BBIQ
Vychováva ľudí...

User manual for access control software BBIQ

The User manual describes the basic setting and functions of the aplication. If you need more information please contact us at rys@rys.sk

www.rys.sk
www.bezpecnebyvanie.sk

RYS®

WHAT YOU FIND IN USER MANUAL

Software BBIQ offers a number of user friendly functions for comprehensive management of the access control system in apartment buildings, office buildings and industrial complexes.

This manual describes only the basic settings for operating-memory units DS-01 (iButton) and BES-01 (RFID), creating database files (in multi-database setting) and basic functions for type of installations "Apartment buildings".

In case you will not find information necessary for your installation in this manual, please contact us at rys@rys.sk and ask about the specific function and characteristics or you may find the information on our web site www.rys.sk

Issued: ***25.8.2009***

Software: version ***3.94***
Processor used in ***DS-01****: version* ***5.2***
Processor used in ***BES-01****: version* ***4.2***

Content

PC requirements 4
Overview of supported devices and connection parameters settings 4
Installing BBIQ software 6
Starting the application 8
Creating a new database 8
Importing a database from older version of BBIQ application 11
Importing a database from DEK SIET application 12
Importing a database from RAK and MODUL DEK application 13
Adding a new device 15
On-line connection 18
Creating User groups 19
Adding a new identifier 20
Updating devices 23
Event log 24
Setting time zones 26
Activating time zone in identifier properties 27
Activating time zone in user group properties 28
Inventory Check of identifiers 29
Update using a Data Carrier 30
Settings 31
What do you need to program the identifier? 32
Operating-memory unit DS-01/485 33
Operating-memory unit BES-01 34
Technical characteristics of devices 35

PC REQUIREMENTS

Before installing the BBIQ software make sure that your computer meets the minimum hardware requirements to run the application.

Minimum configuration necessary for running the BBIQ application on your computer: 333 MHz processor, 64MB RAM, 10MB free HDD for installation of the software, 600MB free HDD space for database, graphic card and monitor with 800x600 resolution, serial port (RS232), USB port (converter USB/RS232 if necessary), or RJ45 port (for DEK SIET with Ethernet connection), CD ROM drive, keyboard, mouse, Operating system Windows 2000 SP4, Windows XP SP2, Windows VISTA.

Recommended configuration: 1 GHz processor, 128MB RAM, 1 GB free HDD, graphic card and screen with 1024x768 resolution, serial port (RS232), or RJ45 port (for DEK SIET with Ethernet connection), USB port (converter USB/RS232 if necessary), CD - Writer drive, keyboard, mouse, sound card and speakers, Operating system Windows 2000 SP4, Windows XP SP2, Windows VISTA.

OVERVIEW OF SUPPORTED DEVICES AND CONNECTION PARAMETERS SETTINGS

BBIQ software is designed especially for the operating-memory units used in access control systems and for traffic (entry/exit) control in secured areas, remote system management and photo-identification. BBIQ also supports devices suitable for office and industrial application such as the MEK – manager of electronic keys or the simple Time & Attendance system.

The BBIQ parameters settings depend on system/network connection (e.g. RS485, Ethernet…)

TYPES OF HARDWARE DEVICES SUPPORTED BY BBIQ

Access control system DEK SIET with iButton technology

OPJ DS-01/232	standard unit with RS232 interface, autonomous
OPJ DS-01/485-ZPK-PPM	standard network unit with RS485 interface
OPJ DS-01/ETH	standard network unit with Ethernet interface (connection via ETHERNET)
OPJ DS-01/KLON	network unit enables optional control of one or two relays at the same time using one touch probe. Does not support door status time control function.
OPJ DS-01/DUO	network unit enables independent control of two relays (doors) using two separate touch probes. Does not support door status time control function.
OPJ DS-01/4RELE	network unit with independent control of 4 relays (using 4 touch probes), suitable for lift control.

Proximity access control system BES with RFID technology

OPJ BES-01	Standard network unit with RS485 interface
OPJ BES-01/ETH	Standard network unit with Ethernet interface (connection via ETHERNET)
OPJ BES-01/KLON	network unit enables optional control of one relay or two relays at the same time using one touch probe. Does not support door status time control function.
OPJ BES-01/DUO	network unit enables independent control of two relays (doors) using two touch probes. Does not support door status time control function.

Low consumption DEK SIET system with iButton technology

OPJ DS-01/EDC	Stand alone unit with own power source, RS232 interface

Other devices

GSM concentrator	GSM concentrator device enables connection and communication between operating-memory unit via existing GSM network – remote control
MEK	manager of electronic keys, device for electronic control and management of keys, the electronic tag with iButton technology is used for registration of the keys.

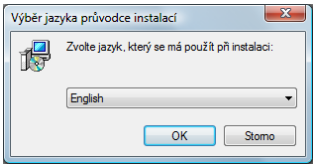
Table shows how to assign available hardware devices (operating-memory units = OMU) to a BBIQ device description.

Description of the device in BBIQ application / Hardware device	DEK(iButton) / BES(RFID) memory unit	KLON memory unit	4RELÉ memory unit	EDC low-consumption memory unit	GSM concentrator	MEK manager of electronic keys
DS-01/485-ZPK-PPM	X					
DS-01/485 (with voting option)	X					
DS-01/232	X					
DS-01/DUO	X					
DS-01/KLON		X				
DS-01/ETH	X					
DS-01/ETH+DUO	X					
DS-01/4RELE			X			
BES-01	X					
BES-01/DUO	X					
BES-01/KLON		X				
BES-01/ETH	X					
BES-01/ETH-DUO	X					
BES-01/FLASH	X					
DS-01/EDC				X		
GSM concentrator					X	
MEK						X

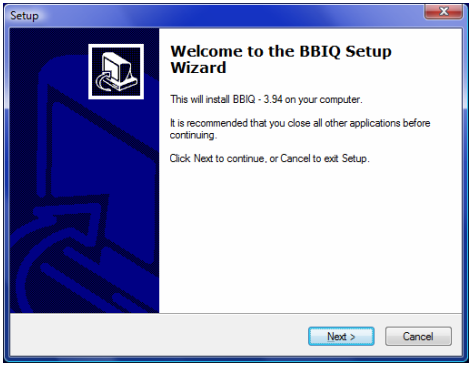
INSTALLING BBIQ SOFTWARE

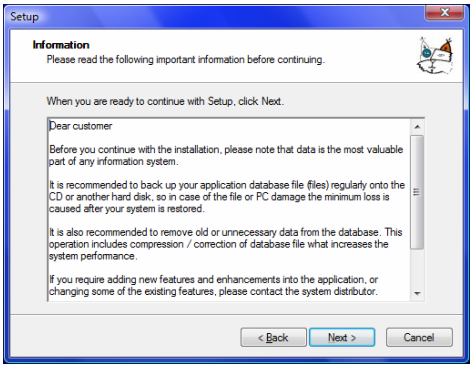
Software can be installed directly from the distribution CD or from your PC, just copy all the installation files into selected folder. The latest version of installation file for BBIQ can be downloaded free from our web site www.rys.sk

- Run the installation file **bbiq_X_XX_setup.exe** (X_XX is number of latest software version). After you run the exe file you will be asked to select the installation language, select the desired language and click **OK**.

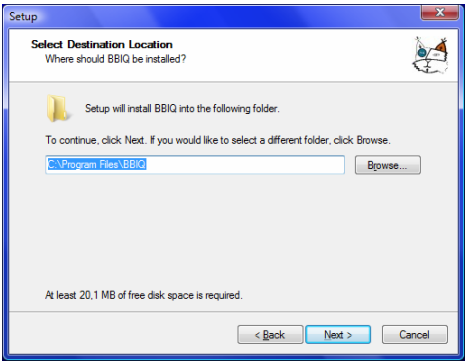


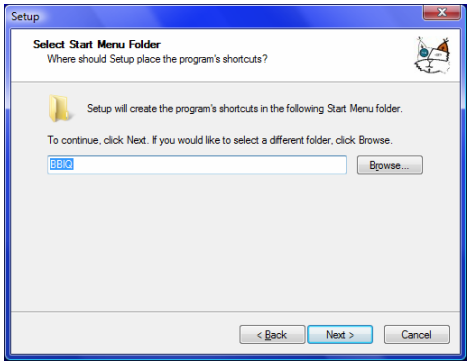
- The setup window **Welcome to BBIQ Setup wizard** is displayed. Click **Next**.
- Next window displayed is **Information**. You are advised to read the data security recommendation carefully before proceeding with the installation. Then click **Next** and proceed with the installation.



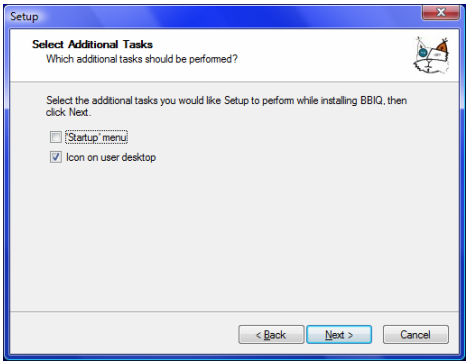


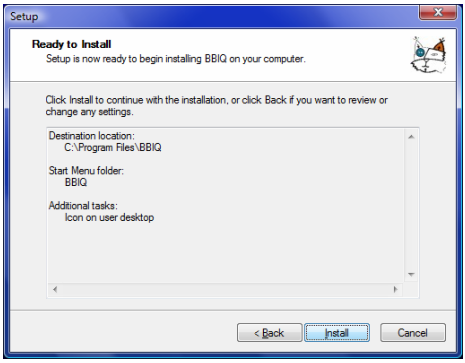
- In the displayed window **Select Destination Location,** choose your target folder for BBIQ installation. The application automatically offers you the **Program Files/BBIQ folder**, you can leave the present one or change it as you wish by clicking Browse. After setting the target folder click **Next**.
- In **Select Start Menu Folder** window, choose the folder to create application shortcut in Start Menu. After setting the folder click **Next**.



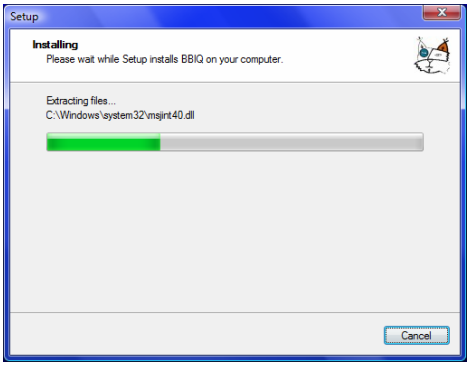


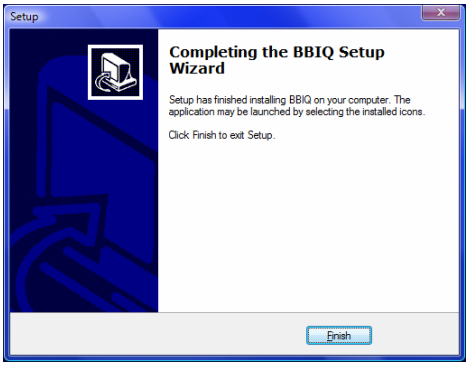
- In **Select Additional Task** window define what other tasks you want to perform in Setup . If you wish to place the application shortcut on your Desktop screen tick the option **Icon on user desktop**. You can also set the application to be run at the computer startup by ticking the option Startup menu. Click **Next**.





- Check your setting in **Ready to Install window**. If you do not wish to make any more changes click **Install**.
- Installation will start.





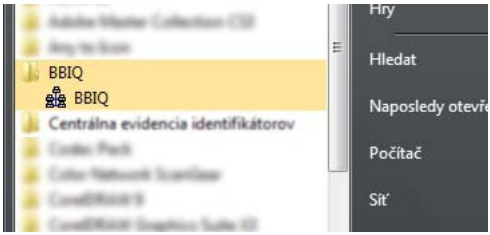
- To complete the installation click **Finish** in **Complete the BBIQ Setup Wizard** window.

A message box asking you to restart your computer may appear before the installation is finished. In that case you must restart your computer to complete installation successfully.

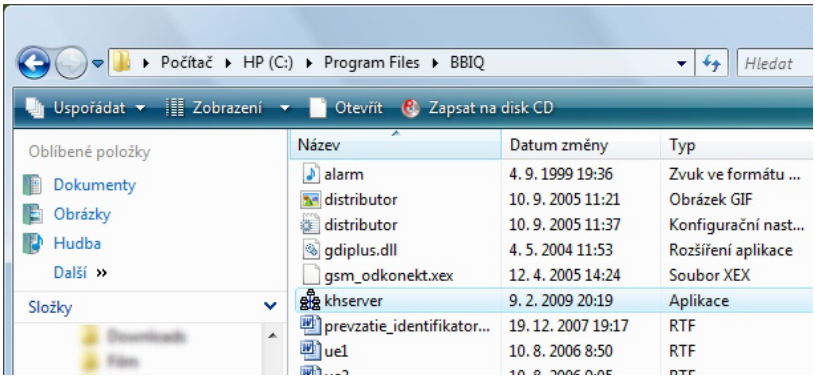
It is recommended to restart the computer after the installation of BBIQ is completed even the restart message does not appear.

STARTING THE APPLICATION

- To start the application go to **Start** → **All programs** and click the folder **BBIQ** (the folder name might be different based on your settings during the installations).
- You can start the application by clicking the shortcut (icon BBIQ) on your desktop. This is possible only if you set this option during the installation.



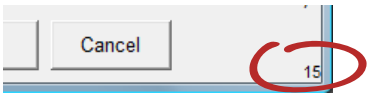
- The application can be started also directly from the **Program Files/BBIQ** (or from a directory which you selected during installation). In Start Menu click **Computer** (This computer) and then find the above specified location.



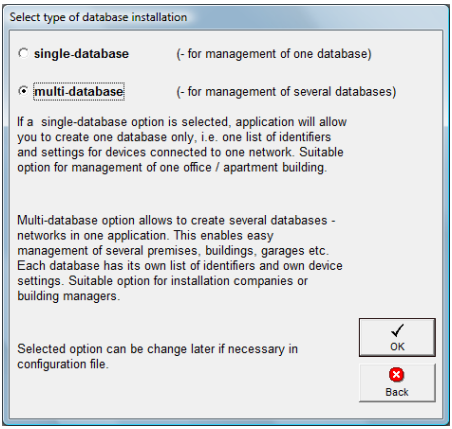
CREATING A NEW DATABASE

When the application is started for the first time no database exists in the system. It is necessary to create a new database.

BBIQ application restricts the view of dialogue windows/boxes to 25 seconds. If no option is selected within this time, the window will automatically close. To call the dialogue window again it is necessary to repeat the particular option. 25 seconds countdown is shown in right bottom corner of the dialogue window.



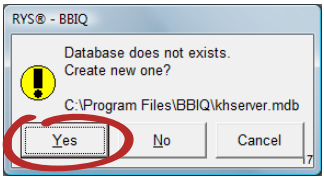
- When the application is started the **Type of installation** must be selected – *single-database* for managing one database of identifiers (one building, system is managed e.g. by the owner, building janitor) or *multi-database* for managing several different databases (several entrances, buildings, premises and the systems are managed by an installing company or a building management company). Select type of installation and click **OK**.



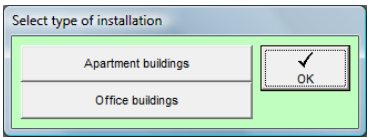
It is recommended to select the multi-database installation .

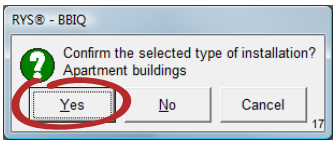
Type of the database installation (single/ multi database setting) can not be changed in application settings later on. This change can be done only in the configuration file. If the change is necessary please contact your distributor / supplier or RYS technical support for more information.

- Next step is to create a new database file. Confirm **Yes**.



- Select **Type of installation** - Apartment buildings or Office buildings. Click **OK** and then click **Yes** to confirm your choice.

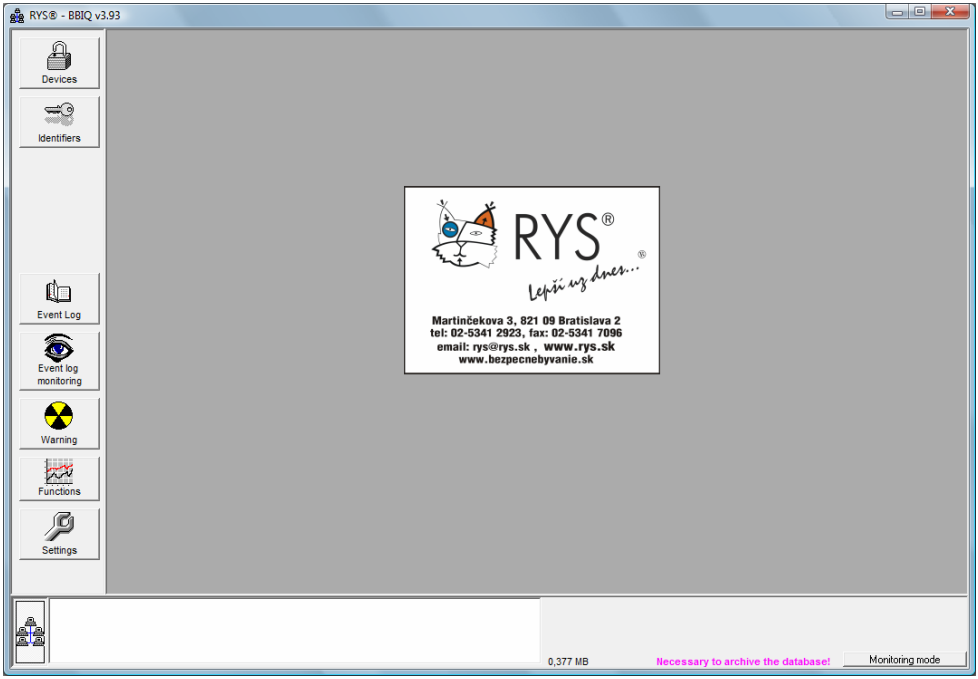




- ***Apartment buildings*** *– standard function suitable for managing the access control system in a multi-apartment building / block of flats*
- ***Office buildings*** *– extended options for identifier properties, additional functions like Time & Attendance, Guard Tour system etc.*

This manual describes only the basic functions for Apartment buildings type of installation.

- The main application window will display after confirming one of the installation type options .

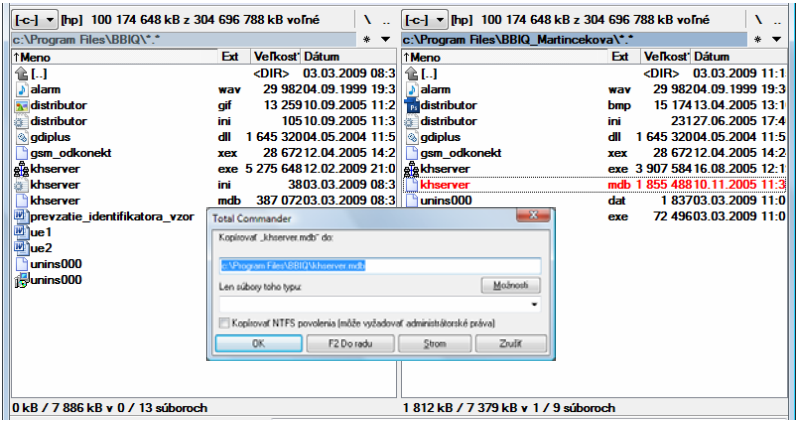


BBIQ application enables import of already existing databases which were created in older versions of BBIQ or different applications (for access control systems) like DEK SIET, Modul DEK and RAK. ***If you want to create completely new database go to page 15.***

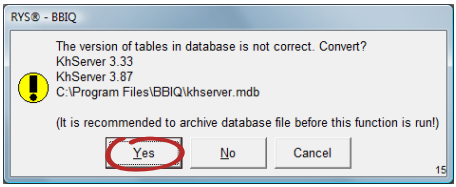
IMPORTING A DATABASE FROM OLDER VERSION OF BBIQ APPLICATION

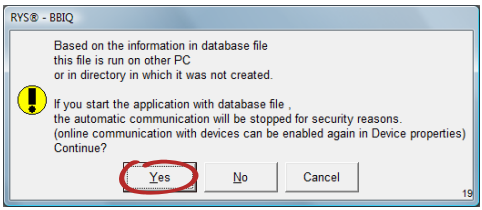
If you wish to work with the already existing database created in a lower version of BBIQ or created on other computer in BBIQ, follow these steps:

- Copy the existing database **khserver.mdb** (if it has a different name, change the name to khserver) into BBIQ folder (the folder you created during the installation of the latest version of BBIQ).



- Run the **BBIQ** application. There is no need to create new database (page 8), but the application will warn you that the database you are about to open, was not created in the currently run program. If you want to continue working with the copied database, click **Yes**.
- Application will require a table conversion if the copied database was created in a lower version of BBIQ. Click **Yes**.





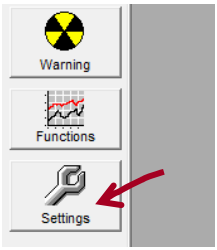
- If the application is started with the copied database, the communication with devices will be automatically stopped for security reasons. Click **Yes**. The communication must be restored later on in the application *Settings*.

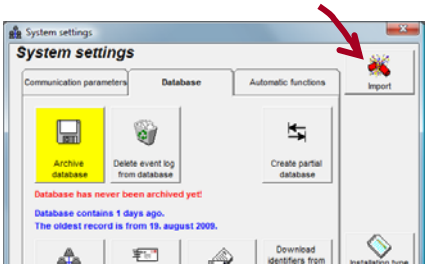
IMPORT A DATABASE FROM DEK SIET

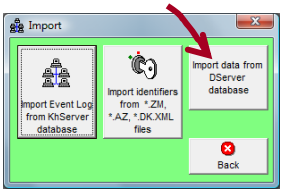
BBIQ application enables to import the data from **DServer.MDB** file created in DEK SIET application. Only the list of identifiers and devices is imported, not the event log.

To use this Import, no identifiers or devises can be defined in the BBIQ application; the application must be "empty". Otherwise the Import button will not be displayed. It is recommended to import this type of the file into newly installed BBIQ application.

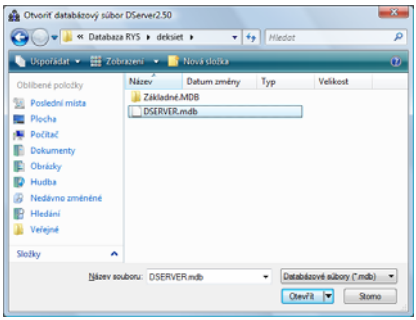
- To set the system parameters click on **Settings** button in the main application window.
- Then click **Import** button and in the next dialogue box click **Import data from DServer database**.

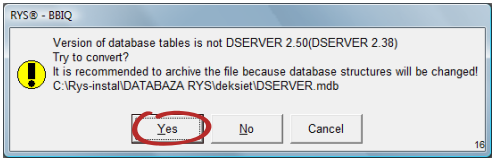






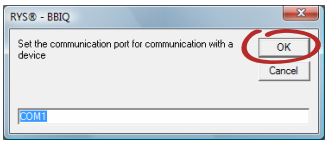
- Confirming the type of imported file a new window will display. Locate the folder with DEK SIET database file and click **Open**. A dialogue window with warning message about converting the database will open. Confirm **Yes**.

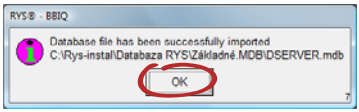




- Set the communication port. This is necessary to continue import (after you complete the import, the communication port can be changed). Click **OK** to start the import of database into BBIQ application.

- If the database file was imported correctly, a message will be displayed. Click **OK**.





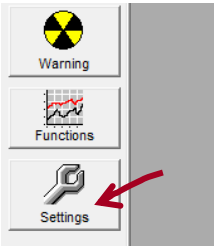
- You will return to the **Import** dialogue window. You can return to main application window and view imported data:
  - In the main window click **Devices** – imported **List of devices** will display, all device will be in off-line mode.
  - Click **Identifiers** in the main window – imported **List of identifiers** will display.
  - Click **User groups** in the **List of identifiers** - imported **User groups** will display.

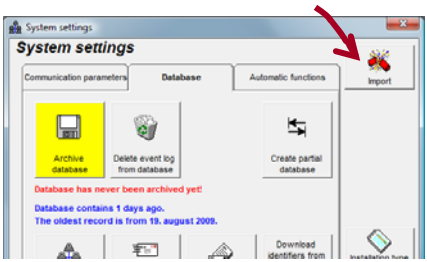
IMPORTING A IDENTIFIERS FROM RAK AND MODUL DEK

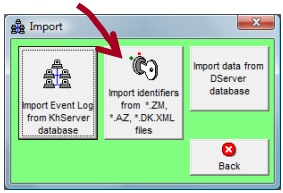
BBIQ application supports import of identifiers from file with extension DK.XML (e.g. martincekova.dk.xml) created in RAK application software or from files with AZ and ZM extensions (e.g. martincekova.zm).

Before importing, create devices (page 15) or user groups (page 19) to which you assign the identifiers during the import process.

- Click **Settings** button in the main application window, Settings options will display.

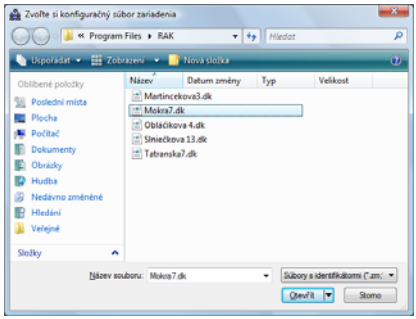






- Click **Import** button and then select **Import identifiers from ZM, AZ an DK.XML files**.

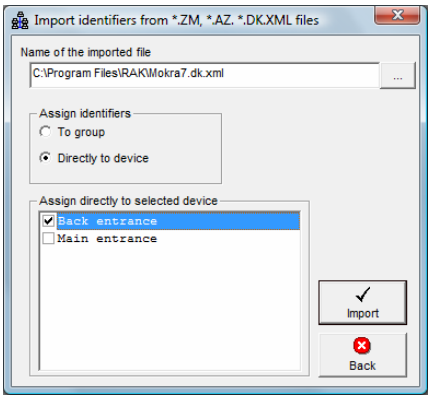
- Confirming the type of imported file. A new window will display where you can locate the folder with database to be imported.
- Then click **Open**.

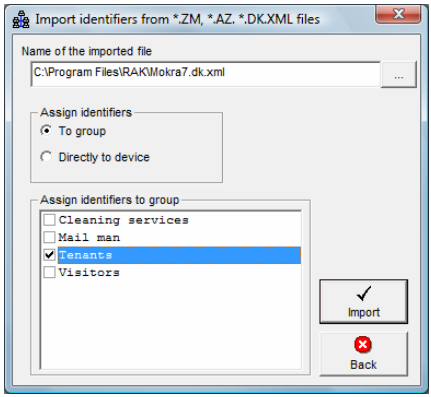


- Application will ask you to define the options for the identifier import based on pre-set definitions of *Devices* and *User groups*.

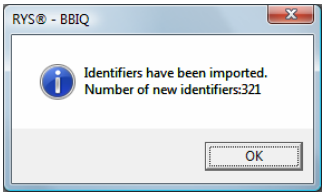
If you have no Devices or User groups defined you have to disrupt the import process and first set these definitions (page 15 and 19).

- Identifiers can be assigned directly to the selected device or user groups.





- Confirm settings by clicking **Import**. Identifiers will be imported. When the import is finished the following message will display:

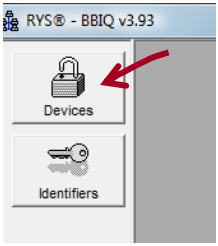


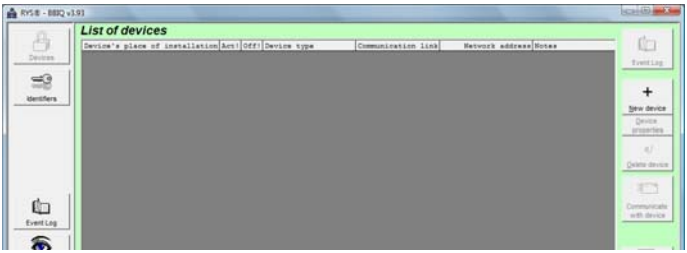
- Click **OK** to return to *Import* window, then you can return to main application window and view the imported list of identifiers. All identifiers from imported database will be displayed.

If you imported identifiers into the application with already existing list of identifiers, the imported identifiers are added to the existing list. Make sure you archive the original database before each import to avoid any unwanted overwriting.

ADDING A NEW DEVICE

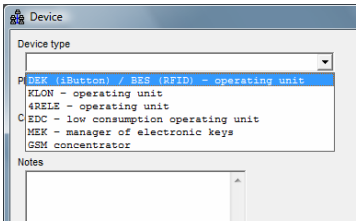
- Click **Devices** button in the main application window. A new window with **List of devices** will display.

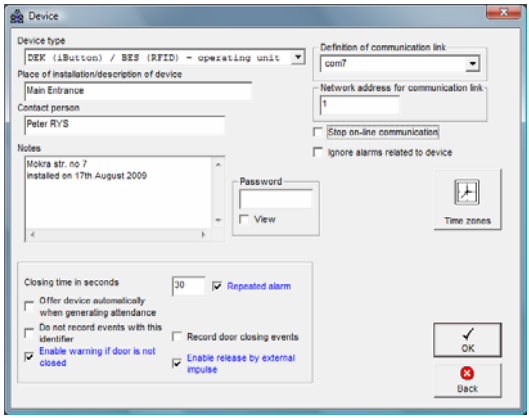




- In **List of Devices** click **New device**. The **Device** window will display.

Type of setting described in this manual is suitable for operating-memory units DS-01 and BES-01 which operate with different technology of identifiers (iButton/RFID). The rest of software characteristics are the same for both units and so they are defined under one name – DEK/RFID network module in BBIQ application.
(more about hardware devices on page 4,5)





Description of *Device* settings

Place of installation – defines where the unit is installed in the building/on the premises.

Contact person – a person responsible for access control system management and maintenance.

Notes – information concerning the unit or installation.

Definition of communication link – communication port on PC used for communication with the device. Define port as e.g. **com1** *(a programming-converter unit is necessary for connection of the device to PC, page 35).*

Network address for communication link – network address of the device (address can be set from 0 to 31). The same address must be set on the device (hardware setting with DIP switch).

Stop on-line communication – the communication is automatically turned off when adding the new device into the list in order to protect other connected devices. If the device is off-line, the name of the device is red with *Off!* indication in the list of devices.

If you want to turn the device to on-line operation untick the check box "On-line communication switched off". The on-line operation for the device will be restored.

Ignore alarms related to device – this function is used when there is no need to display warnings related to the device.

Closing time in seconds – time limit for closing the door before the alarm is set off. This function requires installation of electric lock/door strike with tamper. If the door is not closed properly within the set time, the alarm goes off. Another hardware e.g. siren, buzzer, warning light is necessary for the alarm function. If this hardware is not available, the alarm event will be recorded into the event log but there will be no acoustic or visual alarm signalling.

Repeated alarm – when the door is open too long (exceeds the set time) the alarm is set to go off only once. If it is necessary to repeat the alarm until the door is closed, select this option.

Offer device automatically when generating attendance – function is suitable for installation in Office building with simple time&attendance control of employees.

Do not record events related to identifier – select the option if it is not necessary to record the events with identifiers assigned to particular device, e.g. to save the space on the PC disk or the device is installed in the discrete area.

Enable warning if door is not closed – if the person uses the identifier to open the door and then does not close the door correctly within the set time limit, this function will set warning for the user. Next time the identifier is used the alarm goes off automatically. The access control system operates as warning or caution element.

Record closing events – selecting this option the system will make a record of events reporting opening and also closing the door. This function requires electromagnet with signaling output or some other detecting component – tamper.

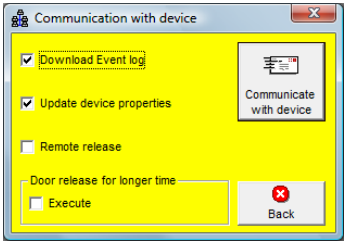
Enable release by external impulse – this option can be used for operating-memory units with ZPK (switching contacts) function supported. Function enables to release the door by impulse sent from e.g. apartment phone or exit button to the switching contact on the operating-memory unit. Door are released for the time set on the operating – memory unit, this setting is done with DIP switches, the event log will display a line with "*Release by external impulse*" reference.

Password – it must be define if Data Carrier (memory iButton) is used. Detail description of this function and settings is on page 26.

Time zones – description of the function is on page 26.

Setting time zones requires to have complex overview of user rights and identifier properties, therefore this function is explained separately. It is recommended to set time zones after the basic device and identifier settings are finished.

- After setting the device properties confirm **OK**. The device will be added to the list of devices. Two buttons **Communicate with device** and **Update info** will start flashing on the right menu bar.
- If the device is correctly connected to PC start the update by clicking the **Communicate with device**. A new dialogue box **Communication with device** is displayed.



Description of *Communication with device* options

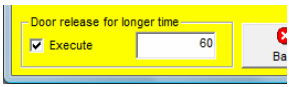
Communicate with device
The button is used to establish immediate and direct communication connection with the selected device even the on-line communication function is off. When the connection is activated, these options can be selected:

Donwload Event log
Select if you want to download the Event log from the device during the download communication.

Update the device parameters
Select when the update of device parameters is needed, e.g. the properties of the device were changed; some identifiers were added or deleted into the database etc. If the update is required this option will be automatically selected.

Remote opening
Select if you want to activate the immediate remote door release.

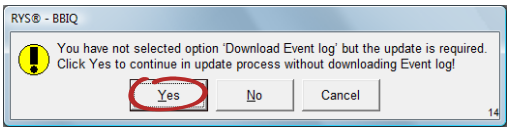
Door release for longer time – when the option **Execute** is selected the door will stay released remotely from PC for the duration set in minutes, max. 250 min. Door will be automatically secured (locked) after the set time will pass.



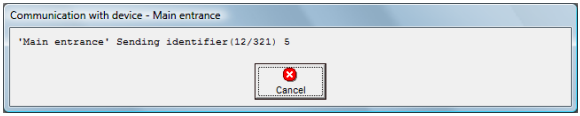
If you want to disrupt the door release and secure the door sooner (e.g. the set time might be 60 min. but it is necessary to secure the door after 30 min.), you can do so by repeatedly selecting the option "Door release for longer time" and setting the duration for 1 minute. Door will be secured in 1 minute.

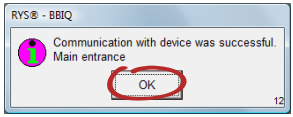
In case you need to add quickly one or several identifiers into the device and you did not downloaded the event log from this device for a long time, it is recommended not to select the option Load the event log*. This will save your time because the Update will be proceeded very quickly as only the new data will be sent to the device.*

- When the properties are being set for the first time, select only the function **Update device parameters**. Click **Communicate with device** and communication will start according to the settings. Application might ask to confirm the update action. Click **Yes** if you really want to update the device.



- Click **Yes** and the communication will start according to the settings.
- After the communication was successfully finished click **OK**.





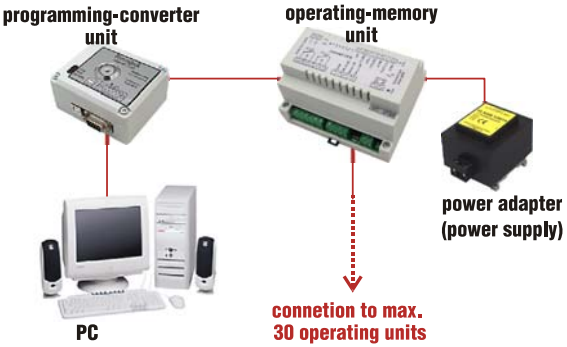
The update of the device and the download of the Event log requires that the device is connected on-line to PC from which the data is sent.

Update info

This function is used to view information about changes in device property settings that require the update. After the update is finished the information from the list in *Update info* will be automatically deleted and the button disappears.

ON-LINE CONNECTION

The on-line connection is required for update and download of the Event log. The operating-memory unit is connected to PC via programming-converter unit PPM/USB-485, (for OMU with RS232 output use suitable cable).



Access control system DEK SIET and BES enable connection of 31 operating-memory units into one network. These units can operate on-line and off-line. The units are connected to converter in parallel.

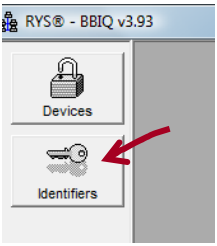
In case, there are several operating-memory units connected to the network, it is necessary to select suitable and sufficient power supply, because it can supply also other devices like door strikes or a siren.

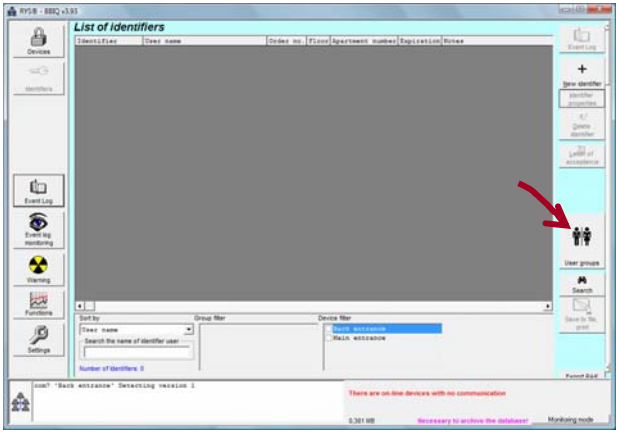
In order to provide the correct operation of the network with several OMUs, it is recommended to install a separate power supply for each unit .

CREATING USER GROUPS

If it is necessary to give users different access rights, the User groups can be created. Each group has defined conditions for using selected devices. ***It is recommended to created the user groups before adding identifiers into the database.***

- Click **Identifiers** button in the main application window. The **List of identifiers** will display.
- Click **User groups** on the right menu bar.





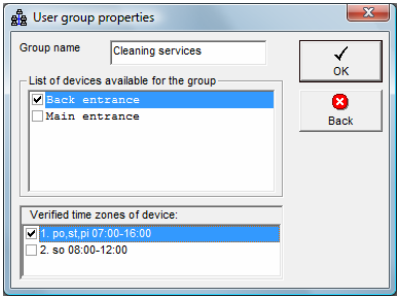
- In the User group window click **New group** to set the group properties.

Description of the Group properties settings

Group name – the name for the group of identifiers

List of devices available for the group – select those devices which will be enabled for the group, e.g. the door used by the group to enter/exit premises.

Verified time zones of device:
The time zones set for the selected devices are displayed. If you wish to set the time zone for the group, select the particular time zone/zones.



Time zone will not display in this window if the condition "Door always open" is set for the time zone.

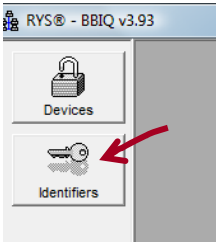
- After settings are done, click **OK**.
- Identifiers can be assigned to the user group in identifier properties – see page 20.

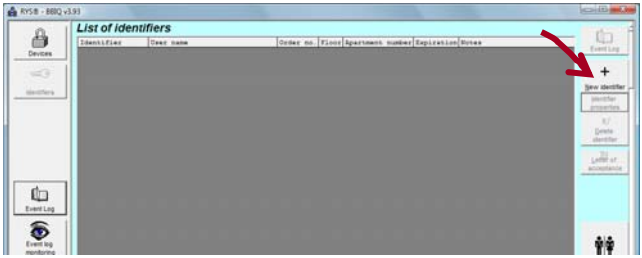
ADDING A NEW IDENTIFIER

What are identifiers?

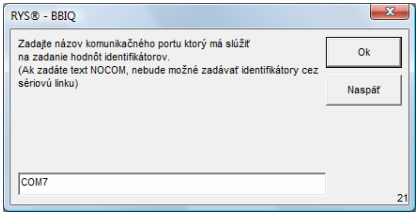
Identifiers are electronic devices with a microchip inside. They are parts of access control systems used for controlling the electronically secured door. System DEK SIET uses iButton identifiers (touch electronic keys), and system BES uses RFID proximity tags and cards.

- In the main application window click **Identifier** button. The list of identifiers will display, here you can set the properties.



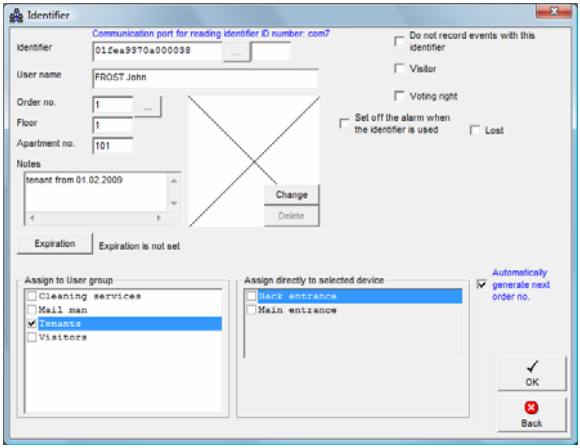


- Click the **New identifier**, the application may ask you to define the communication port for reading identifier ID number – communication port used by programming-converter unit.



The setting/modifying communication port can be also done in **Settings → Communication properties → Communication port for reading identifiers ID no**.

- Confirm **OK** and the window with identifier properties will display.
- Place the identifier to the reader/ touch probe on the programming-converter unit. The ID number of the identifier will appear in the **Identifier** code text box.
- Set other identifier properties.



Description or settings in *Identifier* window

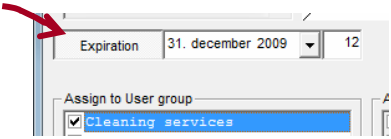
Automatically generate next order number
This function is used when several identifiers with same properties (name, floor, apartment, user group) are being added. After setting the first identifier, application will automatically set the same properties for the next one but will change its order no.

Order no.
Click the button … and the application automatically generates the order no. for identifier which is assigned to the already existing user.

It is recommended to use order no. for the flat not the user name (i.e. order number represents the number of identifier assigned to one particular flat). When this automatic function is used, it is possible to change the name of the user.

Practical use of the function – Order number
This function is helpful when identifier is added to existing database. It is not necessary to go through the whole list and check how many identifiers the user/flat already has assigned, application will detect this automatically and generates the next order no.

Expiration
Function is used to set duration of identifier validity. Click **Expiration** and define the date (calendar will appear when clicking the arrow) and hour of the expiration. The identifier will be still active during the set hour.



Expiration function can be used only with on-line connection and the Automatic update must be set too (see Settings).

Do not record events related to the identifier
If you do not wish to record events related to the identifier into the Event log select this option.

Visitor
If the identifier user is not a resident in the apartment building but still authorized to enter the premises (grand mother, nanny, nurse etc.) it is recommended to indicate this identifier as a Visitor. If this option is set in the identifier properties, the identifier will be singled out to a special group for evaluation of some functions like e.g. inventory check. The option Voting right is disabled for identifier set as a Visitor.

Practical use of function – Visitor
This function can be used to monitor black tenants. It is possible to generate inventory check for identifiers set as a Visitor and based on frequency of entries and exits find out whether the user is really just a visitor or whether he/she permanently inhabits the apartment (this is important in apartment buildings where the amount of rent payment depends on the number of co-tenants in one flat).

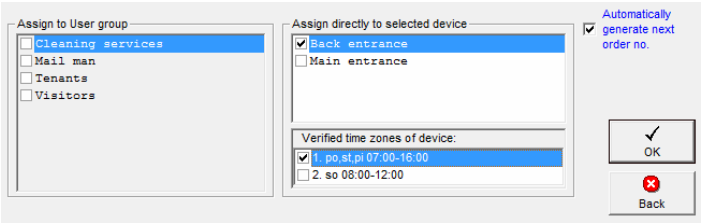
Voting right
This function requires hardware adjustment – operating-memory unit must have outputs for voting buttons. If the hardware supports this function and the identifier has voting rights, select the option.

Set the alarm when identifier is used
Select this option if you want the application to set off the alarm every time a particular identifier is used. As soon as the identifier is used the visual and acoustic alarm is set off. To stop the alarm click **Confirm**. To have the acoustic alarm the sound card and speakers on your PC is required.

Lost
Select this option if the user reports the identifier as a lost one. The identifier will be deactivated but it stays registered in the database. In case the user finds the identifier simply untick the check box and the identifier will be activated again. This function is also useful for special service SaNI (Lost and Founds of Identifiers) www.rys.sk/sani.

Change
Click the button **Change** to add the user photograph in jpg format.

Assigning to the group / assigning directly to the device
One of the very important identifier properties is the ability to control devices connected within the access control system. The devices that can be controlled by the identifier as well as the time restriction for the identifier can be set in boxes **Assigning to the group** and **Assigning to the device**.

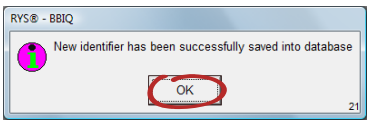


It is recommended to set only one of the assignment options for the identifier. Using both options for one identifier can cause confusion.

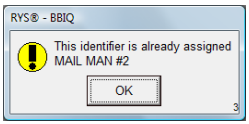
Assigning to the group
If the user groups are created, the identifiers can be assigned to the selected group/groups by ticking the particular check box.

Assigning to the device
Identifier can be assigned directly to the device. When the device is selected, the time zones set for the device are displayed in box *Verified time zones*. Selected the time zone will be activated for the identifier.

- When all properties are set, click **OK** to confirm your settings. If the identifier was successfully added to the database, a confirmation message will appear. Click **OK**.
- To add next identifier, follow the same procedure.



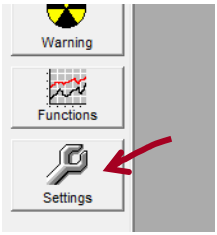
In case you are trying to add an identifier which is already in the database, a warning message will appear.

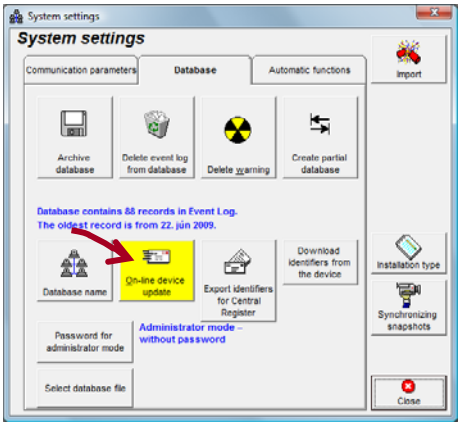


UPDATING OF THE DEVICES

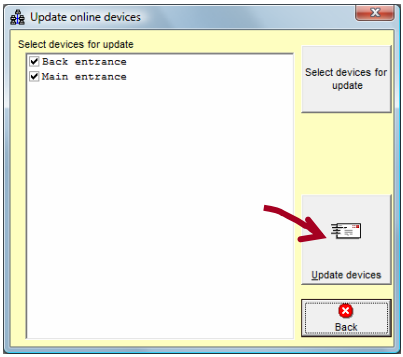
The update of devices is necessary if you did some changes in system or identifier database settings. An on-line device (connected to PC, with on-line communication switched on) can be updated using the **On-line devices update**.

- Click the **Settings** button in the main application window. New window with menu for system parameters settings will display.



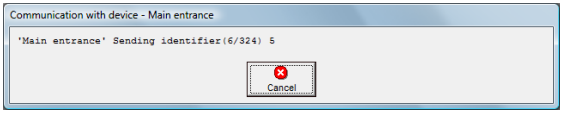


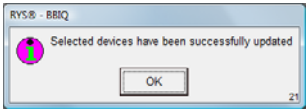
- Click **On-line devices update** button to display the list of on-line devices.
- Select devices and click **Update devices**.



*When you click **On-line devices update** the application will automatically select the devices which should be updated. But you can do so also manually by clicking **Select devices for update** in the right menu.*

- The progress of the update process can be monitored in displayed a dialogue box **Communication with device**. When the process is finished, click **OK**.





*The update of devices can be done also in the menu **Devices** → **Communicate with devices** – page 17, 18 or using the **Data Carrier**, page 30.*

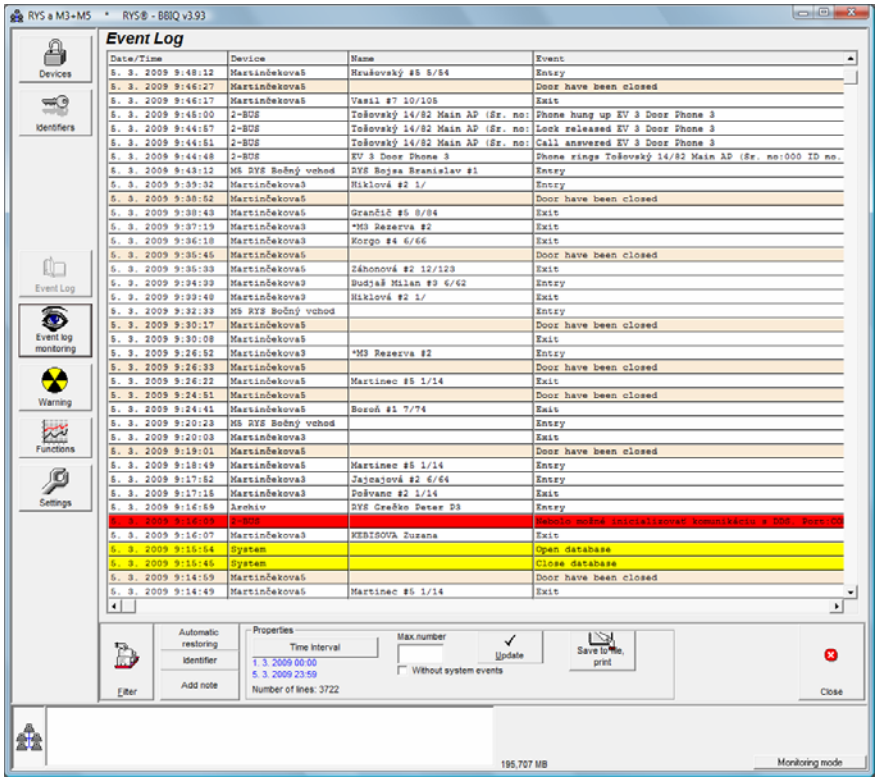
EVEN LOG

Open Event log to view the new and older user or system events (entries, exits, remote opening, addressable opening from apartment, updates, warnings etc.). Event log supports also events filter – by date, device, identifier or some other specific characteristics. When the event log window is open, only the events from current day are displayed.

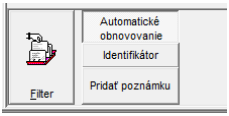
The lines in the event log have different colours to indicate different types of events:

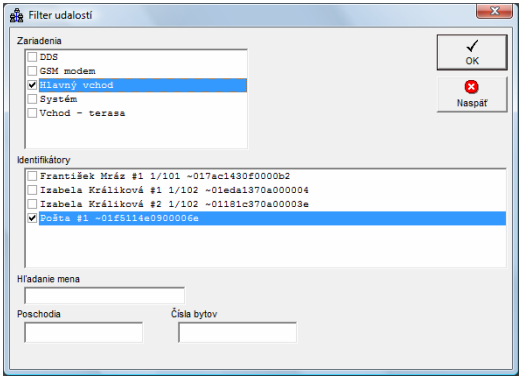
White line – standard event
Red line – warning, notice, alarm, e.g. unclosed door
Yellow line – system event
Orange line – user note
Blue/Green line – communication event
Pale orange – records of door closing

*When the **Event log** is open only events from the current day are displayed. If you need to view events from a different time period use the function "**Automatic restoring**", page 25.*



Description of settings in *Event* log window



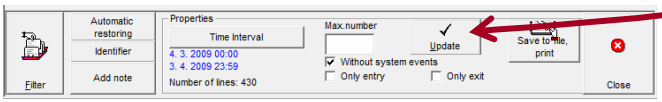


Filter

Click Filter and specify the terms of sorting the events. The event can be sorted by device, identifier, name etc. (the options can be combine). When the terms are set, click *Update*.

Automatic restoring

If this function is not active, the event log will display only events from the current day. Click *Automatic restoring* to expand Filter menu.



*Set/change the terms for displaying Event log and click **Update**.*

Identifier

To view the identifier ID code in the Event log, click *Identifier* button. After activating this option, Event log will be empty. Click *Update* button to refresh the Event log window. A new column with ID code will appear in the log. To cancel this option click *Identifier* button again – deactivate the button.

Add note

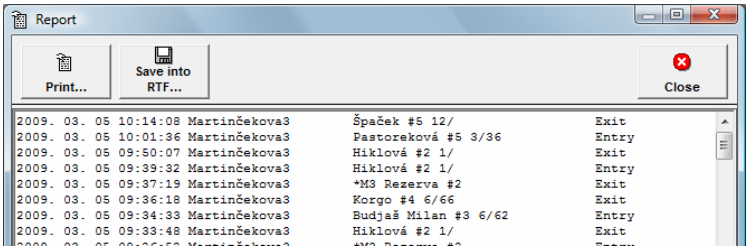
This function is used to add a note into the Event log. Relevant information can be noted for selected identifier or device.

Update

The Event log window will stay empty after each change of Filter settings. The button ***Update*** must be clicked to refresh the window and view the events based on the selected Filter options.

Save to file, print

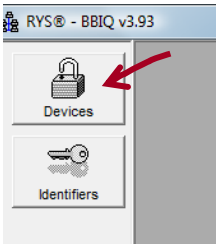
To generate events *Report* suitable for printing, click **Save to file, print** button. Then click **Print …** to sent the file to printer or **Save in RTF …** to save the file in .rtf format, application will ask to select the target directory and enter the name of the file.

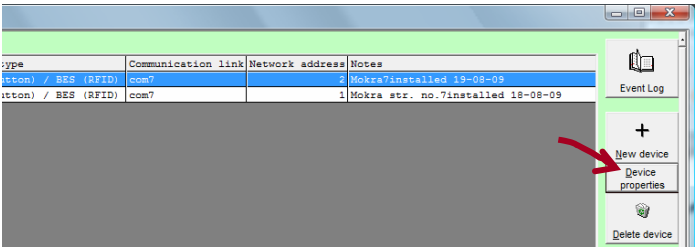


SETTING TIME ZONES

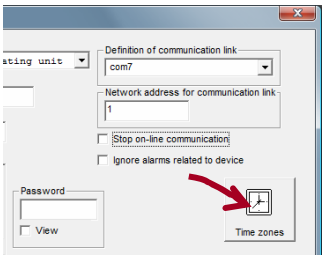
Time zones can be set in device properties. Time zones are defined in order to restrict use of selected devices for specific hours and days. If the traffic control in the building requires time control of premises and entrances, time zones are suitable solution. Time zones are set for each device separately.

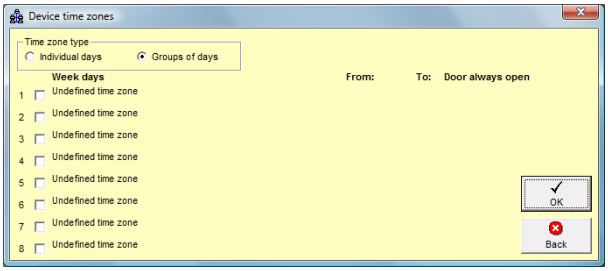
- Click **Devices** in the main application window. **List of devices** will display.
- Select the device (with cursor) for which you want to set the time zones and then click **Device properties**.





- Click **Time zones** and a new window **Device time zones** for zone settings will display.

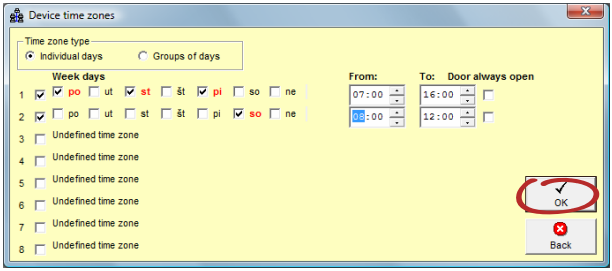




- Select one of the options to define the time zone **Individual days** or **Groups of days**. Only one of the options can be selected for the device, they can not be combined.

Individual days

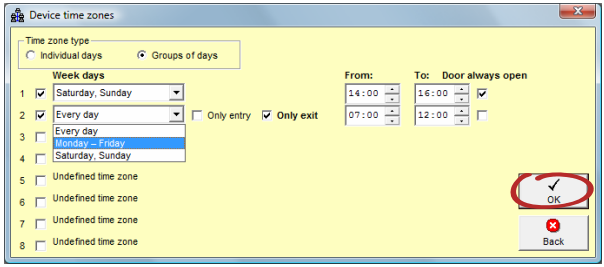
- Select option **Individual days**.
- Tick the box next to the *Undefined time zone*, more options will display.
- To set the time zones validity period, select the **Days in week** and specify the time **From – To**.



- If the door should be permanently open (released) during the time zone validity period (e.g. opening/ office hours), tick the box **Door always open**.
- Confirm **OK**.

Groups of days

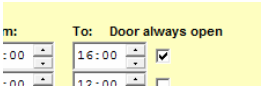
- Select the **Groups of days**.
- Tick the box next to the "*Udefined time zone*" order number, more options will display.
- Click the arrow of select menu and choose of the three time intervals (**Every day**; **Monday – Friday**; **Saturday, Sunday**).



- **Only Entry / Only Exit** select if only entry or exit should be permitted during the time zone validity period.
- Set the time interval **From – To** for the time zone validity period.
- If the door should be permanently open during the time zone validity period (e.g. opening/office hours) tick the box **Door always open**.
- Confirm **OK**.

*If the **Door always open** option is selected, there is no need to do any setting in identifier properties. Time zone will be active after confirming **OK** in Device time zones window.*

In case other types of time zones are selected, it is necessary to modify settings in the identifier properties to activate the zones.

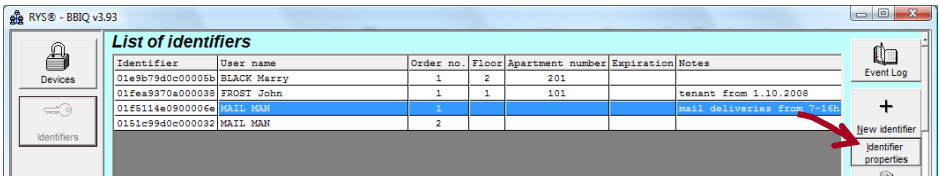


- When the time zones are set, the **Time zones** button will be yellow in the **Device properties** window (it means the time zones are set and can be activated).
- To activate the time zones go to identifier properties or to user group properties.

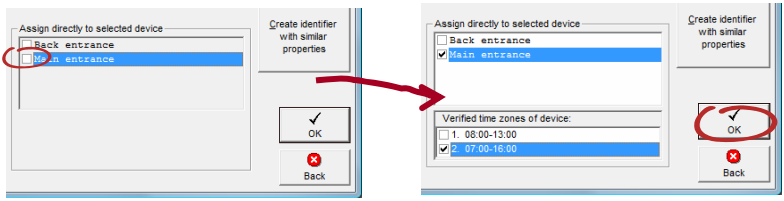
ACTIVATING TIME ZONES IN IDENTIFIER PROPERTIES

The time zone can be activated in section Identifiers and then either in **User groups** or **Identifier properties**. These settings are possible only when the list of identifiers is already created.

- To assign the time zone, select the identifier in the **List of identifier**. Click the line of the selected identifier and then click **Identifier properties** button from the right menu.

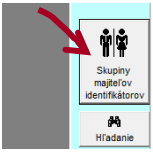


- Assign the identifier to the device with defined time zones – select the device in **Assigning directly to selected device**.

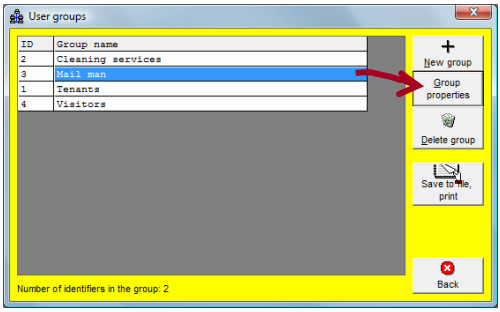


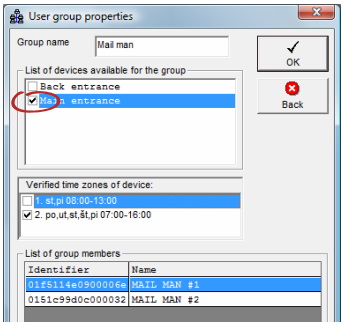
- When the device is selected, the defined time zones for this device will appear – **Verified time zones of device**. Select the time zone which you want to assign to the identifier (if the identifier is already assigned to this device, the device time zones will display automatically after the Identifier properties window is opened).
- Confirm **OK**. The time zone is activated for the selected identifier.

ACTIVATING TIME ZONE IN USER GROUP PROPERTIES



- In **List of identifiers** click **User groups**, existing user groups will display.
- Select the group for which you want to set the time zones and click **User group properties**. The members of group will display.





- To assign the time zone to the group, first select the device in **List of devices available for the Group** with defined time zones.

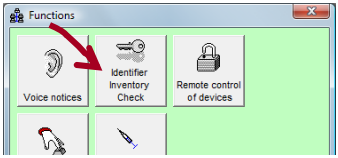
- When the device is selected, the defined time zones for this device will appear – **Verified time zones of device**. Select the time zone, which you want to assign to the user group (if the user group is already assigned to this device, the device time zones will display automatically after the User group properties window is opened).
- Confirm **OK**. The time zone is activated for the selected user group.

Practical use of Time zones
When the apartment building has two elevators – residential and freight one, it is possible to restrict the use of the freight elevator from 23h to 5 h for the energy saving reason. Another possible use is to control the access of the mailman, cleaning services who visit the building only during the week days, etc).

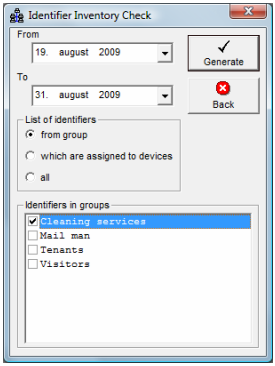
INVENTORY CHECK OF IDENTIFIERS

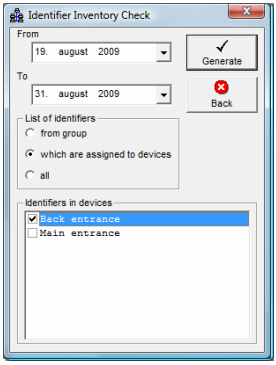
This function is used to check the existence and usage frequency of identifiers in the database in selected time period.

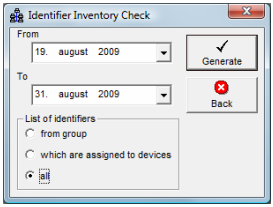
- Click **Functions** button in the main application window and then click the **Identifier Inventory Check** button. New window for inventory settings will display.



- To set the inventory time period, set the dates **From / To** in the **Identifier Inventory check** window. Select the **List of identifiers** using one of the offered options (**from group / which are assigned to device / all**).





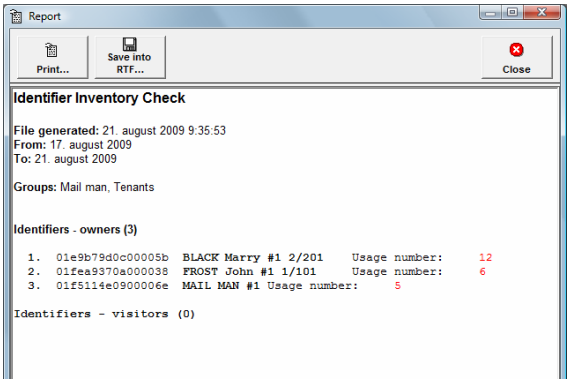


The generating of the inventory check results might take several minutes *(depends on the time period selected and quantity of data that has to be processed). The process can be monitored in progress dialogue window which appears after the inventory setting are confirmed by clicking* ***Generate****.*

- Click **Generate**. The application will generate the inventory list, which can be printed by clicking the **Print …** button or saved into the file, for this option click **Save into RFT …** and then select the target directory and enter the name of the file.

Practical use of the Inventory Check function

This function helps to keep the security of the building on high level. It is possible to check which identifiers have not been used for a longer time, so they might be lost or stolen from the user. The facts can be verified with the user and the identifiers can be indicated as a Lost one in the database or completely deleted from the database to eliminate any misuse or unauthorized entries.

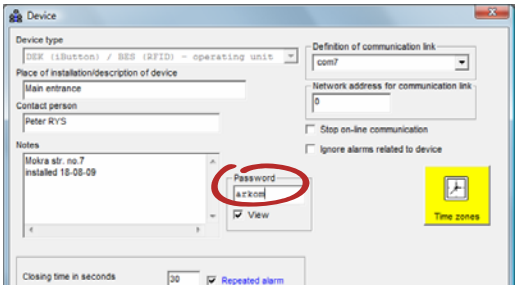


UPDATE USING A DATA CARRIER

First programming* of operating-memory unit must be done *in on-line connection to PC!
The Password must be set in the device properties.

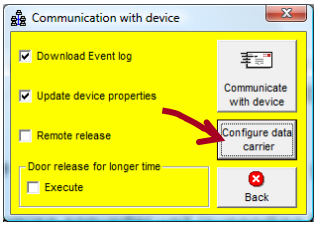
Before you use a Data carrier

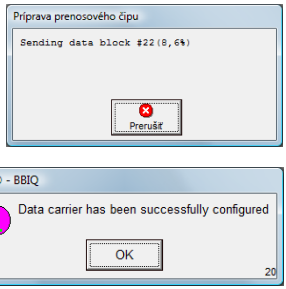
- Select the device from the **List of devices** and click the **Device properties** button.
- Define the **Password** in the **Device properties** window. The password is important to identify the device with the correct database. The password setting must be done on-line, only then the password is valid and the Data Carrier can be used.



If you need to add/delete identifiers from the database of an operating-memory unit which is already installed in the premises, the Data Carrier can be used. In this case the unit does not have to bee on-line.

- Make the desired changes in the application. Save the database to Data Carrier, go to **List of devices** and click **Communicate with device**. If the password has been set correctly before, an option **Configure data carrier** will appear .
- Place the Data Carrier to the touch probe of programming-converter unit (supporting PPM function and connected to PC). Click **Configure data carrier** and the modified database will be copied to memory of Data Carrier (process is displayed in progress dialogue window).





- The programmed Data Carrier can be taken to the place of access control system installation and the operating-memory unit can be updated. Place the Data Carrier on the **entry touch probe connected to the operating-memory unit that has to be updated**. HOLD the carrier STEADY on the probe during the whole transfer! Operating memory unit verifies the password and accepts the database.
- During the data transfer the **clicking sound** from the operating unit can be heard, the data transfer is finished when the sound stops and after a short pause **the relay is switched** (one click is heard).
- If the acoustic devices (piezo-buzzer and siren) is connected to RELE 2 of the operating memory unit, this device will signal the process of data transfer. The **intermittent tone** indicates the start of transfer; the **steady tone** indicates the end of transfer.

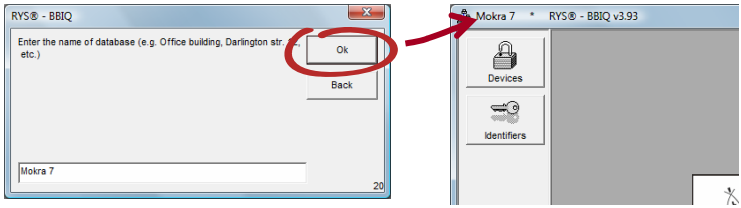
- When the transfer is finished the operating-memory unit is ready to operate with new programmed data.
- It is strongly recommended to set different password for each operating-memory unit in order to avoid any unwanted database overwriting. It is also important **to archive all the databases** for security reasons (the database in the unit might get damaged or lost).

If there is several operating-memory units connected in the access control system (in one network), each unit must be programmed by Data Carrier individually.

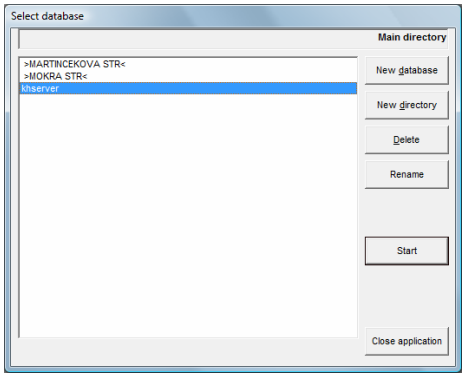
SETTINGS

Archive database – this function is used to create archive database file in compressed format .zip.

Database name - to name the database, click **Database name**, then enter a new name or modify existing one and confirm OK. The name will appear in the title bar at the top of the window. The database name will also give you quick information if you work with the correct file.



Selecting database file – multi-database setting (page 9) enables you to work with several databases in one application. This function offers easy management of database files, creating new directories and files or re-naming database files.



When selecting the database file, please make sure you have the right operating-memory unit connected to PC in order to avoid any unwanted data overwrite.

WHAT DO YOU NEED TO PROGRAM IDENTIFIERS?

These components are necessary for basic programming of identifiers:

IBUTTON TECHNOLOGY
DEK SIET access control system

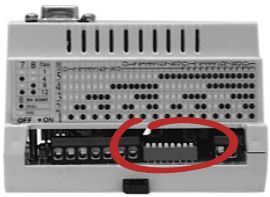
1. Identifiers - iButtons
2. Operating-memory unit – DS-01/485-ZPK-PPM
3. Programming-converter unit PPM/USB-RS485
4. Power supply for OMU

RFID TECHNOLOGY
BES proximity access control system

1. Identifiers - RFID tags, EM4100 and compatible
2. Operating-memory unit – DS-01/485-ZPK-PPM
3. Programming-converter unit PPM/USB-RS485
4. Power supply for OMU

Hardware settings
The hardware setting of a unit network address must be done before any software settings. The address is set by the DIP switches and it is important for the correct recognition of the unit in the system.

To set the OMU's address use the table on the side of the unit's cover. To set the network address use DIP switches 1—5.



Activate CSD—door status time-control function — put DIP switch 6 to ON position.

Note: There is also a table describing how to set the door release time (DIP switch 7 & 8), and there is also a connector points description on the unit.

Operating-memory unit must be reset after each modification of hardware settings!

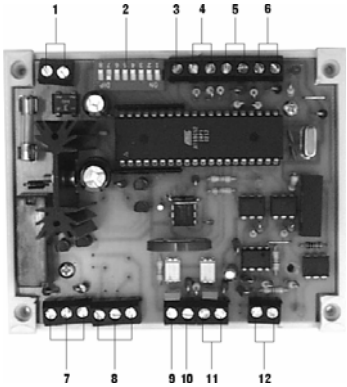
DS-01/485-ZPK-PPM - OPERATING-MEMORY UNIT

ADDRESSABLE ACCESS CONTROL SYSTEM WITH IBUTTON TECHNOLOGY (DEKSIET)

Standard operating-memory unit DS-01/485-ZPK-PPM is a device suitable **for two way traffic control (entry/exit).** The unit support: network connection—up to 32 units in one network and **the** door status time control. DIP switches on the unit are used to set network address, door release time for 1,4,8 and 12 seconds. The capacity of EEPROM is 1800 records. When the unit is connected on-line the capacity of the event log depends on PC's HDD free space and so the large number of events can be recorded into the log.

Device is suitable for **an effective entry / exit control in multi-apartment buildings**, office and industrial buildings, schools etc.

- max. 32 operating-memory units - addressable system
- **two-way door control**—possibility to connect two touch probes to one OMU DS-01, (ENTRY/EXIT have independent records in the event log and two-LED signalling)
- integrated door status time control function with possibility to connect an acoustic signalling device – siren
- output RS485
- adjustable door release time—set by DIP switches
- communication signalling using two LEDs on the unit's PCB (receiving/sending data)
- capacity EEPROM 1800 events, 900 identifiers
- on-line connection recording of events directly to PC
- real time clock
- Switching contact ZPK for releasing the door from 2-bus apartment phone (DDS) or from the exit button
- PPM function for programming the unit using Data Carrier (memory iButton)
- possibility to connect devices for an addressable door release or monitoring of the digital entry door system DDS



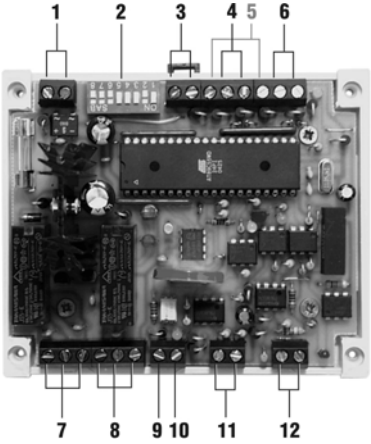
1. power source 12 V AC/DC (AC recommended)
2. DIP switches:
   - 1 - 5 – network address setting (addresses from 0 to 31)
   - 6 – activate the door status time control - CSD
   - 7 and 8 – door release time / set relay 1
3. power source for LEDs on the touch probe (TP)
4. LEDs signalling touch probe status
5. connection of first touch probe (GND – edge, T1 – centre)
6. connection of second touch probe (GND – edge, T2 – centre)
7. switching relay controlled from touch probe
8. switching control relay for connection of signalling devices like siren, alarm etc.
9. ground
10. door contact used for the door status control function and for the monitoring of the door opening (moment of opening) and the duration of the door opening, it is connected to the electromagnet
11. switching contact ZPK
12. output RS 485

BES-01 - OPERATING-MEMORY UNIT
ADDRESSABLE ACCESS CONTROL SYSTEM WITH RFID TECHNOLOGY (TAG, CARD)

Standard operating-memory unit BES-01 is a device able to control two proximity readers **for two way traffic control (entry/exit).** The unit support: network connection—up to 32 units in one network and the door status time control. DIP switches on the unit are used to set network address, door release time for 1,4,8 and 12 seconds. The capacity of EEPROM is 1800 records. When the unit is connected on-line the capacity of the event log depends on PC's HDD free space and so the large number of events can be recorded into the log.

Device is suitable for **an effective entry / exit control in multi-apartment buildings**, office and industrial buildings, schools etc.

- max. 32 operating-memory units - addressable system
- **two-way door control**—possibility to connect two touch probes to one OMU DS-01, (ENTRY/EXIT have independent records in the event log and two-LED signalling)
- integrated door status time control function with possibility to connect an acoustic signalling device – siren
- output RS485
- adjustable door release time—set by DIP switches
- communication signalling using two LEDs on the unit's PCB (receiving/sending data)
- capacity EEPROM 1800 events, 900 identifiers
- on-line connection recording of events directly to PC
- real time clock
- Switching contact ZPK for releasing the door from 2-bus apartment phone (DDS) or from the exit button
- PPM function for programming the unit using Data Carrier (memory iButton)



1. power source 12 V AC/DC (AC recommended)
2. DIP switches:
   - 1 - 5 – network address setting (addresses from 0 to 31)
   - 6 – activate the door status time control - CSD
   - 7 and 8 – door release time / set relay 1
3. power source for reader (12 VDC, GND)
4. connection of first reader (W0, W1)
5. connection of iButton touch probe which is used only for Data Carrier configuration
6. connection of second reader (W0, W1)
7. switching relay controlled from the reader, e.g to control door strike.
8. switching control relay for connection of signalling devices like siren, alarm etc..
9. ground
10. door contact used for door status control function and also to monitore the moment of door opening and the duration of door opening, it is connected to the electromagnet
11. switching contact ZPK
12. output RS 485 – for connection of other system OMUs to PC

TECHNICAL CHARACTERISTICS

OPERATING-MEMORY UNIT - DS-01/485-ZPK-PPM
- iButton technology
- voltage: 8 - 12 V AC, DC/150 mA
- inputs: input for 2 touch probes
- outputs: 2 x relay 8 A / 250 V AC (1 x door, 1 x signalling)
- Identifier type: iButton **DS1990R-F5**
- user capacity: 900 iButtons
- door release time: adjustable from 1 to 12 s
- mounting box dimensions: 80 x 105 x44 mm (hxwxd)
- DIN installation

OPERATING-MEMORY UNIT - OPJ BES-01
- RFID technology
- reading protocol Wiegand 26bit, 125kHz
- voltage: 8 - 12 V /150 mA
- inputs: input for 2 proximity readers
- outputs: relé 8 A / 250 V AC (1x door, 1x signalling)
- Identifier type: **EM4100** and compatible (tags, cards)
- user capacity: 900 tags
- door release time: adjustable from 1 to 12 s
- mounting box dimensions: 80 x 105 x44 mm (hxwxd)
- DIN installation

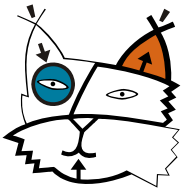
PROGAMMING-CONVERTER UNIT PPM/USB- RS485
- programming identifiers to OMU DS-01
- on-line connection of OMU and PC even for longer distances
- support of PPM function (Data Carrier)
- converter USB-RS485
- power source: via USB
- integrated touch probe CZ-2-S with signalling LED
- socket USB / RS485

PROGAMMING-CONVERTER UNIT BES USB-RS485
- programming identifiers to OMU BES-01
- on-line connection of OMU and PC even for longer distances
- converter USB-RS485
- power source: via USB
- integrated RFID reader
- socket USB / RS485

When installing the Access control system follow the recommended wiring diagrams!
(the complete catalogue of wiring diagrams can be downloaded free at www.rys.sk)

The length of connection between DS-01 and touch probe **must not exceed 20 m** and **twisted pair cables must be used** for connection of these two components. *Warning: if the touch probe is installed **into metal door frame, the door frame must have the same electrical potential as the touch probe**.* It is recommended to install the touch probe into the special mount .

The length of connection between BES-01 and proximity reader **must not exceed 50 m** and **twisted pair cable must be used** for these two components.



RYS®

Martinčekova 3, 82109 Bratislava 2
SLOVAKIA
tel.: +421 2 53412923, fax.: +421 2 53417096
e-mail: rys@rys.sk
www.bezpecnebyvanie.sk
www.rys.sk

dokument: BBIQ_TPmala2.3-25082009/ENG