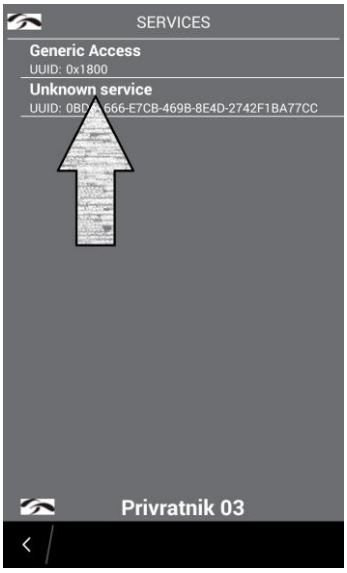

Fig. 8

then select the device option (**Fig. 9**)

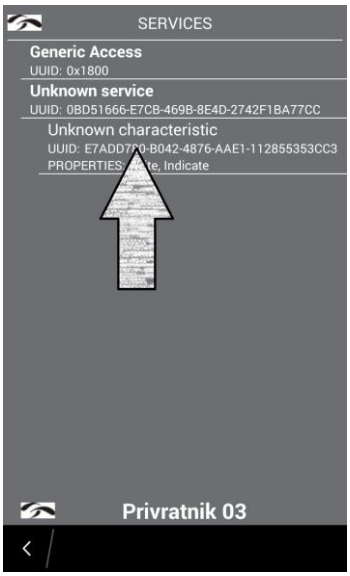

Fig. 9

After the above mentioned actions the PRIVRATNIK 03 program menu will appear on the screen (**Fig. 10**). After that, you need to upload to the menu windows the current settings for the controller (by default). To do this, please click on the upload icon - the symbol in the upper right corner of the menu.

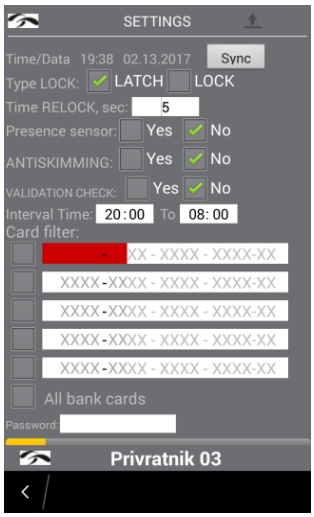

Fig. 10

If your actions are correct, a yellow sliding bar will appear below indicating your query progress. After the query execution the menu windows will be filled with the current settings for the controller. (**Fig. 11**)

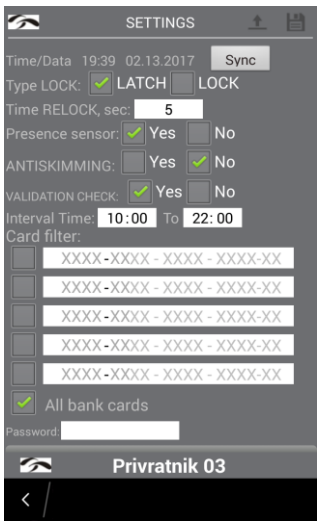

Fig. 11

Description of the PRIVRATNIK 03 application menu windows

Figure 12 shows the screenshot of the application main menu screen.

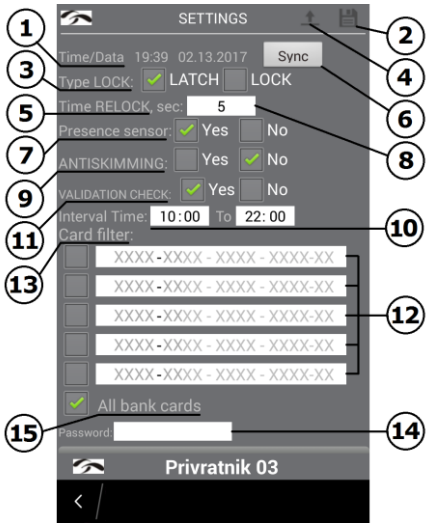

Fig. 12

1	Current system time of the smartphone
3	Blocking device type (electromagnetic lock/door latch)
5	Lock opening time
7	Presence sensor selection
9	Selecting the skimming presence sensor
11	Selecting to check the card expire date
13	Card filter section
15	Selecting passage through all card types

2	Downloading the setting in the controller
4	Uploading the settings from the controller
6	Time synchronization
8	Entering field of the lock opening time
10	Entering field of the controller operation time
12	Entering field of card numbers
14	Entering field of the password to access the log menu

Comments:

1 and **6** – if local time **is different from Moscow time**, **you need to** synchronize the system time of the smartphone with the controller;

4 and 2 – the icons are used to upload the controller settings on the smartphone and to further download the modified settings on the device.

3 – select the blocking device type based on the option that is used in a particular case - electromagnetic lock/door latch;

5 and **8** – this setting determines the time interval during which the door is opened through the card or the exit button, the value in seconds shall be entered in the corresponding window;

7 – select, wether or not, the sensor for detecting the client's presence in the ATM area, is used;

9 – select, wether or not, the sensor for detecting the skimming covers over the system reader, is used;

Note – if the specified sensors will not be used in the system – be sure to check the NO boxes. Otherwise, the controller will generate the appropriate sound and light signals !

10 – these fields are for entering the system start time and end time for passage by cards;

11 - enable or disable the mode for monitoring the expire dates of the cards presented for passage;

12 – enter the most significant 6 characters of the bank card numbers, if the card filter is used;

13 – card filter activation section. The device supports 5 different masks based on the most significant 6 symbols of the credit card number. To activate the filter, check the appropriate field and fill it in with the necessary numbers;

14 – field for entering the password to access the controller's log menu;

15 – card filter reset, activation of the mode for passing all bank cards (of any bank, any payment system);

Features for using external sensors

Along with the exit button several external sensors (circuits) can be connected to the device.

1. Client presence sensor.
2. External blocking of the system.
3. Sensor for detecting the skimming cover.

As a presence sensor we recommend to use usual infrared sensor covering the operating area near the ATM. If there is a client within the service area, the system will not allow to open the door from outside with the help of the card. The activation of this mode will be signalled by the light and sound indication. Meanwhile, the exit button will work, allowing the client to freely leave the ATM lobby.

The sensor for detecting the skimming cover records the presence of abnormal devices and constructions over the reader panel. Upon detection of such devices, the controller blocks entry through the entrance door, goes into alarm mode, and outputs the **E** level of +12V. It is possible to connect to the output the light (sound) alarms with power supply current of less than 0.7 A. In this case, the exit button will work, allowing the client to freely leave the ATM lobby.

Figure 4 shows a standard connection diagram for all possible external circuits (sensors and actuators).

The external blocking is designed to completely block the door for entering the ATM area. This blocking can be carried out both by external switch and relay outputs of the control panels of security alarm or video recorders. The function is relevant for blocking the door in the event of collection of ATM or when detecting fraud evidence in regard to unauthorized persons near the ATM.

Operating the card filters

The controller system software allows you to organize 5 different masks for the implementation of the filter based on the numbers of the bank cards presented for the passage.

The availability of this functionality allows to restrict access to the card ATM, both by the payment system type, and the card-issuing bank.

The function is useful when the ATM owner wants to limit the list of the served persons only by a circle of his clients (through loyalty programs, payroll card program, etc.).

To start working with card filters, simply touch the screen where the check mark shall be placed opposite the field for filling in the most significant characters of the credit card number (**Fig.13**). After the check mark is placed, the field for entering the number will highlight in red and be ready to be filled in with characters.

After entering the most significant characters of the card numbers simply touch any open area of the screen with your finger. The red filling area will disappear, then you should test the controller with the settings (floppy icon in the top right corner of the screen). Now, (**Fig.14**) when reading the card numbers, the controller will check them against the input masks and allow (or not allow) the passage into the ATM lobby.

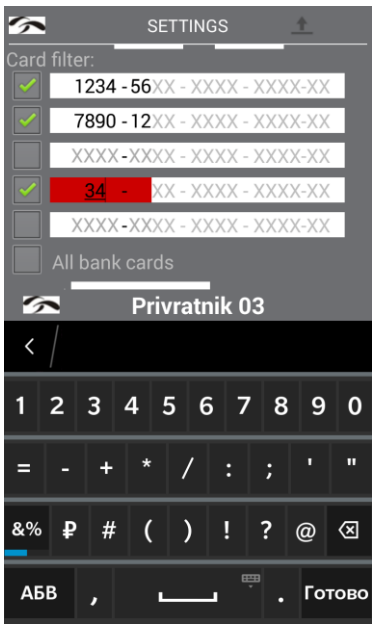

Fig. 13

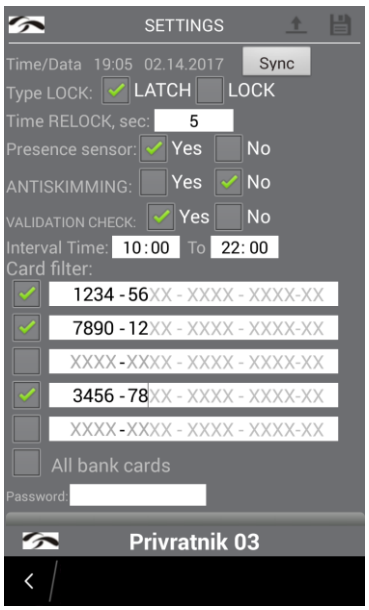

Fig. 14

Operating with the logfile of the controller

The controller can save the logfile based on passages. The log information contains the following: card number, passage time and system response to an attempt to pass. Working with the log file is available as on a smartphone – by viewing a data table with event codes. It is also possible to upload the logfile (*.csv file to a smartphone – for further work with the data table). In this case, the event codes are already replaced by the description (in English) of the events themselves, as, for example:

- *Successful passage;*
- *The card is prohibited for passage;*
- *The card has expired;*
- *The lobby is occuped by a client;*

To access the log file through the application, you must have a password. This password (PINCODE) is unique for each controller and is installed at the factory. This password is issued when selling the controller, and is specified on the final back page of this Manual.

To enter the password just go to the menu for PINCODE enter – **Fig. 16**

Fig. 16

Then you need to fully enter the password. Then you should test the controller with the settings (floppy icon in the top right corner of the screen).

After the password is correctly entered, and the controller is tested, an active **Logs** button (**Fig. 17**) will appear on the menu screen.

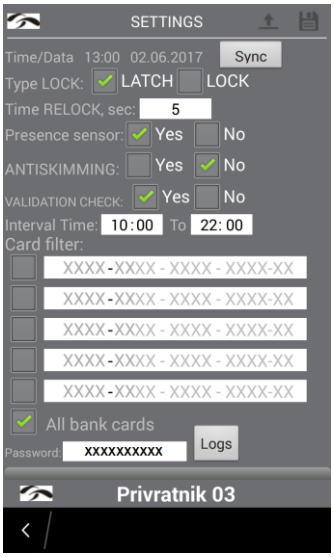

Fig. 17

Clicking the **Logs** button results in the application going to the screen for working with the log file (**Fig. 18**).

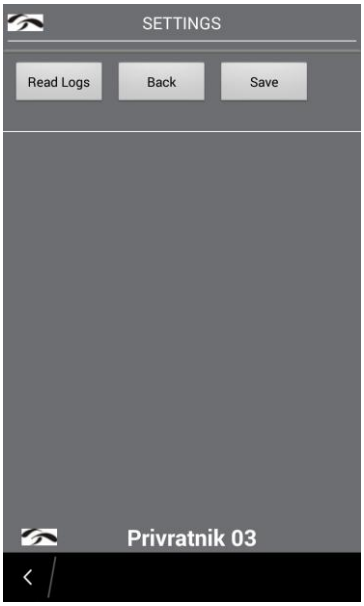

Fig. 18

Data	Time	#Card	Alarm
15/11/16	17:42:41	6390-0238-9056-715100	01
15/11/16	17:42:52	6762-3069-9516-027800	06
15/11/16	17:43:03	5106-2140-0018-524800	01
15/11/16	17:43:30	5136-9175-9959-045300	06
15/11/16	17:43:41	2204-8802-0200-206400	01
20/11/16	20:18:46	0000-0000-0000-000000	02
20/11/16	20:20:23	0000-0000-0000-000000	02
20/11/16	21:38:47	0000-0000-0000-000000	02
22/11/16	18:20:45	6390-0240-9013-753700	01
22/11/16	18:21:56	6390-0240-9013-753700	01
22/11/16	18:22:12	6390-0240-9013-753700	01
22/11/16	18:23:05	6390-0240-9013-753700	01
22/11/16	18:23:49	6390-0240-9013-753700	01
22/11/16	18:24:06	6390-0240-9013-753700	01
22/11/16	18:24:56	6390-0240-9013-753700	01
22/11/16	11:16:22	2155-2201-2311-162210	19
22/16/23	16:22:11	2422-3223-1116-221152	22
32/23/11	22:11:53	2232-2311-1622-115441	32
23/11/16	11:55:06	1623-1116-2211-555722	23
11/16/22	56:35:22	2311-1622-1209-382232	11

Fig. 19

The uploading will result in **LogFile.csv** file that will be placed by the Application in the **Download** directory on the smartphone. This file is a table one. When viewed in any table editor, the data is presented as shown in **Table 1**

Table 1

"Data"	Time	#Card	Alarm
15/11/16"	17:42:41	6290-0732-9056-715100	Successfully.
15/11/16"	17:42:52	6762-9769-3416-027800	Card prohibited.
15/11/16"	17:43:03	5206-2243-0018-524800	Successfully.
23/11/16"	12:09:32	2304-7602-0200-206400	Successfully.
23/11/16"	12:50:54	5481-7325-0154-991900	Card prohibited. Validity of the card has expired.
23/11/16"	13:05:21	2104-8102-0220-640022	Successfully.

To return to the main menu, simply press the **Back** button. The application opens with the main screen with no actual parameter settings (**Fig. 20**). After that, you need to upload to the menu windows the current settings for the controller. To do this, click on the upload icon - the symbol in the upper right corner of the menu.

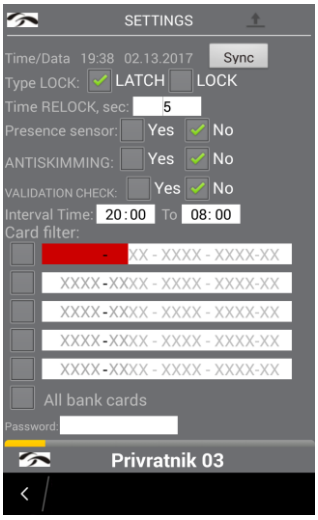

Fig. 20

After the query execution the menu windows will be filled with the current settings for the controller. (**Fig. 21**)

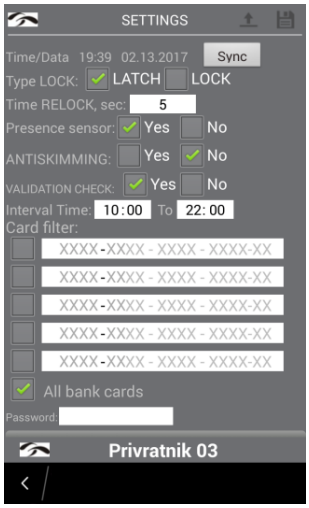

Fig. 21

Service OBD functions of the universal reader-controller "Privratnik-03A"

A distinctive feature of the controller is a built-in diagnostic function of the access control system equipment - such as the integrity of the supply and control lines for external devices (electromagnetic lock, exit button), the state of the controller itself being diagnosed as well.

This service is built on the OBD principle, the table of blink codes and audio signals indicating the equipment states is listed below:

Table 2

	System state, faults	LED illumination			Sound source
		Green	Red	Yellow	
modes	Free passage	continuously			
	Standby mode	blinks	blinks		
	Entry allowed	continuously			continuously
	Card prohibited[1]		blinks		with interval
	Skimming detected	blinks	blinks	blinks	with interval
	Client in			continuously	
	Blocking[2]		blinks		with interval
faults	Key fault[3]	blinks	blinks		continuously
	Open load		blinks	blinks	
	Card not extracted		blinks		with interval
	Communication fault	not illuminated	not illuminated	not illuminated	with interval

Note:

1. If a card of the unauthorized format is installed into the reader, the passage by its means is not allowed, and this fact is signalled by short (0.3 sec.) pulses of sound and light indication sources.
2. If Blocking mode is activated, sound and light indications are followed with pulses of 1.5-2 seconds.
3. If the exit button is pressed through, the device goes into alarm mode, in which the door is unlocked. The green LED becomes continuosly illuminated.

Additional information:

Error of the device controller communication with the reader module requires intervention at the hardware level. All other errors are reset automatically upon elimination of their causes.