AMS Offline Doors

Configuration and Operation

en Software manual

Table of contents

1 Introduction

The **PegaSys** locking system is an offline system used to secure objects that cannot, should not or must not be monitored online.
Offline systems are normally used where the lack of a need for continuous synchronization makes the high availability of individual components unnecessary, where the terrain prevents a direct connection (e.g. excessive cabling distances between installations) or where the installation of online components would be too expensive. In comparison with conventional locking systems (security locks with specially manufactured keys), the advantage of offline systems is that significant investment costs are only incurred when installing or extending the system. Locks and keys do not need to be updated or replaced (e.g. in the event of loss or theft), as the software can deactivate the units concerned (badges) and thus render them unusable.
Suitable objects for offline systems are generally installations with a number of individual rooms to secure, such as hotels, student residences and hospitals.
PegaSys components are integrated into the access control system and managed from there.

1.1 Explanation of terms

In order to differentiate between the individual access control components, the following terms are used for the various components:

- **Access control system**
  This refers to the online components
  - The data management level (dialog system, database, event log etc.).
  - Access controllers, which grant or deny access on the basis of data received from the data management level.
  - Readers, which read the data from the cards and forward it to the controllers.
- **Locking system**
  The offline system elements (by contrast, the term **system** refers to only a subset of the locking system.)
  - Cards, which contain the authorization data.
  - Door terminals, which grant or deny access on the basis of the authorization data read from the cards.

The locking system as an integrated unit also makes use of the access control system's dialogs, access controllers and readers.

1.2 Special features of locking systems

In access control systems, code data is read off the card and stored in the database in combination with the personnel data and access authorizations. When scanned at an access control reader, the code number is read again and compared with the stored data. If this check is positive, the person in question is granted access.
A connection to a data storage element of the system (i.e. online system) is therefore essential.

With offline systems, access authorizations for certain doors are stored on the card. When scanned, these authorizations are read and checked as to whether they contain the identification for the door concerned and are up-to-date.

The offline variant poses a basic security risk, as it is essentially impossible to prevent misuse in the event of loss or theft. In online systems, misused cards can be blocked, deleted from the database or assigned an expiration date, whereas offline systems offer no means of direct

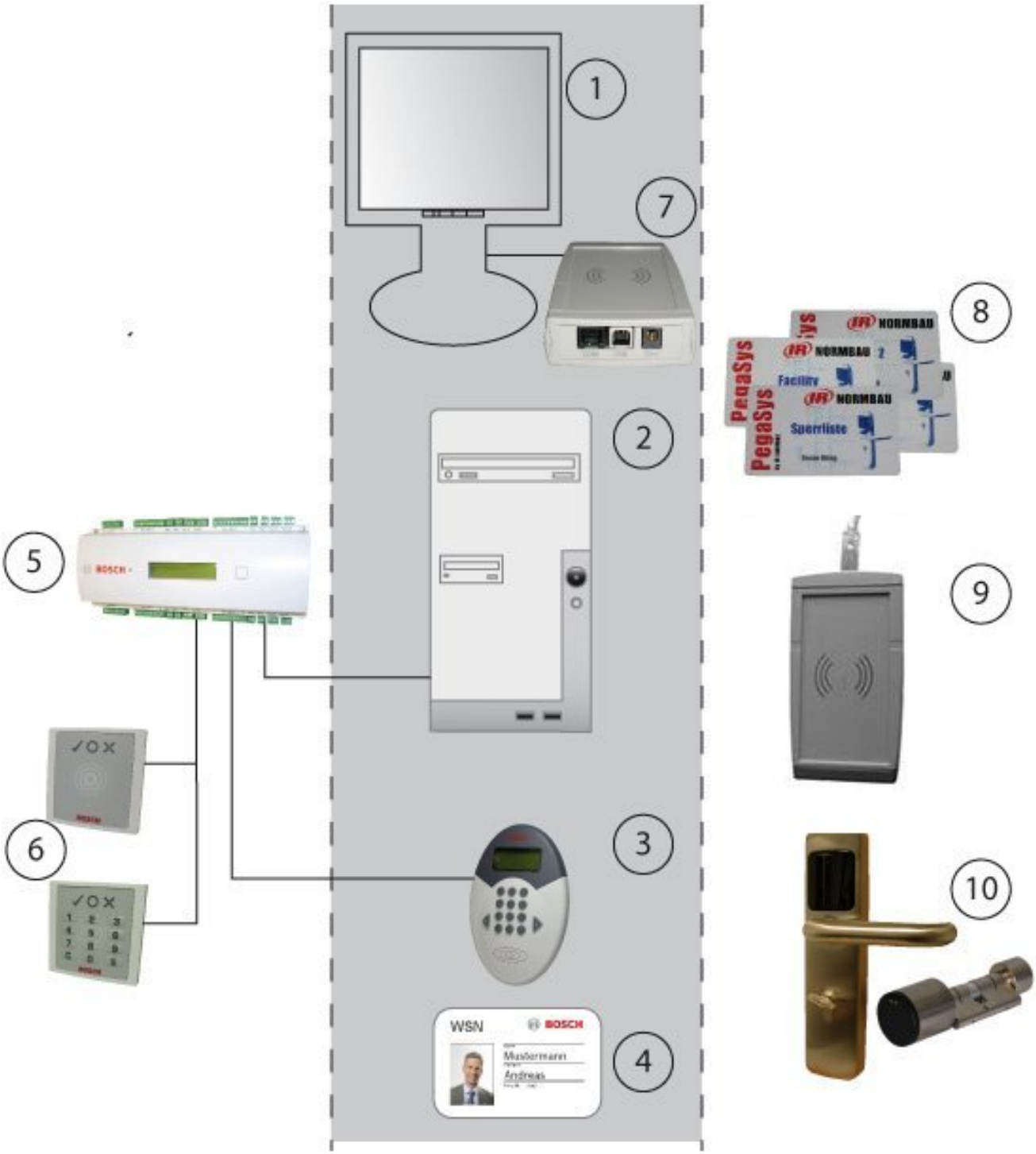
intervention. However, in order to keep the risk of misuse as low as possible, the authorizations are assigned an expiration date/time. At this deadline, the authorizations lose their validity. In order to reactivate them, the validity period must be extended. This is carried out via a special reader with write capability. If the authorizations have not been deleted or blocked in the meantime, they are extended or renewed when the card is scanned at this online reader.

1.3 PegaSys components

When the offline locking system is installed, the following applications and extensions are set up:

- **Software**
  - **Configuration dialog** for PegaSys
    This application is used to set up the systems and make all the general settings (e.g. validity period), create time models, and configure doors and door groups.
  - AMS Dialog manager > **Configuration** > Device editor
  - When door models are created, write capability can be activated and configured on the **Additional settings** tab.
  - **Persons > Cards** in the dialog manager
    This dialog contains an additional tab called **PegaSys**, where you can allocate authorizations for the locking system.
  - **Reports > Master data lists > PegaSys persons**
    Lists about equipment and allocation of authorizations for offline doors can be created using different filter and search criteria.
- **Hardware**
  - **System cards**
    System cards are used to initialize the door terminal and to update data (e.g. blacklists).
  - A **read-write device** for user cards and system cards must be connected to the workstation(s) at which PegaSys data is processed.
  - A **mobile read-write device** (timesetter) for the time stamp which in turn is used to update/initialize the door terminals (optional).
  - **Terminals** to read the user and system cards at the doors in the offline locking system.

2 System overview



1. Workstation
2. Server with configuration application and database
3. Access control reader with write unit
4. Card - for both systems
5. AMC2 access controller
6. Access control readers
7. Dialog read-write unit for online and offline data

8. Various system cards for the locking system
9. Mobile read-write units for date/time stamping
10. Door terminal/cylinder with read unit

When the PegaSys locking system is integrated with a Bosch access control system, certain components are used by both systems. The gray area in the diagram above contains the system components that are used by both the access control system and the locking system.

3 System Components

3.1 Workstation

The same dialog interface [**1**] is used to create and view personnel data in the access control system and the offline locking system. Access authorizations for both the main access control system and offline system can be assigned simultaneously.

3.2 Server

The software for the access control system and the locking system runs on this computer [**2**]. The Configuration Browser for the BIS system is also used to configure the readers [**3**] for the locking system.
PegaSys data is managed in special tables of the database of the main access control system.

3.3 Read-write units

At least one read-write unit [**3**] must be available. Ideally, these are placed at entrances that are used on a frequent basis (e.g. the main entrance) so that authorization for the locking system is extended at the same time as access is granted to the secured facility.
However, it is also possible to install these readers at special locations, independently of the access control system, so that PegaSys rights are not extended automatically but have to be obtained specially.

3.4 Card

The offline locking system does not require its own special cards [**4**]. The data required for the locking system is written to dedicated sectors of the access control card.

3.5 AMC2 4R4 Controller

An AMC2 4R4 [**5**] (= access control panel with RS-485 reader interface) is required for the DELTA 7020/1000/1010 [**3**] that is used as a read-write unit for the locking system.
The readers dedicated solely to access control [**6**] can use any protocols and read procedures, and can be operated with any AMC2 variant.

3.6 Access control readers

These readers [**6**] have nothing to do with the locking system; they simply regulate access requests in the access control system. Cardholders who are able to use the doors in the **offline** locking system [**9**] can also have authorizations for doors in the **online** access control system.

3.7 Read-write unit at the workstation

This device [**7**] is connected directly to the workstation computer via a USB interface and is used to transfer authorizations to user cards and system-related data (e.g. door and time initialization data) to special system cards [**8**]. It can be used simultaneously as an enrollment reader for cards from the online system.

3.8 System cards

Special system cards [**8**] are required to transfer access data - e.g. initialization data - to the door terminals [**9**].
The following system card types exist:

Facility cards
This card contains general system data such as system identification code, data type and record size. It is used as an "initialization card" both for the software and for each door terminal.

Door initialization cards
Used for transmitting door data to the relevant door terminal.

Time initialization cards
Used for transmitting time models and the time to the door terminals.

Clock initialization cards
Used exclusively for transmitting the clock time (date and time accurate to the minute).

Blocking cards
Information about blocked cards can be transmitted to the door terminals using these cards.

Booking cards
Access data saved in the door terminals can be retrieved and transferred to the database using this card type.

Battery-replacement cards
Cylinders cannot be opened for a battery change (for example) until a battery-change card has been read correctly.

Disassembly cards
The cylinder cannot be removed from the door fitting until a disassembly card has been scanned at the door.

3.9 Mobile read-write unit (optional) - timesetter

In order for the times to be updated, particularly following a power failure at the terminals, this unit writes the current date and time to clock initialization cards. These cards can then be used to reset the terminals.

3.10 PegaSys - door terminal/cylinder

This read unit checks the identification of an individual door or its group against the access rights for the cardholder.
The access rights on the badge must be continually updated via special readers with write capability [**3**].
If emergency access is required, e.g. if the electronics fail, the terminals also have mechanical cylinder locks.

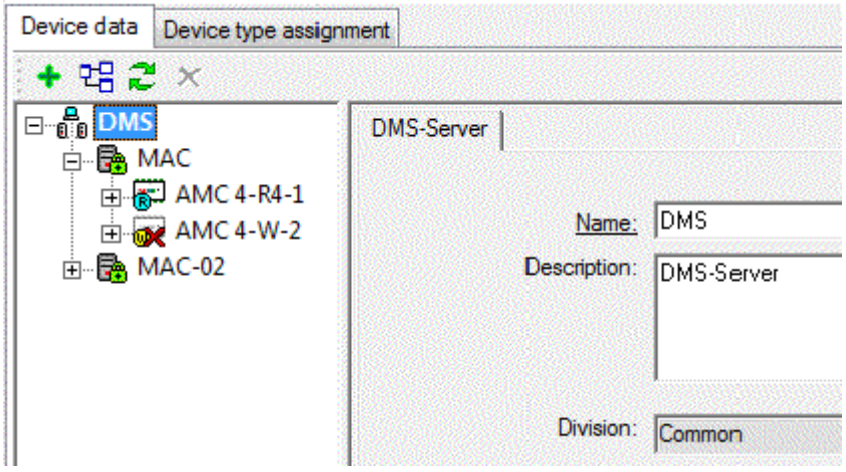
4 Offline Doors - Device Data Editor

Readers with write capability are used for the offline system to load authorizations to the card. They can also be used in parallel as access control readers.

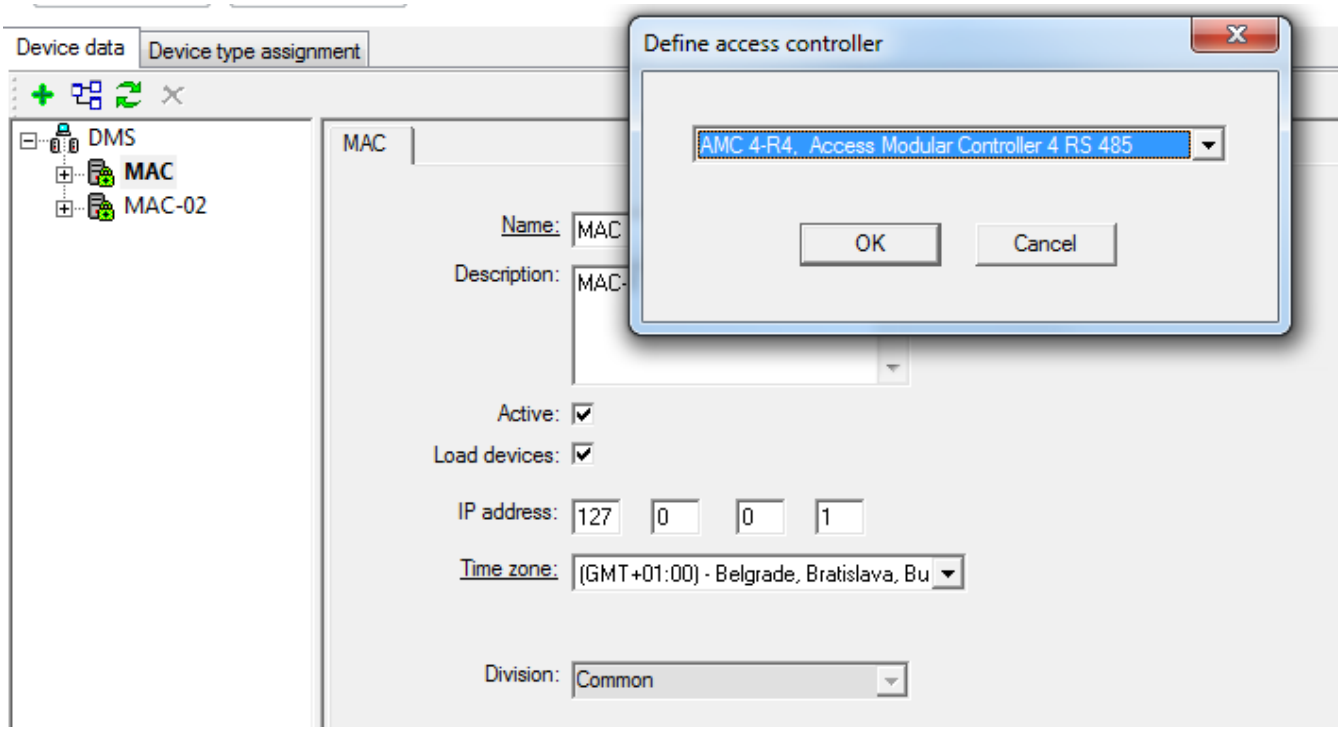
4.1 Adding hardware components

Open the Device Editor.

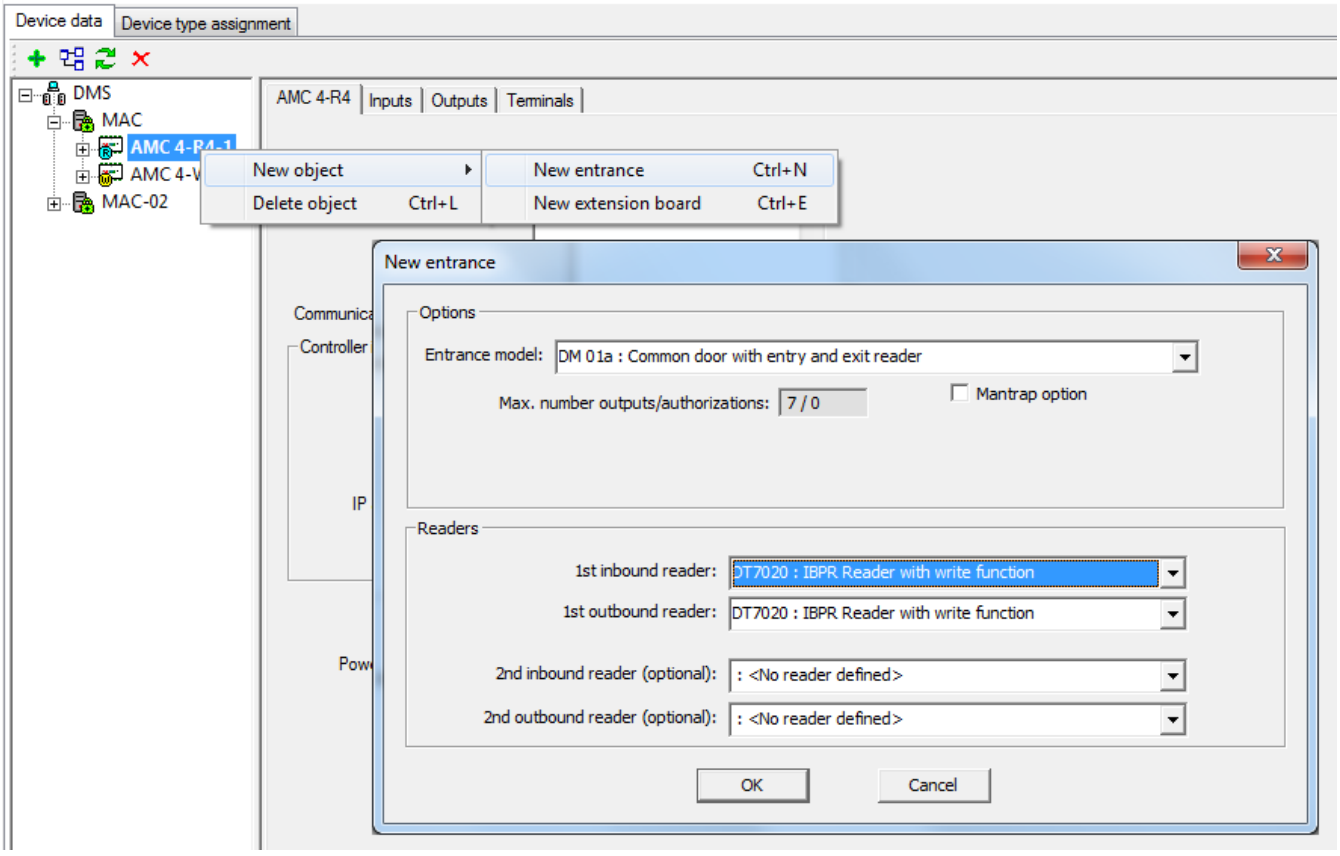
– AMS Dialog manager > **Configuration** > Device editor



1. Select the entry **MAC** in the device overview.
2. Select the option **New object ...** in the popup menu .
3. Select the entry **AMC2 4R4** in the selection dialog for the controller.



4. Select the option **New object ...> from the popup menu for the new controller New entrance**.
5. Choose the desired door model from the selection list.
6. Select the entry **DELTA 7020** for at least one reader.



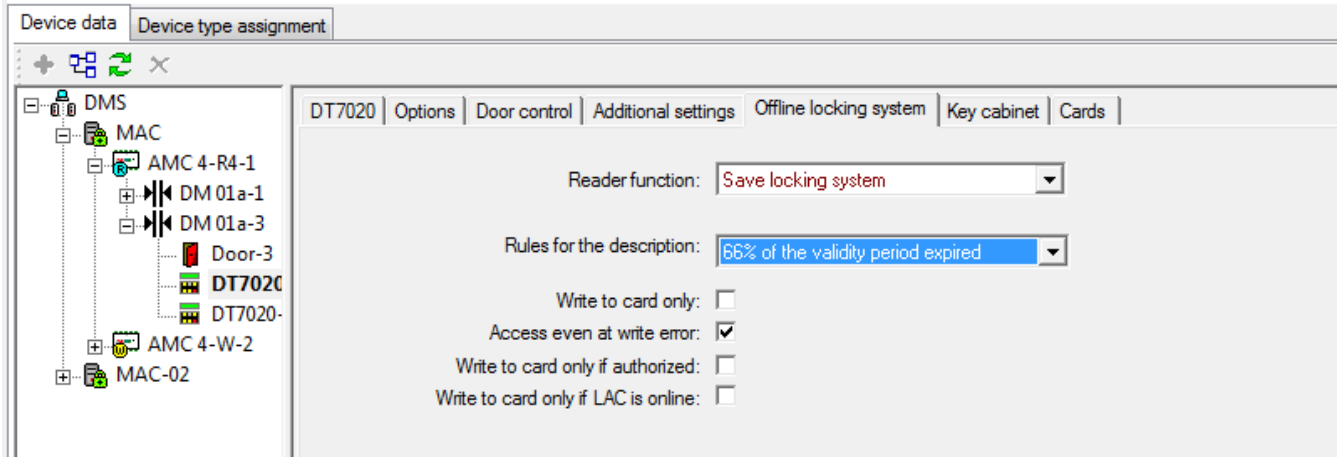
The following readers can be used as read-write units for PegaSys authorizations

- **DELTA 1000** (with special firmware)
- **DELTA 1010** (with special firmware)

4.2 Configuring the read-write unit

If this reader is also used as an access control reader you may configure it as such. For further information about the relevant parameters, please see the online help for the online access control system.

Parameters for **extended reader functions**, which can be used to configure the settings for the locking system, have been combined on the **Offline Locking System settings** tab.



Reader function
Read only (= default setting)
This reader is purely an access control reader and is not part of the locking system.
All other parameters in this area are deactivated.
Read/Write
This reader has access control functions and is also activated for the locking system.
Activation of the following functions.

The drop-down list is only enabled when the selected reader type is a DELTA 7020.
The **Read only** setting prevents readers from using the Write function at certain times, for example, when offline system components are not available or (in cases where several write-capable readers exist) when only a select few are to have write-capability, such as during peak periods of use.

Write to card only
The access control and door control functions for the online system are deactivated.
Deactivated (check box is cleared (default setting)): The usual access control checks are performed after data is written to the card.
Activated (check box is selected): No access control performed after data is written to the card.

This check box should be selected if the reader is only used as a read-write unit for the offline system. Otherwise the additional signal traffic would cause unnecessary delays.

Access even with write error
Access control (in the online system) does not depend on the success of the write process (in the offline system).
Access control is performed even after unsuccessful write attempts.
Deactivated (check box cleared): If it is not possible to write to the card, access is also denied.
Activated (check box is selected (default setting)): The write process has no impact on the access control.

Write to card only if authorized
Rights for the locking system will only be written to the card if the cardholder has (online) access authorization for the entrance.
Deactivated (check box cleared (default setting)): Data is always written to the card.
Activated (check box selected): Data is only written to the card if valid authorization is present.

If the check box is selected the write process will be prevented, even if authorizations are only temporarily suspended (e.g. by a time model).

Only write if LAC online The rights are only written to the card or updated when the Local Access Controller (LAC) is guaranteed to have received the latest data from the access control system. For security reasons any deletions due are always performed.
Deactivated (check box is cleared (default setting)): Data is always written to the card.
Activated (check box selected): Data is only written when there is a connection between the controller and MAC.

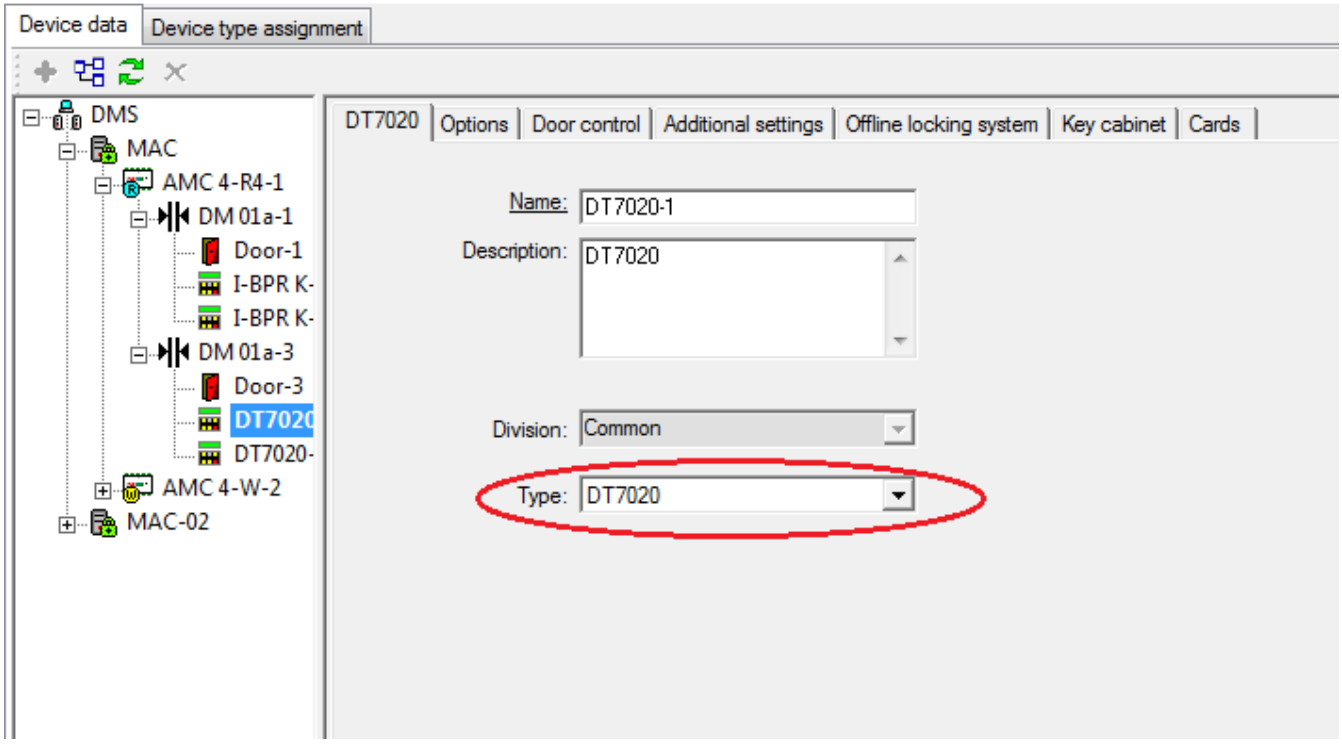
If this check box is selected and the check box **Access even on write error** not selected, then the online system denies access if the LAC/MAC link is broken and the card's offline data is not up-to-date.

Rule for writing In the default setting, the validities are extended when two thirds (66%) of the validity period specified for the person has expired. See also *Example of default writing rules, page 58*.
This parameter can be used to extend validity periods by individually specified amounts.
Possible values:
Locking system specification
Always write
[when ... of the validity period has expired:]
16%, 33%, 50%, 66%, 83%, 100%

Locking system specification - see *Standard validity, page 21*.

4.2.1 Changing the reader type

As a rule, readers with write capability are installed at major entrances (e.g. as the entry reader at the main entrance), so that when personnel enter the site in the morning, the access rights for the locking system are automatically updated.
When refitting an installation with PegaSys, at least one reader in the facility must be replaced with a write-capable reader. The Device Editor does not allow the subsequent modification of door models and their readers.
Staying with the example of the entrance reader at the main entrance, the existing entrance would need to be deleted and a DELTA 7020 reader added in its place.
If an existing entrance is deleted it is also removed from all access authorizations. All authorizations would therefore need to be added to the new entrance.
To avoid this laborious and error-prone process, the drop-down list **Type** has been added to the first page of the reader configuration.



This drop-down list is set up for all readers so that replacements can be configured by selecting and assigning the type **DELTA 7020**, without the need to delete existing entries.

4.3 Dialog read-write unit

In contrast to the online system, where a card number can also be entered centrally, offline data can only be transferred to or read from a card by peripheral read-write units. These read-write units can be either dialog readers connected directly to the workstation or access control readers (e.g. DELTA 1000, or DELTA 1010).
The dialog reader for writing and reading system and user cards from the offline system, as well as recording card data for the online system, is installed using the online system.

- AMS main menu > **Configuration** > **Options** > **Card reader**
- Select the relevant workstation in the Workstations field.
- In the **Type** drop-down list, select the PegaSys reader that corresponds to the card-type used.

Reader name	Reader type	Coding
PegaSys-MF-BC-USB	MIFARE Classic	Bosch Code
PegaSys-MF-SN-USB	MIFARE Classic	Serial number
PegaSys-MFDESFire-BC-USB	MIFARE DESFire EV1	Bosch Code
PegaSys-HITAG-BC-USB	HITAG 1	Bosch Code
PegaSys-HITAG-SN-USB	HITAG 1	Serial number
PegaSys-Legic-BC-USB	LEGIC Prime	Bosch Code
PegaSys-Legic-SN-USB	LEGIC Prime	Serial number

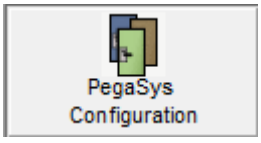
Reader name	Reader type	Coding
PegaSys-LegicAdvant-BC-USB	LEGIC Advant	Bosch Code

Restart the access control system to make the selected reader available in the personnel data dialogs of the access control system.

5 Offline Doors - Configuration dialog

5.1 Getting started

After the PegaSys component is installed, the configuration dialog for the component is located in the **System data** menu of the Dialog Manager of the access control system, and can be opened by clicking the



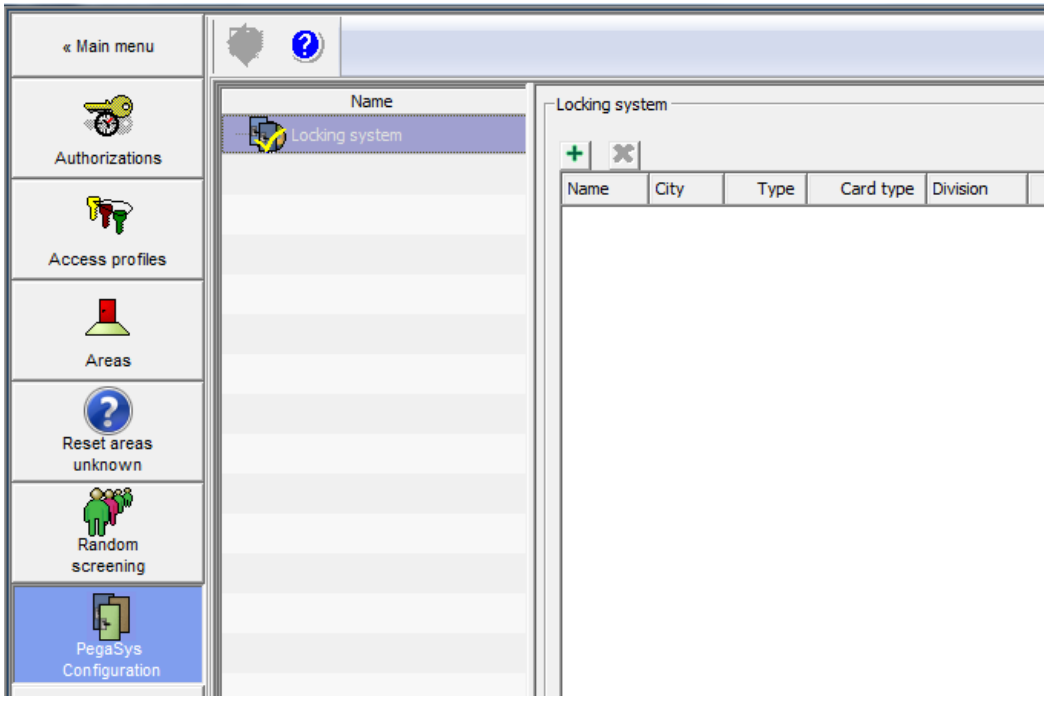
button.

5.2 Locking systems

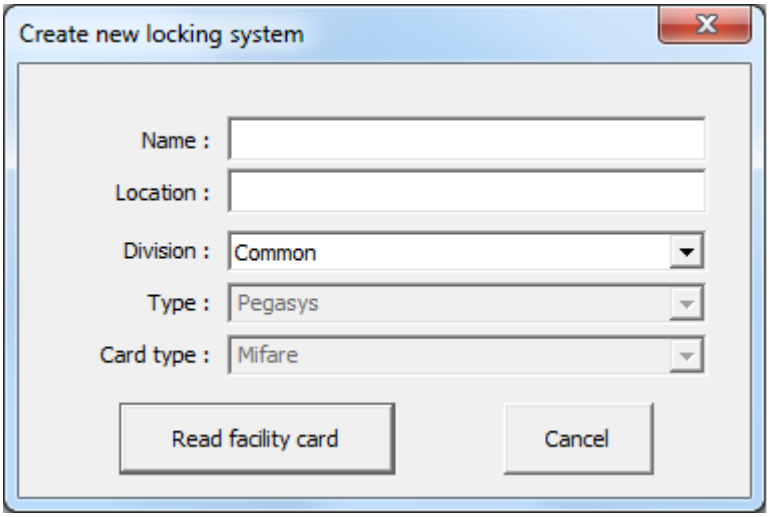
During installation the **Locking systems** node is added as a base entry in the explorer tree (left dialog pane). Autonomous systems that operate independently from one another can now be set up under this entry.

Setting up systems

– Select the base entry **Locking systems**.
Systems that have already been set up appear in a list on the right hand side.



– Click the + button (above the list field) to set up additional systems.



Name Give the system a unique name.
This information also appears in the access rights dialog.

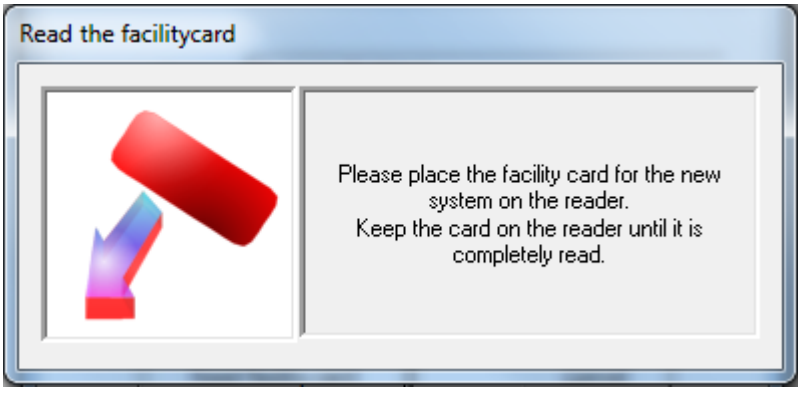
Location This information appears in the access rights dialog.

Division If you have set up divisions, you can also assign the individual systems to one of these divisions.

Type "PegaSys" - is card is the only one supported offline locking system for now.

Card type Display field (HITAG1, MIFARE classic, LEGIC prime and LEGIC advant) - is informed by the connected read-write device.

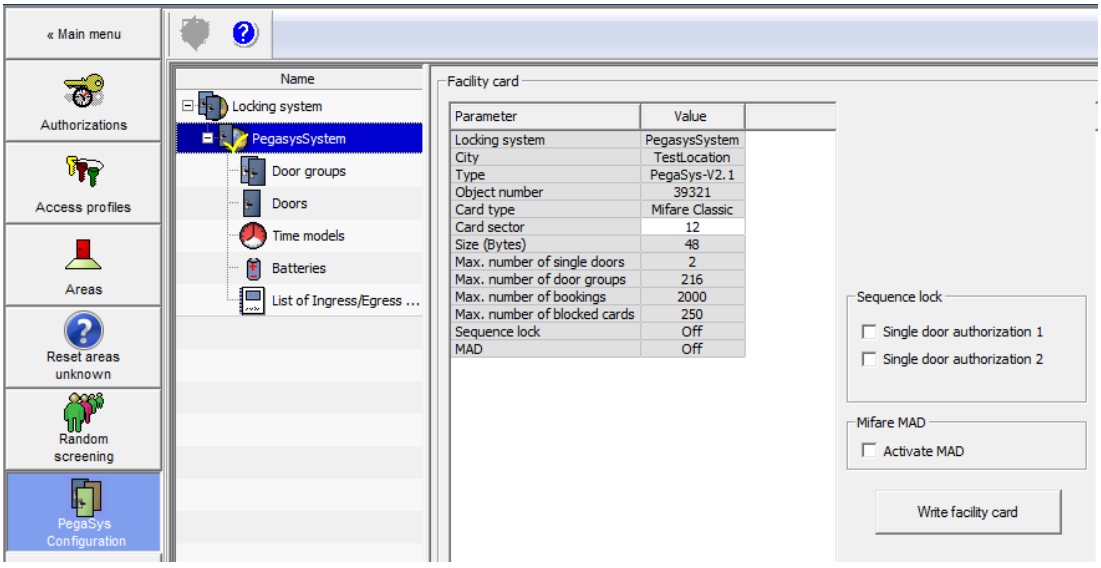
– Place the facility card for this system on the read-write unit and then press the **Read facility card** button.



When a facility card is read, the system offers to create a working copy. This option should be accepted at least once for each facility card to guard the original from accidental overwriting or loss.

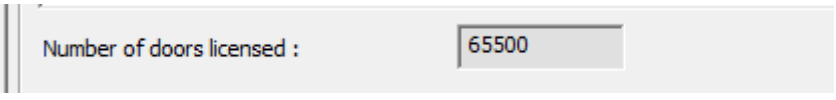
Notice!
Automatic data correction, and consequences
If data unsuitable for the size of the record is added to the card, a message appears after the facility card is read indicating that the data has been corrected automatically.
In this case a new facility card must be written and the door terminals reinitialized with it.

Click **Yes** to confirm that a new facility card should be written.
A list entry and another Explorer entry with the specified name are generated. Depending on the version of the facility card read, the Explorer entry contains a different number of subentries required to configure the system - see also *Configuring locking systems, page 20*.



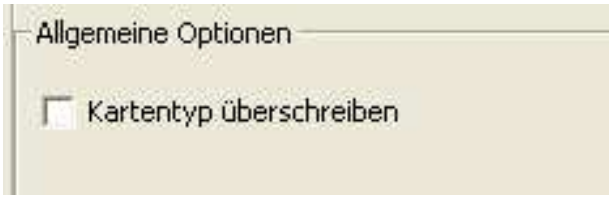
Notice!
List entries with a white background can be modified at any time. As an additional indicator, the mouse pointer changes when moved over one of these fields:
Double-clicking in the relevant list field activates write mode - press the ENTER key to exit the field after making any changes.

The **number** of **licensed** door terminals is displayed under the list field for the individual systems.



This value is the upper limit for all of the locking systems. The basic version of PegaSys includes 25 door licenses with the software. The number of licenses can be increased in multiples of 25.

Overwriting the card type



When overwriting system cards, a confirmation prompt appears once for each system card type - after that, the card is overwritten without further warning.

Deleting systems

Selected list entries can be removed again using the button.
Click **Yes** to confirm that you wish to delete the system.

5.3 Configuring locking systems

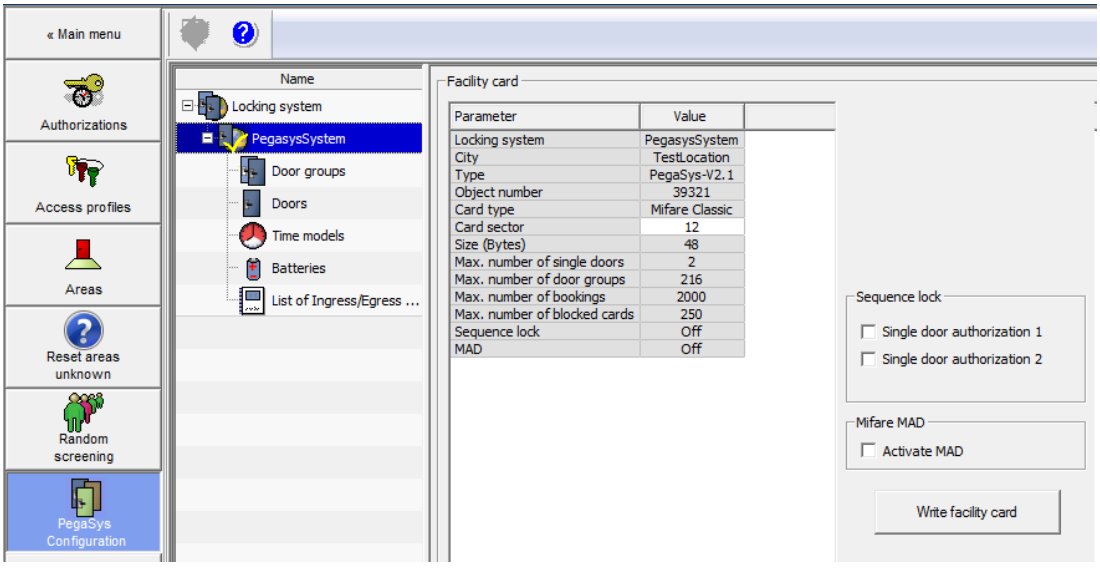
A system is configured in four steps which can be invoked from the corresponding tree node. Each type of node has its own icon; the icons of selected nodes contain a yellow checkmark.

Explorer node	Icon	When selected
<System name>		
Door groups		
Doors		
Time models		

The following sections describe which settings are configured, where and how.

5.3.1 Systems (PegasysSystem)

Specified system parameters and the data read from the **facility card** are displayed in the list window for this entry.



Locking system Name of the system as specified at setup.

Location Name of the location as specified at setup.

Type PegaSys-<Version no.>

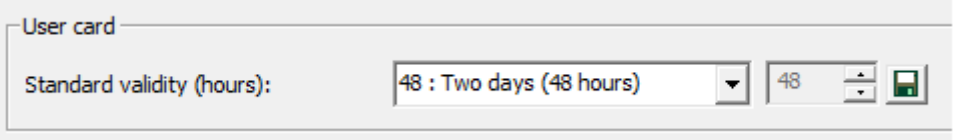
Object number Customer-specific code

Card type	Information on the reading and coding method: – HITAG 1 – MIFARE Classic – MIFARE DESFire EV1 – LEGIC prime – LEGIC advant
Card sector	Area on the card where the coding of PegaSys authorizations begins.
Data size (Bytes)	Number of bytes required to store the authorizations. 48 = default - the record length must be adapted depending on the size of the system - see also the table in *Possible data structures, page 36*.

Caution:
If using HITAG1 check these values carefully when first setting up the system, as this card type does not have a function to prevent areas already in use from being overwritten accidentally.

Max. number of single doors **Max. number of door groups** **Max. number of bookings** **Max. number of blocked cards**	Upper limits for the system, defined by card type and data size. **Remark:** Blocking cards i.e. Transport cards that can be used to transmit blocked cards to the terminals.

Standard validity
Furthermore, a **Standard validity** time for **User cards** can be set here. This will be used by the **Cards** dialog in the Access control system as default when assigning PegaSys authorizations.



The drop-down list contains a number of predefined periods and the option of selecting a specific number of hours.

One day (24 hours) Two days (48 hours) One week (7 days) One month (30 days) One year (365 days)	= Default setting Fixed periods that are counted from the moment the badge was encoded or the rights were extended.

Max. card validity	The validity defined in the dialog system ... – **Valid until** - Date (in online authorization dialog) – **Valid until** - Date (in the offline authorization dialog) – Block – Deletion
User setting	Freely defined period - in hours [1 to 17520 (two years)]. The input field for entering the hours is activated when this option is selected.

Click the button to save any changes in the validity period of user cards.
If the default value is changed, all personnel to whom the default validity period was assigned receive new values the next time their badges are updated.

Notice!
Each card has only 1 validity period
Each offline locking card has only one validity period. It is not possible to assign different validity periods to different door terminals on the same card.

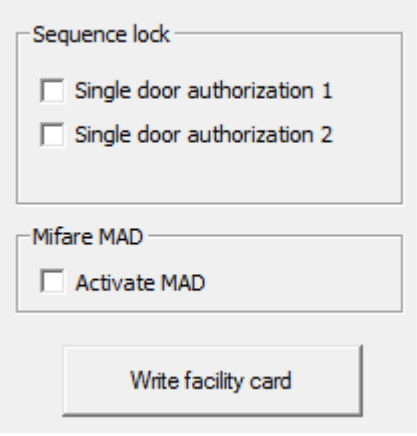
Extended functions

– **Check user card**
When the facility card is read, the card segment and the access code for offline authorizations are defined for the user cards. In order to check whether the settings are correct, the current settings can be written to a user card by pressing this button. A valid yet expired user card is created without authorizations. If this function fails, the system cannot be put into operation with these user cards and this facility card.
Each card technology has different prerequisites:
  – **HITAG 1**
  The preset start sector on these cards could be blocked. The start sector is a facility card parameter and can be adjusted in this dialog.
  – **MIFARE Classic**
  The preset start sector on these user cards may have already been encoded using a different code from the one on the facility card. If the start sector was set incorrectly, it can be modified in the same way as with HITAG1.
  In MIFARE Classic, the start sector of an application (such as PegaSys) can also be defined in the MAD (MIFARE application directory) of the user card. If the MAD is activated, the access code to the sector with the MAD must be known - see also *Configuring MAD (for MIFARE Classic only), page 23*.
  – **LEGIC prime/advant**
  With LEGIC, it is assumed that the user cards have been preformatted and that the required segment already exists on the user card. The required segment is displayed in the LEGIC segment parameter. All readers (online and offline) must have authorization to access the preset segment. This authorization may have already been programmed into the readers at the factory or set at a later time via so-called

initialization cards (=SAM63). If the system is rebuilt and new user cards are ordered, the so-called PegaSys segment can be installed directly by the card manufacturer.
If the segment is missing from the user card then, when the user cards are encoded by the dialogs (offline configurator and badge dialogs), an automatic prompt asks whether the segment should be created. If the dialog read-write devices have the necessary authorization (preset via XAM card), or the customer has an IAM LEGIC card that gives him authorization for just this preset PegaSys segment, then the required segment can be created and data written onto it. The offline segment is only created once. It should then be possible to read/write data to the user card from all (online/offline) terminals.
The software performs no checks as to whether data is already stored on the user card. If the card technology does not protect that data then it may be overwritten.

– **Creating a disassembly card**
The disassembly card can be created from any system card (except the facility card). Cylinders that belong to this offline system can be disassembled using this card. System affiliation is transferred to the offline terminals via the facility cards.

Writing facility cards



If any facility card parameter, the sequence lock or the MIFARE MAD settings are changed, then the facility card should be updated by pressing the **Write facility card** button. The online system uses the new settings directly. Leave the check boxes for the Sequence lock empty (i.e. switch Sequence lock off) unless use of this PegaSys feature has been carefully prepared in advance.

Notice!
If you change data on the facility card, ensure that you update all the door terminals with it.

Configuring MAD (for MIFARE Classic only)

When the MAD is enabled, the A and B access codes can be configured in the MAD sector of the user cards. A0 to A5 and B0 to B5 are default codes and therefore known to all companies (i.e. access is enabled for everyone). Only the A code is transferred to the offline terminals via

the facility card because the terminals only need to read and not write data to the MAD, if it is activated. The online system uses the B code to write the MAD for the offline system to the user cards.

Notice!
The MAD cannot be configured for Mifare DESFire EV1.

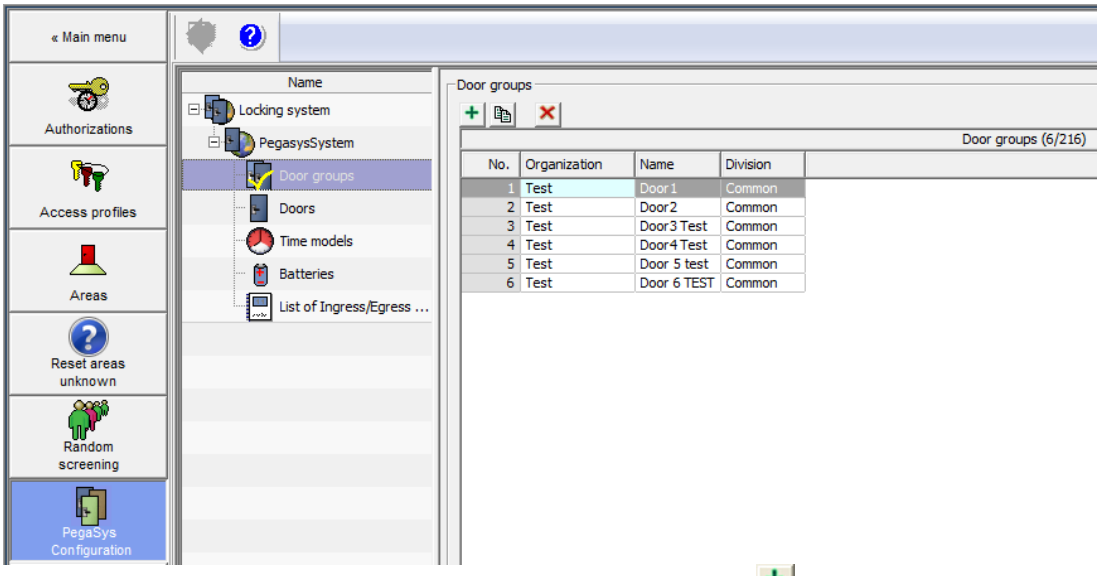
Refer to
– *Special settings, page 55*

5.3.2 Door groups

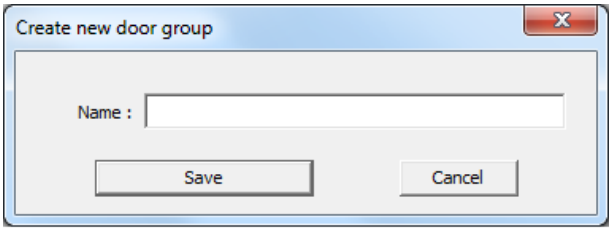
The segmentation of badges allows only a relatively low allocation of individual doors in comparison with door groups. This is because it is more convenient and common to assign authorizations to door groups than to individual doors.

Creating door groups

The required door groups are created as records in the list field without a link being initially established to individual doors.

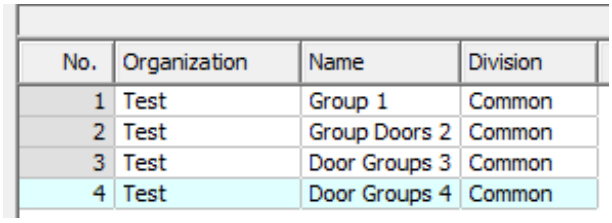


The creation dialog for the door groups is opened by clicking the + button.



Specifying a designation (**name**) for the door group and clicking the **Create** button generates a further list entry with its own ID number. The Division configured when the system (*Locking systems, page 17*) was set up appears in the **Division** column. It can be reset separately for each door group causing these door groups (as authorizations) to appear only within their own divisions.

A limited number of door groups can be created depending on the data size and card type - see also the table in *Possible data structures, page 36*. With the default size of 48 bytes and HITAG1 cards, the upper limit for door groups is 240 (for LEGIC and MIFARE, 256). The number of door groups already created, and the maximum number, are displayed in the list header: Door groups (4/216)

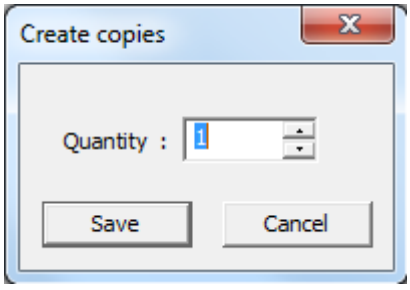


No.	Organization	Name	Division
1	Test	Group 1	Common
2	Test	Group Doors 2	Common
3	Test	Door Groups 3	Common
4	Test	Door Groups 4	Common

Copying door groups

Existing list entries can be copied, to make data-entry easier.

1. Select a list entry.
2. Click the button above the list field. The following dialog opens:



3. Enter the number of copies you wish to create.
4. Click the **Save** button to generate the list entries.

In order to guarantee that the designation is unique, the entries are assigned the designation of the selected entry and a sequential number (e.g. **Door groups n**).

The designations for the door groups can be modified at any time by double-clicking the relevant line in the **Name** column. The sequential number cannot be modified.

The number of copies that can be made depends on the card size. The arrow buttons in the **Create copies** dialog do not allow the selection of a value higher than the available remaining quantity and the dialog no longer opens when the maximum value is reached.

Deleting door groups

Door groups that are no longer required can be selected in the list and deleted by pressing the button. At this point, a security prompt appears, which must be confirmed to avoid accidental deletion.

Click **Yes** to confirm that you wish to delete the door group

Door groups that still have doors assigned to them can only be deleted after these assignments have been canceled.

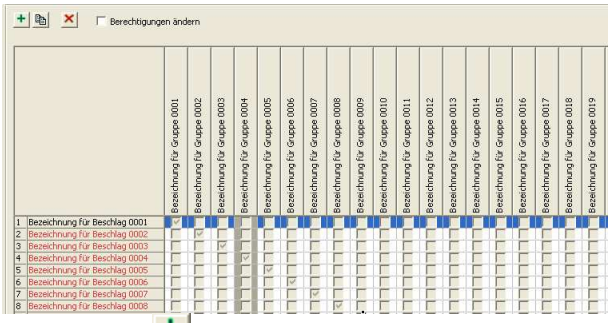
The doors are assigned in the next configuration step.

5.3.3 Doors

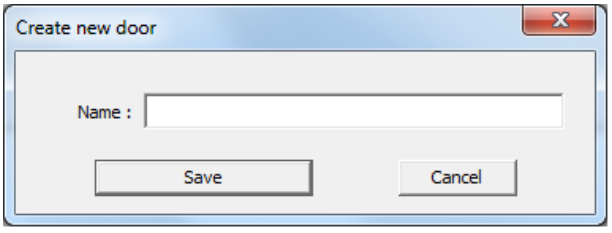
A list entry must be created and configured in this dialog for each door terminal in the locking system. These can then be assigned to certain door groups.

Creating doors

In this list field an entry is generated for each door terminal.



Pressing the + button opens the dialog for creating the doors.



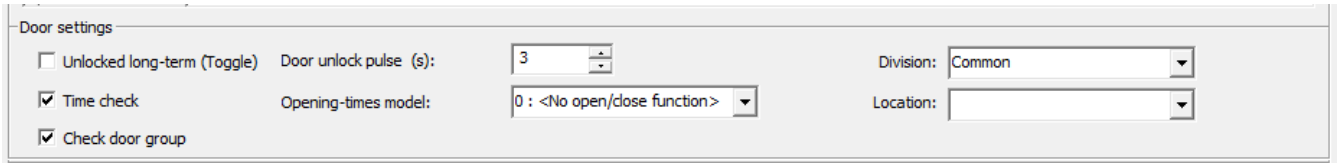
When a designation is specified for the door (**Name**), clicking the **Save** button generates a new list entry, which can then be assigned and configured.
Wherever possible use descriptive names for the doors.

Assigning doors

The list field of the dialog contains a column for each door group created. Select the relevant check boxes ☑ to assign the doors to the door groups. First activate edit mode by selecting the **Change authorizations** check box.
There is no limit to the number of door groups to which a door can be assigned.
Doors marked red are doors whose configuration has been changed but whose door card has not yet been encoded. The door designation turns black when the door card is encoded.

Configuring doors

The parameters under the list field are used to configure the selected door.



Unlocked long-term (Toggle) — Users with a special authorization can also unlock this door for an extended period - e.g. office or shop opening hours.
Default setting = not selected.

Time check — Setting that determines whether time models and validity periods are taken into consideration at all.
Default setting = check box selected

Checking door groups	An authorization for the locking system can consist of individual and/or door group authorizations. If this parameter is not selected, only individual authorizations are considered and checked. Default setting = check box selected
Door opening time (s)	Time in seconds (1 - 255), defining how long the door contact should release the door for opening. Default setting = 3
Opening-hours time model	Selection of a time model - the door is unlocked automatically for specified periods defined by their start and end times.
Division	Selection of a division with which the door should be associated. The default division is the one selected for the locking system, but it can be modified separately for each individual door.
Location	The location of the door (e.g. city, building, corridor, etc.). When access rights are allocated the location parameter is used to group and help identify individual doors.

Copying doors

Doors can be copied in the same way as door groups. To simplify the data entry, first a single door is created and configured, then copied as required.

– Select a list entry for the copying process.
– Click the  button above the list field. The **Create copies** dialog opens:
– Enter the required number of copies you wish to create or select them using the arrow keys.
– Pressing the **Save** button generates the required list entries.
  In order to guarantee that each designation is unique, copies are given a sequentially numbered suffix (e.g. **Door n**).

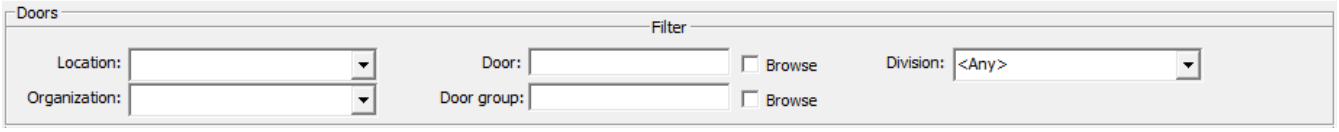
The designations for the doors can be modified at any time by double-clicking the relevant line in the **Name** column. The ID number in the first column (**No.**) cannot be modified.
The number of copies that can be made is limited by the licenses available. The arrow buttons in the **Create copies** dialog do not allow the selection of a value higher than the available remaining quantity and the dialog no longer opens when the maximum value is reached.

Deleting doors

Selected list entries can be removed again using the  button. At this point, a security prompt appears, which must be confirmed to avoid accidental deletion.
Click **Yes** to confirm that you wish to delete the list entry.

Filters for doors

On offline systems with a large number of doors, sorting the doors alphabetically can have a negative impact on the overview and make working more difficult. **Filters** located above the list field can be used to adapt the view in different ways and reduce the display to a small number of relevant entries.



Location	Filters out all doors in a specific location.
Organization	Filters out all doors within a specific door group.
Door	Filters out all doors with a specific character in the name. The columns show all door groups - the groups containing the relevant doors have selected check boxes.
Door group	Filters door groups with a specific character in the name. The lines show all doors - the doors contained in the relevant door groups have selected check boxes.
Browse	In the default setting, the system searches the start of the name for the characters specified in the top three fields. If this option is enabled, entries that contain the specified characters at any point in the name are selected.
Division	Only doors or door groups from the selected division are displayed. Default setting: **Any** - i.e. entries from all divisions are displayed.

Writing door cards

In contrast to the online access control system, configuration data in the offline systems cannot be distributed via system components and transmitted to the relevant installations; instead, it must be brought to the devices via another route. In the *System overview, page 7*, various system cards have already been mentioned - one of these system card types is the **door initialization card**, to which door parameter settings are written and which are scanned at the door terminals. After configuration, a door is selected in the list and then the **Write door card** button is pressed and one of the door initialization cards is placed on the read-write unit of the workstation computer.

A dialog box prompts you to place the badge in position and then shows the progress of the write process.

A message appears indicating that the write process was successful and then the time is recorded and displayed in the **Last coding** field as confirmation.

Notice!
Only the configuration data from **one** door can be written to a door initialization card. Not until the data has been transferred to the door terminal can the card be used for other write processes. Any existing data is overwritten.
The time models are also stored on a door initialization card. The time models should therefore be created in advance if possible, otherwise each door will have to be initialized again with time cards.

The new doors, door groups and parameters are transferred to the terminals via these door initialization cards. During the data transmission process, the LED on terminals lights up orange. Successful transmission of the data is then confirmed.

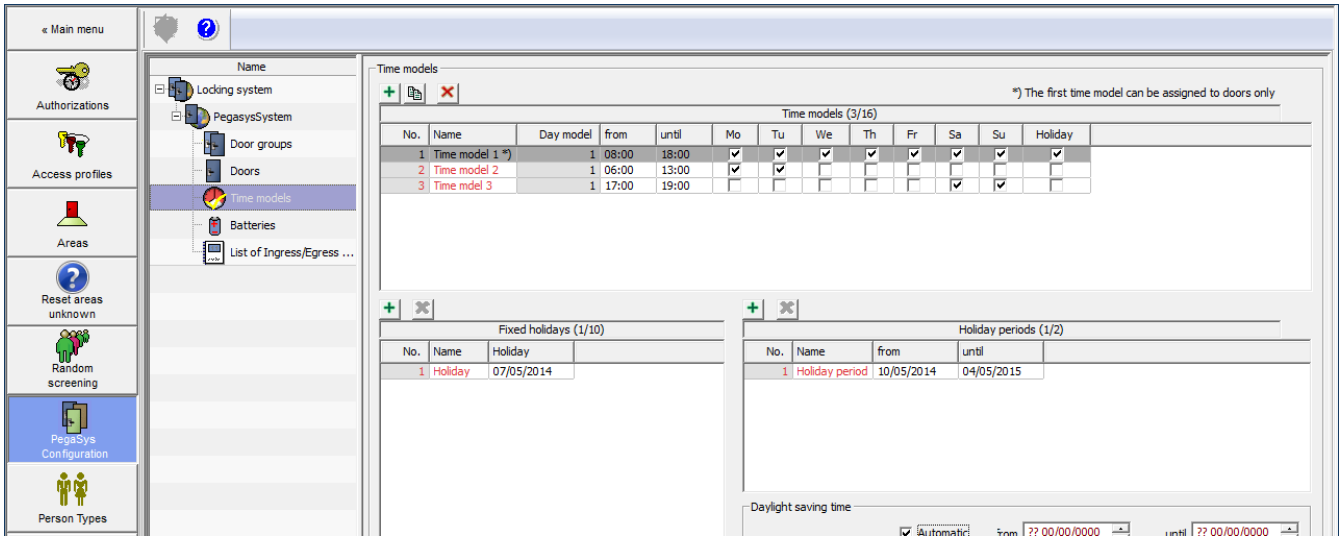
Checking the cards
Before the current card is written, the system checks whether it is actually a door initialization card. If the card has already been encoded in a different way (e.g. as a time or booking card), a warning to this effect is displayed with the option of overwriting the card and using it in the future as a door initialization card.

Notice!
If the parameter **Program > Overwrite the card type** (menu bar) is selected, a confirmation prompt appears once for each card type - after that, the card is overwritten without further warning.
Facility and user cards cannot be overwritten with a different card type.

Refer to
– *Locking systems, page 17*

5.3.4 Time models

The **Time models** dialog has three panes:
– The top half contains a list of all the time models and their assignment to the days of the week.
– Special days (**Fixed holidays**) that differ from the norm can be defined in the bottom left pane.
– Several days can be grouped to form a **Holiday period**, in the bottom right pane.

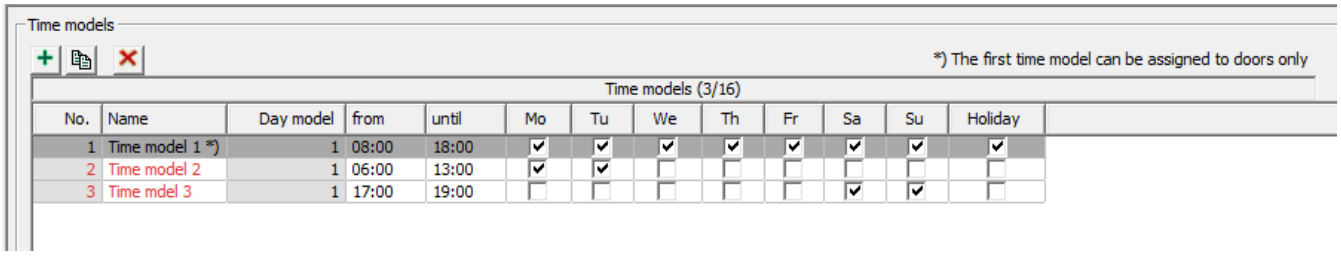


Time model vs time period

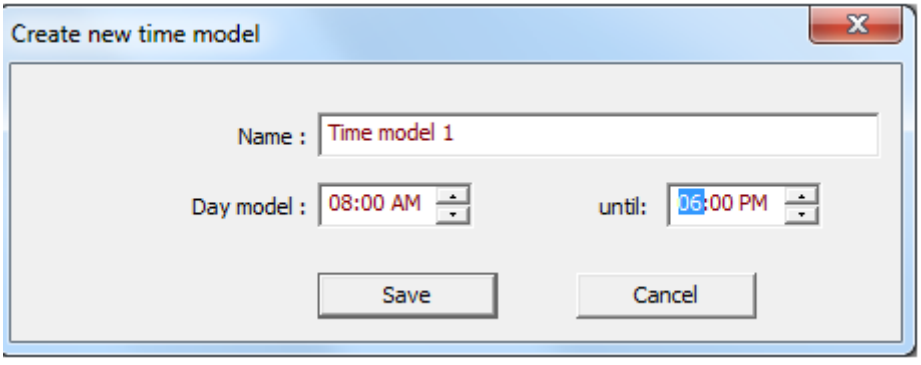
A time model can contain up to four time periods in one 24 hour day. Start and end times typically delimit periods where different regulations apply (e.g. office hours). The periods can be any length and can overlap. Each period can be allocated to any day of the week or holiday. The user is thereby responsible for ensuring that the period limits are set and allocated to the days in a logical and consistent manner.

Creating time models

Time models can be used to restrict allocated authorizations or perform automatic door opening and closing operations. A maximum of 16 time models, each with 4 time periods can be configured for each system.



Like the other configuration data, time models are also created by opening the creation dialog with the + button.



Make sure that no list entries are selected, otherwise more time periods will be created instead of a new time model.

The time model is assigned a unique designation (**Name**), as well as time limits related to the period. Clicking the **Save** button creates a new list entry with the information provided.

Time models with the same start and end time can also be created. This can be used to lock the door automatically at the specified time.

Configuring time models

The time models and activity periods (first and third columns) have fixed sequential IDs. [the time model with the sequential number **1** cannot be assigned to personnel, but only for operations like extended unlocking, for example.]

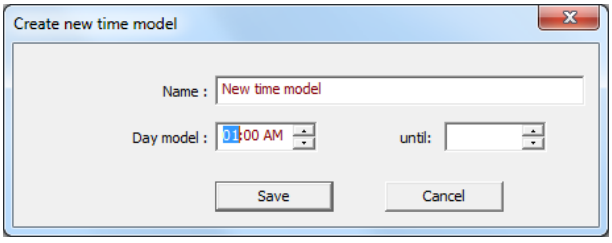
In addition to the name and start/end times, each entry contains seven check boxes for weekdays and one for a holiday.

Selecting the relevant check boxes defines the days on which the activity period should apply. When the **Holiday** check box is selected, the time period is applied to all defined holidays and holiday periods.

The maximum number of available time models (16) applies separately for each system.

Creating additional time periods

To create additional time periods, first select from the list the time model to which the new period should be added. Then click the button  as when creating a time model. The **Name** field contains the name of the selected time model and cannot be modified.



If you define new limits for an activity period then a new list entry is created which has the same number (first column) and the same name (second column) as the list entry that was selected. The number of the period (third column) increases by one.

The weekdays on which the new period should apply can now be defined. It is possible to activate several time periods for one day.

A maximum of four periods can be defined for each time model in this way.

Deleting time periods

Selected list entries can be removed again using the  button.

Click **Yes** to confirm that you wish to delete the time period.

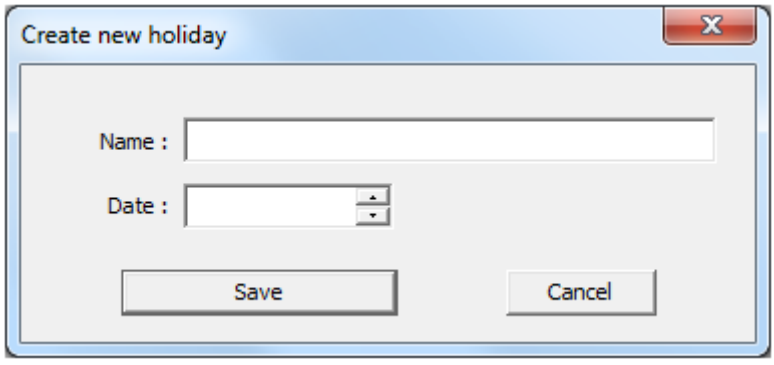
5.3.5 Holidays, holiday periods, daylight saving time

Compared to the normal week, holidays represent an exception and must be treated differently in terms of control functions. A **maximum of ten holidays** can be defined for every system, together with the date on which different activity periods should apply.

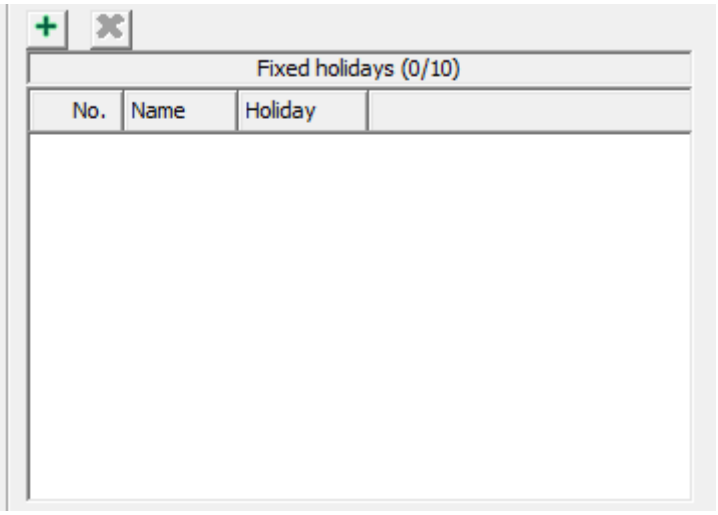
Holiday periods are also times with deviant time periods. Holiday periods may extend over several days - e.g. company holidays. **Two holiday periods** can be defined for each system

Creating holidays

The buttons for creating and deleting holidays are located above the **Fixed holidays** list window. The creation dialog is opened by pressing 



A unique designation (**Name**) and the **Date** when this holiday next occurs are specified. Clicking the **Create** button creates a list entry with the information provided.



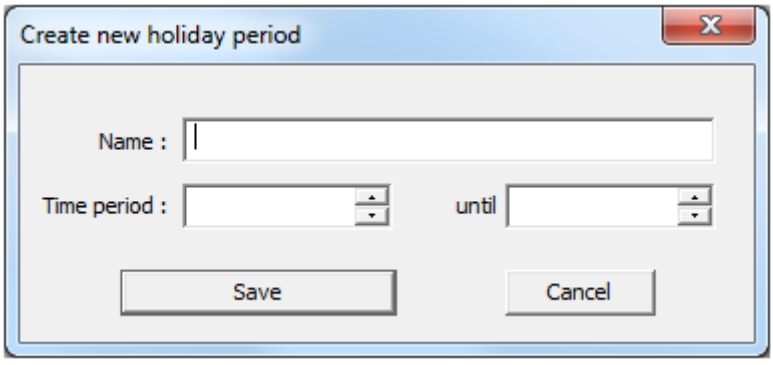
A fixed sequential ID, as well as the name and date of the holiday, are assigned to the entries - the last two fields can be moved and modified as required by double-clicking the edit state.
A maximum of ten holidays can be defined for each system.
Holidays are created with a specific date and must be redefined and adapted every year.

Deleting holidays

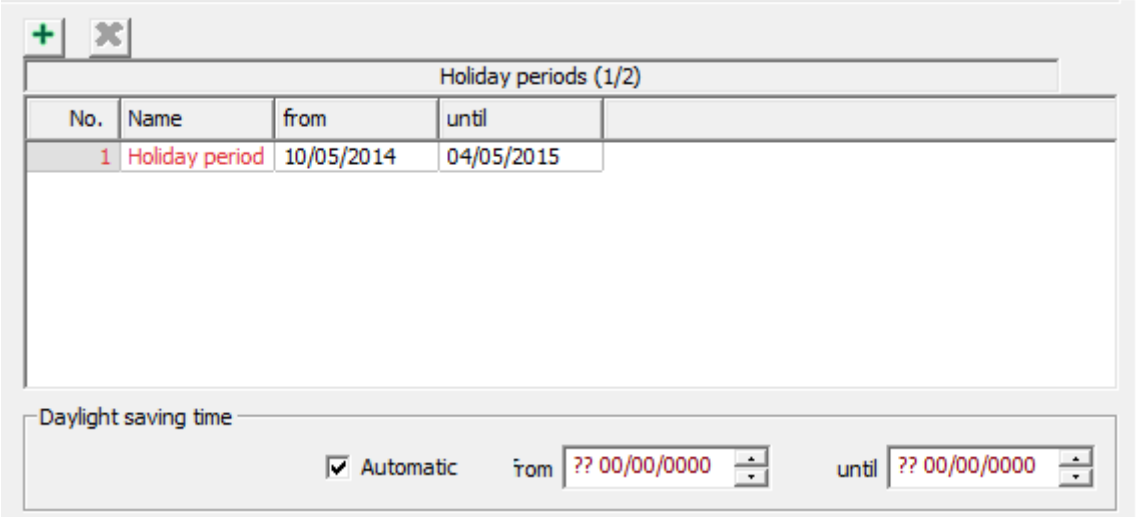
Selected list entries can be removed again using the  button.
Click **Yes** to confirm that you wish to delete the holiday.

Creating a holiday period

The creation dialog is opened by pressing the button.



A unique designation (**Name**) and a start and end date must be specified before a new list entry can be created using the **Save** button.



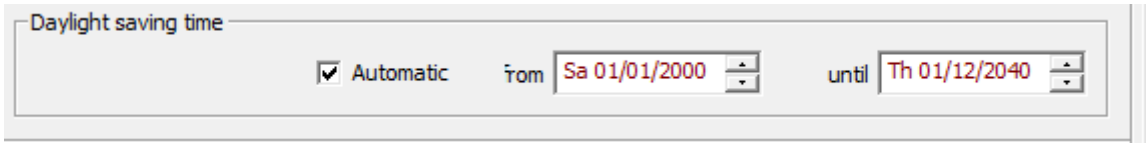
Two periods can be defined for each system.
Holiday periods are holidays that cover several days, and are created using specific data. Consequently, they must be redefined and adapted every year.

Deleting a holiday period

Selected list entries can be removed again using the button.
Click **Yes** to confirm that you wish to delete the holiday period.
When the **Holiday** check box is selected for a time period, this applies for all defined holidays and holiday periods - it is not possible to differentiate between the holidays.
The maximum number of holidays (ten) and special holiday periods (two) means the maximum number that can be stored simultaneously on the terminals.
If more are required, then expired holidays or holiday periods can be deleted to make room for them. However these must then be copied to the terminals using time initialization cards.

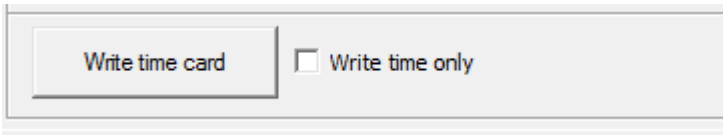
Daylight saving time

The daylight saving time setting can be defined (**automatically**) by the system or by making manual entries in the two date fields (from / to). Date information entered manually must be adapted every year.



5.3.6 Writing time cards

One of these system card types mentioned in the *System overview, page 7*, is the **time initialization card**, to which parameter settings of all time models and the current time are written and which are scanned at the door terminals.



The time models are ignored if the **Write time only** check box is selected and then the **Write time card** button is pressed.
A dialog box prompts you to place the badge in position and then shows the progress of the write process.
A message confirms whether the write process was successful. If the clock time was not the only element selected then the time is recorded and displayed in the **Last coding** field.
With the HITAG card type, more than one time card may be required to accommodate all the time models.
The time models are transferred to the terminals via these time initialization cards. During the data transmission process, the LED on terminals lights up orange. Successful transmission of the data is then confirmed.

Notice!
The **Time check** door parameter must be selected so that the time models are taken into account at the terminals.

Checking the cards
Before the card on the enrollment reader is written, the system checks whether it is actually a time initialization card. If the card has already been encoded in a different way (e.g. as a door or booking card), a warning to this effect is displayed with the option of overwriting the card and using it in the future as a time initialization card.
If the parameter **Program > Overwrite the card type** (menu bar) is selected, a confirmation prompt appears once for each card type - after that, the card is overwritten without further warning.
The parameter is only reset when the configuration program is restarted.
Facility and user cards cannot be overwritten with a different card type.

5.3.7 Updating the date and time

In addition to the door and time model data, the current time stamp (datetime) is also written to the transport cards. In order to use the most precise time data, especially for bookings, use a **mobile read-write device** (timesetter) and always update the transport cards with it immediately before scanning at the terminal.

Initializing the timesetter
The timesetter must first be initialized. It requires:
– Facility data from a facility card.

– An initial time from a transport card, for example: a door initialization or time initialization card.

To initialize the timesetter:

1. Place the system card (facility or transport card) on the read head of the device (gray field).
2. Press **1**.
3. Hold down **1** and press **2**.

Writing to the transport cards

Update the datetime on the transport cards immediately before scanning them at a door terminal.

1. Place the transport card (door initialization or time initialization card) on the read head of the timesetter device (gray field).
2. Press **2**.

The write process is indicated by colored LEDs. For details on what the color sequences mean, please see *LED display signals, page 41*.

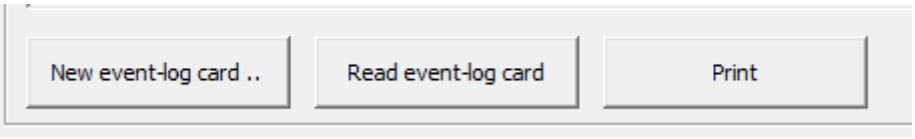
5.4 Event-log (booking) cards

Successful and unsuccessful access attempts are saved in the door terminals. The last 800 bookings are saved in a ring buffer. These can be retrieved with special booking cards and entered in the database.

First event-log cards are created, then the bookings retrieved from the terminals, then the cards scanned via the dialog. Different card types accommodate different numbers of bookings: HITAG1 holds 32, MIFARE holds 244, LEGIC holds 294. You must therefore create sufficient event-log cards and set up appropriate retrieval schedules.

Creating event-log cards

An event-log card must be initialized before the bookings can be scanned.



1. Place the event-log card on the read-write unit at the workstation.
2. Select the event-log dialog in the Explorer list.
3. In order for the terminal to accept an event-log card as new, create a new event-log card or empty a used one by clicking the **New event-log card...** button.

A message indicates that the event-log card was created successfully.

Reading bookings from the terminal

This system card can then be presented at the read unit of the corresponding terminal. While the LED shows orange, the terminal is writing data to the event-log card. If the event-log card is removed during this time, the data transfer will be interrupted. When the LED flashes green three times, the bookings have been successfully written to the card.

The memory of the terminal is erased during this process, i.e. the bookings cannot be retrieved after this again.

Scanning event-log cards

The card with the transferred bookings is then scanned via the dialog reader.

1. Place the event-log card containing the access data on the dialog reader.
2. Select the event-log dialog in the Explorer list.
3. Press the **Read event log card** button.

The read data will be shown in the list field. The following data is listed for each booking: datetime, surname, first name, event, door no., personnel no., company
The data read can be printed. Furthermore, all bookings are saved in the database and can be converted back to list format, printed, exported and edited further at any time using special reports in the Dialog Manager of the main access control system.

Notice!
Apparent sequencing errors in the event log
The door terminal always stores events in chronological order, but the time stamps in the event log are derived from the last time-setting at the door terminal. If any recent time-setting was not performed with the correct datetime, then time stamps of some events may appear to be out of sequence.

5.5 Possible data structures

Door groups Individual doors	256	512	768	1024
2	48 (= default)	80	112	144
4	52	84	116	148
8	60	92	124	156
16	76	108	140	172

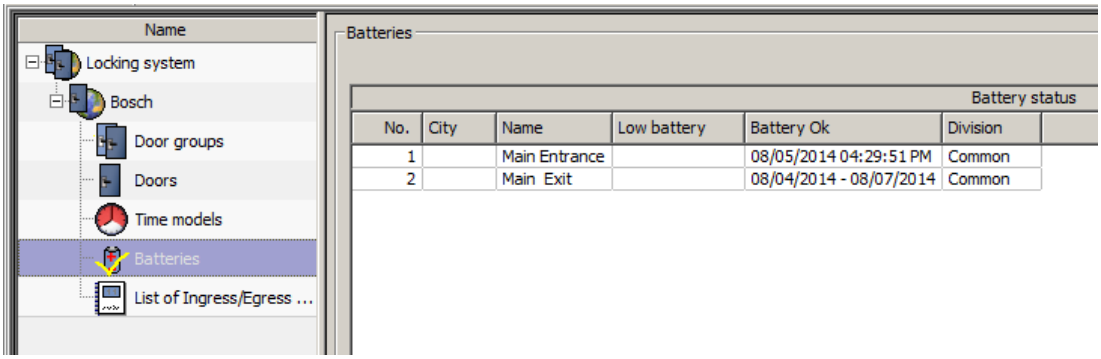
Tab. 5.1: The figures refer to the dataset length in bytes.

Notice!
HITAG1 cards can only be encoded with the default size (48 bytes). Only 240 door groups are possible instead of the 256 specified above.
The specified data sizes apply for PegaSys Version 2.0. PegaSys Version 2.1 with additional battery status requires 5 more bytes so the memory size is increased from 172 to 177 bytes. HITAG1 is an exception: only a maximum of 200 door groups are possible with a constant 48 bytes.

The dataset length should be selected in line with current requirements. Do not order storage space in anticipation of possible requirements. As data is written to all enabled sectors, increasing the storage space can significantly lengthen the time required for extending or renewing authorizations.

5.6 Batteries

The last known battery status of the PegaSys terminals can be viewed in the **Batteries** dialog. The battery status is only available from Version 2.1 of PegaSys (depending on the facility card).



The messages **Battery LOW** and **Battery OK** are written when the terminal attempts to access the user card.

There are three battery warning levels:

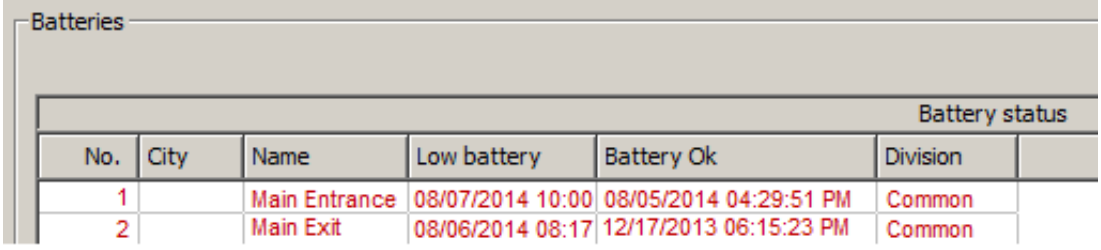
1. at 3.9 V: the next 5 badges receive a warning message consisting of a date and the number of the terminal.
2. at 3.6 V: when an access attempt is made with a user card, a RED signal is issued for 1 second together with 3 acoustic beeps. The next 5 ID badges receive a warning message the same as the first level.
3. at 3.4 V: when an access attempt is made with a user card, a RED signal is issued for 3 seconds together with a continuous acoustic beep that lasts 5 seconds. The next 5 badges receive a warning message the same as the other levels.

These battery-level warnings are available with terminal Firmware Version 4.1 and higher. The measuring tolerance is approx. 100mV for each level.

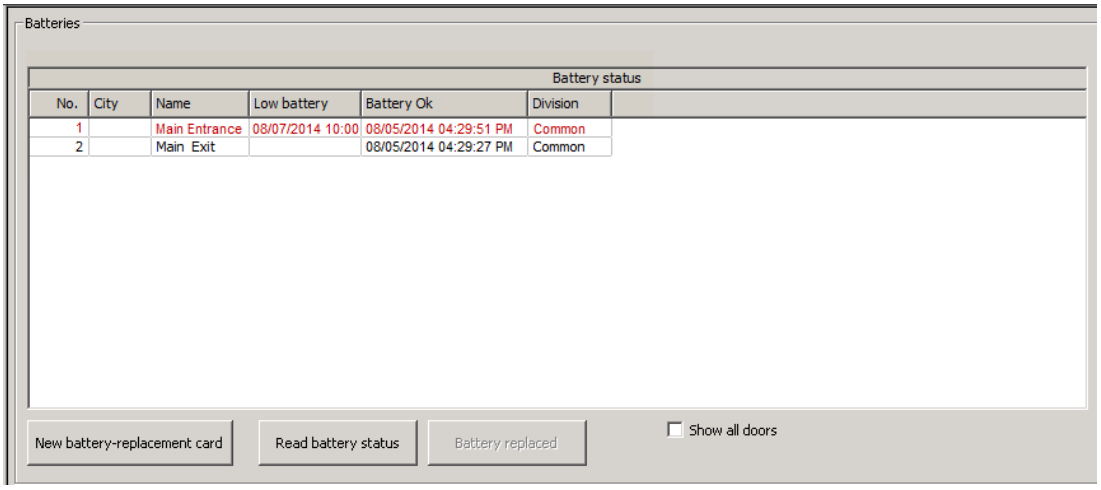
With every move to a higher warning level, messages are written to the next 5 user cards (one each). With every move to a lower warning level (e.g. after a change of batteries), 5 positive messages are issued including date and terminal number. As soon as a user card receives a battery status message, no other status messages can be written to this card until it has been updated on the online terminal, i.e. automatically read and reset.

The status message (positive or negative) is updated in the database if no other newer information is available.

The **Batteries** dialog provides in its upper list an overview of the terminals with weak battery messages.



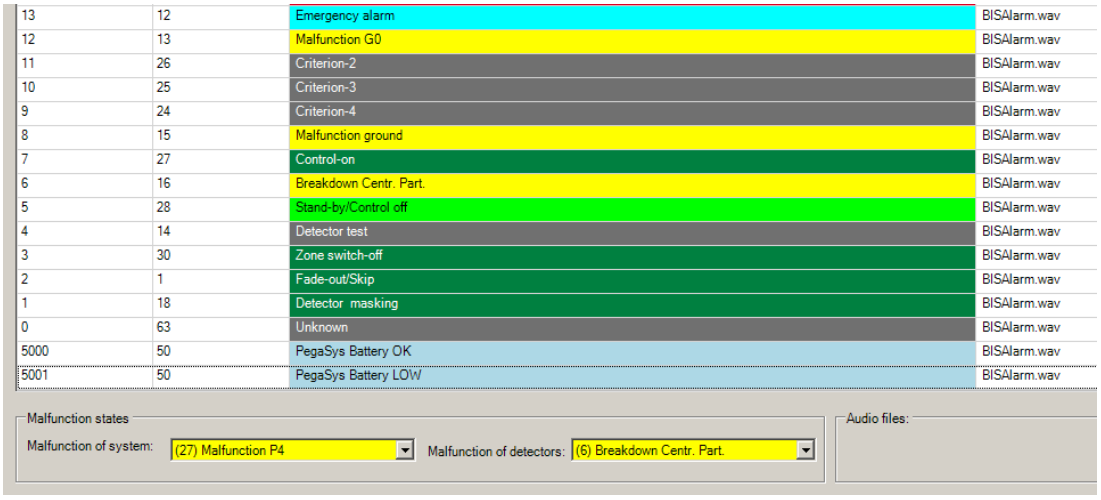
As soon as one of the batteries is changed and the online system receives a positive status message, the entries disappear from this list. If the **Show all doors** check box is selected, all doors are displayed together with their battery status. The lines marked in red contain terminals that have a weak battery or have not received a positive battery status message.



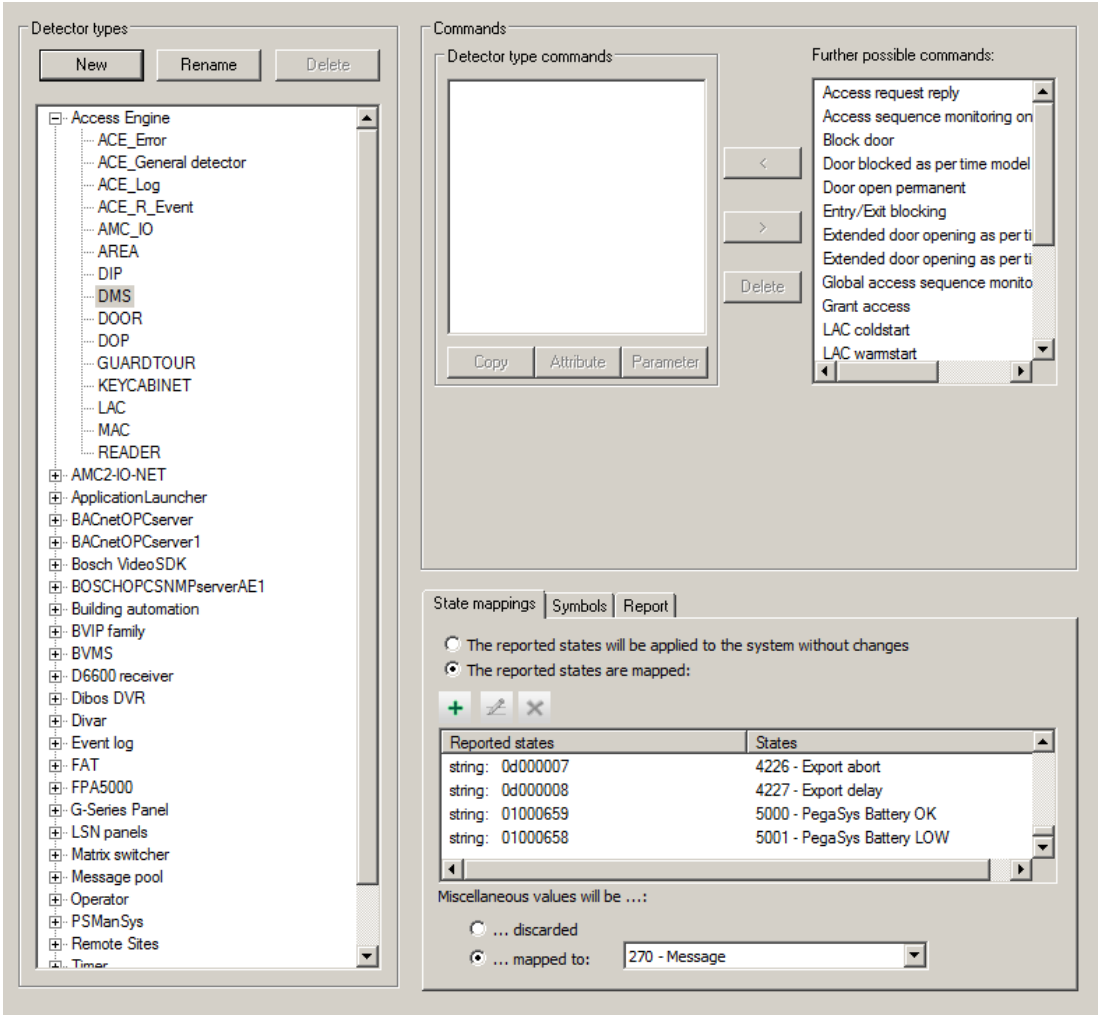
In some cases, terminals are used only rarely. In this case, the battery warnings would not be retrieved frequently enough, and the battery status would not be updated. For this reason all terminals with a **Battery OK** date older than one year are marked red as if a warning had been issued.
The date for the **Battery OK** display can also be set manually to the current date by pressing the **Battery replaced** button.
The user card with a battery status message can be read directly on the dialog reader by pressing the **Read battery status** button.

Battery status messages in the BIS

Battery status messages can also be displayed in the BIS.



The states **5000: PegaSys Battery OK** and **5001: PegaSys Battery LOW** are added to the states list of the BIS Configuration Browser.



– Select the entry **Access Engine > DMS** in the Detector types list.
– Add both statuses (with the status numbers 01000658 and 01000659) to the list on the **Status mapping** tab.

Only one message (**Battery OK** or **Battery LOW**) is displayed on each terminal, even if the online system receives up to five messages.

Battery replacement card

The **New battery-replacement card** button creates a battery-replacement card for cylinder-type terminals because they require clearance before their batteries can be changed.
A battery-replacement card can be used for all cylinder-type terminals in a system.

6 Offline Doors - System limits

Offline Locking Systems per access control system	1
Systems per Locking System	1 A **System** is a subdivision of the overall Offline Doors locking system. Each **System** is governed by its own facility card.
Doors per Locking System	65,000 total distributed across all Door Groups.
Door Groups per System	A maximum of 1024 door groups can be defined on any one facility card.
Time models per System	16
Holidays per System	10
Holiday periods per System	2

7 LED display signals

Signals for user cards

Door opened with single-unlock function:

Door opened with extended unlock function:

Door closed with extended unlock function:

Battery change request:

Special signals

Read-write confirmation for system cards:

No badge in range:

Read/write error:

Invalid authorization:

Time invalid:

Door initialization missing:

Facility data missing:

Data transmission:

7.1 Display with explanations

7.1.1 Signals for user cards

Door opened with single-unlock function

Meaning	The door is unlocked with a single-unlock card. This message also appears if the door is already unlocked for an extended period.
Booking entry	**valid single door booking** or **valid door-group booking**

Door opened with extended unlock function

Meaning	The door has been unlocked by an extended-unlock card, or by a time model.
Booking entry	**Door unlocked**

Door closed with extended unlock function

Meaning	The door has been locked by an extended-unlock card, or by a time model.
Booking entry	**Door in normal mode**

Battery change request

Meaning	Red LED signal of one to three seconds' duration. As long as the battery is not completely empty, a card-specific signal will follow. If the batteries are empty, no further signal will be displayed and no bookings will be possible. The battery change request is only displayed for user badges.

Booking entry	The **battery low** entry is shown after every 25 bookings.
Solution	Replace batteries.

7.1.2 Special signals

Read-write confirmation for system cards

Meaning	A system card was successfully read or written.
Booking entry	**Initializing**

No card in range

Meaning	The electronics have been activated, however no card has been detected in front of the reader.
Booking entry	No booking made
Solution	Present the badge to the reader again.

Read/write error

Meaning	Failed to read or write to a system card.
Booking entry	No booking made
Solution	Present the system card to the reader again.

Invalid authorization

Meaning	The card has no valid authorization.
Booking entry	**Access denied, card blocked**, **Not authorized**, **Access denied, card expired** or **Booking outside of time frame**

Solution	If necessary, change the authorization for this badge.

Time invalid

Meaning	The terminal does not know the current time.
Booking entry	No booking made
Solution	A time initialization card must be created and scanned at the terminal.

Door initialization missing

Meaning	The terminal has not been initialized.
Booking entry	No booking made
Solution	A door initialization card must be created and scanned at the terminal.

Facility data missing

Meaning	The terminal has not been initialized for this facility.
Booking entry	No booking made
Solution	The terminal must be initialized with a facility card.

Data transmission

Meaning	The LED lights up orange while data is being exchanged between a system card and a terminal. The duration depends on the volume of data to be transferred. The read/write process is then signaled.

7.1.3 LED displays for mobile read-write device

Write-confirmation for time model cards

Meaning Data has been successfully written to time model card.

Read-confirmation for the time model card

Figure 7.1:

Meaning The time model card has been successfully read.

Read-confirmation for facility card

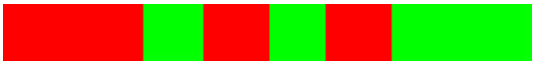
Meaning The facility card has been successfully read.

Read/write error

Meaning It was not possible to read or write to the system card successfully.

Solution Hold the system card to the reader again.

Facility data missing



Meaning The timesetter has not been initialized for this facility.

Solution The timesetter must be reinitialized with the facility card.

Time invalid

Meaning	The timesetter does not know the current time.
Solution	An appropriate time initialization card must be created and the timesetter must be synchronized.

Key:

The length of the colored bars in the examples shown indicates how long the signals are. The length shown here indicates that the signal remains lit for approx. 1 second.

 green LED

 red LED

 orange LED

 blue LED

 - additional acoustic signal

8 Offline doors - Managing Personnel Data

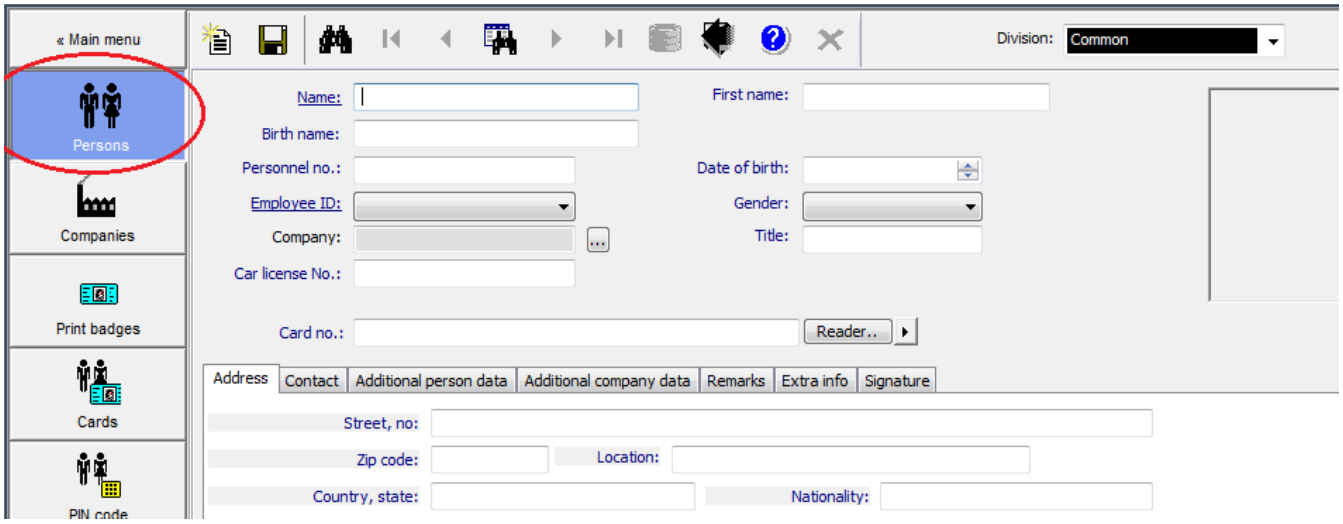
The database of the main access control system is used to store personnel data for the offline system as well.
Accordingly this data is entered via the access control system dialogs, and each cardholder for the offline system requires a valid card for the online access control system

8.1 Adding personnel data

Online data

To add personnel data and assign online authorizations, follow the steps below:

1. Switch to the dialog manager of the main access control system.
2. Open the dialog the **Personnel data** > **Persons**
3. Enter at least the mandatory data for the person.
4. Save the new record.



5. Create a badge in the **Print badges** dialog, if there is not one available yet.
6. Switch to the **Cards** dialog.
7. If an **enrollment reader** is already configured in the system, select it.
8. Press the **Record card** button to register the card in the system.

Offline data

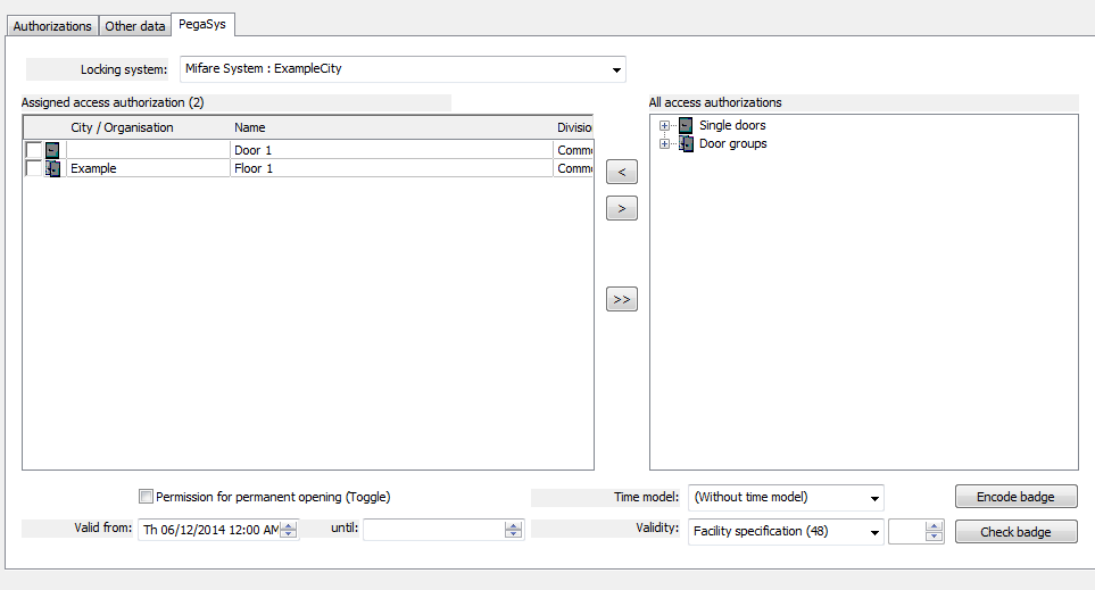
The corresponding authorizations for the locking systems are allocated separately.

1. In the **Cards** dialog, switch to the **PegaSys** tab with the selected personnel data.
2. Select the relevant locking system from the upper drop-down list - the doors and door groups set up for this system are displayed in the **Available access authorizations** list field.
3. Double-click to add individual entries or select several list entries and press the left arrow button to add the required doors and door groups. Repeat steps 2 and 3 for other systems - the selections made previously are retained. The authorizations for a maximum of three systems can be saved onto one (HITAG) card.
4. If necessary, overwrite the parameter values (validity dates, time model, etc.) if you do not wish them to have default values.
   - **Permission for extended unlocking (toggle)**:
     If the parameter **Extended unlocking (toggle)** is set on the door, then the cardholder can unlock that door for extended periods by presenting his badge at the read terminal for three seconds.
   - **Valid from:**

This field contains the current date and time by default, but these can be overwritten with future dates.

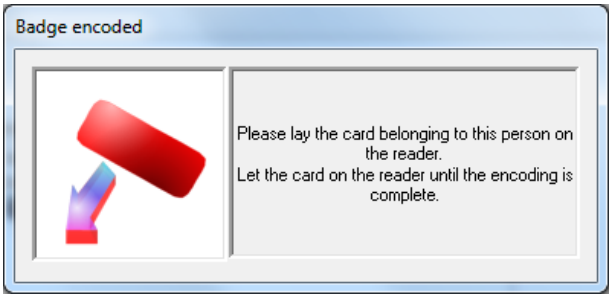
- **Valid until:**
  A date that specifies an absolute validity period for rights can be entered in this field - e.g. calendar year.
  Any date entered here supersedes information in the **Validity** field.
- **Time model:**
  One of the offline time models can restrict use of the badge to the times defined by the parameters.
  [time model no. 1 is not included in the selection list. It cannot be assigned to personnel.]
  The **Time check** parameter must be selected for the terminal.
- **Validity:**
  The default value specified when the system was configured is displayed in the default settings. This value can be modified individually for each cardholder.
  The validity period can be defined in different ways and on different levels - see also *Special settings, page 55*.

5. Writing to the card
6. Choose one of the following options:
   - Place the badge on the read-write unit at the workstation and press the **Encode card** to initiate the write process. [The system automatically activates the dialog reader for the offline system without you having to select it beforehand.]
   - Alternatively, the badge can also be encoded on one of the online readers (DELTA 7020/1000/1010).



Notice!
The validity limits of the online access control system apply to the offline system and take precedence in case of conflict.

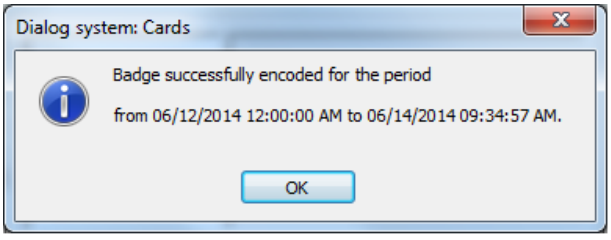
Data check during write process
When the Encode card button is clicked, a dialog box appears prompting you to place the card on the read-write unit.



The following circumstances result in error messages and in the termination of the write process.

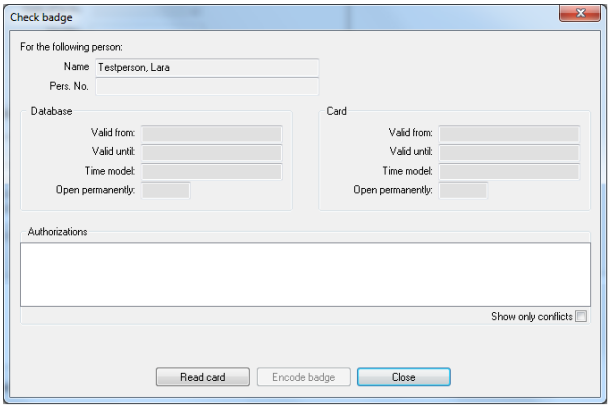
– No card is place on the unit or the code data cannot be read.
– The card is not a user card.
– The card does not belong to the selected person.

Display of the validity period indicates that the write process has been successful. The current date and time of 00:00 are used as a start time to ensure access even to terminals showing the incorrect time.



Validating cards

Pressing the **Validate card** button opens a dialog that validates the authorizations just encoded on the card by comparing them with the database.



This function can also be used as an initial troubleshooting measure, for example if a card does not work. One reason for malfunctions is data conflicts between card and database.

1. Select the relevant record from the database using the search fields in the dialog header.
2. Press the **Validate card** button on the **PegaSys** tab to open the **Check authorizations** dialog.
   Data for the selected person is entered in the **Name** and **Pers. no.** fields as well as the fields in the **Authorizations in the database** dialog field.
3. Place the badge on the dialog reader for the workstation.
4. Now press the **Read card** button at the bottom of the dialog.
5. Compare the **Authorizations in the database** with the **Authorizations on the card**.

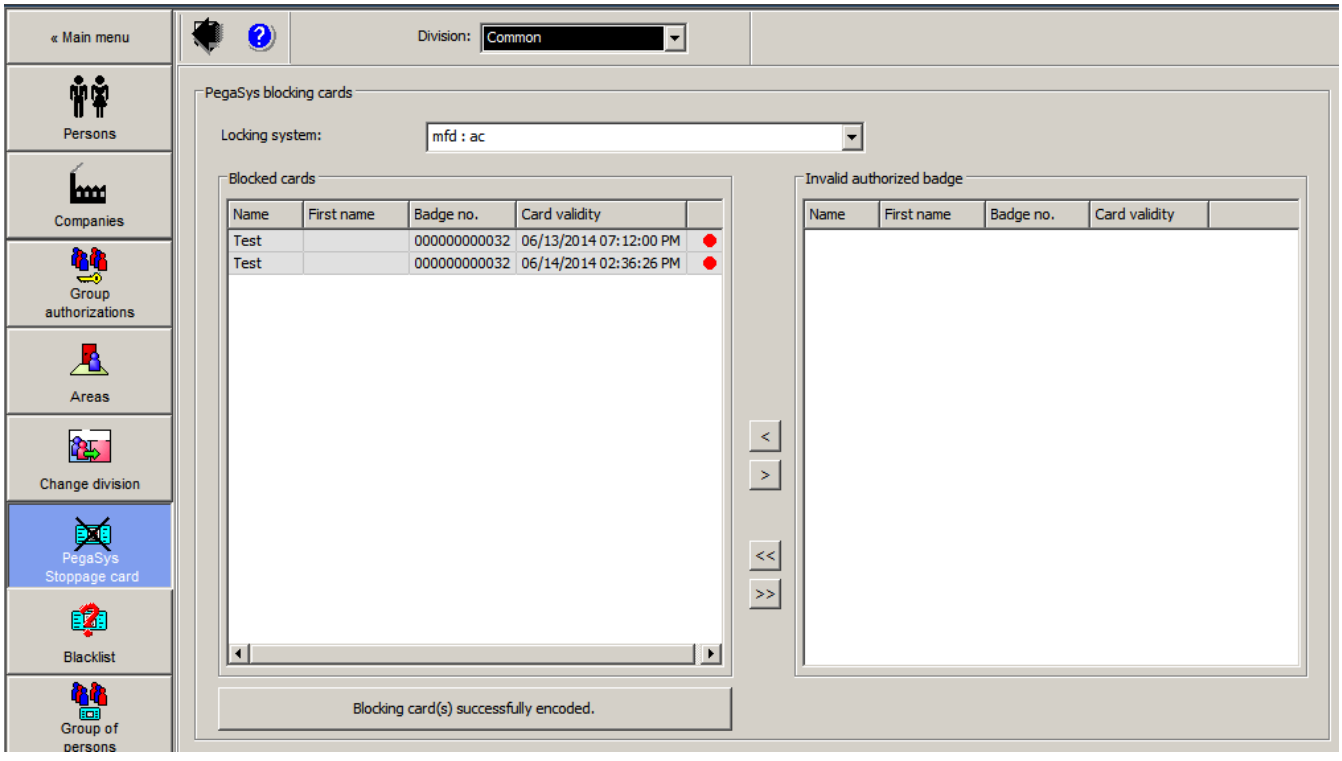
If the comparison reveals differences in the dates, the badge should be encoded again. The displayed dates do not have to match exactly. Rather the dates on the badge should fall completely within the validity period in the database.

8.2 PegaSys - Blocked cards

If the dialog authorization is valid, the **PegaSys Blocking** dialog appears in the **Personnel data** menu. When the locking system is selected, a list of currently invalid user cards is displayed on the right.
Currently invalid means:

- Personnel who have been actively blocked but whose cards still have active authorizations.
- Personnel whose card's validity has been terminated online but where the cards themselves still have active authorizations.

The offline terminals only have a limited memory for the entries in the blocked cards list. Therefore user cards that are to be blocked must be selected manually.
The expiry date of the user card is displayed in the **Card validity** column. Entries in the **Invalid authorized badge** list can be added to the Blocked cards list using the arrow buttons.



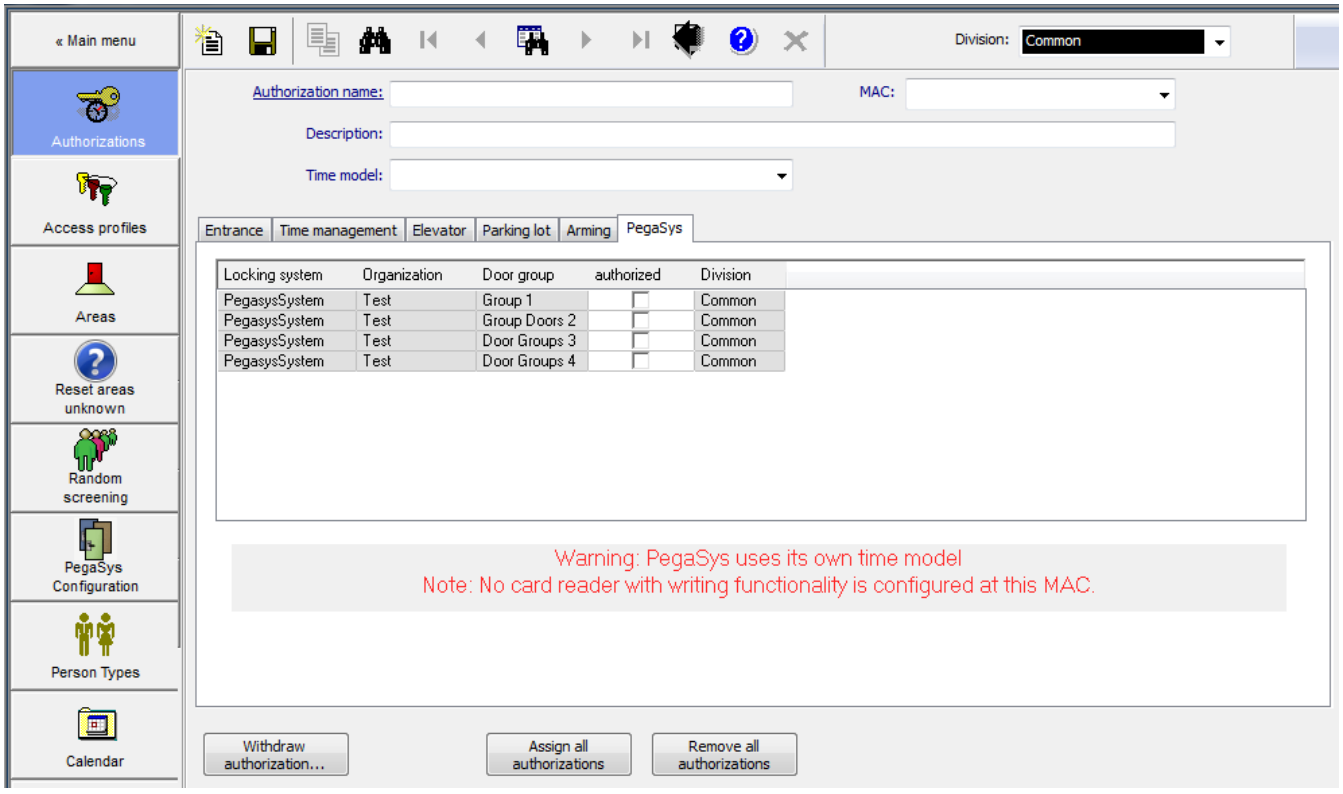
Pressing the **Encode** button adds the entries to so-called Blocking Cards. These encoded Blocking Cards must then be read into the offline terminals. Only then it is no longer possible to use these badges on these terminals.
The left list also provides an overview of which badges are currently on the PegaSys blocked list. A green/red lamp indicates whether or not the relevant entry can be removed from the list again.

- Red
  Card should be blocked.
- Green
  Card either re-authorized or expired and therefore no longer active.

The green entries are removed automatically the next time the blocking cards are encoded.

8.3 Online/offline access authorizations

The **Access authorizations** and **Room/time authorizations** dialogs in the **System data** menu contain a tab named **PegaSys**. All defined door groups (not individual doors) are listed in this tab.



Door groups of the offline locking system can be assigned to any access authorization in the online system. In order for the cardholder to access the door group, their card must be re-encoded.

Door groups that were assigned as a result of the access authorizations cannot be removed in the **Cards** dialog.

This also applies for the room/time authorizations, even though the time models for the online system do not apply to offline installations. This is highlighted in a message under the list field: **Note: PegaSys uses its own time models]**. In terms of offline authorizations, there is no difference between access authorizations and room/time authorizations - online room/time authorizations and offline authorizations are grouped together here.

8.4 Offline data on Temporary cards

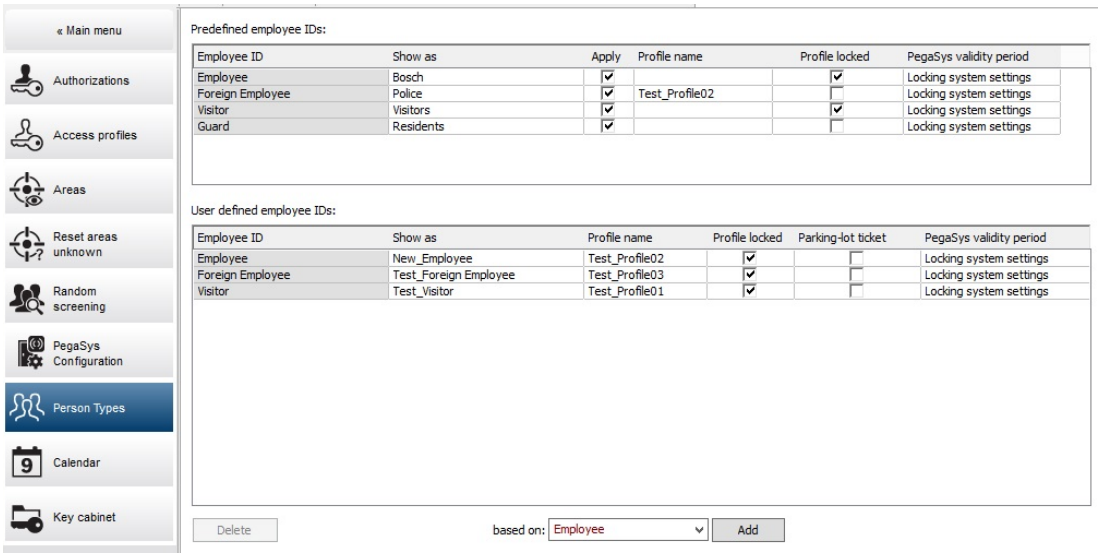
Avoid putting offline data on temporary cards

Online access control systems can generate temporary replacements for cards, potentially including cards containing offline data. The offline data will remain valid on the card even when the online data has expired.

To prevent possible security breaches, it is safest to ensure that you do not generate temporary cards for cards containing offline data.

8.5 Personnel classes - Validity period

If software for the offline locking system is installed, the additional column **PegaSys validity period** is displayed in the two list fields in the **Personnel classes** dialog.
If the relevant personnel class is selected when creating new personnel records in the **Persons** dialog, the validity period specified here is assigned to the offline authorizations. This validity period supersedes the default validity period that can be set when the offline locking system is configured.
The validity period can be defined in different ways and on different levels - see also *Special settings, page 55*.



Clicking the corresponding line in the **PegaSys validity period** column opens a dialog for selecting and setting a new value.

8.6 Status bar in main access control system

In addition to the displays for the access control system (Known, Blocked, Currently not valid and Random screening) the status bar also contains a colored visualization of the authorizations for the offline system (PegaSys).
This display and varying captions indicate the following states according to the processing state of the offline data.

LED	Caption	Meaning
	PegaSys	This card is not defined for the offline system.
	Encoded	A card with valid authorizations was encoded.
	Expired	The validity period for the offline system has been exceeded.
	Not current	The validity period for the offline system has not yet started - the start time is in the future.

8.7 Lists for offline data

The **Reports > Reports master data** menu in the main access control system has been extended to include the **Persons PegaSys** dialog, which allows users to print offline data.

Filter options

- **Personnel data**
  Individual people or groups (e.g. all personnel from a company/department) can be filtered out using the input fields.
- **Offline elements**
  - Locking system
  - Door groups
  - Doors
  - Organization (= grouping door groups)
  - Area (= area where door is located)
- All filters can be combined with one another.

Layout selection

The layout determines how the search results are displayed and which information is included. Four predefined list layouts are available.

Persons with doors/groups	Every person who has been assigned authorizations is listed together with the most important access control data. A system, location, and doors/door groups are listed for each person.
Doors with persons	The persons authorized for each door are listed and sorted according to the system.
Door groups with persons	The persons authorized for each door group are listed and sorted according to their offline systems.
Crosstab persons	Table view. The columns contain the designations of the doors and door groups (G), while the lines contain the names of the persons from the offline system. A cross (X) at the intersection of a column and a row indicates an existing authorization.
Event log by doors	All bookings (containing personnel information) at these terminals are listed according to their respective doors.
Logbook by person	All doors at which persons have booked are listed by person.

Blocked cards	List of all PegaSys cards that will be blocked or unblocked by the next encoding process.

8.7.1 PegaSys data in online reports

The reports

- Access authorization for each person
  with a display of PegaSys authorizations in the form:
  - Individual door, location, system
  - Door group, organization, offline system
- Access authorizations and room/time authorizations
  with a display of PegaSys authorizations in the form:
  - Door group, offline system

contain information about the PegaSys system.

8.8 Special settings

Unlike online systems, authorizations for offline locking systems are only allocated for relatively short periods and must be renewed and extended at regular intervals. The validity period can be defined in three different ways and on three different levels.

1. Individual setting for each person.
   See *Offline data, page 48*.
2. Assignment via personnel class.
   See *Personnel classes - Validity period, page 53*.
3. Specification of a default validity period for the entire locking system.
   See *Standard validity, page 21*.

The sequence specified reflects the relative importance of the information. An individual setting supersedes personnel class assignments and settings of the locking system. Personnel class assignments supersede settings of the locking system.

9 Offline doors - Description of Procedures

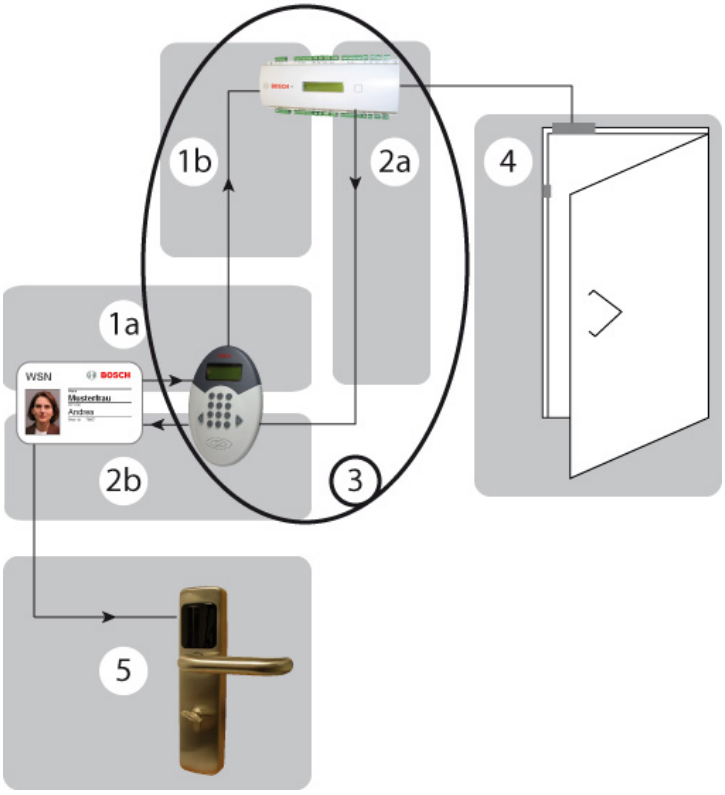
The following procedures for offline / online hybrid systems differ from those for pure online systems.

9.1 Data creation

The following procedure is recommended for new objects.

1. Definition of door groups
2. Definition of time models
3. Definition of terminals (doors)
4. Management of Personnel Data
   - Adding personnel data
   - Authorization allocation - online (optional)
   - Card allocation - online
   - Authorization allocation - offline
   - Card encoding - offline

9.2 Access



1a Read card

1b Card number sent to the AMC

2a Current data shared with the reader

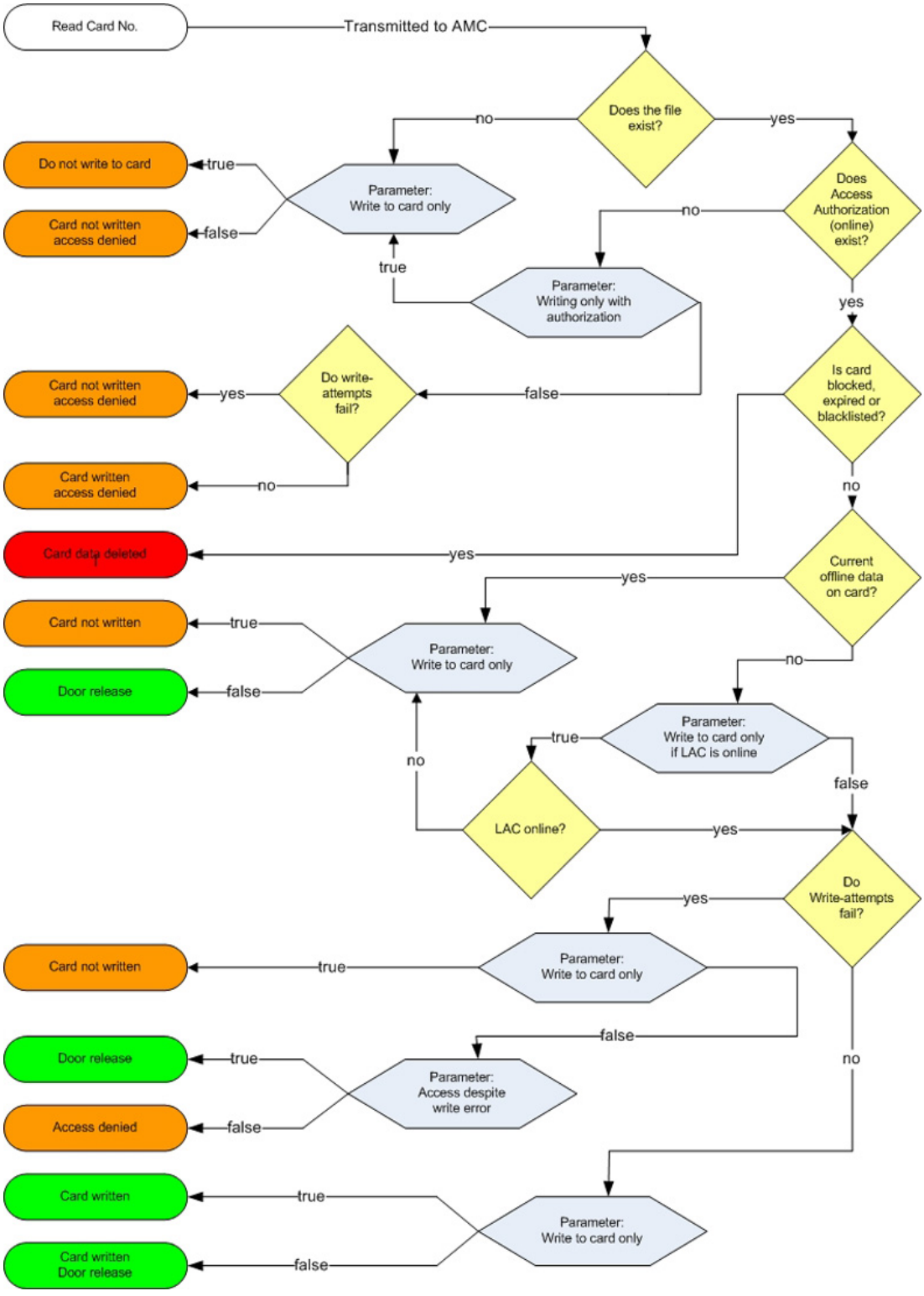
2b Current data written to the card

3 For details on the validation and write process on the AMC, please see the flow diagram in *Write process, page 57*.

4 Door release for the online system (if configured)

5 Authorization check at door terminals

9.2.1 Write process



In the majority of cases write processes are used to extend access authorizations by the amount of time specified.
For this reason, the last write date is also stored in the database. The need for extension is determined by means of a comparison with the current date or the current time. However, as this would mean that expiration data would be updated every time the card is scanned, a write process would also need to be carried out each time. To avoid unnecessary waiting times and delays at read-write units, a validity period and the preset writing rules (see also *Configuring the read-write unit, page 12*) are used to determine a point in time until which the badge data is considered valid.
In the default setting, the data is only updated when two-thirds of the validity period have expired.

Example of default writing rules
Validity period: 1 day = 24 hours
2/3 of the validity period: 16 hours
If a cardholder scans the card when he starts work and his expiration date is updated, he can pass the read-write unit for the rest of the day without a new write process being triggered - the data is only updated after sixteen hours.
This ensures that the validity period is only updated once a day, for example.

10 Offline doors - Application Examples

The following examples demonstrate parameter settings for special requirements. Each example deals with one specific parameter.
Other variations can be produced by combining parameter settings. Hence the examples can also be combined with each other.

Access control reader and/or write-capable reader?
The decision regarding the way in which the DELTA 7020 is used depends on a number of different factors; it can make sense to omit the reader from the access control system (online).

- Is there an entrance (e.g. main entrance) that must be passed by most of the cardholders?
  - **Yes**: A DELTA 7020 with simultaneous access control function for the online system is recommended.
  - **No** (There are a number of possible entrances, for example): The use of DELTA 7020 readers at each entrance would not be recommended for cost reasons. In this case, the reader (or possibly two readers) should be installed in the most frequented area as a simple recharging station.
- Should extensions of authorizations be possible at all times?
  - **Yes**: We recommend the use of a DELTA 7020 (with or without access control function) in the most frequented area.
  - **No** (As a rule, fixed expiration dates are used): If the read-write unit at the operator workstation is not enough, any DELTA 7020 will suffice for ad hoc extensions.

Example 1: Read-write unit only
Ideally a hotel should be accessible to everyone, at least as far as the reception desk. Therefore, access control readers are mainly installed at doors that require particular security, in the event that the settings in the **Example 2** in Single doors or door groups (see below)are not sufficient.
Accordingly, the DELTA 7020 is not linked with access control functions; instead, it is configured purely as a read-write unit for the offline system.
Condition:
The **Reader function** parameter in BIS Configuration Browser > Connections > ... > Offline locking system must be set to **Write locking system** and the **Write to card only** check box is selected.
The DELTA 7020 needs only to be installed in a central location for hotel personnel, so that their authorizations can be updated and extended. If possible, choose a location that all affected persons pass on a regular basis, e.g. staff room.
For hotel guests, authorization for the hotel room door is assigned at check-in, and written to the card via a DELTA 7020 at reception. Authorizations normally need not be changed, but this can be carried out at reception if required. Hence the reader need not be installed in a freely accessible area.

Example 2: Read-write unit with access control function
Student residences: Here, only residents must be allowed access. One access control reader for the main entrance can secure the building against unauthorized access. One DELTA 7020 can simultaneously update and extend locking system rights for authorized persons.
Condition:
The **Reader function** parameter must be set to **Write locking system** and the **Write card only** check box is cleared.

If the **Write without access rights** check box is not selected, then only people with access authorization (online) for the main entrance will have their offline rights updated and extended.

Single doors or door groups
Each door created in the system can be assigned as an individual authorization as well as belonging to any number of door groups. The following examples are intended to demonstrate how these two types of authorization should be handled.

Example 1: Hotel
At reception, the validity period for the room in question is assigned as an **individual authorization** in accordance with the booking. It is also possible, for example, to assign another door group containing all general-use areas (restaurant, breakfast room, sauna, sports facilities etc.), provided that these areas are secured by terminals.
In contrast, hotel personnel are assigned a **door group** containing all (or at least most) doors.
Condition:
The **Check door groups** parameter must be selected (checked).
Procedure:
The guest can open the door to his room, in line with the assigned individual authorization, and can also open all doors in the door group. Hotel personnel are able to open all doors in the assigned door group, which also includes all doors to the guest rooms.

Example 2: Areas within the offline system that are subject to increased security requirements and may only be accessed by certain people.
The authorized people are assigned these doors as individual authorizations. It is irrelevant whether these doors belong to door groups and it is also irrelevant to whom these door groups have been assigned.
Condition:
The **Check door groups** check box must be cleared.
Procedure:
Only individual authorizations are accepted at the doors. People who are only assigned door group authorizations for these doors will not be granted access

More holidays per year
The maximum limits for holidays (= 10) and holiday periods (= 2) are based on the permitted volume of data that can be saved simultaneously in the terminals via initialization cards.
It is possible e.g. to define more holidays and holiday periods throughout a period of one year, albeit with a slight increase in the administrative workload.
Example
At the end of 2007, the dates of ten holidays for the 2008 calendar year were stored in the terminals. At the start of April 2008, the holidays that have already passed (e.g. New Year's Day, Good Friday, Easter Monday) can be deleted and replaced with three new dates.
This new list must be distributed back to the terminals via the time initialization cards.

Normal or extended unlock
If the badge is valid, the LED on the terminal flashes green three times. The door may be opened within a predefined unlocking pulse of 3 seconds (default value). If the door is in **extended unlock** mode, the LED also flashes green three times when a valid badge is presented.

A card with the **Permission for extended unlocking (Toggle)** unlocks the door normally if the card is removed during these three flashes. If, instead, the card is held to the terminal's read unit for longer than 3 seconds, then a continuous green signal is displayed and the door remains unlocked until a card with extended unlock authorization is held to the terminal again for at least three seconds. The door is then locked; i.e. access is only possible with authorized badges.

Condition:

The **Extended unlock (Toggle)** check box must also be selected for the terminal.

By time model:

The same function can be controlled via a time model. A time model is selected for the **Opening hours model** door parameter and the door is unlocked between the "from" time and the "until" time.

Time models with the same "from" and "until" times can be used to lock doors that are in extended unlock mode.

Notice!

Unlocks governed by time models always contain the risk that unsupervised areas could be made freely accessible.

Examples: Office buildings with public access

1. **Manual extended unlock/lock**
   The office is unlocked each morning using the extended unlocking function and made accessible to the public. When the office closes, extended locking comes into effect. Thereafter only people with a valid card have access.
2. **Extended unlock/lock controlled via a time model**
   If the public visiting hours are not the same as the staff hours, door locking and unlocking can also be controlled via a time model.
   Personnel hours: 8.00 - 12.00 and 13.00 - 17.00
   Public visiting hours: 9.00 - 11.00 and 14.00 - 16.00
   To correctly comply with the hours and avoid the need for manual unlocking/locking, a time model can be used with two periods that correspond to the public visiting hours.
3. **Extended locking controlled via time model**
   The office is unlocked manually each morning by the first staff member to arrive, using the extended unlocking function. A time model with identical "from" and "to" times is used to perform extended locking and unlocking at those times.

Refer to

– *Single doors or door groups, page 60*

Bosch Access Systems GmbH
Charlottenburger Allee 50
52068 Aachen
Germany
www.boschsecurity.com

202102231922