AMS Offline Türen

Konfiguration und Bedienung

de Software manual

Inhaltsverzeichnis

1 Einführung

Das **PegaSys** Schließsystem ist ein Offline-System, das zur Sicherung von Objekten verwendet wird, die nicht online überwacht werden können oder müssen.
Offline-Systeme werden in der Regel verwendet, wenn keine kontinuierliche Synchronisierung erforderlich und dadurch die hohe Verfügbarkeit von individuellen Komponenten unnötig ist, wenn das Gelände eine direkte Verbindung verhindert (z. B. durch extrem lange Kabelentfernungen zwischen Installationen) oder die Installation von Online-Komponenten zu teuer wäre. Im Vergleich zu konventionellen Schließsystemen (Sicherheitsschlösser mit speziell hergestellten Schlüsseln) liegt der Vorteil von Offline-Systemen darin, dass hohe Investitionskosten nur anfallen, wenn das System installiert oder erweitert wird. Schlösser und Schlüssel müssen nicht aktualisiert oder ersetzt werden (z. B. im Fall von Verlust oder Diebstahl), da die Software die betroffenen Einheiten (Ausweise) deaktiviert und sie so unbrauchbar macht.
Offline-Schließsysteme sind in der Regel Installationen mit einer Anzahl von individuellen Räumen, die zu sichern sind, z. B. Hotels, Studentenwohnheime und Krankenhäuser.
Die PegaSys Komponenten werden im Zutrittskontrollsystem integriert und von dort aus verwaltet.

1.1 Begriffserläuterungen

Um zwischen den individuellen Zutrittskontrollkomponenten zu unterscheiden, werden die nachfolgenden Begriffe für die verschiedenen Komponenten verwendet:

- **Zutrittskontrollsystem**
  Dies bezieht sich auf die Online-Komponenten
  - Die Datenverwaltungsebene (Dialogsystem, Datenbank, Logbuch usw.)
  - Zutrittskontrollzentralen, die den Zutritt auf Grundlage der von der Datenverwaltungsebene empfangenen Daten gewähren oder verweigern.
  - Leser, die die Daten von den Ausweisen ablesen und diese an die Controller weiterleiten.
- **Schließsystem**
  Die Offline-Systemelemente (im Gegensatz dazu bezieht sich der Begriff **System** auf nur eine Untergruppe des Schließsystems.)
  - Ausweise, die die Autorisierungsdaten enthalten.
  - Türterminals, die den Zutritt auf Grundlage der von den Ausweisen gelesenen Autorisierungsdaten gewähren oder verweigern.

Das Schließsystem als integrierte Einheit nutzt auch die Dialoge, Zutrittskontrollzentralen und Leser des Zutrittskontrollsystems.

1.2 Besonderheiten von Schließanlagen

Bei Zutrittskontrollsystemen werden Codedaten in Kombination mit den Personaldaten und den Zutrittsberechtigungen vom Ausweis abgelesen und in der Datenbank gespeichert. Beim Scannen an einem Zutrittskontrollleser wird die Codenummer gelesen und mit den gespeicherten Daten verglichen. Wenn die Überprüfung positiv ausfällt, wird der betreffenden Person Zutritt gewährt.
Deshalb ist eine Verbindung zu einem Datenspeicherelement des Systems (d. h. des Online-Systems) zwingend.

Bei Offline-Systemen werden die Zutrittsberechtigungen für gewisse Türen auf dem Ausweis gespeichert. Diese Berechtigungen werden beim Scannen abgelesen und überprüft, um sicherzustellen, dass der Ausweis die Identifikation für die betreffende Tür enthält und über aktuelle Daten verfügt.

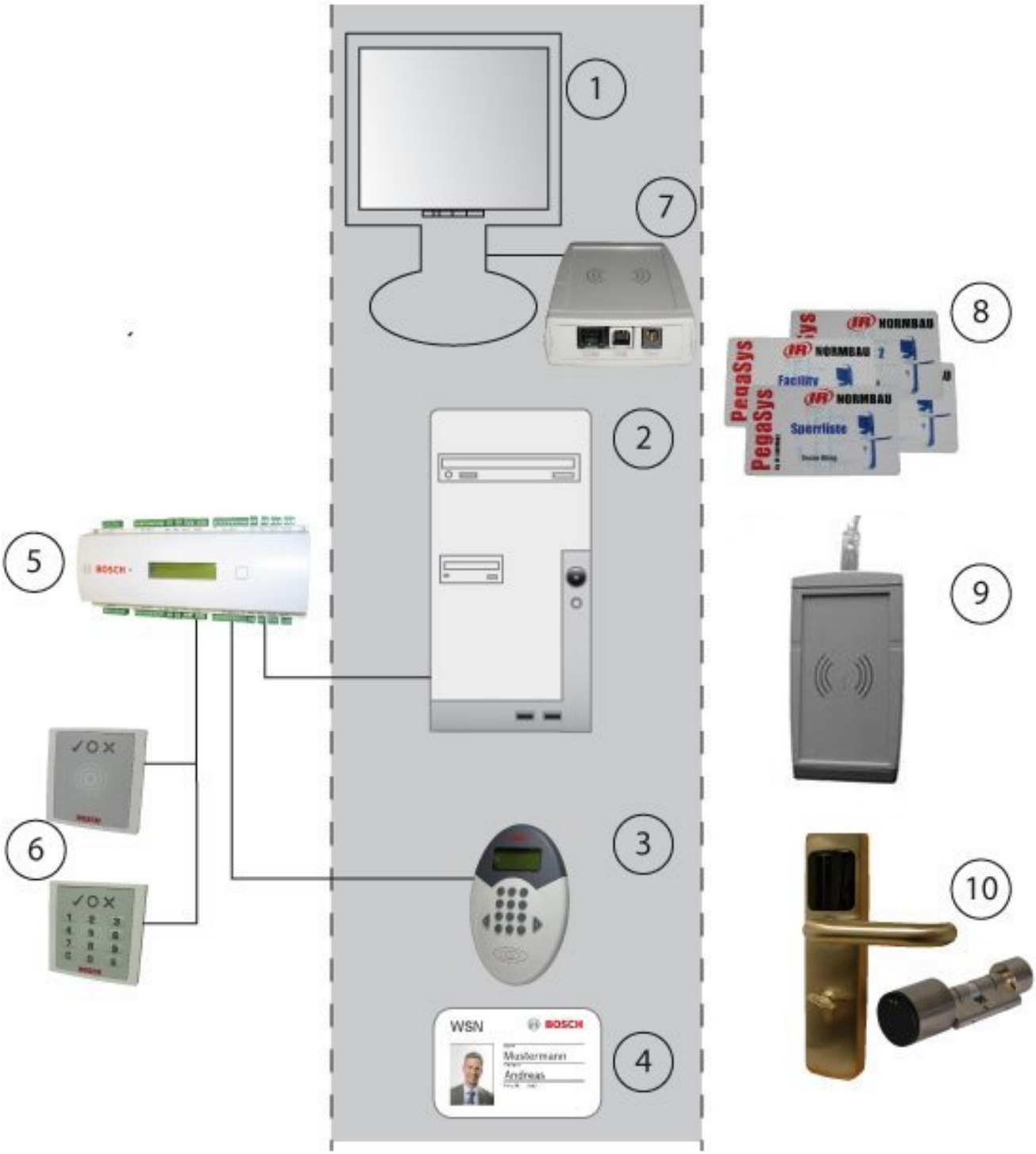
Die Offline-Variante stellt ein einfaches Sicherheitsrisiko dar und es ist praktisch unmöglich, Missbrauch im Falle von Verlust oder Diebstahl zu verhindern. In Online-Systemen können missbrauchte Ausweise blockiert, aus der Datenbank gelöscht oder ein Ablaufdatum zugewiesen bekommen, während Offline-Systeme keine direkte Intervention zulassen. Um das Risiko von Missbrauch möglichst klein zu halten, werden den Berechtigungen ein Ablaufdatum/eine Verfallzeit zugewiesen. Zu diesem Zeitpunkt verlieren die Berechtigungen ihre Gültigkeit. Um sie zu reaktivieren, muss die Gültigkeitsdauer verlängert werden. Dies erfolgt über einen Spezialleser mit Schreibfunktion. Wenn die Berechtigungen in der Zwischenzeit nicht gelöscht oder gesperrt wurden, werden sie verlängert oder erneuert, wenn der Ausweis an diesem Online-Leser gescannt wird.

1.3 Bestandteile von PegaSys

Wenn das Offline-Schließsystem installiert ist, müssen folgende Anwendungen und Erweiterungen eingerichtet sein:

- **Software**
  - **Konfigurationsdialog** für PegaSys
    Diese Anwendung wird verwendet, um die Systeme einzurichten und die allgemeinen Einstellungen (z. B. Gültigkeitsdauer) vorzunehmen, Zeitmodelle zu erstellen und Türen und Türgruppen zu konfigurieren.
  - AMS Dialog Manager (AMS-Dialogmanager) > **Configuration** (Konfiguration) > Device editor (Geräteeditor)
  - Bei der Erstellung von Türmodellen kann die Schreibfunktion auf der Registerkarte **Additional settings** (Zusätzliche Einstellungen) aktiviert und konfiguriert werden.
  - **Persons (Personen) > Cards (Ausweise)** im Dialog-Manager
    Dieses Dialogfeld enthält eine zusätzliche Registerkarte mit dem Namen **PegaSys**, in der Sie Berechtigungen für das Schließsystem zuweisen können.
  - **Reports (Berichte) > Master data lists (Stammdatenlisten) > PegaSys persons (PegaSys Personen)**
    Listen über die Ausstattung und die Zuweisung von Berechtigungen für Offline-Türen können mit verschiedenen Filter- und Suchkriterien erstellt werden.
- **Hardware**
  - **Systemausweise**
    Systemausweise werden zur Initialisierung des Türterminals und zur Datenaktualisierung (z. B. schwarze Listen) verwendet.
  - Ein **Lese-/Schreibgerät** für Benutzerausweise und Systemausweise muss mit der/den Arbeitsstation(en), die PegaSys Systemdaten verarbeiten, verbunden sein.
  - Ein **mobiles Lese-/Schreibgerät** (Timesetter) für den Zeitstempel, der wiederum zur Aktualisierung/Initialisierung der Türterminals (optional) verwendet wird.
  - **Terminals** zum Lesen der Benutzer- und Systemausweise an den Türen im Offline-Schließsystem.

2 Systemübersicht



1. Bedienplatz
2. Server mit Konfigurationsanwendung und Datenbank
3. Zutrittskontrollleser mit Schreibeinheit
4. Ausweis – für beide Systeme
5. AMC2-Zutrittskontrollzentrale
6. Zutrittskontrollleser
7. Dialogeinheit zum Lesen und Schreiben von Online- und Offline-Daten

8. Verschiedene Systemausweise für das Schließsystem
9. Mobile Lese-/Schreibeinheiten für Daten-/Zeitstempel
10. Türterminal/Zylinder mit Leseeinheit

Wenn das PegaSys Schließsystem in ein Bosch Zutrittskontrollsystem integriert ist, werden gewisse Komponenten von beiden Systemen verwendet. Der graue Bereich im Diagramm oben enthält die Systemkomponenten, die sowohl vom Zutrittskontrollsystem wie auch vom Schließsystem verwendet werden.

3 Systemkomponenten

3.1 Bedienplatz

Über die gleiche Dialogoberfläche [**1**] werden die Personendaten für die Zutrittskontrolle als auch für die Schließanlage angelegt. In einem Arbeitsschritt können neben den Zutrittsbrechtigungen für das Zutrittskontrollsystem auch die Begehungsrechte für das PegaSys System vergeben werden.
Listen über den Stand der Berechtigungsvergabe für die Schließanlage können über die gleichen Menüpunkte aufgerufen werden wie für die Zutrittskontrolle.

3.2 Server

Auf diesem Rechner [**2**] läuft die Software des Zutrittskontrollsystems und der Schließanlage. Über den Configuration Browser des BIS-Systems werden auch die Leser [**3**] für die Schließanlage parametriert.
Die Datenverwaltung für PegaSys erfolgt in speziellen Tabellen der Datenbank des Zutrittskontrollsystems.

3.3 Lese/Schreibeinheiten

Es muss mindestens eine Lese-/Schreibeinheit [**3**] verfügbar sein. Idealerweise werden diese an häufig benutzten Eingängen angebracht (z. B. Haupteingang), damit die Berechtigung für das Schließsystem zur gleichen Zeit erweitert werden kann, wie der Zutritt zur gesicherten Einrichtung gewährt wird.
Es ist aber auch möglich, diese Leser an speziellen Orten anzubringen, unabhängig vom Zutrittskontrollsystem, damit die PegaSys Rechte nicht automatisch erweitert werden, sondern speziell angefordert werden müssen.

3.4 Ausweis

Für das Offline-System sind keine speziellen Ausweise [**4**] erforderlich. Die für das Schließsystem erforderlichen Daten werden in dedizierten Sektoren des Zutrittskontrollausweises geschrieben.

3.5 AMC2 4R4 Controller

Für den DELTA 7020/1000/1010 [**3**], der als Lese- /Schreibeinheit für die Schließanlage eingesetzt wird, ist ein AMC2 4R4 [**5**] (= Zutrittskontrollzentrale mit RS-485 Leserschnittstellen) notwendig.
Die reinen Zutrittskontroll-Leser [**6**] können beliebige Protokolle und Leseverfahren benutzen und mit jeder AMC2-Variante betrieben werden.

3.6 Zutrittskontrollleser

Diese Leser [**6**] haben nicht zu tun mit dem Schließsystem; sie regeln nur Zutrittsanfragen im Zutrittskontrollsystem. Ausweisinhaber, die die Türen im **Offline**-Schließsystem verwenden können [**9**], können auch Berechtigungen für Türen im **Online**-Zutrittskontrollsystem haben.

3.7 Lese/Schreib-Einheit am Bedienplatz

Dieses Gerät [**7**] wird über eine USB-Schnittstelle direkt an den Arbeitplatzrechner angeschlossen und dient der Übertragung von Berechtigungen auf Benutzerkarten bzw. von systemrelevanten Daten (z.B. Tür- und Zeitinitialisierungsdaten) auf spezielle Systemkarten [**8**] und kann gleichzeitig als Bekanntmachungsleser für Ausweise des Online-Systems genutz werden.

3.8 Systemausweise

Zum Übertragen von Zutrittsdaten – z. B. Initialisierungsdaten – an die Türterminals [**9**] sind spezielle Systemausweise [**8**] erforderlich.
Es gibt folgende Arten von Systemausweisen:

Einrichtungsausweise
Dieser Ausweis enthält allgemeine Systemdaten wie den System-Identifikationscode, den Datentyp und die Datensatzgröße. Er wird als „Initialisierungsausweis“ für die Software und für jedes Türterminal verwendet.

Türinitialisierungsausweise
Verwendet für die Übertragung der Türdaten an das jeweilige Türterminal

Zeitinitialisierungsausweise
Verwendet für die Übertragung von Zeitmodellen und der Uhrzeit an Türterminals

Uhrinitialisierungsausweise
Ausschließlich verwendet für die Übertragung der Uhrzeit (Datum und minutengenaue Uhrzeit).

Sperren der Ausweise
Informationen zu gesperrten Ausweisen können mit diesen Ausweisen an die Türterminals übertragen werden.

Registrierungsausweise
Mit dieser Art von Ausweisen können in den Türterminals gespeicherte Daten abgerufen und an die Datenbank übertragen werden.

Batterieersatzausweise
Zylinder können erst dann (beispielsweise) zum Wechseln der Batterie geöffnet werden, wenn ein Batterieersatzausweis korrekt gelesen wurde.

Demontageausweis
Der Zylinder kann erst dann aus der Tür genommen werden, wenn an der Tür ein Demontageausweis gescannt wurde.

3.9 Mobile Lese-/Schreibeinheit (optional) - Timesetter

Zur Aktualisierung der Zeiten - vor allem nach einem Energieausfall an den Terminals - werden Zeitinit-Karten über diese Einheit mit aktuellem Datum und Uhrzeit beschrieben, mit denen dann in unmittelbarer zeitlicher Folge die Terminals initialisiert werden können.

3.10 PegaSys - Türterminal/Zylinder

Diese Leseeinheit gleicht die Identifikation einer einzelnen Tür oder ihrer Gruppe mit den Zutrittsrechten für den Ausweisinhaber ab.
Die Zutrittsrechte auf dem Ausweis müssen laufend über Spezialleser mit Schreibfunktion aktualisiert werden [**3**].
Wenn ein Notzutritt erforderlich wird, z. B. wenn die Elektronik versagt, haben die Terminals auch mechanische Zylinderschlösser.

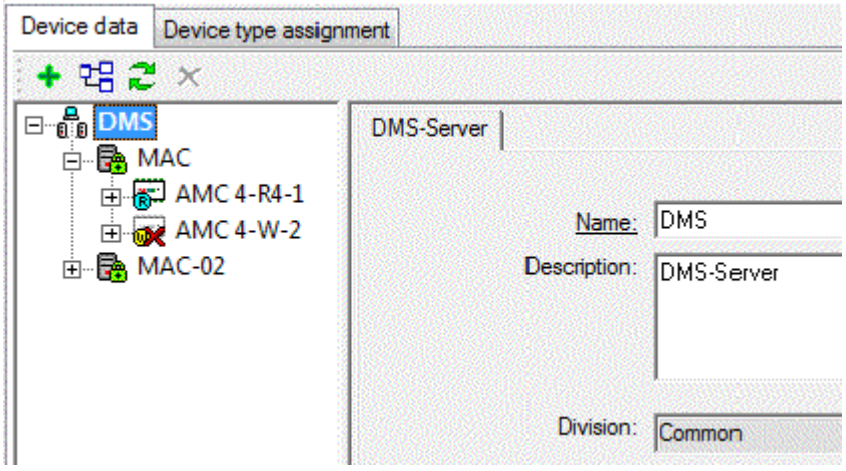
4 Offline Türen – Geräteeditor

Leser mit Schreibfunktion werden für das Offline-System verwendet, um Berechtigungen auf den Ausweis zu laden. Sie können auch parallel als Zutrittskontrollleser verwendet werden.

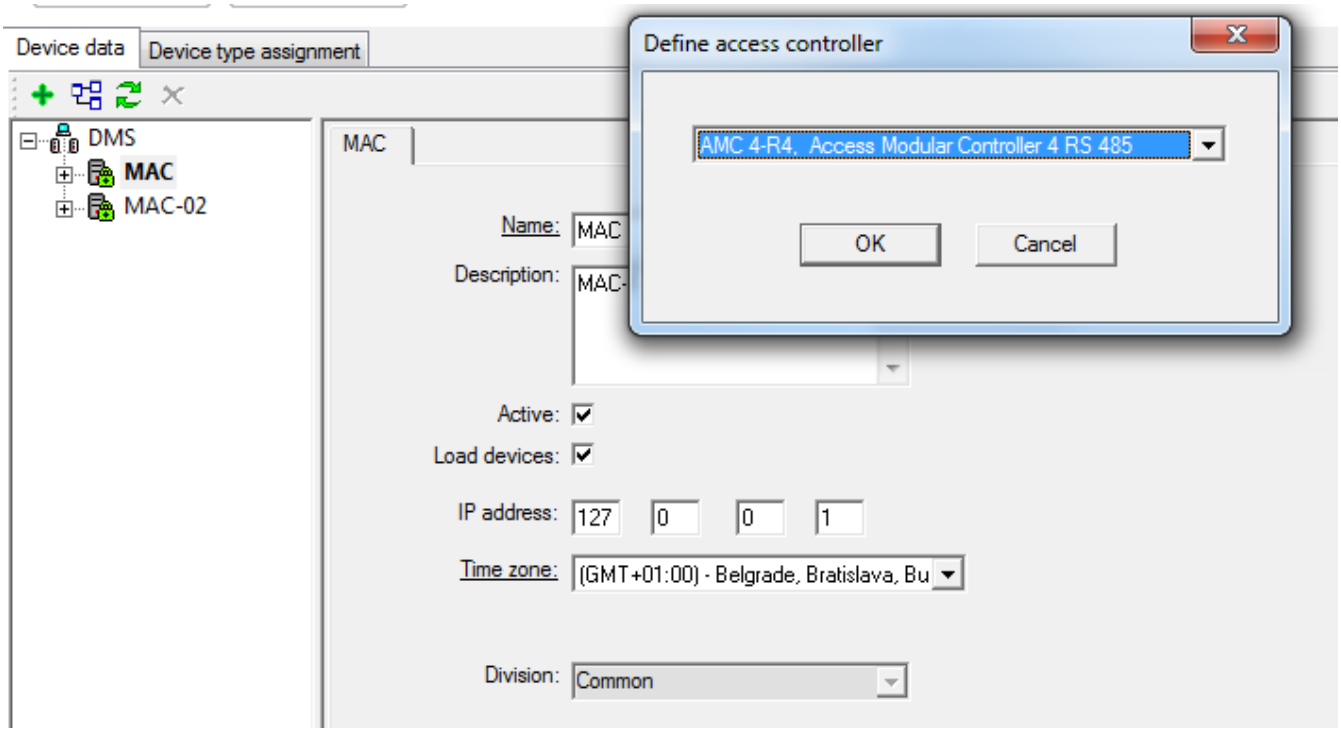
4.1 Anlage der Hardware Komponenten

Öffnen Sie den Geräteeditor.

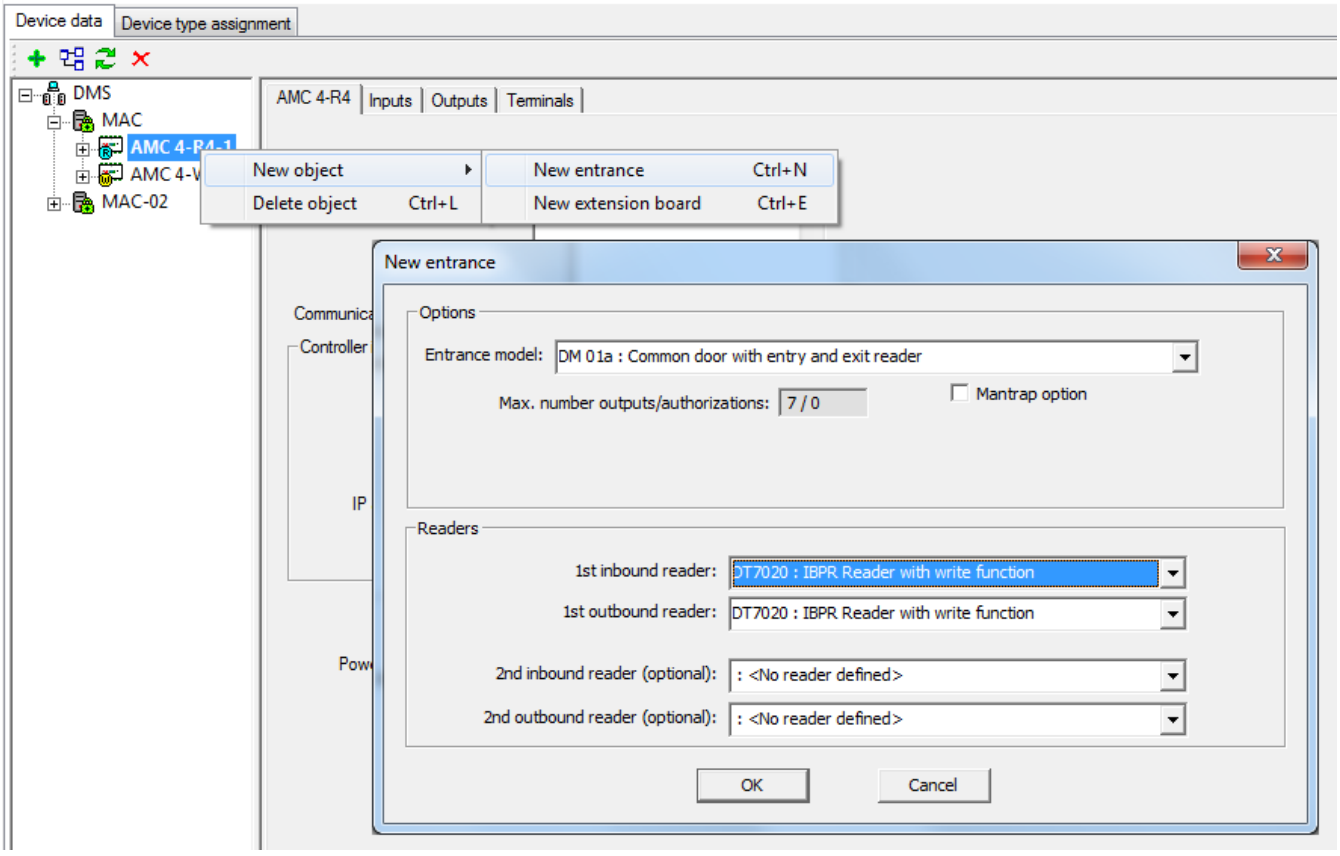
– AMS Dialog Manager (AMS-Dialogmanager) > **Configuration** (Konfiguration) > Device editor (Geräteeditor)



1. Wählen Sie in der Geräteübersicht den Eintrag **MAC** aus.
2. Wählen Sie die Option **New object...** (Neues Objekt) im Kontextmenü aus.
3. Wählen Sie im Auswahldialog für den Controller den Eintrag **AMC2 4-R4** aus.



4. Wählen Sie die Option **New object... >** (Neues Objekt) aus dem Kontextmenü für den neuen Controller.
5. Wählen Sie das gewünschte Türmodell aus der Auswahlliste aus.
6. Wählen Sie den Eintrag **DELTA 7020** für mindestens einen Leser aus.



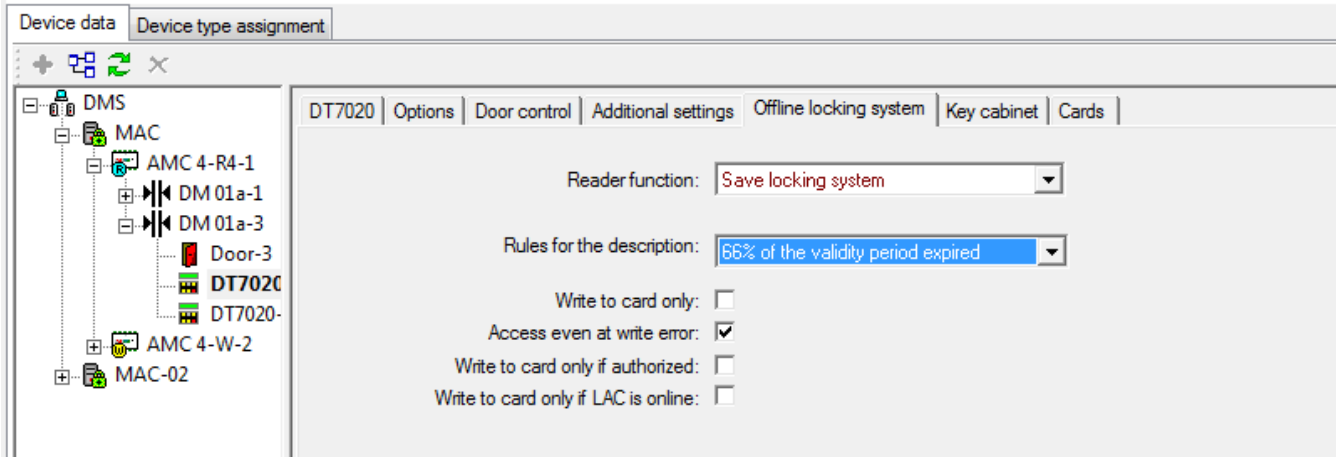
Die folgenden Leser können als Lese-/Schreibeinheiten für PegaSys Berechtigungen verwendet werden:

- **DELTA 1000** (mit spezieller Firmware)
- **DELTA 1010** (mit spezieller Firmware)

4.2 Konfiguration der Lese-/Schreibeinheit

Wenn dieser Leser auch als Zutrittskontrollleser verwendet wird, können Sie ihn entsprechend konfigurieren. Weitere Informationen über die relevanten Parameter finden Sie in der Online-Hilfe zum Online-Zutrittskontrollsystem.

Parameter für **erweiterte Leserfunktionen**, die zum Konfigurieren der Einstellungen für das Schließsystem konfiguriert werden können, wurden auf der Registerkarte **Offline Locking System settings** (Einstellungen für Offline-Schließsystem) zusammengefasst.



Reader function (Leser-Funktion)

Read only (Nur Lesezugriff) (= Standardeinstellung)
Dieser Leser ist ein reiner Zutrittskontrollleser und nicht Teil des Schließsystems.
Alle anderen Parameter in diesem Bereich sind deaktiviert.

Read/Write (Lesen/Schreiben)
Dieser Leser hat Zutrittskontrollfunktionen und ist auch für das Schließsystem aktiviert.
Aktivierung der folgenden Funktionen:

Die Dropdown-Liste ist nur aktiviert, wenn es sich bei dem ausgewählten Lesertyp um DELTA 7020 handelt.
Die Einstellung **Read only** (Nur Lesezugriff) verhindert, dass Leser zu bestimmten Zeiten die Schreibfunktion verwenden. Dies kann zum Beispiel der Fall sein, wenn Offline-Systemkomponenten nicht verfügbar sind oder (wenn mehrere schreibfähige Leser vorhanden sind) nur ein paar ausgewählte schreibfähig sein sollen, wie während der Spitzenzeiten der Verwendung.

Write to card only (Nur auf Ausweis schreiben)

Die Zutrittskontrolle und die Türkontrollfunktionen für das Online-System sind deaktiviert.

Deactivated (Deaktiviert) (Kontrollkästchen ist deaktiviert (Standardeinstellung)): Die normalen Zutrittskontrollprüfungen werden nach dem Schreiben von Daten auf den Ausweis durchgeführt.

Activated (Aktiviert) (Kontrollkästchen ist aktiviert): Nach dem Schreiben von Daten auf den Ausweis wird keine Zutrittskontrolle durchgeführt.

Dieses Kontrollkästchen sollte aktiviert sein, wenn der Leser nur als Lese-/Schreibeinheit für das Offline-System verwendet wird. Andernfalls würden die zusätzlichen Verbindungen unnötige Verzögerungen verursachen.

Access even at write error (Zutritt auch bei Schreibfehler)
Die Zutrittskontrolle (im Online-System) hängt nicht vom Erfolg des Schreibprozesses (im Offline-System) ab.
Die Zutrittskontrolle wird auch nach nicht erfolgreichen Schreibversuchen durchgeführt.
Deaktiviert (Kontrollkästchen ist deaktiviert): Wenn es nicht möglich ist, auf den Ausweis zu schreiben, wird der Zutritt ebenfalls verweigert.
Aktiviert (Kontrollkästchen ist aktiviert (Standardeinstellung)): Der Schreibprozess hat keinen Einfluss auf die Zutrittskontrolle.

Write to card only if authorized (Nur bei Autorisierung auf Ausweis schreiben)
Rechte für das Schließsystem werden nur auf den Ausweis geschrieben, wenn der Ausweisinhaber die (Online-)Zutrittsberechtigung für den Durchtritt hat.
Deaktiviert (Kontrollkästchen ist deaktiviert (Standardeinstellung)): Daten werden immer auf den Ausweis geschrieben.
Aktiviert (Kontrollkästchen ist aktiviert): Daten werden nur auf den Ausweis geschrieben, wenn eine gültige Berechtigung vorliegt.

Bei Aktivierung des Kontrollkästchens wird der Schreibprozess verhindert, selbst wenn Berechtigungen nur vorübergehend aufgehoben sind (zum Beispiel durch ein Zeitmodell).

Only write if LAC online (Nur schreiben, wenn LAC online ist)
Die Rechte werden nur auf den Ausweis geschrieben oder aktualisiert, wenn gewährleistet ist, dass die lokale Zutrittssteuerung (Local Access Controller, LAC) die neuesten Daten aus dem Zutrittskontrollsystem hat. Aus Sicherheitsgründen werden alle fälligen Löschvorgänge immer durchgeführt.
Deaktiviert (Kontrollkästchen ist deaktiviert (Standardeinstellung)): Daten werden immer auf den Ausweis geschrieben.
Aktiviert (Kontrollkästchen ist aktiviert): Daten werden nur geschrieben, wenn eine Verbindung zwischen dem Controller und dem MAC vorliegt.

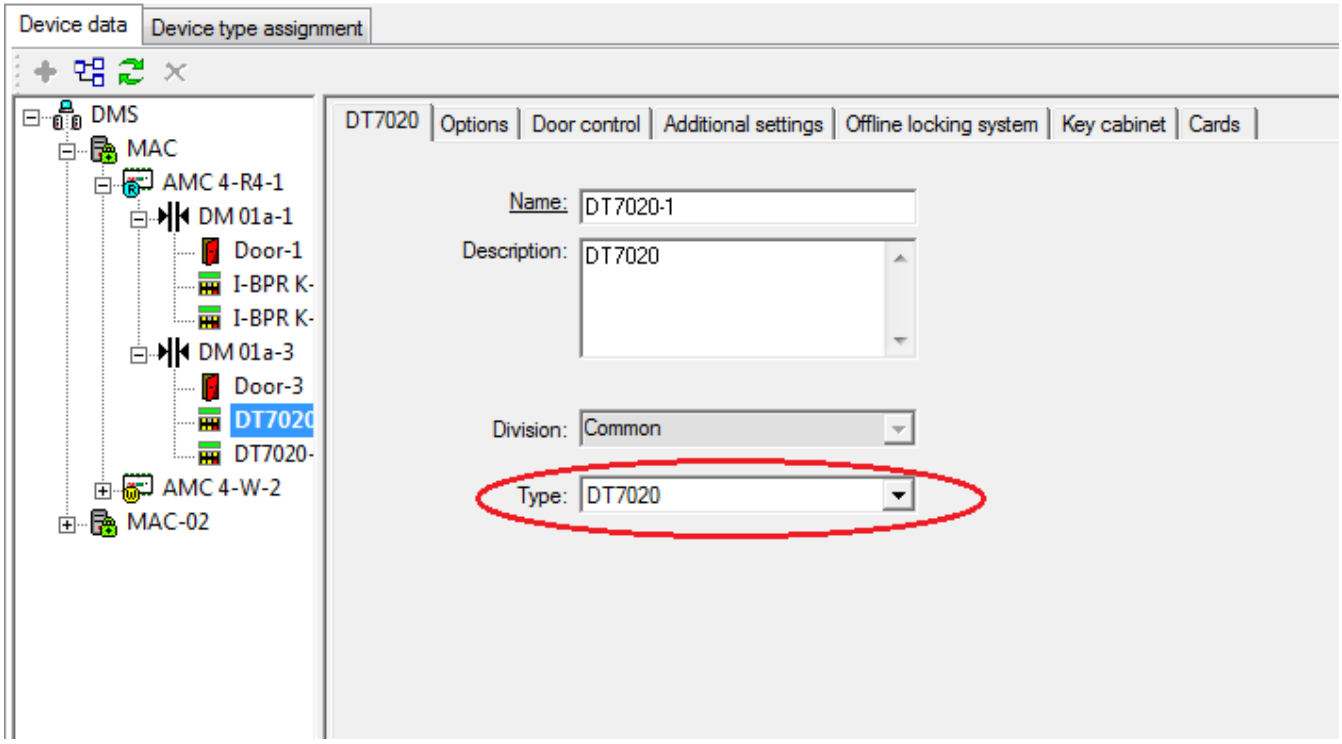
Wenn dieses Kontrollkästchen aktiviert ist und das Kontrollkästchen **Access even on write error** (Zutritt auch bei Schreibfehler) nicht aktiviert ist, verweigert das Online-System den Zutritt, wenn der LAC/MAC-Link nicht funktioniert und die Offline-Daten des Ausweises nicht aktuell sind.

Rule for writing (Schreibregel) Laut Standardeinstellung wird die Gültigkeit verlängert, wenn zwei Drittel (66 %) der für die Person festgelegten Gültigkeitsdauer abgelaufen ist. Siehe auch *Beispiel zur Standardbeschreibungsregel, Seite 62*.
Dieser Parameter kann zum Verlängern der Gültigkeitsdauer von individuell festgelegten Daten verwendet werden.
Mögliche Werte:
Spezifikation für Schließsystem
Immer schreiben
[wenn ... der Gültigkeitsdauer abgelaufen ist:]
16 %, 33 %, 50 %, 66 %, 83 %, 100 %

Spezifikation für Schließsystem – siehe *Standardgültigkeit, Seite 23*.

4.2.1 Tausch des Lesertyps

In der Regel werden Leser mit Schreibfunktionen an wichtigen Durchtritten installiert (z. B. als Eintrittsleser beim Hauptdurchtritt), damit die Zutrittsrechte für das Schließsystem der Mitarbeiter, die am Morgen den Standort betreten, automatisch aktualisiert werden.
Bei einer Installation mit PegaSys muss mindestens ein Leser in der Anlage durch einen schreibfähigen Leser ersetzt werden. Der Geräteeditor lässt keine spätere Änderung von Türmodellen und deren Lesern zu.
Wir bleiben beim Beispiel des Eingangslesers am Haupteingang: Der bestehende Durchtritt muss gelöscht und ein DELTA 7020 Leser an seiner Stelle hinzugefügt werden.
Wenn ein bestehender Durchtritt gelöscht wird, wird er auch aus allen Zutrittsberechtigungen entfernt. Es müssten deshalb alle Berechtigungen dem neuen Durchtritt hinzugefügt werden.
Um diesen mühsamen und fehleranfälligen Prozess zu vermeiden, wurde die Dropdown-Liste **Type** (Typ) der ersten Seite der Leserkonfiguration hinzugefügt.



Diese Dropdown-Liste ist für alle Leser eingerichtet, sodass Ersetzungen konfiguriert werden können, indem der Typ **DELTA 7020** ausgewählt und zugewiesen wird, ohne dass vorhandene Einträge gelöscht werden müssen.

4.3 Dialog Lese-/Schreibeinheit

In ein Online-System kann eine Ausweisnummer auch zentral eingegeben werden. Im Gegensatz dazu können Offline-Daten nur von peripheren Lese-/Schreibeinheiten auf einen Ausweis übertragen oder von einem Ausweis gelesen werden. Diese Lese-/Schreibeinheiten können entweder Dialogleser sein, die direkt mit der Dialogstation verbunden sind, oder Zutrittskontrollleser (beispielsweise DELTA 1000 oder DELTA 1010).
Der Dialogleser zum Schreiben und Lesen von System- und Benutzerausweisen aus dem Offline-System sowie zum Aufzeichnen von Ausweisdaten für das Online-System wird mithilfe des Online-Systems installiert.

- AMS-Hauptmenü > **Configuration** > **Options** > **Card reader** (Konfiguration > Optionen > Ausweisleser)
- Wählen Sie die relevante Dialogstation im Feld „Workstations“ (Dialogstation) aus.
- Wählen Sie in der Dropdown-Liste **Type** (Typ) den PegaSys Leser, der dem verwendeten Ausweistyp entspricht.

Name des Lesers	Lesertyp	Codierung
PegaSys-MF-BC-USB	MIFARE classic	Bosch Code
PegaSys-MF-SN-USB	MIFARE classic	Seriennummer
PegaSys-MFDESFire-BC-USB	MIFARE DESFire EV1	Bosch Code
PegaSys-HITAG-BC-USB	HITAG 1	Bosch Code

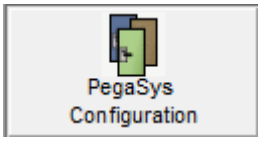
Name des Lesers	Lesertyp	Codierung
PegaSys-HITAG-SN-USB	HITAG 1	Serial number (Seriennummer)
PegaSys-Legic-BC-USB	LEGIC Prime	Bosch Code
PegaSys-Legic-SN-USB	LEGIC Prime	Serial number (Seriennummer)
PegaSys-LegicAdvant-BC-USB	LEGIC Advant	Bosch Code

Starten Sie das Zutrittskontrollsystem neu, um den ausgewählten Leser in den Dialogfelder zu den Personendaten des Zutrittskontrollsystems verfügbar zu machen.

5 Offline Türen – Dialog Configuration (Konfiguration)

5.1 Erste Schritte

Nachdem die PegaSys Komponente installiert wurde, befindet sich der Konfigurationsdialog für die Komponente im Menü **System data** (Systemdaten) des Dialog-Managers für das Zutrittskontrollsystem. Er kann durch Klicken auf die



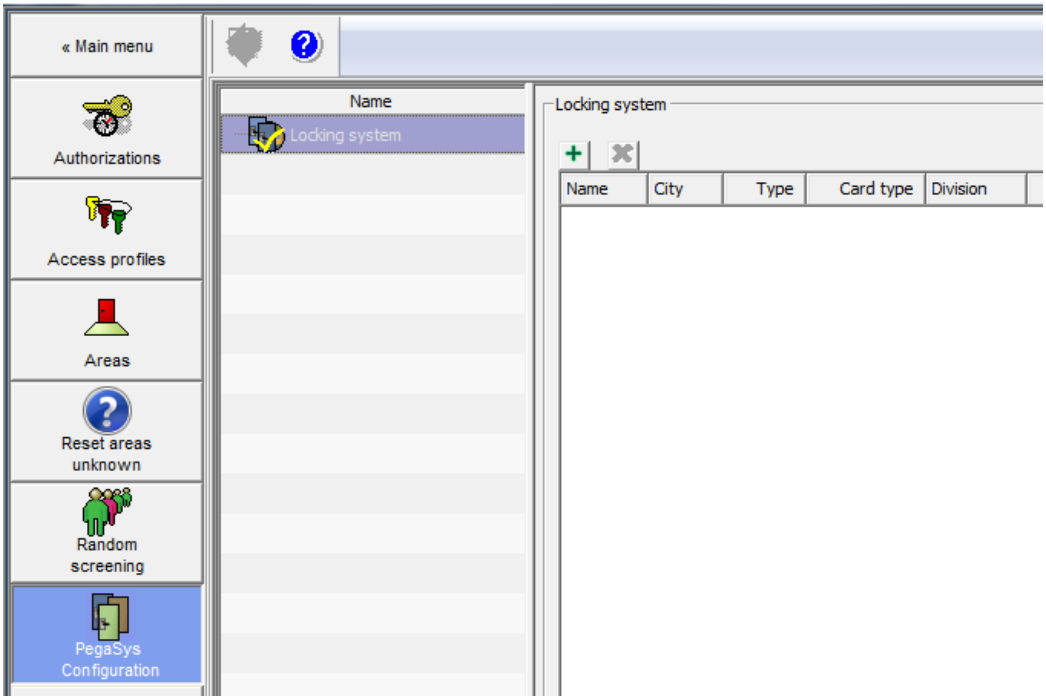
Schaltfläche geöffnet werden.

5.2 Schließanlagen

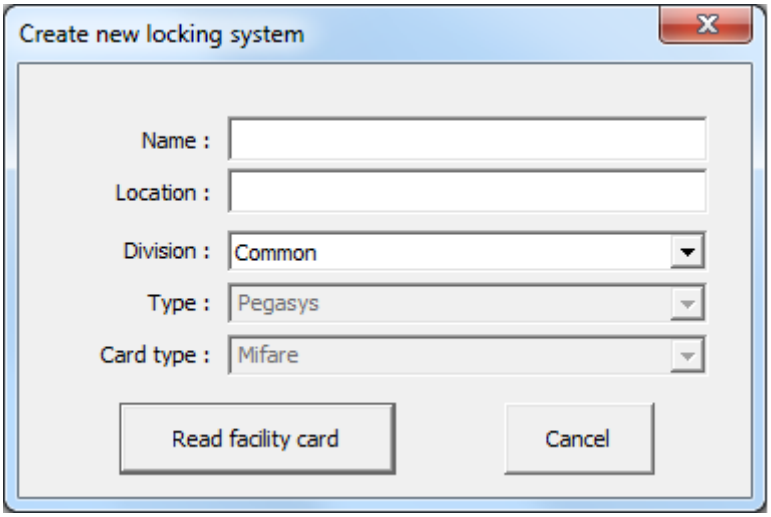
Während der Installation wird der Knoten **Locking systems** (Schließsysteme) als Basiseintrag im Explorer-Baum (linker Dialogbereich) hinzugefügt. Autonome Systeme, die unabhängig voneinander arbeiten, können jetzt unter diesem Eintrag eingerichtet werden.

Einrichten von Systemen

– Wählen Sie den Basiseintrag **Locking systems** (Schließsysteme).
Bereits eingerichtete Systeme werden in einer Liste auf der rechten Seite angezeigt.

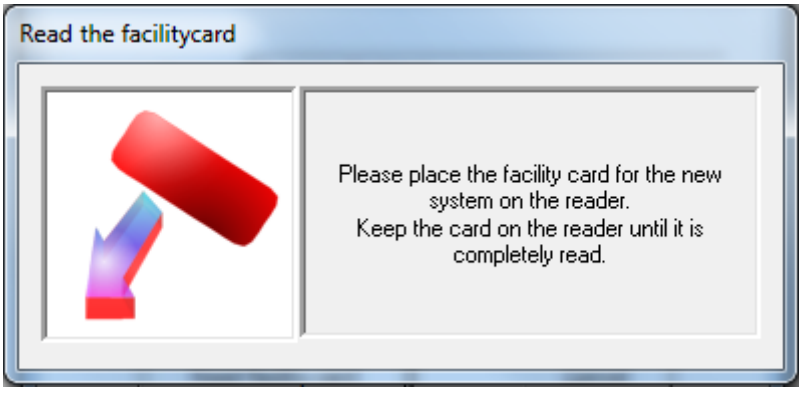


– Klicken Sie auf die Schaltfläche  (über dem Listenfeld), um zusätzliche Systeme einzurichten.



Name	Geben Sie dem System einen eindeutigen Namen. Diese Information wird auch in dem Dialog „access rights“ (Zutrittsrechte) angezeigt.
Location (Standort)	Diese Information wird in dem Dialog „access rights“ (Zutrittsrechte) angezeigt.
Division (Mandant)	Wenn Sie Mandanten eingerichtet haben, können Sie die einzelnen Systeme auch einem dieser Mandanten zuweisen.
Typ	„PegaSys“ – ist zurzeit das einzige unterstützte Offline-Schließsystem.
Card type (Ausweisart)	Anzeigefeld (HITAG1, MIFARE classic, LEGIC prime und LEGIC advant): wird vom verbundenen Lese-/Schreibgerät informiert.

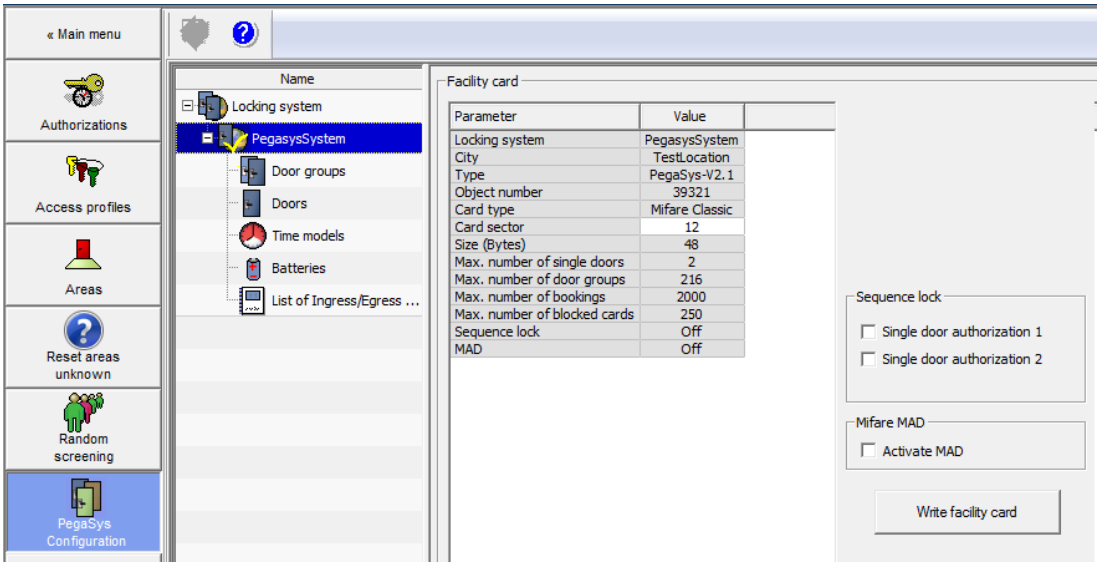
– Legen Sie den Kundenausweis für dieses System auf die Lese-/Schreibeinheit, und klicken Sie auf **Read facility card** (Kundenausweis lesen).



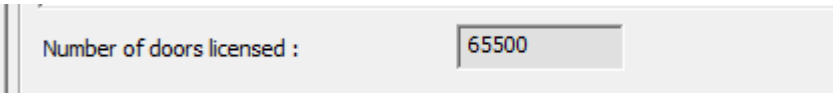
Nach dem Lesen des Kundenausweises besteht die Option, eine Arbeitskopie zu erstellen. Diese Option sollte zumindest einmal für jede Ausweiskarte angenommen werden, damit das Original vor versehentlichem Überschreiben oder Verlust geschützt wird.

Hinweis!
Automatische Datenkorrektur und ihre Auswirkungen
Wenn für die Datensatzgröße ungeeignete Daten dem Ausweis hinzugefügt werden, wird nach dem Lesen des Kundenausweises eine Meldung angezeigt, dass die Daten automatisch korrigiert wurden.
In diesem Fall muss ein neuer Kundenausweis geschrieben werden, mit dem die Türterminals neu initialisiert werden müssen.

Klicken Sie auf **Yes** (Ja), um zu bestätigen, dass ein neuer Kundenausweis geschrieben werden soll.
Es werden ein Listeneintrag und ein weiterer Explorer-Eintrag mit dem angegebenen Namen erzeugt. Je nach Version des gelesenen Kundenausweises enthält der Explorer-Eintrag eine unterschiedliche Anzahl von Untereinträgen, die zum Konfigurieren des Systems erforderlich sind. Siehe auch *Schließanlagen konfigurieren, Seite 21*.

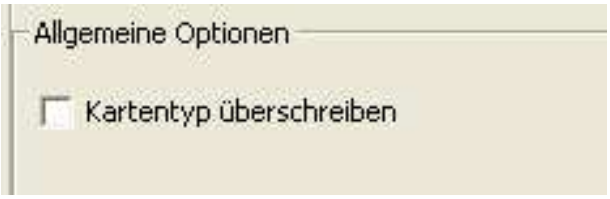


Hinweis!
Listeneinträge mit einem weißen Hintergrund können jederzeit geändert werden. Als zusätzlicher Indikator ändert sich der Mauszeiger beim Bewegen über diese Felder: 
Der Schreibmodus wird durch Doppelklicken auf das entsprechende Listenfeld aktiviert. Drücken Sie die Eingabetaste, um das Feld nach dem Vornehmen der Änderungen zu verlassen.

Die **Anzahl** von **lizenzierten** Türterminals wird unter dem Listenfeld für die einzelnen Systeme angezeigt. 

Dieser Wert ist die Höchstgrenze für alle Schließsysteme. Die Basisversion von PegaSys enthält 25 Türlizenzen mit der Software. Die Anzahl der Lizenzen kann auf ein Vielfaches von 25 angehoben werden.

Überschreiben der Ausweisart



Beim Überschreiben von Systemausweisen wird einmal für jeden Systemausweistyp eine Bestätigungsaufforderung angezeigt. Danach wird der Ausweis ohne weitere Warnungen überschrieben.

Löschen von Systemen

Ausgewählte Listeneinträge können mit der Schaltfläche wieder entfernt werden. Klicken Sie auf **Yes** (Ja), um zu bestätigen, dass Sie das System löschen möchten.

5.3 Schließanlagen konfigurieren

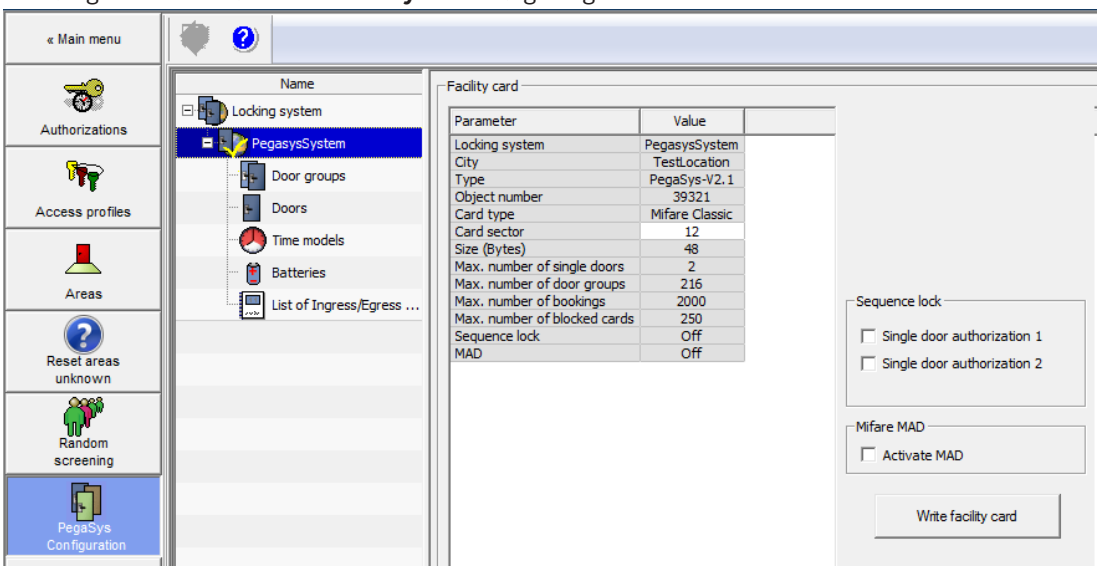
Die Konfiguration einer Anlage erfolgt in vier Schritten, die über die entsprechende Explorerknoten aufgerufen werden können. Jeder Knoten wird mit einem speziellen Icon gekennzeichnet - selektierte Einträge erhalten zusätzlich einen gelben Haken.

Explorereintrag	Icon	Wenn selektiert
<Name der Anlage>		
Türgruppen		
Türen		
Zeitmodelle		

Welche Einstellungen wo und wie vorgenommen werden, wird in den folgenden Abschnitten beschrieben.

5.3.1 Systeme (PegasysSystem)

Im Listenfenster werden zu diesem Eintrag die bei der Anlage angegebenen Parameter sowie die ausgelesenen Daten der **Facility Karte** angezeigt.



Schließanlage Bezeichnung der Anlage, wie sie bei der Einrichtung angegeben wurde.

Ort Bezeichnung des Ortes, wie sie bei der Einrichtung angegeben wurde.

Art PegaSys-<Versions-Nr.>

Objekt-Nummer Kundenspezifische Kennung

Kartentyp Angabe des Lese- und Codierverfahrens:
- Hitag1
- MIFARE Classic
- MIFARE DESFire EV1
- Legic Prime
- Legic Advant

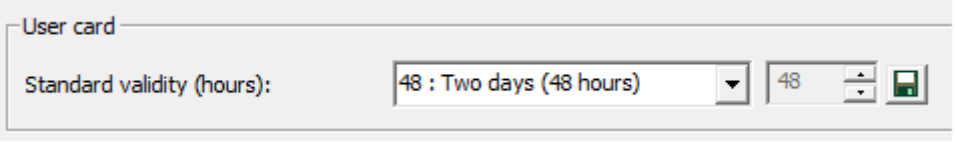
Kartensektor Bereich auf der Karte, der als Startpunkt für die Kodierung der PegaSys Berechtigungen verwendet wird.

Datengröße (Bytes) Anzahl Bytes, die zur Speicherung der Berechtigungen benötigt werden.
48 = Standard - je nach Größe der Anlage muss die Datensatzlänge angepasst werden - vgl. dazu die Tabelle im *Mögliche Datenstrukturen, Seite 39*.

Achtung:
Bei der Verwendung von Hitag1 sollten diese Werte bei der Ersteinrichtung einer Anlage überprüft werden, da dieser Kartentyp nicht über eine Schutzfunktion vor unbeabsichtigtes Überschreiben bereits benutzter Bereiche verfügt.

max. Anzahl Einzeltüren **max. Anzahl Türgruppen** **max. Anzahl Buchungen**	Höchstgrenzen für die jeweilige Anlage, die sich aus dem Kartentyp und der Datengröße ergeben.
max. Anzahl Sperrkarten	**Anmerkung:** Sperrkarten = Transportkarten, mit denen gesperrte Ausweise in die Terminals übertragen werden.

Standardgültigkeit
Darüber hinaus kann eine Zeit für die **Standard validity** (Standardgültigkeit) für **User cards** (Benutzerausweise) hier festgelegt werden. Diese wird im Dialog **Cards** (Ausweise) im Zutrittskontrollsystem beim Zuweisen von PegaSys Berechtigungen als Standard verwendet.



Die Dropdown-Liste enthält eine Anzahl vordefinierter Zeiträume sowie die Option zum Auswählen einer bestimmten Anzahl von Stunden.

One day (24 hours) (Ein Tag (24 Stunden)) Two days (48 hours) (Zwei Tage (48 Stunden)) One week (7 days) (Eine Woche (7 Tage)) One month (30 days) (Ein Monat (30 Tage)) One year (365 days) (Ein Jahr (365 Tage))	= Standardeinstellung Feste Zeiträume, die vom Zeitpunkt der Codierung des Ausweises oder der Verlängerung der Rechte gezählt werden.
Max. Ausweisgültigkeit	Die im Dialogsystem definierte Gültigkeit ... – **Valid until** (Gültig bis) – Datum (im Online-Berechtigungsdialog) – **Valid until** (Gültig bis) – Datum (im Offline-Berechtigungsdialog) – Blockieren – Löschvorgang

Benutzereinstellung	Frei definierter Zeitraum – in Stunden [1 bis 17520 (zwei Jahre)]. Das Eingabefeld zum Eingeben der Stunden wird aktiviert, wenn diese Option ausgewählt ist.

Klicken Sie auf die Schaltfläche  , um Änderungen an der Gültigkeitsdauer von Benutzerausweisen zu speichern.
Wenn der Defaultwert geändert wird, erhalten alle Personen, denen die Standardgültigkeitsdauer zugewiesen war, beim nächsten Aktualisieren der Ausweise neue Werte.

Hinweis!
Jeder Ausweis hat nur eine Gültigkeitsdauer
Jeder Offline-Sperrausweis hat nur eine Gültigkeitsdauer. Es ist nicht möglich, verschiedenen Türterminals auf demselben Ausweis unterschiedliche Gültigkeitsdauern zuzuweisen.

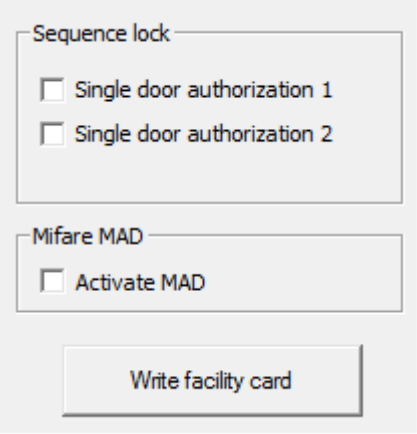
Erweiterte Funktionen

- **Benutzerausweis überprüfen**
  Wenn der Kundenausweis gelesen wird, werden das Ausweissegment und der Zutrittscode für Offline-Berechtigungen für die Benutzerausweise definiert. Zur Überprüfung, ob die Einstellungen korrekt sind, können die aktuellen Einstellungen auf einen Benutzerausweis geschrieben werden, indem Sie auf diese Schaltfläche klicken. Ein gültiger, aber abgelaufener Benutzerausweis wird ohne Berechtigungen erstellt. Wenn diese Funktion fehlschlägt, kann das System mit diesen Benutzerausweisen und diesem Kundenausweis nicht in Betrieb genommen werden.
  Für jede Ausweistechnologie gelten unterschiedliche Voraussetzungen:
  - **HITAG 1**
    Der voreingestellte Startsektor auf diesen Ausweisen könnte gesperrt sein. Beim Startsektor handelt es sich um einen Kundenausweisparameter, der in diesem Dialog angepasst werden kann.
  - **MIFARE Classic**
    Der voreingestellte Startsektor auf diesen Ausweisen ist möglicherweise bereits mit einem anderen Code als dem auf dem Kundenausweis codiert. Falls der Startsektor nicht richtig eingegeben wurde, kann er wie mit HITAG1 geändert werden.
    In MIFARE Classic kann der Startsektor einer Anwendung (wie PegaSys) auch über MAD (MIFARE Application Directory) des Benutzerausweises definiert werden. Bei aktiviertem MAD muss der Zutrittscode zum Sektor mit MAD bekannt sein. Siehe auch *Konfigurieren von MAD (nur für MIFARE Classic), Seite 25*.
  - **LEGIC prime/advant**
    Bei LEGIC wird davon ausgegangen, dass die Benutzerausweise vorformatiert sind und das erforderliche Segment bereits auf dem Benutzerausweis vorhanden ist. Das erforderliche Segment wird im LEGIC-Segmentparameter angezeigt. Alle Leser (online und offline) müssen eine Berechtigung für den Zutritt in das voreingestellte Segment besitzen. Diese Berechtigung wurde möglicherweise bereits in den Lesern im Werk programmiert oder zu einem späteren Zeitpunkt über sogenannte

Initialisierungsausweise (= SAM 63) festgelegt. Wenn das System neu erstellt wird und neue Benutzerausweise bestellt werden, kann das sogenannte PegaSys Segment direkt vom Ausweishersteller installiert werden.
Wenn das Segment auf dem Benutzerausweis beim Codieren der Benutzerausweise von den Dialogen (Offline-Konfigurator- und Ausweis-Dialoge) fehlt, wird automatisch gefragt, ob das Segment erstellt werden soll. Unter den folgenden Voraussetzungen kann das erforderliche Segment erstellt werden und es können Daten darauf geschrieben werden: Die Lese-/Schreib-Dialoggeräte besitzen die erforderliche Berechtigung (voreingestellt über XAM Ausweis) oder der Kunde besitzt einen IAM LEGIC Ausweis mit Berechtigung für nur dieses voreingestellte PegaSys Segment.
Das Offline-Segment wird nur einmal erstellt. Dann sollte es möglich sein, von allen Terminals – online und offline – Daten von dem Benutzerausweis zu lesen und darauf zu schreiben.
Von der Software wird nicht überprüft, ob sich die Daten bereits auf dem Benutzerausweis befinden. Wenn die Ausweistechnologie die Daten nicht schützt, können sie überschrieben werden.

– **Erstellen eines Demontageausweises**
  Der Demontageausweis kann von einem beliebigen Systemausweis erstellt werden (abgesehen vom Kundenausweis). Zylinder, die zu diesem Offline-System gehören, können mithilfe dieses Ausweises demontiert werden. Die Systemzugehörigkeit wird über die Kundenausweise auf die Offline-Terminals übertragen.

Schreiben von Kundenausweisen



Wenn ein Kundenausweisparameter, die Sequenzsperre oder die MIFARE MAD-Einstellungen geändert werden, muss der Kundenausweis durch Klicken auf die Schaltfläche **Write facility card** (Kundenausweis schreiben) aktualisiert werden. Das Online-System verwendet die neuen Einstellungen direkt. Lassen Sie die Kontrollkästchen für die Sequenzsperre leer (d. h. deaktivieren Sie die Sequenzsperre), es sei denn, die Verwendung dieser PegaSys Funktion wurde im Voraus sorgfältig vorbereitet.

Hinweis!
Wenn Sie Daten auf dem Kundenausweis ändern, müssen Sie sicherstellen, dass auch alle Türterminals aktualisiert werden.

Konfigurieren von MAD (nur für MIFARE Classic)

Wenn MAD aktiviert ist, können die A- und B-Zutrittscodes im MAD-Bereich der Benutzerausweise konfiguriert werden. A0 bis A5 und B0 bis B5 sind Standardcodes und daher allen Unternehmen bekannt (d. h. der Zutritt ist für alle Benutzer aktiviert). Nur der A-Code wird über den Kundenausweis an die Offline-Terminals übertragen, da die Terminals nur lesen und keine Daten in MAD schreiben müssen, wenn es aktiviert ist. Das Online-System verwendet den B-Code, um MAD für das Offline-System auf die Benutzerausweise zu schreiben.

Hinweis!
MAD kann nicht für Mifare DESFire EV1 konfiguriert werden.

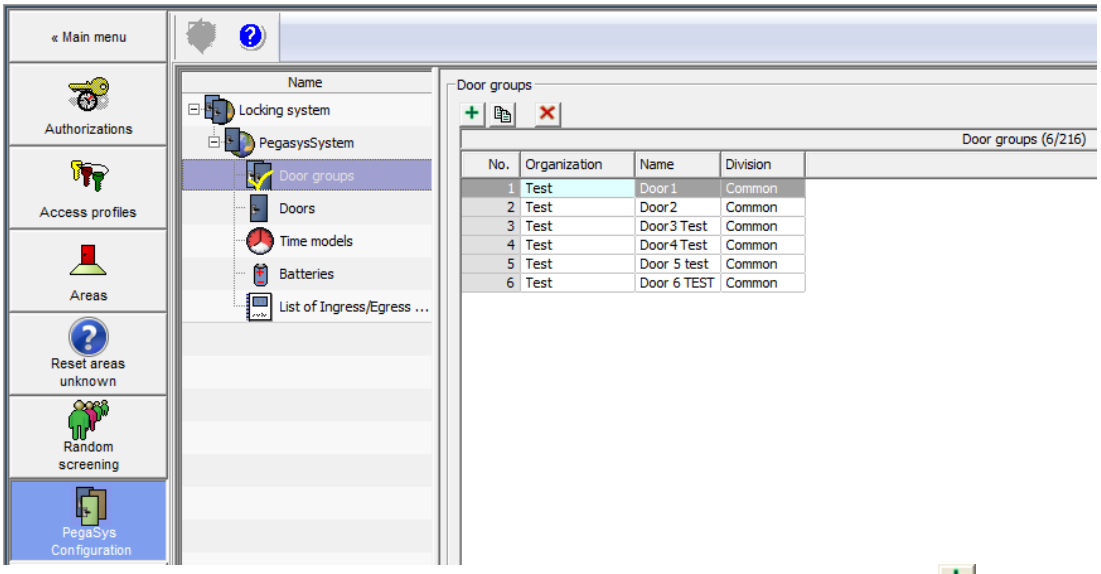
Siehe
– *Spezielle Einstellungen, Seite 59*

5.3.2 Türgruppen

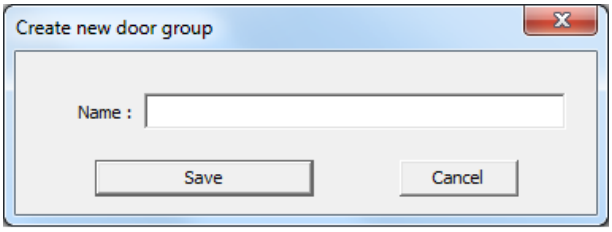
Die Ausweissegmentierung erlaubt nur eine verhältnismäßig geringe Zuweisung von Einzeltüren im Vergleich zu Türgruppen. Da Einzeltüren-Berechtigungen aber nur für spezielle Gegebenheiten eingesetzt werden und die Zuweisung der Berechtigungen für bestimmte Türen in der Regel über die Zusammenfassung mehrerer Türen in Türgruppen erfolgt, reicht die Anzahl der Einzeltüren-Berechtigungen aus.

Erstellen von Türgruppen

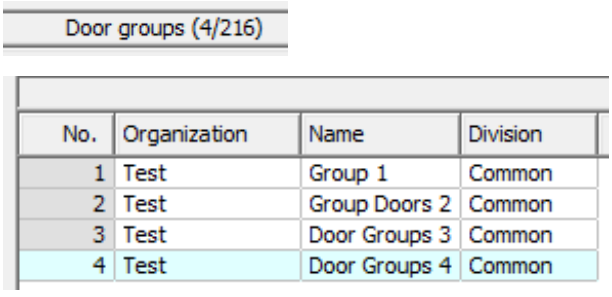
Die erforderlichen Türgruppen werden als Datensätze im Listenfeld erstellt, ohne dass eine Verbindung zu einzelnen Türen zunächst hergestellt wird.



Der Dialog zum Erstellen der Türgruppen wird durch Klicken auf die Schaltfläche + geöffnet.



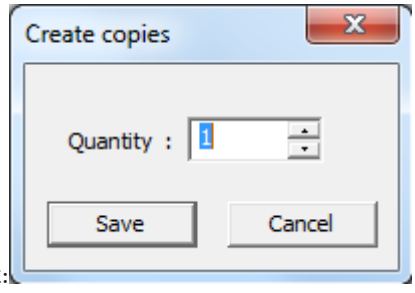
Durch das Angeben einer Bezeichnung (**Name**) für die Türgruppe und durch Klicken auf die Schaltfläche **Erstellen** wird ein weiterer Listeneintrag mit einer eigenen ID-Nummer erstellt. Der Mandant, der beim Einrichten des Systems (*Schließanlagen, Seite 18*) konfiguriert wurde, wird in der Spalte **Mandant** angezeigt. Er kann für jede Türgruppe einzeln zurückgesetzt werden, wodurch diese Türgruppen (als Berechtigungen) nur innerhalb ihrer eigenen Mandanten angezeigt werden.
Eine begrenzte Anzahl von Türgruppen kann abhängig von der Datengröße und dem Ausweistyp erstellt werden – siehe auch die Tabelle in *Mögliche Datenstrukturen, Seite 39*. Mit der Standardgröße von 48 Byte und HITAG1-Ausweisen beträgt die Obergrenze für Türgruppen 240 (für LEGIC und MIFARE liegt sie bei 256). Die Anzahl der bereits erstellten Türgruppen sowie die maximale Anzahl werden im Listenkopf angezeigt:



Kopieren von Türgruppen

Vorhandene Listeneinträge können kopiert werden, um die Dateneingabe zu erleichtern.

1. Wählen Sie einen Listeneintrag aus.
2. Klicken Sie auf die Schaltfläche über dem Listenfeld. Das folgende Dialogfenster wird geöffnet:



3. Geben Sie die Anzahl der Kopien ein, die Sie erstellen möchten.
4. Klicken Sie auf die Schaltfläche **Save** (Speichern), um die Listeneinträge zu erstellen.

Um sicherzustellen, dass die Bezeichnung eindeutig ist, werden den Einträgen die Bezeichnung des ausgewählten Eintrags und eine fortlaufende Nummer (z. B. die **Türgruppe n**) zugewiesen.
Die Bezeichnungen für die Türgruppen können jederzeit durch Doppelklicken auf die entsprechende Zeile in der Spalte **Name** geändert werden. Die fortlaufende Nummer kann nicht geändert werden.

Die Anzahl der Kopien, die erstellt werden können, hängt von der Ausweisgröße ab. Über die Pfeiltasten im Dialog **Kopien erstellen** kann kein Wert ausgewählt werden, der höher ist als die verbleibende verfügbare Menge. Der Dialog lässt sich nicht mehr öffnen, wenn der maximale Wert erreicht ist.

Löschen von Türgruppen

Türgruppen, die nicht mehr benötigt werden, können in der Liste ausgewählt und durch Klicken auf die Schaltfläche gelöscht werden. An diesem Punkt wird ein Sicherheitshinweis angezeigt, der bestätigt werden muss, um versehentliches Löschen zu verhindern.

Klicken Sie auf **Yes** (Ja), um zu bestätigen, dass Sie die Türgruppe löschen möchten. Türgruppen, denen noch Türen zugewiesen sind, können erst nach dem Abbruch dieser Zuweisungen gelöscht werden.

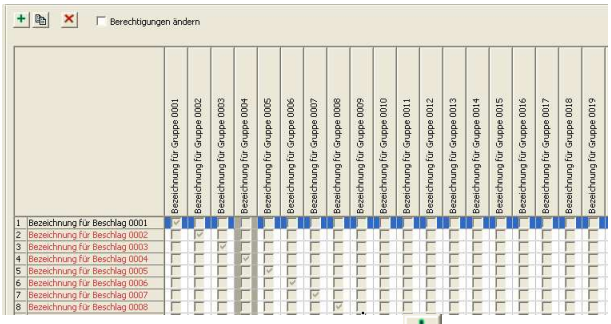
Die Türen werden im nächsten Konfigurationsschritt zugewiesen.

5.3.3 Türen

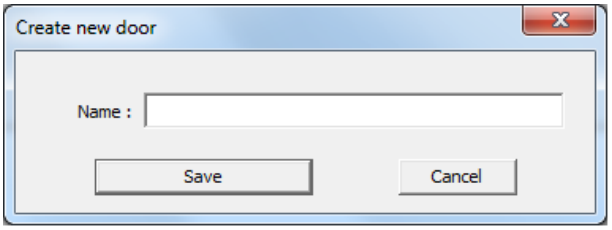
Für jedes Türterminal der Schließanlagen muss in diesem Dialog ein Listeneintrag erstellt und konfiguriert werden. Diese werden dann bestimmten Türgruppen zugewiesen.

Erstellen von Türen

In diesem Listenfeld wird ein Eintrag für jedes Türterminal erstellt.



Durch Klicken auf die Schaltfläche wird der Dialog zum Erstellen der Türen geöffnet.



Wenn eine Bezeichnung für die Tür angegeben ist (**Name**), wird durch Klicken auf die Schaltfläche **Speichern** ein neuer Listeneintrag erzeugt, der anschließend zugewiesen und konfiguriert werden kann.

Verwenden Sie nach Möglichkeit stets aussagekräftige Namen für die Türen.

Zuweisen von Türen

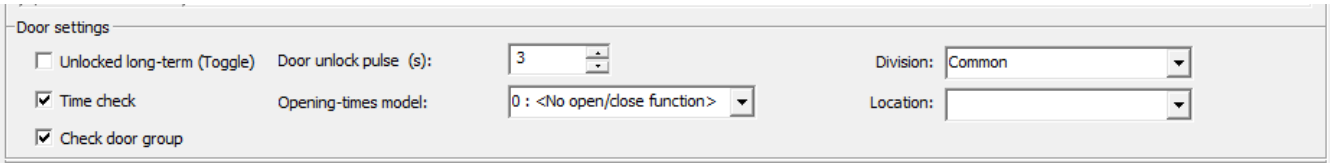
Das Listenfeld des Dialogs enthält eine Spalte für jede erstellte Türgruppe. Aktivieren Sie die entsprechenden Kontrollkästchen, um die Türen den Türgruppen zuzuweisen. Aktivieren Sie zuerst den Bearbeitungsmodus, indem Sie das Kontrollkästchen **Change authorizations** (Berechtigungen ändern) aktivieren.

Die Anzahl der Türgruppen, denen eine Tür zugewiesen werden kann, ist nicht begrenzt.

Rot markierte Türen sind Türen, deren Konfiguration geändert, deren Ausweis aber noch nicht codiert wurde. Die Türbezeichnung wird schwarz, wenn der Ausweis codiert ist.

Konfigurieren von Türen

Die Parameter im Listenfeld werden zur Konfiguration der ausgewählten Tür verwendet.



Unlocked long-term (Toggle) (Dauerhaft geöffnet (umschalten))	Benutzer mit einer Sonderberechtigung können diese Tür auch für einen längeren Zeitraum freigeben – z. B. Büro- oder Ladenöffnungszeiten. Standardeinstellung = nicht ausgewählt.
Time check (Zeitprüfung)	Einstellung, die bestimmt, ob Zeitmodelle und Gültigkeitsdauern überhaupt berücksichtigt werden. Standardeinstellung = Kontrollkästchen aktiviert
Checking door groups (Überprüfen von Türgruppen)	Eine Berechtigung für das Schließsystem kann aus individuellen und/oder Türgruppenberechtigungen bestehen. Wenn dieser Parameter nicht ausgewählt ist, werden nur einzelne Berechtigungen berücksichtigt und überprüft. Standardeinstellung = Kontrollkästchen aktiviert
Door opening time(s) (Türöffnungszeit(en))	Zeit in Sekunden (1–255), die definiert, wie lange der Türöffnungskontakt die Tür zum Öffnen freigeben soll. Standardeinstellung = 3
Opening-hours time model (Öffnungszeiten – Zeitmodell)	Auswahl eines Zeitmodells – die Tür wird automatisch für bestimmte Zeiträume geöffnet, die durch ihre Start- und Endzeiten definiert sind.
Division (Mandant)	Auswahl eines Mandanten, mit dem die Tür verknüpft werden soll. Der Standardmandant ist für das Schließsystem ausgewählt, kann aber für jede einzelne Tür separat geändert werden.

Location (Standort) Die Position der Tür (z. B. Stadt, Gebäude, Korridor usw.). Wenn Zutrittsrechte zugewiesen werden, wird der Standortparameter verwendet, um einzelne Türen zu gruppieren und zu identifizieren.

Kopieren von Türen

Türen können auf gleiche Weise wie Türgruppen kopiert werden. Zur Vereinfachung der Dateneingabe wird zunächst eine einzelne Tür erstellt und konfiguriert und anschließend nach Bedarf kopiert.

- Wählen Sie einen Listeneintrag für den Kopiervorgang.
- Klicken Sie auf die Schaltfläche  über dem Listenfeld. Der Dialog **Kopien erstellen** wird geöffnet:
- Geben Sie die Anzahl der Kopien an, die Sie erstellen möchten, oder wählen Sie sie mithilfe der Pfeiltasten aus.
- Durch Klicken auf die Schaltfläche **Speichern** werden die erforderlichen Listeneinträge erstellt.
  Um sicherzustellen, dass jede Bezeichnung eindeutig ist, werden Kopien mit einem fortlaufend nummerierten Suffix versehen (z. B. **Tür n**).

Die Bezeichnungen für die Türen können jederzeit durch Doppelklicken auf die entsprechende Zeile in der Spalte **Name** geändert werden. Die ID-Nummer in der ersten Spalte (**Nr.**) kann nicht geändert werden.

Die Anzahl der Kopien, die erstellt werden können, ist durch die verfügbaren Lizenzen beschränkt. Über die Pfeiltasten im Dialog **Kopien erstellen** kann kein Wert ausgewählt werden, der höher ist als die verbleibende verfügbare Menge. Der Dialog lässt sich nicht mehr öffnen, wenn der maximale Wert erreicht ist.

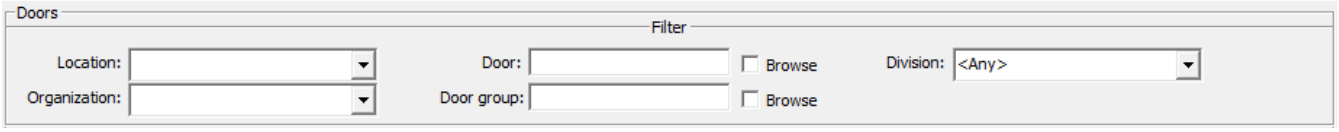
Türen löschen

Markierte Listeneinträge können über die Schaltfläche  wieder entfernt werden. Dazu erscheint eine Sicherheitsabfrage, die bestätigt werden muss, um unbeabsichtigtes Löschen zu vermeiden.

Klicken Sie **Ja** zur Bestätigung, wenn Sie den Listeneintrag löschen wollen.

Filter für Türen

Bei Offline Systemen mit einer großen Anzahl Türen kann die alphabetische Sortierung die Übersichtlichkeit und Arbeit erschweren. Um die Darstellung auf relevante Einträge reduzieren zu können, befinden sich oberhalb des Listenfeldes **Filter**, mit denen die Ansicht in unterschiedlicher Weise angepasst werden kann.



Ort Filtert nach allen Türen an einem Ort.

Organisation Filtert nach allen Türen, deren zugeordnete Türgruppe der Organisation entsprechen.

Tür	Filtern Sie nach Türen mit bestimmten Zeichen im Namen. Die Spalten zeigen alle Türgruppen - die Gruppen, in denen die betreffenden Türen enthalten sind, werden gekennzeichnet (mit Haken).
Türgruppe	Filtern Sie nach Türgruppen mit bestimmten Zeichen im Namen. Die Zeilen zeigen alle Türen - die Türen, die in den betreffenden Türgruppen enthalten sind, werden gekennzeichnet (mit Haken).
Durchsuchen	In der Standardeinstellung werden die zu den oberen drei Feldern angegebenen Zeichen jeweils am Anfang des Namens gesucht. Mit der Aktivierung dieser Option werden Einträge selektiert, die die angegebenen Zeichen an einer beliebigen Stelle im Namen enthalten.
Mandant	Nur Türen oder Türgruppen des ausgewählten Mandanten werden angezeigt. Standardeinstellung: **Beliebig** - d.h. Einträge aller Mandanten werden angezeigt.

Schreiben von Türausweisen

Im Gegensatz zum Online-Zutrittskontrollsystem können Konfigurationsdaten im Offline-System nicht über Systemkomponenten verteilt und auf die relevanten Installationen übertragen werden; stattdessen müssen sie auf anderem Weg zu den Geräten gelangen. Im *Systemübersicht, Seite 7* wurden bereits verschiedene Systemausweise erwähnt. Eine Art der Systemausweise sind **Türinitialisierungsausweise**, auf die Türparametereinstellungen und Zeitmodelle geschrieben und die an den Türterminals gescannt werden. Nach der Konfiguration wird eine Tür in der Liste ausgewählt. Anschließend wird auf die Schaltfläche **Türausweis schreiben** geklickt, und einer der Türinitialisierungsausweise wird auf der Einheit zum Lesen und Schreiben der Dialogstation platziert.

Ein Dialogfeld fordert Sie auf, den Ausweis zu positionieren und zeigt dann den Fortschritt des Schreibprozesses an.

Es wird eine Meldung angezeigt, dass der Schreibprozess erfolgreich war. Dann wird die Zeit erfasst und als Bestätigung im Feld **Letzte Codierung** angezeigt.

Hinweis!

Es können nur die Konfigurationsdaten **einer** Tür auf einen Türinitialisierungsausweis geschrieben werden. Der Ausweis kann erst dann für andere Schreibprozesse verwendet werden, wenn die Daten an das Türterminal übertragen wurden. Sämtliche vorhandenen Daten werden überschrieben.

Die Zeitmodelle werden auch auf einem Türinitialisierungsausweis gespeichert. Wenn möglich sollten die Zeitmodelle daher im Vorfeld erstellt werden, da ansonsten jede Tür erneut mit Zeitausweisen initialisiert werden muss.

Die neuen Türen, Türgruppen und Parameter werden über diese Türinitialisierungsausweise an die Terminals übertragen. Während des Datenübertragungsvorgangs leuchtet die LED auf den Terminals orange. Die erfolgreiche Übertragung der Daten wird dann bestätigt.

Überprüfen der Ausweise

Bevor der aktuelle Ausweis geschrieben wird, überprüft das System, ob es sich tatsächlich um einen Türinitialisierungsausweis handelt. Wenn der Ausweis bereits auf eine andere Weise codiert wurde (z. B. als Zeit- oder Registrierungsausweis), wird eine entsprechende Warnung angezeigt, mit der Option, den Ausweis zu überschreiben und ihn in Zukunft als Türinitialisierungsausweis zu verwenden.

Hinweis!

Wenn der Parameter **Program (Programm) > Overwrite the card type (Ausweistyp überschreiben)** (Menüleiste) ausgewählt ist, wird eine Bestätigungsaufforderung einmal für jeden Ausweistyp angezeigt. Danach wird der Ausweis ohne weitere Warnung überschrieben. Einrichtungs- und Benutzerausweise können nicht mit einem anderen Ausweistyp überschrieben werden.

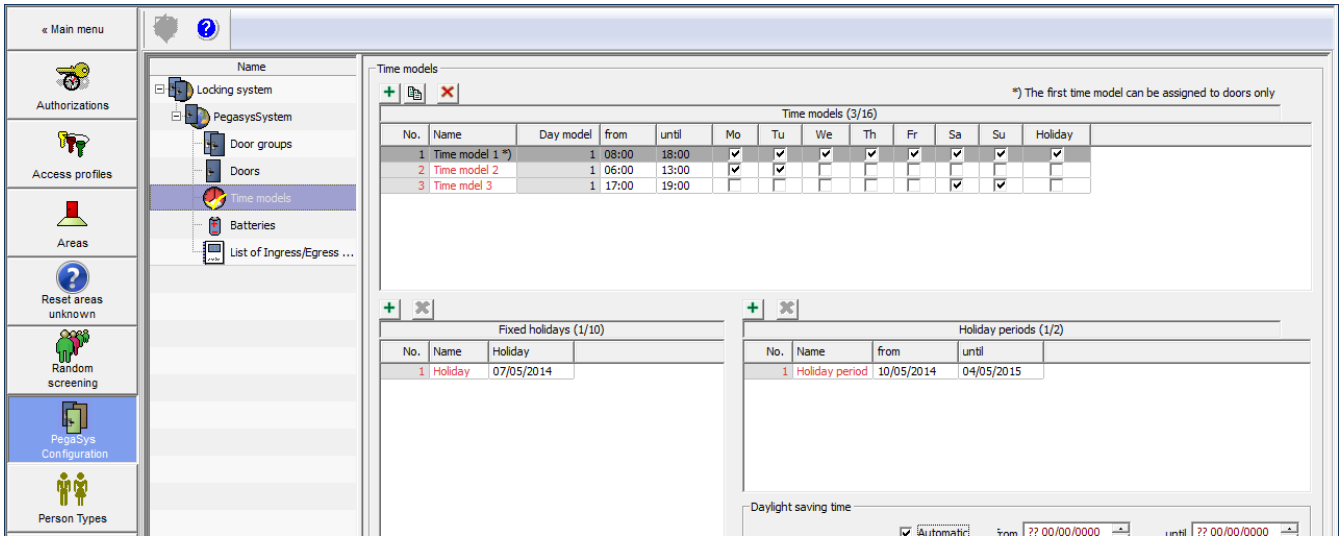
Siehe

– *Schließanlagen, Seite 18*

5.3.4 Zeitmodelle

Das Dialogfeld **Time models** (Zeitmodelle) ist in drei Bereiche unterteilt:

– Die obere Hälfte enthält eine Liste aller Zeitmodelle und deren Zuweisung zu den Wochentagen.
– Feier- und Sondertage (**Fixed holidays**) (Feste Feiertage), die von der Norm abweichen, können im linken unteren Bereich definiert werden.
– Im unteren rechten Bereich können mehrere Tage zu einer **Holiday period** (Feiertagszeitraum) gruppiert werden.



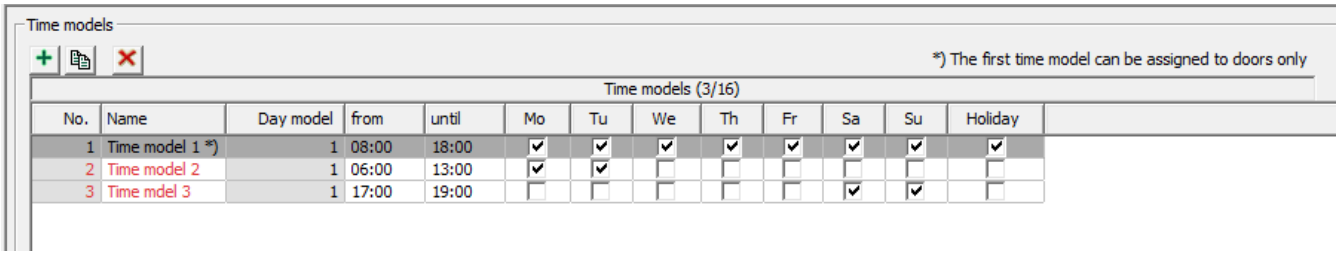
Zeitmodelle versus Zeitperioden

Ein Zeitmodell kann bis zu vier Zeitperioden in einen 24-Stunden-Tag enthalten. Start- und Endzeiten begrenzen in der Regel Zeiträume, in denen unterschiedliche Regeln gelten (z. B. Bürozeiten). Die Zeitperioden können beliebig lang sein und sich überschneiden. Jede Periode kann einem beliebigen Wochen- oder Feiertag zugewiesen werden.

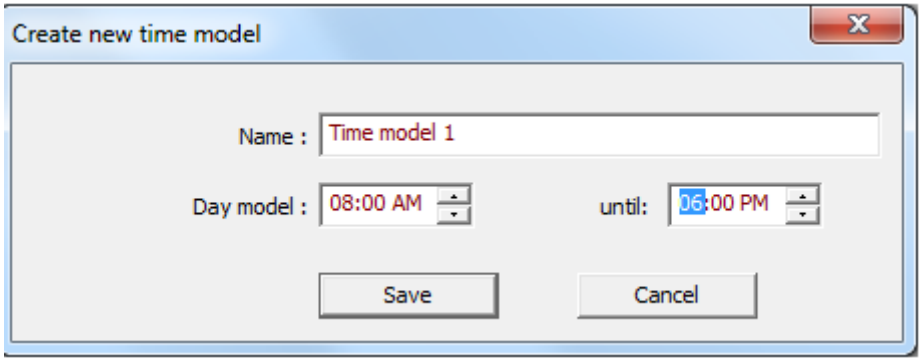
Der Benutzer ist dabei dafür verantwortlich sicherzustellen, dass die Periodengrenzen gesetzt und den Tagen in einer logischen und konsistenten Art zugewiesen werden.

Erstellen von Zeitmodellen

Zeitmodelle können zum Beschränken der zugewiesenen Berechtigungen oder zum Durchführen automatischer Türöffnungs- und Türschließungsvorgänge verwendet werden. Maximal 16 Zeitmodelle mit jeweils 4 Zeiträumen können für jedes System konfiguriert werden.



Wie auch die anderen Konfigurationsdaten werden Zeitmodelle erstellt, indem der Dialog zur Erstellung über die Schaltfläche + geöffnet wird.



Stellen Sie sicher, dass keine Listeneinträge ausgewählt sind. Andernfalls werden weitere Zeiträume anstelle eines neuen Zeitmodells erstellt.

Dem Zeitmodell wird eine eindeutige Bezeichnung (**Name**) sowie die Zeitbeschränkungen für den Zeitraum zugewiesen. Durch Klicken auf die Schaltfläche **Save** (Speichern) wird ein neuer Listeneintrag mit den bereitgestellten Informationen erstellt.

Zeitmodelle mit einer identischen Start- und Endzeit können auch erstellt werden. Damit kann die Tür zur angegebenen automatisch Zeit gesperrt werden.

Konfigurieren von Zeitmodellen

Die Zeitmodelle und Aktivitätsperioden (erste und dritte Spalte) haben feste fortlaufende IDs. [Das Zeitmodell mit der fortlaufenden Nummer **1** kann nicht Personal zugewiesen werden, sondern nur für Vorgänge wie z. B. verlängerte Freigabe.]

Zusätzlich zu den Namen und Start-/Endzeiten enthält jeder Eintrag sieben Kontrollkästchen für Wochentage und einen für einen Feiertag.

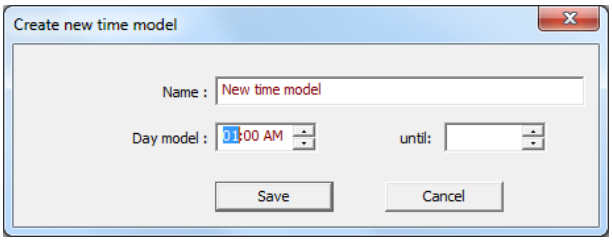
Wenn Sie die entsprechenden Kontrollkästchen aktivieren, werden die Tage festgelegt, an denen der Aktivitätszeitraum gelten soll.

Wenn das Kontrollkästchen **Holiday** (Feiertag) aktiviert ist, wird der Zeitraum auf alle definierten Feiertage und Feiertagszeiträume angewendet.

Die maximale Anzahl der verfügbaren Zeitmodelle (16) gilt separat für jedes System.

Erstellen von zusätzlichen Zeiträumen

Wählen Sie zum Erstellen zusätzlicher Zeiträume zunächst aus der Liste das Zeitmodell aus, zu dem der neue Zeitraum hinzugefügt werden soll. Klicken Sie anschließend auf die Schaltfläche  , als würden Sie ein Zeitmodell erstellen. Das Feld **Name** enthält den Namen des ausgewählten Zeitmodells und kann nicht geändert werden.



Wenn Sie neue Grenzen für einen Aktivitätszeitraum definieren, wird ein neuer Listeneintrag erstellt, der die gleiche Nummer (erste Spalte) und den gleichen Namen (zweite Spalte) wie der ausgewählte Listeneintrag hat. Die Nummer des Zeitraums (dritte Spalte) wird um eins erhöht.

Die Wochentage, auf die der neue Zeitraum angewendet werden soll, können jetzt definiert werden. Es ist möglich, mehrere Zeiträume für einen Tag zu aktivieren.

Auf diese Weise können maximal vier Zeiträume für jedes Zeitmodell definiert werden.

Löschen von Zeitperioden

Ausgewählte Listeneinträge können mit der Schaltfläche  wieder entfernt werden.

Klicken Sie auf **Yes** (Ja), um zu bestätigen, dass Sie die Zeitperiode löschen möchten.

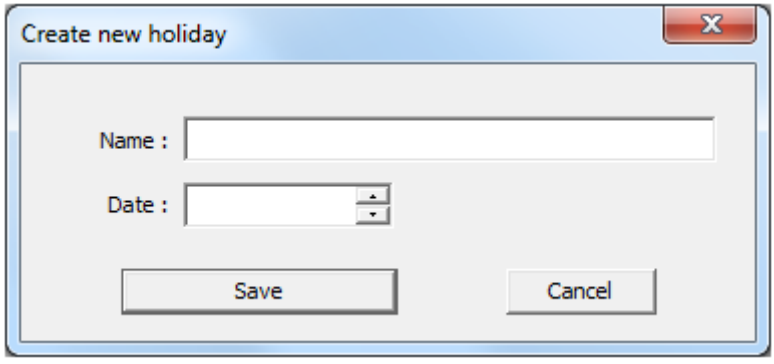
5.3.5 Sondertage, Sondertagszeiträume, Sommerzeit

Sondertage stellen im Vergleich zum normalen Wochenverlauf eine Ausnahme dar und müssen ggf. bezüglich der Kontrollfunktionen anders beachtet werden. Für jede Anlage können **maximal zehn Sondertage** unter Angabe des entsprechenden Jahresdatums definiert werden, an denen andere Zeitintervalle gelten sollen als an den jeweiligen Wochentagen.

Sondertagszeiträume sind ebenfalls Zeiten mit abweichenden Intervallen und erstrecken sich über mehrere Tage - z.B. Betriebsferien. Für jede Anlage können **zwei Sondertagszeiträume** definiert werden

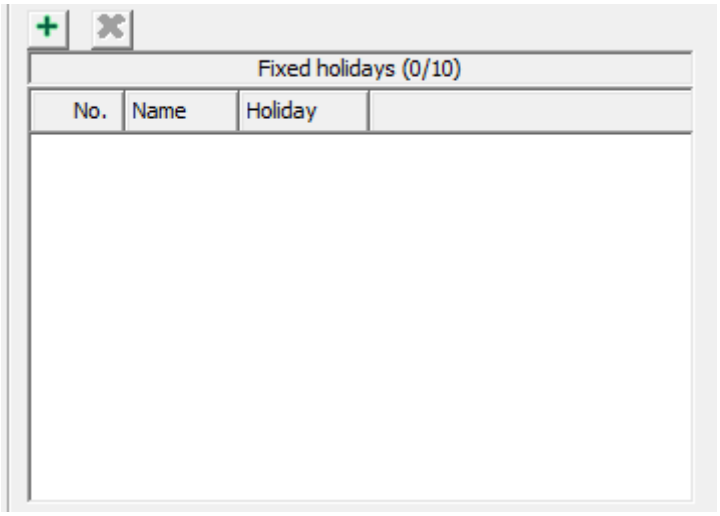
Erstellen von Feiertagen

Die Schaltflächen zum Erstellen und Löschen von Feiertagen befinden sich über dem Listenfenster **Fixed holidays** (Feste Feiertage). Der Dialog zum Erstellen wird durch Klicken auf die Schaltfläche 



geöffnet.

Eine eindeutige Bezeichnung (**Name**) und das **Date** (Datum), wann dieser Feiertag als nächstes auftritt, werden angegeben. Durch Klicken auf die Schaltfläche **Create** (Erstellen) wird ein neuer Listeneintrag mit den bereitgestellten Informationen erstellt.



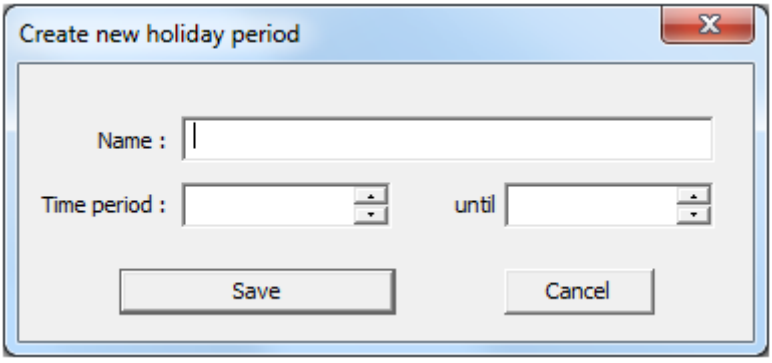
Eine feste fortlaufende ID sowie Name und Datum des Feiertags werden den Einträgen zugewiesen. Die letzten beiden Felder können wie gewünscht verschoben und geändert werden, indem Sie auf den Bearbeitungsstatus doppelklicken.
Für jedes System können maximal zehn Feiertage definiert werden.
Feiertage werden mit einem bestimmten Datum erstellt und müssen jedes Jahr neu definiert und angepasst werden.

Löschen von Feiertagen

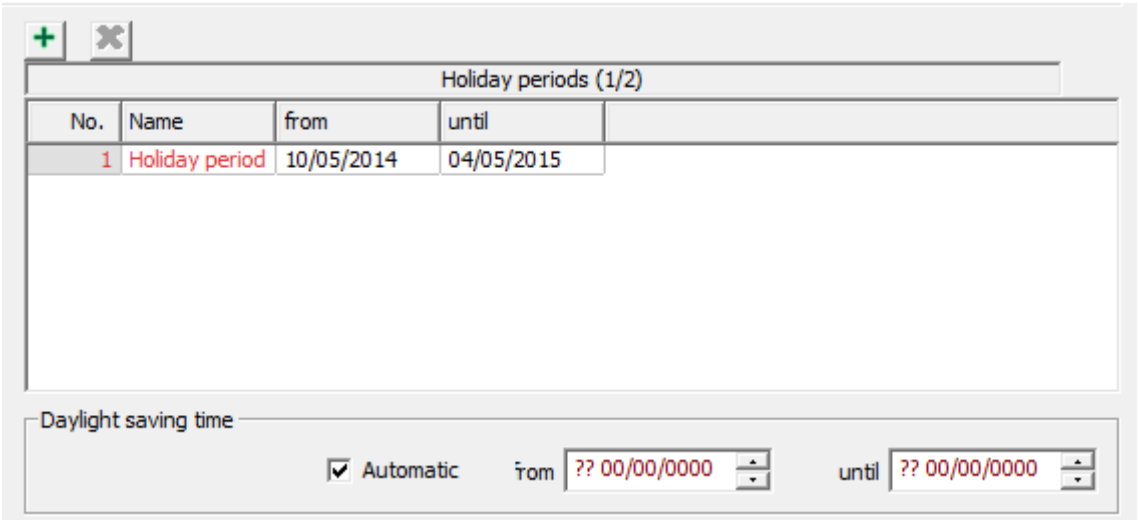
Ausgewählte Listeneinträge können mit der Schaltfläche wieder entfernt werden.
Klicken Sie auf **Yes** (Ja), um zu bestätigen, dass Sie den Feiertag löschen möchten.

Erstellen eines Feiertagszeitraums

Der Dialog zum Erstellen wird durch Klicken auf die Schaltfläche geöffnet.



Eine eindeutige Bezeichnung (**Name**) und ein Start- und Enddatum müssen angegeben werden, bevor ein neuer Listeneintrag mit der Schaltfläche **Save** (Speichern) erstellt werden kann.



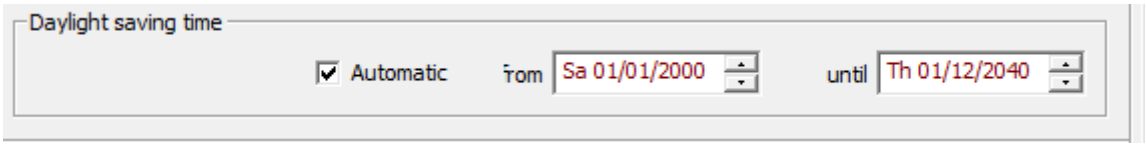
Für jedes System können zwei Zeitperioden definiert werden.
Feiertagszeiträume sind Feiertage, die mehrere Tage umfassen und mit bestimmten Daten erstellt werden. Sie müssen daher jedes Jahr neu definiert und angepasst werden.

Löschen eines Feiertagszeitraums

Ausgewählte Listeneinträge können mit der Schaltfläche wieder entfernt werden.
Klicken Sie auf **Yes** (Ja), um zu bestätigen, dass Sie den Feiertagszeitraum löschen möchten.
Wenn das Kontrollkästchen **Holiday** (Feiertag) für eine Zeitperiode aktiviert ist, gilt dies für alle definierten Feiertage und Feiertagszeiträume. Es ist nicht möglich, zwischen den Feiertagen zu unterscheiden.
Die maximale Anzahl an Feiertagen (zehn) und besonderen Feiertagszeiträumen (zwei) ist zugleich die maximale Anzahl, die gleichzeitig auf den Terminals gespeichert werden kann. Wenn weitere erforderlich sind, können abgelaufene Feiertage oder Feiertagszeiträume gelöscht werden, um wieder Platz freizugeben. Diese müssen dann jedoch mithilfe von Zeitinitialisierungsausweisen auf die Terminals kopiert werden.

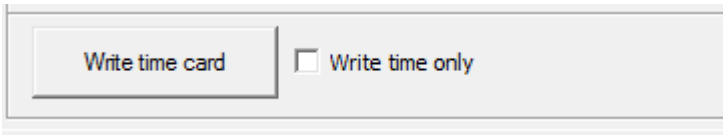
Sommerzeit

Die Einstellung der Sommerzeit kann vom System (**automatisch**) oder über manuelle Eingaben in die beiden Datumsfelder (von / bis) erfolgen. Die manuellen Datumsangaben müssen jährlich angepasst werden.



5.3.6 Zeitkarte schreiben

Eine dieser Systemausweise, der bereits im *Systemübersicht, Seite 7* erwähnt wurde, ist der **Zeitinitialisierungsausweis**, auf den Parametereinstellungen aller Zeitmodelle und die aktuelle Zeit geschrieben und der an den Türterminals gescannt wird.



Wenn das Kontrollkästchen **Nur Zeit schreiben** aktiviert ist und anschließend auf die Schaltfläche **Zeitausweis schreiben** geklickt wird, werden die Zeitmodelle ignoriert.

Ein Dialogfeld fordert Sie auf, den Ausweis zu positionieren und zeigt dann den Fortschritt des Schreibprozesses an.
Eine Meldung bestätigt, ob der Schreibprozess erfolgreich war. Wenn die Uhrzeit nicht das einzige ausgewählte Element war, wird die Zeit erfasst und im Feld **Letzte Codierung** angezeigt.
Beim HITAG-Ausweistyp kann mehr als ein Zeitausweis erforderlich sein, um alle Zeitmodelle zu übertragen.
Die Zeitmodelle werden über diese Zeitinitialisierungsausweise an die Terminals übertragen. Während des Datenübertragungsvorgangs leuchtet die LED auf den Terminals orange. Die erfolgreiche Übertragung der Daten wird dann bestätigt.

Hinweis!
Der Türparameter **Zeitprüfung** muss ausgewählt werden, sodass die Zeitmodelle an den Terminals berücksichtigt werden.

Überprüfen der Ausweise
Bevor der Ausweis auf den Bekanntmachungsleser geschrieben wird, überprüft das System, ob es sich tatsächlich um einen Zeitinitialisierungsausweis handelt. Wenn der Ausweis bereits auf eine andere Weise codiert wurde (z. B. als Tür- oder Registrierungsausweis), wird eine entsprechende Warnung angezeigt, mit der Option, den Ausweis zu überschreiben und ihn in Zukunft als Zeitinitialisierungsausweis zu verwenden.
Wenn der Parameter **Program (Programm) > Overwrite the card type (Ausweistyp überschreiben)** (Menüleiste) ausgewählt ist, wird eine Bestätigungsaufforderung einmal für jeden Ausweistyp angezeigt. Danach wird der Ausweis ohne weitere Warnung überschrieben. Der Parameter wird nur zurückgesetzt, wenn das Konfigurationsprogramm neu gestartet wird. Einrichtungs- und Benutzerausweise können nicht mit einem anderen Ausweistyp überschrieben werden.

5.3.7 Aktualisierung von Datum und Uhrzeit

Zusätzlich zu den Tür- und Zeitmodelldaten wird der aktuelle Zeitstempel (datetime) ebenfalls auf den Transportausweis geschrieben. Um die präzisesten Zeitdaten, insbesondere für Buchungen, zu verwenden, verwenden Sie ein **mobiles Lese-/Schreibgerät** (Timesetter), und aktualisieren Sie die Transportausweise immer sofort vor dem Scannen am Terminal.

Initialisierung des Timesetters
Der Timesetter muss zuerst initialisiert werden. Er erfordert:
– Kundendaten von einem Kundenausweis.
– Eine anfängliche Zeit von einem Transportausweis, z. B. ein Türinitialisierungs- oder Zeitinitialisierungsausweis.

So initialisieren Sie den Timesetter:
1. Legen Sie den Systemausweis (Kunden- oder Transportausweis) auf den Leserkopf des Gerätes (graues Feld).
2. Drücken Sie die Taste **1**.
3. Halten Sie die Taste **1** gedrückt und drücken Sie dann die Taste **2**.

Die Transportausweise werden geschrieben
Aktualisieren Sie Datum und Uhrzeit auf den Transportausweisen sofort, bevor Sie sie an einem Türterminal scannen.
1. Legen Sie die Transportausweise (Türinitialisierungs- oder Zeitinitialisierungsausweise) auf den Leserkopf des Timesetter-Gerätes (graues Feld).

2. Drücken Sie die Taste **2**.

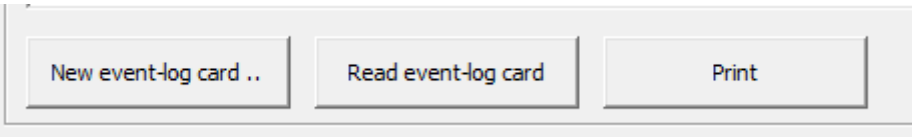
Der Schreibprozess wird durch farbige LEDs angezeigt. Erläuterungen zu den Farbfolgen finden Sie unter *LED Anzeigesignale, Seite 44*.

5.4 Logbuchausweise (Buchung)

Erfolgreiche und fehlgeschlagene Zutrittsversuche werden in den Türterminals gespeichert. Die letzten 800 Registrierungen werden in einem Ringspeicher gespeichert. Diese können mit besonderen Registrierungsausweisen abgerufen und in der Datenbank erfasst werden.
Zuerst werden Logbuchausweise erstellt. Dann werden die Registrierungen von den Terminals abgerufen, und die Ausweise werden über den Dialog eingescannt. Unterschiedliche Ausweistypen lassen eine unterschiedliche Anzahl Registrierungen zu: mit HITAG1 32, mit MIFARE 244 und mit LEGIC 294. Sie müssen daher genügend Logbuchausweise erstellen und die entsprechenden Abruffristen festlegen.

Erstellen von Logbuchausweisen

Ein Logbuchausweis muss initialisiert werden, bevor die Registrierungen gescannt werden können.



1. Legen Sie den Logbuchausweis auf die Schreib-/Leseeinheit der Dialogstation.
2. Wählen Sie den Logbuchdialog in der Explorer-Liste aus.
3. Damit das Terminal einen Logbuchausweis als neu akzeptiert, erstellen Sie einen neuen Logbuchausweis, oder leeren Sie einen verwendeten, indem Sie auf die Schaltfläche **New event-log card...** (Neuer Logbuchausweis...) klicken.

Eine Meldung informiert darüber, dass der Logbuchausweis erfolgreich erstellt wurde.

Lesen der Registrierungen vom Terminal

Dieser Systemausweis kann dann an der Lesereinheit des entsprechenden Terminals präsentiert werden. Während die LED-Anzeige orange leuchtet, schreibt der Terminal Daten auf den Logbuchausweis. Wenn der Logbuchausweis währenddessen entfernt wird, wird die Datenübertragung unterbrochen. Wenn die LED-Anzeige dreimal grün aufleuchtet, wurden die Registrierungen erfolgreich auf den Ausweis geschrieben.
Der Speicher des Terminals wird während dieses Prozesses gelöscht. Das bedeutet, dass die Registrierungen danach nicht erneut abgerufen werden können.

Scannen von Logbuchausweisen

Die Ausweise mit den übertragenen Registrierungen werden dann über den Dialogleser gescannt.

1. Legen Sie den Logbuchausweis mit den Zutrittsdaten auf den Dialogleser.
2. Wählen Sie den Logbuchdialog in der Explorer-Liste aus.
3. Klicken Sie auf **Read event log card** (Logbuchausweis lesen).

Die gelesenen Daten werden im Listenfeld angezeigt. Die folgenden Daten werden für jede Registrierung aufgelistet: DateTime, Nachname, Vorname, Ereignis, Türnummer, Personalnummer, Firma.
Die gelesenen Daten können gedruckt werden. Darüber hinaus werden alle Registrierungen in der Datenbank gespeichert. Sie können jederzeit zurück in das Listenformat konvertiert, gedruckt, exportiert und bearbeitet werden. Hierfür werden besondere Berichte im Dialog-Manager des Zutrittskontrollsystems verwendet.

Hinweis!
Offensichtliche Sequenzfehler im Logbuch
Das Türterminal speichert Ereignisse immer in chronologischer Reihenfolge. Die Zeitstempel im Logbuch werden allerdings von der letzten Zeiteinstellung am Türterminal abgeleitet. Wenn eine aktuelle Zeiteinstellung nicht mit der korrekten DateTime-Format durchgeführt wurde, sind Zeitstempel einiger Ereignisse möglicherweise in der falschen Sequenz.

5.5 Mögliche Datenstrukturen

Türgruppen Einzelne Türen	256	512	768	1024
2	48 (= Standard).	80	112	144
4	52	84	116	148
8	60	92	124	156
16	76	108	140	172

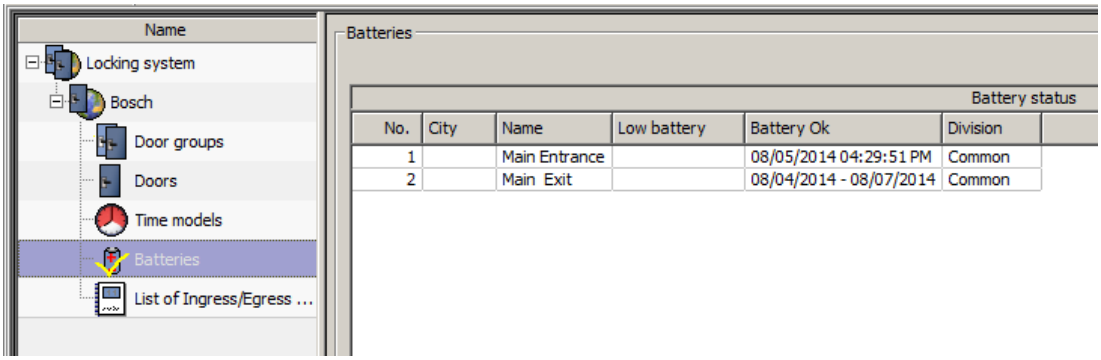
Tab. 5.1: Die Zahlen beziehen sich auf die Datensatzlänge in Byte.

Hinweis!
HITAG1-Ausweise können nur mit der Standardgröße (48 Byte) codiert werden. Anstatt den oben angegebenen 256 Türgruppen sind nur 240 möglich.
Die angegebenen Datengrößen gelten für PegaSys Version 2.0. PegaSys Version 2.1 mit zusätzlichem Batteriestand erfordert fünf Byte mehr, sodass die Speichergröße von 172 auf 177 Byte erhöht wurde. HITAG1 ist eine Ausnahme: Es sind nur maximal 200 Türgruppen mit konstanten 48 Byte möglich.

Die Datensatzlänge sollte in Übereinstimmung mit den aktuellen Anforderungen gewählt werden. Bestellen Sie keinen Speicherplatz im Hinblick auf mögliche Anforderungen. Da Daten auf alle aktivierten Sektoren geschrieben werden, kann sich die Erhöhung von Speicherplatz stark auf die zur Erweiterung oder Erneuerung von Berechtigungen benötigte Zeit auswirken.

5.6 Batterien

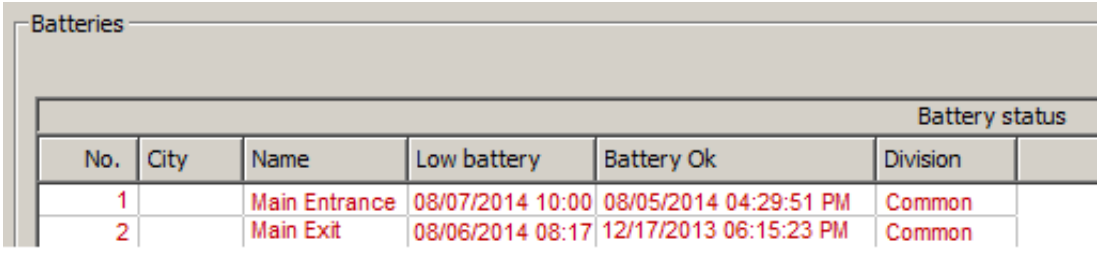
Der letzte bekannte Batteriestand der PegaSys Terminals kann im Dialog **Batteries** angezeigt (Batterien) werden. Der Batteriestand ist nur in Version 2.1 von PegaSys verfügbar (je nach Kundenausweis).



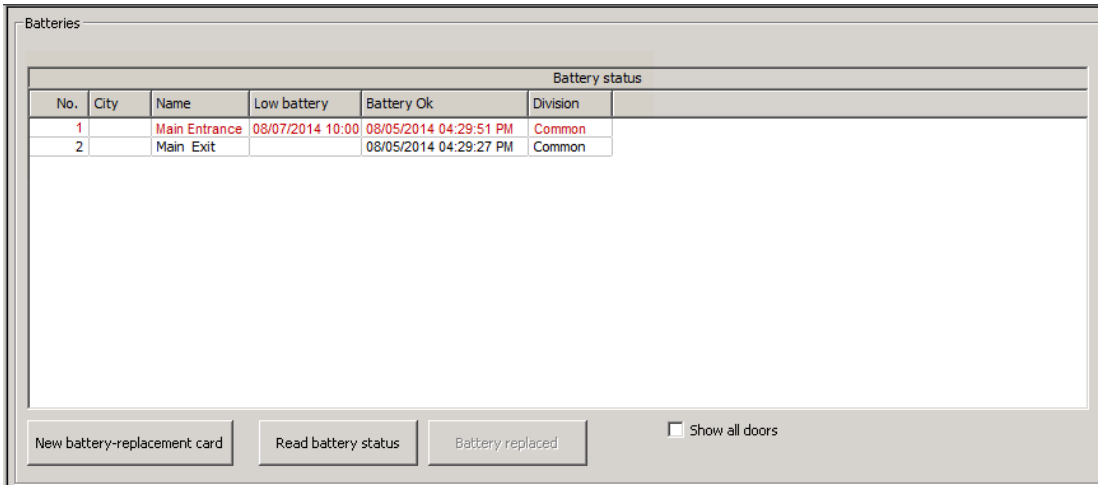
Die Meldungen **Battery LOW** (Niedriger Akkuladestand) und **Battery OK** (Akku OK) werden ausgegeben, wenn der Terminal versucht, auf den Benutzerausweis zuzugreifen.
Es gibt drei Batteriewarnstufen:

1. Bei 3,9 V: Die nächsten 5 Ausweise erhalten eine Warnmeldung, die ein Datum und die Nummer des Terminals enthält.
2. Bei 3,6 V: Bei einem Zutrittsversuch mit einem Benutzerausweis wird eine Sekunde lang ein rotes Signal mit drei Signaltönen ausgegeben. Die nächsten 5 Ausweise erhalten eine Warnmeldung, die mit der auf der ersten Stufe identisch ist.
3. Bei 3,4 V: Bei einem Zutrittsversuch mit einem Benutzerausweis wird drei Sekunden lang ein rotes Signal mit einem kontinuierlichen Signalton von 5 Sekunden ausgegeben. Die nächsten 5 Ausweise erhalten eine Warnmeldung, die mit der der anderen Stufen identisch ist.

Diese Batteriestandwarnungen sind mit Terminal-Firmware Version 4.1 und höher verfügbar.
Die Messtoleranz liegt bei etwa 100 mV für jede Stufe.
Für jeden Schritt auf die nächsthöhere Warnstufe werden Meldungen an die nächsten 5 Benutzerausweise geschrieben (eine für jeden). Für jeden Schritt auf die nächstniedrigere Warnstufe (das heißt nach einem Batteriewechsel) werden 5 positive Meldungen einschließlich Datum und Terminalnummer ausgegeben. Sobald ein Benutzerausweis eine Batteriestandmeldung erhält, können weitere Statusmeldungen auf diesen Ausweis erst wieder geschrieben werden, wenn er auf dem Online-Terminal aktualisiert, das heißt automatisch gelesen und zurückgesetzt, wurde.
Die Statusmeldung (positiv oder negativ) wird in der Datenbank aktualisiert, wenn keine neueren Informationen verfügbar sind.
Der Dialog **Batteries** (Batterien) zeigt in seiner oberen Liste eine Übersicht der Terminals mit Meldungen zu schwachen Batterien an.



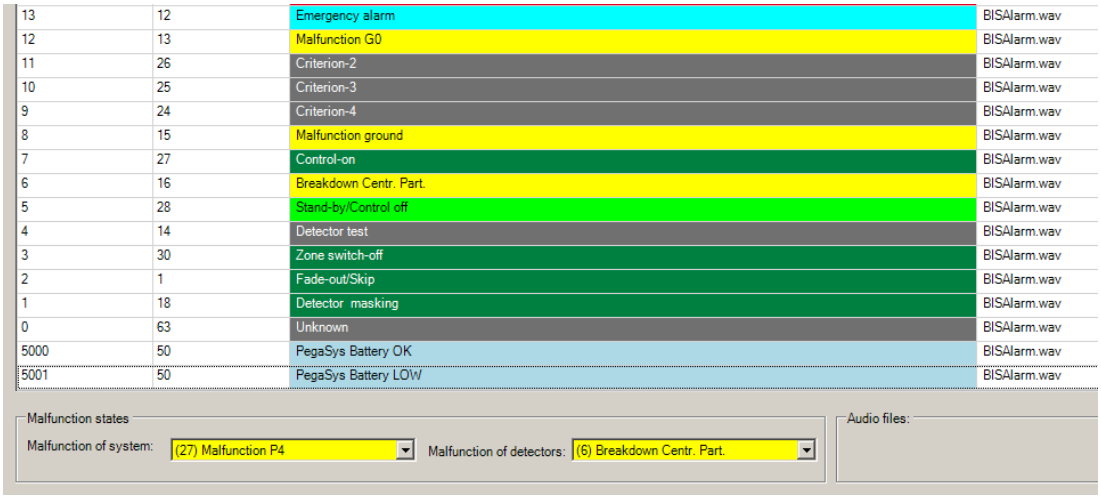
Sobald eine der Batterien gewechselt wurde und das Online-System eine positive Statusmeldung erhält, verschwinden die Einträge aus dieser Liste. Wenn das Kontrollkästchen **Show all doors** (Alle Türen anzeigen) aktiviert ist, werden alle Türen zusammen mit dem jeweiligen Batteriestand angezeigt. Die rot markierten Zeilen weisen auf Terminals hin, die eine schwache Batterie haben oder keine positive Batteriestandmeldung erhalten haben.



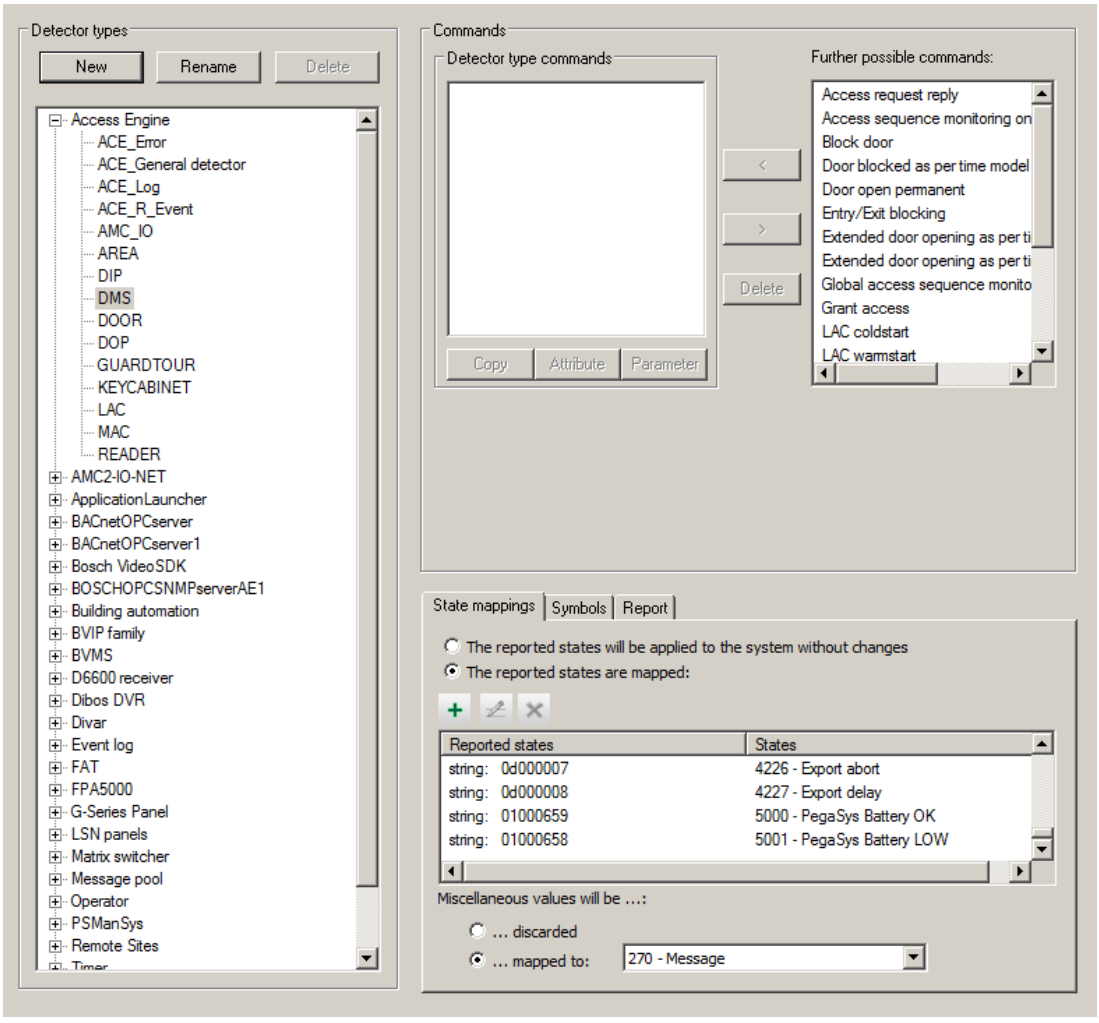
In einigen Fällen werden Terminals nur selten verwendet. Dann können Batteriewarnungen nicht ausreichend häufig abgerufen werden, und der Batteriestand wird nicht aktualisiert. Aus diesem Grund werden alle Terminals mit einem **Battery OK**(Akku OK)-Datum, das älter als ein Jahr ist, rot markiert, als ob eine Warnung ausgegeben worden wäre.
Sie können das Datum für die Anzeige **Battery OK** (Akku OK) auch manuell auf das aktuelle Datum festlegen, indem Sie auf die Schaltfläche **Battery replaced** (Batterie ersetzt) klicken.
Der Benutzerausweis kann mit einer Batteriestandmeldung direkt auf dem Dialogleser gelesen werden, indem Sie auf die Schaltfläche **Read battery status** (Batteriestand lesen) klicken.

Batteriestandmeldung im BIS

Batteriestandmeldungen können auch im BIS angezeigt werden.



Die Zustände **5000: PegaSys Battery OK** (5000: PegaSys Akku OK) und **5001: PegaSys Battery LOW** (5001: PegaSys Niedriger Akkuladestand) werden zur Zustandsliste im BIS Configuration Browser hinzugefügt.



– Wählen Sie in der Liste „Detector types“ (Meldertypen) **Access Engine > DMS** aus.
– Fügen Sie der Liste auf der Registerkarte **Status mapping** (Zustandszuordnung) beide Zustandszuordnungen (mit den Zustandsnummern 1000658 und 01000659) hinzu.

Nur eine Meldung (**Akku OK** oder **Niedriger Akkuladestand**) wird auf jedem Terminal angezeigt, selbst wenn das Online-System bis zu fünf Meldungen erhält.

Batterieersatzausweis

Die Schaltfläche **New battery-replacement card** (Neuer Batterieersatzausweis) erstellt nur für Zylinder-Terminals einen Batterieersatzausweis, weil sie eine Leerung erfordern, bevor die Batterien ersetzt werden können.

Ein Batterieersatzausweis kann für alle Zylinder-Terminals in einem System verwendet werden.

6 Offline Türen – Systemgrenzen

Offline-Schließsysteme per Zutrittskontrollsystem	1
Systeme per Schließsystem	1 Ein **System** ist ein Teil des gesamten Offline-Türen-Schließsystems. Jedes **System** unterliegt einem eigenen Einrichtungsausweis.
Türen per Schließsystem	65,000 insgesamt, verteilt über alle Türgruppen.
Türgruppen per System	Für einen Einrichtungsausweis können maximal 1024 Türgruppen definiert werden.
Zeitmodelle per System	16
Feiertage per System	10
Feiertagszeiträume per System	2

7 LED Anzeigesignale

Signale für Benutzerkarten

Öffnung mit Einzelöffnungsfunktion:

Öffnung mit Daueröffnungsfunktion:

Schließung mit Daueröffnungsfunktion:

Aufforderung zum Batteriewechsel:

Sondersignale

Lese-/Schreibbestätigung für Systemkarten:

Kein Ausweis im Feld:

Lese-/Schreibfehler:

Ungültige Berechtigung:

Uhrzeit ungültig:

Fehlende Türinitialisierung:

Fehlende Facilitydaten:

Datenübertragung:

7.1 Darstellung mit Erläuterungen

7.1.1 Signale für Benutzerkarten

Öffnung mit Einzelöffnungsfunktion

Bedeutung	Die Türöffnung erfolgte mit einer Einzelöffnungskarte. Diese Meldung erscheint auch, wenn bereits dauergeöffnet ist.
Buchungseintrag	**gültige Einzeltürbuchung** oder **gültige Gruppenbuchung**

Öffnung mit Daueröffnungsfunktion

Bedeutung	Die Türöffnung erfolgte mit einer Daueröffnungskarte oder durch ein Zeitmodell.
Buchungseintrag	**Dauer Auf**

Schließung mit Daueröffnungsfunktion

Bedeutung	Die Türschließung erfolgte mit einer Daueröffnungskarte oder durch ein Zeitmodell.
Buchungseintrag	**Dauer Zu**

Aufforderung zum Batteriewechsel

Bedeutung	Rotes LED-Signal von einer bis drei Sekunden Dauer - so lange die Batterie noch nicht vollständig leer ist, folgt ein kartenspezifisches Signal. Bei leeren Batterien wird kein weiteres Signal angezeigt und es sind auch keine Buchungen möglich. Diese Batteriewechselaufforderung wird nur bei Benutzerausweisen angezeigt.

Buchungseintrag	Alle 25 Buchungen erfolgt der Eintrag **Batterie fast leer**.
Abhilfe	Batterien erneuern.

7.1.2 Sondersignale

Lese-/Schreibbestätigung für Systemkarten

Bedeutung	Eine Systemkarte wurde erfolgreich ausgelesen bzw. beschrieben.
Buchungseintrag	**Initialisierung**

Kein Ausweis im Feld

Bedeutung	Die Elektronik wurde "geweckt", es konnte aber kein Ausweis vor dem Leser erkannt werden.
Buchungseintrag	kein Eintrag
Abhilfe	Den Ausweis nochmals vor den Leser halten.

Lese-/Schreibfehler

Bedeutung	Eine Sytemkarte konnte nicht erfolgreich ausgelesen bzw. beschrieben werden.
Buchungseintrag	kein Eintrag
Abhilfe	Die Systemkarte nochmals vor den Leser halten.

Ungültige Berechtigung

Bedeutung	Der Ausweis verfügt über keine gültige Berechtigung.
Buchungseintrag	**Ausweis gesperrt**, **Ungültige Berechtigung**,

	Ausweis nicht mehr gültig oder **Buchung außerhalb Zeitfenster**
Abhilfe	Ggf. die Berechtigung für diesen Ausweis ändern.

Uhrzeit ungültig

Bedeutung	Das Terminal kennt die aktuelle Uhrzeit nicht.
Buchungseintrag	kein Eintrag
Abhilfe	Eine Zeitinit-Karte muss erstellt und am Terminal eingelesen werden.

Fehlende Türinitialisierung

Bedeutung	Das Terminal ist nicht initialisiert.
Buchungseintrag	kein Eintrag
Abhilfe	Eine Türinit-Karte muss erstellt und am Terminal eingelesen werden.

Fehlende Facilitydaten

Bedeutung	Das Terminal ist nicht objektspezifisch getauft.
Buchungseintrag	kein Eintrag
Abhilfe	Das Terminal muss mit einer Facilitykarte getauft werden.

Datenübertragung

Bedeutung	Während Daten zwischen einer Systemkarte und einem Terminal ausgetauscht werden, leuchtet die LED orange.

Die Dauer ist abhängig von der zu übertragenden Datenmenge. Anschließend erfolgt die Signalisierung des Lese-/Schreibvorgangs.

7.1.3 LED Anzeigen für mobiles Lese-/Schreibgerät

Schreibbestätigung Zeitmodellkarte

Bedeutung Die Zeitmodellkarte wurde erfolgreich beschrieben.

Lesebestätigung Zeitmodellkarte

Abbildung 7.1:

Bedeutung Die Zeitmodellkarte wurde erfolgreich ausgelesen.

Lesebestätigung Facilitykarte

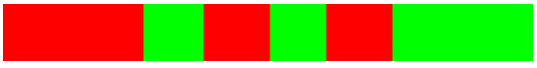
Bedeutung Die Facilitykarte wurde erfolgreich ausgelesen.

Lese-/Schreibfehler

Bedeutung Die Systemkarte konnte nicht erfolgreich ausgelesen bzw. beschrieben werden.

Abhilfe Die Systemkarte nochmals von den Leser halten.

Fehlende Facilitydaten



Bedeutung Der Timesetter ist nicht objektspezifisch getauft.

Abhilfe Der Timesetter ist mit der Facility-Karte neu zu taufen.

Uhrzeit ungültig

Bedeutung	Der Timesetter kennt die aktuelle Uhrzeit nicht.
Abhilfe	Es ist eine entsprechende Zeitinitkarte zu erstellen und an dem Timesetter einzulernen.

Legende:

Die Länge der Farbbalken in den gezeigten Beispielen gibt die Länge der Brenndauer an. Die mittlere Länge, wie hier gezeigt, bedeutet ein Brenndauer on ca. 1 Sekunde.

 grüne LED

 rote LED

 orange LED

 blaue LED

 - zusätzliches akustisches Signal

8 Offline Türen – Bearbeiten von Personaldaten

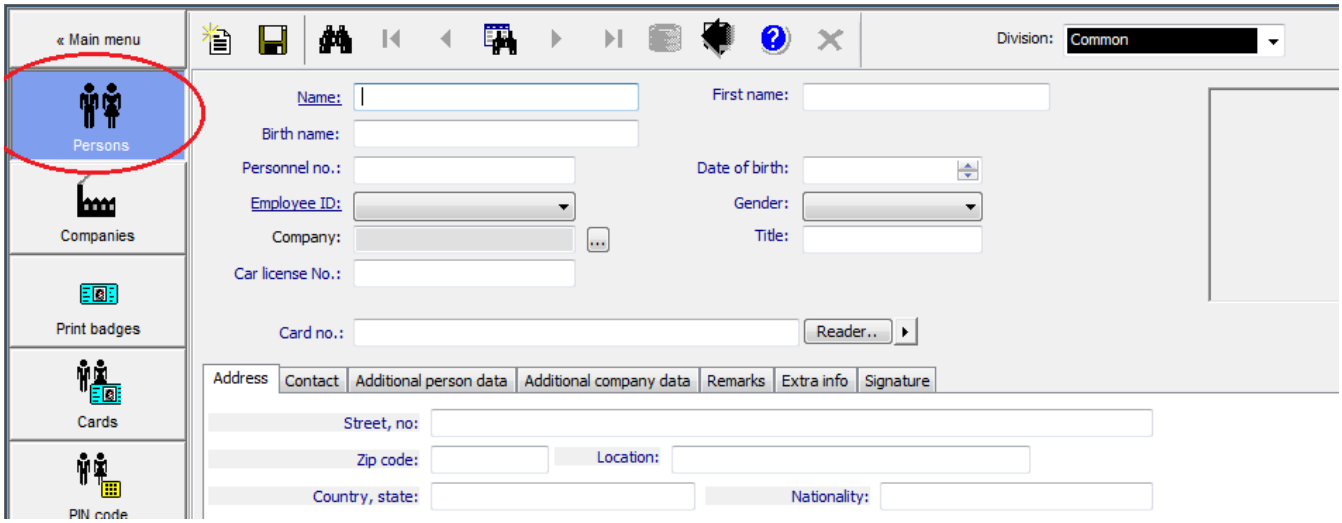
Die Datenbank des Haupt-Zutrittskontrollsystems wird auch zum Speichern von Personaldaten für das Offline-System verwendet.
Dementsprechend werden diese Daten über die Dialoge des Zutrittskontrollsystems eingegeben und jeder Ausweisinhaber für das Offline-System benötigt einen gültigen Ausweis für das Online-Zutrittskontrollsystem.

8.1 Anlage der Personendaten

Online-Daten

Um Personaldaten hinzuzufügen und Online-Berechtigungen hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie zum Dialogsystem des Haupt-Zutrittskontrollsystems.
2. Öffnen Sie im Datenmenü „Personnel“ (Personal) den Dialog **Persons** (Personen).
3. Geben Sie mindestens die grundlegenden Daten für die betreffende Person in die entsprechenden Spalten ein.
4. Speichern Sie den neuen Datensatz.



5. Erstellen Sie im Dialog **Print badges** (Ausweise drucken) einen Ausweis, falls noch keiner verfügbar ist.
6. Wechseln Sie zum Dialog **Cards** Ausweise.
7. Wenn ein **enrollment reader** (Bekanntmachungsleser) bereits im Zutrittskontrollsystem definiert wurde, wählen Sie ihn aus.
8. Klicken Sie auf die Schaltfläche **Record card** (Ausweis erfassen), um den Ausweis im System zu registrieren.

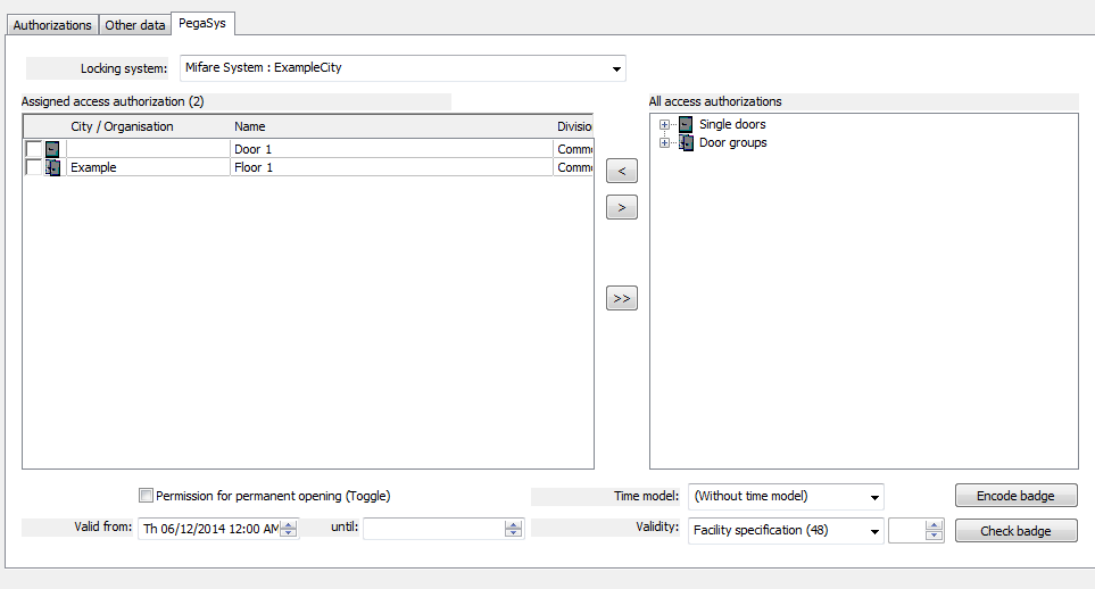
Offline-Daten

Die entsprechenden Berechtigungen für die Schließsysteme werden separat zugewiesen.

1. Wechseln Sie im Dialog **Cards** (Ausweise) zur Registerkarte **PegaSys** mit den ausgewählten Personaldaten.
2. Wählen Sie das entsprechende Schließsystem aus der oberen Dropdown-Liste aus - die Türen und Türgruppen, die für dieses System eingerichtet wurden, werden im Listenfeld **Available access authorizations** (Verfügbare Zutrittsberechtigungen) angezeigt.
3. Doppelklicken Sie auf einzelne Einträge, um sie hinzuzufügen, oder wählen Sie mehrere Listeneinträge aus und klicken Sie auf die Schaltfläche mit dem Pfeil nach links, um die gewünschten Türen und Türgruppen hinzuzufügen. Wiederholen Sie die Schritte 2 und 3

für andere Systeme - die zuvor vorgenommenen Auswahlen werden beibehalten. Auf einem (HITAG) Ausweis können Berechtigungen für maximal drei Systeme gespeichert werden.

4. Überschreiben Sie ggf. die Parameterwerte (Gültigkeitsdaten, Zeitmodell usw.), wenn sie nicht die Standardwerte haben sollen.
   - **Permission for extended unlocking (toggle)** (Berechtigung für verlängerte Freigabe (umschalten))
     Wenn der Parameter **Extended unlocking (toggle)** (Verlängerte Freigabe (umschalten)) bei der Tür festgelegt ist, kann der Ausweisinhaber die Tür für längere Zeit entsperren, indem er seinen Ausweis für drei Sekunden am Leserterminal präsentiert.
   - **Valid from** (Gültig ab)
     Dieses Feld enthält standardmäßig das aktuelle Datum und die aktuelle Uhrzeit. Hier können auch Daten eingegeben werden, die in der Zukunft liegen.
   - **Valid until** (Gültig bis)
     In diesem Feld kann ein Datum angegeben werden, das eine absolute Gültigkeitsdauer für Rechte angibt (z. B. ein Kalenderjahr).
     Jedes hier eingegebene Datum ersetzt die Informationen im Feld **Validity** (Gültigkeit).
   - **Time model** (Zeitmodell)
     Eines der Offline-Zeitmodelle kann die Ausweisverwendung auf die durch die Parameter definierten Zeiten einschränken.
     [Zeitmodell Nr. 1 ist nicht in der Auswahlliste enthalten. Es kann Personal nicht zugewiesen werden.]
     Der Parameter **Time check** (Zeitprüfung) muss für das Terminal ausgewählt werden.
   - **Validity** (Gültigkeit)
     Der Standardwert, der bei der Konfiguration des Systems angegeben wurde, wird in den Standardeinstellungen angezeigt. Dieser Wert kann individuell für jeden Ausweisinhaber geändert werden.
     Die Gültigkeitsdauer kann auf verschiedene Weise und auf unterschiedlichen Ebenen definiert werden - siehe auch *Spezielle Einstellungen, Seite 59*.
5. Schreiben auf den Ausweis
6. Wählen Sie eine der folgenden Optionen aus:
   - Platzieren Sie den Ausweis auf der Lese-/Schreibeinheit an der Workstation und drücken Sie auf **Encode card** (Ausweis codieren), um den Schreibprozess zu initiieren. [Das System aktiviert den Dialogleser für das Offline-System automatisch, ohne dass Sie ihn vorher auswählen müssen.]
   - Alternativ kann der Ausweis auch auf einem der Online-Leser (DELTA 7020/1000/1010) codiert werden.



Hinweis!
Die Gültigkeitsgrenzen des Online-Zutrittskontrollsystems gelten für das Offline-System und haben im Konfliktfall Vorrang.

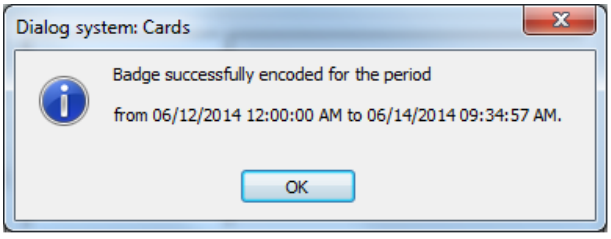
Datenkontrolle beim Schreibvorgang

Nach der Betätigung der Schaltfläche Ausweis kodieren erscheint ein Dialogfenster mit der Aufforderung, die Karte auf die Lese-/Schreibeinheit zu legen.

Folgende Umstände führen zu Fehlermeldungen und dem Abbruch des Schreibvorgangs:

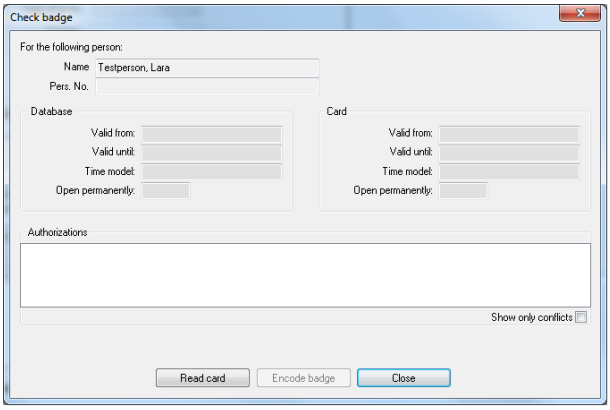
- Es wurde keine Karte aufgelegt oder die Codedaten konnten nicht gelesen werden.
- Bei der Karte handelt es sich nicht um eine Benutzerkarte.
- Die Karte gehört nicht der ausgewählten Person.

Ein erfolgreicher Schreibvorgang wird unter Angabe des Gültigkeitszeitraums angezeigt. Als Startzeit wird das aktuelle Datum mit der Uhrzeit 00:00 verwendet, damit auch an Terminals mit ungenauer Uhrzeit Zutritt gewährt wird.



Validieren von Ausweisen

Durch Klicken auf die Schaltfläche **Validate card** (Ausweis validieren) wird ein Dialog geöffnet, in dem die Berechtigungen, die gerade auf dem Ausweis kodiert wurden, durch Abgleich mit der Datenbank validiert werden.



Diese Funktion kann auch als erste Maßnahme zur Fehlerbehebung verwendet werden, zum Beispiel wenn ein Ausweis nicht funktioniert. Ein Grund für Fehlfunktionen sind Datenkonflikte zwischen Ausweis und Datenbank.

1. Suchen Sie über die Suchfelder im Dialogkopf nach dem relevanten Datensatz aus der Datenbank.
2. Klicken Sie auf die Schaltfläche **Validate card** (Ausweis validieren) auf der Registerkarte **PegaSys**, um den Dialog **Check authorizations** (Berechtigungen prüfen) zu öffnen. Daten für die ausgewählte Person werden in die Felder **Name** und **Pers. no.** (Pers.-Nr.) sowie in das Dialogfeld **Authorizations in the database** (Berechtigungen in der Datenbank) eingegeben.
3. Platzieren Sie den Ausweis auf dem Dialogleser für die Dialogstation.
4. Klicken Sie dann auf die Schaltfläche **Read card** (Ausweis lesen) unten im Dialog.
5. Vergleichen Sie **Authorizations in the database** (Berechtigungen in der Datenbank) mit **Authorizations on the card** (Berechtigungen auf dem Ausweis).

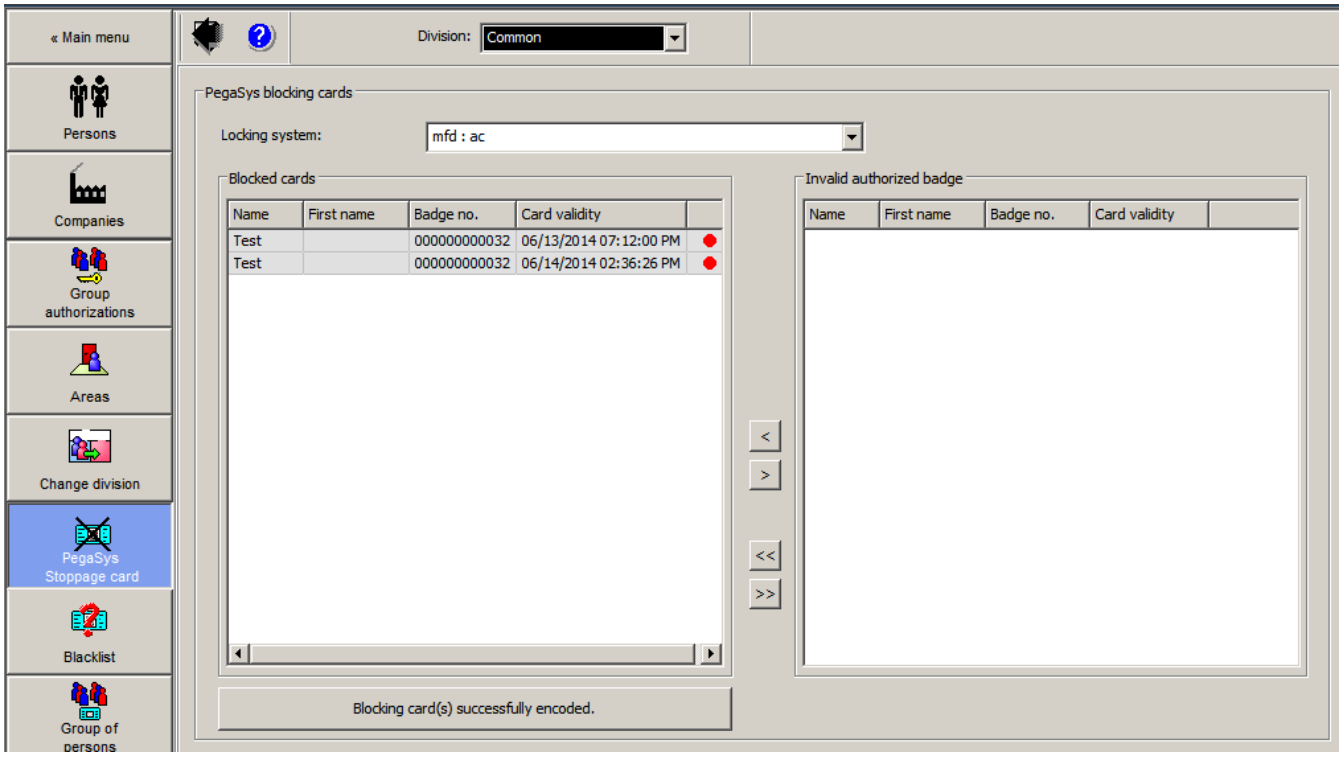
Wenn beim Vergleich Abweichungen der Daten erkannt werden, sollte der Ausweis erneut kodiert werden. Die angezeigten Daten müssen nicht genau übereinstimmen. Sie sollten jedoch komplett innerhalb der Gültigkeitsdauer in der Datenbank liegen.

8.2 PegaSys - Sperrkarten

Wenn die Dialogberechtigung gültig ist, wird der Dialog **PegaSys Blocking** (Pegasys-Sperrung) im Menü **Personnel data** (Personaldaten) angezeigt. Wenn das Schließsystem ausgewählt ist, wird rechts eine Liste der aktuell ungültigen Benutzerausweise angezeigt.
„Aktuell ungültig“ bedeutet:

- Personen, die aktiv gesperrt wurden, aber deren Ausweise noch aktive Berechtigungen haben.
- Personen, deren Ausweisgültigkeit online beendet wurde, bei denen die Ausweise selbst aber noch aktive Berechtigungen haben.

Die Offline-Terminals haben nur einen begrenzten Speicher für Einträge in der Liste mit gesperrten Ausweisen. Daher müssen Benutzerausweise, die gesperrt werden sollen, manuell ausgewählt werden.
Das Ablaufdatum des Benutzerausweises wird in der Spalte **Card validity** (Ausweisgültigkeit) angezeigt. Einträge in der Liste **Invalid authorized badge** (Ungültiger autorisierter Ausweis) können mit den Pfeilschaltflächen zur Liste mit gesperrten Ausweisen hinzugefügt werden.



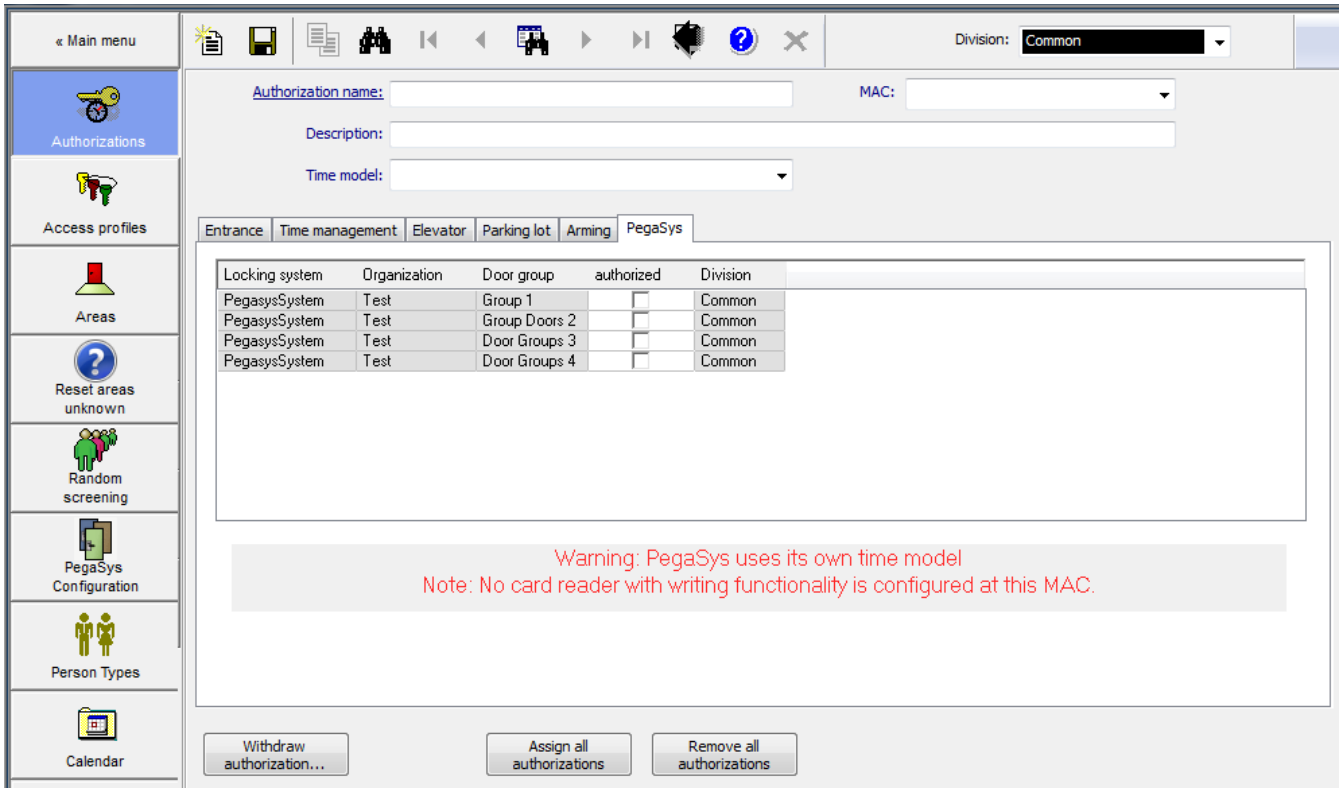
Durch Klicken auf die Schaltfläche **Encode** (Codieren) werden die Einträge zu sogenannten „Sperrausweisen“ hinzugefügt. Diese codierten Sperrausweise müssen dann in die Offline-Terminals eingelesen werden. Nur dann ist es nicht mehr möglich, diese Ausweise auf diesen Terminals zu verwenden.
Die Liste auf der linken Seite bietet außerdem einen Überblick der Ausweise, die derzeit in der PegaSys-Sperrliste aufgeführt sind. Eine grüne/rote Lampe gibt an, ob der entsprechende Eintrag erneut aus der Liste entfernt werden kann.

- Rot
  Der Ausweis sollte gesperrt werden.
- Grün
  Der Ausweis wurde entweder erneut autorisiert oder ist abgelaufen und daher nicht mehr aktiv.

Die grünen Einträge werden automatisch beim nächsten Codieren der Sperrausweise entfernt.

8.3 online/offline Zutrittsberechtigungen

Die Dialoge **Access authorizations** (Zutrittsberechtigungen) und **Room/time authorizations** (Raum/Zeit-Berechtigungen) im Menü **System data** (Systemdaten) enthalten eine Registerkarte mit dem Namen **PegaSys**. Alle definierten Türgruppen (keine einzelnen Türen) werden auf dieser Registerkarte aufgeführt.



Türgruppen des Offline-Schließsystems können einer beliebigen Zutrittsberechtigung im Online-System zugewiesen werden. Damit der Ausweisinhaber Zutritt zur Türgruppe haben kann, muss sein Ausweis erneut codiert werden.
Türgruppen, die basierend auf Zutrittsberechtigungen zugewiesen wurden, können im Dialog **Cards** (Ausweise) nicht entfernt werden.
Dies gilt ebenso für die Raum/Zeit-Berechtigungen, auch wenn die Zeitmodelle für das Online-System nicht für Offline-Installationen gelten. Dies wird in einer Meldung unter dem Listenfeld hervorgehoben: **Note: PegaSys uses its own time models** (Hinweis: PegaSys verwendet seine eigenen Zeitmodelle). Im Hinblick auf Offline-Berechtigungen gibt es keinen Unterschied zwischen Zutrittsberechtigungen und Raum/Zeit-Berechtigungen – die Online-Raum/Zeit-Berechtigungen und Offline-Berechtigungen werden hier zusammengefasst.

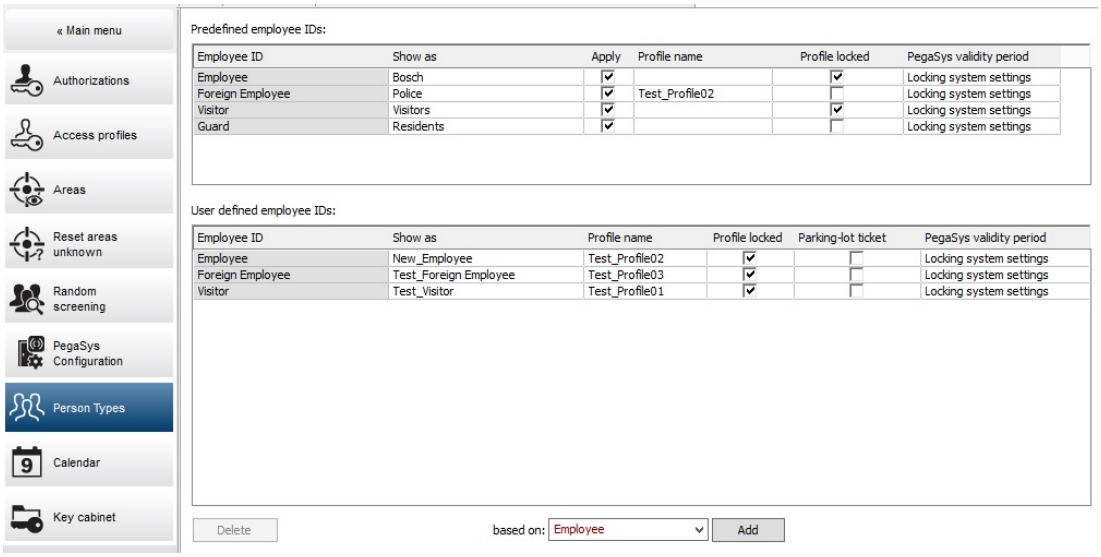
8.4 Offline-Daten auf temporären Ausweisen

Vermeiden von Offline-Daten auf temporären Ausweisen
Mit Online-Zutrittskontrollsystemen können temporäre Ersatzausweise erstellt werden, einschließlich Ausweisen, die Offline-Daten enthalten. Die Offline-Daten auf dem Ausweis bleiben gültig, auch wenn die Online-Daten abgelaufen sind.
Um mögliche Sicherheitsverstöße zu verhindern, sollten Sie sicherstellen, dass Sie keine temporären Ausweise erstellen, die Offline-Daten enthalten.

8.5 Personalklassen - Gültigkeitsdauer

Wenn Software für das Offline-Sperrsystem installiert ist, wird die zusätzliche Spalte **PegaSys validity period** (PegaSys-Gültigkeitsdauer) in den beiden Listenfeldern im Dialog **Personnel classes** (Personalklassen) angezeigt.

Wenn die relevante Personalklasse beim Erstellen neuer Personaldatensätze im Dialog **Persons** (Personen) ausgewählt ist, wird die hier angegebene Gültigkeitsdauer den Offline-Berechtigungen zugewiesen. Diese Gültigkeitsdauer ersetzt die Standard-Gültigkeitsdauer, die beim Konfigurieren des Offline-Sperrsystems festgelegt werden kann.
Die Gültigkeitsdauer kann auf verschiedene Weise und auf unterschiedlichen Ebenen definiert werden – siehe auch *Spezielle Einstellungen, Seite 59*.



Durch Klicken auf die entsprechende Zeile in der Spalte **PegaSys validity period** (PegaSys-Gültigkeitsdauer) wird ein Dialog für das Auswählen und Festlegen eines neuen Werts geöffnet.

8.6 Statusleiste des Dialogsystems

Zusätzlich zu den Anzeigen für das Zutrittskontrollsystem - Known (Bekannt), Blocked (Gesperrt), Currently not valid (Aktuell ungültig) und Random Screening (Mitarbeiterauslosung) - enthält die Statusleiste auch eine farbige Visualisierung der Berechtigungen für das Offline-System (PegaSys).
Diese Anzeige und unterschiedliche Beschriftungen geben die folgenden Zustände entsprechend dem Verarbeitungsstatus der Offline-Daten an.

LED	Beschriftung	Bedeutung
	PegaSys	Dieser Ausweis ist nicht für das Offline-System definiert.
	Encoded (Codiert)	Ein Ausweis mit gültigen Berechtigungen wurde codiert.
	Abgelaufen	Der Gültigkeitszeitraum für das Offline-System wurde überschritten.
	Not current (Nicht aktuell)	Der Gültigkeitszeitraum für das Offline-System wurde noch nicht gestartet - die Startzeit liegt in der Zukunft.

8.7 Listen zu den Offline Daten

Das Menü **Berichte** des Haupt-Zutrittskontrollsystems wurde um den Dialog **Personen PegaSys** erweitert, der den Ausdruck von Offline Daten ermöglicht.

Filteroptionen

- **Personaldaten**
  Einzelne Personen oder Gruppen (z. B. das gesamte Personal eines Unternehmens/einer Abteilung) können über die Eingabefelder gefiltert werden.
- **Offline-Elemente**
  - Schließsystem
  - Türgruppen
  - Türen
  - Organisation (= Gruppierung von Türgruppen)
  - Bereich (= Bereich, in dem sich die Tür befindet)
- Alle Filter können miteinander kombiniert werden.

Layoutauswahl

Die Darstellung der Suchergebnisse und welche Informationen jeweils angezeigt werden, bestimmt die Auswahl des Layouts. Vier vordefinierte Listenlayouts stehen zur Verfügung.

Personen mit Türen/ Gruppen	Jede Person, die Berechtigungen für die Schließanlage erhalten hat, wird unter Angabe der wichtigsten Zutrittskontrolldaten aufgeführt. Zu jeder Person werden Anlage, Standort und Türen/Türgruppen aufgelistet.
Türen mit Personen	Nach Anlagen sortiert werden zu jeder Tür die berechtigten Personen aufgelistet.
Türgruppen mit Personen	Nach Anlagen sortiert werden zu jeder Türgruppe die berechtigten Personen aufgelistet.
Personen Crosstab	Tabellendarstellung. Die Spalten enthalten die Bezeichnungen der Türen und Türgruppen (G) - die Zeilen die Namen der Personen des Offline Systems. Durch ein Kreuz (X) an der Schnittstelle von Spalte und Zeile wird eine vorhandene Berechtigung kenntlich gemacht.
Logbuch nach Türen	Gefiltert nach speziellen Türen, werden alle Buchungen (mit Personenangaben) an diesen Terminals aufgelistet.

Logbuch nach Personen	Gefiltert nach bestimmten Personen, werden alle Türen, an denen diese Personen gebucht haben, aufgelistet.
Sperrkarten	Liste aller PegaSys Karten, die bei der nächsten Kodierung ge- oder entsperrt werden.

8.7.1 PegaSys-Daten in online Berichten

Die Berichte

- Zutrittsberechtigung pro Person
  mit Anzeige der PegaSys Berechtigungen in der Form
  - Einzeltür, Ort, Anlage
  - Türgruppe, Organisation, Anlage
- Zutrittsberechtigungen und Raum-Zeit-Berechtigungen
  mit Anzeige der PegaSys Berechtigungen in der Form
  - Türgruppe, Anlage

enthalten u.a. Informationen des PegaSys Systems.

8.8 Spezielle Einstellungen

Im Gegensatz zu Online-Systemen werden für die Schließanlagen die Berechtigungen nur für verhältnismäßig kurze Zeiträume vergeben und müssen regelmäßig erneuert und verlängert werden. Die Gültigkeitsdauer kann auf drei unterschiedlichen Arten und Ebenen festgesetzt werden.

1. Individuelle Einstellung zu jeder Person.
   Siehe *Offline-Daten, Seite 51*.
2. Zuweisung über die Personalklasse.
   Siehe *Personalklassen - Gültigkeitsdauer, Seite 56*.
3. Vorgabe einer Standardgültigkeitsdauer für die gesamte Schließanlage.
   Siehe *Standardgültigkeit, Seite 23*.

Die angegebene Reihenfolge gibt auch die Wertigkeit der jeweiligen Angaben an. Eine individuelle Einstellung überschreibt Zuweisungen über die Personalklasse und Vorgaben der Schließanlage. Zuweisungen über die Personalklassen setzen die Vorgabe der Schließanlage außer Kraft.

9 Offline Türen – Beschreibung der Vorgehensweisen

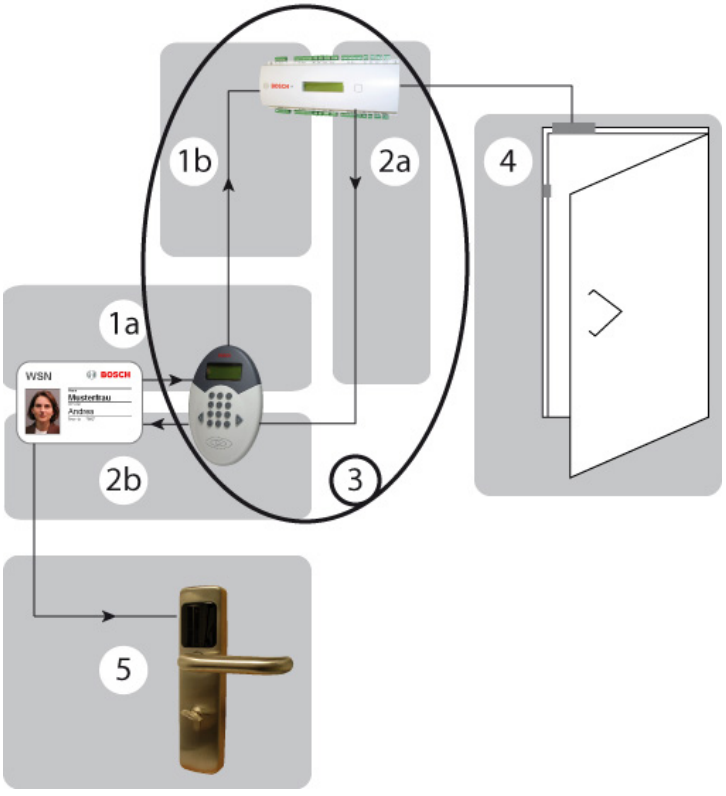
Die folgenden Ablaufbeschreibungen sollen kurze Darstellungen notwendiger Arbeitsschritte bzw. Arbeitsabläufe sein und somit Besonderheiten von Offline-Systemen - vor allem im Zusammenhang mit Zutrittskontrollsystemen (online) - aufzeigen und erläutern.

9.1 Datenanlage

Bei neuen Objekten wird folgende Vorgehensweise empfohlen.

1. Definition der Türgruppen
2. Definition der Zeitmodelle
3. Definition der Terminals (Türen)
4. Personendaten Verwaltung
   - Anlage der Personendaten
   - Berechtigungsvergabe - online (optional)
   - Ausweiszuordnung - online
   - Berechtigungsvergabe - offline
   - Ausweiscodierung - offline

9.2 Zutritt



1a Ausweis lesen

1b Ausweisnummer wird an den AMC weitergeleitet

2a Aktuelle Daten werden an den Leser übermittelt

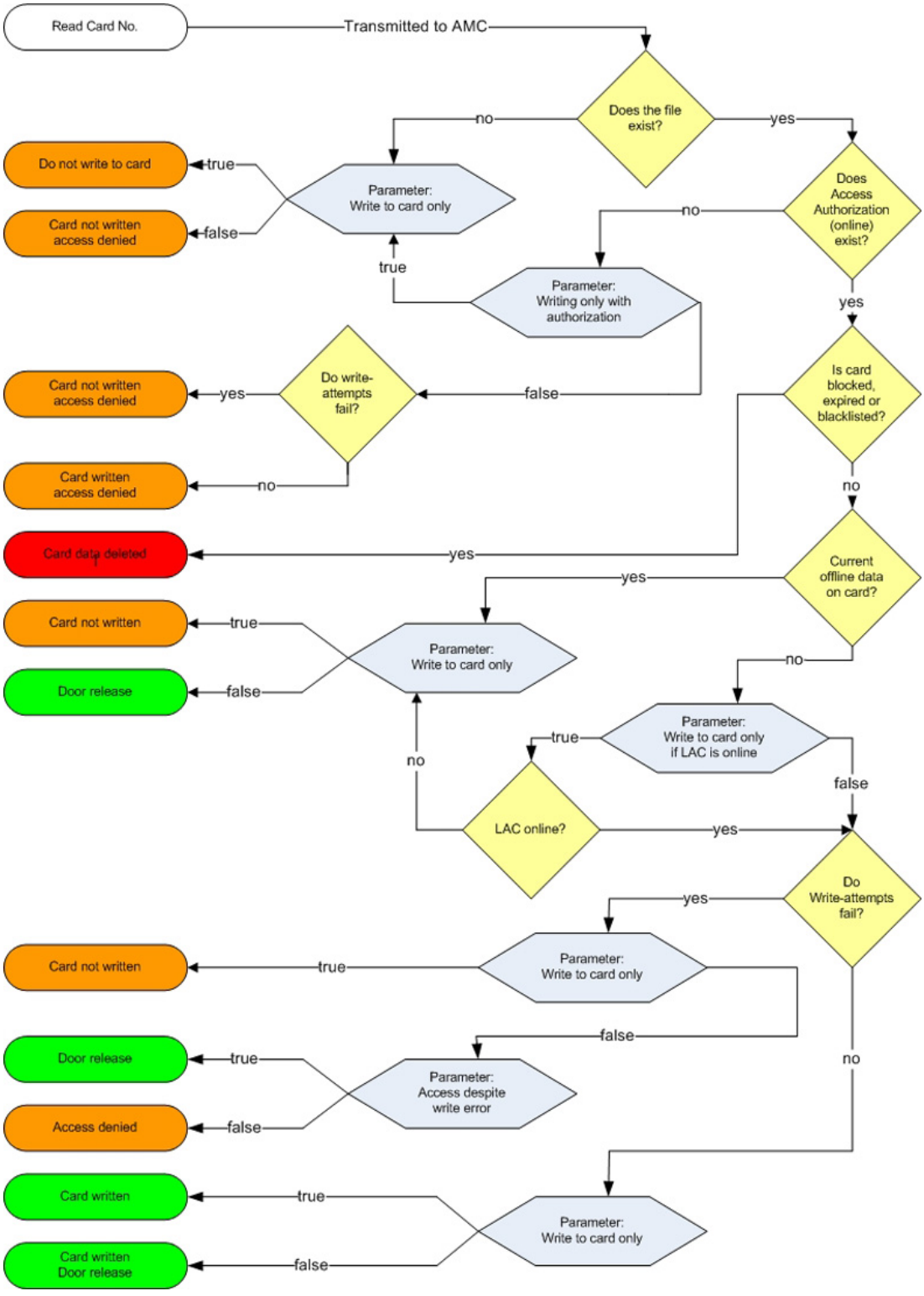
2b Aktuelle Daten werden auf den Ausweis geschrieben

3 Zum Prüf- und Schreibvorgang auf dem AMC- siehe Ablaufdiagramm in *Schreibvorgang, Seite 61*.

4 Türfreigabe für das Online-System (falls parametriert)

5 Berechtigungsprüfung an den Türterminals

9.2.1 Schreibvorgang



Bei den Schreibvorgängen handelt es sich in den meisten Fällen um eine Verlängerung der Zutrittsberechtigungen entsprechend der vorgegebenen Zeiträume.
Aus diesem Grunde wird in der Datenbank auch das letzte Aktualisierungsdatum gespeichert. Im Vergleich mit dem aktuellen Tagesdatum bzw. mit der aktuellen Uhrzeit wird die Notwendigkeit zur Verlängerung ermittelt. Da dies aber bei jeder Buchung dazu führen würde, dass die Ablaufdaten der Berechtigungen aktualisiert würden, müsste auch jedes Mal ein Schreibvorgang ausgeführt werden. Um unnötige Wartezeiten und Verzögerungen an den Lese-/Schreibeinheiten zu vermeiden, wird anhand der Gültigkeitsdauer und der eingestellten Beschreibungsregel (siehe dazu *Konfiguration der Lese-/Schreibeinheit, Seite 12*) ein Zeitpunkt ermittelt, bis zu dem die Ausweisdaten als aktuell anzusehen sind.
In der Standardeinstellung werden die Daten erst aktualisiert, wenn zwei Drittel der Gültigkeitsdauer abgelaufen sind.

Beispiel zur Standardbeschreibungsregel
Gültigkeitsdauer: 1 Tag = 24 Stunden
2/3 der Gültigkeitsdauer: 16 Stunden
Bucht ein Ausweisinhaber bei Arbeitsbeginn und wird sein Ablaufdatum aktualisiert, kann er während des restlichen Tages den Lese-/Schreibleser passieren, ohne dass ein erneuter Schreibvorgang ausgelöst wird - erst nach Ablauf der sechszehn Stunden werden die Daten aktualisiert.
Damit kann z.B. gewährleistet werden, dass nur ein Mal pro Tag der Gültigkeitszeitraum aktualisiert wird.

10 Offline Türen – Anwendungsbeispiele

Anhand der folgenden Beispiele soll deutlich gemacht werden, wie das System für besondere Anforderungen oder Begebenheiten über entsprechende Parametereinstellungen eingerichtet werden kann. Dabei beschränken sich die Beispiele auf einen bestimmten Aspekt.
Weitere Variationen können sich aus der Kombination mit anderen Parametereinstellungen ergeben. Es können demnach auch die Beispiele miteinander kombiniert werden.

Zutrittskontrollleser und/oder schreibfähiger Leser?
Die Entscheidung, wie das DELTA 7020 verwendet werden soll, hängt von einer Reihe verschiedener Faktoren ab. Es kann sinnvoll sein, den Leser nicht in das Zutrittskontrollsystem (online) aufzunehmen.

- Gibt es einen Durchtritt (z. B. Hauptdurchtritt), den die meisten Ausweisinhaber passieren müssen?
  - **Ja**: Es wird ein DELTA 7020 mit gleichzeitiger Zutrittskontrollfunktion für das Online-System empfohlen.
  - **Nein**: (Es gibt zum Beispiel eine Reihe von möglichen Durchtritten): Die Verwendung von DELTA 7020 Lesern an jedem Durchtritt wird aus Kostengründen nicht empfohlen. In diesem Fall sollte der Leser (oder möglicherweise zwei Leser) im frequentiertesten Bereich als einfache Aufladestation installiert werden.
- Sollten Berechtigungserweiterungen jederzeit möglich sein?
  - **Ja**: Es wird ein DELTA 7020 (mit oder ohne Zutrittskontrollfunktion) an den am meisten frequentierten Bereichen empfohlen.
  - **Nein**: (Als Regel werden feste Ablaufdaten verwendet): Wenn die Lese-/Schreibeinheit am Bedienplatz nicht ausreicht, genügt ein DELTA 7020 für diese Ad-hoc-Erweiterungen.

Beispiel 1: Nur Lese-/Schreibeinheit
Idealerweise sollte ein Hotel von allen zugänglich sein, mindestens bis zur Rezeption. Aus diesem Grund sollten Zutrittskontrollleser hauptsächlich an Türen installiert werden, die eine bestimmte Sicherheit erfordern, falls die Einstellungen im **zweiten Beispiel** unter Einzeltüren oder Türgruppen? (siehe unten) nicht ausreichen.
Entsprechend ist ein DELTA 7020 nicht mit den Zutrittskontrollfunktionen verbunden; stattdessen wird er als reine Lese-/Schreibeinheit für das Offline-System konfiguriert.
Bedingung:
Der Parameter **Reader function** (Lesefunktion) unter „BIS Configuration Browser“ > „Connections“ (Anschlüsse) > ... > „Offline locking system“ (Offline-Schließsystem) muss auf **Write locking system** (Schließsystem schreiben) gesetzt werden, und das Kontrollkästchen **Write to card only** (Nur auf Ausweis schreiben) ist aktiviert.
Das DELTA 7020 muss nur für Hotelangestellte an einem zentralen Ort installiert werden, damit ihre Berechtigungen aktualisiert und erweitert werden können. Wählen Sie wenn möglich einen Standort aus, den alle betroffenen Personen regelmäßig passieren, beispielsweise einen Mitarbeiterraum.
Die Berechtigung für die Hotelzimmertür für Hotelgäste wird beim Einchecken zugewiesen und mithilfe eines DELTA 7020 an der Rezeption auf den Ausweis geschrieben. Berechtigungen müssen in der Regel nicht geändert werden, dies erfolgt, sofern erforderlich, an der Rezeption. Daher muss der Leser nicht in einem frei zugänglichen Bereich installiert werden.

Beispiel 2: Lese-/Schreibeinheit mit Zutrittskontrollfunktion

Studentenwohnheime: Hier müssen nur die Bewohner Zutritt haben. Ein Zutrittskontrollleser für den Hauptdurchtritt kann das Gebäude gegen unberechtigten Zutritt schützen. Ein DELTA 7020 kann Schließsystemrechte für autorisierte Personen gleichzeitig aktualisieren und verlängern.

Bedingung:

Die Parameter **Reader function** (Leser-Funktion) muss auf **Write locking system** (Schließsystem schreiben) eingestellt sein, und das Kontrollkästchen **Write card only** (Nur Ausweis schreiben) ist deaktiviert.

Wenn das Kontrollkästchen **Write without access rights** (Schreiben ohne Zutrittsrechte) nicht aktiviert ist, können nur Personen mit Zutrittsberechtigung (online) für den Hauptdurchtritt ihre Offline-Rechte aktualisieren und erweitern.

Einzeltüren oder Türgruppen

Jede im System erstellte Tür kann als individuelle Berechtigung zugewiesen werden und gehört zu einer beliebigen Anzahl von Türgruppen. Die nachfolgenden Beispiele zeigen auf, wie mit diesen zwei Berechtigungsarten umgegangen werden soll.

Beispiel 1: Hotel

An der Rezeption wird die Gültigkeitsdauer für das fragliche Zimmer als **individuelle Berechtigung** entsprechend der Buchung zugewiesen. Beispielsweise ist es auch möglich, eine weitere Türgruppe mit allgemeinen Bereichen (Restaurant, Frühstücksraum, Sauna, Sporteinrichtungen etc.) zuzuweisen, sofern diese Bereiche von einem Terminal gesichert sind.

Demgegenüber wird Hotelangestellten eine **Türgruppe** zugewiesen, die alle (oder mindestens die meisten) Türen umfasst.

Bedingung:

Der Parameter **Türgruppen überprüfen** (Check door groups) muss aktiviert (markiert) sein.

Ablauf:

Der Gast kann die Tür zu seinem Zimmer entsprechend der zugewiesenen individuellen Berechtigung öffnen und kann auch alle Türen in den Türgruppen öffnen. Hotelangestellte können alle Türen in der zugewiesenen Türgruppe öffnen, die auch alle Türen zu den Gästezimmern umfasst.

Beispiel 2: Bereiche innerhalb des Offline-Systems, die erhöhten Sicherheitsanforderungen unterliegen und nur von bestimmten Personen betreten werden können.

Den berechtigten Personen werden diese Türen als individuelle Berechtigungen zugewiesen. Es ist irrelevant, ob diese Türen zu Türgruppen gehören und es ist auch irrelevant, wem diese Türgruppen zugewiesen wurden.

Bedingung:

Das Kontrollkästchen **Check door groups** (Türgruppen überprüfen) muss deaktiviert sein.

Ablauf:

An den Türen werden nur individuelle Berechtigungen akzeptiert. Personen, denen nur Türgruppenberechtigungen für diese Türen zugewiesen wurden, erhalten keinen Zutritt.

Mehr Sondertage pro Jahr

Die Höchstgrenzen für Sondertage (= 10) und Sondertagszeiträume (= 2) beziehen sich auf die zulässige Datenmenge, die gleichzeitig über die Init-Karten in den Terminals gespeichert werden können.

Mit leicht erhöhtem administrativem Aufwand ist es aber möglich, z.B. über einen Jahreszeitraum gesehen, mehr Sondertage und Sondertagszeiträume zu definieren.
Beispiel:
Auf den Terminals sind Ende 2007 die Daten von zehn Sondertagen für das Kalenderjahr 2008 gespeichert worden. Anfang April 2008 können die bereits verstrichenen Sondertage (z.B. Neujahr, Karfreitag, Ostermontag) gelöscht und statt dessen drei neue Termine angelegt werden.
Diese neue Liste muss über die Zeitinit-Karten wieder an die Terminals verteilt werden.

Standard- oder Daueröffnung
Bei einem gültigen Ausweis blinkt die LED des Terminals drei Mal grün. Während der eingestellten Türöffnungszeit (= Standard 3 Sekunden) kann die Tür geöffnet werden. Befindet sich die Tür im Modus **Daueröffnung** blinkt die LED bei einem gültigen Ausweis ebenfalls drei Mal grün.
Ein Ausweis mit der **Erlaubnis für Daueröffnung (Toggle)** kann zur Standardöffnung benutzt werden, indem der Ausweis während des dreimaligen Blinkens wieder entfernt wird. Wird er stattdessen weiterhin vor die Leseeinheit des Terminals gehalten (> drei Sekunden), erfolgt ein grünes Dauersignal und die Tür bleibt so lange offen, bis ein zur Daueröffnung berechtigter Ausweis erneut für mindestens drei Sekunden vor das Terminal gehalten wird. Die Tür wird verschlossen - d.h. es sind nur Begehungen mit berechtigten Ausweisen möglich.
Bedingung:
Auch für das Terminal muss der Parameter **Daueröffnung (Toggle)** gesetzt sein (mit Haken).

Zeitmodellgesteuert:
Die gleiche Funktion kann über ein Zeitmodell gesteuert werden. Zum Türparameter **Öffnungszeitmodell** wird ein Zeitmodell ausgewählt und entsprechend der Intervallzeiten erfolgt die Daueröffnung (von Uhrzeit) oder -schließung (bis Uhrzeit) der Tür.
Zeitmodelle mit der selben Uhrzeit für die von- und bis-Intervallgrenze können zur Schließung dauergeöffneter Türen verwendet werden.

Hinweis!
Zeitmodellgesteuerte Öffnungen enthalten stets das Sicherheitsrisiko, dass unbeaufsichtigte Räume öffentlich zugänglich gemacht werden.

Beispiele: Bürogebäude mit Publikumsverkehr

1. **Manuelle Daueröffnung / -schließung**
   Das Büro wird morgens per Daueröffnungsfunktion geöffnet und für das Publikum frei gegeben. Zum Büroschluss erfolgt die Dauerschließung, so dass ab diesem Zeitpunkt nur noch Personen mit gültigem Ausweis das Büro betreten können.
2. **Zeitmodellgesteuerte Daueröffnung / -schließung**
   Sind die Publikumszeiten nicht mit den Anwesenheitszeiten des Personals identisch, kann die Türöffnung und -schließung auch per Zeitmodell geregelt werden.
   Personalanwesenheit: 8 - 12 Uhr und 13 - 17 Uhr
   Publikumsverkehr: 9 - 11 Uhr und 14 - 16 Uhr
   Um die Zeiten korrekt einzuhalten und eine manuelle Öffnung und Schließung zu vermeiden, kann dies über ein Zeitmodell mit zwei Intervallen, die den Publikumszeiten entsprechen, gewährleistet werden.

3. **Zeitmodellgesteuerte Dauerschließung**
   Das Büro wird morgens vom ersten Mitarbeiter per Daueröffnungfunktion manuell geöffnet. Über ein Zeitmodell deren von und bis Zeit identisch ist, wird zu einem bestimmten Zeitpunkt die zeitmodellgesteuerte Dauerschließung veranlasst.

Siehe

– *Einzeltüren oder Türgruppen, Seite 64*

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

202102231926