Access PE - Offline Locking System

BOSCH

de Installation Manual

Inhaltsverzeichnis

1 Übersicht

Das Access Professional Edition System (im Folgenden als **Access PE** bezeichnet) bietet eigenständige Zutrittskontrolle für kleine und mittelgroße Unternehmen. Es besteht aus mehreren Modulen:

- LAC-Service: ein Prozess, der ständig mit den lokalen Zutrittscontrollern (Local Access Controller, LAC – im Folgenden als Controller bezeichnet) kommuniziert. Als Controller werden AMCs (Access Modular Controller) verwendet.
- Konfigurator
- Personalverwaltung
- Log-Viewer
- Alarmmanagement
- Videoverifikation

Die Module werden in Server- und Client-Module aufgeteilt.
Der LAC-Service muss sich in ständigem Kontakt mit den Controllern befinden, da er erstens von ihnen ständig Nachrichten über Bewegungen sowie An- und Abwesenheit von Ausweisinhabern erhält, zweitens Datenänderungen, z. B. die Zuweisung neuer Ausweise, an die Controller überträgt, aber vor allem deshalb, weil er Prüfungen auf Metaebene durchführt (Zutrittsfolgekontrollen, Zutrittswiederholkontrollen, Mitarbeiterauslosung).
Der Konfigurator sollte ebenfalls auf dem Server ausgeführt werden; allerdings lässt er sich auch auf Client-Bedienplätzen installieren und kann von dort aus betrieben werden.
Die Module Personalverwaltung und Log-Viewer gehören zur Client-Komponente und können zusätzlich auf dem Server oder auf einem anderen PC mit einer Netzwerkverbindung zum Server ausgeführt werden.
Die folgenden Controller können verwendet werden:

- AMC2 4W (mit vier Wiegand-Leserschnittstellen) – kann durch das AMC2 4W-EXT erweitert werden

– AMC2 4R4 (mit vier RS485-Leserschnittstellen)

2 Allgemein

2.1 Benutzeranmeldung

Die folgenden Anwendungen sind verfügbar. Weitere Informationen finden Sie in den entsprechenden Benutzerhandbüchern:

Personalverwaltung

Konfigurator

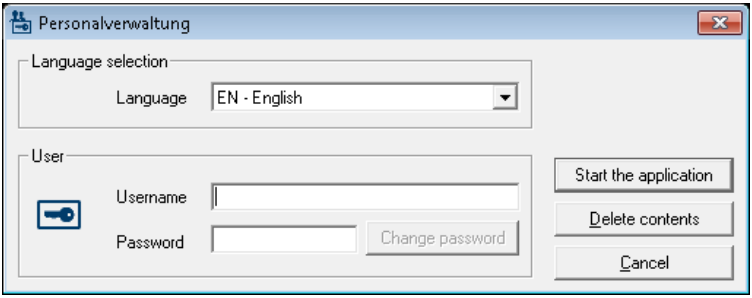
Log-Viewer

Lageplan-Anzeige und Alarmmanagement

Videoverifikation

Die Anwendungen des Systems sind vor unbefugter Verwendung geschützt. Die **Standardzugangsdaten** für die erste Verwendung sind:

- Benutzername: **bosch**
- Kennwort: **bosch**

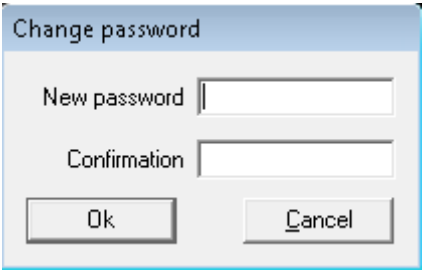


In der oberen Dropdown-Liste kann die gewünschte **Sprache** für die Interaktion ausgewählt werden. Standardmäßig ist die Sprache ausgewählt, die bei der Installation der Anwendung verwendet wurde. Bei einem Benutzerwechsel ohne Neustart der Anwendung bleibt die zuletzt ausgewählte Sprache erhalten. Aus diesem Grund kann ein Dialogfeld in einer unerwünschten Sprache erscheinen. Melden Sie sich erneut bei Access PE an, damit die gewünschte Sprache angezeigt wird.
Anwendungen von Access PE können in den folgenden Sprachen ausgeführt werden:

- Englisch
- Deutsch
- Französisch
- Japanisch
- Russisch
- Polnisch
- Chinesisch (VRC)
- Niederländisch
- Spanisch
- Portugiesisch (Brasilien)

Hinweis!
Alle Einrichtungen, wie Gerätenamen, Bezeichnungen, Modelle und Schemata für Benutzerrechte, werden in der Sprache angezeigt, in der sie eingegeben wurden. Entsprechend werden Schaltflächen und Bezeichnungen, die über das Betriebssystem gesteuert werden, möglicherweise in der Sprache angezeigt, in der das Betriebssystem installiert wurde.

Sobald ein gültiger Benutzername und das entsprechende Kennwort angegeben wurden, wird die Schaltfläche **Kennwort ändern** angezeigt. Über diese Schaltfläche wird ein neues Dialogfenster aufgerufen, in dem das Kennwort geändert werden kann.



Hinweis!
Vergessen Sie nicht, das Kennwort zu ändern!

Über die Schaltfläche **Anwendung starten** werden die Benutzerberechtigungen geprüft, und die Anwendung wird ggf. gestartet. Ist das System nicht in der Lage, die Anmeldung zu authentifizieren, wird die folgende Fehlermeldung angezeigt: **Benutzername oder Kennwort nicht korrekt!**

3 Offline-Schließsystem

Das Offline-Schließsystem ist ein **PegaSys** System von **Normbau** (im Folgenden als „Schließsystem“ oder „Offline-System“ bezeichnet). Es dient dazu, Objekte zu sichern, die nicht online überwacht werden können, sollten oder dürfen.
Offline-Systeme werden in der Regel dort verwendet, wo die Nicht-Echtzeit-Datenübertragung bedeutet, dass die hohe Verfügbarkeit von individuellen Komponenten nicht erforderlich ist, die Infrastruktur keine direkte Verbindung zulässt (z. B. die Verkabelung von Installationen, die weiter entfernt sind) oder die Installation von Online-Komponenten zu teuer ist. 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 (Karten) deaktiviert und sie so unbrauchbar macht.
Offline-Schließsysteme sind in der Regel Installationen mit einer Anzahl von individuellen Bereichen, die zu sichern sind, z. B. Hotels, Studentenwohnheime und Krankenhäuser.
Die PegaSys Komponenten werden im Access PE Zutrittskontrollsystem integriert und von dort aus verwaltet.

3.1 Erläuterung der Begriffe

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

- **Zutrittskontrollsystem**
  Dies bezieht sich auf die Online-Komponenten
  Dazu gehören
-
  - Die Datenerfassungsstufe (Dialogsystem, Datenbank, Logbuch etc.), d. h. oberste Stufe
  - Controller, die anhand der von oberster Stufe empfangenen Daten über den Zutritt entscheiden.
  - Leser, die die Codedaten von den Ausweisen ablesen und diese an die Controller weiterleiten.
- **Schließsystem**
  Darunter fallen die Offline-Schließelemente
-
  - Ausweise, die die Autorisierungsdaten enthalten.
  - Türterminals, die anhand der gelesenen Autorisierungsdaten über den Zutritt entscheiden.

Das Schließsystem als integrierte Einheit nutzt auch teilweise das Dialogsystem und das Zutrittssystem der Controller des und die Leser.

3.2 Besonderheiten des Schließsystems

Bei Zutrittskontrollsystemen (beispielsweise beim Access PE) 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 (= Online-System) zwingend.

Bei Offline-Systemen werden die Zutrittsberechtigungen für gewisse Türen auf dem Ausweis gespeichert. [Die Schließsystemvarianten, für die die Berechtigungen im Türterminal (Armatur oder Zylinder) gespeichert werden, sind hier nicht beschrieben.] 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 Zutrittskontrollsystemen können Karten dieser Art blockiert, gelöscht oder ein Gültigkeitsende zugewiesen werden, während Offline-Systeme keine direkte Intervention zulassen. Um das Risiko von Missbrauch möglichst klein zu halten, werden den Berechtigungen ein Ablaufdatum/ eine Verfallzeit zugewiesen. Wenn diese Frist abläuft, sind die Berechtigungen nicht mehr gültig. Um sie zu reaktivieren, muss die Gültigkeitsdauer verlängert werden. Dies erfolgt über einen Spezialleser mit Schreibfunktion (z. B. DELTA 7020). 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.

3.3 Schließsystem-Komponenten

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

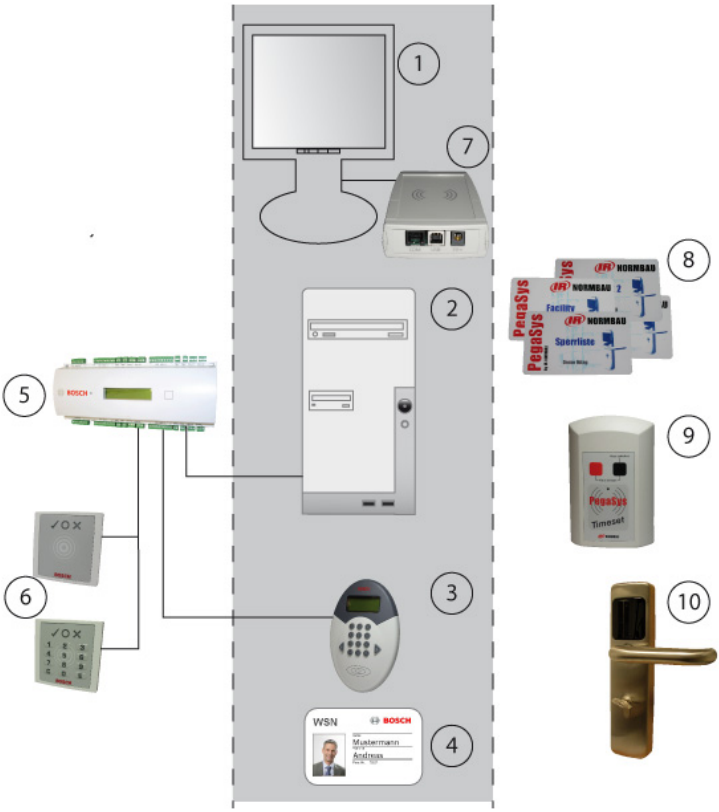
- **Software**
-
  - Konfigurator > **Offline-Schließsystem**

Diese Anwendung wird verwendet, um die Funktionen einzurichten und die allgemeinen Einstellungen vorzunehmen, Zeitmodelle zu erstellen und Türen und Türgruppen zu konfigurieren.

- Konfigurator > **Durchtritte**
  Bein Einstellen von Durchtritten können Schreibfunktionen für die Leser aktiviert und konfiguriert werden.
- Personalverwaltung > **Personaldaten**
  Dieser Dialog enthält (nach der Initialisierung mit einem Kundencode) eine weitere Registerkarte mit dem Namen **Offline-Zutrittsberechtigungen**; hier können Sie Berechtigungen zuweisen und Ausweise für das Schließsystem aufzeichnen.

- **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 Offline-Systemdaten verarbeiten, verbunden sein.
  - Ein **mobiles Lese-/Schreibgerät** (Timesetter), das Tür- und Zeitmodell-Initialisierungsausweise aktualisiert, die im Gegenzug dazu verwendet werden, die Türterminals zu aktualisieren/initialisieren (optional).
  - **Terminals** zum Lesen der Benutzer- und Systemausweise an den Türen im Schließsystem.
  - Mindestens ein schreibfähiger Leser für die Verteilung und Erweiterung der Zutrittsberechtigungen für das Schließsystem.

3.4 Systemübersicht



Wenn das Schließsystem in das Access PE 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. Die Elemente links sind reine Zutrittskontrollinstallationen und die Elemente rechts gehören nur zum Schließsystem.

1. Arbeitsplatz
2. Server mit Konfigurationsanwendung und Datenbank

3. Zutrittskontrollleser mit Schreibeinheit („schreibfähiger Leser“)
4. Ausweis – für beide Systeme
5. AMC2 4R4 Zutrittskontrollpanel
6. Zutrittskontrollleser
7. Dialogeinheit zum Lesen und Schreiben von Online- und Offline-Systemdaten
8. Verschiedene Systemausweise für das Schließsystem
9. Mobile Lese-/Schreibeinheiten für Daten-/Zeitstempel
10. Türterminal mit Leseeinheit

3.4.1 Beschreibung von Systemkomponenten

Die folgenden Abschnitte beschreiben die oben aufgeführten Komponenten für beide Systeme und fokussieren sich hauptsächlich auf die Funktion allgemeiner Elemente.

Arbeitsplatz

Die gleiche Dialogschnittstelle **1**] wird verwendet, um Personaldaten für das Zutrittskontrollsystem und für das Schließsystem zu erstellen. Um sowohl Zutrittsberechtigungen für das Access PE und Zutrittsrechte für das Offline-Schließsystem zuzuweisen, ist nur ein einzelner Schritt erforderlich.
Listen mit einem Überblick über den Status der Berechtigungszuweisungen für das Schließsystem können über das gleiche Menüelement abgerufen werden, das auch für die Zutrittskontrolle verwendet wird.

Server

Die Software für das Zutrittskontrollsystem und das Schließsystem wird auf diesem Computer ausgeführt**2**]. Der Access PE Konfigurator wird auch für die Konfiguration der Leser [**3**] für das Schließsystem verwendet.
Daten für das Offline-System werden in speziellen Tabellen der Access PE Datenbank verwaltet.

Schreibfähige Leser

Mindestens ein Leser dieses Typs [**3**] muss 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 Rechte nicht automatisch erweitert werden, sondern speziell angefordert werden müssen.
Ein RS485 Leser wird auf einem AMC2 4R4 mit L-Bus-Protokoll zum Einrichten konfiguriert.

Hinweis!
Aktivieren Sie für diesen Leser keine Videoverifikation.
Dieser Lesertyp kann nicht zur Scharfschaltung/ Unscharfschaltung (DM 10 und 14) verwendet werden.

Ausweis

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

Hinweis!
Für das Offline-System kann nur ein Ausweis 1 einer Person verwendet werden.

AMC2 4R4 Controller

Ein AMC2 4R4 L-Bus [**5**] (= Zutrittskontrollpanel mit RS485 Leserschnittstelle) ist für den schreibfähigen Leser[**3**] erforderlich, der als Lese-/Schreibeinheit für das Schließsystem verwendet wird.

Die Leser, die nur für die Zutrittskontrolle bestimmt sind [**6**], können beliebige Protokoll- und Leseprozesse verwenden und können mit einer beliebigen AMC2-Variante betrieben werden.

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

Dialogeinheit zum Lesen und Schreiben
Dieses Gerät [**7**] ist direkt über eine USB-Schnittstelle mit dem Bedienplatz-Rechner verbunden und dient dazu, Berechtigungen auf Benutzerausweise und systembezogene Daten (z. B. Tür-und Zeitinitialisierungsdaten) auf spezielle Systemausweise zu übertragen [**8**]. Es wird auch dazu verwendet, Online-Ausweise anzumelden.

Systemausweise
Unterschiedliche Systemausweise [**8**] (Zeit-, Tür- und Kundenausweise) sind für das Schließsystem zur Übertragung von relevanten Daten – z. B. Initialisierungsdaten – an die Türterminals erforderlich [**9**].

Mobile Lese-/Schreibeinheiten (optional) - Timesetter
Damit die Terminals aktualisiert werden können, werden die aktuellen Terminal-Initialisierungsdaten über diese Einheit auf Tür- und Zeitmodell-Initialisierungsausweise geschrieben.

PegaSys - Türterminal
Diese Leseeinheit verwendet die individuelle Türidentifikation oder die eigene Türgruppenidentifikation, um die Zutrittsrechte für die Ausweisinhaber zu überprüfen.

Die Zutrittsrechte auf dem Ausweis müssen laufend über Spezialleser mit Schreibfunktion aktualisiert werden [**3**]. Wenn eine Notöffnung erforderlich wird, z. B. wenn die Elektronik versagt, haben die Terminals mechanische Zylinderschlösser.

3.4.2 Systemgrenzen

Die folgenden Werte gelten als obere Grenze für einzelne Installationen im Schließsystem.

Durchtritte (Türen)	Es gibt keine Einschränkungen im Bezug auf die Erstellung und Konfiguration von Durchtritten. Die Anzahl, die einzelne Türberechtigungen zugewiesen werden kann, hängt von der Länge des bestellten Datensatzes ab, vgl. , *Seite 18*.
Türgruppen	Die maximale Anzahl hängt von der Länge des Datensatzes für Offline-Daten ab; vgl. , *Seite 18*.
Zeitmodelle	15
Zeiträume/Zeitmodell	4
Feiertage	10

Türgruppen **Einzelne Türen**	**256**
2	48

Tabelle 3.1: Die Zahlen beziehen sich auf die Datensatzlänge in Byte.

Hinweis!

Bei der Verwendung von **Hitag1**-Ausweisen können nur zwei einzelne Türen erstellt werden; auf die selbe Art können nur 240 (anstelle der definierten 256) Türgruppen erstellt werden – hier sind keine weiteren Formate 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.

3.5 Access PE – Konfigurator

Es sind spezielle schreibfähige Leser erforderlich, um Zutrittsberechtigungen für das Schließsystem zu erweitern oder zu erneuern.
Diese Leser mit Schreibfunktion werden als Zutrittskontrollleser erstellt und es werden ihnen in der Regel auch Türkontrollfunktionen zugewiesen. Sie können aber auch nur als „Auflader“ für Offline-Systemberechtigungen verwendet werden.

3.5.1 Hinzufügen von Hardware-Komponenten

IIm Access PE Zutrittskontrollsystem sind keine spezifischen Lesertypen ausgewählt, wenn Hardware-Komponenten hinzugefügt werden; das entsprechende Protokoll, das von den AMCs verwendet wird, wird für jeden Leser ausgewählt.
Um Schließsystemkomponenten hinzuzufügen und zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Starten Sie den Access PE **Konfigurator**.
- Wechseln Sie zur Registerkarte **Einstellungen**.
-
  - Fügen Sie einen **AMC2 4R4 L-Bus** hinzu.
- Wechseln Sie zur Registerkarte **Durchtritte**.
-
  - Fügen Sie einen Durchtritt mit einem beliebigen Türmodell (ausgenommen DM 10 und 14) und einen oder zwei **RS485** Leser hinzu. Mindestens ein schreibfähiger Leser muss an diesem Durchtritt verfügbar sein.

– Wählen Sie für den schreibfähigen Leser im Feld **Schreibzugriff lesen/schreiben**.
– Bestätigen Sie den neuen Eintrag mit **OK**, um den Dialog zu schließen.
– Für die Leseroptionen setzen Sie die Parameter **Zutritt bei Schreibfehler** und **Schreiben ohne Zutrittsrechte**, sofern diese auf Ihr System zutreffen.

3.5.2 Den schreibfähigen Leser konfigurieren

Wenn dieser Leser auch als Zutrittskontrollleser verwendet wird und die Einstellungen von den Standardeinstellungen abweichen, konfigurieren Sie ihn entsprechend Ihren Anforderungen. Weitere Informationen über die fraglichen Parameter finden Sie im Abschnitt „Durchtritte hinzufügen“.

Hinweis!
Aktivieren Sie für diesen Leser keine Videoverifikation. Dieser Lesertyp kann nicht zur Scharfschaltung/ Unscharfschaltung (DM 10 und 14) verwendet werden.

Die folgenden Parameter sind für das Schließsystem wichtig.

Zutritt schreiben	**nur Lesezugriff** Dieser Leser ist ein reiner Zutrittskontrollleser und nicht Teil des Schließsystems. **Lesen/Schreiben** Dieser Leser hat Zutrittskontrollfunktionen und ist auch für das Schließsystem aktiviert.
Zutritt bei Schreibfehler gewähren	Die Zutrittsüberprüfung und Absicherung (im Online-System) hängt nicht vom Erfolg des Schreibprozesses des Schließsystems ab. Die Tür wird nach mehreren fehlgeschlagenen Schreibversuchen freigegeben. **Deaktiviert** (deaktiviert): Wenn es nicht möglich ist, auf den Ausweis zu schreiben, wird der Zutritt ebenfalls verweigert. **Aktiviert** (aktiviert): Der Schreibprozess hat keinen Einfluss auf die Zutrittsüberprüfung.
Ohne Zutrittsrechte schreiben	Rechte für das Schließsystem werden nur auf den Ausweis geschrieben, wenn der Ausweisinhaber die (online) Zutrittsberechtigung für den Durchtritt hat. **Deaktiviert** (deaktiviert): Daten werden nur auf den Ausweis geschrieben, wenn eine gültige Berechtigung vorliegt. **Aktiviert** (aktiviert): Daten werden immer auf den Ausweis geschrieben.

Hinweis!
Wenn der Parameter deaktiviert ist, wird der Schreibprozess untersagt, selbst wenn die Berechtigungen nur vorübergehend ungültig sind (z. B. wenn Zeitmodelle verwendet werden).

3.5.3 Das Leserprotokoll umschalten

In der Regel werden Leser mit Schreibfunktionen an zentralen 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.
Wenn in der Folge das Offline-System eingerichtet wird, muss mindestens ein Leser am Standort mit einem schreibfähigen Leser ersetzt werden. Wenn dazu wieder eine Durchtritt hinzugefügt werden muss, würde der bestehende Durchtritt gelöscht und müsste zusammen mit dem schreibfähigen Leser wieder hinzugefügt werden.
Wenn der bestehende Durchtritt gelöscht wurde, würde dieser auch aus allen Zutrittsberechtigungen gelöscht. Es müssten deshalb alle Berechtigungen dem neuen Durchtritt hinzugefügt werden.
Um diesen mühseligen Prozess zu verhindern, der zu Fehlern führen könnte, kann der fragliche AMC neu konfiguriert werden.

- Gehen Sie im Access PE Konfigurator zur Registerkarte **Einstellungen** .
- Wählen Sie aus dem Listenfeld den relevanten AMC aus.
- Klicken Sie auf die Schaltfläche  , um das Dialogfenster zum Bearbeiten zu öffnen.
-
  - Wählen Sie im Feld **Geräteart** den Eintrag **AMC2 4R4 L-Bus**.
  - Testen Sie den AMC, damit die neue Software heruntergeladen wird und bestätigen Sie die Änderungen mit **OK**.

– Speichern Sie die Änderungen  und senden Sie diese an den LAC-Serviceprozess  .

Hinweis!

Andere Leser auf diesem AMC müssen dieses Protokoll ebenfalls verstehen. Wenn nötig müssen diese Leser auch ersetzt werden.

Wenn Sie den Gerätetyp von AMC2 4W auf AMC2 4R4 L-Bus geändert haben, muss der AMC auch ersetzt werden.

3.6 Konfigurator - Offline-Schließsystem

in diesem Dialog, auf den Sie über die Werkzeugleiste

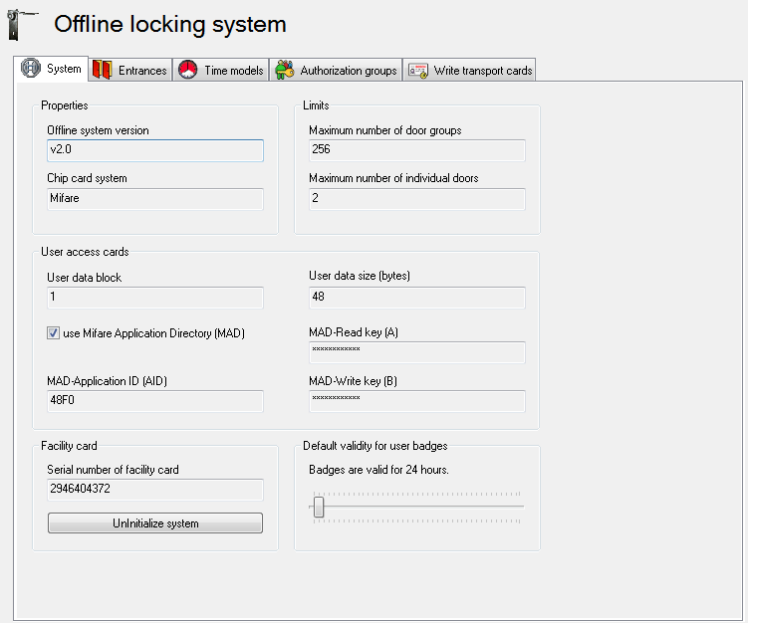
„Konfigurator“ mit einem Klick auf die Schaltfläche zugreifen können, werden die notwendigen Schließsystemeinstellungen auf fünf unterschiedlichen Registerkarten konfiguriert. Im Interesse der Benutzerfreundlichkeit haben die Registerkarten für die Konfiguration des Schließsystems die gleichen Namen und Symbole wie die entsprechenden Dialoge der Zutrittskontrolle. Soweit dies in Anbetracht der spezifischen Datenstruktur des Offline-Systems möglich war, wurden die Struktur- und Datenverarbeitungsmerkmale des Online-Konfigurationsprozesses ebenfalls verwendet.
Die individuellen Registerkarten werden für die Verwaltung folgender Daten verwendet:

- **System**
  Spezielle Offline-Systemdaten wie Systemgrenzen, Schlüssel und Seriennummern.
- **Durchtritte**
  Wie im Dialog mit dem gleichen Namen im Zutrittskontrollsystem werden hier die Durchtritte verwaltet, aber in diesem Fall die Schließsystemzutritte.
- **Zeitmodelle**
  Da das Offline-System die Zutrittskontrollzeitmodelle nicht verwenden kann, müssen diese, sofern sie erforderlich sind, separat für das Schließsystem aufgesetzt werden.
- **Berechtigungsgruppen**
  Wie beim gleichnamigen Dialog im Zutrittskontrollsystem wird diese Registerkarte ebenfalls dazu verwendet, eine Reihe von Durchtritten im Schließsystems in Berechtigungsgruppen zu kombinieren.
- **Transportausweise schreiben**

Um aktualisierte Daten über die Schließsysteminstallationen zu erhalten, können einzelne Durchtritte und Zeitmodelle auf Transportausweise geschrieben werden. Diese werden von den Terminals gelesen.

3.6.1 Offline-Schließsystem: System

Beim Kauf des Schließsystems erhält der Kunde unter anderem einen „Kundenausweis“. Dieser enthält Details über die Systemeinstelllungen, die der Kunde auf dem Bestellformular des Herstellers angegeben hat.
Alle Felder auf dieser Seite sind schreibgeschützt und können nicht überschrieben werden. Der Inhalt wird vom Kundenausweis gelesen und in die entsprechenden Felder eingetragen.
Bevor das Schließsystem eingerichtet wird: Das Dialogfeld unten auf der Seite des **Kundenausweises** enthält die Schaltfläche **System mit Kundenkarte initialisieren**. Die Systemdaten werden übertragen und eingerichtet, wenn die Kundenkarte auf den Dialogleser für das Offline-System gelegt und die Schaltfläche angeklickt wird.



Eigenschaften Dialogfeld

– **Offline-Systemversion**
  Softwareversion des Schließsystems – im Access PE werden nur Version V2.0 Funktionalitäten verwendet.
– **Chipausweissystem**
  Zeigt die Ausweistechnologie – MIFARE classic und Hitag 1 können für Access PE verwendet werden.

Schränkt Dialogfeld ein
– **Maximale Anzahl der Türgruppen**
  Maximal mögliche Anzahl der Zutrittsberechtigungsgruppen.
– **Maximale Anzahl einzelner Türberechtigungen**
  Maximal mögliche Anzahl der einzelnen Türberechtigungen.

Diese Einträge korrelieren miteinander und definieren die verfügbare Länge des Datensatzes [=Benutzerdatengröße (Byte)] auf den Ausweisen – vgl. auch *, Seite 18*.

Dialogfeld **Benutzerzutrittsausweise**
– **Benutzerdatenblock**
  Details auf dem Ausweissektor, in dem der Offline-Datenschreibprozess beginnt.
– **Benutzerdatengröße (Byte)**
  Länge des Datensatzes – bestimmt auch die maximalen Werte für die Berechtigungen.

Hinweis!
Bei Verwendung von Hitag 1 sollten diese Werte überprüft werden, wenn ein System zum ersten Mal eingerichtet wird, da diese Ausweisarten keine Funktion haben, Bereiche, die bereits verwendet werden, vor dem unbeabsichtigten Überschreiben zu schützen.

Daten werden nur in die nachfolgenden vier Felder geschrieben, wenn MAD in der MIFARE Ausweistechnologie aktiviert wurde.
– **Mifare Applikation Directory (MAD)** verwenden

Wenn dieses Kontrollkästchen aktiviert (markiert) ist, werden die Daten für die andern MAD-Felder ebenfalls angezeigt.
Wenn MAD aktiviert ist, entspricht der Benutzerdatenblock einfach dem Standardbereich und wird für jeden Benutzerausweis dynamisch definiert, wenn der betreffende Block besetzt ist.

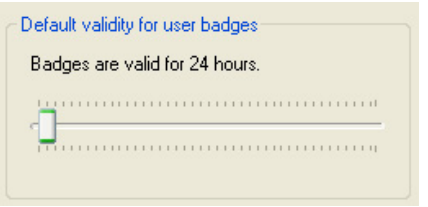
– **MAD-Application ID (AID)**
Identifikationsnummer für das MAD auf diesem System.
– **MAD-Leseschlüssel (A)**
Leseschlüssel für dieses System.
– **MAD-Schreibschlüssel (B)**
Schreibschlüssel für dieses System.

Dialogfeld **Kundenausweis**

– **Seriennummer des Kundenausweises**
Seriennummer auf dem Kundenausweis, der eingelesen wurde – wenn diese Seriennummer gespeichert wird, kann der Kundenausweis nicht überschrieben werden.

Dialogfeld **Standardgültigkeit für die Zutrittsausweise**

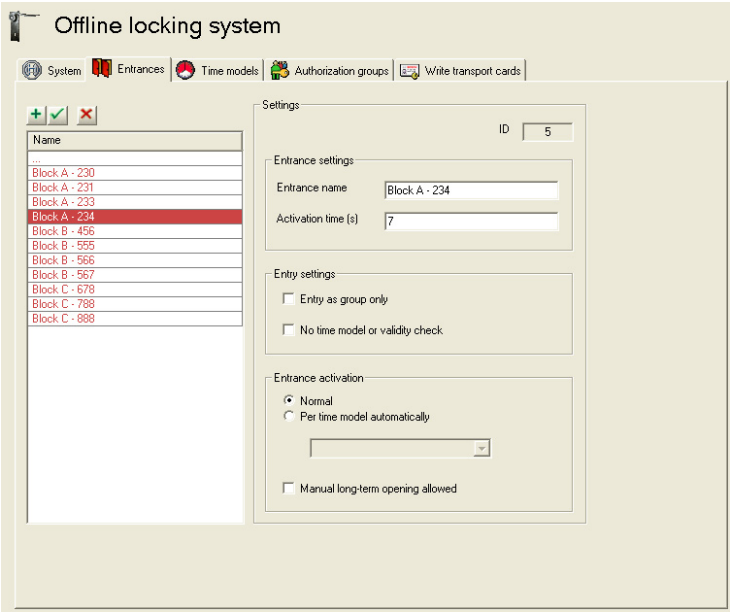
– Verwenden Sie den Schieber, um die Standardgültigkeitsperiode in Stunden für die Zutrittsausweise des Offline-Systems einzustellen. Es können Werte von 1 bis 1000 verwendet werden. Halten Sie die linke Maustaste und schieben Sie, um den ungefähren Wert zu setzen. Verwenden Sie dann die Pfeiltasten, um den Wert auf die Stunde genau zu setzen.



Das Offline-Schließsystem wird unmittelbar nach der Initialisierung innerhalb der angezeigten Grenzen aktiviert. Die Registerkarte **Offline-Zutrittsberechtigungen** wird nun unter Personalverwaltung angezeigt.

3.6.2 Offline-Schließsystem: Durchtritte

In diesem Dialog muss für jeden Türterminal im Schließsystem ein Listeneintrag erstellt und konfiguriert werden. Sie können dann bestimmten Türgruppen zugewiesen werden.



Das Listenfeld enthält alle Durchtritte, die eingerichtet und mit Schließsystemterminals ausgestattet wurden. Die Schaltfläche über der Liste ermöglicht es, neue Listeneinträge zu erstellen  und bestehende Einträge zu bearbeiten  oder zu löschen  .

Die Parameter für den ausgewählten Durchtritt in der Liste werden in den Feldern rechts angezeigt. Hier können sie eingegeben und bearbeitet werden.

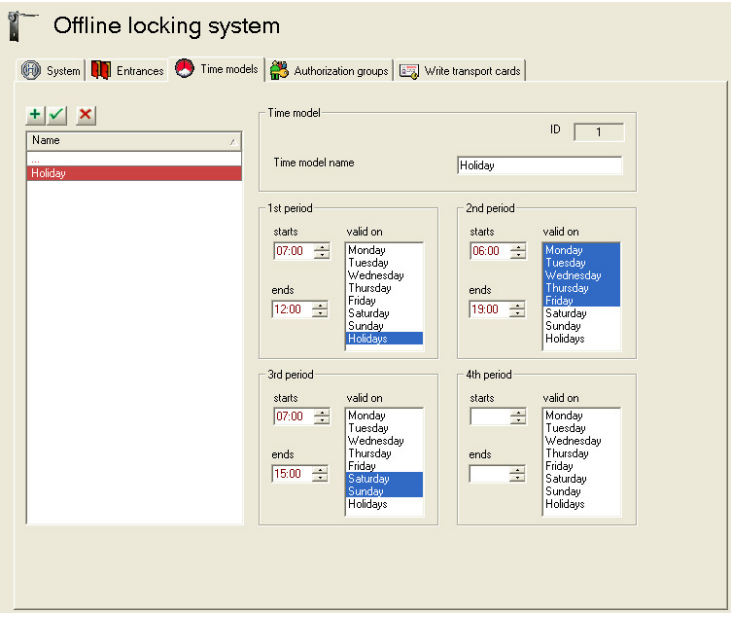
Parameter	**Beschreibung**
Kennung	Vom System zugewiesen, wenn der Listeneintrag erstellt wird, kann nicht bearbeitet werden. Sequentielle Zahl, die den Datensatz eindeutig identifiziert.
Durchtrittseinstellungen	
Durchtrittsname	Der Durchtritt kann über den Namen präziser definiert werden. Max. 29 Zeichen
Aktivierungszeit(en)	Eintrag in Sekunden definiert, wie lange die Tür nach der positiven Überprüfung offen bleibt. (Standard = 7).
Eintragseinstellungen	
Eintritt nur als Gruppe	Eine Gruppe definiert sich als zwei Personen. Damit wird sichergestellt, dass das Doppelkontrollprinzip verwendet wird, da es immer notwendig ist, dass zwei berechtigte Personen Ihre Ausweise an diesen Durchtritten scannen, damit die Tür geöffnet wird. Bietet erhöhte Sicherheit.

Parameter	Beschreibung
Keine Zeitmodell- oder Gültigkeitsprüfung	Wenn diese Option aktiviert ist, wird nur die allgemeine Berechtigung für diesen Durchtritt überprüft – Einschränkungen wie Zeitmodelle oder Ablaufdaten werden ignoriert. Bietet verringerte Sicherheit.
Durchtrittsaktivierung	
Normalbetrieb	Jede berechtigte Person kann die Tür aus Zutrittsgründen öffnen. Wenn der Parameter **Manuelles langfristiges Öffnen erlaubt** gesetzt ist und der Ausweisinhaber die entsprechende Berechtigung hat, ist die Dauerfreigabe ebenfalls möglich.
Pro Zeitmodell automatisch	Außerhalb des Zeitmodells = Normalbetrieb Innerhalb = Dauerfreigabe Zum automatischen Schließen wird nur die Endzeit der Perioden gesetzt.
Manuell langfristig öffnen erlaubt	Das langfristige Öffnen der Tür ist nur möglich, wenn dieser Parameter gesetzt und der Ausweisinhaber für diese Funktion berechtigt ist. Ein Ausweis mit der Berechtigung muss ebenfalls während 5 Sekunden an den Türterminalleser gehalten werden.

3.6.3 Offline-Schließsysteme: Zeitmodelle

Das Listenfeld enthält alle festgelegten Zeitmodelle. Die Schaltfläche über der Liste kann dazu verwendet werden, weitere Listeneinträge zu erstellen , bestehende Einträge zu bearbeiten oder zu löschen .

Die Parameter für den ausgewählten Durchtritt in der Liste werden in den Feldern rechts angezeigt. Hier können sie eingegeben und bearbeitet werden.



Parameter	Beschreibung
Zeitmodell	
Kennung	Vom System zugewiesen, wenn der Listeneintrag erstellt wird, kann nicht bearbeitet werden. Sequentielle Zahl, die den Datensatz eindeutig identifiziert. Es können maximal 15 Zeitmodelle für das Schließsystem definiert werden.
Zeitmodellname	Das Zeitmodell kann über den Namen präziser definiert werden. Max. 29 Zeichen
1. 1. Periode bis 4. Periode	
beginnt ... endet	Anfangs- und Endzeit der betreffenden Periode. Wenn nur Endzeiten definiert werden, können diese Zeitmodelle für die automatische Türschließung verwendet werden.
gültig am	Tage der Woche sind ausgewählt, an denen die Periode gültig ist. Einträge werden ausgewählt, indem mit der Maus darauf geklickt wird – ausgewählte Tage sind in Blau angezeigt. Um die Auswahl aufzuheben, klicken Sie erneut darauf.

Feiertage

Feiertage und Sondertage werden von der Liste im Online-System abgerufen.

Im Dialog **Sondertage** können bis zu zehn Feiertage für das Offline-System ausgewählt werden, indem die Parameter **aktiv für Offline-Schließsystem** aktiviert werden. Unabhängig von der

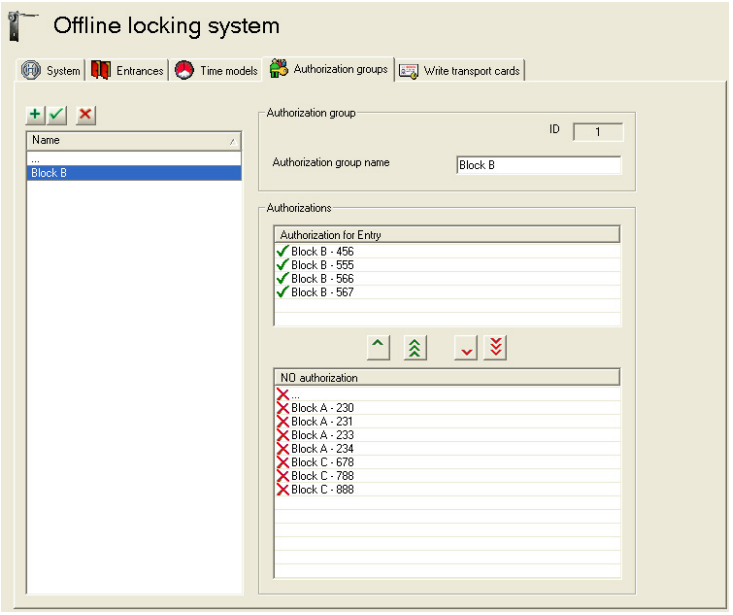
Kategorie, die den Feiertagen für das Online-System zugewiesen wird oder dem Aktivierungsstatus in diesem System, können sie als Feiertag im Offline-System verwendet werden.
Eine Aktivierung für das Schließsystem ist unabhängig von der Verwendung des Feiertags im Zutrittskontrollsystem – dies bedeutet, dass Feiertage, die für das Online-System deaktiviert wurden, trotzdem im Offline-System aktiviert werden können.

Zeitmodelle versus Zeitperioden
Ein Zeitmodell kann bis zu vier Zeitperioden in einen 24-Stunden-Tag enthalten. Das Definieren von Anfangs- und Endzeiten einer Periode bedeutet, dass in dieser Periode, verglichen mit dem Rest des Tages, eine andere Regelung gilt (z. B. Tür dauerhaft freigeben). Die Perioden können beliebig lang sein und sich überschneiden. Wenn nur Endzeiten definiert werden, können diese für die automatische Türschließung verwendet werden, wenn sie aber bestimmten Personen zugewiesen sind, haben sie überhaupt keinen Zutritt.
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.
Die Gesamtheit aller Zeitperioden und deren Zuweisungen auf die Tage ergibt das Zeitmodell, das als Einheit im System verwendet werden kann.

3.6.4 Offline-Schließsystem: Berechtigungsgruppen

Das Listenfeld enthält alle Berechtigungsgruppen, die festgelegt wurden. Die Schaltfläche über der Liste dienen dazu, weitere Listeneinträge zu erstellen  , bestehende Einträge zu bearbeiten  oder zu löschen  .

Die Parameter für den ausgewählten Durchtritt in der Liste werden in den Feldern rechts angezeigt. Hier können sie eingegeben und bearbeitet werden.



Parameter	**Beschreibung**
Berechtigungsgruppe	
Kennung	Vom System zugewiesen, wenn der Listeneintrag erstellt wird, kann nicht bearbeitet werden. Sequentielle Zahl, die den Datensatz eindeutig identifiziert. Die Zahl der Türgruppen, die erstellt werden können, hängt von der Datengröße ab (, *Seite 18*) und entspricht den Daten für die **Maximale Anzahl Türgruppen** in der Registerkarte **System**.

Parameter	Beschreibung
Gruppenberechtigungsname	Die Berechtigungsgruppe kann über den Namen präziser definiert werden. Max. 29 Zeichen
Berechtigungen	
Zutrittsberechtigung	Alle Durchtritte, die vom unteren Listenfeld zugewiesen wurden, für die die Zutrittsberechtigung gewährt wurde.
KEINE Berechtigung	Alle Türen im Offline-System, die in der Registerkarte **Durchtritte** definiert wurden, aber nicht auf das obere Listenfeld übertragen wurden.

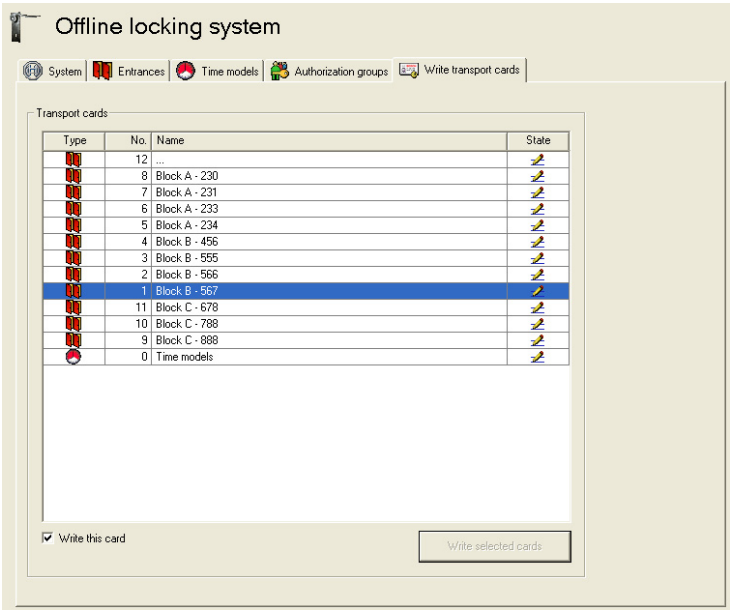
Einzel ausgewählte Einträge können dem oberen Listenfeld ˄ hinzugefügt oder von dort ˅ entfernt werden. Verwenden Sie die Pfeiltasten, um zwischen den beiden Listenfeldern zu navigieren. Es ist ebenfalls möglich, alle Einträge von einer Liste auf die andere zu übertragen ⩔ oder ⩖.

Hinweis!

Die Segmentierung der Ausweise lässt im Vergleich zu den Türgruppen nur eine relativ geringe Allokation von einzelnen Türen zu. Aber in Anbetracht dessen, dass einzelne Türberechtigungen nur für besondere Umstände verwendet werden, dass Berechtigungen für bestimmte Türen in der Regel in Kombination mit einer Reihe von Türen zusammen in einer Türgruppe zugewiesen werden und dass es ebenfalls möglich ist, eine Türgruppe mit nur einer Tür zu bilden, ist die Zahl der zugelassenen einzelnen Türberechtigungen ausreichend.

3.6.5 Offline-Schließsystem: Schreiben von Transportausweisen

Im Gegensatz zum Online-System 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. In der *Systemübersicht, Seite 13* wurden bereits verschiedene Systemausweise erwähnt, einschließlich **Türinitialisierungs-** und **Zeitmodell**ausweise, auf die Türparametereinstellungen und Zeitmodelle geschrieben und die an den Türterminals gescannt werden.



Transportausweise für Türen (Türinitialisierungsausweise)

Das Listenfeld auf der Dialogseite **Transportausweis schreiben** enthält für jede einzelne konfigurierte Türe einen Eintrag. Um die Auswahl zu erleichtern und den Schreibprozess auszuführen, sind die Türen, für die Transportausweise geschrieben werden

müssen, in der Liste nach der Konfiguration markiert. Wenn der entsprechende Listeneintrag ausgewählt wird und das Kontrollkästchen **Diesen Ausweis schreiben** aktiviert ist (oder wenn ein Doppelklick auf den Listeneintrag erfolgt), werden diese Einträge dem Symbol in der Spalte **Status** zugewiesen und deshalb für den nächsten Schreibprozess ausgewählt. Zusätzlich zu diesen Identifikationsmerkmalen werden die nicht ausgewählten Türen grau hinterlegt dargestellt.
Die Schaltfläche **Ausgewählten Ausweis schreiben** wird verwendet, um den Dialogleser zu aktivieren; dieser schreibt **für jede Türe einen separaten Transportausweis**.

Hinweis!
Bitte stellen Sie sicher, dass die erforderliche Anzahl Transportausweise für die ausgewählte Anzahl Türen verfügbar ist.

Ein Dialogfeld fordert Sie auf, den Ausweis in Position zu legen und zeigt dann den Fortschritt des Schreibprozesses an.
Wenn die Türdaten auf den Transportausweis, der in Position ist, geschrieben wurde, wird der Benutzer aufgefordert, einen neuen Ausweis für den nächsten Datensatz in Position zu legen.

Hinweis!
Türdaten enthalten Informationen über Berechtigungsgruppen, denen die Türen zugeordnet sind.

Bei Verwendung von mehreren Türinitialisierungsausweisen sollten diese klar markiert werden, damit die Daten der korrekten Tür zugewiesen werden können. Aus diesen Grund werden die Daten auf dem Ausweis gelöscht, nachdem der Türinitialisierungsausweis am relevanten Terminal gescannt wurde.

Transportausweise für Zeitmodelle (Zeitmodellausweise)
Es gibt auch einen Listeneintrag für das Zeitmodell, dieser wird immer am Ende der Liste hinzugefügt. Im Gegensatz zu den Türen werden die Zeitmodelle zusammen kombiniert und alle zusammen – bis zu 15 – werden mit der aktuellen Zeit auf einen einzelnen Ausweis geschrieben.
Entsprechend werden **alle** Zeitmodelle ebenfalls an **allen** Türterminals gescannt.

Überprüfung der Ausweisart
Bevor der aktuelle Ausweis geschrieben wird, überprüft das System, ob es sich tatsächlich um einen Türinitialisierungsausweis handelt. Wenn der Ausweis bereits auf eine andere Art codiert wurde (z. B. als Benutzer- unter Kundenausweis), wird eine Warnung angezeigt.

3.6.6 Aktualisierung von Datum und Uhrzeit

Zusätzlich zu den Tür- und Zeitmodelldaten wird der aktuelle Zeitstempel (Datum/Uhrzeit) ebenfalls auf den Transportausweis geschrieben. Abhängig von der Größe der zu sichernden Einrichtung kann eine gewisse Verzögerung eintreten, bevor die Ausweise an den Türen gescannt werden können. Die Zeitverzögerung erhöht sich beträchtlich mit der Anzahl der zu konfigurierenden Türen, insbesondere bei Zeitmodellausweisen.
Um möglichst genau Zeitdaten zu erhalten, besonders wenn die Ausweise gescannt werden, sollte ein **mobiles Lese-/Schreibgerät** (Timesetter) verwendet werden. Mit dieser Einheit können die Zeiten auf den Transportausweisen unmittelbar vor dem Scannen am Terminal aktualisiert und sichergestellt werden, dass die Zeitverzögerung in einem vertretbaren Rahmen bleibt.

Systemausweise scannen

1. Der Timesetter muss zuerst mit den kundenspezifischen Daten initialisiert werden. Dazu muss der Kundenausweis einmal "getauft" werden.
2. Zusätzlich zu den Tür- und Zeitmodelldaten enthalten die oben beschriebenen Transportausweise (Türinitialisierungs- und Zeitmodellausweise) auch die aktuelle Systemzeit. Diese können verwendet werden, um dem Timesetter die Zeitdaten zur Verfügung zu stellen.
3.
   - Legen Sie den Systemausweis (Kunden- oder Transportausweis) auf den Leserkopf des Gerätes (graues Feld).
   - Drücken Sie die Taste **1**.
   - Halten Sie die Taste **1** gedrückt und drücken Sie dann die Taste **2**.

Die Transportausweise werden geschrieben

Unmittelbar bevor die Transportausweise gescannt werden, sollten die Zeitdaten aktualisiert werden – Tür- und Zeitmodelldaten sind davon nicht betroffen.

- Legen Sie die Transportausweise (Türinitialisierungs- oder Zeitmodellausweise) auf den Leserkopf des Gerätes (graues Feld).
- Drücken Sie die Taste **2**.

Hinweis!
Der Schreib- und Leseprozess wird durch eine LED-Anzeige angezeigt. Erläuterungen zu den Farbfolgen finden Sie unter *LED Displaysignale, Seite 59*.

3.6.7 Registrieren von Ausweisen

Izusätzlich zu den Transportausweisen für die Türen und die Zeitmodelle; andere Spezialausweise können ebenfalls für den Datentransfer im Offline-System verwendet werden. Sie werden

Zutritts- oder Registrierungsausweise genannt; diese werden verwendet, um Aufzeichnungen von Zutrittsversuchen von den Türterminals zu kopieren und auf das Managementsystem zu übertragen.
Erfolgreiche und fehlgeschlagene Öffnungsversuche 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.
Die unterschiedlichen Ausweisarten lassen unterschiedliche Anzahl Registrierungen zu, die auf den Ausweis geschrieben werden: Hitag 1 enthält 32, MIFARE classic enthält 244. Sie müssen genügend Registrierungsausweise erstellen und die entsprechenden Abruffristen festlegen.

Lesen der Registrierungen am Terminal
Der Systemausweis wird gegen die Lesereinheit des entsprechenden Terminals gehalten. Während die LED-Anzeige orange leuchtet, schreibt der Terminal Daten auf den Registrierungsausweis. Wenn die LED-Anzeige dreimal grün aufleuchtet, wurden die Registrierungen erfolgreich auf den Ausweis geschrieben. Wenn der Registrierungsausweis während dem Schreibprozess entfernt wird, wird die Datenübertragung unterbrochen.

Scannen von Registrierungsausweisen
Die Ausweise mit den übertragenen Registrierungen werden dann über den Dialogleser gescannt und im Dialogfeld **LogViewer** angezeigt.
Die Nachrichten werden automatisch in die Protokolldatei übertragen und können von dort jederzeit gleich wie Online-Nachrichten abgerufen werden.

Da die Offline-Nachrichten zusammen mit den Online-Nachrichten in der Standardansicht angezeigt werden, kann der vordefinierte Filter in der Symbolleiste im Dialog  verwendet werden, um nur die Offline-Nachrichten anzusehen.

Hinweis!
Die Daten werden von der Übertragungseinheit gelöscht:
Wenn der Terminal gelesen wird, wird der Speicher gelöscht.
Wenn der Registrierungsausweis an der Dialogstation gescannt wird, wird der Ausweis gelöscht.

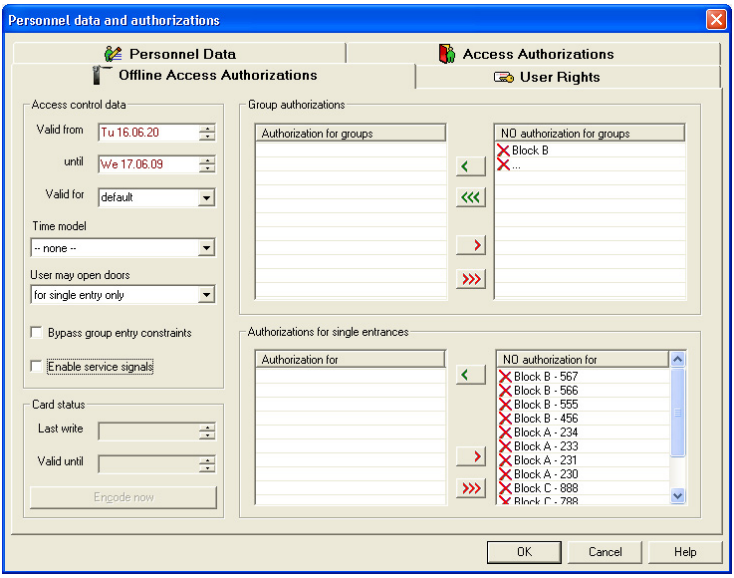
3.7 Bearbeiten von Personaldaten

Um Personaldaten für das Offline-System zu speichern, wird ebenfalls die Datenbank des Access PE Zutrittskontrollsystems verwendet.
Diese Daten werden entsprechend über die Zutrittskontrollsystemdialoge erfasst.

Hinweis!
Jeder Ausweisinhaber für das Offline-System benötigt einen gültigen Ausweis für das Zutrittskontrollsystem (Online-System).

3.7.1 Beschreibung der Dialoge

Wenn das Offline-System aktiv ist (nachdem der Kundenausweis gescannt wurde), enthält der Dialog für die Eingabe von Personal- und Ausweisdaten die zusätzliche Seite **Offline-Zutrittsberechtigungen**.
Hier sind sämtliche personenbezogenen Einstellungen für das Schließsystem konfiguriert.



Die vier Listenfelder auf der rechten Seite des Dialogs werden verwendet, um **Gruppenberechtigungen** (oberes Listenfeld) und **Berechtigungen für einzelne Durchtritte** (unteres Listenfeld) zuzuweisen. Der Prozess zum Zuweisen und Zurückziehen von Berechtigungen ist gleich wir für die Online-Zutrittsberechtigungen.

Hinweis!

Einzelne Berechtigungen können nur in Übereinstimmung mit der Datengröße zugewiesen werden. Die maximale Anzahl für jedes Schließsystem finden Sie in den Systemdaten im Access PE Konfigurator.

Andere Einstellungen für die Offline-Ausweise werden links vom Listenfeld für Zutrittsberechtigungen konfiguriert.
Dialogfeld **Zutrittskontrolldaten**

– **Gültig von... bis**

Die allgemeine Gültigkeit des Ausweises kann hier definiert werden. Erweiterungen (Gültig für) können nicht länger sein als das definierte Datum „bis“. Das Anfangsdatum (Gültig ab) kann als Datum in der Zukunft festgelegt werden. In diesem Fall können die Erweiterungen erst an diesem Datum auf den Ausweis geschrieben werden. Erfolgen keine Einträge, ist der Ausweis ab Zeitpunkt der Codierung auf unbestimmte Zeit gültig.
Die Gültigkeit der zugewiesenen Zutrittsberechtigungen wird aber durch die Einstellungen im Feld **Gültig für** bestimmt. Nur wenn der Eintrag **Ablauf der Gültigkeit** hier ausgewählt wurde, gilt das Datum „bis“ auch für die Zutrittsberechtigungen.

– **Gültig für**
Das Feld wird verwendet, um die Erweiterungsperioden für Berechtigungen zu definieren. Es enthält eine Liste von vordefinierten Perioden zur Schnellauswahl, aber es können ebenfalls andere Daten erfasst werden. [Abhängig von der Zeiteinheit können Zeitperioden von bis zu vier Jahren definiert werden. Sofern erforderlich können Zeitdaten in größeren Einheiten, z. B. 14 Tage als 2 Wochen aufgeführt werden].
Zusätzlich zu den Zeitperioden 1 Stunde, 1 Tag, 1 Woche, 1 Monat und 1 Jahr kann die Liste auch die Einträge **Standard** und **Ablauf der Gültigkeit** enthalten.

–
  - Standard
    Dies ist ein vordefinierter Eintrag und entspricht einer Erweiterungsperiode von zwei Tagen.
  - Ablauf der Gültigkeit
    Sie wird verwendet, um die Periode der allgemeinen Ausweisgültigkeitsperiode (Datum „bis“) während dem Codierungsprozess oder dem initialen Schreibprozess zu erweitern.

Hinweis: Wenn kein Ablaufdatum für die Verwendung des Ausweises festgelegt wird, ist der Ausweis auf unbestimmte Zeit gültig.

- **Zeitmodell**
  Die Wahl eines Zeitmodells begrenzt die Verwendung des Ausweises auf die definierten Zeitperioden.
  Es können nur diejenigen Zeitmodelle ausgewählt werden, die im Dialog mit dem gleichen Namen für das Offline-Schließsystem im Access PE Konfigurator erstellt wurden.
  Zeitmodelle für Zutrittskontrollsystem (Online-System) können hier nicht verwendet werden.
- **Benutzer kann Türen**
-
  - **nur für Einzeleintritte öffnen**.
    Entspricht einer normalen Zutrittsberechtigung – abhängig von der Berechtigung kann der Ausweisinhaber die Tür öffnen oder nicht.
  - **nur langfristig**
    Die Standardzutrittsberechtigung gilt nicht für diesen Ausweisinhaber. Er kann nur entsprechend konfigurierte Türen (Parameter **Manuelle längere Öffnung erlaubt**) langfristig öffnen, indem er seinen Ausweis kurz an den Türöffnerterminal hält.
  - **beide**
    Abhängig von seinen Berechtigungen kann der Ausweisinhaber die Tür entweder dauerhaft (indem er seinen Ausweis während 5 Sekunden an den Leser hält, sofern die fragliche Tür entsprechend konfiguriert ist) oder für einen einmaligen Zutritt (indem er den Ausweis kurz, d. h. weniger als 5 Sekunden an den Leser hält) freigibt.
- **Umgehung Gruppeneintrittseinschränkungen**

Wenn diese Berechtigung ausgewählt ist, kann ein Ausweisinhaber Türen, die mit **Eintritt nur als Gruppe** konfiguriert sind, selber öffnen, d. h. die Gruppenanforderung aufheben.

– **Servicesignale aktivieren**
Wenn der Batteriestatus beim Türterminal niedrig ist, wird dies dem Benutzer, für den die Option aktiviert wurde, mithilfe einem optischen Signal angezeigt. Dadurch kann die Ankündigung auf Personen beschränkt werden, die für Systemreparaturen und -wartung verantwortlich sind.

Dialogfeld **Ausweisstatus**

– **Zuletzt geschrieben**
Das Datum und die Zeit der letzten Erweiterung werden auf dem Codierungsleser an der Dialogstation oder am schreibfähigen Leser angezeigt.
– **Gültig bis**
Ablaufdatum (Datum/Zeit) für die Zutrittsberechtigungen basierend auf der letzten Erweiterung.
– **Jetzt codieren**
Daten für das Schließsystem können über einen angeschlossenen Codierungsleser (Interflex - RWD) auf den Benutzerausweis geschrieben werden.
Wenn der Ausweis beim Aufsetzen oder Ändern der Offline-Einstellungen nicht verfügbar ist, kann der Ausweis beim nächsten Scannen an einem schreibfähigen Leser neu geschrieben werden.

3.7.2 Personaldaten hinzufügen

Personen, denen Zutrittsberechtigungen für das Schließsystem (Offline-System) gewährt wird, müssen als Datensätze im Zutrittskontrollsystem (Online-System) erfasst werden.
Da der gleiche Ausweis für beide Systeme verwendet wird und Zutrittsberechtigungen für das Offline-System über (schreibfähige) Leser (z. B. DELTA 7020) in den Online-

Systemen erweitert wird, müssen Ausweisinhaber auch gültige Zutrittsberechtigungen für das Zutrittskontrollsystem haben, abgestimmt auf die Parametereinstellungen **Schreiben ohne Zutrittsrechte**.

Voraussetzungen
Um die Ausweise an der Dialogstation zu codieren, benötigen Sie eine **Lese-/Schreib-Dialogeinheit**. Diese wird direkt mit dem Bedienplatz-Rechner verbunden und über **Access PE Personalverwaltung** aufgesetzt.

1. Verbinden Sie den Leser mit der Dialogstation.
2. Öffnen Sie **Access PE Personalverwaltung**.
3. Wählen Sie im Menü **Tools** die Funktion **Eigenschaften**, um den Dialog **Konfiguration ändern** zu öffnen.
4. Aktivieren Sie das Kontrollkästchen **Dialogleser**.
5. Wählen Sie im Feld **Leser** den Eintrag **Interflex USB Hitag, Mifare (IFRW)**.
6. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Sie benötigen ebenfalls einen schreibfähigen Leser (z. B. DELTA 7020), um die Offline-Berechtigungen zu erweitern. Dieser Leser kann als Zutrittskontrollleser im Online-System installiert werden, z. B. an stark frequentierten Durchtritten (Hauptdurchtritt) und kann gleichzeitig mit Schreibfunktionen für das Schließsystem konfiguriert werden, siehe auch. *Den schreibfähigen Leser konfigurieren, Seite 20*.

Online-Daten
Für Personen, die im System noch nicht erfasst wurden, muss zuerst ein Datensatz hinzugefügt werden. Um Personaldaten hinzuzufügen und dem Zutrittskontrollsystem Berechtigungen hinzuzufügen, gehen Sie wie folgt vor:

1. **Personalverwaltung** öffnen.
2.

- Um einen neuen Datensatz hinzuzufügen klicken Sie auf  oder öffnen Sie das Menü **Personen > Neue Person ...** und gehen Sie zum Dialogfeld **Personaldaten und Berechtigungen**.
- Ergänze Sie in der Registerkarte **Personaldaten** mindestens die Pflichtfelder für die betreffende Person.
- Weisen Sie der Person einen Ausweis zu.

3. Wechseln Sie zur Registerkarte **Zutrittsberechtigungen**.
4.
   - Geben Sie der Person die notwendigen Zutrittsberechtigungen für das Online-System.
   - Wenn der Parameter **Schreiben ohne Zutrittsrechte** (*Den schreibfähigen Leser konfigurieren, Seite 20*) für den schreibfähigen Leser nicht aktiviert ist, muss die Zutrittsberechtigung für diesen Durchtritt zugewiesen werden.

Sie können die Offline-Zutrittsberechtigungen sofort verteilen, ohne den Dialog zu schließen.

Offline-Daten

Wenn Sie einem bestehenden Datensatz Offline-Daten hinzufügen möchten oder wenn Sie beim Aufsetzen des neue Datensatzes das Dialogfeld geschlossen haben, können Sie ihn entweder durch einen Doppelklick auf den relevanten Eintrag in der Liste der verfügbaren Elemente öffnen oder den Eintrag auswählen und die Schaltfläche  anklicken.

Hinweis!

Nur Personen mit einem gültigen Ausweis für das Zutrittskontrollsystem (Online-System) können Berechtigungen für das Schließsystem (Offline-System) zugewiesen werden.

1. Wechseln Sie zur Registerkarte **Offline-Zutrittsberechtigungen**.
2. Geben Sie der Person die notwendigen Gruppen- und Einzelberechtigungen.
3. Geben Sie Benutzungseinschränkungen (Gültigkeitsdaten, Gültigkeitsperiode, Zeitmodell etc.) ein.
4. Legen Sie den Ausweis auf den Dialogleser.
5. Klicken Sie die Schaltfläche **jetzt codieren** an, um den Ausweis zu codieren.
   Die Felder **Zuletzt geschrieben** und **Gültig bis** werden mit den relevanten Daten ergänzt.
   [Wenn die physische Karte nicht verfügbar ist, erfolgt die Codierung automatisch beim nächsten Scannen an einem schreibfähigen Leser.
6. Nachdem die Codierung erfolgreich abgeschlossen wurde, klicken Sie **OK**, um den Dialog zu schließen.

Überprüfung der Daten während den Schreibprozess.
Wenn die Schaltfläche **Jetzt codieren** angeklickt wird, erscheint ein Dialogfeld, das Sie auffordert, den Ausweis auf die Lese-/Schreibeinheit zu legen.
Die folgenden Umstände erzeugen Fehlernachrichten und der Schreibprozess wird beendet.

– Kein Ausweis auf der Einheit oder die Codedaten können nicht gelesen werden.
– Der Ausweis ist kein Benutzerausweis.
– Der Ausweis gehört nicht der ausgewählten Person.

Die Anzeige der Gültigkeitsperiode zeigt an, dass der Schreibprozess erfolgreich war.

3.7.3 Daten ändern

Änderungen an den Offline-Daten (Erweiterung oder Reduzierung der Zutrittsberechtigungen, neue Erweiterungszyklen etc.) werden an die Controller verteilt, wie

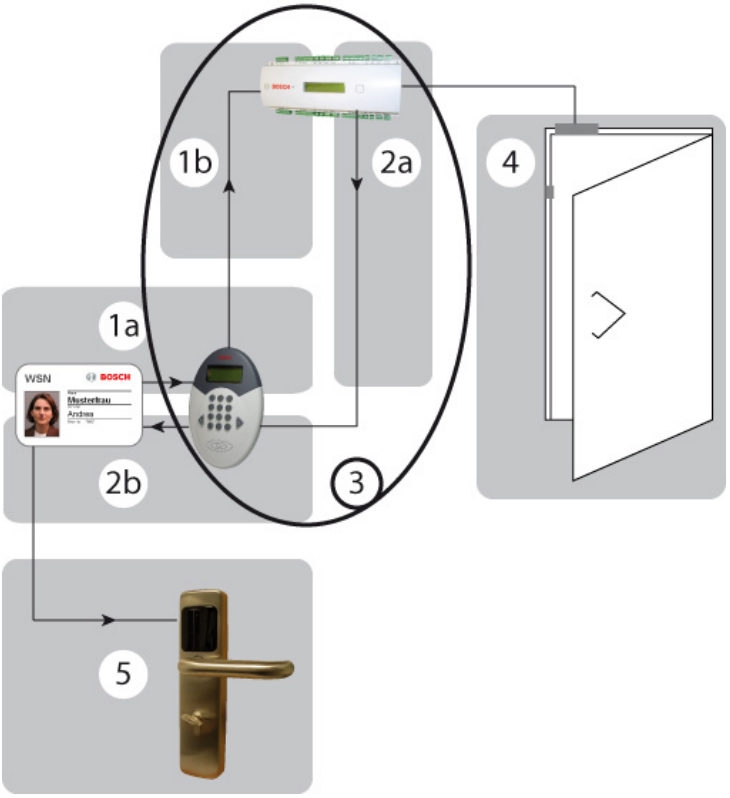
bei den Online-Daten. Wenn der Ausweis das nächste Mal an einem schreibfähigen Leser gescannt wird, werden die geänderten Daten auf den Ausweis übertragen.

Hinweis!
Gewisse Online-Daten können ebenfalls einen Einfluss auf die Offline-Berechtigungen haben.
Bei Personen, die im Online-System gesperrt sind, werden beim nächsten Lese-/Schreibprozess sämtliche Offline-Daten vom Ausweis gelöscht.

3.8 Beschreibung der Vorgehensweisen

Im Folgenden wird eine kurze Übersicht über die erforderlichen Schritte und Prozesse gegeben und die Besonderheiten des Offline-Systems gezeigt und erklärt; speziell im Zusammenhang mit dem Zutrittskontrollsystem (online).

3.8.1 Zutritt



1a Ausweis lesen

1b Ausweisnummer an AMC gesendet

2a Aktuelle Daten mit dem Leser geteilt

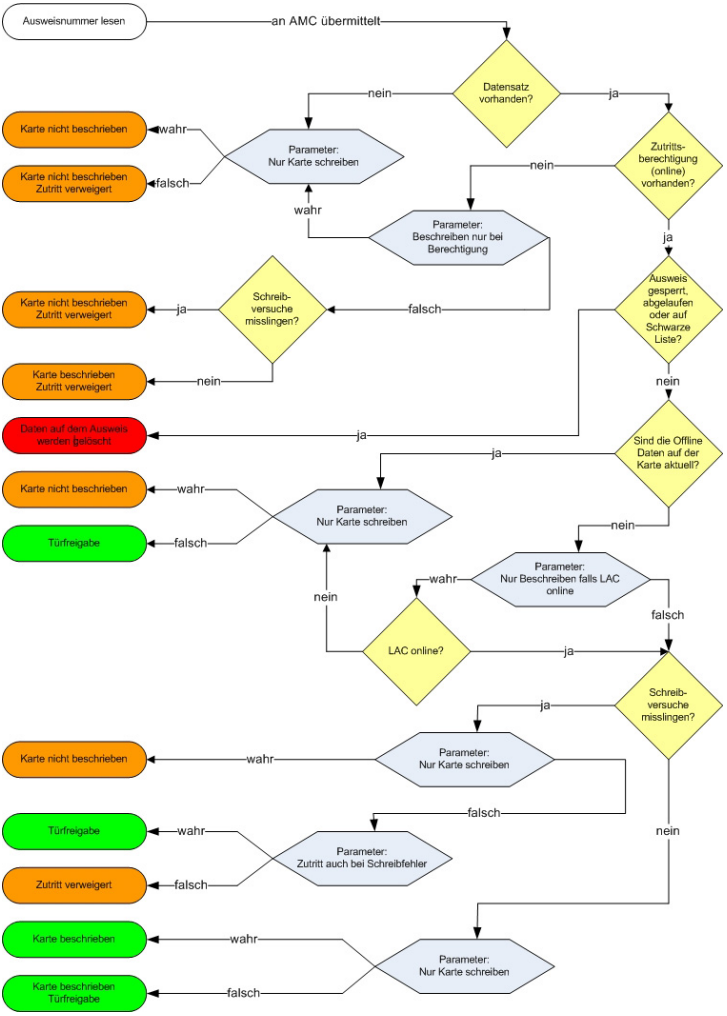
2b Aktuelle Daten auf den Ausweis geschrieben

3 Weitere Informationen zum Überprüfungs- und Schreibprozess des AMC finden Sie im Flussdiagramm unter *Schreibprozess, Seite 52*.

4 Türfreigabe für das Online-System (sofern konfiguriert)

5 Zutrittsberechtigungskontrolle an den Türterminals

3.8.2 Schreibprozess



In den meisten Fällen werden die Schreibprozesse dazu verwendet, Zutrittsberechtigungen mit dem bestimmten Zeitbedarf zu erweitern.
Aus diesem Grund wird das letzte Schreibdatum ebenfalls in der Datenbank gespeichert. Der Bedarf nach Erweiterung wird durch den Vergleich des aktuellen Datums oder der aktuellen Zeit bestimmt. Da dies aber bedeuten würde, dass das Ablaufdatum jedes mal bei Scannen des Ausweises aktualisiert würde, müsste auch jedes mal ein Schreibprozess durchgeführt werden. Um unnötige Wartezeiten und Verzögerungen an Lese-/Schreibeinheiten zu vermeiden, wird eine Gültigkeitsdauer verwendet, um einen Zeitpunkt zu bestimmen, bis zu dem der Ausweis gültig sein soll.
Daten werden nur aktualisiert, wenn ein Drittel der Gültigkeitsdauer abgelaufen ist.

Beispiel:
Gültigkeitsdauer: 1 Tag = 24 Stunden
1/3 der Gültigkeitsdauer: 8 Stunden
Wenn ein Ausweisinhaber den Ausweis scannt, wenn er die Arbeit aufnimmt und sein Ablaufdatum aktualisiert wird, kann er die Lese-/Schreibeinheit in den darauf folgenden acht Stunden passieren, ohne dass ein neuer Schreibprozess ausgelöst wird - die Daten werden erst nach Ablauf der acht Stunden aktualisiert.
Hinweis: Wenn die Gültigkeitsdauer in den Beispiele oben verdoppelt wird (= 48 Stunden), erhöht sich die Aktualisierungsperiode entsprechend (= 16 Stunden). Damit wird sichergestellt, dass die Gültigkeitsdauer nur einmal pro Tag aktualisiert wird.

3.9 Anwendungsbeispiele:

Die folgenden Beispiele zeigen, wie das System für besondere Anforderungen oder Ereignisse über die entsprechenden Parametereinstellungen aufgesetzt werden kann. Die Beispiele sind auf ein spezifisches Element beschränkt.
Andere Varianten können vorkommen, wenn eine Kombination von Parametereinstellungen verwendet wird. Die Beispiele können auch entsprechend miteinander kombiniert werden.

Zutrittskontrollleser und/oder schreibfähiger Leser?
Der Entscheid, wie ein schreibfähiger Leser verwendet werden soll, hängt von einer Reihe verschiedener Faktoren ab; es kann sinnvoll sein, den Leser nicht in das Zutrittskontrollsystem (online) zu integrieren.

- Gibt es einen Durchtritt (z. B. Hauptdurchtritt), den die meisten Ausweisinhabern passieren müssen?
-
  - **Ja**: Es wird ein schreibfähiger Leser mit gleichzeitiger Zutrittskontrollfunktion für das Online-System empfohlen.
  - **Nein** (Es gibt eine Reihe von möglichen Durchtritten, zum Beispiel): Die Verwendung von schreibfähigen Lesern an jedem Durchtritt würde 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 schreibfähiger Leser (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 beliebiger schreibfähiger Leser für diese besonderen 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 für den Fall, dass die Einstellungen im zweiten Beispiel unter *Einzeltüren oder Türgruppen?, Seite 56* nicht ausreichen.
Entsprechend ist ein schreibfähiger Leser nicht mit den Zutrittskontrollfunktionen verbunden; stattdessen wird er als reine Lese-/Schreibeinheit für das Offline-System konfiguriert.
Voraussetzungen:
Die Leserparamater der **Lesefunktion** müssen auf **Schließsystem schreiben** eingestellt sein und der Parameter **nur auf Karte schreiben** ist aktiviert (=Kontrollkästchen aktiviert).
Der schreibfähige Leser muss nur für Hotelangestellte an einem zentralen Ort installiert werden, damit ihre Rechte aktualisiert und erweitert werden können. Wählen Sie wenn möglich einen Ort aus, den alle relevanten Personen regelmäßig passieren, z. B. Mitarbeiterraum.
Die Berechtigung für die Hotelzimmertür für Hotelgäste wird entsprechend der Zimmerbuchung zugewiesen und mithilfe einem schreibfähigen Leser an der Rezeption auf den Ausweis geschrieben. Berechtigungen müssen in der Regel nicht geändert werden, dies erfolgt sofern erforderlich an der Rezeption; der Leser muss 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 unberechtigte Zutritt schützen. Ein schreibfähiger Leser kann die Rechte für das Schließsystem für autorisierte Personen gleichzeitig aktualisieren und erweitern.
Voraussetzungen:

Die Leserparamater der **Lesefunktion** müssen auf **Schließsystem schreiben** eingestellt sein und der Parameter **nur auf Karte schreiben** ist deaktiviert (=Kontrollkästchen deaktiviert).
Wenn der Parameter **Schreiben ohne Zutrittsrechte** nicht gesetzt ist (aktiviert), 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.
Voraussetzungen:
Der Parameter **Türgruppen überprüfen** muss aktiviert 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.
Voraussetzungen:
Der Parameter **Türgruppen überprüfen** muss deaktiviert sein (Kontrollkästchen nicht markiert).
Ablauf:
An den Türen werden nur individuelle Berechtigungen akzeptiert. Personen, denen nur Türgruppenberechtigungen für diese Türen zugewiesen wurden, erhalten keinen Zutritt.

Normale Freigabe oder Dauerfreigabe
Wenn der Ausweis gültig ist, blinkt das grüne Licht am Terminal dreimal. Die Türe wird für die festgelegte Zeit (der Standard ist 3 Sekunden) geöffnet. Wenn sich die Türe im Modus **Dauerfreigabe** befindet, blinkt die LED-Anzeige dreimal Grün auf, wenn ein gültiger Ausweis vorgewiesen wird.
Ein Ausweis mit der Erlaubnis für einen **Einzeldurchtritt**kann die Türe nur für einen Durchtritt öffnen. Ein Ausweis mit einer **Dauerfreigabe**funktion aktiviert sofort die Dauerfreigabe (der Ausweis muss nicht fünf Sekunden an den Leser gehalten werden). Ausweise, die für **beide Funktionen** berechtigt sind, können für normale Öffnungen verwendet werden, wenn der Ausweis während dem dreimaligen Blinken entfernt wird. Wenn der Ausweis stattdessen weiter an die Leseeinheit des Terminals gehalten wird (> fünf Sekunden), leuchtet ein kontinuierliches grünes Signal auf und die Tür bleibt geöffnet, bis ein Ausweis mit **Dauerfreigabe**berechtigung [**beide**] an den Terminal gehalten wird (während mindestens 5 Sekunden). Die Türe ist dann geschlossen; d. h. Zutritt ist nur mit Berechtigungsausweis möglich.

Voraussetzungen:
Der Parameter **Dauerfreigabe (Umschalten)** muss für den Terminal auch ausgewählt (aktiviert) werden.

Durch Zeitmodell:
Die selbe Funktion kann über ein Zeitmodell kontrolliert werden. Für den Türparameter **Zeitöffnungsmodell** wird ein Zeitmodell ausgewählt und die Tür ist dauerhaft offen („Anfangszeit“) oder verschlossen („Endzeit“), in Abstimmung mit den spezifizierten Zeitperioden.
Zeitmodelle, die „bis Zeiten“ enthalten, können zum Schließen von Türen verwendet werden, die schon vor langer Zeit zur Dauerfreigabe geöffnet wurden.

Hinweis!
Freigaben, die durch Zeitmodelle gesteuert werden, enthalten immer das Risiko, dass nicht überwachte Bereiche frei zugänglich sein könnten.

Beispiel: Bürogebäude ohne öffentlichen Zutritt

1. **Manuell dauerhaft freigeben/sperren**
   Das Büro wird jeden Morgen mit der Dauerfreigabefunktion geöffnet und der Öffentlichkeit zugänglich gemacht. Wenn die Büros schließen, wird die Dauerschließung durchgeführt, das heißt, nur Personen mit einem gültigen Ausweis haben während dieser Zeit Zutritt zum Büro.
2. **Dauerfreigabe/Dauerschließung über ein Zeitmodell kontrollieren**
   Wenn sich die öffentlichen Besuchsstunden von den Mitarbeiterstunden unterscheiden, kann die Türöffnung/-Schließung über ein Zeitmodell gesteuert werden.
   Personalstunden: 8:00-12:00 Uhr und 13:00-17:00 Uhr
   Öffentliche Besuchsstunden: 9:00-11:00 Uhr und 14:00-16:00 Uhr

Um die Stunden korrekt abzudecken und das manuelle Öffnen und Schließen zu vermeiden, kann ein Zeitmodell mit zwei Perioden verwendet werden, das den öffentlichen Besuchsstunden entspricht.

3. **Steuerung der Dauerschließung über ein Zeitmodell**
   Das Büro wird jeden Morgen manuell vom ersten Mitarbeiter, der eintrifft, mithilfe der Dauerfreigabefunktion geöffnet. Ein Zeitmodell ohne Startzeiten wird verwendet, um die Dauerschließung an einem bestimmten Zeitpunkt zu initialisieren.

3.10 LED Displaysignale

Signale für Benutzerausweise

Türe mit Einzelentsperrfunktion geöffnet

Bedeutung	Die Türe wird mit einem einzelnen Dauerfreigabeausweis geöffnet. Diese Nachricht wird ebenfalls angezeigt, wenn die Türe bereits mittels Dauerfreigabe geöffnet wurde.
Registrierungseintrag	**Zutritt, Einzeltürberechtigung** oder **Zutritt, Türgruppenberechtigung**

Türe mit Einzeldauerfreigabefunktion geöffnet

Bedeutung	Die Tür wurde von einem Dauerfreigabeausweis oder einem Zeitmodell geöffnet.
Registrierungseintrag	**Türe entsperrt**

Türe mit Dauerschließfunktion geschlossen

Bedeutung	Die Tür wurde von einem Dauerfreigabeausweis oder einem Zeitmodell gesperrt.
Registrierungseintrag	**Tür befindet sich im Normalmodus**

Aufforderung zum Batteriewechsel

Bedeutung	Rotes LED-Signal leuchtet eine bis drei Sekunden. Solange die Batterie nicht vollständig leer ist, folgt ein Ausweis spezifisches Signal. Wenn die Batterien leer sind, wird kein weiteres Signal angezeigt und es sind keine Registrierungen möglich. Die Aufforderung zum Batteriewechsel wird nur für Benutzerausweise angezeigt.
Registrierungseintrag	Die **Batteriespannung ist zu tief** Eintrag wird immer nach 25 Registrierungen angezeigt.
Lösung	Batterien austauschen.

Sondersignale

Lese-/Schreibbestätigung für Systemausweise

Bedeutung	Ein Systemausweis wurde erfolgreich gelesen oder geschrieben.
Registrierungseintrag	**Initialisierung**

Kein Ausweis im Bereich

Bedeutung	Die Elektronik wurde aktiviert, aber der Ausweis wurde vor dem Leser nicht erkannt.
Registrierungseintrag	<Kein Eintrag erfolgt>
Lösung	Halten Sie den Systemausweis erneut gegen den Leser.

Lese-/Schreibfehler

Bedeutung	Es war nicht möglich, erfolgreich den Systemausweis zu lesen oder darauf zu schreiben.
Registrierungseintrag	<Kein Eintrag erfolgt>
Lösung	Halten Sie den Systemausweis erneut gegen den Leser.

Ungültige Berechtigung

Bedeutung	Der Ausweis hat keine gültige Berechtigung.
Registrierungseintrag	**Zutritt verweigert, Ausweisstatus blockiert**, **Nicht berechtigt**, **Zutritt verweigert, Ausweis abgelaufen** oder **Zutritt verweigert, außerhalb des Zeitmodells**
Lösung	Ändern Sie wenn nötig die Berechtigung für diesen Ausweis.

Zeit ungültig

Bedeutung	Der Terminal kennt die aktuelle Zeit nicht.
Registrierungseintrag	<Kein Eintrag erfolgt>
Lösung	Es muss ein Initialisierungsausweis erstellt und am Terminal gescannt werden.

Türinitialisierung fehlt

Bedeutung	Der Terminal wurde nicht initialisiert.
Registrierungseintrag	<Kein Eintrag erfolgt>
Lösung	Es muss ein Türinitialisierungsausweis erstellt und am Terminal gescannt werden.

Kundendaten fehlen

Bedeutung	Der Terminal wurde für diesen Kunde nicht initialisiert.
Registrierungseintrag	<Kein Eintrag erfolgt>
Lösung	Der Terminal muss mit einem Kundenausweis initialisiert werden.

Datenübertragung

Bedeutung	Die LED leuchtet Orange auf, während die Daten zwischen dem Systemausweis und einem Terminal ausgetauscht werden. Die Dauer hängt vom zu übertragenden Datenvolumen ab. De Lese/ Schreibprozess wird dann signalisiert.

LED-Anzeigen für mobiles Gerät mit Lese-/Schreibfunktion

Schreibbestätigung für Zeitmodellausweise

Bedeutung	Daten wurden erfolgreich auf den Zeitmodellausweis geschrieben.

Lesebestätigung für den Zeitmodellausweis

Bedeutung	Der Zeitmodellausweis wurde erfolgreich gelesen.

Lesebestätigung für den Zeitmodellausweis

Bedeutung	Der Kundenausweis wurde erfolgreich gelesen.

Lese-/Schreibfehler

Bedeutung	Es war nicht möglich, den Systemausweis erfolgreich zu lesen oder darauf zu schreiben.
Lösung	Halten Sie den Systemausweis gegen den Leser.

Kundendaten fehlen

Bedeutung	Der Timesetter wurde für diesen Kunde nicht initialisiert.
Lösung	Der Timesetter muss mit dem Kundenausweis neu initialisiert werden.

Zeit ungültig

Bedeutung	Der Timesetter kennt die aktuelle Zeit nicht.
Lösung	Es muss ein entsprechender Zeitinitialisierungsausweis erstellt und der Timesetter synchronisiert werden.

Taste:

- LED-Signal leuchtet eine Sekunde.
- LED-Signal leuchtet bis zu drei Sekunden.
- grüne LED
- rote LED
- orange LED
- zusätzliches akustisches Signal


- zusätzliches akustisches Signal

 - Signalunterbruch

Bosch Access Systems GmbH
Charlottenburger Allee 50
52068 Aachen
Germany
www.boschsecurity.com
© Bosch Access Systems GmbH, 2017