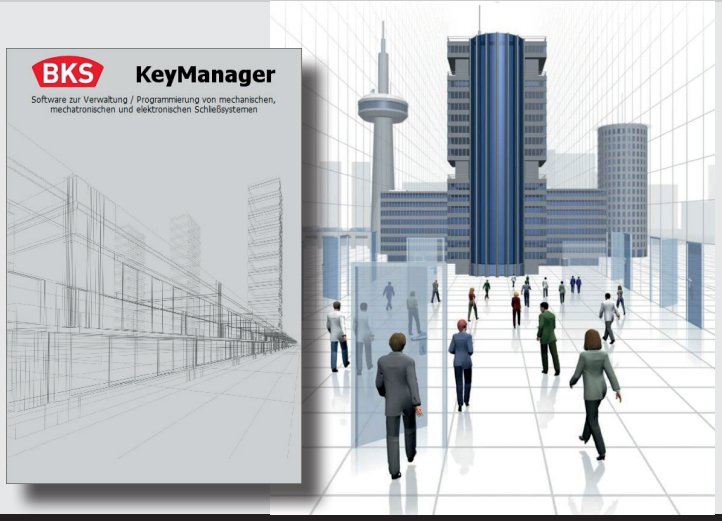
G-U

C5950114S
08 | 10.2022 | Designed in Germany



ixalo

SE

TÜRTECHNIK

BKS

BKS KeyManager

DE

ixalo | SE-Elektronik-Programmierung

Benutzerhandbuch

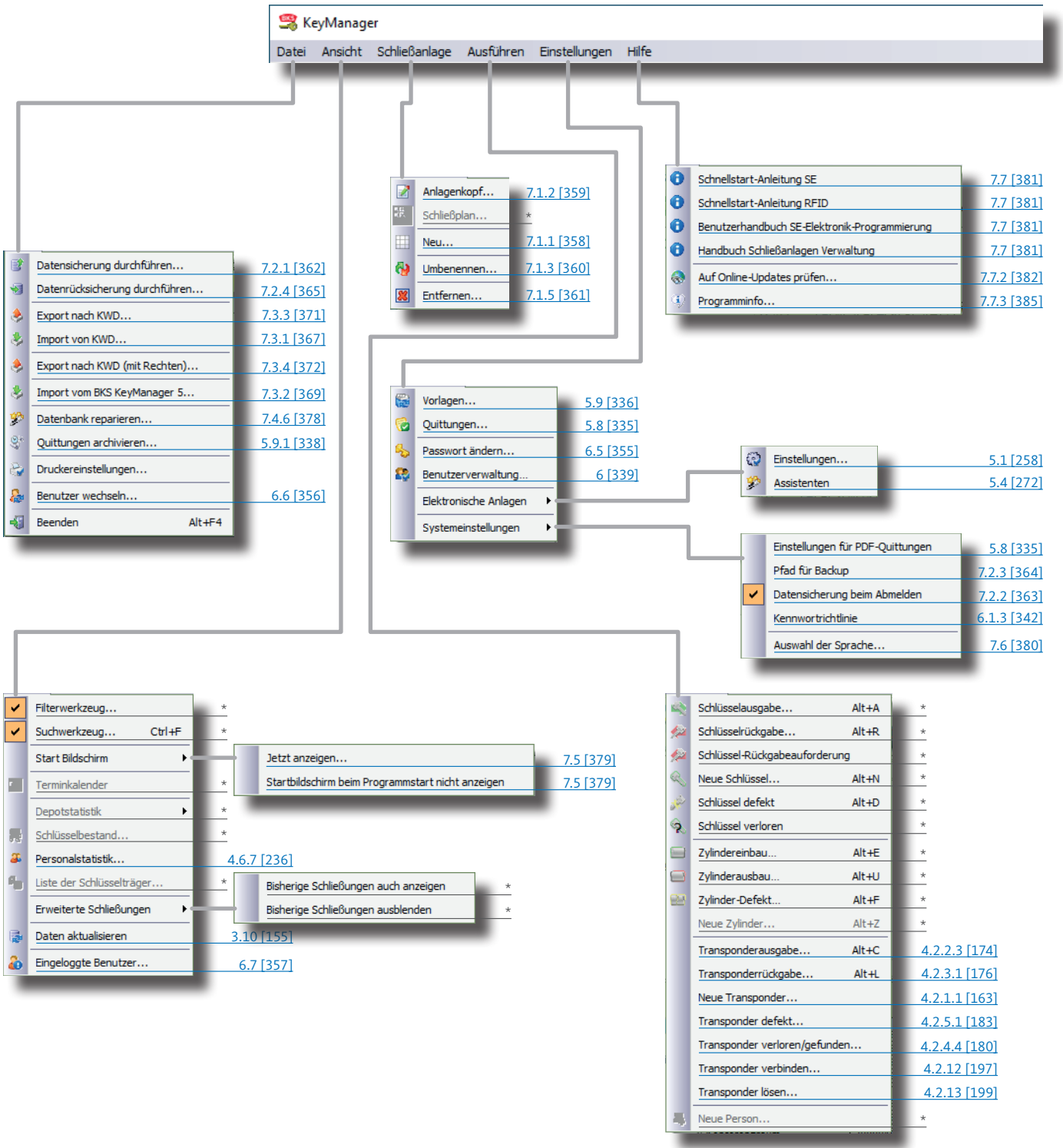
Vorsprung mit System

G-U BKS FERCO

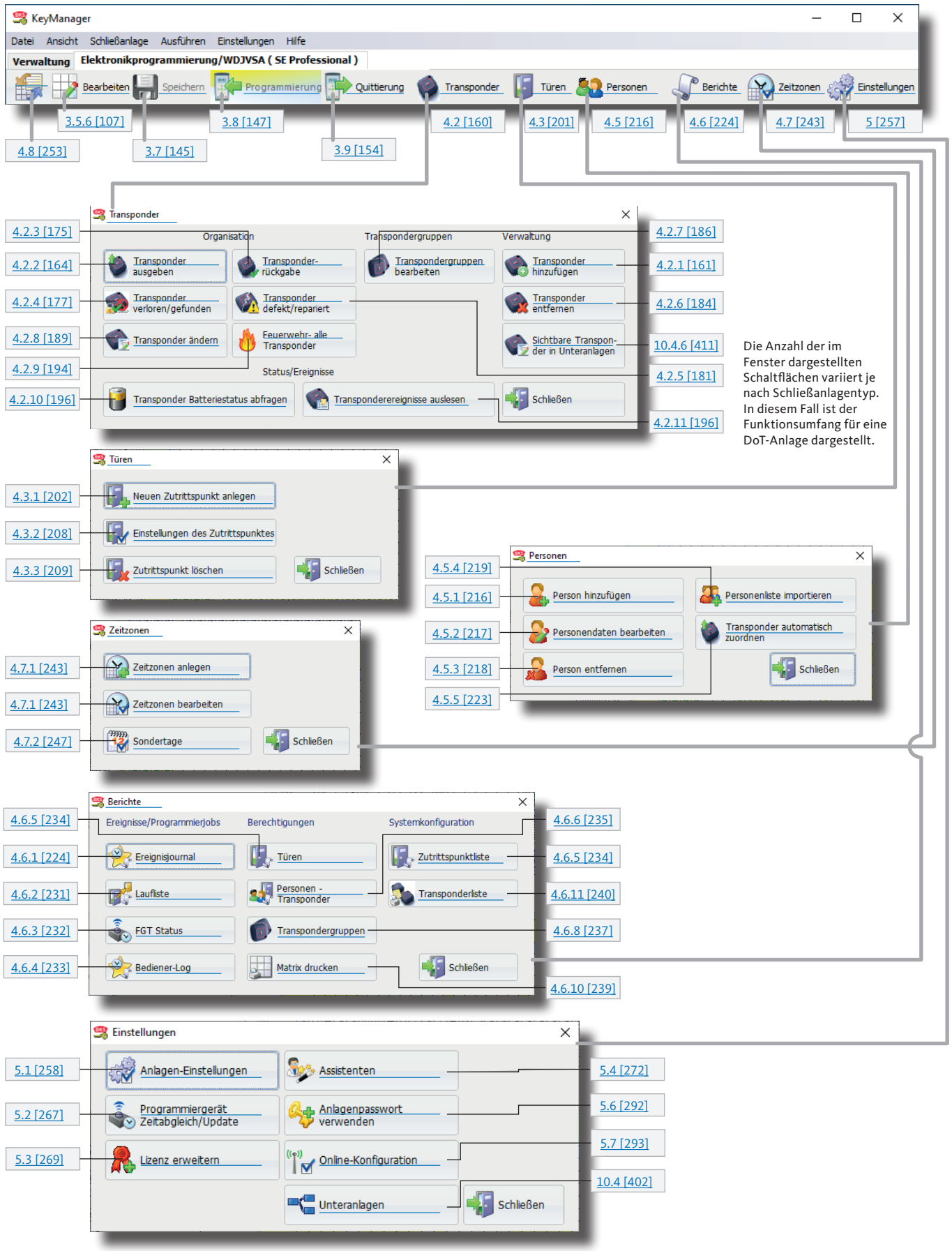
Quick Reference Card

HINWEIS

Übersicht der Menüs im BKS KeyManager mit Querverweisen zur Kapitelnummer [Seite].
■ Drücken Sie auf den Link, um zur Erklärung der gewählten Funktion zu gelangen.



* Diese Funktion wird nur bei der mechanischen Schließanlagenverwaltung benötigt. Eine Verwendung in elektronischen Schließanlagen ist nicht zwingend vorgesehen


KeyManager
Datei Ansicht Schließanlage Ausführen Einstellungen Hilfe
Verwaltung
Elektronikprogrammierung/WDJVSA (SE Professional)
Bearbeiten
Speichern
Programmierung
Quittierung
Transponder
Türen
Personen
Berichte
Zeitzonen
Einstellungen
3.5.6 [107]
3.8 [147]
4.2 [160]
4.3 [201]
4.5 [216]
4.6 [224]
4.7 [243]
5 [257]
4.8 [253]
3.7 [145]
3.9 [154]
Transponder
Organisation
Transpondergruppen
Verwaltung
4.2.3 [175]
4.2.2 [164]
4.2.4 [177]
4.2.8 [189]
4.2.9 [194]
4.2.10 [196]
4.2.7 [186]
4.2.1 [161]
4.2.6 [184]
10.4.6 [411]
4.2.5 [181]
4.2.11 [196]
Transponder ausgeben
Transponder-rückgabe
Transpondergruppen bearbeiten
Transponder hinzufügen
Transponder verloren/gefunden
Transponder defekt/repariert
Transponder entfernen
Transponder ändern
Feuerwehr- alle Transponder
Sichtbare Transpon-der in Unteranlagen
Status/Ereignisse
Transponder Batteriestatus abfragen
Transpondereregnisse auslesen
Schließen
Die Anzahl der im Fenster dargestellten Schaltflächen variiert je nach Schließanlagentyp. In diesem Fall ist der Funktionsumfang für eine DoT-Anlage dargestellt.
Türen
4.3.1 [202]
4.3.2 [208]
4.3.3 [209]
Neuen Zutrittspunkt anlegen
Einstellungen des Zutrittspunktes
Zutrittspunkt löschen
Schließen
Personen
4.5.4 [219]
4.5.1 [216]
4.5.2 [217]
4.5.3 [218]
4.5.5 [223]
Person hinzufügen
Personenliste importieren
Personendaten bearbeiten
Transponder automatisch zuordnen
Person entfernen
Schließen
Zeitzonen
4.7.1 [243]
4.7.1 [243]
4.7.2 [247]
Zeitzonen anlegen
Zeitzonen bearbeiten
Sondertage
Schließen
Berichte
Ereignisse/Programmierjobs
Berechtigungen
Systemkonfiguration
4.6.5 [234]
4.6.1 [224]
4.6.2 [231]
4.6.3 [232]
4.6.4 [233]
4.6.6 [235]
4.6.5 [234]
4.6.11 [240]
4.6.8 [237]
4.6.10 [239]
Ereignisjournal
Türen
Zutrittspunktliste
Laufliste
Personen - Transponder
Transponderliste
FGT Status
Transpondergruppen
Bediener-Log
Matrix drucken
Schließen
Einstellungen
5.1 [258]
5.2 [267]
5.3 [269]
5.4 [272]
5.6 [292]
5.7 [293]
10.4 [402]
Anlagen-Einstellungen
Assistenten
Programmiergerät Zeitabgleich/Update
Anlagenpasswort verwenden
Lizenz erweitern
Online-Konfiguration
Unteranlagen
Schließen

Inhaltsverzeichnis

1. Allgemeine Informationen ..... Seite 11

1.1 Warnsymbole ..... Seite 11
1.2 Systemanforderungen ..... Seite 12
1.3 Systemarchitektur ..... Seite 13
1.3.1 Systemdarstellung Client-Server-Installation ..... Seite 14
1.3.2 Systemdarstellung Einzelplatzversion mit interner Datenbank ..... Seite 14
1.3.3 Funktionelle Unterscheidung der Schließanlagen ..... Seite 15
1.4 Empfehlungen zur Datenschutz-Grundverordnung (DSGVO) ..... Seite 16
1.4.1 Grundsätzliche Empfehlungen zur Datenspeicherung ..... Seite 16
1.4.2 Empfehlungen zur Datenbankinstallation ..... Seite 16
1.4.3 Empfehlungen zum werkseitigen Administrator-Zugang ..... Seite 16

2. Installation ..... Seite 17

2.1 Installationsarten ..... Seite 17
2.2 Installation der Einzelplatz- und Serverversion mit Microsoft SQL Server ..... Seite 18
2.2.1 Installation des Microsoft SQL Servers ..... Seite 19
2.2.2 Konfiguration des Microsoft SQL Servers bei Client-/Serverinstallation ..... Seite 24
2.2.3 Installation der Einzelplatzversion ..... Seite 26
2.3 Installation eines Clients der Netzwerkversion ..... Seite 32
2.4 Installation der Einzelplatzversion mit interner Datenbank ..... Seite 40
2.5 Installation des Servers der Netzwerkversion ..... Seite 47
2.5.1 Installation und Konfiguration des Microsoft SQL Servers ..... Seite 48
2.5.2 Installation der Serverversion für die Netzwerkversion ..... Seite 48
2.6 Aufrufen der Programmverwaltung ..... Seite 54
2.7 Silent Installation ..... Seite 55
2.8 Installation des Ethernetbuskoppler Professional-Dienst ..... Seite 57
2.9 Weitere Menüpunkte ..... Seite 61

3. Konzeption des BKS KeyManager ..... Seite 62

3.1 Programmstart ..... Seite 62
3.2 Anmeldung ..... Seite 62
3.3 Startbildschirm ..... Seite 64
3.3.1 Modul „Schließanlagen Verwaltung“ ..... Seite 64
3.3.2 Modul „Elektronik-Programmierung“ ..... Seite 64
3.4 Anlegen einer elektromechanischen Schließanlage ..... Seite 65
3.4.1 Schließanlage mit der Schließanlagendatei anlegen ..... Seite 65
3.4.1.1 Lizenzen der Schließanlage hinzufügen ..... Seite 67
3.4.1.2 Personenliste der neuen Schließanlage hinzufügen ..... Seite 69
3.4.1.2.1 Automatische Transpondervergabe ..... Seite 72
3.4.2 Schließanlage über Datenrücksicherung wiederherstellen ..... Seite 73
3.4.3 Import einer Schließanlage von Version 5 des BKS KeyManagers ..... Seite 74
3.4.4 Inbetriebnahme-Assistent „Neue Schließanlage“ starten ..... Seite 76
3.4.5 Anlagenpasswort festlegen ..... Seite 77
3.5 Die Hauptfunktionen im Überblick | Berechtigungsmatrix ..... Seite 78
3.5.1 Aufbau des Hauptbildschirms ..... Seite 78
3.5.2 Funktionalitäten der Berechtigungsmatrix und des Listenmenüs ..... Seite 80
3.5.3 Berechtigungsmatrix ..... Seite 81
3.5.3.1 Darstellungsoptionen der Berechtigungsmatrix ..... Seite 81
3.5.3.2 Filter zur Administration und Reduzierung der Matrix ..... Seite 82
3.5.3.2.1 Anlegen des Filters ..... Seite 82
3.5.3.2.2 Aktivierung des Filters ..... Seite 83

3.5.3.2.3 Deaktivierung des Filters ... Seite 84
3.5.3.3 Filterung der Türgruppen ... Seite 85
3.5.3.4 Filterung der Transpondergruppen ... Seite 86
3.5.3.5 Konfiguration der angezeigten Spalten und Zeilen in der Matrix ... Seite 87
3.5.4 Kontextmenüs ... Seite 88
3.5.5 Statusanzeigen der Berechtigungsmatrix ... Seite 90
3.5.5.1 Status der Berechtigung (DoT) ... Seite 91
3.5.5.2 Status von Ereignissen (DoT) ... Seite 95
3.5.5.3 Status der Berechtigung (nonDoT) ... Seite 97
3.5.5.4 Status von Ereignissen (nonDoT) ... Seite 100
3.5.5.5 Ereignissen ohne Anzeige in der Berechtigungsmatrix ... Seite 101
3.5.5.6 Statusmeldungen in einer DoT-Anlage mit FGT ... Seite 102
3.5.5.7 Statusmeldungen in einer DoT-Anlage mit Online-Komponenten ... Seite 104
3.5.5.8 Statusmeldungen in Online-Anlagen ... Seite 105
3.5.5.9 Status der Batterieanzeige ... Seite 106
3.5.6 Bearbeiten der Berechtigungsmatrix im Client-Server-Betrieb ... Seite 107
3.6 Zutrittsberechtigungen, Freigabe|Sperrung ... Seite 108
3.6.1 Verwaltung der Zutrittsberechtigungen ... Seite 108
3.6.1.1 Zutrittsberechtigungen in Data on Transponder-Systemen (DoT) ... Seite 108
3.6.1.2 Zutrittsberechtigungen in Offline-Systemen (nonDoT) ... Seite 110
3.6.1.3 Zutrittsberechtigungen in Online-Systemen (nonDoT und DoT) ... Seite 111
3.6.2 Effiziente Reihenfolge bei Vergabe der Zutrittsberechtigungen ... Seite 111
3.6.3 Berechtigung von Transpondergruppen/Gruppenberechtigungen ... Seite 112
3.6.3.1 Gruppenberechtigungen im Transponder (DoT-Anlagen) ... Seite 112
3.6.3.2 Gruppenberechtigungen in der Tür (nonDoT-Anlagen) ... Seite 115
3.6.4 Berechtigung von Transpondern ... Seite 117
3.6.4.1 Einzelberechtigung im Transponder, Transponder-Recht (DoT-Anlagen) ... Seite 117
3.6.4.2 Einzelberechtigungen in der Tür (nonDoT-Anlagen) ... Seite 119
3.6.5 Berechtigung durch Zeitzonen und/oder Sondertagen ... Seite 121
3.6.5.1 Zeitzonen für Transpondergruppen ... Seite 121
3.6.5.2 Zeitzonen für einzelne Transponder in DoT-Anlagen ... Seite 124
3.6.5.3 Zeitzonen für einzelne Transponder in einer nonDoT-Anlagen ... Seite 126
3.6.6 Berechtigung über Tagesfreigaben ... Seite 127
3.6.6.1 Tagesfreigabe-Modus „Manuell“ (Toggle-Modus) ... Seite 132
3.6.6.2 Tagesfreigabe-Modus „Halbautomatisch“ ... Seite 133
3.6.6.3 Tagesfreigabe-Modus „Automatisch“ ... Seite 134
3.6.7 Gültigkeitsverlängerung der Zutrittsberechtigung über Freigabeterminal (DoT-Anlagen) ... Seite 135
3.6.7.1 DoT-Anlage mit FGT und Gültigkeitsverlängerung ... Seite 135
3.6.7.2 Gültigkeitsverlängerung aktivieren ... Seite 136
3.6.7.3 Status der Gültigkeitsverlängerung in Berechtigungsmatrix ... Seite 137
3.6.8 Zutrittsberechtigung entziehen/sperren ... Seite 138
3.6.8.1 Sperren über die Berechtigungsmatrix ... Seite 138
3.6.8.2 Sperren über das Menü Transponder ... Seite 139
3.6.8.3 Sperren und Ersetzen mit einem anderen Transponder (DoT) ... Seite 142
3.7 Speichern ... Seite 145
3.7.1 Speichern in DoT-Anlagen mit FGTs und Übertragung der Daten ... Seite 146
3.7.2 Speichern in Online-Anlagen und Übertragung der Daten ... Seite 146
3.8 Programmierung ... Seite 147
3.8.1 Programmierung der Transponder (DoT-Anlagen) ... Seite 147
3.8.1.1 Programmierung der Transponder über FGT (DoT-Anlagen) ... Seite 149
3.8.2 Programmierung der Transponder (nonDoT-Anlagen) ... Seite 149

3.8.3 Programmierung der Türen/Zutrittspunkte ..... Seite 150
3.8.4 Türen mit Programmiergerät programmieren ..... Seite 152
3.8.5 Programmierung der Türen in Online-Anlagen ..... Seite 153
3.9 Quittierung ..... Seite 154
3.9.1 Quittierung Anlagen in DoT-Anlagen mit FGT ..... Seite 155
3.9.2 Quittierung in Online-Anlagen ..... Seite 155
3.10 Daten aktualisieren ..... Seite 155
3.11 Transponder an Personen ausgeben und programmieren (DoT) ..... Seite 156

4. Grundfunktionen des BKS KeyManagers ..... Seite 158

4.1 Hinzufügen neuer Komponenten durch Import der KWD-Datei ..... Seite 158
4.2 Transponder ..... Seite 160
4.2.1 Transponder hinzufügen ..... Seite 161
4.2.1.1 Neue Transponder (Verwaltungsmodul) ..... Seite 163
4.2.2 Transponder ausgeben ..... Seite 164
4.2.2.1 Transponder ausgeben in DoT-Anlagen ..... Seite 165
4.2.2.2 Transponder ausgeben in nonDoT-Anlagen ..... Seite 172
4.2.2.3 Transponderausgabe (Verwaltungsmodul) ..... Seite 174
4.2.3 Transponderrückgabe ..... Seite 175
4.2.3.1 Transponderrückgabe (Verwaltungsmodul) ..... Seite 176
4.2.4 Transponder verloren/gefunden ..... Seite 177
4.2.4.1 Transponder als Verloren markieren, aber die Berechtigungen nicht sperren ..... Seite 177
4.2.4.2 Transponder als Verloren markieren und den Zutritt zu den Türen sperren ..... Seite 178
4.2.4.3 Verlorener Transponder ist gefunden worden ..... Seite 179
4.2.4.4 Transponder verloren/gefunden (Verwaltungsmodul) ..... Seite 180
4.2.5 Transponder defekt/repariert ..... Seite 181
4.2.5.1 Transponder defekt (Verwaltungsmodul) ..... Seite 183
4.2.6 Transponder entfernen ..... Seite 184
4.2.7 Transpondergruppen (DoT) ..... Seite 186
4.2.8 Transponder ändern ..... Seite 189
4.2.9 Feuerwehr-Transponder ..... Seite 194
4.2.10 Batteriestatus der Transponder abfragen (DoT) ..... Seite 196
4.2.11 Ereignisse aus den Transpondern lesen ..... Seite 196
4.2.12 Transponder mit mechanischen Schlüsseln verbinden ..... Seite 197
4.2.13 Verbindung Transponder mit mechanischen Schlüsseln lösen ..... Seite 199
4.3 Türen/Zutrittspunkte ..... Seite 201
4.3.1 Anlegen neuer Türen/Zutrittspunkte ..... Seite 202
4.3.2 Einstellungen Türen/Zutrittspunkte ..... Seite 208
4.3.3 Türen/Zutrittspunkte löschen ..... Seite 209
4.3.4 Berechtigungen zu Türen/Zutrittspunkte ..... Seite 210
4.4 Türgruppen (Gruppen von Zutrittspunkten) ..... Seite 212
4.4.1 Türgruppen hinzufügen ..... Seite 213
4.4.2 Türgruppen entfernen ..... Seite 213
4.4.3 Türgruppen ändern ..... Seite 214
4.4.4 Zuordnung der Türgruppen ..... Seite 214
4.5 Personen ..... Seite 216
4.5.1 Personen hinzufügen ..... Seite 216
4.5.2 Personen bearbeiten ..... Seite 217
4.5.3 Personen entfernen ..... Seite 218
4.5.4 Personenlisten importieren ..... Seite 219
4.5.5 Transponder automatisch zuordnen ..... Seite 223
4.6 Berichte ..... Seite 224

4.6.1 Ereignisjournal ... Seite 224
4.6.1.1 Sicherheitsstufen beim Zugriff auf die Ereignisjournale ... Seite 228
4.6.1.2 Löschung von personenbezogenen Daten ... Seite 230
4.6.2 Laufliste ... Seite 231
4.6.3 Status der Freigabeterminals (FGT Status) ... Seite 232
4.6.4 Bediener-Log ... Seite 233
4.6.5 Berechtigungen der Türen/Zutrittspunkte ... Seite 234
4.6.6 Berechtigungen der Transponder und Personen ... Seite 235
4.6.7 Anzeige der Personenliste, Personalstatistik ... Seite 236
4.6.8 Transpondergruppen (Berechtigungen) ... Seite 237
4.6.9 Matrix ausdrucken (Berechtigungen) ... Seite 238
4.6.10 Zutrittspunktliste (Konfiguration) ... Seite 239
4.6.11 Transponderliste (Konfiguration) ... Seite 240
4.6.11.1 Sicherheitsstufen beim Zugriff auf die Transponderliste ... Seite 241
4.7 Zeitzonen und Sondertage für Zutrittsberechtigungen ... Seite 243
4.7.1 Einrichtung und Bearbeitung der Zeitzonen ... Seite 243
4.7.2 Einrichten und Bearbeiten der Sondertage ... Seite 247
4.7.2.1 Auswahl der Ansicht der Sondertage (A) ... Seite 248
4.7.2.2 Sondertage aus den Vorlagen importieren (B) ... Seite 249
4.7.2.3 Zusätzliche Sondertage hinzufügen (C) oder bearbeiten ... Seite 250
4.8 Listenmenü ... Seite 253
4.8.1 Transponder (Listenansicht) ... Seite 253
4.8.2 Transpondergruppen (Listenansicht) ... Seite 253
4.8.3 Türen/Zutrittspunkten (Listenansicht) ... Seite 254
4.8.4 Türgruppen/Gruppen von Zutrittspunkten ... Seite 254
4.8.5 Personen (Listenansicht) ... Seite 255
4.8.6 Zeitzonen (Listenansicht) ... Seite 255
4.8.7 Sondertage (Listenansicht) ... Seite 256

5. Einstellungen ... Seite 257

5.1 Anlagen-Einstellungen ... Seite 258
5.1.1 Globale Einstellungen der Anlage ... Seite 259
5.1.1.1 Programmiergerät ... Seite 259
5.1.1.2 Sicherheitsstufen beim Zugriff auf Ereignisjournal und Transponderliste ... Seite 260
5.1.1.3 Sommerzeit ... Seite 263
5.1.2 Standardeinstellungen für die ausgewählte Anlage ... Seite 264
5.1.2.1 Aktuelle Lizenzen ... Seite 264
5.1.2.2 Standardwerte für Zutrittspunkte ... Seite 265
5.1.2.3 Gültigkeitsverlängerung der Transponder ... Seite 266
5.1.2.4 Anzeigeoptionen in der Matrix ... Seite 266
5.1.2.5 Anlagenpasswort verwenden ... Seite 266
5.1.2.6 Optionen ... Seite 266
5.2 Programmiergerät ... Seite 267
5.2.1 Zeitabgleich Programmiergerät ... Seite 267
5.2.2 Update Programmiergerät ... Seite 268
5.3 Lizenzen erweitern ... Seite 269
5.4 Inbetriebnahme-Assistent ... Seite 272
5.4.1 Schließanlage mit der Schließanlagendatei anlegen ... Seite 273
5.4.1.1 Lizenzen der Schließanlage hinzufügen ... Seite 275
5.4.1.2 Personenlisten der Schließanlage hinzufügen ... Seite 277
5.4.1.3 Automatische Transpondervergabe ... Seite 280
5.4.2 Schließanlage anlegen (ohne Schließanlagendatei) ... Seite 281

5.4.2.1 Lizenzen der Schließanlage hinzufügen ....Seite 282
5.4.2.2 Transponder der Schließanlage hinzufügen ....Seite 283
5.4.2.3 Zutrittspunkte der Schließanlage hinzufügen ....Seite 284
5.4.2.4 Personenliste der Schließanlage hinzufügen ....Seite 287
5.4.2.5 Automatische Transpondervergabe ....Seite 290
5.5 Offline Zutrittspunkte mit altem Datenmodell auf das Neue umstellen ....Seite 291
5.6 Anlagenpasswort festlegen....Seite 292
5.7 Online-Konfiguration....Seite 293
5.7.1 Systemstatus der Dienste überprüfen ....Seite 293
5.7.1.1 Systemstatus mit dem KeyManager Online-Service Manager....Seite 294
5.7.1.2 Datenbank konfigurieren mit dem EBK Pro Server Config ....Seite 296
5.7.1.3 Anzeige des Dienstes in Windows ....Seite 296
5.7.2 Funktionen Online-Konfiguration....Seite 297
5.7.2.1 Topologie....Seite 297
5.7.2.1.1 Darstellung der Topologie....Seite 300
5.7.2.2 Zutrittspunktliste ....Seite 301
5.7.2.3 Gerätedaten aktualisieren....Seite 301
5.7.2.4 Gerätedaten aktualisieren....Seite 302
5.7.2.5 Einstellungen ....Seite 302
5.7.2.6 Schnittstellen (TCP/IP) ....Seite 303
5.7.2.6.1 DS-Manager....Seite 305
5.7.2.6.2 Settings im DS-Managers....Seite 306
5.7.2.7 Drucken und Schließen der Online-Konfiguration....Seite 308
5.7.2.7.1 Druckansicht....Seite 309
5.7.3 Konfiguration einer Data on Transponder-Anlage (DoT) mit Freigabeterminal (FGT)....Seite 310
5.7.3.1 Systemübersicht DoT-Anlage mit FGT....Seite 310
5.7.3.2 Installation für eine DoT-Anlage mit FGT ....Seite 311
5.7.3.3 Erforderliche Lizenz-Erweiterung der Schließanlage (DoT mit FGT)....Seite 312
5.7.3.4 Identifikation der IP-Adresse des BKS KeyManagers ....Seite 312
5.7.3.5 Systemstatus des EBK Pro-Dienstes....Seite 313
5.7.3.6 Konfiguration der Ethernetbuskoppler und Freigabeterminals ....Seite 313
5.7.3.6.1 Konfiguration des EBK 2 Pro ....Seite 314
5.7.3.6.2 Konfiguration des EBK Pro ....Seite 318
5.7.3.6.3 Freigabeterminal (FGT), Wandleser 2 und Ixalo Relaismodul ....Seite 321
5.7.3.7 Aktualisierung der Topologie ....Seite 322
5.7.4 Konfiguration einer Online-Anlage....Seite 323
5.7.4.1 Systemübersicht Online-Anlage....Seite 323
5.7.4.2 Installation für eine Online-Anlage ....Seite 324
5.7.4.3 Erforderliche Lizenz-Erweiterung der Schließanlage (Online) ....Seite 324
5.7.4.4 Systemstatus des Online-Dienstes....Seite 324
5.7.4.5 Funk-Zutrittspunkte mit den EBK FM / SE FM verbinden ....Seite 325
5.7.4.6 Konfiguration des Ethernetbuskopplers (EBK / EBK FM)....Seite 326
5.7.4.6.1 Liste der Schnittstellen (TCP/IP) ....Seite 327
5.7.4.6.2 Auswahl/Identifizierung der Schnittstelle im DS-Manager....Seite 328
5.7.4.6.3 Settings im DS-Manager....Seite 329
5.7.4.6.4 Einrichtung der Schnittstellen (TCP/IP) ....Seite 330
5.7.4.7 Funk-Komponenten in die Schließanlage übernehmen....Seite 331
5.7.4.8 Anzeige der Online-Zutrittspunkte in der Berechtigungsmatrix....Seite 333
5.8 Quittungen der Vorgänge ....Seite 335
5.9 Layout der Quittungen der Vorgänge ....Seite 336
5.9.1 Archivierung der Quittungen ....Seite 338

6. Benutzerverwaltung ..... Seite 339

6.1 Benutzer neu anlegen ..... Seite 339
6.1.1 Empfehlungen zur Erstellung des Passwort (DGSVO) ..... Seite 341
6.1.2 Zwei Faktor Authentifizierung des Benutzers ..... Seite 341
6.1.3 Kennwortrichtlinie ..... Seite 342
6.2 Zuordnung der Lizenzen zum Benutzer (bei Netzwerkversion) ..... Seite 343
6.3 Benutzerprofile ..... Seite 344
6.3.1 Empfehlungen zu den Benutzerrollen (DGSVO) ..... Seite 346
6.3.2 Empfehlungen zur Rechtevergabe (DGSVO) ..... Seite 346
6.3.3 Übersicht der Transaktionen|Funktionen ..... Seite 346
6.4 Benutzer ..... Seite 347
6.4.1 Benutzerdaten ..... Seite 347
6.4.2 Benutzerprofile zuordnen ..... Seite 348
6.4.3 Transaktionen ..... Seite 349
6.4.4 Anlagen ..... Seite 350
6.4.5 Türgruppen ..... Seite 351
6.4.6 Personengruppen ..... Seite 352
6.4.7 Depotgruppen ..... Seite 353
6.4.8 Transpondergruppen ..... Seite 354
6.5 Passwort des Benutzers ändern ..... Seite 355
6.6 Wechseln des angemeldeten Benutzers ..... Seite 356
6.7 Anzeige der eingeloggten Benutzer ..... Seite 357

7. Sonstiges ..... Seite 358

7.1 Schließanlagenverwaltung ..... Seite 358
7.1.1 Anlegen einer neuen Schließanlage ..... Seite 358
7.1.2 Editieren der Anlagendaten und Bezeichnungen ..... Seite 359
7.1.3 Umbenennen Schließanlage ..... Seite 360
7.1.4 Wechseln der Schließanlage ..... Seite 360
7.1.5 Löschen der Schließanlage ..... Seite 361
7.2 Datensicherung und Wiederherstellung der Schließanlagen-Datenbank ..... Seite 362
7.2.1 Datensicherung der Schließanlagen-Datenbank erstellen ..... Seite 362
7.2.2 Datensicherung beim Abmelden ..... Seite 363
7.2.3 Pfad für den Speicherort der Datensicherung festlegen ..... Seite 364
7.2.4 Wiederherstellung der Schließanlagen-Datenbank durch Datenrücksicherung ..... Seite 365
7.3 Schließanlagendatei (KWD-Datei) ..... Seite 367
7.3.1 Import einer KWD-Datei in eine Schließanlage ..... Seite 367
7.3.2 Import einer Schließanlage von Version 5 des BKS KeyManagers ..... Seite 369
7.3.3 Export der Komponenten einer Schließanlage in eine KWD-Datei ..... Seite 371
7.3.4 Export der Komponenten einer Schließanlage mit Rechten in eine KWD-Datei ..... Seite 372
7.4 Datenbank ..... Seite 373
7.4.1 Auswahl | Wechseln der Datenbank ..... Seite 373
7.4.2 Anlage einer neuen Datenbank ..... Seite 374
7.4.3 Umbenennen einer Datenbank ..... Seite 374
7.4.4 Löschen einer Datenbank ..... Seite 375
7.4.5 Wechsel von interner Datenbank auf Microsoft SQL-Datenbank ..... Seite 376
7.4.6 Wartung der Datenbank ..... Seite 378
7.5 Startbildschirm aktivieren/deaktivieren ..... Seite 379
7.6 Sprache der Benutzeroberfläche wechseln ..... Seite 380
7.7 Hilfe-Menü ..... Seite 381

7.7.1 Anleitungen zum BKS KeyManager ....Seite 381
7.7.2 Update ....Seite 382
7.7.3 Programminfo ....Seite 385
7.8 Installation Programmiergerät ....Seite 386

8. Data on Transponder-Schließanlage (DoT) ....Seite 388

8.1 Data on Transponder-Schließanlage (DoT) mit Freigabeterminal (FGT) und Offline-Zutrittspunkte ....Seite 389
8.1.1 Systemübersicht DoT-Anlage mit FGT und Offline-Zutrittspunkte ....Seite 389
8.1.2 Installationsarten DoT-Anlage mit FGT und Offline-Zutrittspunkte ....Seite 389
8.2 Data on Transponder-Schließanlage (DoT) mit Freigabeterminal (FGT) und Online-Zutrittspunkte ....Seite 390
8.2.1 Systemübersicht DoT-Anlage mit FGT und Online-Zutrittspunkte ....Seite 390
8.2.2 Installationsarten DoT-Anlage mit FGT und Online-Zutrittspunkte ....Seite 391
8.3 Data on Transponder-Schließanlage (DoT) ohne Freigabeterminal (FGT) und Offline-Zutrittspunkte ....Seite 392
8.3.1 Systemübersicht DoT-Anlage ohne FGT und Offline-Zutrittspunkte ....Seite 392
8.3.2 Installationsarten DoT-Anlage ohne FGT und Offline-Zutrittspunkte ....Seite 392

9. Online- und Offline-Schließanlagen (nonDoT) ....Seite 393

9.1 Online-Schließanlage (nonDoT) ....Seite 394
9.1.1 Systemübersicht nonDoT-Anlage online ....Seite 394
9.1.2 Installationsarten nonDoT-Anlage online ....Seite 394
9.2 Offline-Schließanlagen (nonDoT) ....Seite 395
9.2.1 Systemübersicht nonDoT-Anlage offline ....Seite 395
9.2.2 Installationsarten nonDoT-Anlage offline ....Seite 395

10. Mandanten-Modul ....Seite 396

10.1 Installation des Mandanten-Moduls ....Seite 397
10.2 Voraussetzung für die Einführung des Mandanten-Moduls ....Seite 398
10.3 Mandantenanlage auf Grundlage der Benutzerrechte ....Seite 399
10.3.1 Ansicht der Berechtigungsmatrix als angemeldeter Benutzer „Administrator“. ....Seite 401
10.3.2 Ansicht der Berechtigungsmatrix als angemeldeter Benutzer „Mandant A“. ....Seite 401
10.4 Mandantenanlage auf Grundlage von Unteranlagen und Benutzerrechten ....Seite 402
10.4.1 Einrichtung der Unteranlagen ....Seite 404
10.4.2 Verwaltung der Unteranlagen ....Seite 405
10.4.3 Zuordnung von Türen und Transpondern sowie Gruppen von diesen zu einer Unteranlage ....Seite 406
10.4.4 Freigabe von Transpondergruppen für Unteranlagen ....Seite 408
10.4.5 Zuordnung der Buskoppler und Freigabeterminals zur Unteranlage ....Seite 410
10.4.6 Freigabe von Transponder für andere Unteranlagen ....Seite 411
10.4.7 Zeitzonen im Mandanten-Modul ....Seite 413
10.4.8 Einrichtung der Benutzerrechte ....Seite 415
10.4.9 Berechtigungsmatrix mit Unteranlagen ....Seite 416
10.4.9.1 Ansicht der Hauptanlage in der Berechtigungsmatrix ....Seite 416
10.4.9.2 Ansicht der Unteranlage „Mandant A“ in der Berechtigungsmatrix ....Seite 417
10.4.10 Ansichtswechsel zwischen der Hauptanlage und den Unteranlagen ....Seite 418

1. Allgemeine Informationen

Der BKS KeyManager kann als Einzelplatz- sowie als Netzwerkversion installiert werden und ist in der Anzahl seiner Datensätze nicht limitiert. Mit dem BKS KeyManager können alle mechanischen und mechatronischen Schließzylinder inkl. der Wandleser und mechatronischen Schlösser über eine gemeinsame Oberfläche verwaltet und programmiert werden. Die Lizenzen in der Netzwerkinstallation sind flexibel übertragbar.

Funktionen des BKS KeyManagers:

- Individuelle Benutzerverwaltung.
- Anlagenübergreifender Personalstamm (Importmöglichkeit von Personendaten über CSV- oder TXT-Dateien).
- Anlagenübergreifende Abfragen (bequemer Import der BKS Anlagendaten über BKS Datenträger).
- Verwaltung von mehreren Schließanlagen.
- Programmierung der ixalo Produkte über Schließplanmatrix.
- Komfortable Zeitzonenprogrammierung.
- Tagesfreigaben entweder manuell, halb automatisch oder automatisch.
- Ereignisspeicherung kann vom Nutzer selbst aktiviert oder deaktiviert werden.
- Steuerung von Sondertagen sowie Ferienzeiträumen über Kalenderfunktion.
- Komfortable Journalfunktionen.
- Gemeinsame Verwaltung von mechanischen und mechatronischen Schließzylindern, Wandlesern und mechatronischen Schlössern mit integrierter Anzeige der Zeitzonen.
- Komponenten der Anlage und die IDs werden komfortabel über den Import der Schließanlagendatei als Anlagendaten eingelesen.

1.1 Warnsymbole

ACHTUNG

ACHTUNG bezeichnet eine möglicherweise schädliche Situation.

- **Wenn sie nicht gemieden wird, kann die Anlage oder etwas in ihrer Umgebung beschädigt werden.**

HINWEIS

HINWEIS kennzeichnet eine rein informative Aussage.

1.2 Systemanforderungen

Betriebssystem	■ Windows Server 2016 (64-Bit) ■ Windows 10 (64-Bit) ■ Windows 11 (64-Bit)
Arbeitsspeicher	■ Mindestens 2 GB Arbeitsspeicher
Festplatten-speicherplatz	■ Für den BKS KeyManager und die Datenbank muss ein ausreichend großer freier Speicherplatz von mindestens 500 MB vorhanden sein.
Prozessor	■ Für die Installation auf einen Einzelarbeitsplatz wird ein aktueller Workstationprozessor z.B. Intel i5 der aktuellen Generation empfohlen. ■ Für Multiuser-Installationen wird ein aktueller Server-Prozessor z.B. Intel Xeon der aktuellen Generation empfohlen. ■ Mehrere Prozessoren bzw. Prozessorkerne erhöhen die Leistung.
Display/Monitor	■ Mindestens 1024 x 768 Pixel Auflösung
Eingabegerät	■ Tastatur, Maus, Programmiergerät (Optional: und SignoTec-Signatur-Pad)
Virtueller Computer	Virtuelle Maschinen (VMware) können verwendet werden, wenn sie mindestens die oben aufgeführten Systemvoraussetzungen erfüllen.
Bei Verwendung einer virtuellen Maschine (VM) ist die Nutzung von Snapshots, das Klonen oder das Zurücksetzen auf einen zuvor festgehaltenen Ausführungs- oder Sicherungsstand <u>nicht empfohlen</u>. **-> Benutzen Sie zur Datensicherung die integrierte Funktion.**	
Vernetzung	Bei der Verwendung von Client-Server Installationen oder der Vernetzung von Online-Komponenten wie EBK, EBKFM, SEFM, EBK Pro oder EBK 2 Pro sollte ein eigenes Netzwerk (z.B. VLAN) für die elektronische Schließanlage zur Verfügung stehen. Alle Komponenten müssen im gleichen Netzwerksegment miteinander verbunden sein. Das Netzwerk (inklusive Firewalls, Switches, Virenscanner, ...) ist so zu konfigurieren, dass die Kommunikation über die angegebenen Ports jederzeit möglich ist. Es sollte zur Sicherheit ausschließlich für das elektronische Schließsystem verwendet werden.
Portfreigaben	■ Der Microsoft SQL Server verwendet die Ports: TCP: 1433, 1434 | UDP: 1434 ■ Das SignoTec-Signatur-Pad verwendet den Port 49494 Vom BKS KeyManager ausgehende Ports: ■ KeyManager -> EBK / EBKFM: TCP: 12090 und UDP: 65535 ■ KeyManager -> EBK Pro: UDP: 65006 ■ KeyManager -> EBK 2 Pro: UDP: 65006 Zum BKS KeyManager eingehende Ports: ■ EBK / EBKFM -> BKS KeyManager: UDP: 65534 ■ EBK Pro -> BKS KeyManager: TCP: 8090 | TCP: 80 | TCP: 443 | UDP: 65005 ■ EBK 2 Pro -> BKS KeyManager: TCP: 8097 | TCP: 5001 | TCP: 443 | UDP: 65005

ACHTUNG

Firewall: Eingehende Regeln			
Name	Typ	Execute-File	Port
MS SQL Browser UDP	UDP	\\Program Files\Microsoft SQL Server\130\Shared\sqlbrowser.exe	1434
MS SQL Browser	TCP	\\Program Files\Microsoft SQL Server\130\Shared\sqlbrowser.exe	Alle
MS SQL Server MX_DB_KM	TCP	\\Program Files\Microsoft SQL Server\MSSQL13.MX_DB_KM\MSSQL\Binn\sqlservr.exe	Alle
Datenbank	Als Datenbanksystem wird ein Microsoft SQL Server 2016 oder eine interne Datenbank verwendet. Für Client-Server-Installationen oder bei Nutzung des BKS KeyManagers Online-Dienstes bzw. EBK Pro-Dienstes ist der Microsoft SQL Server zu verwenden.		
Programmiergerät	Zur Kommunikation mit dem Programmiergerät wird ein USB-Treiber vom Setup installiert.		

HINWEIS

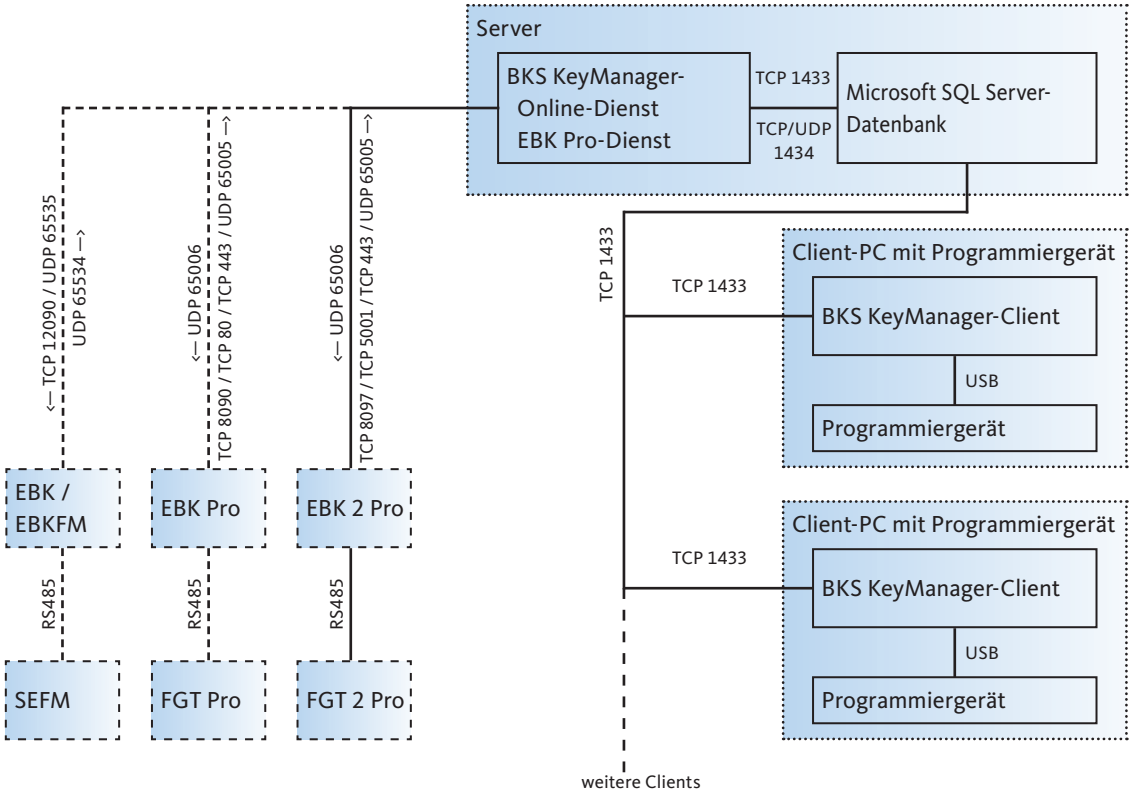
Die Systemanforderungen gelten pro Schließanlage.

1.3 Systemarchitektur

Übersicht der vier Programmversionen des BKS KeyManagers:

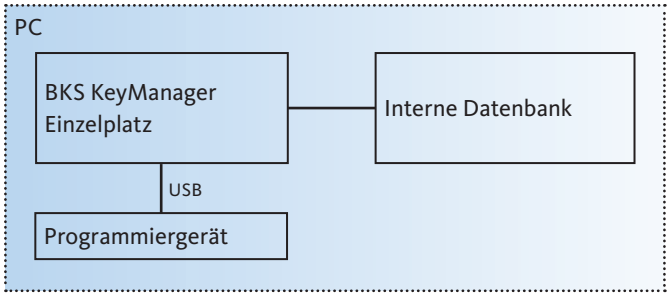
Einzelplatz- und Serverversion mit Microsoft SQL Server
Empfohlene Standardinstallation für Einzelplatz- und Serverinstallationen mit Benutzeroberfläche zur Verwaltung und Programmierung auf einer Microsoft SQL Server Datenbank. Verwaltung von Online- und Offline Anlagen. ■ Verwendung von Data on Transponder (mit Freigabeterminal) wird unterstützt. ■ Erweiterung um Client-Arbeitsplätze ist möglich. Empfohlene Verwendung bei mittleren und großen Anlagen sowie bei Anbindung von Client-Arbeitsplätzen.
Clients der Netzwerkversion
Empfohlene Standardinstallation für Client-Arbeitsplätze mit Benutzeroberfläche zur Verwaltung, Programmierung und zum Zugriff auf eine bereits vorhandene BKS KeyManager-Datenbank auf einem Microsoft SQL Server.
Einzelplatzversion mit interner Datenbank
Einzelplatz-Installation mit interner Datenbank für Anlagen im Offline Betrieb oder Data on Transponder-Betrieb (ohne Freigabeterminal). Diese Version ist nicht netzwerkfähig und kann nicht mit Online-Produkten verwendet werden. Die Erweiterung um Client-Arbeitsplätze ist mit der internen Datenbank nicht möglich. Empfohlene Verwendung bei Einzelplatzinstallationen in kleineren Anlagen, ohne Online- oder Data on Transponder-Modul.
Server der Netzwerkversion
Spezielle Server-Installation ohne Benutzeroberfläche mit Microsoft SQL Server zur Anbindung von Client-Arbeitsplätzen. Empfohlene Verwendung in Verbindung mit Microsoft Servern und Terminal-Zugriff.

1.3.1 Systemdarstellung Client-Server-Installation



EBK	-	Ethernet-Buskoppler
EBK Pro	-	Ethernet-Buskoppler Professional
EBK 2 Pro	-	Ethernet-Buskoppler 2 Professional
FGT Pro	-	Freigabeterminal Professional
FGT 2 Pro	-	Freigabeterminal 2 Professional
EBKFM	-	Ethernet-Buskoppler mit Funkwandmodul
SEFM	-	SE Funkwandmodul

1.3.2 Systemdarstellung Einzelplatzversion mit interner Datenbank



1.3.3 Funktionelle Unterscheidung der Schließanlagen

Der elektronische BKS KeyManager verwaltet sechs verschiedene Typen von Schließanlagen. Diese unterscheiden sich durch den Speicherort der Zutrittsberechtigungen und der Datenübertragung bzw. der Art der Programmierung. Darüber hinaus besteht durch die in der Schließanlage verwendeten Produkte eine Abhängigkeit zum Anlagentyp.

Der Speicherort der Zutrittsberechtigungen und Zutrittsinformationen unterteilt die Schließanlagen in **Data on Transponder**- (DoT) und **On- und Offline**-Anlagen (nonDoT). In DoT-Anlagen sind die Einzelberechtigungen auf dem Transponder gespeichert, währenddessen die Daten bei nonDoT-Anlagen in den Zutrittspunkten gespeichert werden.

Die Übertragung der Daten zwischen dem BKS KeyManager und den Zutrittspunkten sowie den Transpondern (nur DoT) ist über eine direkte oder eine indirekte Verbindung möglicht.

In reinen **Offline-Anlagen** werden die Daten indirekt durch eine Programmierung der Komponenten mit einem Programmiergerät übertragen. Zur Übermittlung wird das Programmiergerät mit dem BKS KeyManager verbunden und die Daten eingespielt. Die Programmierung des Zutrittspunkts wird vor Ort an der Tür ausgeführt. Vorteile sind eine einfache Installation und Einrichtung. Eine Verkabelung ist beispielsweise bei diesen Anlagen nicht notwendig.

Bei **Online-Anlagen** ist der BKS KeyManager über einen Ethernet-Buskoppler (EBK) und Funkmodul direkt mit den Türen verbunden. Die Daten werden auf direktem Weg zum Zutrittspunkt übertragen. Der Komfort der Programmierung auch über größere Entfernungen sind bei diesem Anlagentyp von Vorteil. Eine weitere Option besteht in der Möglichkeit, das Teile der Schließanlage wie eine Offline-Anlage betrieben werden können.

Mit dem **Freigabeterminal** (FGT) werden in DoT-Anlagen die Vorteile von Offline- und Online-Anlagen kombiniert. Basis dieses Systems ist die direkte Anbindung des FGTs an den BKS KeyManager mit einem EBK als Bindeglied. Während des Betriebs der Anlage werden die Transponder, welche sich am FGT einbuchen, mit den aktuellen Daten aus dem BKS KeyManager programmiert. Bei Präsentation des Transponders am Zutrittspunkt öffnet sich dieser (bei vorhandener Berechtigung) und die zuvor empfangenen Daten werden vom Transponder zur Tür übertragen.
In der Praxis ist es empfehlenswert, dass die FGT möglichst an zentralen Punkten wie z. B. dem Haupteingang eingerichtet werden, damit die Transponder sich möglichst oft an den FGTs einbuchen, um eine kontinuierliche Datenübertragung zwischen BKS KeyManager, Transpondern und Zutrittspunkten zu ermöglichen.

- Typen der Data on Transponder-Schließanlage (DoT)
  → siehe Kapitel 9 [393]
  - **Data on Transponder-Schließanlage (DoT) mit Freigabeterminal (FGT) und Offline-Zutrittspunkte**
    → siehe Kapitel 8.1 [389]
  - **Data on Transponder-Schließanlage (DoT) mit Freigabeterminal (FGT) und Online-Zutrittspunkte**
    → siehe Kapitel 8.2 [390]
  - **Data on Transponder-Schließanlage (DoT) ohne Freigabeterminal (FGT) und Offline-Zutrittspunkte**
    → siehe Kapitel 8.3 [392]

- Typen der Online- und Offline-Schließanlagen (nonDoT)
  → siehe Kapitel 9 [393]
  - **Online-Schließanlage (nonDoT)**
    → siehe Kapitel 9.1 [394]
  - **Offline-Schließanlagen (nonDoT)**
    → siehe Kapitel 9.2 [395]

1.4 Empfehlungen zur Datenschutz-Grundverordnung (DSGVO)

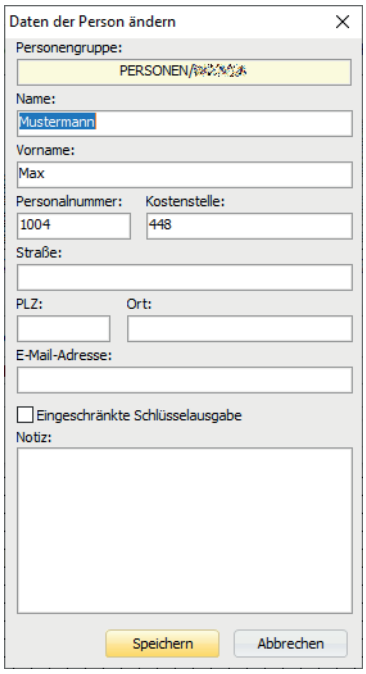
Bei der Verwendung des BKS KeyManagers ist es wichtig, dass Sie die Einhaltung der DSGVO beachten. Aus diesem Grund möchten wir Ihnen in den weiteren Kapiteln dieses Abschnitts, ohne einen Anspruch auf Vollständigkeit, Empfehlungen zur DSGVO bei der Verwendung des BKS KeyManagers geben.

1.4.1 Grundsätzliche Empfehlungen zur Datenspeicherung

Die Datenschutz-Grundverordnung verlangt, möglichst wenig personenbezogene Daten zu sammeln, einzusetzen und den Grundsatz der Datensparsamkeit zu beachten.

Personenbezogene Daten werden grundsätzlich nur gespeichert, wenn deren Verwendung durch den Zweck gerechtfertigt werden kann.

In der Personaldatenpflege des BKS KeyManagers sollen deshalb nur die Felder „Name“ und „Vorname“ des Schlüsselinhabers sowie die „Personalnummer“ und ggf. die „Kostenstelle“ gespeichert werden. Denn mit diesen gespeicherten Daten ist eine Zuordnung der Person zur Transponder-/Schlüsselausgabe und zur Zutrittsberechtigungssteuerung möglich.



1.4.2 Empfehlungen zur Datenbankinstallation

Bei der Installation des Datenbankdienstes soll darauf geachtet werden, dass der Zugriff auf den BKS KeyManager Datenbankkatalog nur für den BKS KeyManager Programmbenutzer erlaubt wird.

Bei der Verwendung des Microsoft SQL Servers sollte die Windows Authentifizierung für den Programmstart des BKS KeyManagers nicht verwendet werden, um unautorisierte Datenbankzugriffe außerhalb des BKS KeyManagers zu verhindern.

1.4.3 Empfehlungen zum werkseitigen Administrator-Zugang

Nach der Installation des BKS KeyManagers und dem ersten Programmstart ist eine Änderung des Standard-Kennwort des „BKS“-Benutzers empfohlen.

2. Installation

Der BKS KeyManager arbeitet mit zwei unterschiedlichen Datenbanken. Entweder mit der Microsoft SQL Server-Datenbank oder mit einer internen Firebird-Datenbank für Kleinstanlagen. Diese basiert auf der Microsoft.NET–Technologie, d. h. es muss eine entsprechende Laufzeitumgebung für die Microsoft SQL-Datenbank zur Verfügung stehen.

HINWEIS

Die Laufzeitumgebung (Microsoft.NET) muss vor der Einzelplatz- oder Server-Installation installiert werden. Für die Client-Installation muss eine Microsoft SQL-Datenbank im Netzwerk auf einem geeigneten physischen oder virtuellen Computer vorhanden sein.

Das Installationsprogramm erkennt selbstständig, ob die benötigten Programme auf dem Computer installiert sind und installiert bei Bedarf die fehlenden Komponenten. Unter Umständen kann durch einen fehlenden Microsoft SQL Server die Installation abgebrochen werden.

Die verwendete Microsoft SQL Server-Version hat folgende Einschränkungen:

- Beachten Sie das Kapitel „Systemanforderungen“.

Zur Installation der Software müssen Sie über Administratorrechte verfügen.

HINWEIS

Schützen Sie Ihre Daten, indem Sie Zugriffe nur berechtigten Nutzern oder Computern erlauben. Verschlüsseln Sie die Festplatte, auf der sich die Datenbank befindet und schränken Sie externe Zugriffe auf den Computer, auf den die Datenbank gespeichert ist ein. Über eine Client-Server-Installation können Sie die Zugriffe auf die Datenbank am besten sichern. Wählen Sie ein sicheres Administrationspasswort für Ihre Datenbank. Die Client-Server-Installation wird empfohlen. Ändern Sie das Installationspasswort des BKS KeyManagers.

2.1 Installationsarten

Für die Einrichtung des BKS KeyManagers existieren grundsätzlich vier Installationsarten

- Einzelplatz–Version (Microsoft SQL-Datenbank)
  Die Einzelplatz-Version ist der Standard für mittlere und große Anlagen, die ggf. auch Online-Produkte beinhalten.
  – Bei dieser Installationsart werden die interne und die Microsoft SQL-Datenbank installiert. Beim Login im BKS KeyManager kann zwischen den Datenbanken gewechselt werden.
  – Diese Installation ist für Errichter empfohlen, welche die Kunden mit unterschiedlichen Installationen bezüglich der Datenbank betreuen.
- Client-Version
  Die Client–Version wird installiert, wenn man eine weitere Arbeitsstation für den Zugriff auf eine bereits vorhandene BKS KeyManager-Datenbank einrichten möchte.
- Einzelplatz-Version (Interne Datenbank)
  Die Einzelplatz-Version wird für Kleinstanlagen installiert. Sie ist nicht netzwerkfähig und kann **nicht** mit Online-Produkten verbunden werden. Bei einem Wechsel der Datenbank kann die Sicherungskopie der internen Datenbank in die Einzelplatz-Version mit Microsoft SQL-Datenbank eingelesen werden. Zur eigentlichen Umstellung ist eine Deinstallation vor der Neuinstallation nötig.
- Serverversion
  Die Serverversion wird installiert, um auf einem geeigneten physischen oder virtuellen Computer die BKS KeyManager-Datenbank zu erzeugen.

2.2 Installation der Einzelplatz- und Serverversion mit Microsoft SQL Server

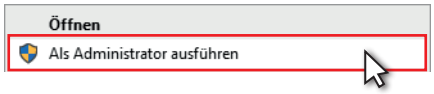
Wir empfehlen diese Installation für mittlere und große Anlagen mit Anbindung von Client-Arbeitsplätzen und Online-Funktionen.

Diese Einzelplatzversion beinhaltet die Benutzeroberfläche zur Verwaltung und Programmierung sowie eine separate Datenbank welche auf einen Microsoft SQL Server läuft. Die Daten werden in einer separaten Datenbank verwaltet. Bei der Einrichtung wird vor der Installation des BKS KeyManagers eine Microsoft SQL Server-Installation benötigt.

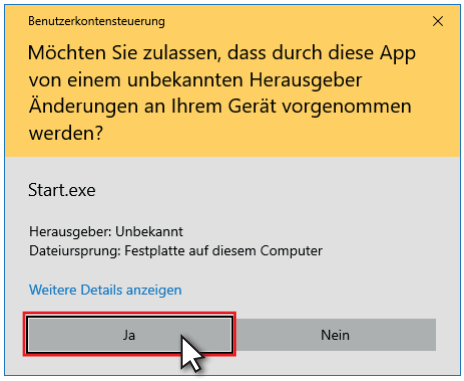
Bei Verwendung dieses Setups ist eine Rückstellung auf eine interne Datenbank nicht möglich.

Sollte der Installationsassistent des BKS KeyManagers nach dem Einlegen des Speichermediums nicht automatisch gestartet werden oder es wird ein anderes Installationsmedium wie z. B. USB-Datenträger oder Download verwendet, ist die Installation manuell zu starten.

- Öffnen Sie den Windows Explorer und navigieren zum Speicherort der Installationsdaten z. B. USB, DVD oder Stammverzeichnis (Root) und öffnen den Installationsordner.
- Sind die Installationsdateien in einem ZIP-Archiv abgelegt, so ist der Inhalt des ZIP-Archivs vor der Installation über das Kontextmenü „Alle extrahieren ...“ in das Stammverzeichnis (Root) des Computers z. B. „C:\“ bzw. „OS (C:)“ zu entpacken.
- Starten Sie den Installationsassistent:
  - Wählen Sie über das Kontextmenü die Datei „ Start.exe“ aus.
  - Führen Sie die Datei „Start.exe“ als Administrator aus.



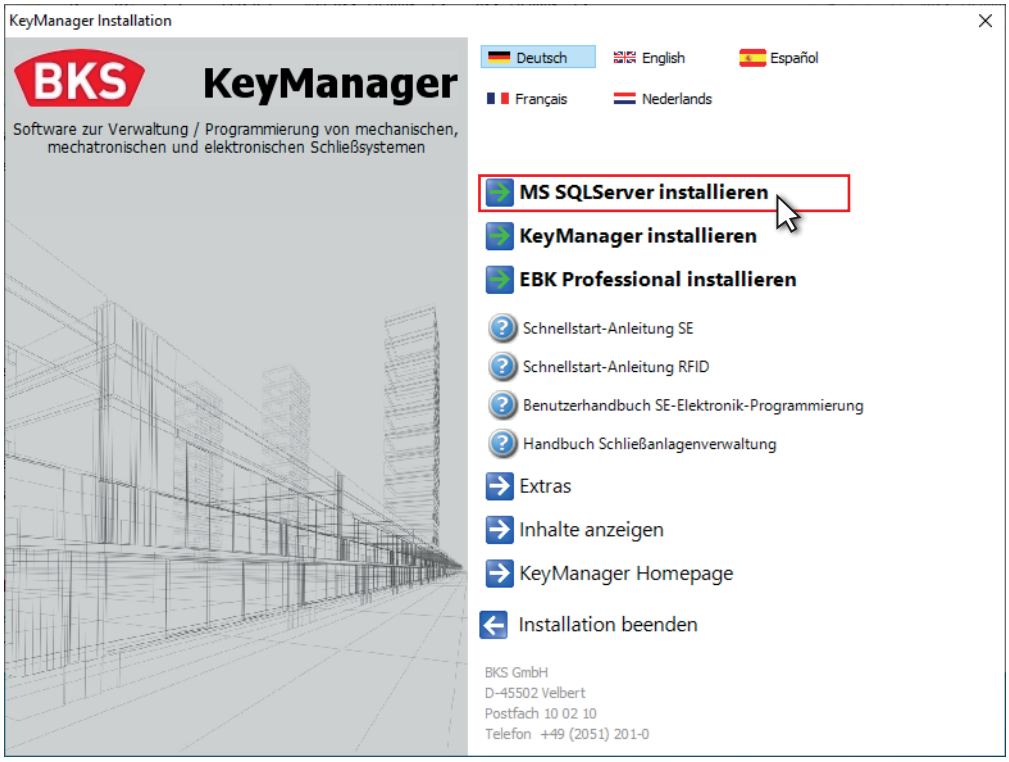
HINWEIS **Bestätigen Sie die während der Installation auftretende Sicherheitswarnung mit „Ja“. Diese treten je nach Sicherheitseinstellung Ihres Systems auf.**



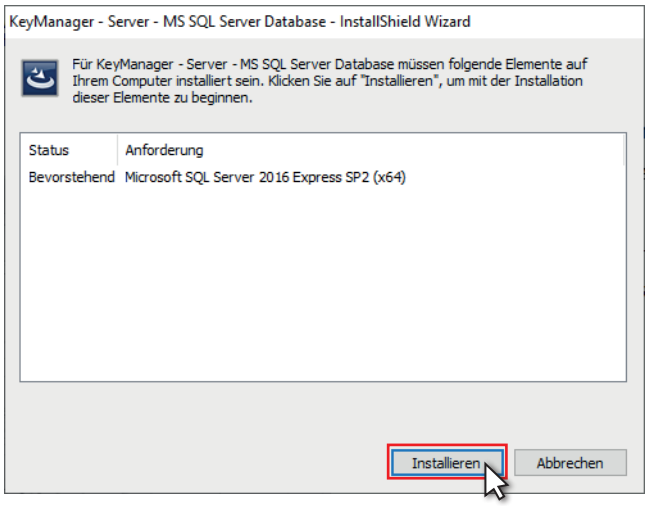
2.2.1 Installation des Microsoft SQL Servers

Die Installation des Microsoft SQL Servers wird durch Auswählen des Menüpunktes gestartet.

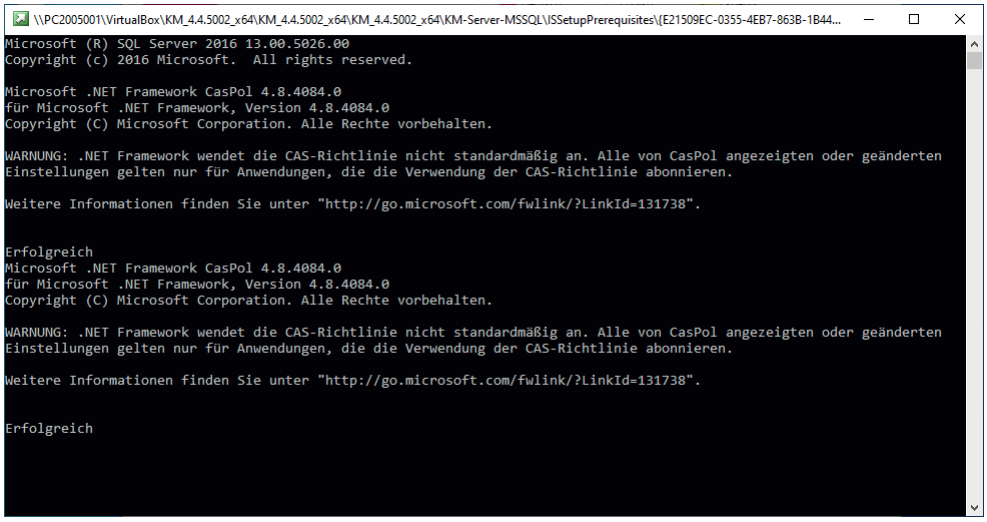
- Drücken Sie den Menüpunkt „Microsoft SQL Server installieren“.



- Drücken Sie auf den Button „Installieren“.



Die Installation verläuft größtenteils im Hintergrund. Bei dem angezeigten Fenster ist keine Benutzeraktion erforderlich. Folgendes Fenster ist während der Installation sichtbar:

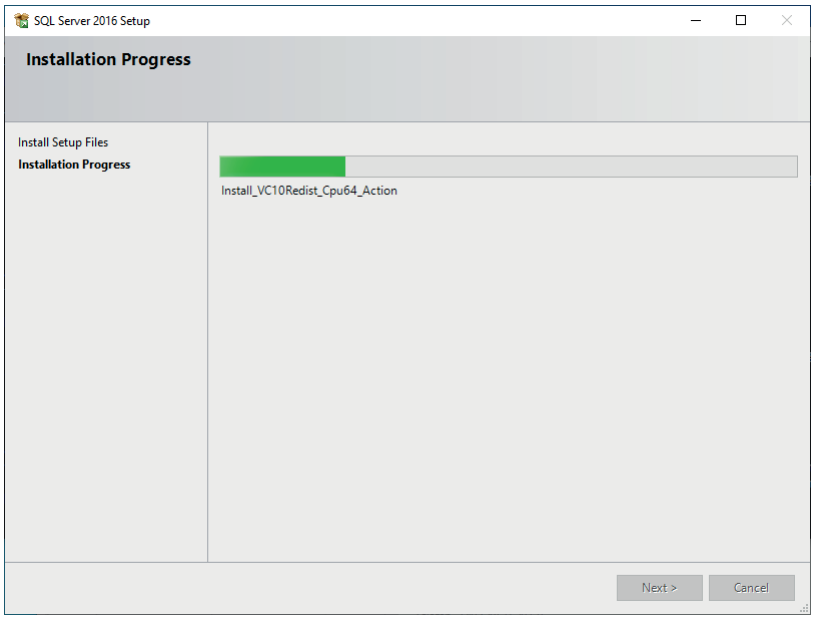


HINWEIS

Sollte die Installation an diesem Punkt abbrechen, überprüfen Sie den Speicherort des Installationsordners. Der Ordner mit den Installationsdateien sollte sich im obersten Verzeichnis des jeweiligen Laufwerks befinden. Bei einem zu langen Pfad wird die Installation abgebrochen.

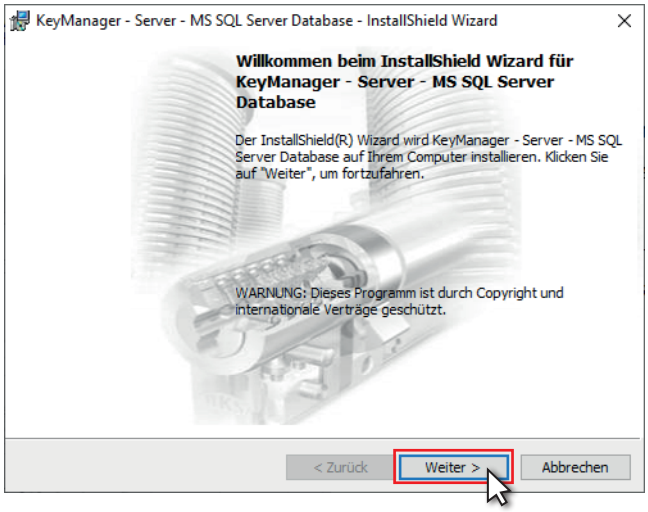
→ **Extrahieren bzw. Entpacken Sie die Installationsdateien in das Stammverzeichnis (Root) des Computers z. B. „C:\“ bzw. „OS (C:)“ und starten die Installation erneut.**

Schließen Sie das Fenster nicht und warten Sie, bis die Installation abgeschlossen ist.

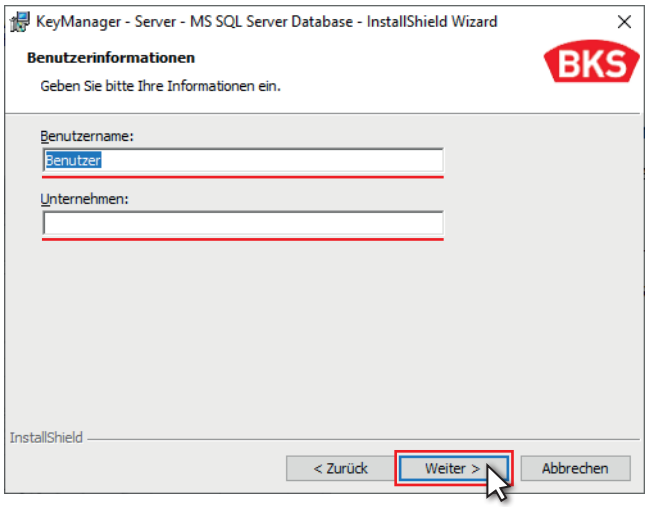


Das Setup zur Installation der Datenbank-Instanz (MX_DB_KM) startet automatisch nach Beendigung der Microsoft SQL Server Installation.

- Drücken Sie auf den Button „Weiter >“.



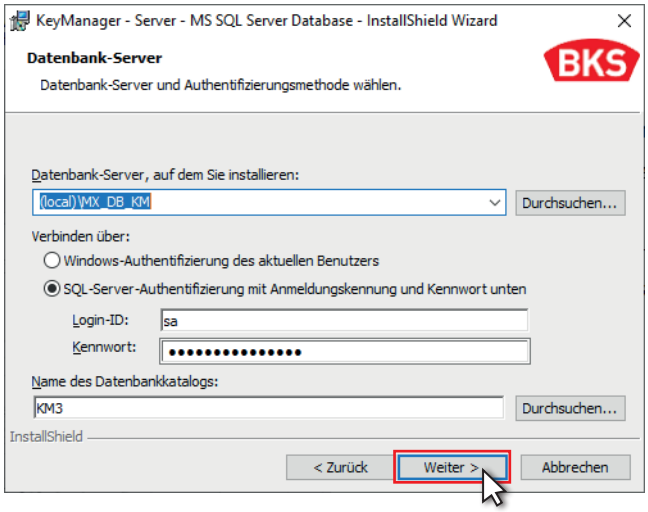
- Geben Sie ggf. Ihre Benutzerinformationen ein und drücken auf den Button „Weiter >“.



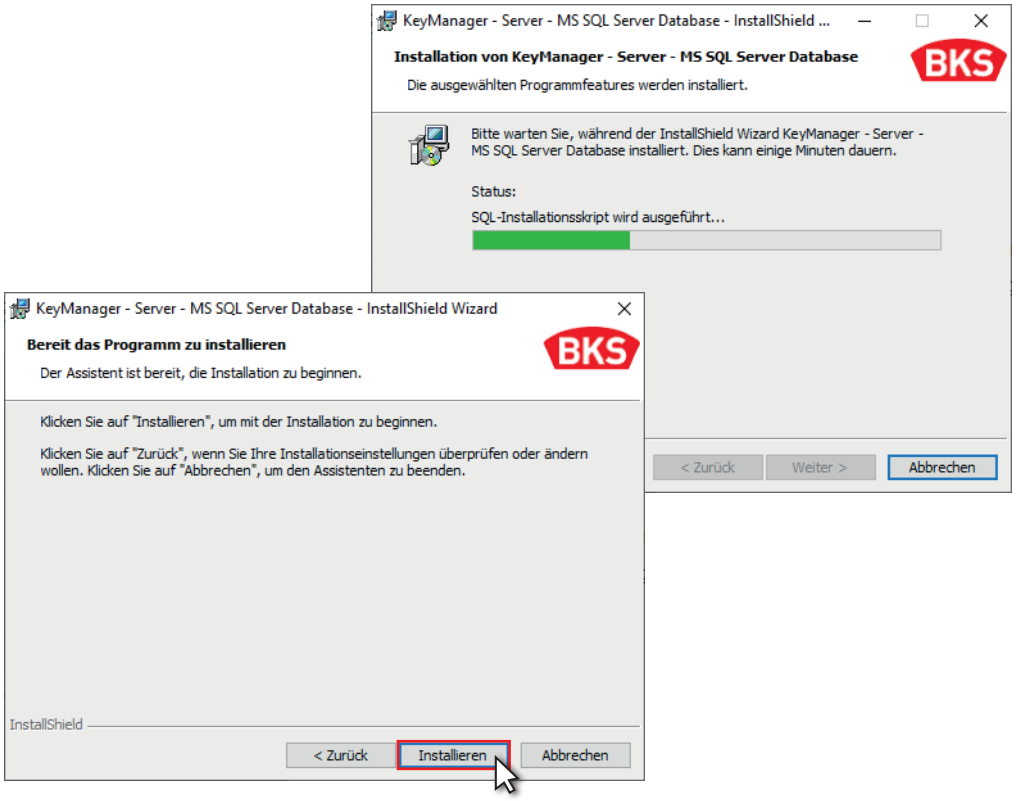
Über das folgende Fenster kann die Voreinstellungen übernommen bzw. angepasst werden.

Wählen Sie ggf. mit „Durchsuchen“ einen anderen Datenbank-Server für den BKS KeyManager aus.

- Drücken Sie auf den Button „Weiter >“.

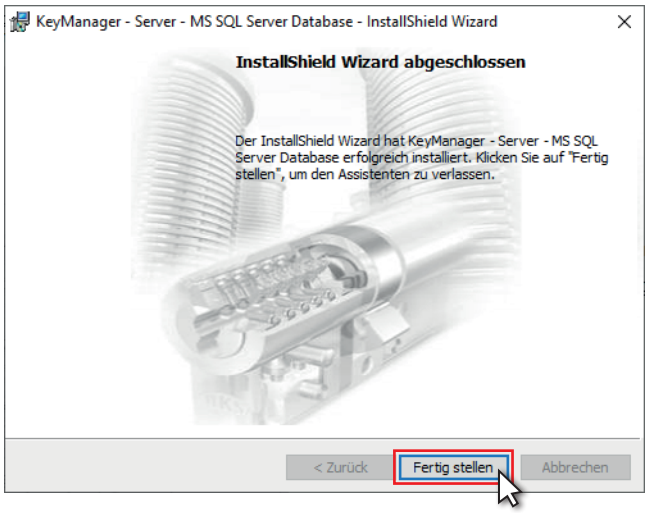


■ Starten Sie die Einrichtung durch Drücken des Buttons „Installieren“.



■ Zur Beendigung der Installation drücken Sie auf den Button „Fertigstellen“.

Nach erfolgreicher Installation werden die Fenster automatisch geschlossen.

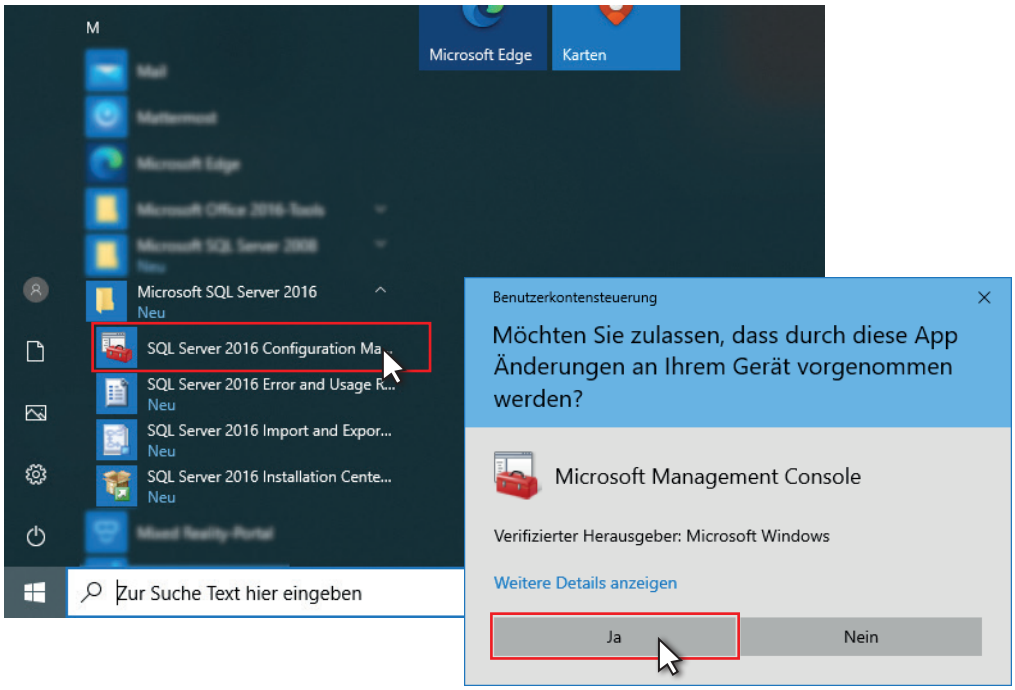


2.2.2 Konfiguration des Microsoft SQL Servers bei Client-/Serverinstallation

Vor dem Einsatz des BKS KeyManagers muss der Microsoft SQL Server konfiguriert werden.

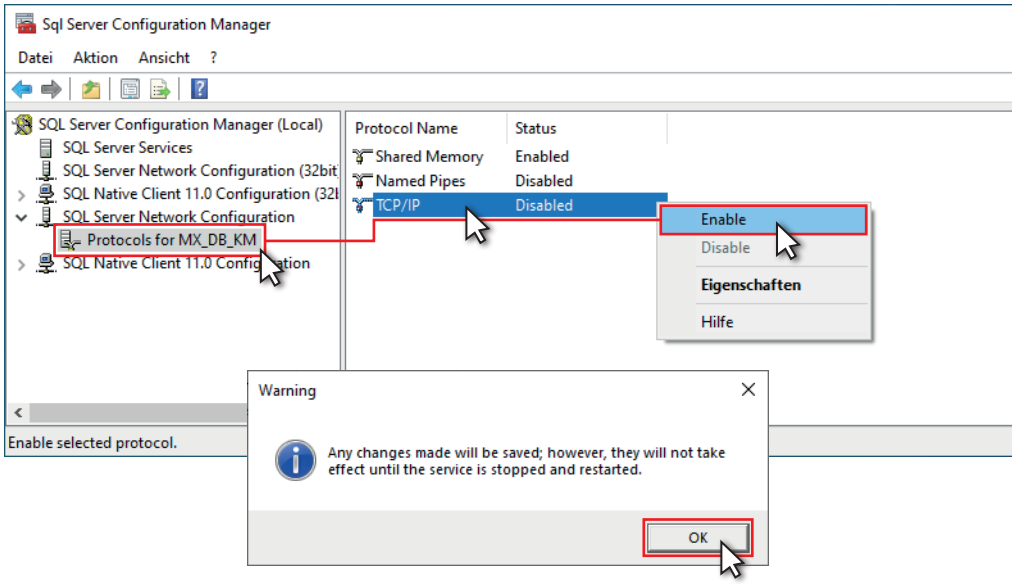
- Starten Sie den „SQL Server Configuration Manager“ und drücken zur Bestätigung auf „Ja“.

HINWEIS **Damit ein Client mit dem Server kommunizieren kann, muss eine evtl. vorhandene Firewall so konfiguriert werden, dass der Microsoft SQL Server nicht behindert wird.**



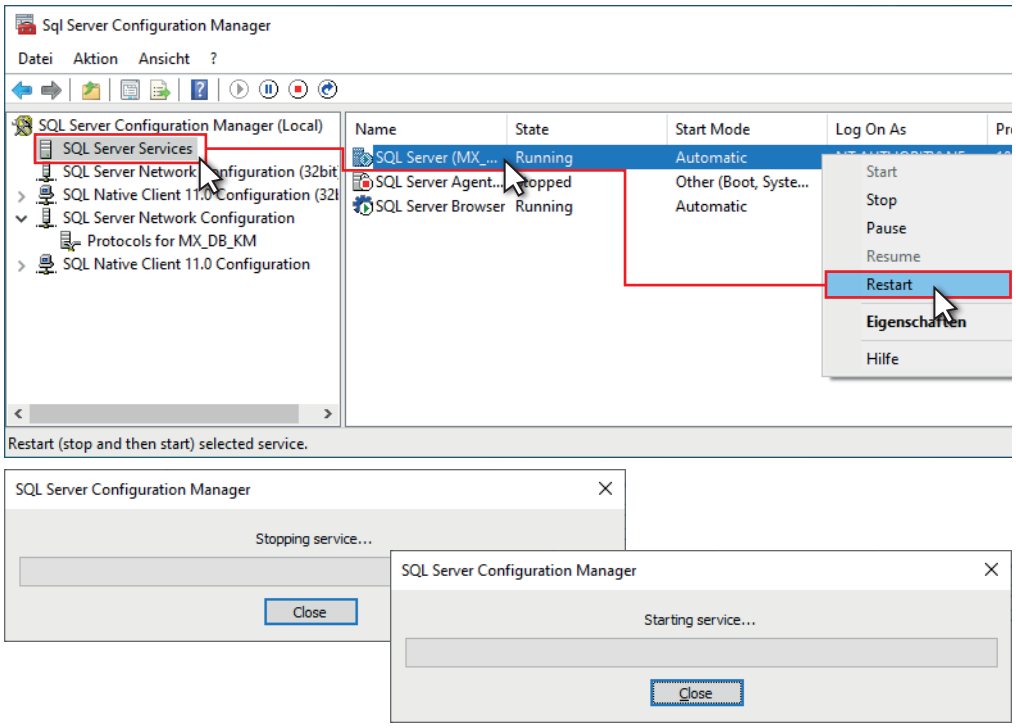
Die TCP/IP-Verbindungen des Microsoft SQL Servers müssen aktiviert sein.

Setzen Sie den Status auf „Enable“ und drücken zur Bestätigung auf „OK“.

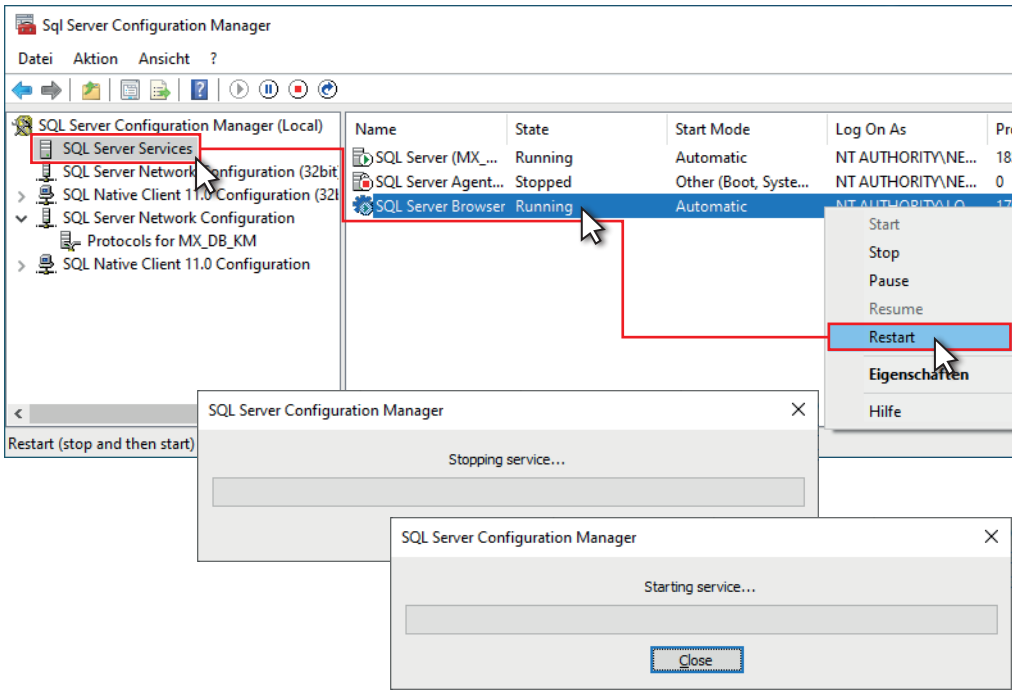


Der Dienst „SQL Server Services“ muss neu gestartet werden.

Setzen Sie den State des „SQL Server (MX_DB_KM)“ auf „Restart“.



■ Setzen Sie den State des „SQL Server Browser“ auf „Restart“.



Der Microsoft SQL Server für die Netzwerkversion ist jetzt einsatzbereit.

2.2.3 Installation der Einzelplatzversion

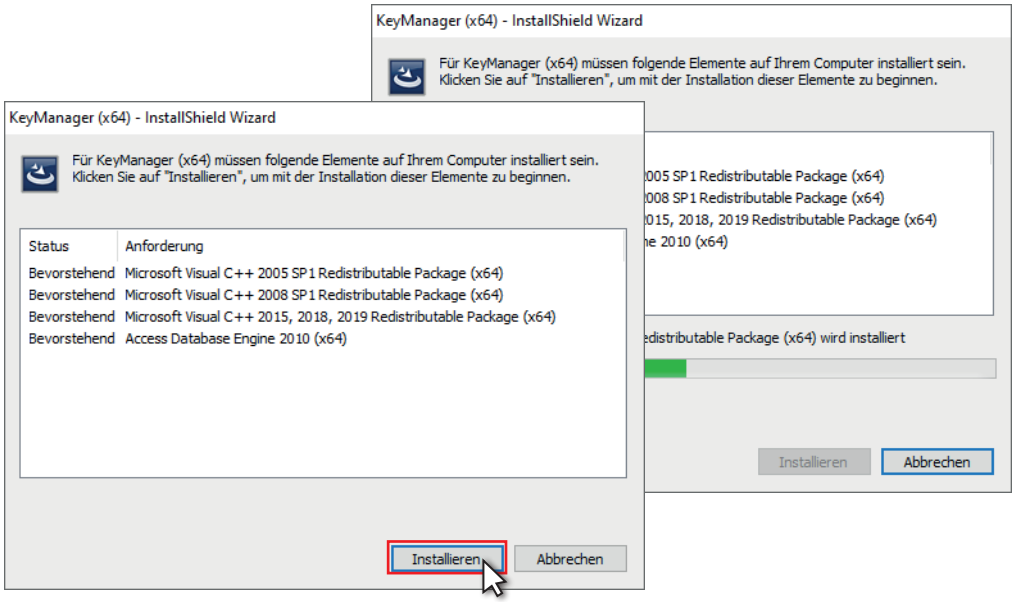
Vor der Installation der Einzelplatz- und Serverversion muss, wie in vorangegangen Kapiteln beschrieben, der Microsoft SQL Server installiert und konfiguriert werden.

Die weitere Installation des BKS KeyManagers wird durch Auswählen des Menüpunktes gestartet.

- Drücken Sie auf den Menüpunkt „KeyManager installieren“.

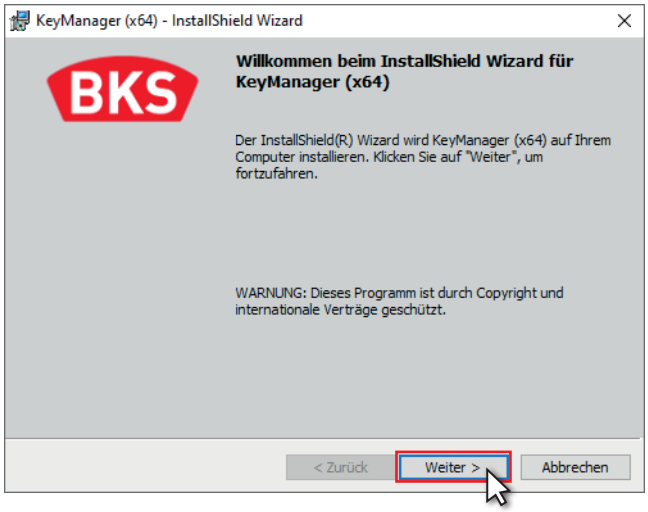
Identifikation und Installation fehlender Treiber und Module vor der BKS KeyManager-Installation.

- Drücken Sie auf den Button „Installieren“, um den Vorgang zu starten.



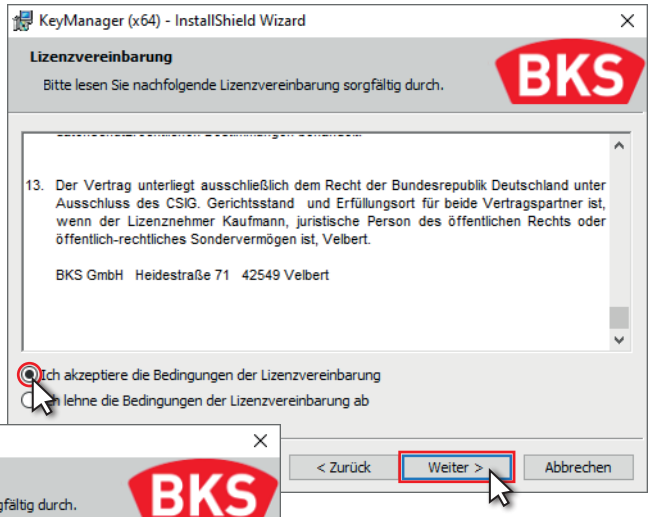
Der BKS KeyManager bereitet die Installation vor.

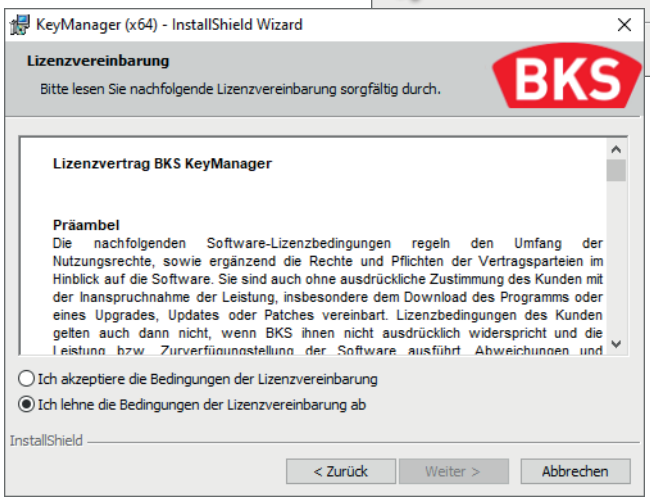
Drücken Sie auf den Button „Weiter >“, um die Installation fortzusetzen.



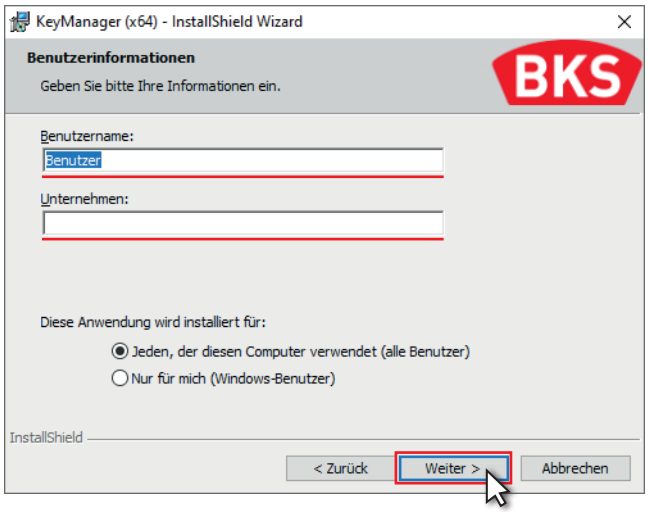
Lesen Sie sich den Lizenzvertrag sorgfältig durch.

- Akzeptieren Sie die gelesenen Bedingungen und Lizenzvereinbarung und drücken auf den Button „Weiter >“.

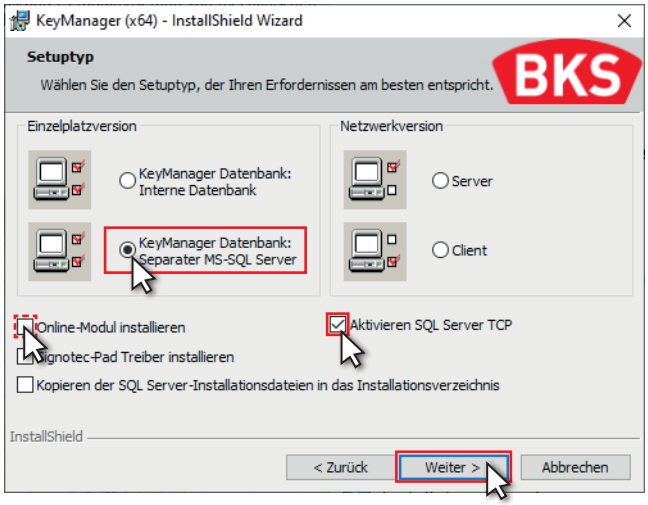




- Geben Sie ggf. Ihre Benutzerinformationen ein und drücken Sie auf den Button „Weiter >“.



- Zur Fortsetzung der Installation aktivieren Sie die Checkbox „KeyManager Datenbank: Separater Microsoft SQL Server“.
- Beabsichtigen Sie den BKS KeyManager in Ihrem Netzwerk als Server einzusetzen, aktivieren Sie auch die Checkbox „Aktivieren SQL Server TCP“, um den Microsoft SQL Server hierzu automatisch zu konfigurieren.



Optional haben Sie die Möglichkeit die folgenden Erweiterungen auszuwählen:

— Wenn Sie in Ihrer Anlage Ethernetbuskoppler (EBK) mit online angebundenen Zutrittspunkten und/oder Freigabeterminals (FGT) verwenden und mit dem BKS KeyManager verbinden möchten, aktivieren Sie die Checkbox „SE-Online-Modul installieren“.

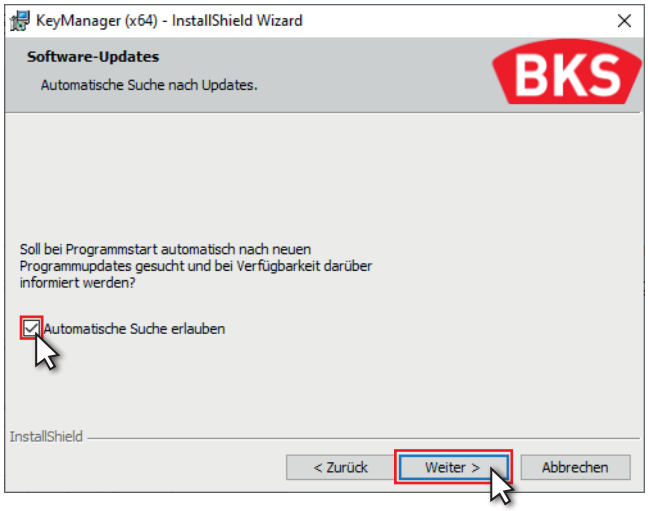
— Wenn in Ihrer Anlage zum Erfassen der Unterschriften als elektronische Signatur ein Signotec-Pad verwenden werden soll, aktivieren Sie die Checkbox „Signotec-Pad Treiber installieren“.

— Sollte eine nachträgliche Installation des Microsoft SQL Servers zu einem späteren Zeitpunkt notwendig werden, können Sie durch Aktivierung der Checkbox „Kopieren der Microsoft SQL Serverinstallationsdateien“ in das Installationsverzeichnis“ die Dateien zum Setup in das Verzeichnis des BKS KeyManagers kopieren.

- Drücken Sie auf den Button „Weiter >“.

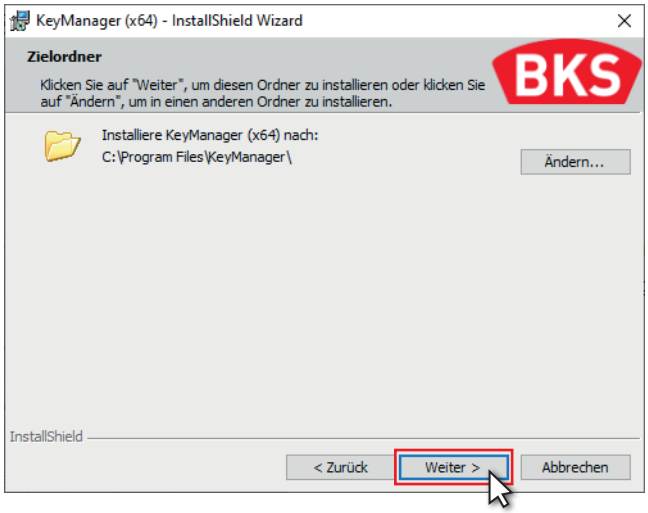
Wählen Sie aus, ob der BKS KeyManager beim Start automatisch nach Updates suchen soll. Um diese Funktion nutzen zu können, wird eine Verbindung vom BKS KeyManager zum Internet benötigt.

- Wenn ja, aktivieren Sie die Checkbox bei „Automatische Suche erlauben“.
- Drücken Sie auf den Button „Weiter >“.

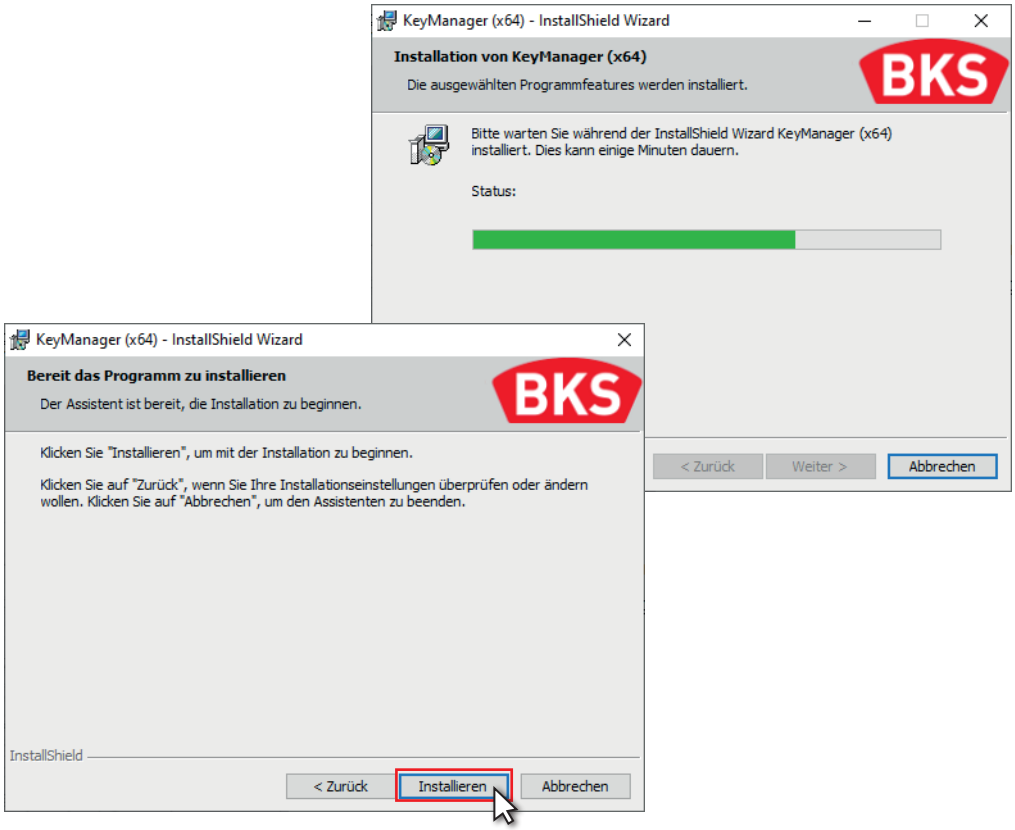


Wählen Sie ggf. mit „Ändern“ einen anderen Installationsordner aus.

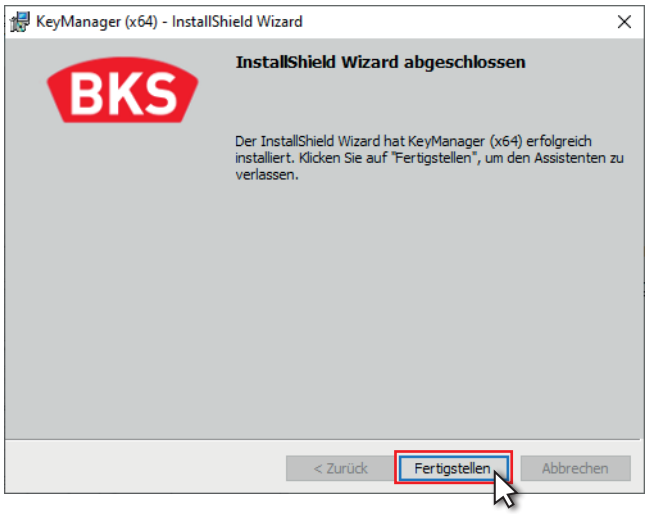
- Drücken Sie auf den Button „Weiter >“.



- Drücken Sie auf den Button „Installieren“, um die Installation fortzusetzen.



- Zur Beendigung der Installation drücken Sie auf den Button „Fertigstellen“.



■ Durch Drücken auf den Menüpunkt „Installation beenden“, schließen Sie das Fenster.

Nach der Installation können Sie das Programmiergerät mit einem USB Kabel an den Computer anschließen. Der USB-Treiber des Programmiergerätes wird dabei automatisch installiert.

Der BKS KeyManager ist jetzt einsatzbereit und Sie können ihn starten. Fahren Sie mit dem Kapitel 3 [62] fort.

2.3 Installation eines Clients der Netzwerkversion

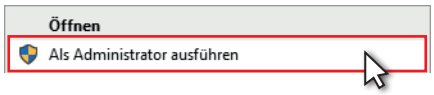
Wir empfehlen diese Installation für mittlere und große Anlagen mit Anbindung von mehreren Client-Arbeitsplätzen und Online-Funktionen. Der Client beinhaltet nur die Benutzeroberfläche zur Verwaltung und Programmierung. Die Datenbank befindet sich auf dem separaten Microsoft SQL Server.

HINWEIS

Zur Installation des Clients für die Netzwerkversion muss eine BKS KeyManager-Datenbank auf einem anderen physischen oder virtuellen Computer vorhanden sein um die Anbindung durchzuführen. Auf dem Computer auf den der Client installiert werden soll, darf kein BKS KeyManager als Netzwerk oder Einzelplatzversion installiert sein.

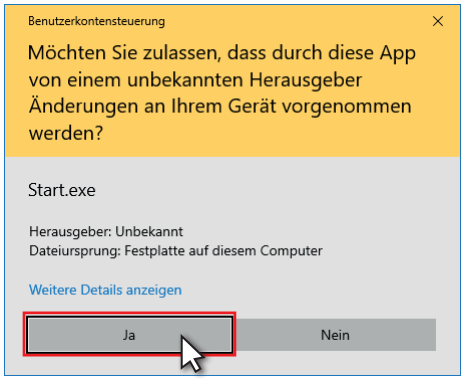
Sollte der Installationsassistent des BKS KeyManagers nach dem Einlegen des Speichermediums nicht automatisch gestartet werden oder es wird ein anderes Installationsmedium wie z. B. USB-Datenträger oder Download verwendet, ist die Installation manuell zu starten.

- Öffnen Sie den Windows Explorer und navigieren zum Speicherort der Installationsdaten z. B. USB, DVD oder Stammverzeichnis (Root) und öffnen den Installationsordner.
- Sind die Installationsdateien in einem ZIP-Archiv abgelegt, so ist der Inhalt des ZIP-Archivs vor der Installation über das Kontextmenü „Alle extrahieren ...“ in das Stammverzeichnis (Root) des Computers z. B. „C:\“ bzw. „OS (C:)“ zu entpacken.
- Starten Sie den Installationsassistent:
  - Wählen Sie über das Kontextmenü die Datei „ Start.exe“ aus.
  - Führen Sie die Datei „Start.exe“ als Administrator aus.



HINWEIS

Bestätigen Sie die während der Installation auftretende Sicherheitswarnung mit „Ja“. Diese treten je nach Sicherheitseinstellung Ihres Systems auf.

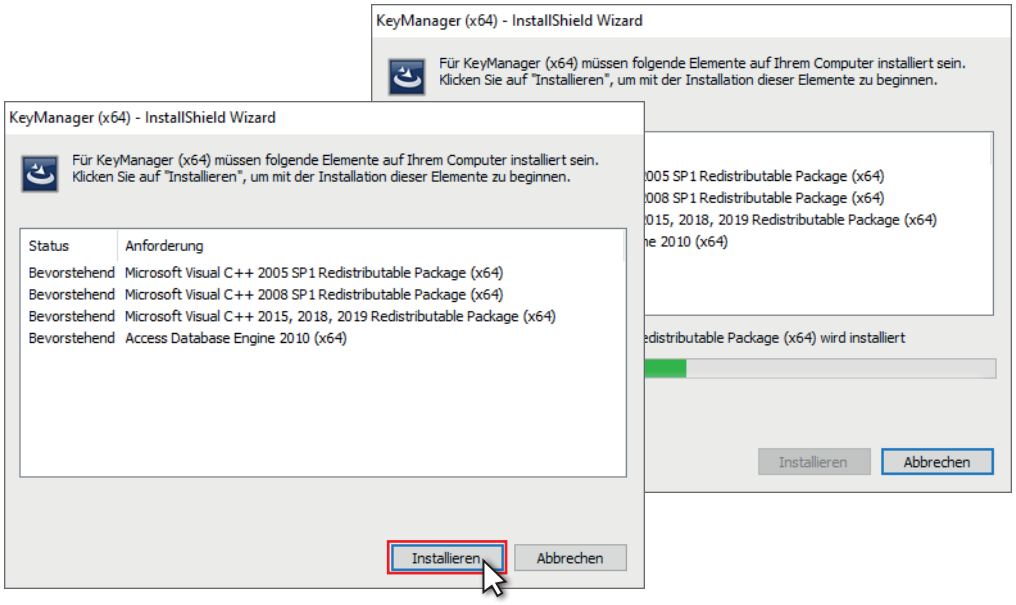


Die Installation des BKS KeyManagers wird durch Auswählen des Menüpunktes gestartet.

- Drücken Sie den Menüpunkt „KeyManager installieren“.

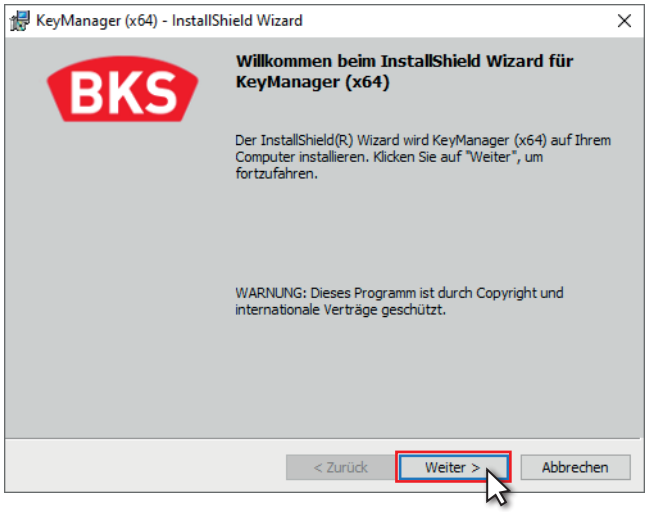
Identifikation und Installation fehlender Treiber und Module vor der BKS KeyManager-Installation.

- Drücken Sie auf den Button „Installieren“, um den Vorgang zu starten.



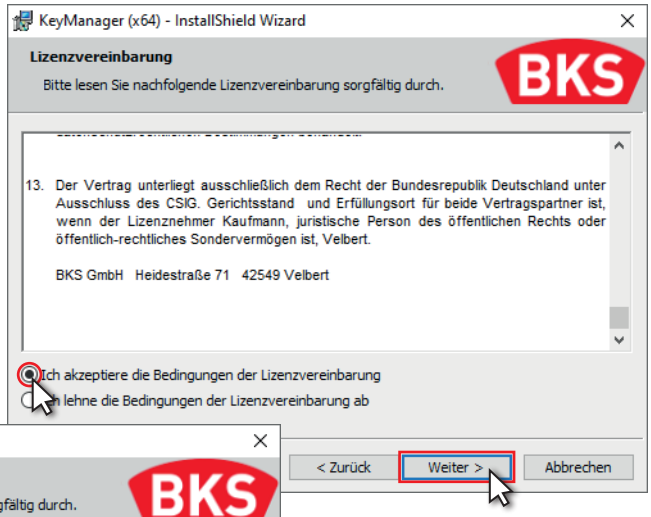
Der BKS KeyManager bereitet die Installation vor.

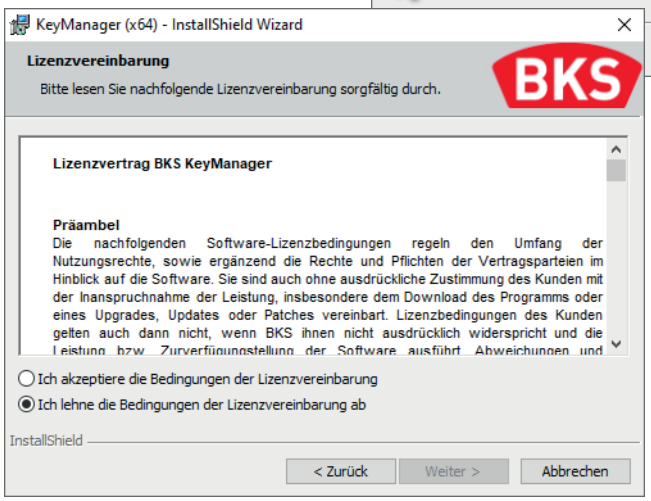
Drücken Sie auf den Button „Weiter >“, um die Installation fortzusetzen.



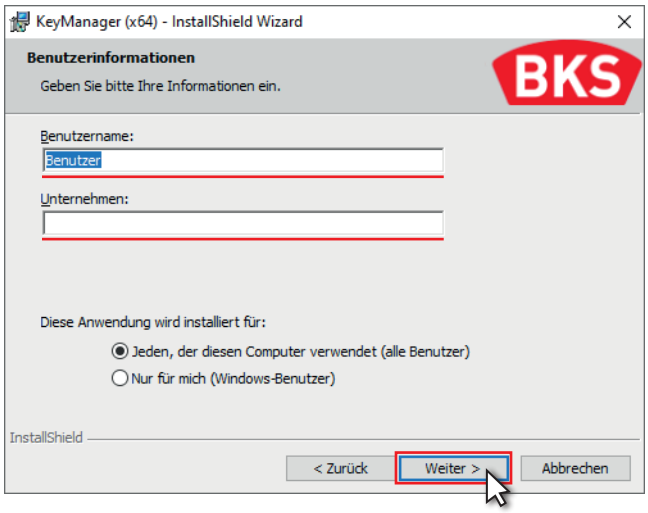
Lesen Sie sich den Lizenzvertrag sorgfältig durch.

- Akzeptieren Sie die gelesenen Bedingungen und Lizenzvereinbarung und drücken auf den Button „Weiter >“.

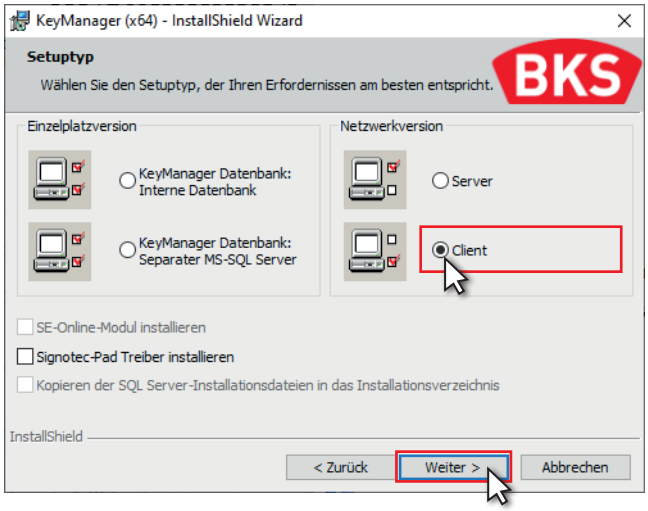




■ Geben Sie ggf. Ihre Benutzerinformationen ein und drücken Sie auf den Button „Weiter >“.



■ Zur Fortsetzung der Installation aktivieren Sie die Checkbox „Client“.



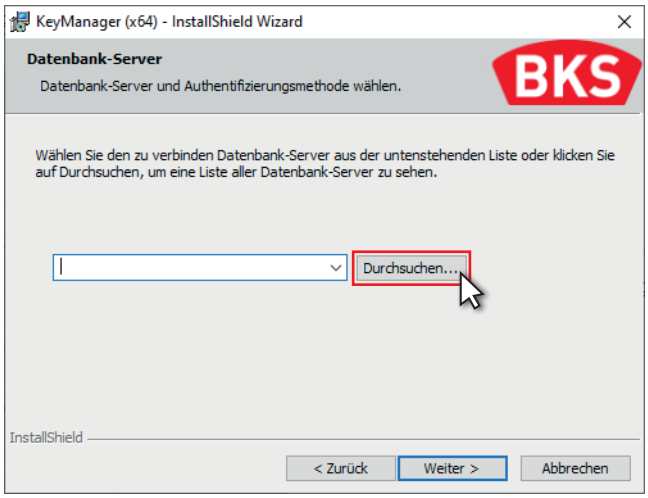
Optional haben Sie die Möglichkeit die folgenden Erweiterungen auszuwählen:

— Wenn in Ihrer Anlage zum Erfassen der Unterschriften als elektronische Signatur ein Signotec-Pad verwenden werden soll, aktivieren Sie die Checkbox „Signotec-Pad Treiber installieren“.

Einige Optionen dürfen bei einer Client-Server-Installation nur auf dem Server installiert werden und können hier nicht ausgewählt werden.

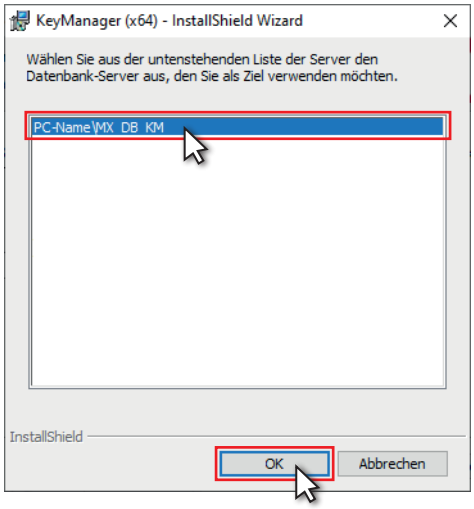
■ Drücken Sie auf den Button „Weiter >“.

- Wählen Sie über das Dropdown-Menü einen Datenbank-Server aus oder drücken Sie auf den Button „Durchsuchen ...“, um einen Datenbank-Server zu suchen.

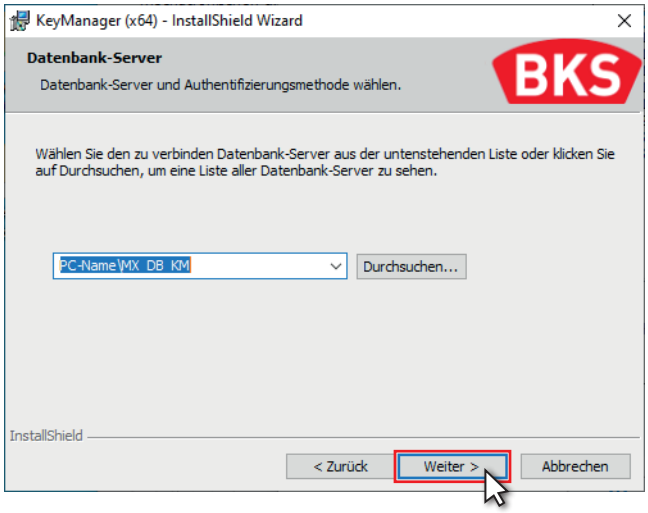


Wählen Sie aus der Liste der zur Verfügung stehenden Datenbank-Server den aus, mit dem der Client verbunden werden soll.

- Drücken Sie zur Bestätigung der Auswahl auf „OK“.

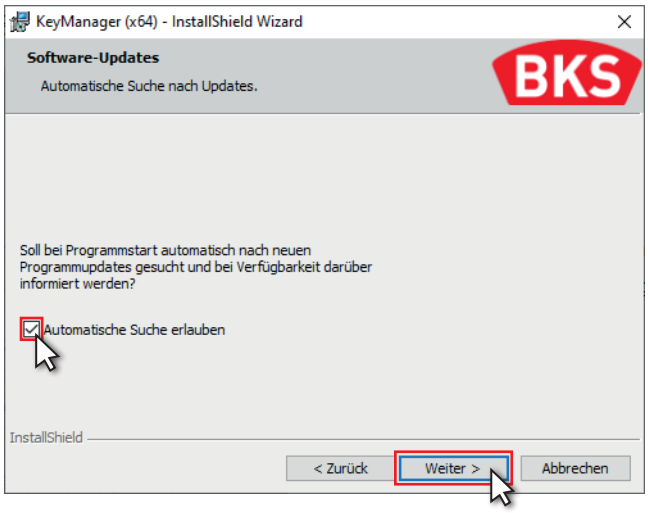


- Drücken Sie auf den Button „Weiter >“.



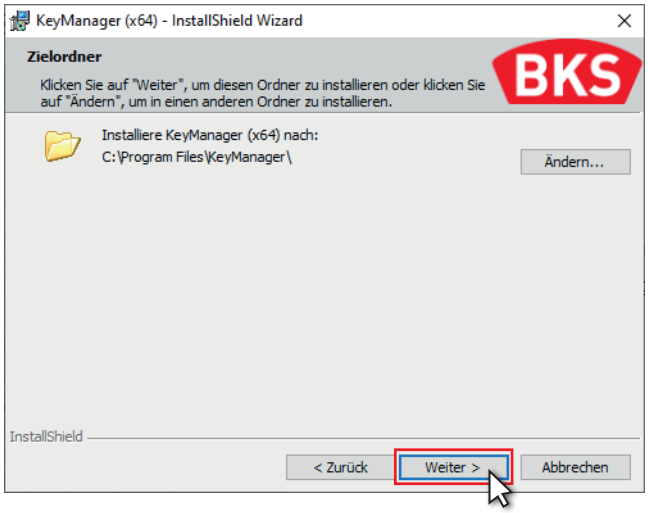
Wählen Sie aus, ob der BKS KeyManager beim Start automatisch nach Updates suchen soll. Um diese Funktion nutzen zu können, wird eine Verbindung vom BKS KeyManager zum Internet benötigt.

- Wenn ja, aktivieren Sie die Checkbox bei „Automatische Suche erlauben“.
- Drücken Sie auf den Button „Weiter >“.

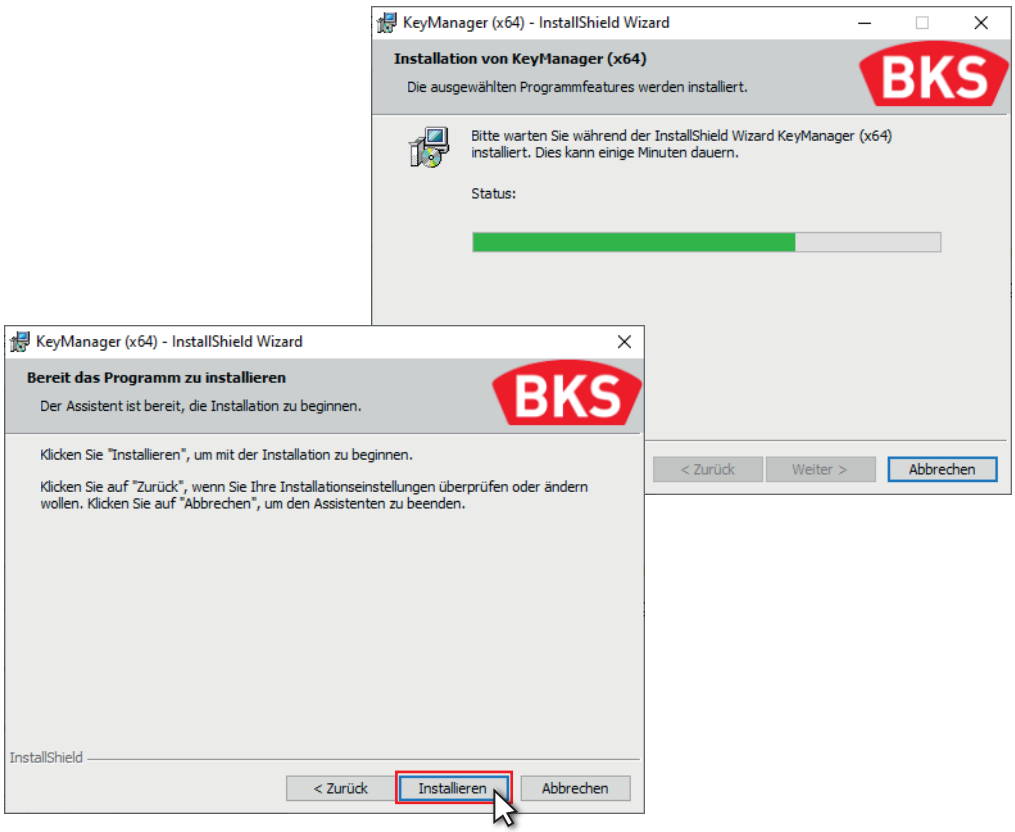


Wählen Sie ggf. mit „Ändern“ einen anderen Installationsordner aus.

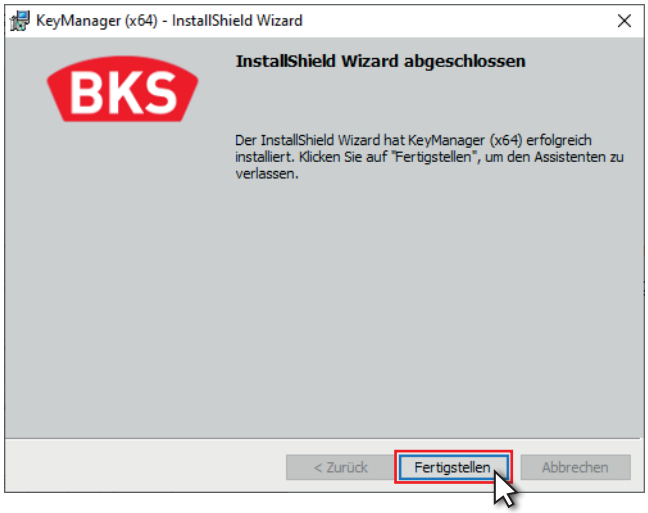
- Drücken Sie auf den Button „Weiter >“.



- Drücken Sie auf den Button „Installieren“, um die Installation fortzusetzen.



■ Zur Beendigung der Installation drücken Sie auf den Button „Fertigstellen“.



■ Durch Drücken auf den Menüpunkt „Installation beenden“, schließen Sie das Fenster.

Nach der Installation können Sie das Programmiergerät mit einem USB Kabel an den Computer anschließen. Der USB-Treiber des Programmiergerätes wird dabei automatisch installiert.

Der BKS KeyManager ist jetzt einsatzbereit und Sie können ihn starten. Fahren Sie mit dem Kapitel 3 [62] fort.

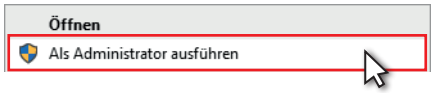
2.4 Installation der Einzelplatzversion mit interner Datenbank

Wir empfehlen diese Installation für Kleinstanlagen im Offline-Betrieb. Die Einzelplatzversion beinhaltet die Benutzeroberfläche zur Verwaltung und Programmierung sowie eine im BKS KeyManager integrierte Datenbank.

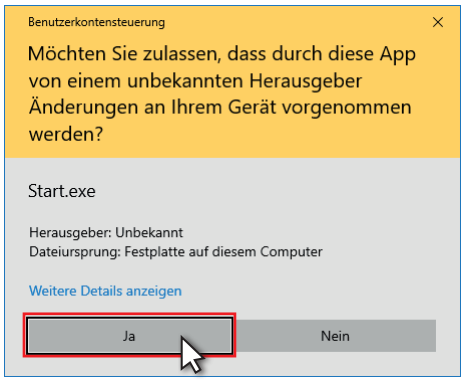
Die Daten werden in einer internen Datenbank verwaltet. Bei Verwendung dieses Setup-Typs ist keine Online-Funktion möglich. Eine Client-Server-Installation ist mit der internen Datenbank nicht möglich.

Sollte der Installationsassistent des BKS KeyManagers nach dem Einlegen des Speichermediums nicht automatisch gestartet werden oder es wird ein anderes Installationsmedium wie z. B. USB-Datenträger oder Download verwendet, ist die Installation manuell zu starten.

- Öffnen Sie den Windows Explorer und navigieren zum Speicherort der Installationsdaten z. B. USB, DVD oder Stammverzeichnis (Root) und öffnen den Installationsordner.
- Sind die Installationsdateien in einem ZIP-Archiv abgelegt, so ist der Inhalt des ZIP-Archivs vor der Installation über das Kontextmenü „Alle extrahieren ...“ in das Stammverzeichnis (Root) des Computers z. B. „C:\“ bzw. „OS (C:)“ zu entpacken.
- Starten Sie den Installationsassistent:
  - Wählen Sie über das Kontextmenü die Datei „ Start.exe“ aus.
  - Führen Sie die Datei „Start.exe“ als Administrator aus.



HINWEIS **Bestätigen Sie die während der Installation auftretende Sicherheitswarnung mit „Ja“. Diese treten je nach Sicherheitseinstellung Ihres Systems auf.**

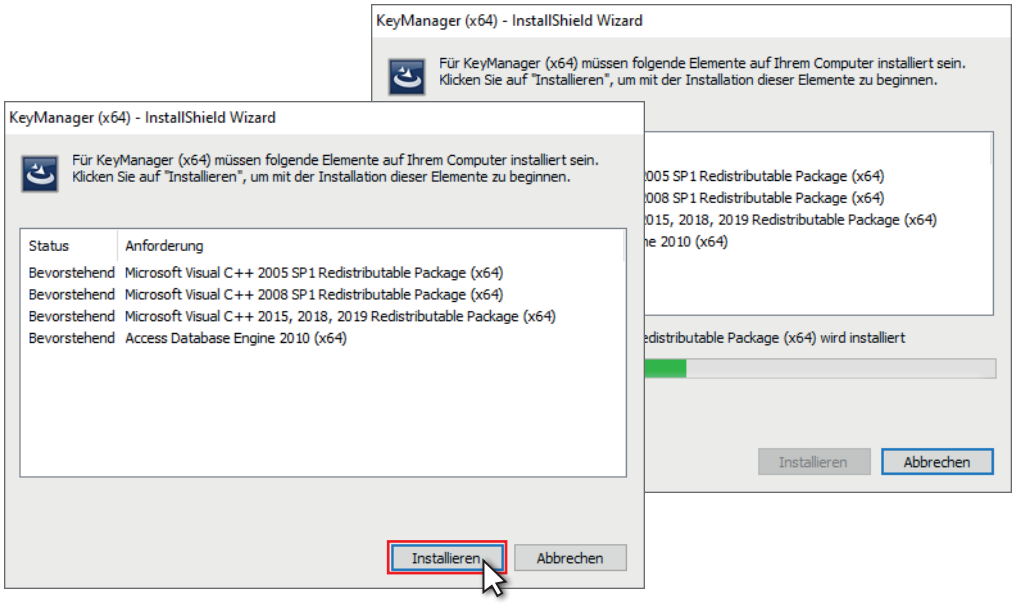


Die Installation des BKS KeyManagers wird durch Auswählen des Menüpunktes gestartet.

- Drücken Sie den Menüpunkt „KeyManager installieren“.

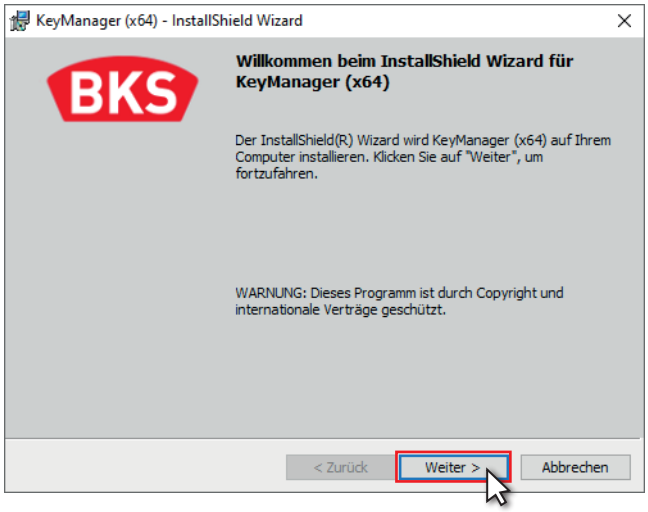
Identifikation und Installation fehlender Treiber und Module vor der BKS KeyManager-Installation.

- Drücken Sie auf den Button „Installieren“, um den Vorgang zu starten.



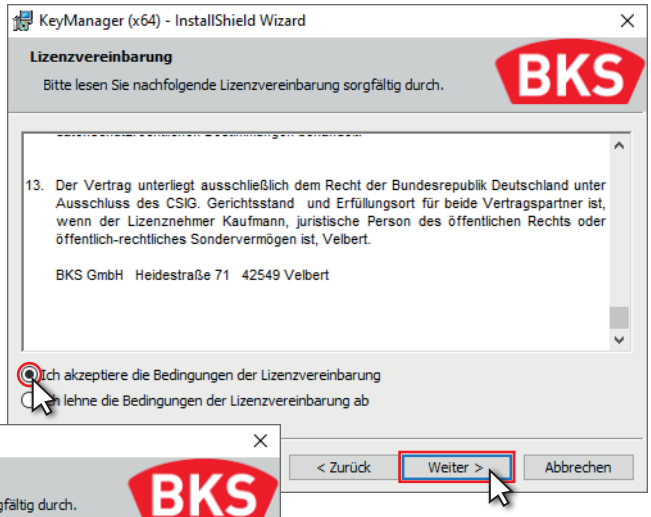
Der BKS KeyManager bereitet die Installation vor.

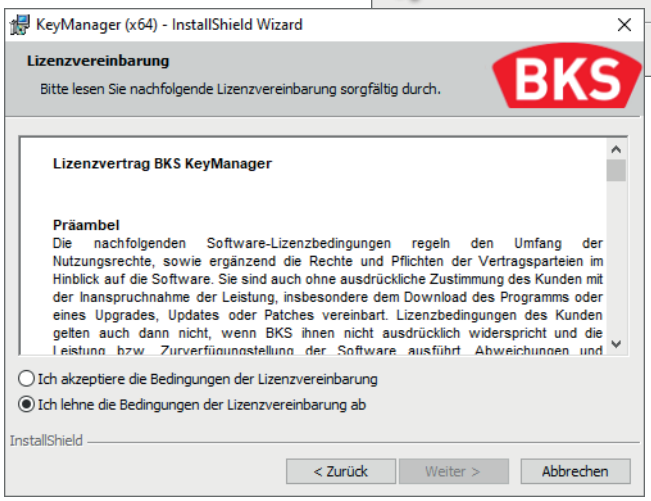
Drücken Sie auf den Button „Weiter >“, um die Installation fortzusetzen.



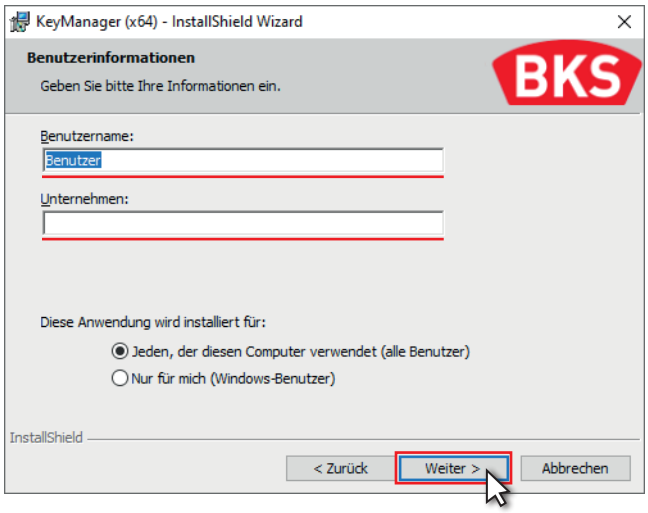
Lesen Sie sich den Lizenzvertrag sorgfältig durch.

- Akzeptieren Sie die gelesenen Bedingungen und Lizenzvereinbarung und drücken auf den Button „Weiter >“.



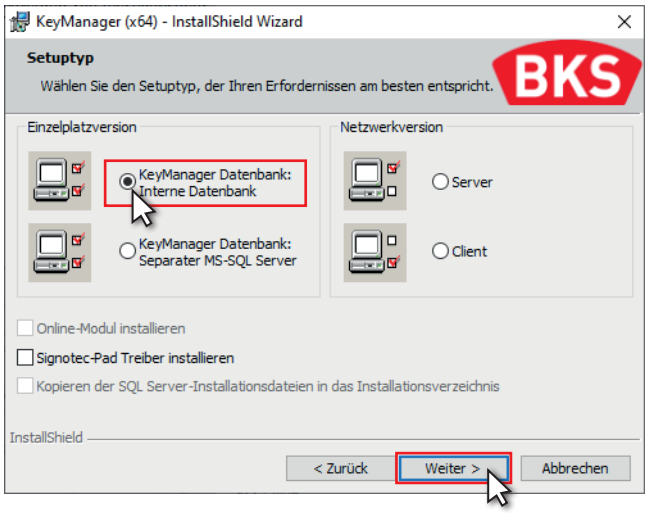


■ Geben Sie ggf. Ihre Benutzerinformationen ein und drücken Sie auf den Button „Weiter >“.



Auswahl des Setup-Typs für die Installationsart sowie ggf. die zu installierenden Zusatzmodule.

■ Aktivieren Sie die Checkbox „KeyManager-Datenbank: interne Datenbank“.



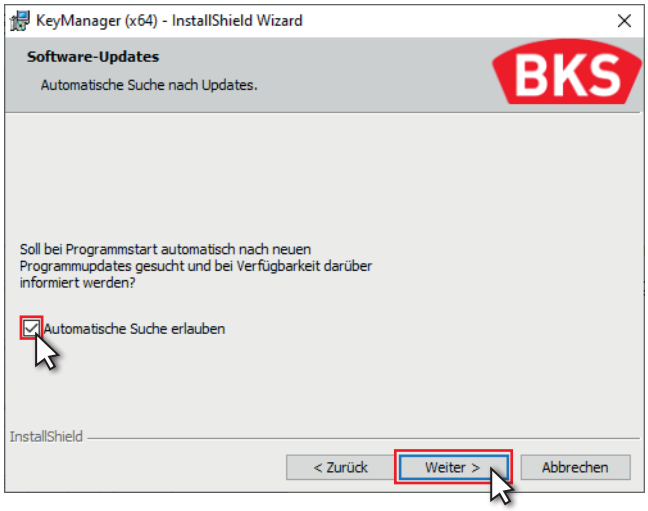
Optional haben Sie die Möglichkeit die folgenden Erweiterungen auszuwählen:

— Wenn in Ihrer Anlage zum Erfassen der Unterschriften als elektronische Signatur ein Signotec-Pad verwenden werden soll, aktivieren Sie die Checkbox „Signotec-Pad Treiber installieren“.

■ Drücken Sie auf den Button „Weiter >“.

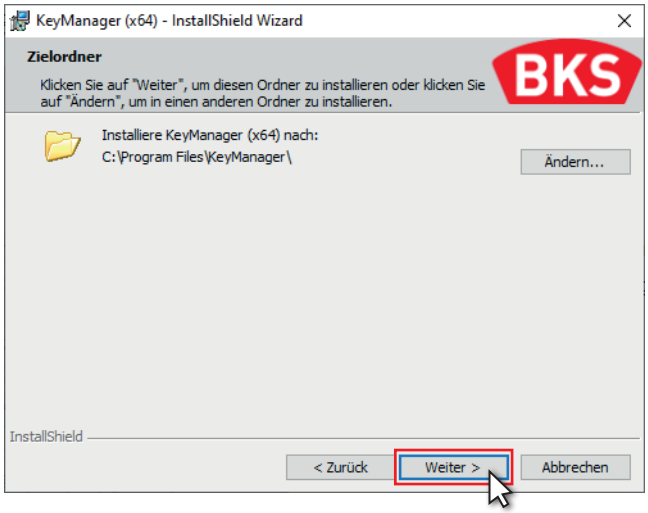
Wählen Sie aus, ob der BKS KeyManager beim Start automatisch nach Updates suchen soll. Um diese Funktion nutzen zu können, wird eine Verbindung vom BKS KeyManager zum Internet benötigt.

- Wenn ja, aktivieren Sie die Checkbox bei „Automatische Suche erlauben“.
- Drücken Sie auf den Button „Weiter >“.

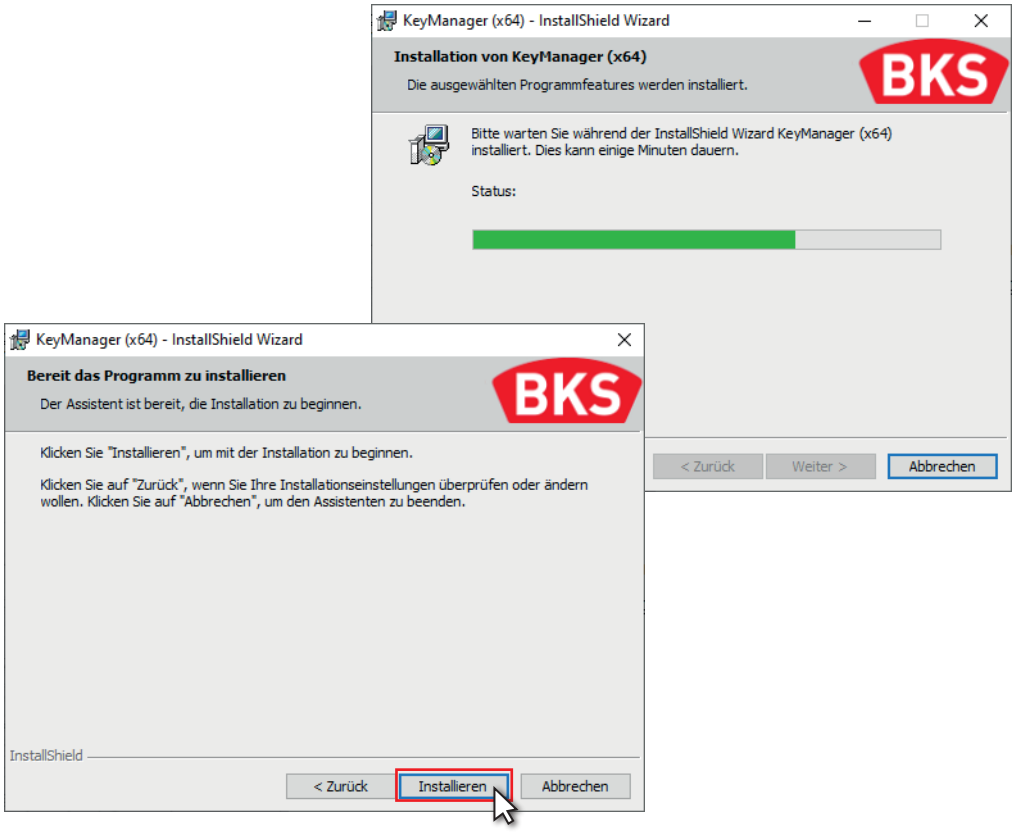


Wählen Sie ggf. mit „Ändern“ einen anderen Installationsordner aus.

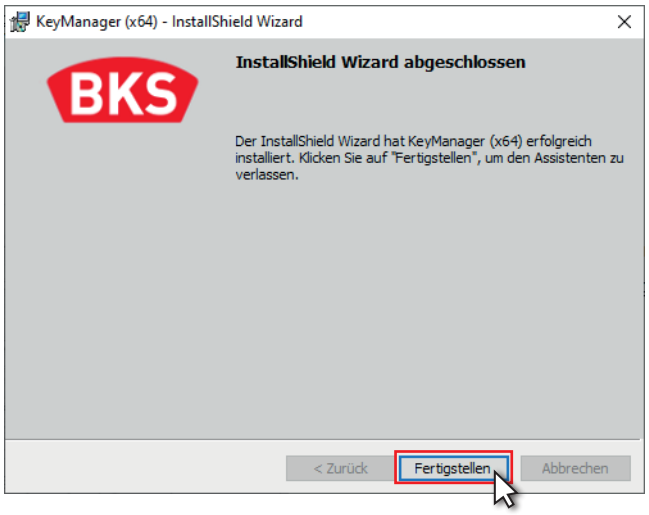
- Drücken Sie auf den Button „Weiter >“.



■ Drücken Sie auf den Button „Installieren“, um die Installation fortzusetzen.



■ Zur Beendigung der Installation drücken Sie auf den Button „Fertigstellen“.



- Durch Drücken auf den Menüpunkt „Installation beenden“, schließen Sie das Fenster.

Nach der Installation können Sie das Programmiergerät mit einem USB Kabel an den Computer anschließen. Der USB-Treiber des Programmiergerätes wird dabei automatisch installiert.

Der BKS KeyManager ist jetzt einsatzbereit und Sie können ihn starten. Fahren Sie mit dem Kapitel 3 [62] fort.

2.5 Installation des Servers der Netzwerkversion

Wir empfehlen diese Installation für mittlere und große Anlagen mit Anbindung von Client-Arbeitsplätzen und Online-Funktionen. Die Serverversion beinhaltet nur die Datenbank auf dem separaten Microsoft SQL Server. Bei Einrichtung der Serverversion ist im ersten Schritt ein Microsoft SQL Server zu installieren.

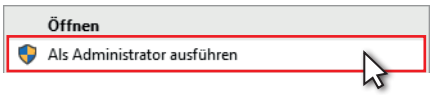
Bei der Serverversion werden die Daten in einer separaten Datenbank verwaltet. Die zur Verwaltung und Programmierung benötigte Benutzeroberfläche muss mit der Client-Version installiert werden, siehe Kapitel 2.3 [32]. Bei Verwendung dieses Setups ist eine Rückstellung auf eine interne Datenbank nicht möglich.

Sollte der Installationsassistent des BKS KeyManagers nach dem Einlegen des Speichermediums nicht automatisch gestartet werden oder es wird ein anderes Installationsmedium wie z. B. USB-Datenträger oder Download verwendet, ist die Installation manuell zu starten.

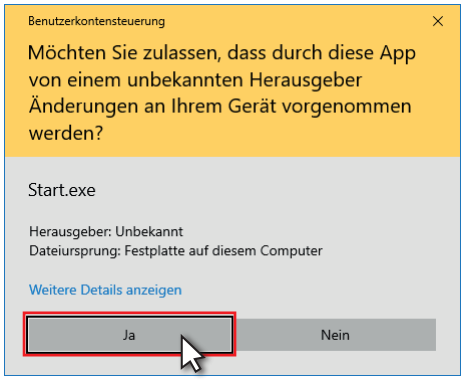
- Öffnen Sie den Windows Explorer und navigieren zum Speicherort der Installationsdaten z. B. USB, DVD oder Stammverzeichnis (Root) und öffnen den Installationsordner.
- Sind die Installationsdateien in einem ZIP-Archiv abgelegt, so ist der Inhalt des ZIP-Archivs vor der Installation über das Kontextmenü „Alle extrahieren ...“ in das Stammverzeichnis (Root) des Computers z. B. „C:\“ bzw. „OS (C:)“ zu entpacken.
- Starten Sie den Installationsassistent:

  – Wählen Sie über das Kontextmenü die Datei „ Start.exe“ aus.

  – Führen Sie die Datei „Start.exe“ als Administrator aus.



HINWEIS **Bestätigen Sie die während der Installation auftretende Sicherheitswarnung mit „Ja“. Diese treten je nach Sicherheitseinstellung Ihres Systems auf.**



2.5.1 Installation und Konfiguration des Microsoft SQL Servers

Bevor Sie die Serverversion installieren können, müssen Sie den Microsoft SQL Server aufspielen und konfigurieren. Beginnen Sie die Installation des BKS KeyManagers mit der Einrichtung des Microsoft SQL Servers und folgen den im Kapitel 2.2.1 [19] beschrieben Ablauf.

Wählen Sie die Installationsart Microsoft SQL Server installieren“.

HINWEIS **Damit ein Client mit dem Server kommunizieren kann, muss eine evtl. vorhandene Firewall so konfiguriert werden, dass der Microsoft SQL Server nicht behindert wird.**

Konfigurieren Sie den Microsoft SQL Server nach den im Kapitel 2.2.2 [24] beschriebenen Ablauf.

- Starten Sie den „SQL Server Configuration Manager“ und drücken zur Bestätigung auf „Ja“.

2.5.2 Installation der Serverversion für die Netzwerkversion

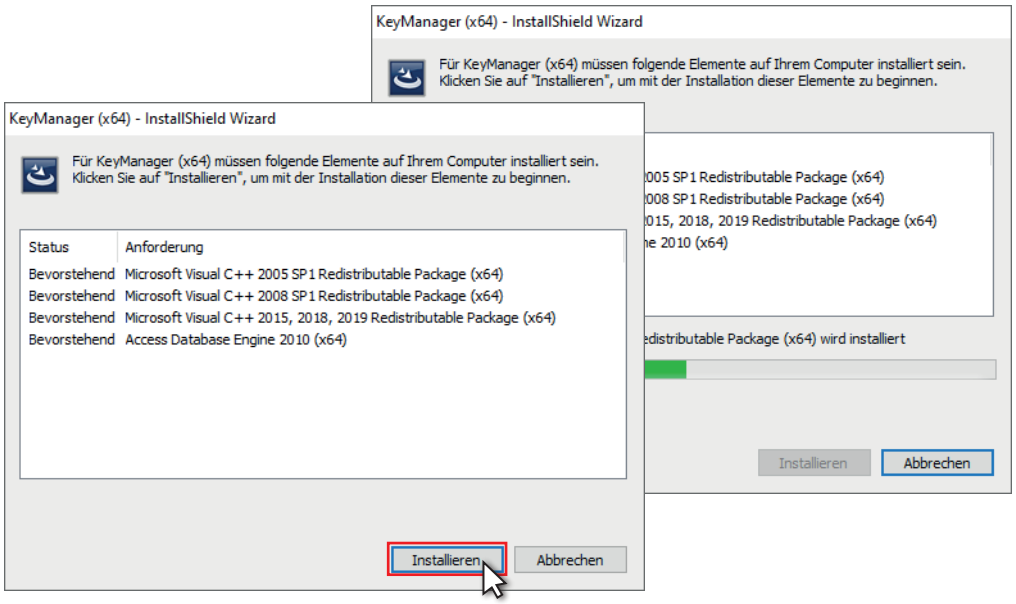
Vor der Installation der Serverversion für die Netzwerkversion muss die Installation und Konfiguration des Microsoft SQL Servers wie im Kapitel 2.2.1 [19] und 2.2.2 [24] beschrieben durchgeführt worden sein.

Die Installation des BKS KeyManagers wird durch Auswählen des Menüpunktes gestartet.

- Drücken Sie den Menüpunkt „KeyManager installieren“.

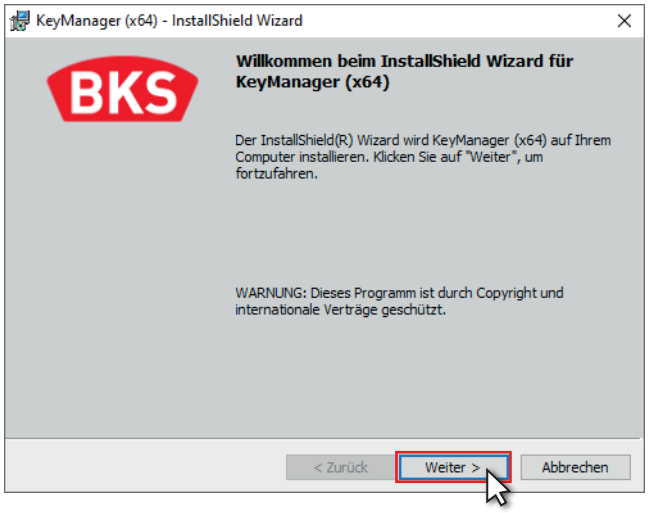
Identifikation und Installation fehlender Treiber und Module vor der BKS KeyManager-Installation.

- Drücken Sie auf den Button „Installieren“, um den Vorgang zu starten.



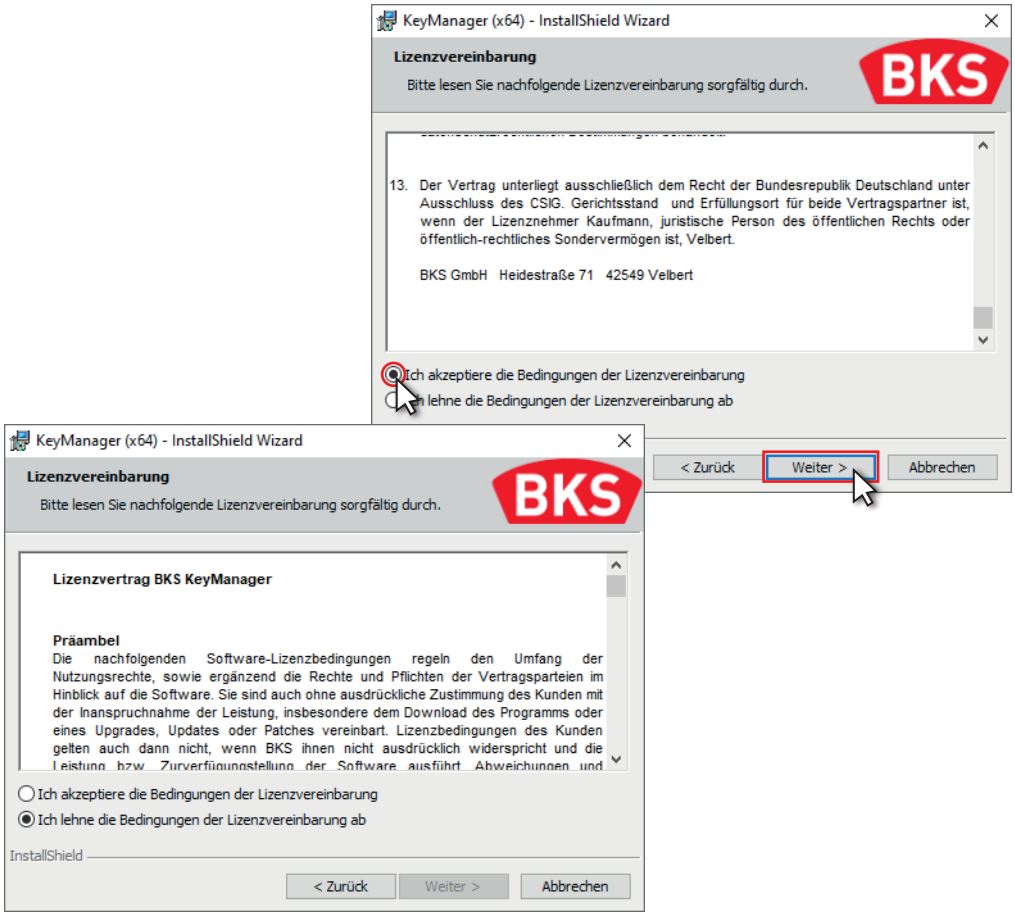
Der BKS KeyManager bereitet die Installation vor.

Drücken Sie auf den Button „Weiter >“, um die Installation fortzusetzen.

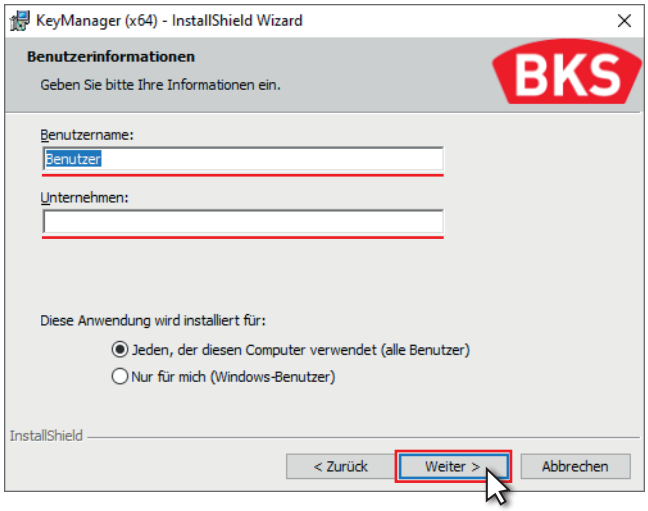


Lesen Sie sich den Lizenzvertrag sorgfältig durch.

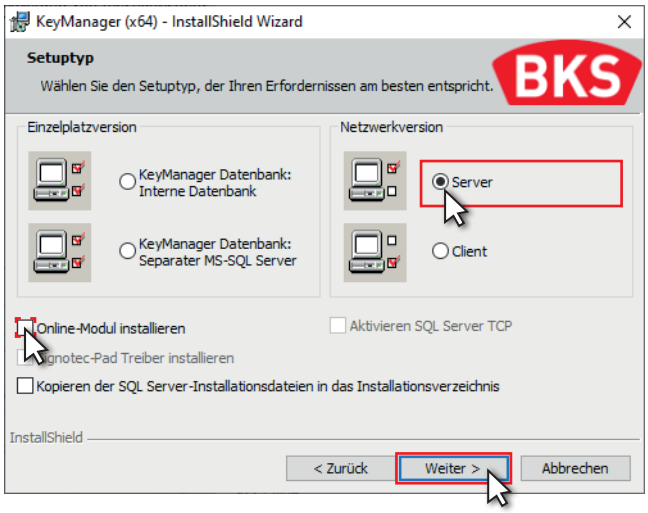
- Akzeptieren Sie die gelesenen Bedingungen und Lizenzvereinbarung und drücken auf den Button „Weiter >“.



- Geben Sie ggf. Ihre Benutzerinformationen ein und drücken Sie auf den Button „Weiter >“.



■ Zur Fortsetzung der Installation der Netzwerkversion aktivieren Sie die Checkbox „Server“.



Optional haben Sie die Möglichkeit die folgenden Erweiterungen auszuwählen:

— Wenn Sie in Ihrer Anlage Ethernetbuskoppler (EBK) mit online angebundenen Zutrittspunkten und/oder Freigabeterminals (FGT) verwenden und mit dem BKS KeyManager verbinden möchten, aktivieren Sie die Checkbox „SE-Online-Modul installieren“.

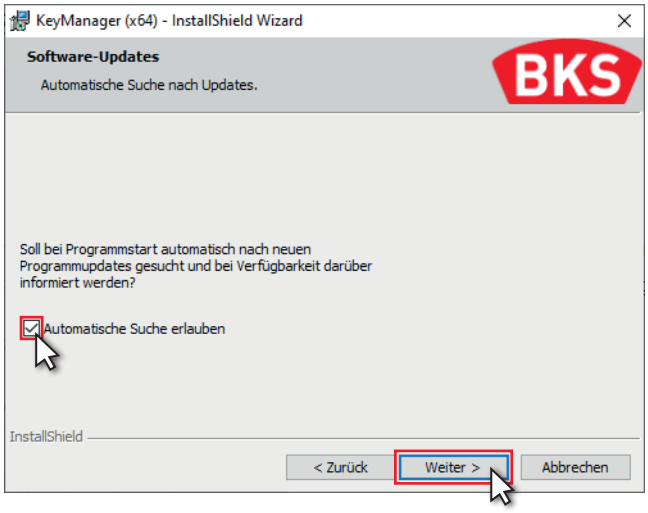
— Sollte eine nachträgliche Installation des Microsoft SQL Servers zu einem späteren Zeitpunkt notwendig werden, können Sie durch Aktivierung der Checkbox „Kopieren der Microsoft SQL Serverinstallationsdateien“ in das Installationsverzeichnis“ die Dateien zum Setup in das Verzeichnis des BKS KeyManagers kopieren.

■ Drücken Sie auf den Button „Weiter >“.

Wählen Sie aus, ob der BKS KeyManager beim Start automatisch nach Updates suchen soll. Um diese Funktion nutzen zu können, wird eine Verbindung vom BKS KeyManager zum Internet benötigt.

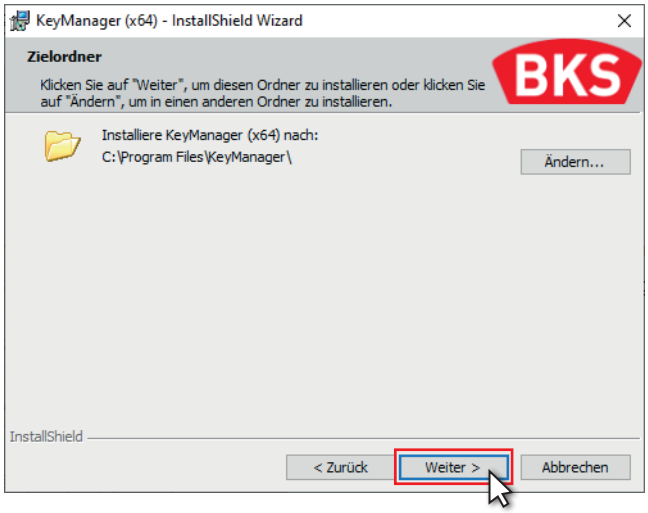
■ Wenn ja, aktivieren Sie die Checkbox bei „Automatische Suche erlauben“.

■ Drücken Sie auf den Button „Weiter >“.

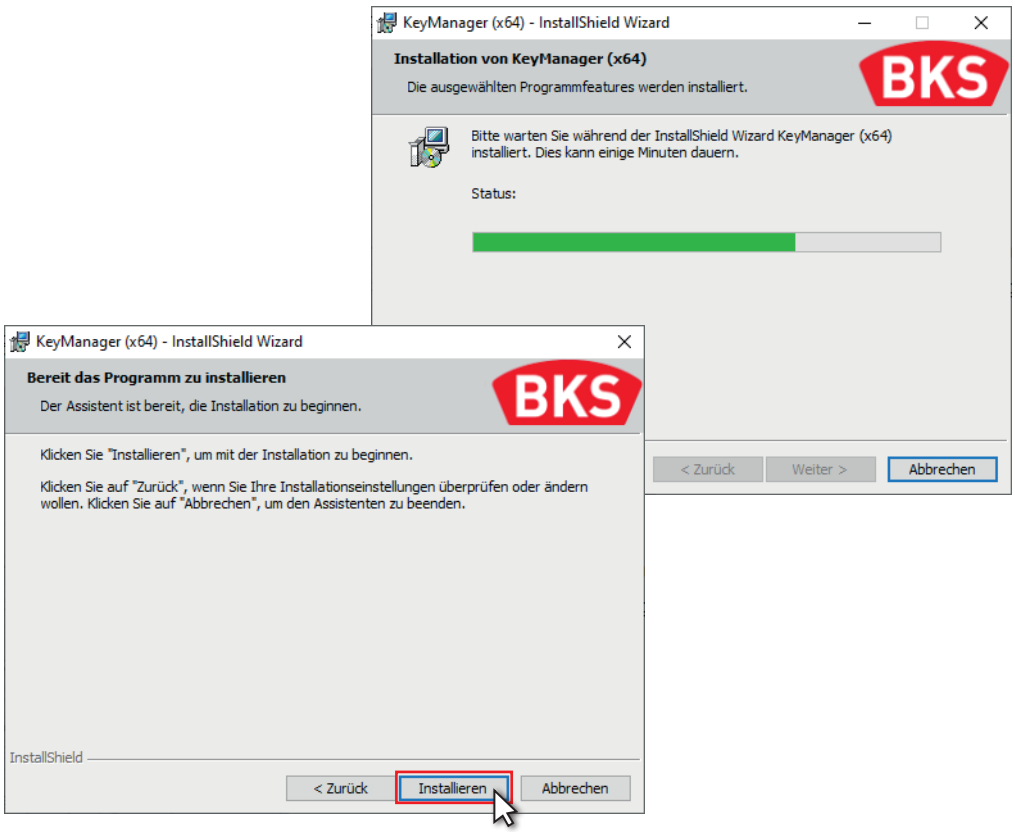


Wählen Sie ggf. mit „Ändern“ einen anderen Installationsordner aus.

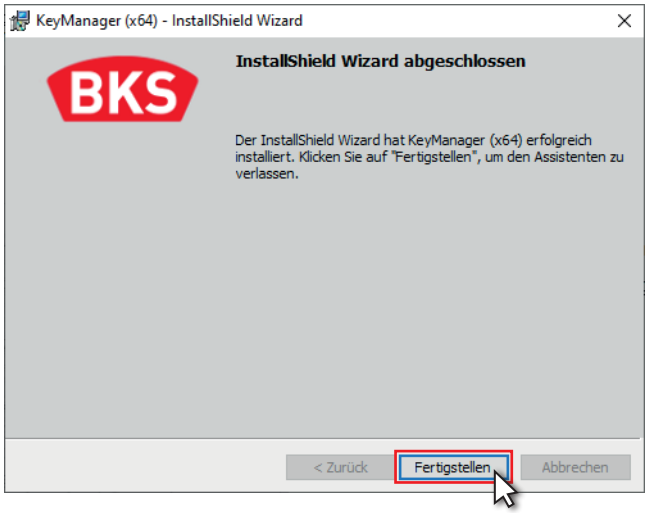
- Drücken Sie auf den Button „Weiter >“.



- Drücken Sie auf den Button „Installieren“, um die Installation fortzusetzen.



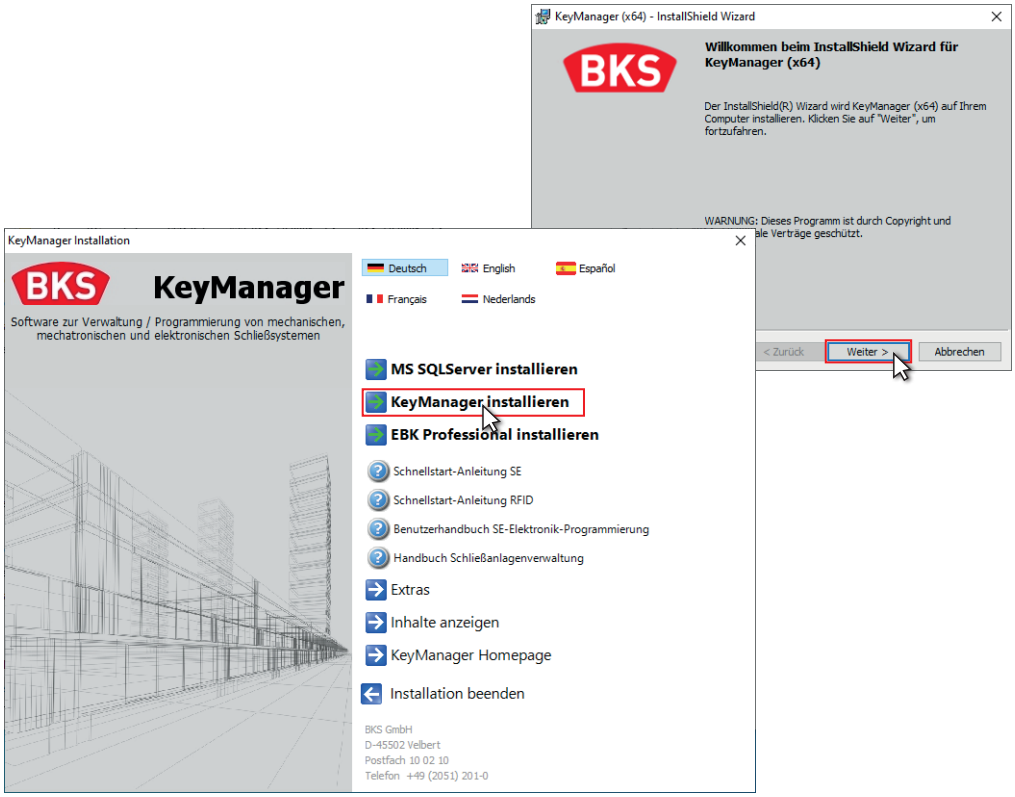
■ Zur Beendigung der Installation drücken Sie auf den Button „Fertigstellen“.



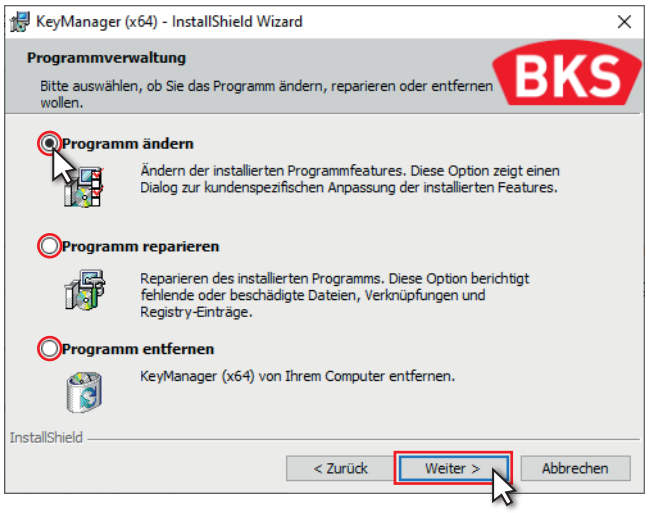
■ Durch Drücken auf den Menüpunkt „Installation beenden“, schließen Sie das Fenster.

2.6 Aufrufen der Programmverwaltung

Eine mehrfache Installation des BKS KeyManagers ist nicht möglich. Durch drücken auf das Menü „KeyManager installieren“ öffnet sich bei einem bereits installierten BKS KeyManager das Fenster „Programmverwaltung“.



Die Programmverwaltung bietet die Option zum Ändern, Reparieren oder Entfernen.



2.7 Silent Installation

Es besteht auch die Möglichkeit den BKS KeyManager mit einer unbeaufsichtigten Installation einzurichten. Mit Ausführen der Datei „setup.exe“ in Verbindung mit Kommandozeilenparameter wird das Setup komplett durchlaufen, ohne dass während der Installation Eingaben des Benutzers erforderlich werden.

Die Installation wird durch Wechseln ins Installationsverzeichnis in der Windows-Eingabeaufforderung (CMD) und der Eingabe des jeweiligen Kommandozeilenbefehls gestartet.
Der Befehl wird aus der „setup.exe“ mit den Kommandozeilenparameter zusammengesetzt.

Alternativ kann die Silent Installation mit einer Batch-Datei gestartet werden. Schreiben Sie den Kommandozeilenbefehl mit dem Editor in eine Zeile des Dokuments und speichern dieses im Format „*.bat“ in das Installationsverzeichnis der „setup.exe“ ab. Zum Start der Silent Installation führen Sie die Batch-Datei aus.

Legende Kommandozeilenparameter:

- Sprache: /L1031 – Deutsch
  /L1033 – Englisch
  /L1036 – Französisch
  /L3082 – Spanisch
  /L1043 – Niederländisch
- Silent Installation mit Anzeige: /qr – Silent Installation mit Anzeige
- Installationstyp: INSTYPE=1 – Client
  INSTYPE=3 – Einzelplatzversion Microsoft SQL
  INSTYPE=4 – Einzelplatzversion interne Datenbank
  INSTYPE=5 – Server
- Datenbank Verbindung:
  IS_SQLSERVER_USERNAME – Benutzer für Microsoft SQL Server Verbindung
  IS_SQLSERVER_PASSWORD – Klartext Passwort für Microsoft SQL Server Verbindung
  IS_SQLSERVER_SERVER – Servername für Microsoft SQL Server Verbindung
  IS_SQLSERVER_DBNAME – DB name auf Microsoft SQL Server Instance

<u>Kommandozeilenbefehl für:</u>

1.) Installation eines Clients.

setup.exe /L1031 /v“/qr INSTYPE=1 IS_SQLSERVER_SERVER=(local)\MX_DB_KM3 ADDLOCAL=Program REMOVE=SE_Online_Module INSTALL_TOPAZ_SIGNOTEC=NO INST_USB=YES“

/L1031	Sprache: Deutsch
/qr	Silent Installation mit Anzeige
INSTYPE=1	Clientinstallation
IS_SQLSERVER_SERVER=(local)\MX_DB_KM3	Datenbank Verbindung: Servername (IP Adresse)\Instanzname
INSTALL_TOPAZ_SIGNOTEC=NO	Topaz Signotec installieren [YES / NO]
INST_USB=YES	CP210x Silicon Lab USB Treiber installieren [YES / NO]

2.) Einzelplatzversion mit Microsoft SQL Server.

setup.exe /L1031 /v“/qr INSTYPE=3 ADDLOCAL=Program REMOVE=SE_Online_Module INSTALL_TOPAZ_SIGNOTEC=YES INST_USB=YES SELECTED_ALLUSERS=1“

/L1031	Sprache: Deutsch
/qr	Silent Installation mit Anzeige
INSTYPE=3	Einzelplatzversion mit Microsoft SQL Server-Datenbank
ADDLOCAL=Program REMOVE=SE_Online_Module	Installation ohne “SE online“
ADDLOCAL=All	Installation mit „SE Online“
INSTALL_TOPAZ_SIGNOTEC=NO	Topaz Signotec installieren [YES / NO]
INST_USB=YES	CP210x Silicon Lab USB Treiber installieren [YES / NO]

3.) Einzelplatzversion mit interner Datenbank.

setup.exe /L1031 /v“/qr INSTYPE=4 ADDLOCAL=Program REMOVE=SE_Online_Module INSTALL_TOPAZ_SIGNOTEC=YES INST_USB=NO SELECTED_ALLUSERS=1“

/L1031	Sprache: Deutsch
/qr	Silent Installation mit Anzeige
INSTYPE=4	Einzelplatzversion mit interner Datenbank
INSTALL_TOPAZ_SIGNOTEC=NO	Topaz Signotec installieren [YES / NO]
INST_USB=YES	CP210x Silicon Lab USB Treiber installieren [YES / NO]

4.) Serverversion für die Netzwerkversion.

setup.exe /L1031 /v“/qr INSTYPE=5 ADDLOCAL=Program REMOVE=SE_Online_Module INSTALL_TOPAZ_SIGNOTEC=NO INST_USB=YES“

/L1031	Sprache: Deutsch
/qr	Silent Installation mit Anzeige
INSTYPE=5	Serverversion
ADDLOCAL=Program REMOVE=SE_Online_Module	Installation ohne “SE online“
ADDLOCAL=All	Installation mit „SE Online“
INSTALL_TOPAZ_SIGNOTEC=NO	Topaz Signotec installieren [YES / NO]
INST_USB=YES	CP210x Silicon Lab USB Treiber installieren [YES / NO]

5.) Installation des Microsoft SQL Servers.

- Vor Eingabe der unten stehenden Kommandozeile, ist es notwendig das Verzeichnis bzw. in den Unterordner „KM-SERVER-MSSQL“ mit dem Befehl [cd KM-SERVER-MSSQL] zu wechseln.

setup.exe /L1031 /s /v“/qr“

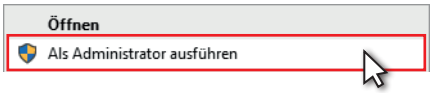
/L1031	Sprache: Deutsch
/s /v“/qr“	Silent Installation mit Anzeige

2.8 Installation des Ethernetbuskoppler Professional-Dienst

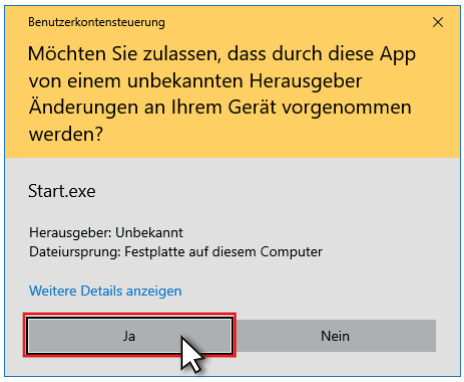
Der Ethernetbuskoppler (EBK) Professional-Dienst wird benötigt, damit der BKS KeyManager mit den EBK Professional-Geräten kommunizieren kann. Der EBK Professional-Dienst wird bei einer Client-Server-Installation nur auf dem Server gebraucht.

Sollte der Installationsassistent des BKS KeyManagers nach dem Einlegen des Speichermediums nicht automatisch gestartet werden oder es wird ein anderes Installationsmedium wie z. B. USB-Datenträger oder Download verwendet, ist die Installation manuell zu starten.

- Öffnen Sie den Windows Explorer und navigieren zum Speicherort der Installationsdaten z. B. USB, DVD oder Stammverzeichnis (Root) und öffnen den Installationsordner.
- Sind die Installationsdateien in einem ZIP-Archiv abgelegt, so ist der Inhalt des ZIP-Archivs vor der Installation über das Kontextmenü „Alle extrahieren ...“ in das Stammverzeichnis (Root) des Computers z. B. „C:\“ bzw. „OS (C:)“ zu entpacken.
- Starten Sie den Installationsassistent:
  - Wählen Sie über das Kontextmenü die Datei „ Start.exe“ aus.
  - Führen Sie die Datei „Start.exe“ als Administrator aus.

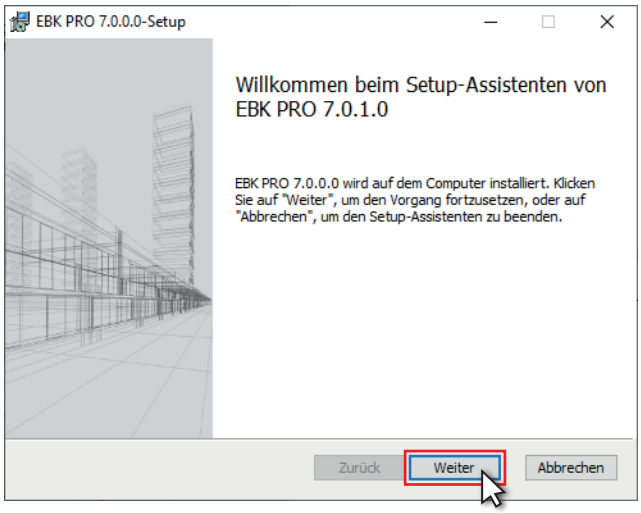


HINWEIS **Bestätigen Sie die während der Installation auftretende Sicherheitswarnung mit „Ja“. Diese treten je nach Sicherheitseinstellung Ihres Systems auf.**



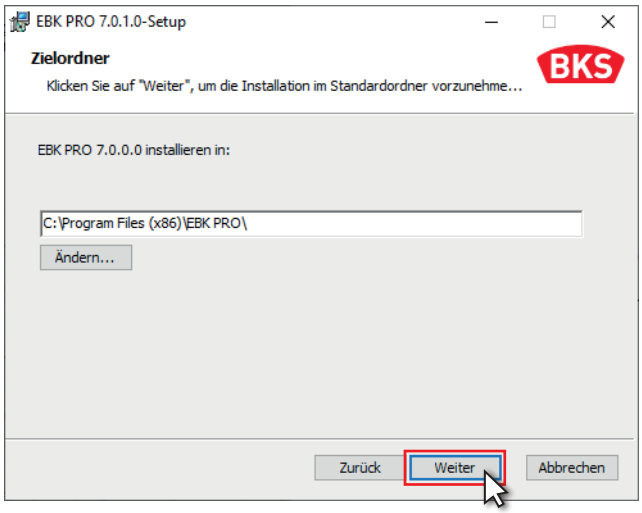
- Drücken Sie den Menüpunkt „EBK Professional installieren“.

- Drücken Sie zum Fortfahren auf den Button „Weiter“.



Wählen Sie ggf. mit „Ändern“ einen anderen Installationsordner aus.

- Drücken Sie auf den Button „Weiter >“.



Geben Sie im Feld „Anlage:“ die Anlagenbezeichnung der Schließanlage (zu finden z. B. auf Ihrer Sicherungskarte) ein, mit welcher der EBK Professional-Dienst zusammenarbeiten soll.

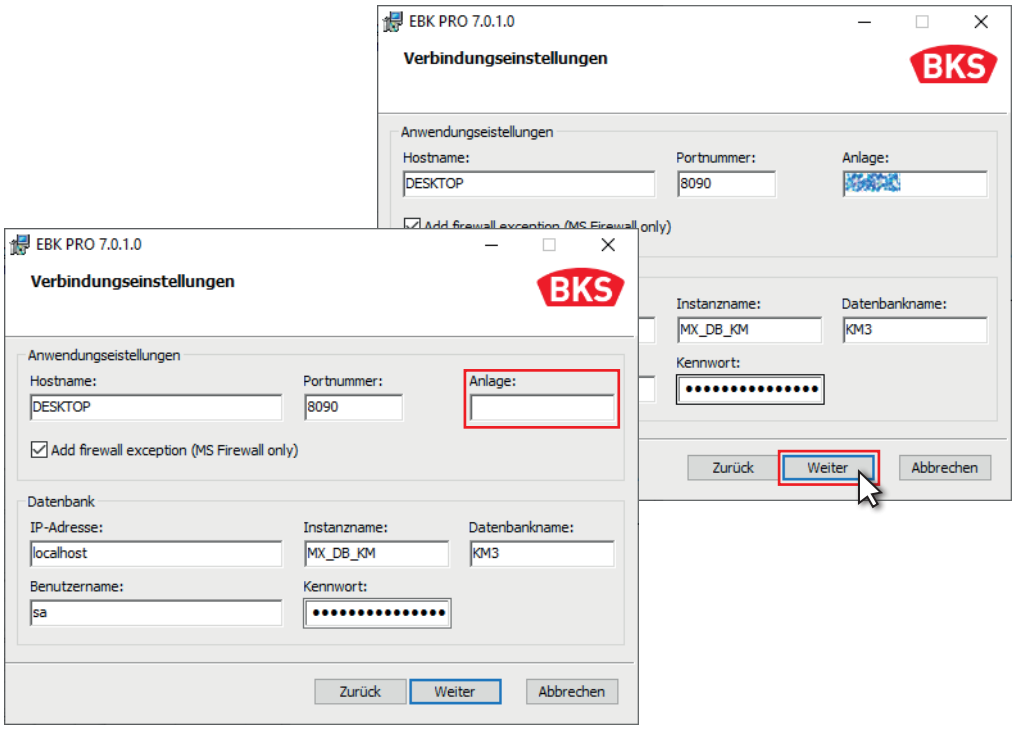
ACHTUNG

Achten Sie darauf, die Anlagenbezeichnung sowie die weiteren Parameter exakt einzugeben.

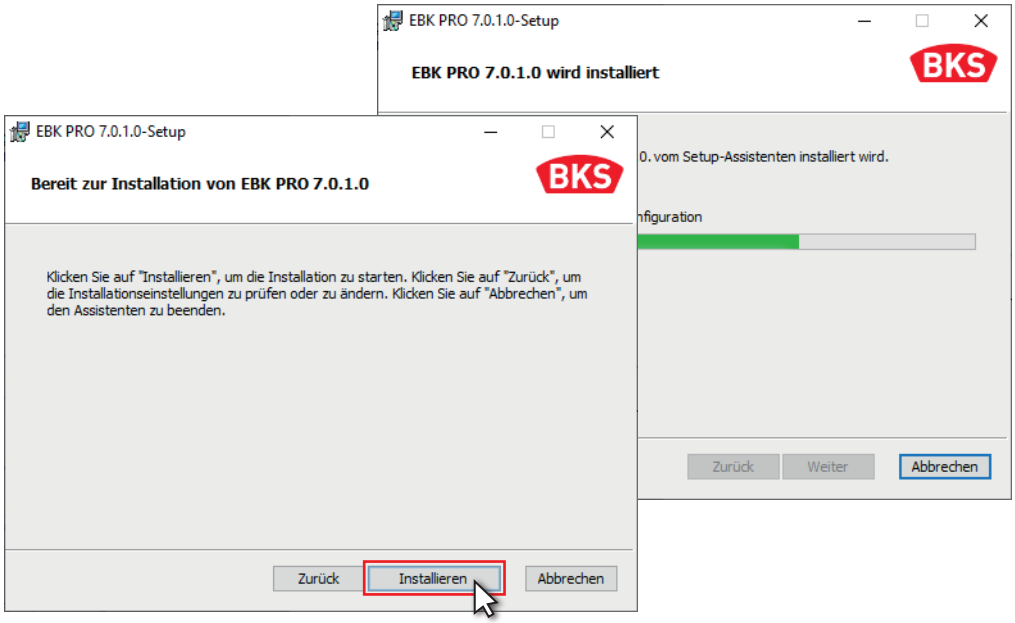
- **Wenn die Einstellungen nicht Korrekt sind, führt dies dazu, dass die weitere Einrichtung und der Betrieb von EBK und FGT nicht funktionieren.**

Die übrigen Einstellungen können ohne Veränderung übernommen werden, wenn Sie die übrigen Module des BKS KeyManagers mit Default-Einstellungen (empfohlen) installiert haben. Ansonsten ändern Sie ggf. abweichende Einstellungen.

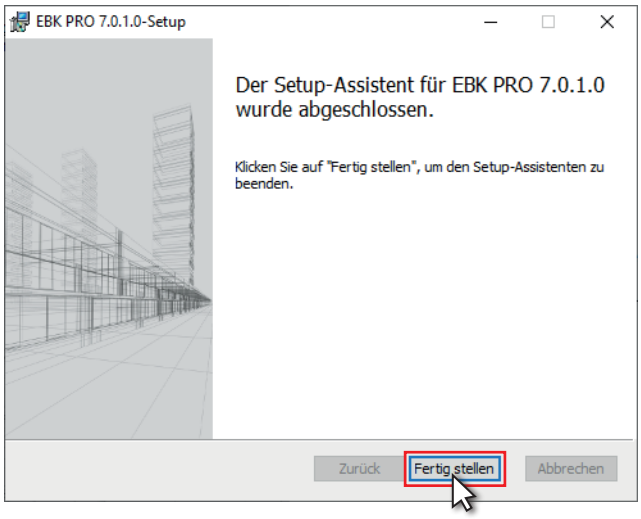
- Drücken Sie zum Fortfahren auf den Button „Weiter“.



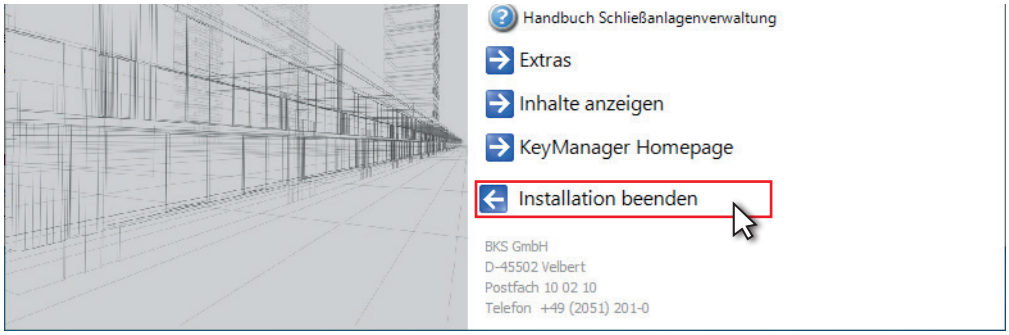
- Drücken Sie auf den Button „Installieren“, um mit der Installation zu beginnen.



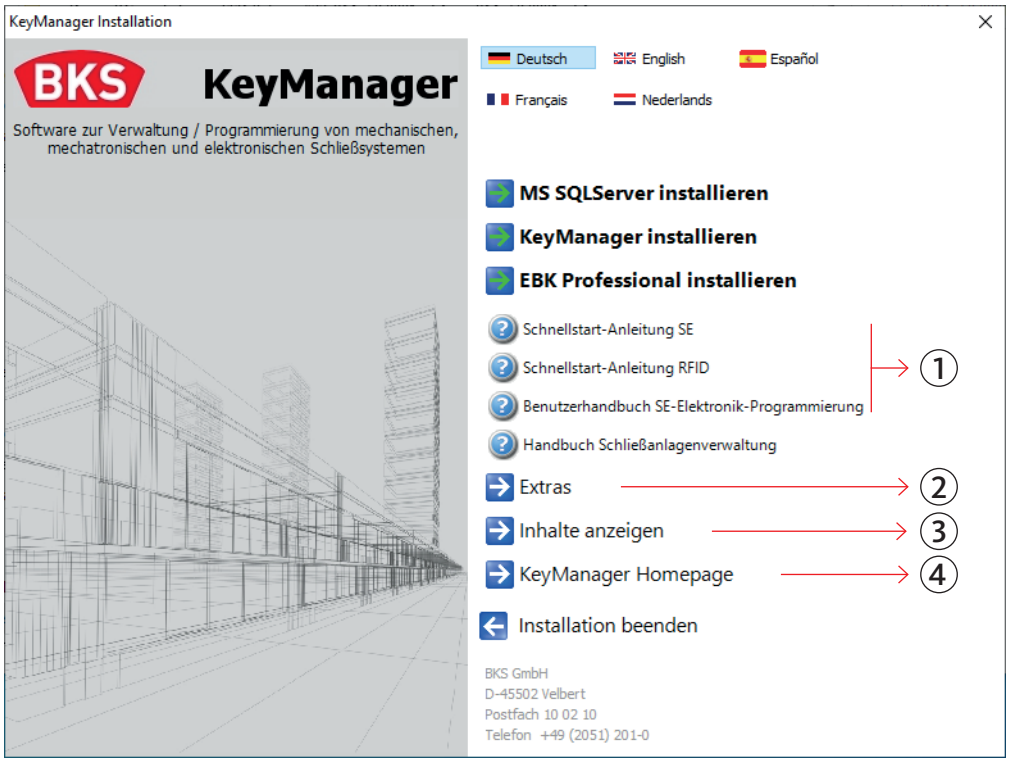
- Zur Beendigung der Installation drücken Sie den Button „Fertigstellen“.



- Durch Drücken auf den Menüpunkt „Installation beenden“, schließen Sie das Fenster.



2.9 Weitere Menüpunkte



Ergänzend zur Installation finden Sie in den weiteren Punkten noch weitere Informationen und Werkzeuge zur Einrichtung und Bedienung des BKS KeyManagers.

1.) Hilfe durch Anzeige der Anleitungen des BKS KeyMangers im PDF-Format.

2.) Weitere Extras.

3.) Inhalte des Installation-Ordners zeigen.

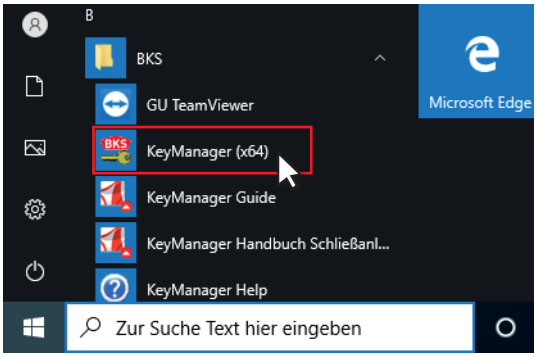
4.) Link zur Homepage.

3. Konzeption des BKS KeyManager

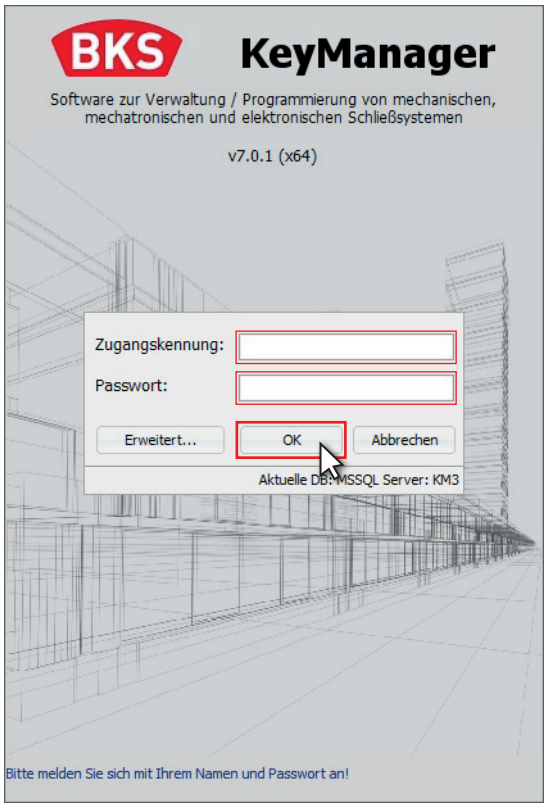
Zu den Grundlagen des BKS KeyManagers zählen die im Folgenden beschriebenen Grundfunktionen der Bedienung sowie die Übersicht der Benutzeroberfläche zur Programmierung und Verwaltung. Diese werden in erster Linie für eine Schließanlage als Offline-System erklärt, dadurch werden bestimmte Funktionen in diesem Kapitel nicht vollständig behandelt.

3.1 Programmstart

- Starten Sie die App durch Doppelklick des „KeyManager“-Symbols auf dem Desktop oder durch Auswählen des Programmpunkts „KeyManager (x64)“ im Windows Startmenü.



3.2 Anmeldung

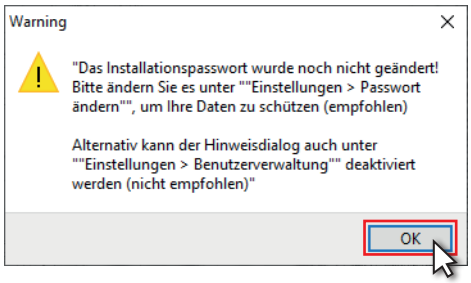


Für die erste Anmeldung nutzen Sie folgende Daten:

- Zugangskennung: BKS
- Passwort: Admin

HINWEIS **Aus Sicherheitsgründen wird dringend empfohlen, das Initialpasswort direkt nach der Installation zu ändern und ein neues Passwort festzulegen.**

Das folgende Fenster wird solange beim Programmstart angezeigt, bis Sie ein neues Passwort festgelegt haben.



Die Beschreibung zur Festlegung eines neuen Passworts oder zum Ändern des vorhanden finden Sie im Kapitel 6.5 [355]. Wir empfehlen die Verwendung eines sicheren Passworts.

ACHTUNG

Bewahren Sie das Passwort an einem sicheren Ort auf.
- **Bei Verlust besteht keine Möglichkeit, das Passwort zurückzubekommen.**

3.3 Startbildschirm

Bei erfolgreicher Anmeldung erscheint der Startbildschirm. Wählen Sie zwischen den Modulen des BKS KeyManagers „Schließanlagen Verwaltung“ oder „Elektronik-Programmierung“. Der BKS KeyManager startet dann im entsprechenden Modul.

HINWEIS **Dieses Benutzerhandbuch beschreibt das Modul für die Bedienung und Programmierung von elektromechanischen Schließanlagen.**

3.3.1 Modul „Schließanlagen Verwaltung“

Das Modul zur Schließanlagenverwaltung (mechanisch) ist nach der Installation des BKS KeyManagers für 60 Tage mit der vollen Funktionalität freigeschaltet. Nach Ablauf dieser Zeitspanne schaltet sich das Verwaltungsmodul ab, wenn es nicht registriert wird. Die Registrierung des Schließanlagenverwaltungsmoduls ist kostenpflichtig und kann auch nachträglich erfolgen. Die Elektronik-Produkte können über „Elektronik-Programmierung“ jederzeit weiter programmiert werden.

Eine detaillierte Beschreibung des Schließanlagenverwaltungsmoduls finden Sie im Benutzerhandbuch „KeyManager Schließanlagen Verwaltung“.

3.3.2 Modul „Elektronik-Programmierung“

Das Modul zur Elektronik-Programmierung wird auf den folgenden Seiten dieses Benutzerhandbuchs detailliert beschrieben. Wird die Auswahlmöglichkeit zwischen den Modulen nicht benötigt, kann durch Aktivierung der Checkbox „Startbildschirm ... nicht anzeigen“ der Startbildschirm bei der Anmeldung übersprungen werden.

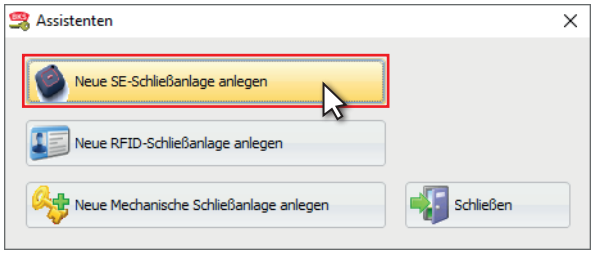
- Drücken Sie zum Start des Moduls auf den Button „Elektronik-Programmierung“.

3.4 Anlegen einer elektromechanischen Schließanlage

Wenn Sie noch keine elektromechanische Schließanlage eingerichtet haben, öffnet sich beim Start des Moduls der Inbetriebnahme-/Einrichtungsassistent automatisch. Über den Button „Einstellungen“ in der Menüzeile ist auch ein manueller Start des Assistenten möglich.

Der Assistent unterstützt Sie beim Anlegen der Schließanlage.

- Drücken Sie auf den Button „Neue SE-Schließanlage anlegen“, um den Assistenten zu starten.

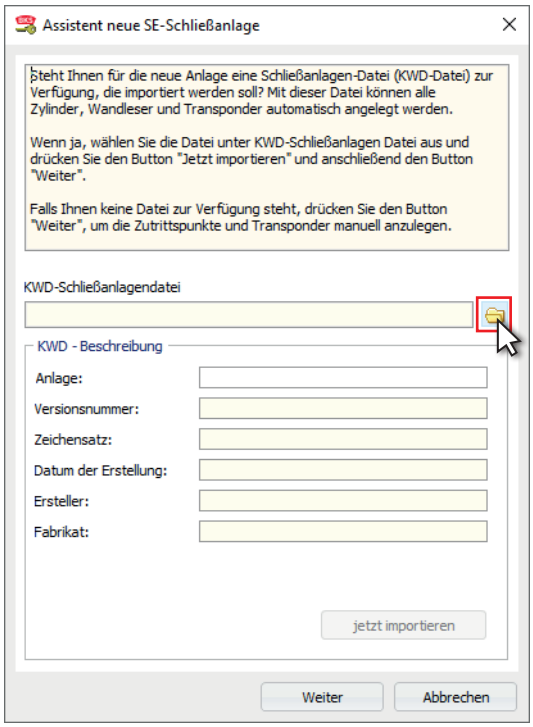


3.4.1 Schließanlage mit der Schließanlagendatei anlegen

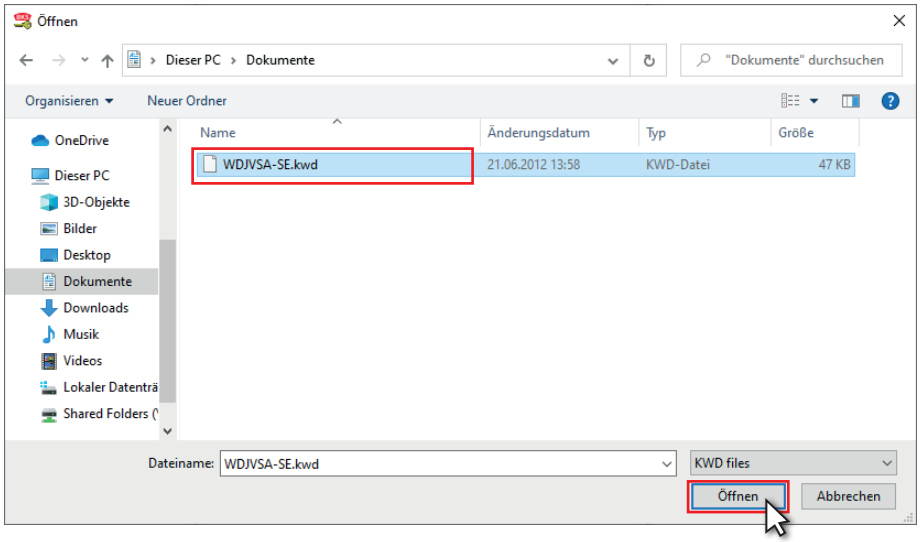
Die von Ihnen verwendeten Produkte können durch den Import der Schließanlagen-Datei der Schließanlage hinzugefügt werden. Der Inhalt dieser KWD-Datei (*.KWD) bildet die verwendeten Komponenten in der Schließanlage ab. Der BKS KeyManager legt diese durch den Import der KWD-Datei in der Schließanlage an.

Bei diesem Vorgang werden sowohl mechanische und elektromechanische Zylinder als auch alle Schlüssel und Transponder angelegt und mit Eigenschaften wie z. B. der Türbezeichnung, in die der Zylinder eingebaut ist, versehen.

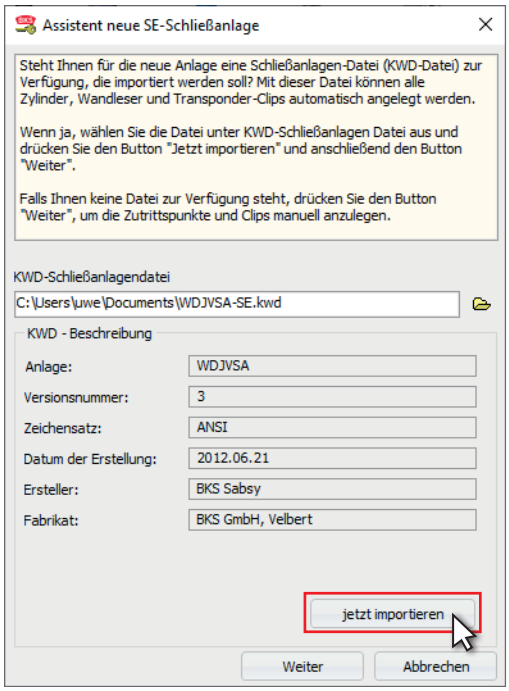
- Drücken Sie auf das Verzeichnissymbol.

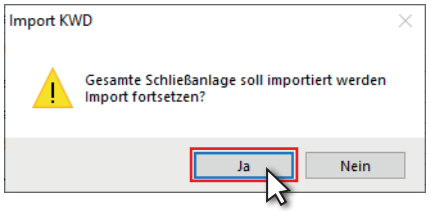


- Navigieren Sie mit dem Dateibrowser zur Schließanlagendatei (*.KWD) und drücken Sie auf den Button „Öffnen“.

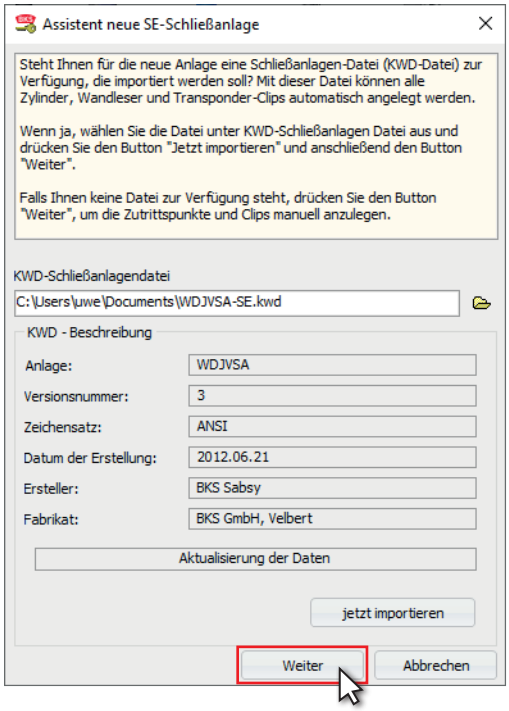


- Drücken Sie auf den Button „jetzt importieren“ und zur Bestätigung auf „Ja“.





■ Mit dem Button „Weiter“ gelangen Sie zum Import der Lizenzen.

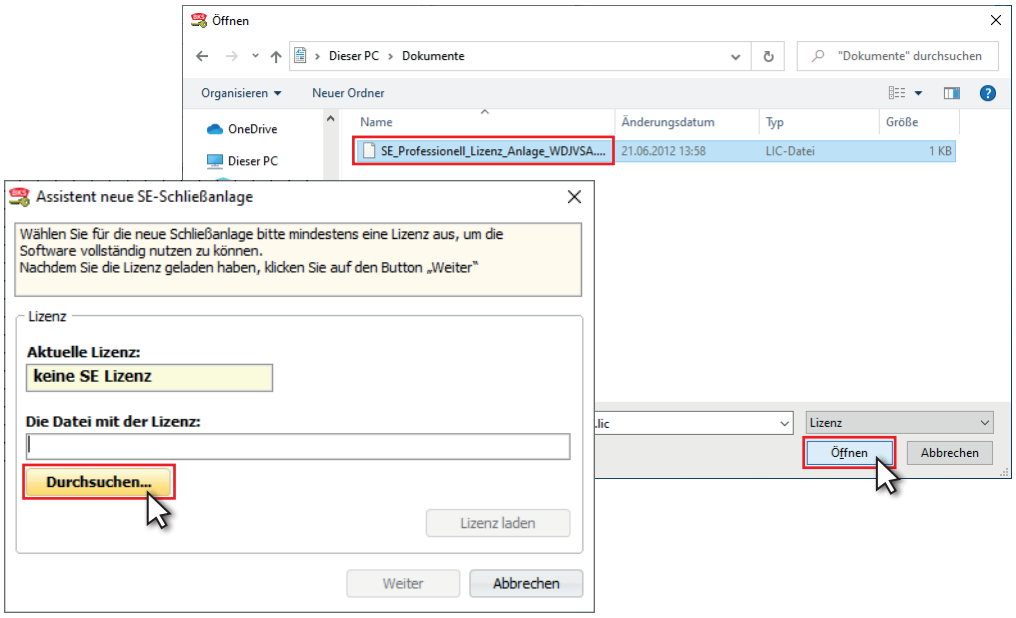


3.4.1.1 Lizenzen der Schließanlage hinzufügen

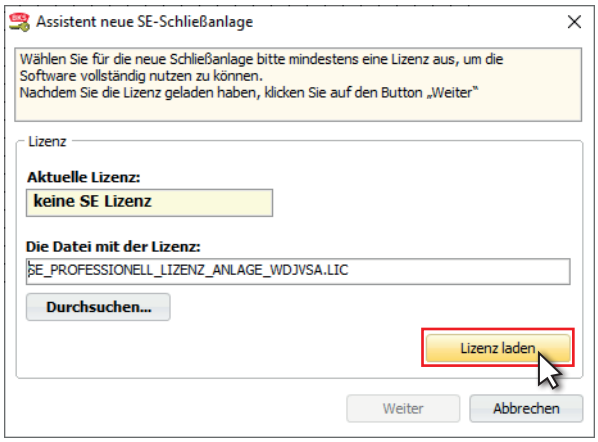
Zur Nutzung des BKS KeyManagers wird eine Lizenz benötigt. Laden Sie die Lizenzen für Ihre Schließanlage in den BKS KeyManager. Die Lizenzdateien enden mit der Bezeichnung „.lic“.

■ Drücken Sie auf den Button „Durchsuchen ...“ und öffnen den Dateibrowser.

■ Wählen Sie die Lizenzdatei aus und laden diese mit dem Button „Öffnen“ in den BKS KeyManager.

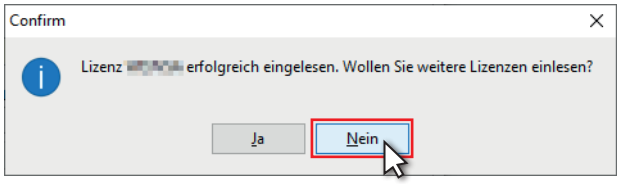


- Drücken Sie auf den Button „Lizenz laden“, um den BKS KeyManager zu lizenzieren.



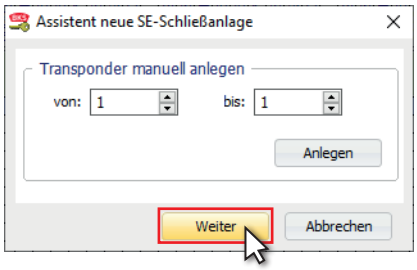
Im nächsten Fenster können Sie auswählen, ob eine weitere Lizenzierung durchgeführt werden soll.

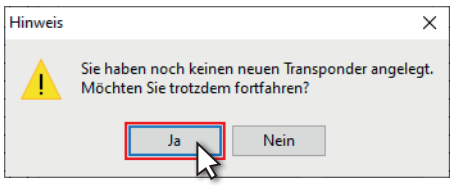
- Drücken Sie auf den Button „Ja“, um eine weitere Lizenz zu laden.
- Drücken Sie auf den Button „Nein“, um fort zu fahren.



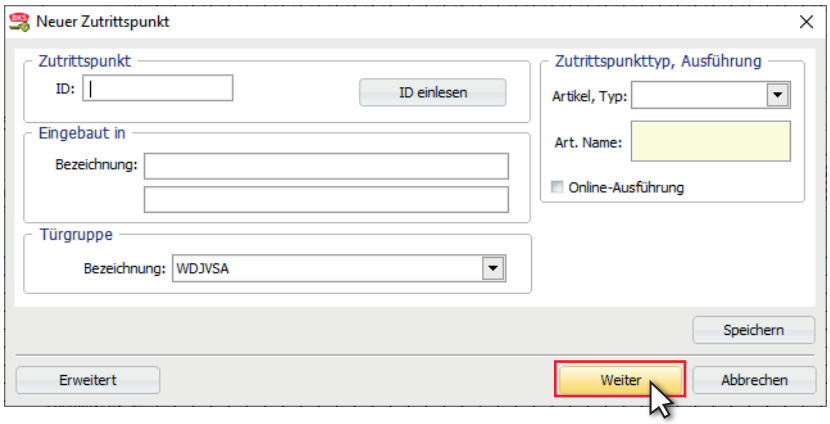
Die Transponder und Zutrittspunkte worden bereits über die KWD-Datei der Anlage hinzugefügt.

- Drücken Sie auf den Button „Weiter“ und zur Bestätigung auf „Ja“.





- Drücken Sie auf den Button „Weiter“.

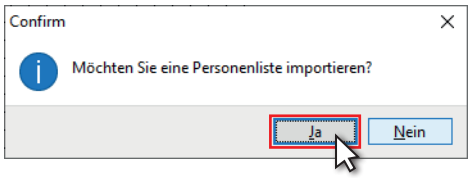


3.4.1.2 Personenliste der neuen Schließanlage hinzufügen

Es kann eine Personenliste für die Schließanlage geladen werden. Die Personenliste können Sie über eine CSV-Datei (*.CSV) importieren.

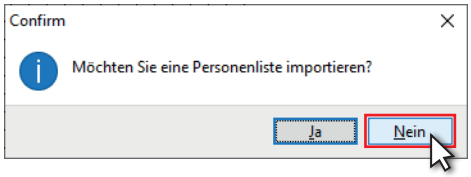
HINWEIS **Achten Sie darauf, dass die CSV-Datei auf eine „UTF-8“-Codierung eingestellt ist, weil es keinen allgemeinen Standard für das Dateiformat CSV gibt!**

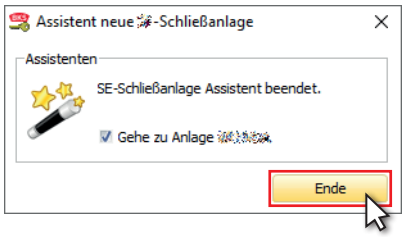
- Drücken Sie auf den Button „Ja“, um eine Personenliste zu importieren.



Sie können auch den Import zu einem späteren Zeitpunkt durchführen, wenn Ihnen keine Personenliste zur Verfügung steht. In diesem Fall ist der Assistent zu beenden.

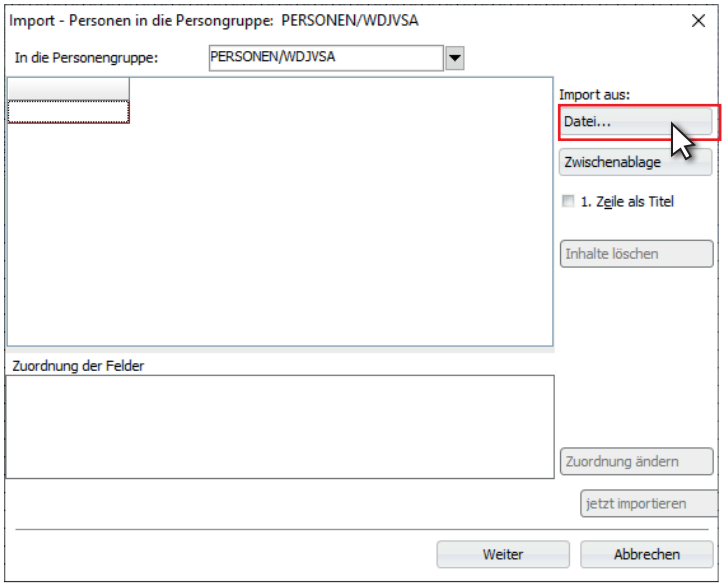
- Drücken Sie auf den Button „Nein“, um die Anlage der Schließanlage zu beenden, ohne eine Personenliste zu importieren.
- Wechseln Sie mit „Ende“ zu der neu angelegten Schließanlage.



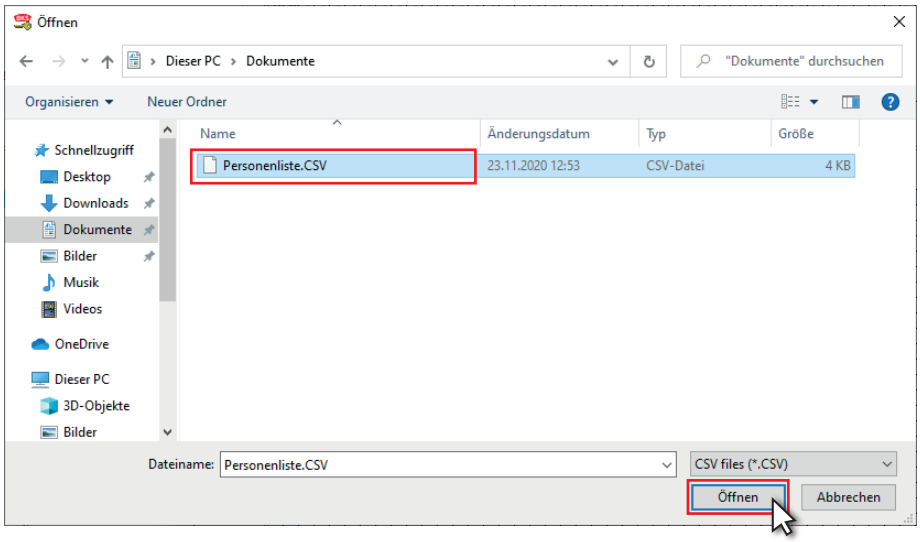


Nach der Auswahl „Personenliste importieren“ öffnet sich folgender Dialog.

- Drücken Sie auf den Button „Datei ...“ in der Spalte „Import aus:“ des Fensters.

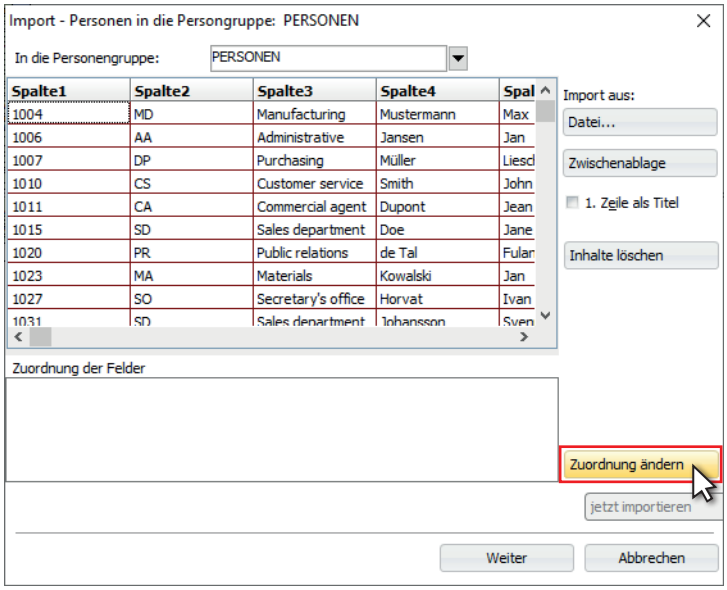


- Navigieren Sie mit dem Dateibrowser zur Personenliste. Die Datei muss im CSV-Format (*.CSV) vorliegen.
- Drücken Sie auf den Button „Öffnen“, um den Import zu starten.



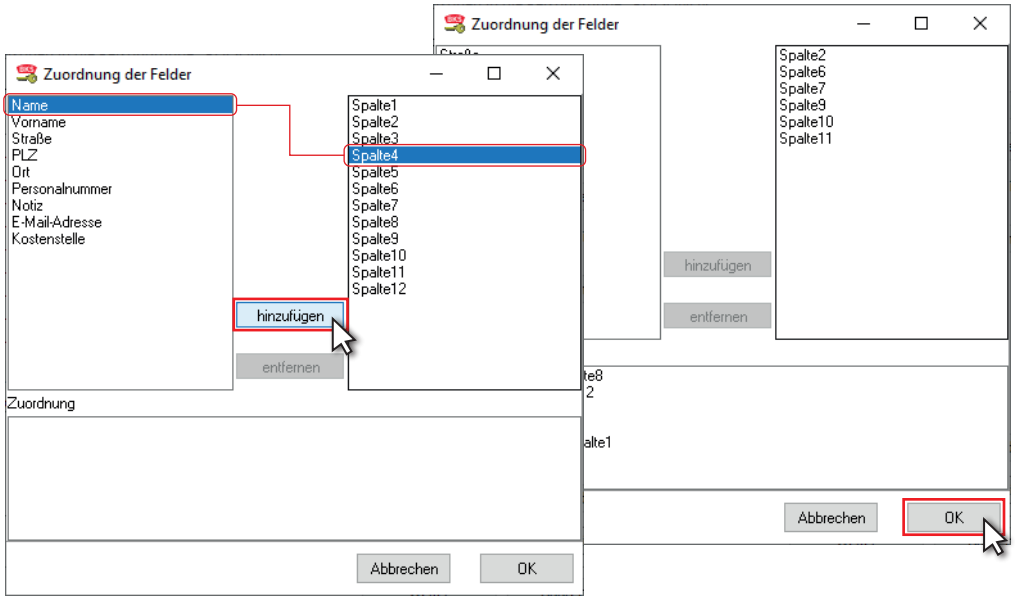
Zur Übersicht wird Ihnen die importierte Personenliste angezeigt. Die Spalten der Personenliste sind den Feldern des BKS KeyManagers zuzuweisen.

- Drücken Sie auf den Button „Zuordnung ändern“.

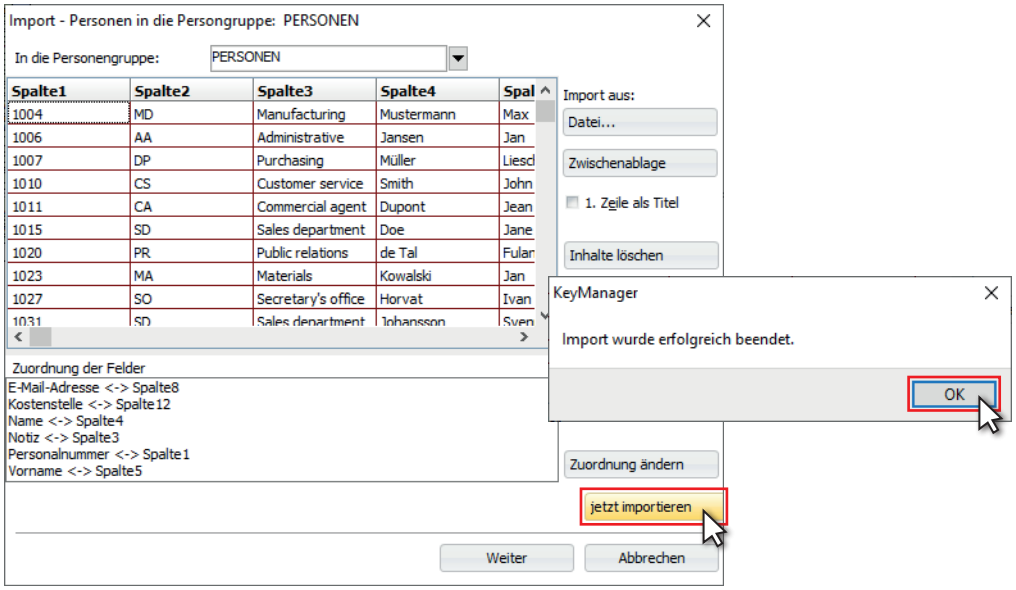


Ordnen Sie im Fenster „Zuordnung der Felder“ die personenbezogenen Daten der dazugehörigen Spalte zu. Zum Beispiel „Name“ und „Spalte 4“.

- Wählen Sie „hinzufügen“ aus und stellen Sie die Zuordnung her.
- Nach der Zuordnung der Spalten der Personenliste mit den Feldern des BKS KeyManagers fahren Sie mit „jetzt importieren“ fort.
- Beenden Sie die Zuordnung und drücken auf den Button „OK“.



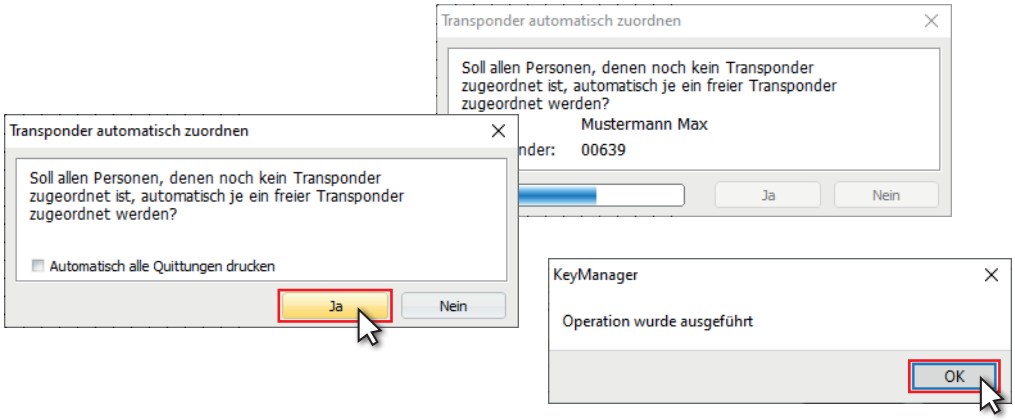
- Lesen Sie die Personenliste mit „jetzt importieren“ ein und drücken zur Bestätigung auf den Button „OK“.



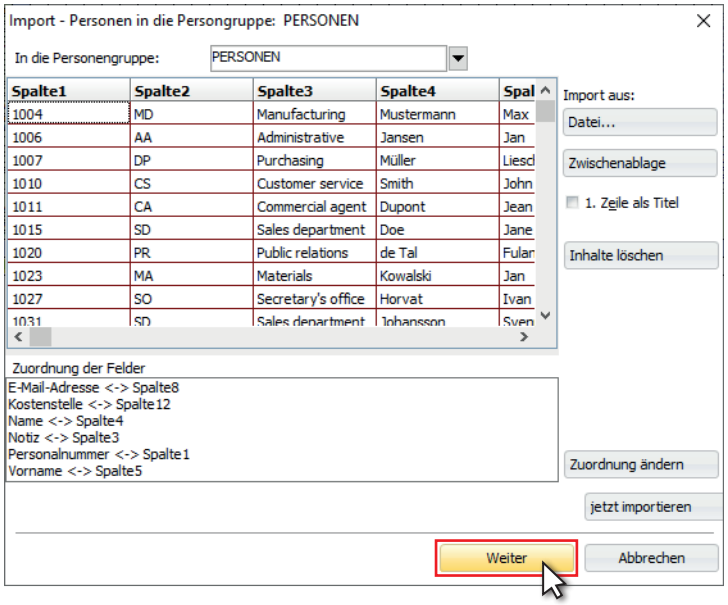
3.4.1.2.1 Automatische Transpondervergabe

Allen Personen, die noch keinen Transponder haben, kann automatisch ein Transponder zugeordnet werden. Bei Ausgabe von mehreren Transpondern kann dies eine große Zeitersparnis sein.

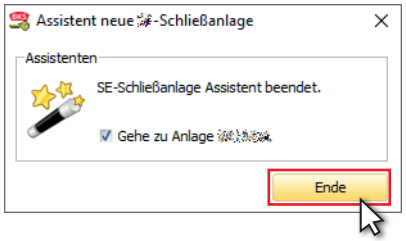
- Drücken Sie auf den Button „Ja“, um die Zuordnung zu starten.



- Drücken Sie auf den Button „Weiter“, um die Zuordnung abzuschließen.



- Zum Beenden des Assistenten drücken Sie auf den Button „Ende“ und schließen Sie den Assistenten der Schließanlage ab.

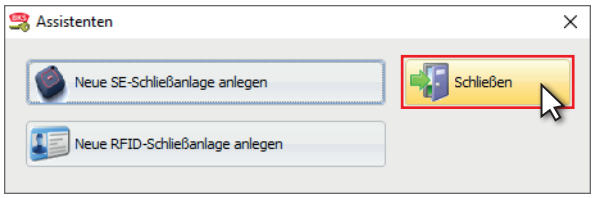


3.4.2 Schließanlage über Datenrücksicherung wiederherstellen

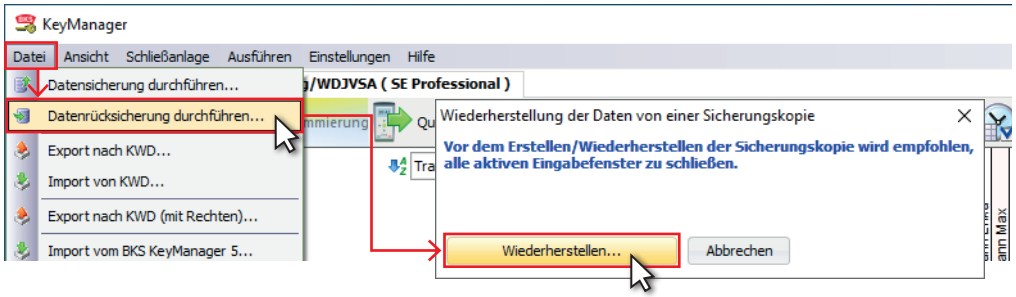
Eine Möglichkeit zur Erstellung einer Schließanlage ist die Wiederherstellung mit einer von Ihnen bereits erstellten und gespeicherten Schließanlage.

Beim Start des BKS KeyManagers öffnet sich automatisch, wenn Sie noch keine elektromechanische Schließanlage eingerichtet haben, der Inbetriebnahme-/Einrichtungsassistent.

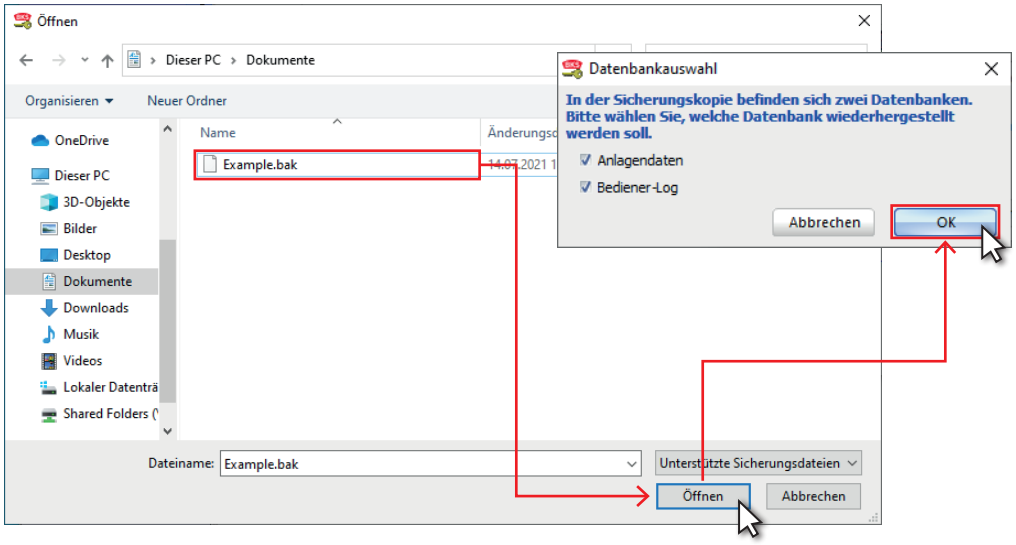
- Drücken Sie auf den Button „Schließen“ zum Beenden des Assistenten.



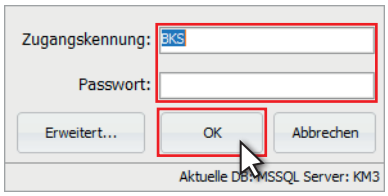
- Wählen Sie über das Dropdown-Menü „Datei“ den Menüpunkt „Datenrücksicherung durchführen ...“ aus.
- Drücken Sie auf den Button „Wiederherstellen ...“.

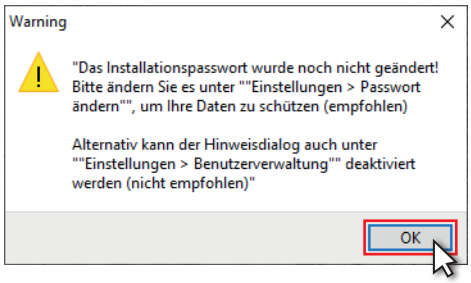


- Navigieren Sie im Dateibrowser zum Speicherort der Wiederherstellungsdatei „*.bak“ oder „*.fbk“. Wählen Sie diese aus und drücken auf den Button „OK“.
- Aktivieren/Deaktivieren Sie ggf. bei Bedarf die Checkboxen und drücken auf den Button „OK“.

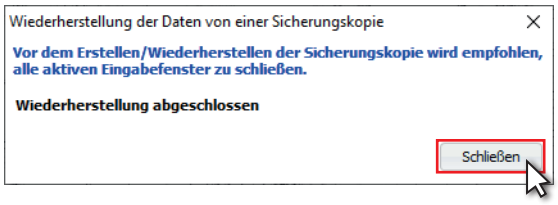


- Melden Sie sich in der Datenbank mit Ihrer „Zugangskennung“ und „Kennwort“ an und drücken auf den Button „OK“. Falls das Passwort noch nicht geändert wurde, ist der Hinweis mit „OK“ zu bestätigen.





- Drücken Sie auf den Button „Schließen“ und beenden den Dialog.

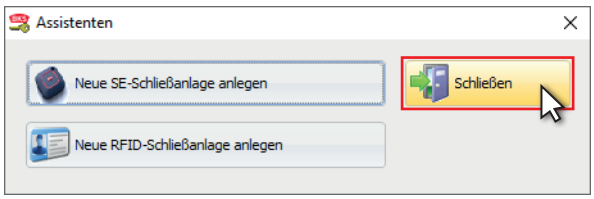


3.4.3 Import einer Schließanlage von Version 5 des BKS KeyManagers

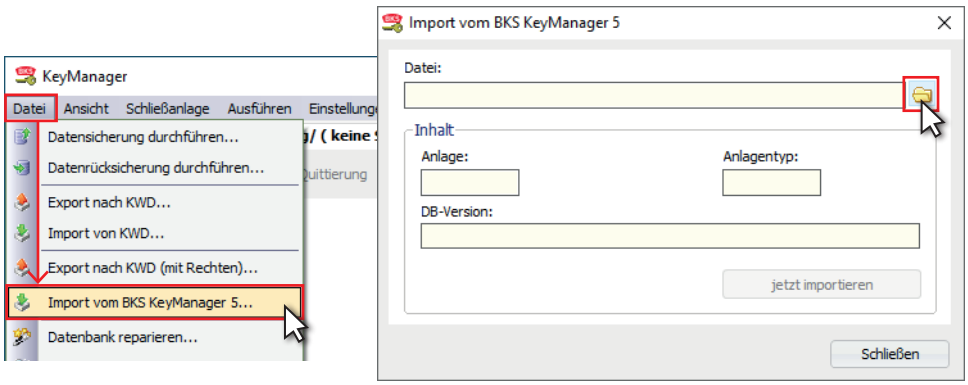
Eine bestehende Schließanlage des BKS KeyManagers 5 ist mit der folgenden Funktion in den BKS KeyManager 7 zu importieren. Grundvoraussetzung ist, dass der BKS KeyManager mit einer MS SQL-Datenbank installiert wurde. Die Version mit interner Datenbank kann hierfür nicht verwendet werden. Weiterhin ist eine in der Programmversion 5 erstellte Datenbank-Datei (*.bak) erforderlich.

Beim Start des Keymanagers öffnet sich automatisch, wenn Sie noch keine elektromechanische Schließanlage eingerichtet haben, der Inbetriebnahme-/Einrichtungsassistent

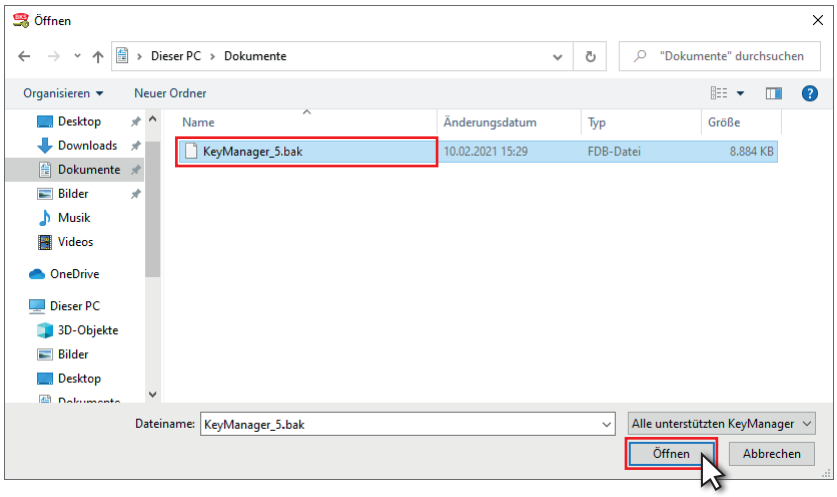
- Drücken Sie auf den Button „Schließen“ um den Assistenten zu beenden.



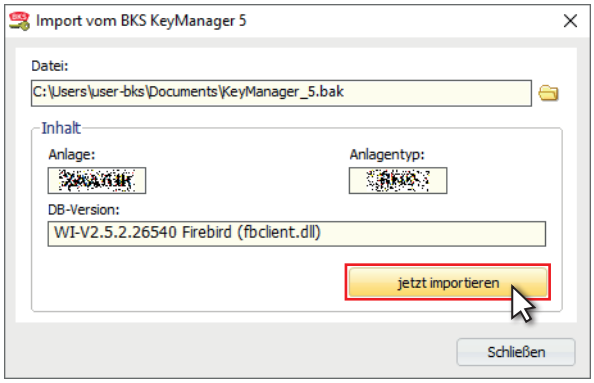
- Wählen Sie über das Dropdown-Menü „Datei“ den Menüpunkt „Import vom KeyManager 5 ...“ aus.
- Drücken Sie auf das Verzeichnissymbol.



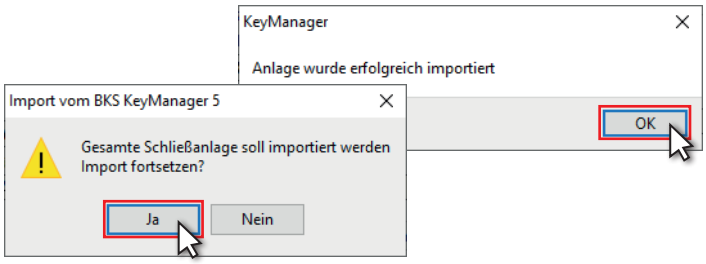
- Navigieren Sie mit dem Dateibrowser zur entsprechenden Sicherungsdatei „*.bak“ und wählen diese aus. Drücken Sie auf den Button „Öffnen“.



- Starten Sie den Import und drücken den Button „jetzt importieren“.



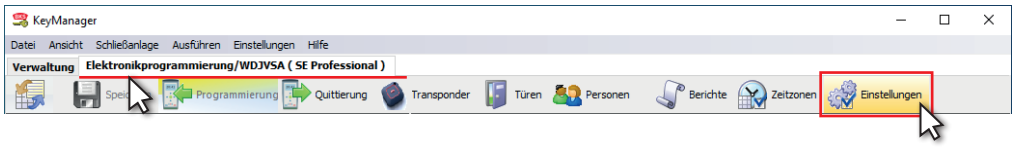
- Beenden Sie den Import der Schließanlage und drücken in den beiden Fenstern jeweils auf den Button „Ja“ und „OK“.



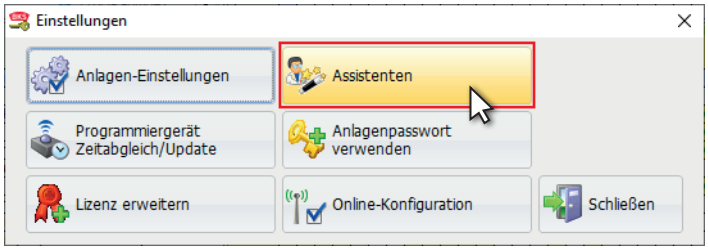
3.4.4 Inbetriebnahme-Assistent „Neue Schließanlage“ starten

Sollte sich der Assistent bei der Inbetriebnahme nicht automatisch öffnen, können Sie diesen auch manuell starten um eine Schließanlage anzulegen.

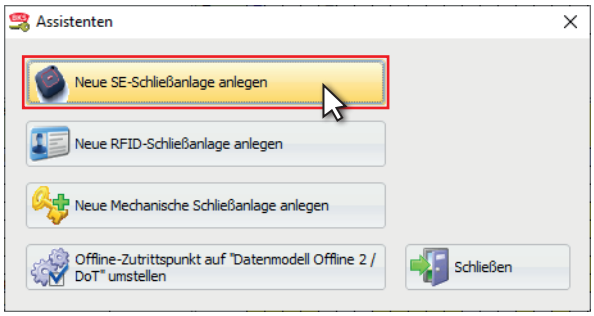
- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Einstellungen“.



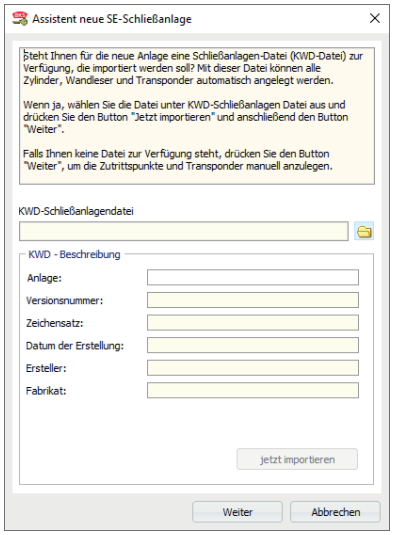
- Drücken Sie auf den Button „Assistenten“ im Menü Einstellungen.



- Starten Sie den Inbetriebnahme-Assistenten manuell und drücken auf den Button „Neue SE -Schließanlage anlegen“ und beginnen mit dem Anlegen.



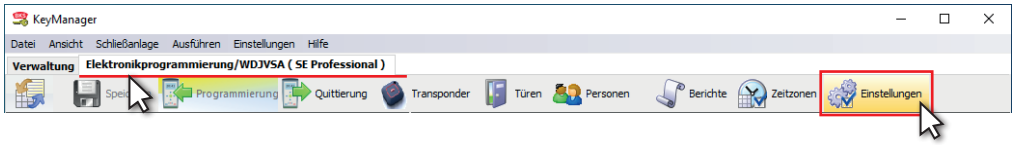
Zur weiteren Einrichtung folgen Sie Kapitel 3 [62] zum Anlegen einer Schließanlage.



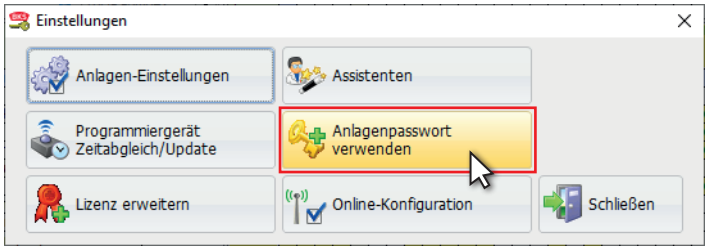
3.4.5 Anlagenpasswort festlegen

Falls Sie das optionale Anlagenpasswort für Ihre Schließanlage verwenden möchten, ist nach dem Anlegen der Schließanlage der beste Zeitpunkt zum Einrichten dieses Passworts. Das einmalig vergebene Anlagenpasswort wird fortan bei jeder Programmierung vom Zutrittspunkt geprüft. Eine missbräuchliche Programmierung wird so verhindert. Bei Verlust des Anlagenpassworts ist ein Rücksetzen des Passworts nicht möglich. Kontaktieren Sie den Service der Firmengruppe Gretsch-Unitas und senden nach Absprache die Zutrittspunkte ein.

- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Einstellungen“.

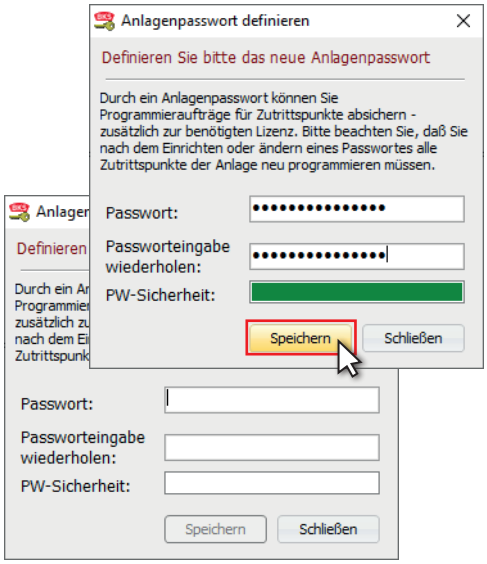


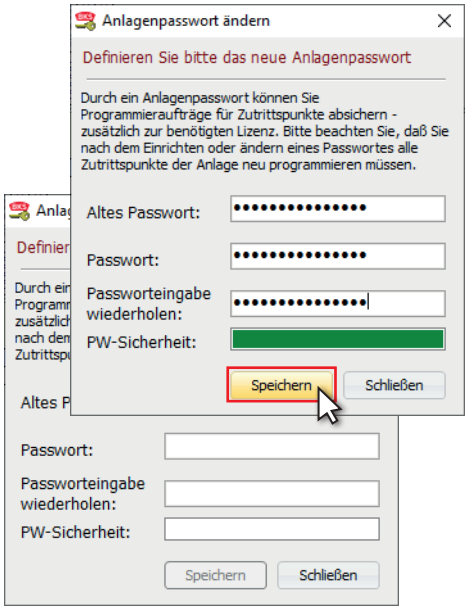
- Drücken Sie den Button „Anlagenpasswort verwenden“ im Menü Einstellungen.



Im folgenden Fenster werden Sie aufgefordert, ein Passwort einzugeben. Ist ein Passwort schon einmal vergeben worden, müssen Sie vor der Neueingabe zuerst das alte Passwort eingeben.

Das Passwort muss aus mindestens 8 Zeichen bestehen. Die Sicherheit des Passworts wird durch die Verwendung von Klein- und Großbuchstaben sowie von Zahlen und Sonderzeichen erhöht.

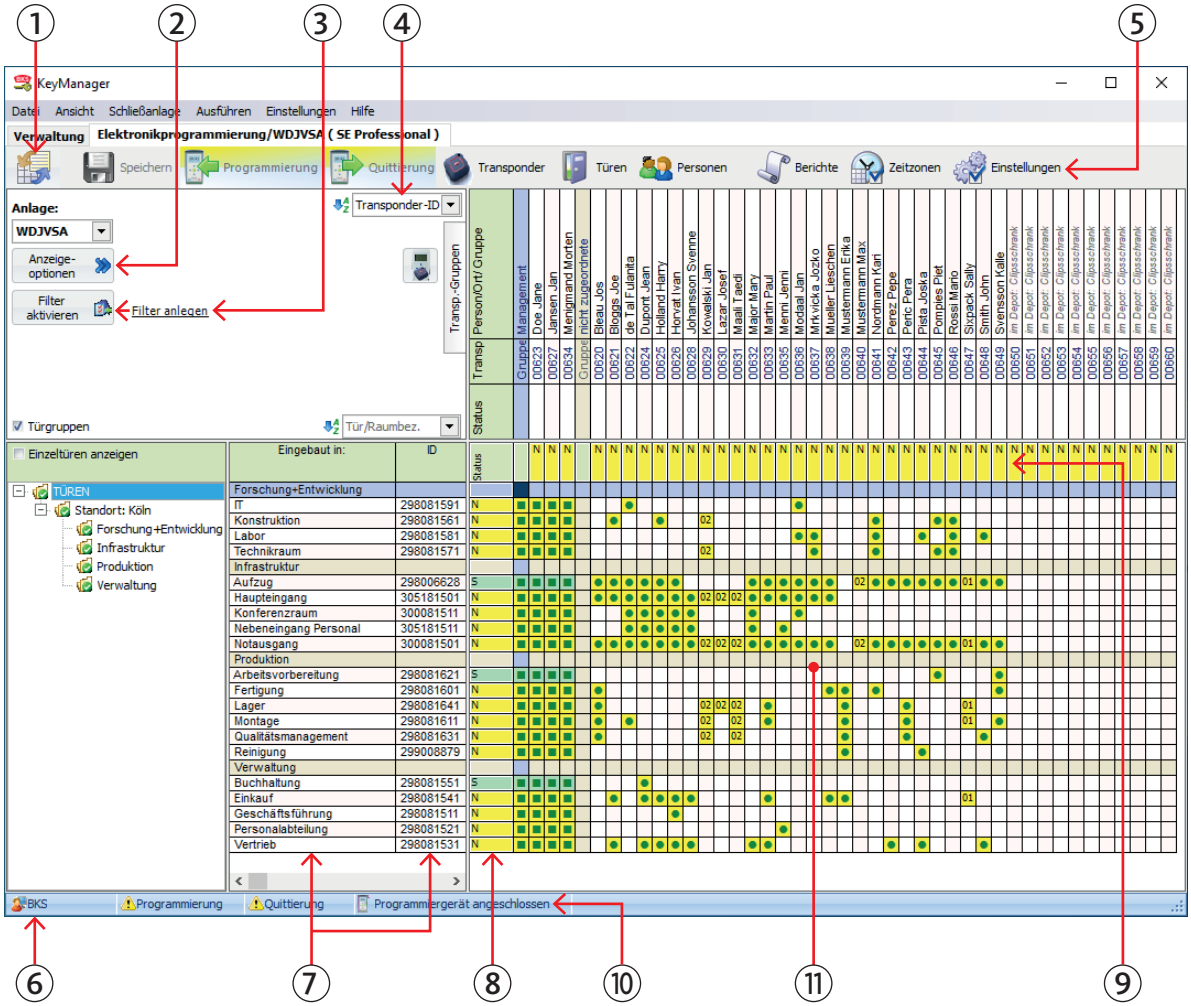


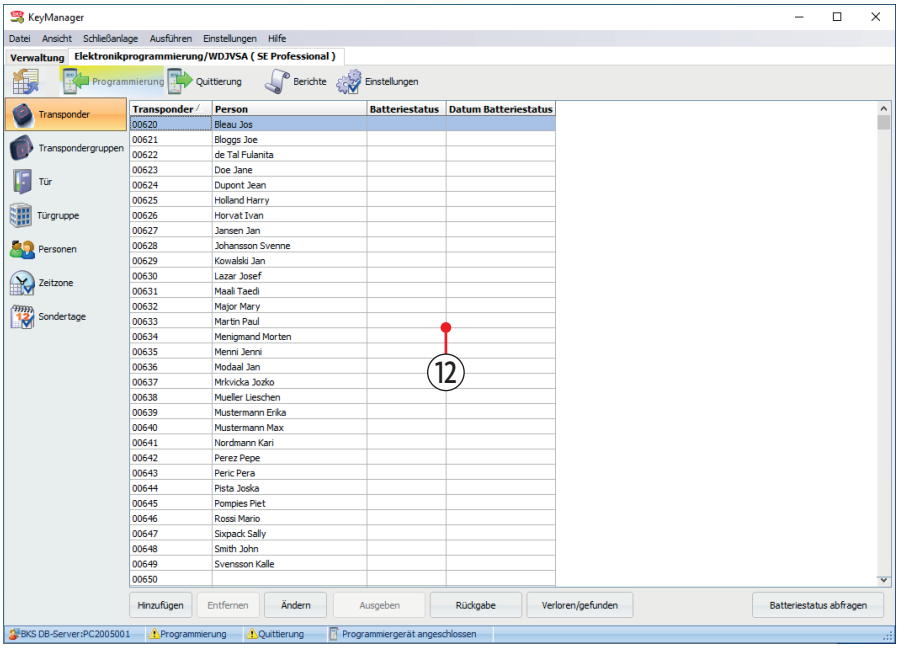


Die Sicherheitsstufe des Passworts wird ihnen als farbiger Balken angezeigt.
Ab Sicherheitsstufe gelb können Sie das Passwort mit „Speichern“ übernehmen.

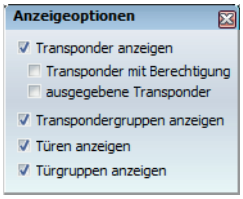
3.5 Die Hauptfunktionen im Überblick | Berechtigungsmatrix

3.5.1 Aufbau des Hauptbildschirms





Wesentliche Bestandteile des Hauptbildschirms „Berechtigungsmatrix“.

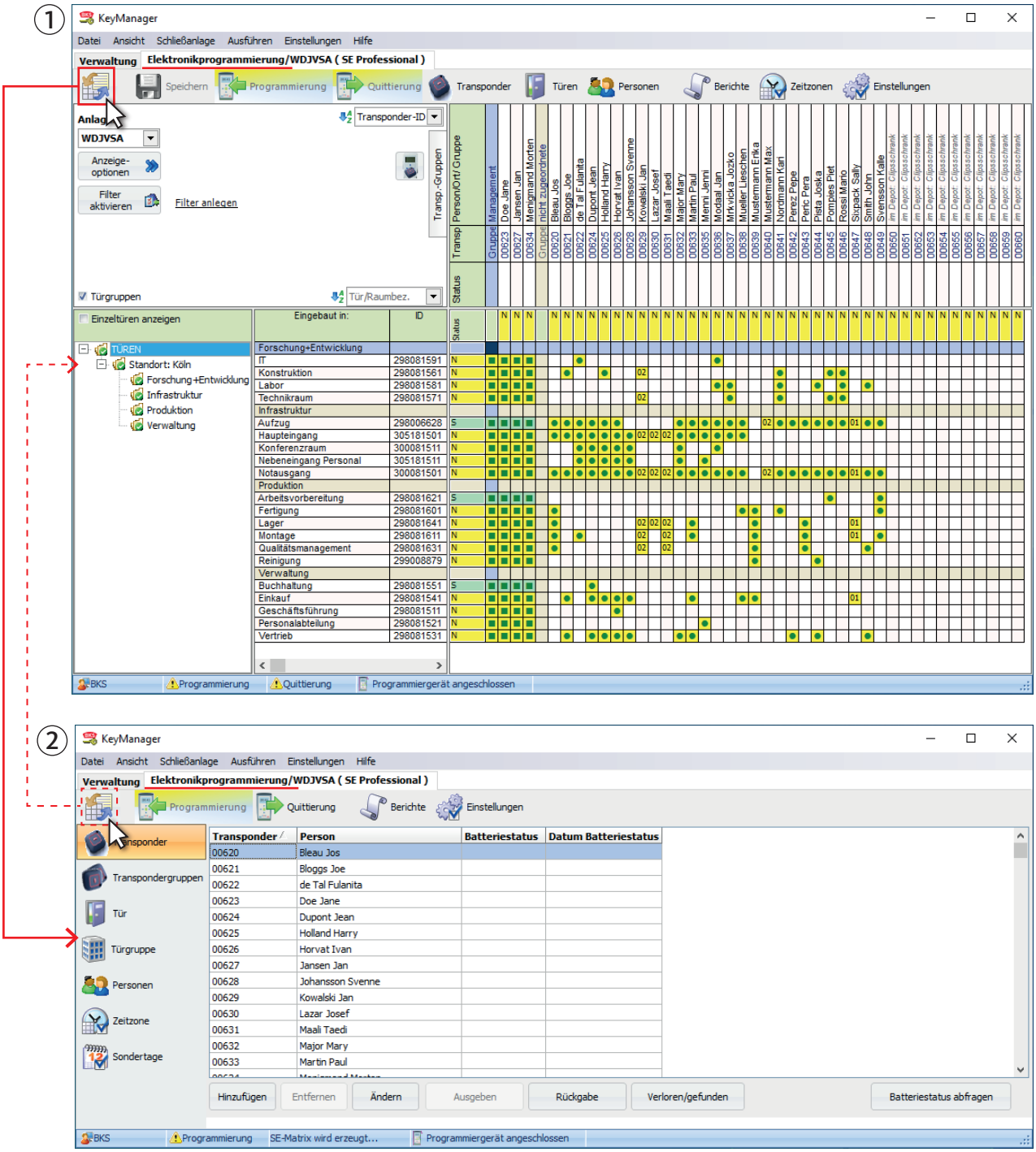
Nr.	Beschreibung
1.	Wechseln der Ansichten „Berechtigungsmatrix“ (11) <-> „Listenmenü“ (12)
2.	Anzeigeoptionen für die Darstellung in der Matrix 
3.	Filter anlegen und aktivieren für Transponder- und Türengruppen
4.	Transponder/Personenname
5.	Matrix-Menüband mit den Buttons zum Aufrufen der Menüpunkte
6.	Aktuell angemeldeter Bediener
7.	Türenliste mit Zutrittspunkt-ID
8.	Programmierstatus der Zutrittspunkte
9.	Programmierstatus der Transponder (nur DoT-Anlage)
10.	Status Programmiergerät
11.	Matrix mit der Übersicht der Berechtigungen
12.	Listenmenü, Übersichtsansicht für die Menüpunkte des Hauptmenüs

3.5.2 Funktionalitäten der Berechtigungsmatrix und des Listenmenüs

Die Grundfunktionen des BKS KeyManagers lassen sich in Berechtigungsmatrix (1) und im Listenmenü (2) aufrufen. Die Listenansicht bietet bei der Bearbeitung Vorteile. Um diese zu nutzen, kann die Anzeige von der beim Programmstart gezeigten Berechtigungsmatrix zum Listenmenü gewechselt werden.

- Drücken Sie zum Wechseln auf den Button mit dem Symbol „Listenmenü anzeigen“.

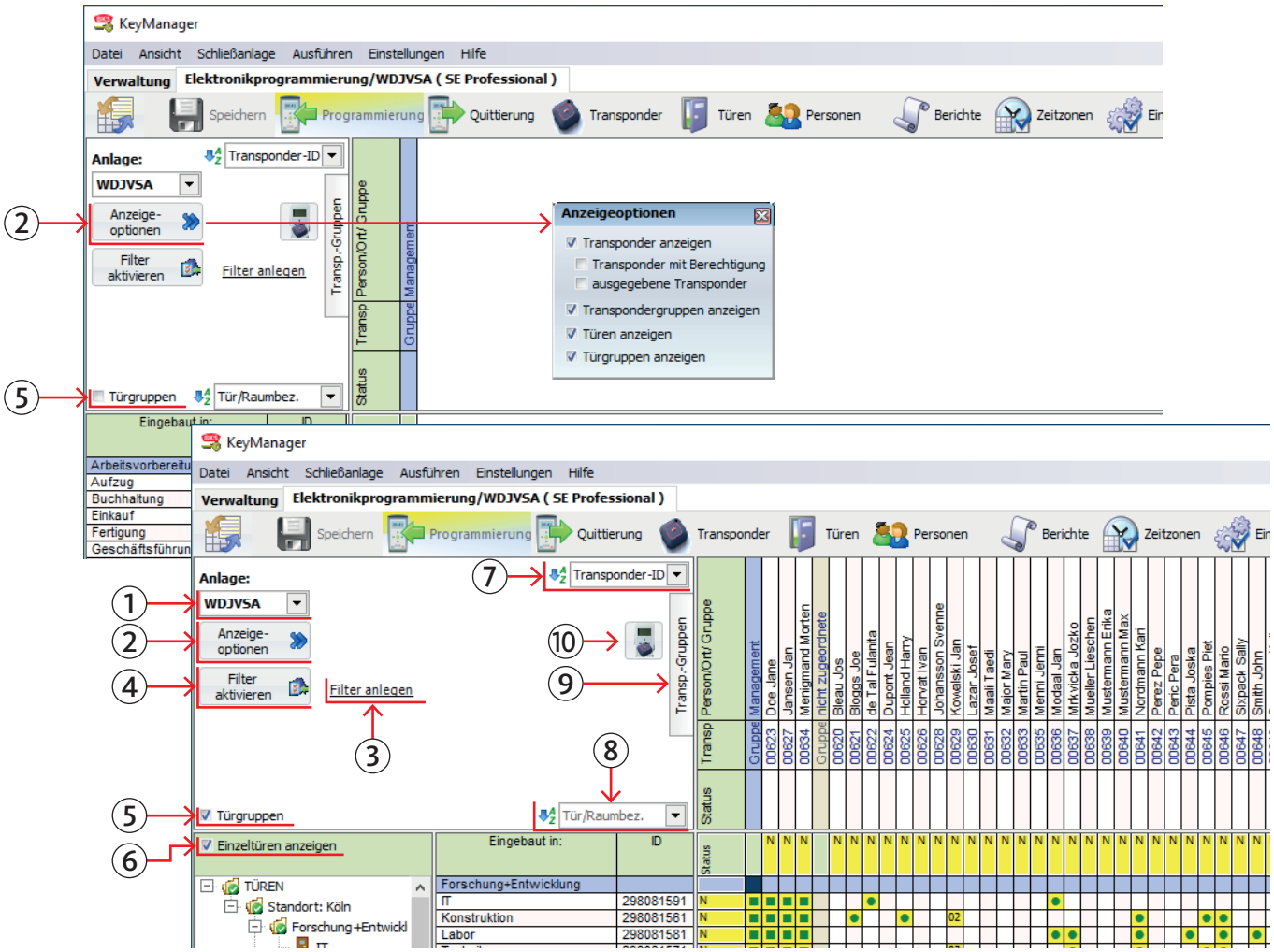
Die Darstellung Listenansicht kann durch Drücken dieses Buttons jetzt mit der Funktion „SE-Matrix anzeigen“ auf die Berechtigungsmatrix zurückgewechselt werden.



3.5.3 Berechtigungsmatrix

3.5.3.1 Darstellungsoptionen der Berechtigungsmatrix

Die Darstellung und der Umfang der angezeigten Elemente in der Berechtigungsmatrix kann über die Funktionen des in der linken oberen Ecke des Fensters befindlichen Menüs angepasst werden.



1	Aktuell aufgerufene bearbeitbare Schließanlage. Dropdown-Menü mit Möglichkeit zur Auswahl einer anderen in der Datenbank vorhandenen Schließanlage.
2	Filter zur Steuerung der Anzeige von Transpondern, Türen und Gruppen. Die Auswahl der Checkboxen erweitert oder schränkt die angezeigten Elemente ein.
3 4	Individueller Filter zur Administration der Ansicht von Transponder- und Türgruppen. Aktivieren oder Deaktivieren des Filters (3).
5 6	Checkbox zum Einblenden der Türgruppen als Verzeichnisbaum in der Matrixansicht. Checkbox zur Anzeige der einzelnen Türen im Verzeichnisbaum der Türgruppen.
7 8	Alphabetische Sortierung der Spalten der Matrix nach Transpondern bzw. Personen. Alphabetische Sortierung der Zeilen der Matrix nach Türen/Raumbezeichnung.
9	Filter zur Einschränkung der Matrix auf die ausgewählten Transpondergruppen.
10	Funktion zur Programmierung der Transponder in DoT-Anlagen, siehe Kapitel 3.8.1 [147].

Mit dem Filter „Anzeigeoption“ ist es möglich, die in der Matrix dargestellten Elemente jeweils getrennt für Türen und Transponder einzuschränken. Der Filter ist entweder durch die Auswahl der Checkboxen auf die einzelnen Türen, Transponder oder auf die Gruppen zu setzen. Eine Anzeige von einzelnen Türen, Transponder und der Gruppen ist auch möglich.

Die Transponder lassen sich zusätzlich auf die Transponder mit einer Berechtigung und/oder die Ausgegebene, welche sich im Besitz einer Person befinden, beschränken.

- Drücken Sie auf den Button „Anzeigeoption“ und wählen über die Checkboxen im nächsten Fenster die gewünschten Elemente aus, welche angezeigt werden sollen.

3.5.3.2 Filter zur Administration und Reduzierung der Matrix

Die Anzahl der angezeigten Türen und Transponder kann durch das Setzen eines individuell erstellten Filters eingerichtet werden. Bei der Konfiguration des Filters können Tür- und Transpondergruppen selektiert werden, die nach Aktivierung des Filters eine Einschränkung der Ansicht auf ausgewählten Gruppen bewirken. Mit aktiviertem Filter werden nur die ausgewählten Daten sichtbar, wodurch die Bearbeitung in Folge der besseren Übersichtlichkeit und Konzentration der Informationen erleichtert wird.

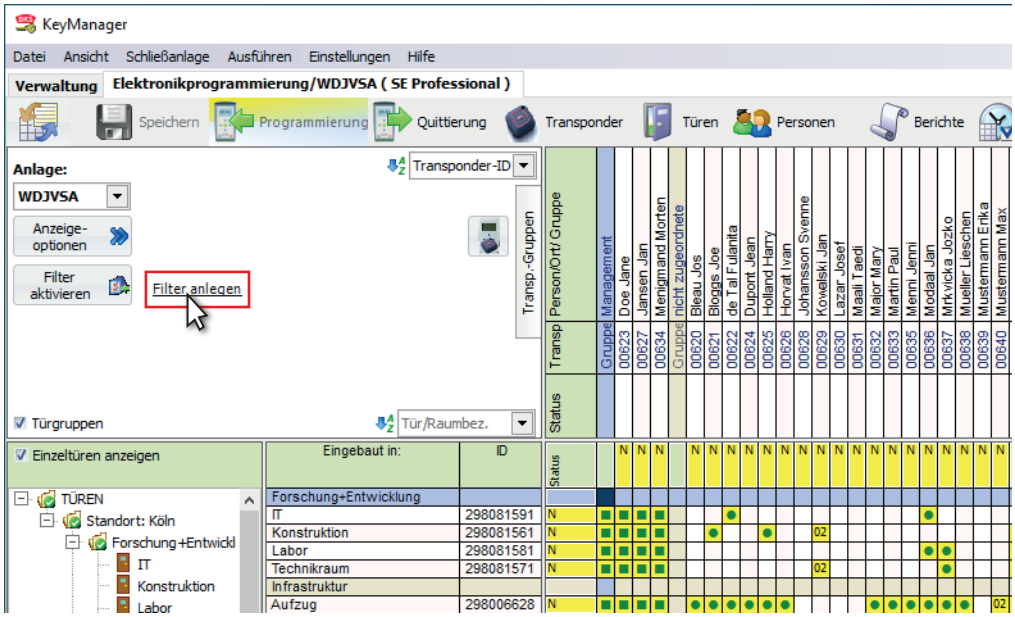
Ein weiterer Aspekt ist, dass nur die gefilterten Türen und Transponder in den BKS KeyManager geladen werden, wodurch die Menge der zu verarbeitenden Daten verkleinert wird. Je nach Reduzierung der Anzahl wird eine deutliche Steigerung der Performance erreicht. Je nach Größe der Schließanlage kann dies einen nicht zu unterschätzenden Vorteil bieten.

Die Administration der Ansicht der Matrix wird jeweils über die jeweiligen Buttons gesteuert.

3.5.3.2.1 Anlegen des Filters

Grundlage der Filterung ist die Festlegung der Filterkriterien. Legen Sie fest welche Tür- und/oder Transpondergruppen bei aktivem Filter angezeigt werden sollen.

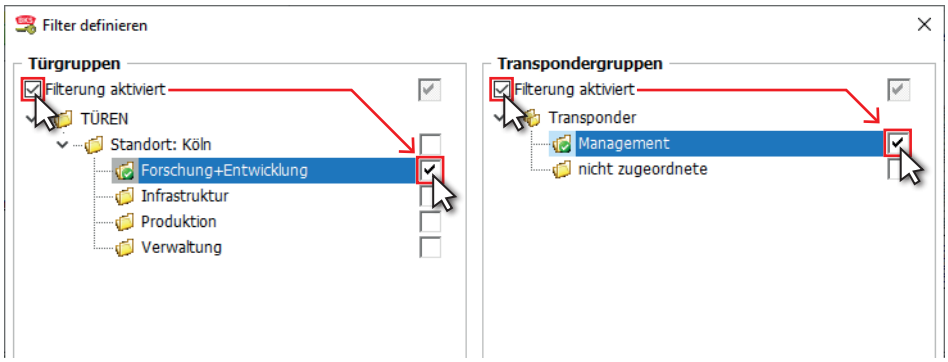
- Drücken Sie auf den Button „Filter anlegen“.



Im Weiteren erfolgt die Auswahl und Selektion der einzelnen Türen und/oder Transponder durch Aktivierung der Checkboxen.

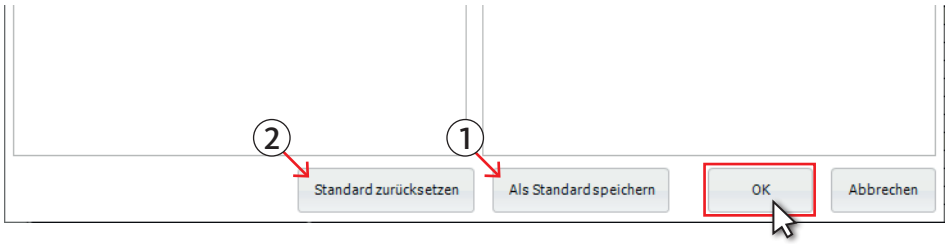
- Aktivieren Sie die Checkbox zur Filterung nach Türgruppen und/oder nach Transpondergruppen.
- Selektieren Sie zur Gruppe die einzelnen Türen und/oder Transponder, auf welche die Ansicht nach Aktivierung des Filters reduziert werden soll durch Aktivierung der jeweiligen Checkboxen.

Die Auswahl ist in einer der Gruppen oder in beiden möglich.



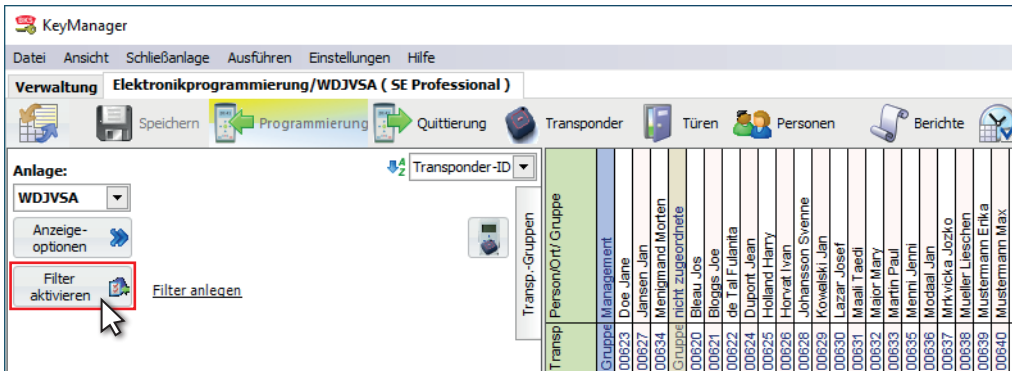
Die aktuell gewählten Einstellungen des Filters werden mit dem Button (1) „Als Standard speichern“ gesichert. Diese Einstellungen können mit dem Button (2) „Standard zurücksetzen“ nach einer Änderung der Filtereinstellungen wieder auf die abgespeicherten Filtereinstellungen gesetzt werden.

- Drücken Sie auf den Button „OK“ um den Filter anzulegen.



3.5.3.2.2 Aktivierung des Filters

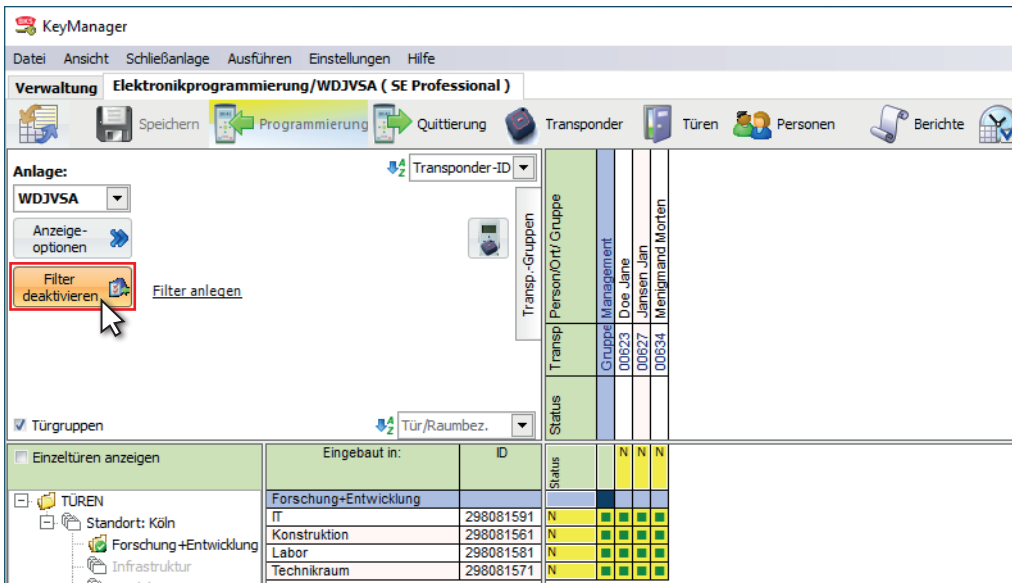
- Drücken Sie auf den Button „Filter aktivieren“, um die Ansicht nach den Filtereinstellungen zu aktualisieren.



3.5.3.2.3 Deaktivierung des Filters

- Drücken Sie auf den Button „Filter deaktivieren“, um die Filterung aufzuheben.

Dadurch werden alle Transponder- und Türgruppen wieder sichtbar, aber auch in die Matrix geladen, die wie z. B. in der Abbildung unten nicht angezeigt werden.



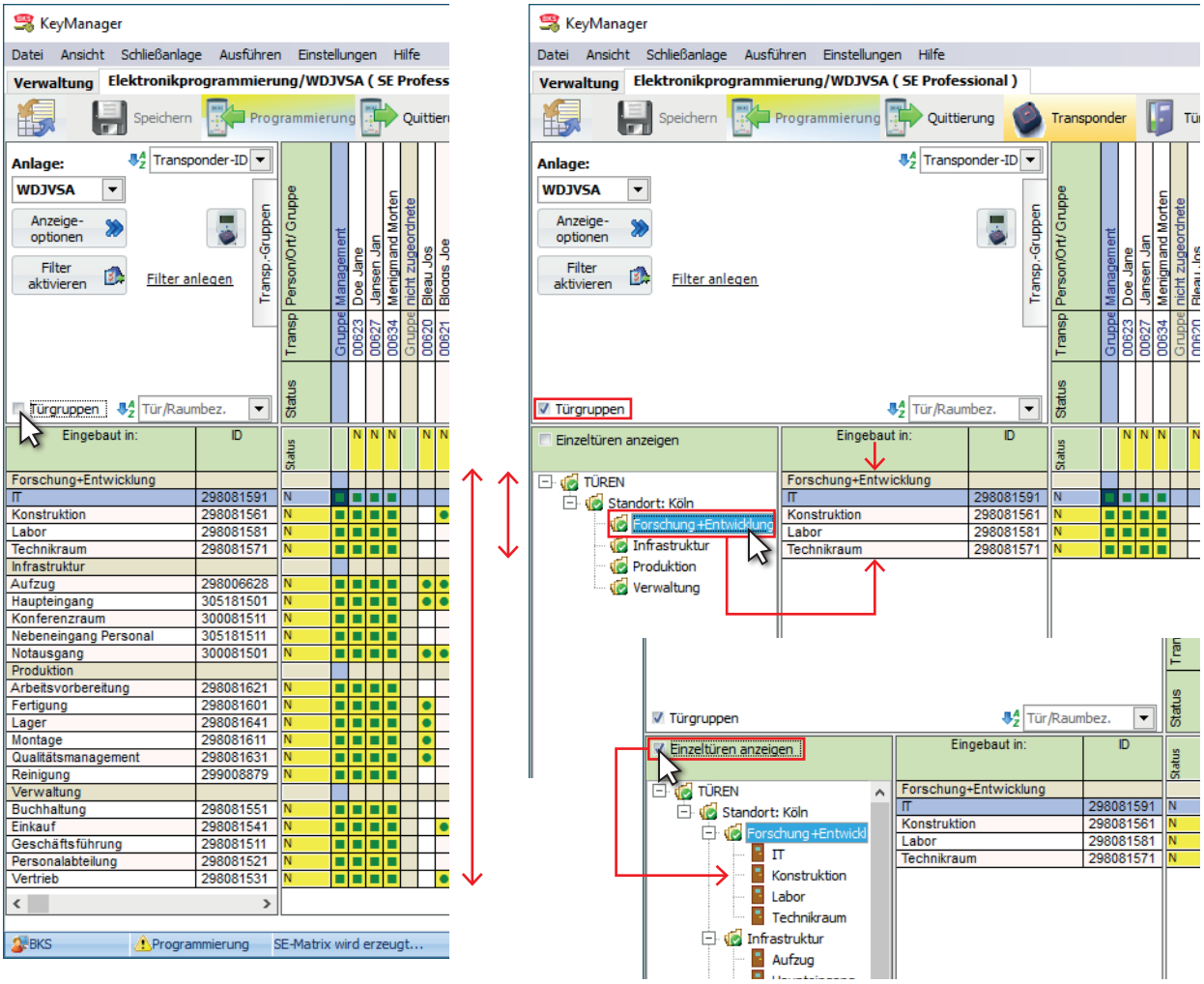
3.5.3.3 Filterung der Türgruppen

Die Türgruppenfilterung dient alleine der Einschränkung der Matrixansicht auf die von Ihnen gewählte Türgruppe und der Anzeige der dazugehörigen Türen. Die nicht ausgewählten Gruppen werden ausgeblendet. Der Filter ist ein Hilfsmittel zur Übersichtlichkeit und so wird auch nicht die zu verarbeitende Datenmenge reduziert.

- Aktivieren Sie die Checkbox „Türen“ zur Anzeige des Verzeichnisbaums.
- Wählen Sie im Verzeichnisbaum die Türgruppe aus, von der die Türen in der Matrix angezeigt werden sollen. Hierbei sind auch die Türen der Untergruppen der Auswahl eingeschlossen und werden angezeigt.
- Durch das Auswählen der obersten Gruppe im Verzeichnisbaum werden alle Türen angezeigt.

Wird die Checkbox „Einzeltüren anzeigen“ aktiviert, werden im Verzeichnisbaum unter den Türgruppen alle diesen zugehörigen Türen angezeigt.

Türgruppen und Türen, die durch setzen des Filters zur Administration und Reduzierung der Matrix ausgeblendet worden sind und dadurch auch nicht in die Matrix geladen wurden, werden ausgegraut angezeigt und können nicht ausgewählt werden.

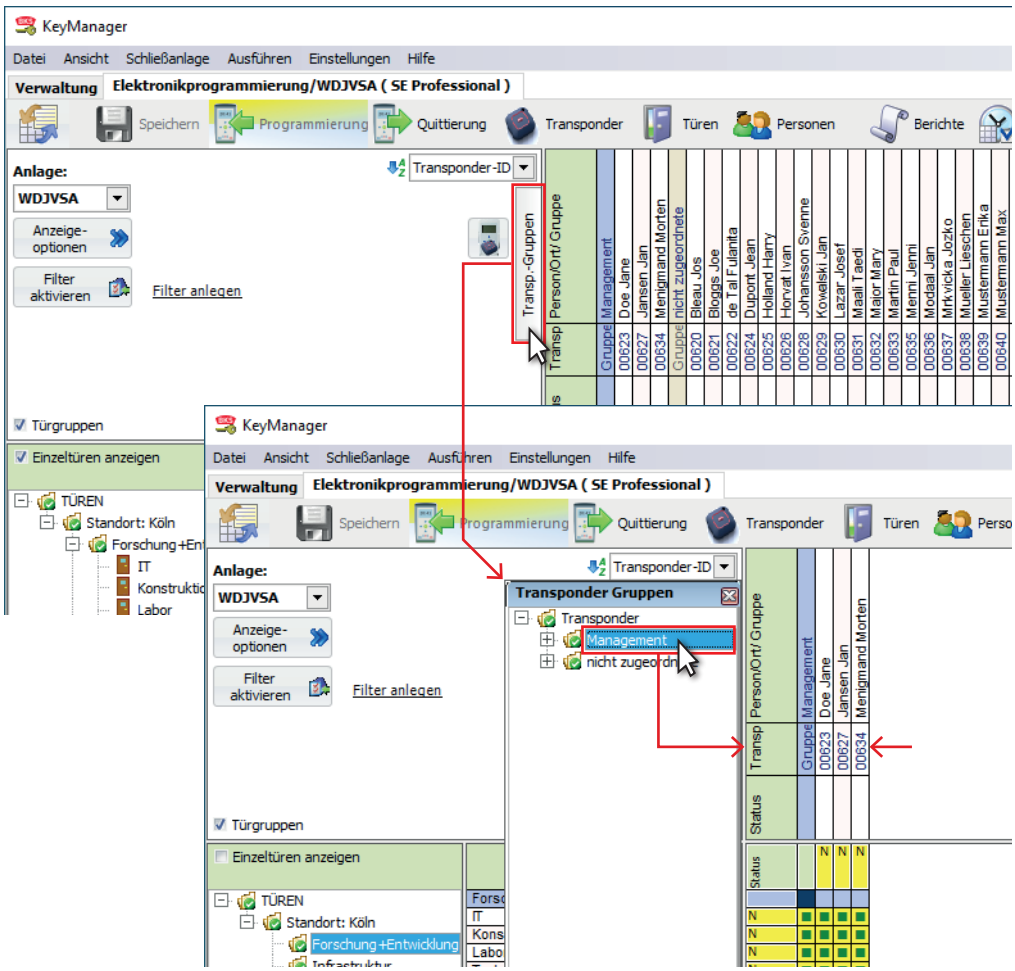


3.5.3.4 Filterung der Transpondergruppen

Die Transpondergruppenfilterung dient alleine der Einschränkung der Matrixansicht auf die von Ihnen gewählten Transpondergruppen und der Anzeige der dazugehörigen Transponder. Die nicht ausgewählten Gruppen werden ausgeblendet. Der Filter ist ein Hilfsmittel zur Übersichtlichkeit und so wird auch nicht die zu verarbeitende Datenmenge reduziert.

- Drücken Sie auf den Button „Transp.-Gruppen“ zum Öffnen des Fensters mit dem Verzeichnisbaum der Transpondergruppen.
- Wählen Sie im Verzeichnisbaum die Transpondergruppe(n) aus, von der/denen die Transponder in der Matrix angezeigt werden sollen. Hierbei sind auch die Transponder der Untergruppen der Auswahl eingeschlossen und werden angezeigt.
- Durch das Auswählen der obersten Gruppe im Verzeichnisbaum werden alle Transponder angezeigt.

Transpondergruppen und Transponder, die durch setzen des Filters zur Administration und Reduzierung der Matrix ausgeblendet worden sind und dadurch auch nicht in die Matrix geladen wurden, werden ausgegraut angezeigt und können nicht ausgewählt werden.



3.5.3.5 Konfiguration der angezeigten Spalten und Zeilen in der Matrix

- Drücken Sie mit der rechten Maustaste auf eine Tür oder einen Transponder und wählen im Kontextmenü den Menüpunkt „Spaltenkonfiguration“ aus.

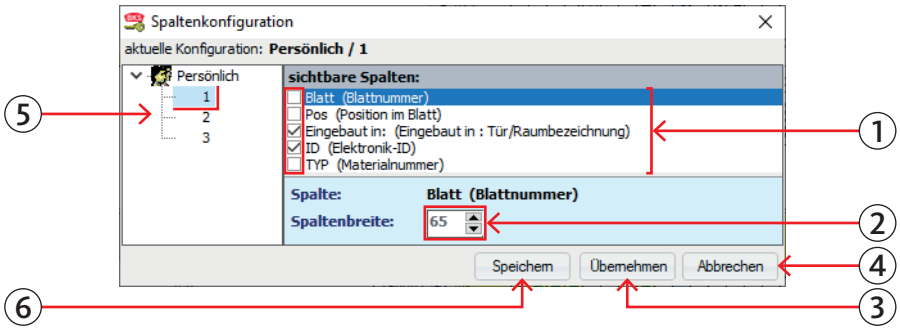
Mit der Spaltenkonfiguration kann festgelegt werden, welche Informationen zur Tür in der Kopfspalte und zu den Transpondern im Tabellenkopf der Berechtigungsmatrix angezeigt werden.

- Zum Ein- oder Ausblenden der „sichtbaren Spalten“ (1), die in der Matrix angezeigt werden sollen, aktivieren oder deaktivieren Sie die gewünschte Checkbox. Gewünschte oder nicht gewünschte Spalten werden durch setzen oder entfernen, der Haken angezeigt bzw. nicht mehr zur Anzeige gebracht.
- Die Spaltenbreite (2) kann über die Pfeiltasten für die jeweils bei „sichtbare Spalten“ (1) ausgewählte, blau unterlegt Spalte verändert werden.
- Drücken Sie auf „Übernehmen“ (3) zum Anwenden der Einstellungen auf die Matrix und zum Schließen des Fensters. Zum Beenden ohne Änderung drücken Sie auf „Abbrechen“ (4).

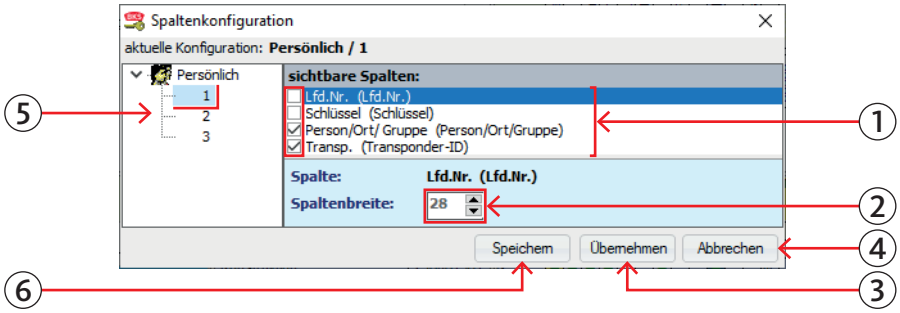
Die Spaltenkonfiguration kann in eine der drei Voreinstellungen/Profile gespeichert werden, um die Einstellung bei späterer Verwendung einfach aufrufen zu können.
Die gespeicherte Spaltenkonfiguration wird durch Auswahl eines Konfigurationsprofiles (5) aufgerufen und durch drücken auf „Übernehmen“ (3) in der Matrix angewendet.

- Zum Anlegen eines Profils wählen Sie das zu editierende Konfigurationsprofil (1 bis 3) aus.
- Markieren Sie die sichtbaren Spalten (1) und stellen die Spaltenbreite (2) ein.
- Sichern Sie das Profil mit „Speichern“ (6) und beenden den Dialog mit „Übernehmen“ (3).

Spalten für Türen bzw. Zutrittspunkte

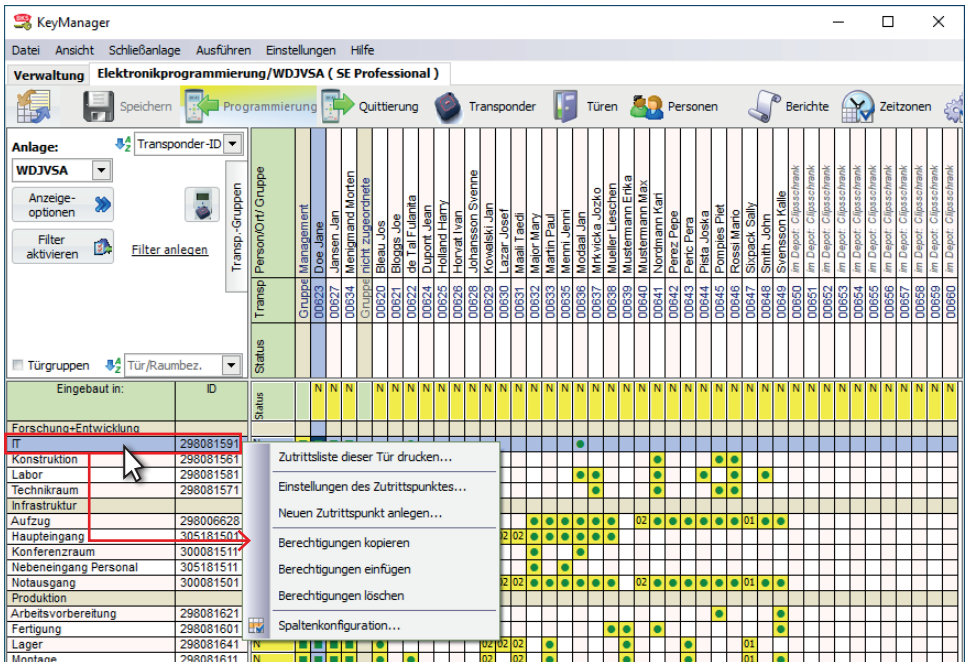


Spalten für Transponder bzw. Personen



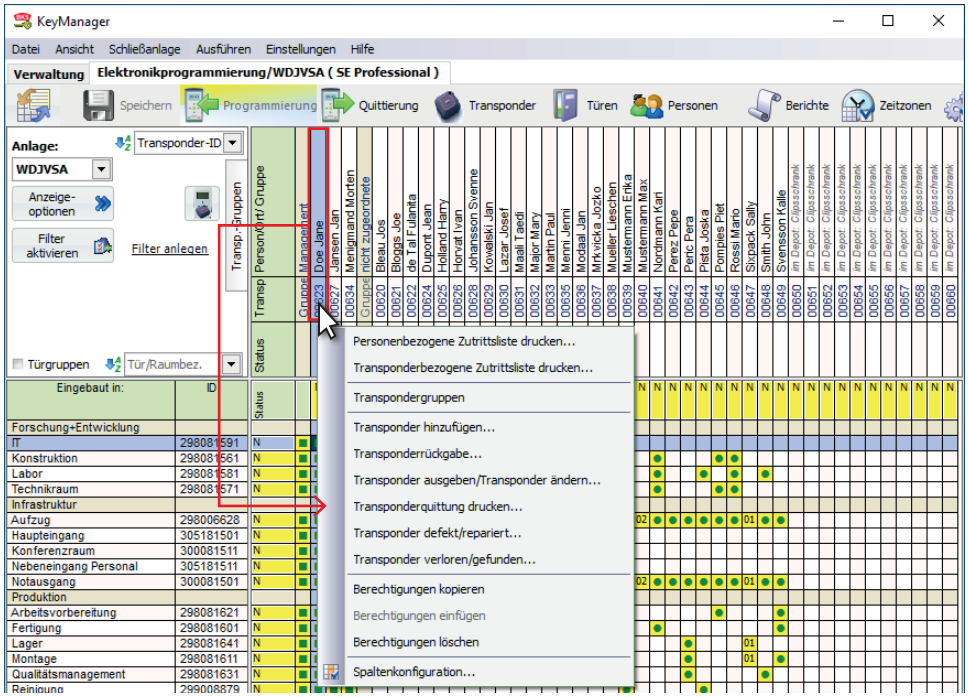
3.5.4 Kontextmenüs

- Drücken Sie mit der rechten Maustaste auf einen Zutrittspunkt in der Berechtigungsmatrix und öffnen das Kontextmenü. Wählen Sie eine der folgenden Funktion im Menü aus.



Auswahl	Beschreibung (→ im Kapitel [Seite])
Zutrittsliste dieser Tür drucken ...	Druckansicht mit allen zutrittsberechtigten Transpondern bzw. Personen zum gewählten Zutrittspunkt erstellen. Weitere Anpassungsoptionen durch die Dropdown-Menüs.
Einstellungen des Zutrittspunktes ...	Konfiguration des gewählten Zutrittspunkts (→ 4.3.2 [208]).
Neuen Zutrittspunkt anlegen ...	Anlegen eines neuen Zutrittspunkts (→ 4.3.1 [202])
Berechtigungen kopieren	Zutrittsberechtigungen des markierten Zutrittspunkts in die Zwischenablage kopieren.
Berechtigungen einfügen	Einfügen der zuvor kopierten Berechtigungen aus der Zwischenablage in den markierten Zutrittspunkt und löschen der ggf. vorhandenen Berechtigungen.
Berechtigungen löschen	Löschen der bestehenden Zutrittsberechtigungen im markierten Zutrittspunkt.
Spaltenkonfiguration ...	Eigenschaften der Anzeige der Türen in der Berechtigungsmatrix konfigurieren (→ 3.5.3.5 [87]).

■ Drücken Sie mit der rechten Maustaste auf einen Transponder in der Berechtigungsmatrix und öffnen das Kontextmenü. Wählen Sie eine der folgenden Funktion im Menü aus.

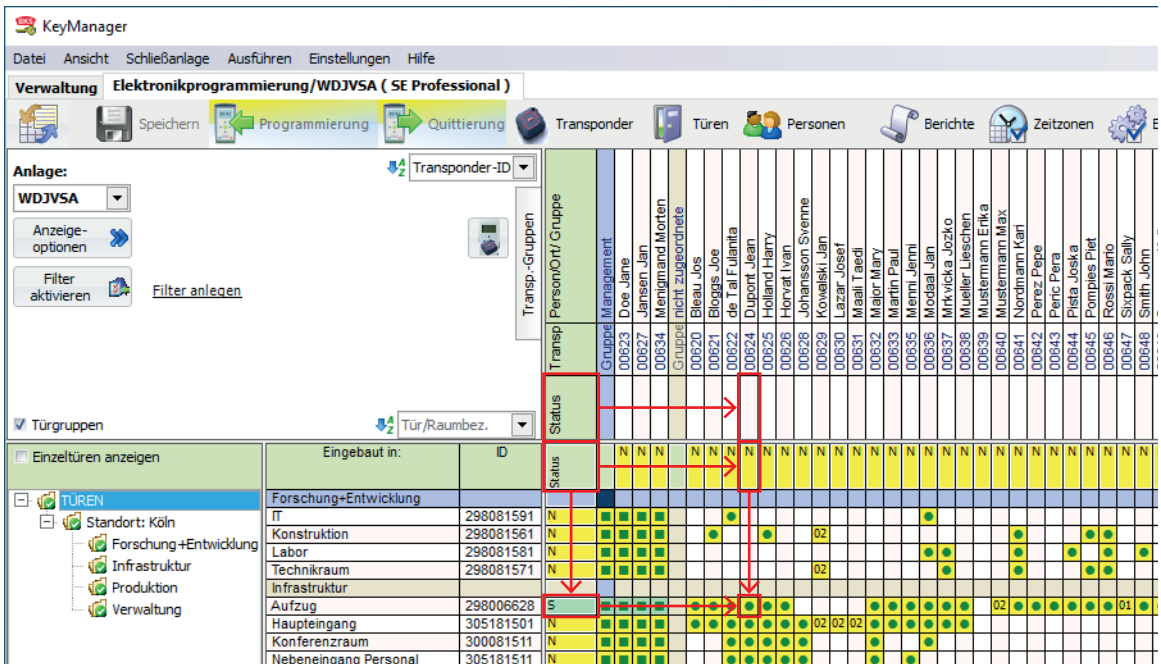


Auswahl	Beschreibung (→ im Kapitel [Seite])
Personenbezogene Zutrittsliste drucken ...	Druckansicht mit allen Türen, an denen die gewählte Person zutrittsberechtigt ist.
Transponderbezogene Zutrittsliste drucken ...	Druckansicht mit allen Türen, an denen der gewählte Transponder zutrittsberechtigt ist, erstellen. Weitere Anpassungsoptionen durch die Dropdown-Menüs.
Transponder-Gruppen	Anlegen und Bearbeiten einer Transpondergruppe (→ 4.2.7 [186]).
Transponder hinzufügen ...	Anlegen eines neuen Transponders (→ 4.2.1 [161]).
Transponder Ausgabe ...	Transponder an eine Person ausgeben (→ 4.2.2 [164]).
Transponder Rückgabe ...	Transponder von Person zurücknehmen (→ 4.2.3 [175]).
Transponder defekt/repariert ...	Transponder als defekt/repariert melden (→ 4.2.5 [181]).
Transponder verloren/gefunden ...	Transponder als verloren/gefunden melden (→ 4.2.4 [177]).
Berechtigungen kopieren	Zutrittsberechtigungen des markierten Transponders in die Zwischenablage kopieren.
Berechtigungen einfügen	Einfügen der zuvor kopierten Berechtigungen aus der Zwischenablage in den markierten Transponder und löschen der ggf. vorhandenen Berechtigungen.
Berechtigungen löschen	Löscht alle Zutrittsberechtigungen des markierten Transponder
Spaltenkonfiguration ...	Eigenschaften der Anzeige der Transponder in der Berechtigungsmatrix konfigurieren (→ 3.5.3.5 [87]).

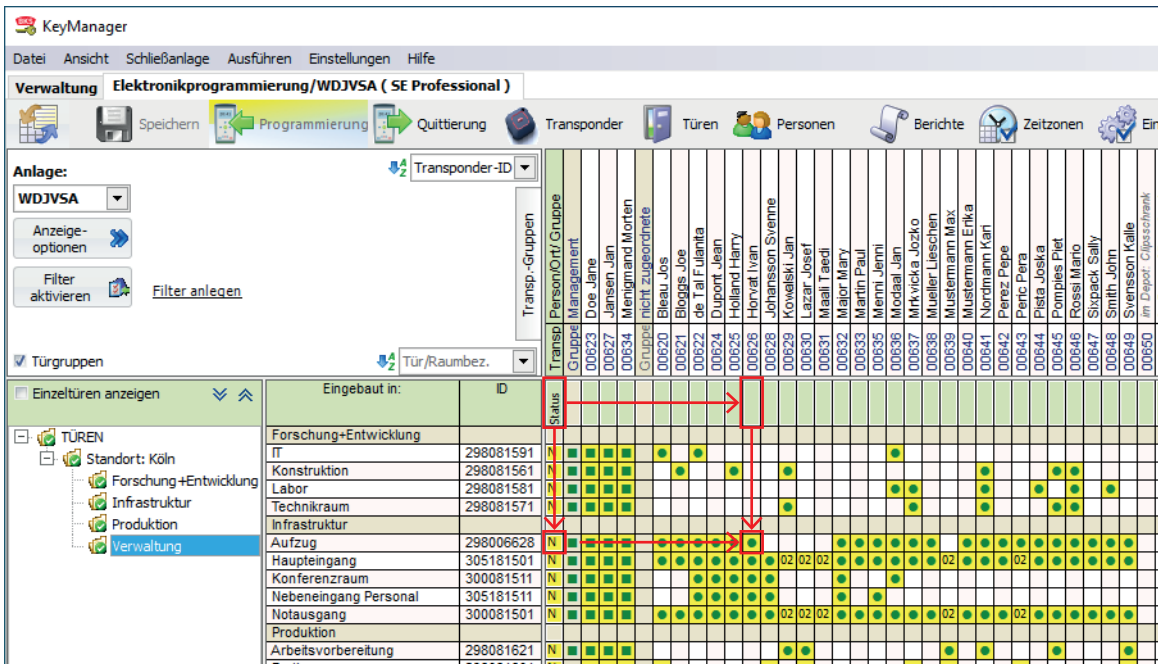
3.5.5 Statusanzeigen der Berechtigungsmatrix

Der Staus der Türen und Transponder wird in der Berechtigungsmatrix durch unterschiedliche Symbole in Spalte und Zeile sowie in deren Schnittpunkt dargestellt.

DoT-Anlage



nonDoT-Anlage



Neben den Berechtigungen wird in der Berechtigungsmatrix der Programmierbedarf der Transponder und Türen im Feld „Status“ angezeigt, der durch Änderungen in der Matrix entsteht.

3.5.5.1 Status der Berechtigung (DoT)

Symbolik	Beschreibung	Anlage
Status	**Keine Berechtigung** eines **einzelnen Transponders** zur Tür (Berechtigung wurde entfernt) →Speichern nötig und Programmierung des Transponders erforderlich	DoT
Status	**Keine Berechtigung** eines **einzelnen Transponders** zur Tür →Quittierung ist erfolgt	DoT
Status	**Keine Berechtigung** einer **Transpondergruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder (Berechtigung wurde entfernt) →Speichern nötig und Programmierung der Tür erforderlich	DoT
Status	**Keine Berechtigung** einer **Transpondergruppe** zur Tür, →Übertragung zur Tür und Quittierung notwendig	DoT
Status	**Keine Berechtigung** einer **Transpondergruppe** zur Tür, →Quittierung ist erfolgt	DoT
Im Weiteren keine Statussymbole für Batterieanzeige; Info Batteriesymbole am Tabellenende		
Status	Zuweisung der **Berechtigung** für eine **Transpondergruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder →Speichern nötig und Programmierung der Tür erforderlich	DoT
Status	**Berechtigung** einer **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT
Status	**Berechtigung** einer **Transpondergruppe** zur Tür →Quittierung ist erfolgt	DoT
Status	**Berechtigung** der **Transponder** durch die **Transpondergruppe** zur Tür →Speichern nötig und Programmierung der Tür erforderlich	DoT
Status	**Berechtigung** der **Transponder** durch die **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT
Status	**Berechtigung** der **Transponder** durch die **Transpondergruppe** zur Tür →Quittierung ist erfolgt	DoT

Symbolik	Beschreibung	Anlage
Status / N / ●	Zuweisung einer **Berechtigung** eines **einzelnen Transponders** zur Tür →Speichern nötig und Programmierung des Transponders erforderlich	DoT
Status / ●	**Berechtigung** eines **einzelnen Transponders** zur Tür →Quittierung ist erfolgt	DoT
Status / Gruppe / N / 01	Zuweisung der **Berechtigung** durch eine **Zeitzone** für eine **Transponder-gruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder (Nummerierung der Zeitzonen 01, 02, 03 etc.) →Speichern nötig und Programmierung der Tür erforderlich	DoT
Status / S / 01	**Berechtigung** durch eine **Zeitzone** für eine **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT
Status / 01	**Berechtigung** durch eine **Zeitzone** für eine **Transpondergruppe** zur Tür →Quittierung ist erfolgt	DoT
Status / N / 01	**Berechtigung** der **Transponder** durch eine **Zeitzone** der **Transponder-gruppe** zur Tür (Nummerierung der Zeitzonen 01, 02, 03 etc.) →Speichern nötig und Programmierung der Tür erforderlich	DoT
Status / S / 01	**Berechtigung** der **Transponder** durch eine **Zeitzone** der **Transponder-gruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT
Status / 01	**Berechtigung** der **Transponder** durch eine **Zeitzone** der **Transponder-gruppe** zur Tür →Quittierung ist erfolgt	DoT
Status / N / 01	Zuweisung der **Berechtigung** durch eine **Zeitzone** für einen **einzelnen Transponder** zur Tür (Nummerierung der Zeitzonen 01, 02, 03 etc.) →Speichern nötig und Programmierung des Transponders erforderlich	DoT
Status / 01	**Berechtigung** durch eine **Zeitzone** für einen **einzelnen Transponder** zur Tür →Quittierung ist erfolgt	DoT
Status / Gruppe / N / T	Zuweisung der **Berechtigung** durch eine **Tagesfreigabe** für eine **Trans-pondergruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder →Speichern nötig und Programmierung der Tür erforderlich	DoT
Status / S / T	**Berechtigung** durch eine **Tagesfreigabe** für eine **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT
Status / T	**Berechtigung** durch eine **Tagesfreigabe** für eine **Transpondergruppe** zur Tür →Quittierung ist erfolgt	DoT

Symbolik	Beschreibung	Anlage
Status N T	**Tagesfreigabe** der **Transponder** durch die **Berechtigung** der **Transpondergruppe** zur Tür →Speichern nötig und Programmierung der Tür erforderlich	DoT
Status S T	**Tagesfreigabe** der **Transponder** durch die **Berechtigung** der **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT
Status T	**Tagesfreigabe** der **Transponder** durch die **Berechtigung** der **Transpondergruppe** zur Tür →Quittierung ist erfolgt	DoT
Status N T	Zuweisung der **Berechtigung** durch eine **Tagesfreigabe** für einen **einzelnen Transponder** zur Tür →Speichern nötig und Programmierung des Transponders ist erforderlich	DoT
Status T	**Berechtigung** durch eine **Tagesfreigabe** für einen **einzelnen Transponder** zur Tür →Quittierung ist erfolgt	DoT
Status N	**Sperren** eines **einzelnen Transponders** oder einer Transpondergruppe und Entzug der Berechtigung zur Tür →Speichern nötig und Programmierung der Tür ist erforderlich	DoT
Status S	**Sperren** eines **einzelnen Transponders** oder einer Transpondergruppe und Entzug der Berechtigung zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT
Status	**Sperren** eines **einzelnen Transponders** oder einer Transpondergruppe und Entzug der Berechtigung zur Tür →Quittierung ist erfolgt	DoT
Status N	**Änderung** im Menü Transponder **ohne Einfluss auf die Tür** z. B. Änderung der Daten wie Gültigkeitszeitraum festlegen etc.; Status Tür und Berechtigung sind quittiert (z. B. keine Berechtigung) →Programmierung des Transponders ist erforderlich	DoT
Status N	**Änderung** im Menü Türen **ohne Einfluss auf den Transponder** z. B. Änderung Daten der Tür, Modus der Tagesfreigabe ändern etc.; Status Transponder und Berechtigung sind quittiert (keine Berechtigung) →Programmierung der Tür ist erforderlich	DoT

Symbolik	Beschreibung	Anlage
Status / N / Gruppe	**Aktivierte** Einstellung „**Transpondergruppenrecht im Zutrittspunkt** speichern“ (Anlagen-Einstellungen/Für Anlage); Zuweisung einer **Berechtigung** der **Transpondergruppe** zur Tür →Programmierung der Tür ist erforderlich	DoT
Status / S	**Aktivierte** Einstellung „**Transpondergruppenrecht im Zutrittspunkt** speichern“; **Berechtigung** der **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT
Status	**Aktivierte** Einstellung „**Transpondergruppenrecht im Zutrittspunkt** speichern“; **Berechtigung** der **Transpondergruppe** zur Tür →Quittierung ist erfolgt	DoT
Status / N / Gruppe	**Deaktivierte** Einstellung „**Transpondergruppenrecht im Zutrittspunkt** speichern“; **Berechtigung** der **Transpondergruppe** zur Tür →Programmierung ist erforderlich	DoT
Status / S	**Deaktivierte** Einstellung „**Transpondergruppenrecht im Zutrittspunkt** speichern“ (Anlagen-Einstellungen/Für Anlage); Zuweisung einer **Berechtigung** der **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT
Status	**Deaktivierte** Einstellung „**Transpondergruppenrecht im Zutrittspunkt** speichern“; **Berechtigung** der **Transpondergruppe** zur Tür →Quittierung ist erfolgt	DoT

3.5.5.2 Status von Ereignissen (DoT)

Symbolik		Beschreibung	Anlage
Status	Verloren	Im Transpondermenü wurde der **Transponder** als **Verloren** gemeldet und im weiteren Dialog **gesperrt** (Berechtigungen); nur bei aktiver Checkbox, siehe Kapitel 5.1.2.4 [266]	DoT
N		Programmierung erforderlich	
S		Übertragung zur Tür und Quittierung notwendig	
		Quittierung ist erfolgt	
Status	Verloren	Im Transpondermenü wurde der **Transponder** als **Verloren*** gemeldet und im weiteren Dialog **nicht gesperrt** (unveränderte Berechtigungen); nur bei aktiver Checkbox, siehe Kapitel 5.1.2.4 [266]	DoT
N		Programmierung erforderlich	
S		Übertragung zur Tür und Quittierung notwendig	
		Quittierung ist erfolgt	
Status	Defekt	Im Transpondermenü wurde der **Transponder** als **Defekt** gemeldet und im weiteren Dialog **gesperrt** (Berechtigungen); nur bei aktiver Checkbox, siehe Kapitel 5.1.2.4 [266]	DoT
N		Programmierung erforderlich	
S		Übertragung zur Tür und Quittierung notwendig	
		Quittierung ist erfolgt	
Status	Defekt	Im Transpondermenü wurde der **Transponder** als **Defekt*** gemeldet und im weiteren Dialog **nicht gesperrt** (unveränderte Berechtigungen); nur bei aktiver Checkbox, siehe Kapitel 5.1.2.4 [266]	DoT
N		Programmierung erforderlich	
S		Übertragung zur Tür und Quittierung notwendig	
		Quittierung ist erfolgt	
Status	Ersetzt	Dieser Transponder ist durch die Funktion „**Ersetzt**“ z. B. beim Verlust des Transponders im Transpondermenü von einem anderen Transponder ersetzt worden, siehe Kapitel 5.1.2.4 [266] im Menüpunkt (g), Programmierung der Tür erforderlich bei Sperrung des Transponders	DoT
Status	N		
N	?		
Status	Ersetzt	Dieser Transponder ist durch die Funktion „Ersetzt“ von einem anderen Transponder ersetzt worden, Übertragung der Sperre zur Tür und Quittierung notwendig	DoT
Status	N		
S	?		

Symbolik		Beschreibung	Anlage
Status	Zeitraum	Im Transpondermenü ist ein **Zeitraum** für den Transponder gesetzt; durch Aktivierung der Checkbox (i) „ein“ bei „Begrenzter Gültigkeit“, siehe Kapitel 4.2.2 [164], wird nach Eingabe eines Zeitpunkts in den Feldern (d) „Transp. gültig von“ und/oder „Transp. gültig bis“ ein Zeitraum gesetzt nach dessen Ablauf der Transponder seine Berechtigung verliert	DoT
Status	E	Störung oder Abbruch der Verbindung z. B. zum Programmiergerät oder online angebunden Komponente bei der Übertragung von Daten zur Programmierung des Transponders →Übertragungsfehler	DoT
Status E		Störung oder Abbruch der Verbindung z. B. zum Programmiergerät oder online angebunden Komponente bei der Übertragung von Daten zur Programmierung der Tür →Übertragungsfehler	DoT

* Bei Transponder, die mit Defekt oder Verloren gekennzeichnet sind und die Berechtigungen zu den Türen nicht gesperrt wurde, werden die Symbole für den Status der Zeitzonen und Tagesfreigaben zur Tür in **Grau** angezeigt.

3.5.5.3 Status der Berechtigung (nonDoT)

Symbolik	Beschreibung	Anlage
Status N	**Keine Berechtigung** eines **einzelnen Transponders** zur Tür (Berechtigung wurde entfernt) →Speichern nötig und Programmierung erforderlich	nonDoT
Status S	**Keine Berechtigung** eines **einzelnen Transponders** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status	**Keine Berechtigung** eines **einzelnen Transponders** zur Tür →Quittierung ist erfolgt	nonDoT
Gruppe Status N	**Keine Berechtigung** einer **Transpondergruppe** zur Tür (Berechtigung wurde entfernt) →Speichern nötig und Programmierung der Tür erforderlich	nonDoT
Status S	**Keine Berechtigung** einer **Transpondergruppe** zur Tür, →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status	**Keine Berechtigung** einer **Transpondergruppe** zur Tür, →Quittierung ist erfolgt	nonDoT
Gruppe Status N	Zuweisung der **Berechtigung** für eine **Transpondergruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder →Speichern nötig und Programmierung der Tür erforderlich	nonDoT
Status S	**Berechtigung** einer **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status	**Berechtigung** einer **Transpondergruppe** zur Tür →Quittierung ist erfolgt	nonDoT
Status N	**Berechtigung** der **Transponder** durch die **Transpondergruppe** zur Tür →Speichern nötig und Programmierung der Tür erforderlich	nonDoT
Status S	**Berechtigung** der **Transponder** durch die **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status	**Berechtigung** der **Transponder** durch die **Transpondergruppe** zur Tür →Quittierung ist erfolgt	nonDoT
Status N	Zuweisung einer **Berechtigung** eines **einzelnen Transponders** zur Tür →Speichern nötig und Programmierung der Tür erforderlich	nonDoT
Status S	**Berechtigung** eines **einzelnen Transponders** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status	**Berechtigung** eines **einzelnen Transponders** zur Tür →Quittierung ist erfolgt	nonDoT

Symbolik	Beschreibung	Anlage
Status N Gruppe 01	Zuweisung der **Berechtigung** durch eine **Zeitzone** für eine **Transponder-gruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder (Nummerierung der Zeitzonen 01, 02, 03 etc.) →Speichern nötig und Programmierung der Tür erforderlich	nonDoT
Status S 01	**Berechtigung** durch eine **Zeitzone** für eine **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status 01	**Berechtigung** durch eine **Zeitzone** für eine **Transpondergruppe** zur Tür →Quittierung ist erfolgt	nonDoT
Status N 01	**Berechtigung** der **Transponder** durch eine **Zeitzone** der **Transponder-gruppe** zur Tür (Nummerierung der Zeitzonen 01, 02, 03 etc.) →Speichern nötig und Programmierung der Tür erforderlich	nonDoT
Status S 01	**Berechtigung** der **Transponder** durch eine **Zeitzone** der **Transponder-gruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status 01	**Berechtigung** der **Transponder** durch eine **Zeitzone** der **Transponder-gruppe** zur Tür →Quittierung ist erfolgt	nonDoT
Status N 01	Zuweisung der **Berechtigung** durch eine **Zeitzone** für einen **einzelnen Transponder** zur Tür (Nummerierung der Zeitzonen 01, 02, 03 etc.) →Speichern nötig und Programmierung der Tür erforderlich	nonDoT
Status S 01	**Berechtigung** durch eine **Zeitzone** für einen **einzelnen Transponder** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status 01	**Berechtigung** durch eine **Zeitzone** für einen **einzelnen Transponder** zur Tür →Quittierung ist erfolgt	nonDoT
Status N Gruppe T	Zuweisung der **Berechtigung** durch eine **Tagesfreigabe** für eine **Trans-pondergruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder →Speichern nötig und Programmierung der Tür erforderlich	nonDoT
Status S T	**Berechtigung** durch eine **Tagesfreigabe** für eine **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status T	**Berechtigung** durch eine **Tagesfreigabe** für eine **Transpondergruppe** zur Tür →Quittierung ist erfolgt	nonDoT

Symbolik	Beschreibung	Anlage
Status N T	**Berechtigung** der **Transponder** durch eine **Tagesfreigabe** der **Transpondergruppe** zur Tür →Speichern nötig und Programmierung der Tür erforderlich	nonDoT
Status S T	**Berechtigung** der **Transponder** durch eine **Tagesfreigabe** der **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status T	**Berechtigung** der **Transponder** durch eine **Tagesfreigabe** der **Transpondergruppe** zur Tür →Quittierung ist erfolgt	nonDoT
Status N T	Zuweisung der **Berechtigung** durch eine **Tagesfreigabe** für einen **einzelnen Transponder** zur Tür →Speichern nötig und Programmierung der Tür ist erforderlich	nonDoT
Status S T	**Berechtigung** durch eine **Tagesfreigabe** für einen **einzelnen Transponder** zur Tür →Übertragung zur Tür und Quittierung notwendig	nonDoT
Status T	**Berechtigung** durch eine **Tagesfreigabe** für einen **einzelnen Transponder** zur Tür →Quittierung ist erfolgt	nonDoT

3.5.5.4 Status von Ereignissen (nonDoT)

Symbolik		Beschreibung	Anlage
Status	Verloren	Im Transpondermenü ist der **Transponder** als **Verloren** gemeldet und ist im weiteren Dialog **gesperrt** (Berechtigung); nur bei aktiver Checkbox, siehe Kapitel 5.1.2.4 [266]	nonDoT
N		Programmierung erforderlich	
S		Übertragung zur Tür und Quittierung notwendig	
		Quittierung ist erfolgt	
Status	Verloren	Im Transpondermenü wurde der **Transponder** als **Verloren*** gemeldet und im weiteren Dialog **nicht gesperrt**, unveränderte Berechtigung; nur bei aktiver Checkbox, siehe Kapitel 5.1.2.4 [266]	nonDoT
N		Programmierung erforderlich	
S		Übertragung zur Tür und Quittierung notwendig	
		Quittierung ist erfolgt	
Status	Defekt	Im Transpondermenü wurde der **Transponder** als **Defekt** gemeldet und im weiteren Dialog **gesperrt** (Berechtigung); nur bei aktiver Checkbox, siehe Kapitel 5.1.2.4 [266]	nonDoT
N		Programmierung erforderlich	
S		Übertragung zur Tür und Quittierung notwendig	
		Quittierung ist erfolgt	
Status	Defekt	Im Transpondermenü wurde der **Transponder** als **Defekt** gemeldet und im weiteren Dialog **nicht gesperrt**, Berechtigung bleibt unverändert; nur bei aktiver Checkbox, siehe Kapitel 5.1.2.4 [266]	nonDoT
N		Programmierung erforderlich	
S		Übertragung zur Tür und Quittierung notwendig	
		Quittierung ist erfolgt	
Status	E	Störung oder Abbruch der Verbindung zum Programmiergerät bei der Übertragung von Daten zur Programmierung des (Feuerwehr-)Transponders →Übertragungsfehler	nonDoT
Status E		Störung oder Abbruch der Verbindung z. B. zum Programmiergerät oder online angebunden Komponente bei der Übertragung von Daten zur Programmierung der Tür →Übertragungsfehler	nonDoT

* Bei Transpondern, die mit Defekt oder Verloren gekennzeichnet sind und die Berechtigungen zu den Türen nicht gesperrt wurden, werden die Symbole für den Status der Zeitzonen und Tagesfreigaben zur Tür in **Grau** angezeigt.

3.5.5.5 Ereignissen ohne Anzeige in der Berechtigungsmatrix

Im BKS KeyManager kann durch die Anlagen-Einstellung die Ansicht der Berechtigungsmatrix so konfiguriert werden, dass defekte oder verlorene Transponder nicht in der Matrix angezeigt werden. Die Anzeige dieser Meldungen in der Berechtigungsmatrix wird durch Aktivierung bzw. Deaktivierung der Checkboxen der Anzeigeoptionen gesteuert, siehe Kapitel 5.1.2 [264].

Status	Beschreibung
Verloren	Nach der Markierung als „Verlorener Transponder“ werden bei aktivierter Checkbox die Transponder nicht mehr in der Berechtigungsmatrix angezeigt. Während der Markierung des Transponders als verloren sollte dieser direkt mit der Auswahl „Programmierung der betroffenen Zutrittspunkte“ gesperrt werden, siehe Kapitel 4.2.4 [177]. Nicht gesperrte Transponder behalten die Zutrittsberechtigungen zu den Türen, obwohl sie nicht mehr in der Matrix angezeigt werden.
Defekt	Nach der Markierung als „Defekter Transponder“ werden bei aktivierter Checkbox die Transponder nicht mehr in der Berechtigungsmatrix angezeigt. Während der Markierung des Transponders als defekt sollte dieser direkt mit der Auswahl „Programmierung der betroffenen Zutrittspunkte“ gesperrt werden, siehe Kapitel 4.2.5 [181]. Nicht gesperrte Transponder behalten die Zutrittsberechtigungen zu den Türen, obwohl sie nicht mehr in der Matrix angezeigt werden. Ein Löschen des Transponders ist nur in diesem Status der Markierung möglich.

HINWEIS

Die Transponder werden nach dem Ausführen der Funktion bei deaktivierter Anzeige in das Depot verschoben und sind nicht mehr editierbar.
Möchten Sie diese Ereignisse in der Berechtigungsmatrix angezeigt bekommen, können Sie die Anzeigeoptionen für die Ereignisse Verloren und/oder Defekt ändern.

Status	Beschreibung
Gelöscht	Nach dem Löschen sind die Transponder im BKS KeyManager nicht mehr existent.

3.5.5.6 Statusmeldungen in einer DoT-Anlage mit FGT

In den Schließanlagen werden in erster Linie das Freigabeterminal 2 Professional und das Freigabeterminal Professional verwendet. Zur Vereinfachung werden diese und das Freigabeterminal, welches ausläuft, im Weiterem als FGT bezeichnet.

Symbolik	Beschreibung	Anlage
Status	**Berechtigung** (in diesem Fall „keine Berechtigung“) mit **Quittierung**, (Transpondergruppenrechte müssen mit dem Programmiergerät in die diese betreffenden Türen programmiert werden) →Berechtigung neu vergeben bzw. vorhandenes Recht ändern	DoT mit FGT
Status	Zuweisung einer **Berechtigung** eines **einzelnen Transponders** zur Tür (Berechtigung z. B. „Immer“ exemplarisch für andere Berechtigungen) →Speichern nötig und Programmierung des Transponders erforderlich →Übertragung zum FGT startet nach Speichern automatisch bzw. Übertragung ggf. im Dialog manuell starten	DoT mit FGT
Status	**Übertragung** der Daten vom BKS KeyManager zum FGT →Bis zum Ende der Übertragung abwarten	DoT mit FGT
Status	**Bereitstellung** am Freigabeterminal, Übertragung abgeschlossen →Für den betroffenen Transponder stehen die Daten am FGT zur Abholung bereit	DoT mit FGT
Status	**Programmierung** des geänderten **Transponders** durch Buchen am FGT erfolgt →Programmierung der Tür durch Transponder erforderlich	DoT mit FGT
Status	Der Transponder wurde an der Tür präsentiert und die Daten übertragen; die **Quittierung** dieses Vorgangs wird durch das erneute Buchen des Transponders am FGT zum BKS KeyManager übertragen →Quittierung ist erfolgt	DoT mit FGT
Wenn der Speicher im FGT nicht mehr ausreicht, um die Programmierinformation abzulegen, werden die Daten im Direktmodus übertragen. Dies bedeutet, dass die Programmierdaten ohne Zwischenspeicherung zum FGT übertragen werden. Die Übertragung startet in diesem Fall erst, wenn der Transponder am FGT eingebucht wird und sich in Kommunikation mit dem FGT befindet.		
Status	Nach dem Speichern und dem Start und Abbruch der Übertragung zum FGT wird der **Direktmodus** durch die Statusmeldung „D“ angezeigt. →Die Daten stehen im BKS KeyManager zur Abholung durch den Transponder am FGT bereit.	DoT mit FGT
Status	**Programmierung** des geänderten **Transponders** durch Buchen am Freigabeterminal erfolgt →Die Daten werden vom BKS KeyManager über das FGT zum Transponder übertragen. →Die erfolgreiche Übertragung wird im Status durch einen grauen Hintergrund symbolisiert.	DoT mit FGT

Symbolik	Beschreibung	Anlage
Status / N / Gruppe	Zuweisung der **Berechtigung** für eine **Transpondergruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder Keine Programmierung der Transponder und Übertragung durch FGT →Speichern nötig und Programmierung der Tür erforderlich	DoT mit FGT
Status / S	**Berechtigung** einer **Transpondergruppe** zur Tür →Übertragung zur Tür und Quittierung notwendig	DoT mit FGT
Status	**Berechtigung** einer **Transpondergruppe** zur Tür →Quittierung ist erfolgt	DoT mit FGT
N	**Erweiterung** der **Transpondergruppe** um zusätzliche Transponder, z. B. über das Menü "Transpondergruppen bearbeiten" →Speichern nötig und Programmierung des Transponders erforderlich →Übertragung zum FGT startet nach Speichern automatisch bzw. Übertragung ggf. im Dialog manuell starten	DoT mit FGT
Status / O	**Übertragung** der Daten vom BKS KeyManager zum FGT →Bis zum Ende der Übertragung abwarten	DoT mit FGT
Status / S	**Bereitstellung** am Freigabeterminal, Übertragung abgeschlossen →Für den betroffenen Transponder stehen die Daten am FGT zur Abholung bereit	DoT mit FGT
Status	**Programmierung** des geänderten **Transponders** durch Buchen am FGT erfolgt →Quittierung ist erfolgt	DoT mit FGT
Status	Der Transponder wurde an der Tür präsentiert und die Daten übertragen; die **Quittierung** dieses Vorgangs wird durch das erneute Buchen des Transponders am FGT zum BKS KeyManager übertragen →Quittierung ist erfolgt	DoT mit FGT
Status / Ersetzt / Status / N / ?	Dieser Transponder ist durch die Funktion „**Ersetzt**“ z. B. beim Verlust des Transponders im Transpondermenü von einem anderen Transponder ersetzt worden, siehe Kapitel 5.1.2.4 [266] im Menüpunkt (g), →Programmierung der Tür erforderlich bei Sperrung des Transponders	DoT
Status / Ersetzt / Status / N / S / ?	Dieser Transponder ist durch die Funktion „Ersetzt“ von einem anderen Transponder ersetzt worden →Übertragung der Sperre zur Tür und Quittierung notwendig	DoT

3.5.5.7 Statusmeldungen in einer DoT-Anlage mit Online-Komponenten

Symbolik	Beschreibung	Anlage
Status	**Berechtigung** (in diesem Fall „keine Berechtigung“) mit **Quittierung**, →Berechtigung neu vergeben bzw. vorhandenes Recht ändern	DoT mit Online
Status Gruppe	Zuweisung der **Berechtigung** für eine **Transpondergruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder (Berechtigung z. B. „Immer“ exemplarisch für andere Berechtigungen) →Speichern nötig und Programmierung der Tür erforderlich →Online-Übertragung zur Tür startet nach Speichern automatisch bzw. Übertragung ggf. im Dialog manuell starten	DoT mit Online
Status	**Online-Übertragung** der Daten vom BKS KeyManager zur Tür (Übertragung auch mit Programmiergerät möglich) →Bis zum Ende der Übertragung abwarten	DoT mit Online
Status	**Speichern** der Daten in der Tür beendet, Übertragung abgeschlossen (Anzeige bei langsamer oder zweistufiger Verbindung möglich) →Quittierung wird gesendet	DoT mit Online
Status	**Berechtigung** einer **Transpondergruppe** zur Tür →Quittierung ist erfolgt	DoT mit Online
Status N	Zuweisung einer **Berechtigung** eines **einzelnen Transponders** zur Tür (Berechtigung z. B. „Immer“ exemplarisch für andere Berechtigungen) →Keine Programmierung der Tür erforderlich →Speichern nötig und Programmierung des Transponders erforderlich siehe 3.5.5.1 [91]	DoT mit Online
Status	Störung oder Abbruch der Online-Verbindung zur Tür z. B. bei der Übertragung der Daten zur Programmierung der Tür →Übertragungsfehler	DoT mit Online
Status	Störung oder Abbruch der Funk-Verbindung zur Tür z. B. bei der Übertragung der Daten zur Programmierung der Tür →Keine Funk-Verbindung	DoT mit Online

3.5.5.8 Statusmeldungen in Online-Anlagen

Symbolik	Beschreibung	Anlage
Status	**Berechtigung** (in diesem Fall „keine Berechtigung“) mit **Quittierung**, →Berechtigung neu vergeben bzw. vorhandenes Recht ändern	nonDoT Online
Gruppe Status	Zuweisung der **Berechtigung** für eine **Transpondergruppe** zur Tür, inklusive der zur Gruppe gehörenden Transponder (Berechtigung z. B. „Immer“ exemplarisch für andere Berechtigungen) →Speichern nötig und Programmierung der Tür erforderlich →Online-Übertragung zur Tür startet nach Speichern automatisch bzw. Übertragung ggf. im Dialog manuell starten	nonDoT Online
Status	**Online-Übertragung** der Daten vom BKS KeyManager zur Tür (Übertragung auch mit Programmiergerät möglich) →Bis zum Ende der Übertragung abwarten	nonDoT Online
Status	**Speichern** der Daten in der Tür beendet, Übertragung abgeschlossen (Anzeige bei langsamer oder zweistufiger Verbindung möglich) →Quittierung wird gesendet	nonDoT Online
Status	**Berechtigung** einer **Transpondergruppe** zur Tür →Quittierung ist erfolgt	nonDoT Online
Status	Zuweisung einer **Berechtigung** eines **einzelnen Transponders** zur Tür (Berechtigung z. B. „Immer“ exemplarisch für andere Berechtigungen) →Speichern nötig und Programmierung der Tür erforderlich →Online-Übertragung zur Tür startet nach Speichern automatisch bzw. Übertragung ggf. im Dialog manuell starten	nonDoT Online
Status	**Online-Übertragung** der Daten vom BKS KeyManager zur Tür (Übertragung auch mit Programmiergerät möglich) →Bis zum Ende der Übertragung abwarten	nonDoT Online
Status	**Speichern** der Daten in der Tür beendet, Übertragung abgeschlossen (Anzeige bei langsamer oder zweistufiger Verbindung möglich) →Quittierung wird gesendet	nonDoT Online
Status	**Berechtigung** eines **einzelnen Transponders** zur Tür →Quittierung ist erfolgt	nonDoT Online
Status	Störung oder Abbruch der Online-Verbindung zur Tür z. B. bei der Übertragung der Daten zur Programmierung der Tür →Übertragungsfehler	nonDoT Online
Status	Störung oder Abbruch der Funk-Verbindung zur Tür z. B. bei der Übertragung der Daten zur Programmierung der Tür →Keine Funk-Verbindung	nonDoT Online

3.5.5.9 Status der Batterieanzeige

Der Status der Batterieanzeige ist der Stand der letzten Programmierung bzw. Quittierung. Führen Sie vor der Überprüfung des Batteriestatus eine Aktualisierung durch eine Programmierung bzw. Quittierung durch. In Online-Anlagen und DoT-Anlagen mit Freigabeterminals werden dagegen die Batteriezustände regelmäßig aktualisiert.

Symbolik	Beschreibung	Anlage
Status	Batteriestatus: OK, Getrennter Status von Tür und Transponder, Anzeige in der Zeile für die Tür bei DoT-Anlagen/Online nonDot-Anlagen, Anzeige in der Spalte für den Transponder nur bei DoT-Anlagen	alle Anlagen-typen
Status	Batteriestatus: Batteriewechsel demnächst sinnvoll bzw. notwendig (Batteriewarnlevel 1)	alle Anlagen-typen
Status	Batteriestatus: Batteriewechsel erforderlich (Batteriewarnlevel 2)	alle Anlagen-typen

In Abhängigkeit der Einstellung Ihres Systems kann es vorkommen, dass der Status der Batterie in der Berechtigungsmatrix nicht angezeigt wird. Die Ursache liegt der Unterbrechung der Übertragungskette durch die Konfiguration einer oder mehrere Komponenten im Übertragungsweg.

Um einen gewünschten Datenschutz einzuhalten, könnte die übermittelte Datenmenge in den Komponenten eingeschränkt worden sein. Sollte dies in Ihrer Anlage keine Rolle spielen, überprüfen Sie bitte und stellen in den Einstellungen sicher, das die Informationen nicht in den Komponenten blockiert werden und die Information des Batteriestatus bis zum BKS KeyManager weitergeleitet wird.

Folgenden Einstellungen sind Anpassungen möglich.

Einstellung der Tür
- Öffnen Sie das Menü „Türen“
- Wählen Sie im Fenster „Eigenschaften des Zutrittspunkts“ einen Zutrittspunkt aus
- Im Feld „Ereignisspeicherung“ wählen Sie im Dropdown-Menü „Aktiv“ aus
- Drücken Sie auf den Button „Ereignisfilter“. Die Checkbox „Zutritt gewährt“ muss aktiviert sein

Einstellungen des Freigabeterminals
- Öffnen Sie das Menü „Einstellungen“
- Drücken Sie im Fenster „Einstellungen“ auf den Button „Online-Konfiguration“
- Im Register „Topologie“ wählen Sie in der Liste ein FGT, öffnen mit der rechten Maustaste das Kontextmenü und wählen Sie im Kontextmenü den Punkt „Einstellungen“ aus
- Im Fenster „Eigenschaften des Freigabeterminals“ sollte im Dropdown-Menü der Punkt „Berechtigte Zutritte (Prio 3)“ eingestellt sein

Anlagen-Einstellung (für neue Komponenten)
- Öffnen Sie das Menü „Einstellungen“
- Drücken Sie im Fenster „Einstellungen“ auf den Button „Anlagen-Einstellungen“
- Wechseln Sie zum Register „Für Anlage ...“
- Im Feld „Ereignisspeicherung-Voreinstellung“ sollte das Dropdown-Menü „Speicherung“ auf aktiv gesetzt sein

3.5.6 Bearbeiten der Berechtigungsmatrix im Client-Server-Betrieb

Um bei Schließanlagen im Client-Server-Betrieb eine parallele Bearbeitung von verschiedenen Arbeitsplätzen auszuschließen, muss am Arbeitsplatz die Schließanlage vor der Bearbeitung ausgecheckt werden. Hierdurch werden Fehler, die durch z. B. eine gleichzeitige Eingabe sich widersprechenden Eingaben entstehen könnten, verhindert. Während die Bearbeitung aktiviert wurde, ist die Verwaltung für andere Arbeitsplätze gesperrt.

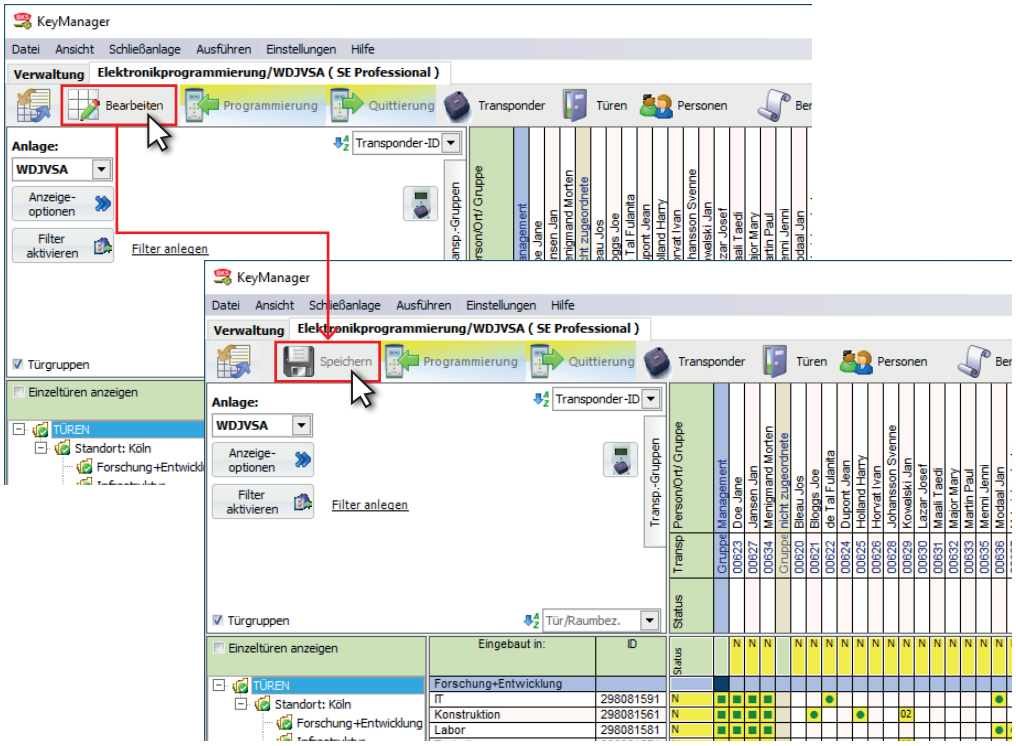
- Drücken Sie auf den Button „Bearbeiten“, um Ihren Arbeitsplatz zur Bearbeitung der Berechtigungsmatrix freizuschalten.

Durch das Auschecken ist im Rahmen der Berechtigungen Ihres Benutzerprofils eine Bearbeitung der Berechtigungsmatrix an Ihrem Arbeitsplatz jetzt möglich.

- Nach Abschluss der Arbeiten drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern und die Berechtigungsmatrix wieder einzuchecken.

Sollten Sie ohne eine Aktivität einen Zeitraum die Berechtigungsmatrix im Modus „Bearbeiten“ ausgecheckt lassen, führt dies zu einem Time-out durch den die Matrix automatisch abspeichert und wieder für andere Arbeitsplätze freigibt.

Die Bearbeitungsmöglichkeit ist jetzt für andere Arbeitsplätze wieder verfügbar.



3.6 Zutrittsberechtigungen, Freigabe|Sperrung

Die Zutrittsberechtigung der Transponder zu den Türen werden in der Berechtigungsmatrix verwaltet. Im Register „Elektronikprogrammierung/...“ wird Ihnen die Matrix angezeigt. In der Berechtigungsmatrix können die Berechtigungen direkt bearbeitet werden. Wählen Sie ein für die Zutrittsberechtigung stehendes Kästchen aus. Dieses referenziert über die Zeile auf die Tür und über die Spalte zur Transpondergruppe oder Transponder. In diesem Kästchen ist die Zutrittsberechtigung als Symbol dargestellt.

3.6.1 Verwaltung der Zutrittsberechtigungen

Der BKS KeyManager ist eine Software, durch welche die Verwaltung und Programmierung der mechanischen, mechatronischen und elektronischen Produkte sowie die Technologien dieser zu einem Gesamtsystem vereint werden.

In Abhängigkeit der Ausstattungsmerkmale Ihrer individuellen Schließanlage ergeben sich systembedingte Einschränkungen bei den Möglichkeiten in der Zutrittsorganisation. Insbesondere die Zutrittskontrolle und die Steuerung der Zutrittsberechtigungen werden durch das eingesetzte Schließsystem reglementiert.

Beachten Sie bei der Einrichtung und Verwaltung Ihrer Schließanlage im KeyManager das jeweilige Konzept der Anlage und die sich daraus ergebene Steuerung der Zutrittsberechtigungen.

3.6.1.1 Zutrittsberechtigungen in Data on Transponder-Systemen (DoT)

Bei einem Data on Transponder-System werden zur Steuerung der Zutrittskontrolle die Einzelrechte, die Gruppenzugehörigkeit und die Zeitzone des Transponders für die Zutrittsberechtigung durch den BKS KeyManager auf den Transpondern gespeichert und beim Zutritt an der Tür über eine sichere Verschlüsselung übermittelt. Die Türen müssen nur initial programmiert werden.

Änderungen in diesen Zutrittsberechtigungen können über den Transponder direkt an die Türen übermittelt werden, ohne dass diese mit einem Programmiergerät programmiert werden müssen. Die Programmierung der Transponder erfolgt über das Programmiergerät oder einem Freigabeterminal (FGT).

Wird die Berechtigung der Transponder über die Zugehörigkeit zu einer Transpondergruppe gewährt, muss die Berechtigung auf den Transpondern als Gruppenzugehörigkeit gespeichert und in den betreffenden Türen als Gruppenrecht programmiert werden. Die betroffenen Türen sind mit dem Programmiergerät zu programmieren.

Folgende Zutrittsberechtigungen sind im Data on Transponder-System (DoT) möglich.

Rechtevergabe im Transponder als Gruppenzugehörigkeit und in der Tür als Gruppenrecht	■ Auf dem Transponder werden die Berechtigungen von Transpondergruppen gespeichert. ■ Neue Transponder werden einer Transpondergruppe zugeordnet und sind an allen Türen berechtigt, an denen die Transpondergruppe zutrittsberechtigt ist. ■ Hat ein Transponder der Gruppe schon eine Einzelberechtigung, so wird diese mit Priorität für den Zutritt verwendet. ■ In der Tür wird die Transpondergruppe mit einem Programmierauftrag berechtigt. Es können Transpondergruppen gespeichert werden. Neue Gruppen und Gruppenrechtsänderungen müssen nur einmalig mit dem Programmiergerät in den Türen gespeichert werden. ■ Zum Sperren einzelner Transponder einer Gruppe müssen diese gesperrt werden. Das Setzen des Transponders auf keine Berechtigung führt nicht zur Sperrung.

Rechtevergabe im Transponder als Einzelrecht	■ Auf dem Transponder können Einzelberechtigungen für die Türen gespeichert werden. Einzelrechte haben Priorität vor Gruppenrechten. ■ Ist eine Transponderzeitzone vergeben, so wird diese für den Zutritt verwendet. Außerhalb der Zeitzone hat der Transponder keinen Zutritt. ■ Die Tür wird initial programmiert. ■ Bei späteren Änderungen der Zutrittsberechtigungen ist nur eine Programmierung der Transponder notwendig. ■ Gruppenrechte können mit Einzelrechten kombiniert werden, um die Zutrittsberechtigung einer Transpondergruppe mit Einzelberechtigungen, die nicht zur Gruppe gehören, zu erweitern.
Zeitgesteuerte Rechtevergabe: Zeitzone der Transpondergruppe	■ Wird diese Zeitzone vergeben, gilt sie für alle Türen, an denen die Transpondergruppe berechtigt ist. ■ Die Transpondergruppe muss einmalig mit einer Zeitzone in der Tür über einen Programmierauftrag berechtigt werden. ■ Wird ein Transponder der Transpondergruppe über eine Einzelberechtigung z. B. „Immer“ berechtigt, so hat das Einzelrecht Priorität vor dem Gruppenrecht. Der Transponder erhält nur nach dem Einzelrecht einen Zutritt. Trotz Transponderzeitzone hat der Transponder durch die Berechtigung „Immer“ ganztägigen Zutritt.
Zeitgesteuerte Rechtevergabe: Zeitzone des Transponders	■ Ist eine Transponderzeitzone als Einzelberechtigung vergeben, so wird diese mit Priorität für den Zutritt verwendet. Außerhalb der Zeitzone hat der Transponder keinen Zutritt.

Die Transponder des Data on Transponder-Systems haben folgende zusätzliche Eigenschaften.

Begrenzte Gültigkeit	Die Transponder können im Data on Transponder-System mit einem begrenzten Gültigkeitszeitraum versehen werden. Ein Transponder wird zukünftig aktiv bzw. wird nach Ablauf der Gültigkeit inaktiv, ohne dass der Transponder erneut programmiert werden muss.
Gültigkeitsverlängerung durch Freigabeterminal	Über den Parameter „Gültigkeitsverlängerung durch Freigabeterminal“ kann festgelegt werden, dass nach einer eingestellten Zeit ein Transponder inaktiv wird. Zur Aktivierung ist dann eine Buchung an einem Freigabeterminal (FGT) notwendig.
Ersatz für	Mit dieser Funktion kann ein Ersatz-Transponder einen verlorenen Transponder bei einem Zutritt in der betroffenen Tür sperren. Sollte nun jemand versuchen, mit dem verlorenen Transponder die Tür zu öffnen, so wird dieser abgelehnt.

3.6.1.2 Zutrittsberechtigungen in Offline-Systemen (nonDoT)

Die Basislösung der verschiedenen Konzepte von Schließsystemen sind die Offline-Systeme. Alle Daten zur Zutrittsorganisation werden ausschließlich in den Türen gespeichert. Die Zutrittsberechtigungen werden in der Berechtigungsmatrix mit dem Stand der Aktualisierung angezeigt.

Alle Änderungen der Schließberechtigungen müssen immer mit dem Programmiergerät manuell in die Türen programmiert werden. Der Vorteil liegt in einer einfachen Installation und das keine Verkabelung erforderlich ist.

Folgende Zutrittsberechtigungen sind in Offline-Systemen (nonDoT) möglich.

Rechtevergabe in der Tür als Gruppenrecht	■ Die Berechtigungen der Transpondergruppen werden nur in den Türen gespeichert. ■ Wurde ein neuer Transponder einer Transpondergruppe zugeordnet, erhält dieser erst nach der Programmierung der Tür die Berechtigung zum Zutritt. ■ Hat ein Transponder der Gruppe schon eine Einzelberechtigung, so wird diese mit Priorität für den Zutritt verwendet. ■ Die Transpondergruppe wird in der Tür mit einem Programmierauftrag berechtigt. Neue Gruppen und Gruppenrechtsänderungen müssen mit dem Programmiergerät an die Türen übertragen werden.
Rechtevergabe in der Tür als Einzelrecht	■ In der Tür können Einzelberechtigungen für den Zutritt gespeichert werden. Einzelrechte haben Priorität vor Gruppenrechten. ■ Die Zutrittsberechtigungen müssen in der Tür initial programmiert werden und die berechtigten Transponder Zutritt erhalten. ■ Bei späteren Änderungen der Zutrittsberechtigungen ist eine Programmierung der Tür notwendig. ■ Gruppenrechte können mit Einzelrechten kombiniert werden, um die Zutrittsberechtigung einer Transpondergruppe mit Einzelberechtigungen, die nicht zur Gruppe gehören, zu erweitern.
Zeitgesteuerte Rechtevergabe: Zeitzone des Transponders	■ Ist eine Zeitzone vergeben, so wird diese mit Priorität für den Zutritt verwendet. Außerhalb der Zeitzone hat der Transponder keinen Zutritt. ■ Ist die Transpondergruppe eines Transponders z. B. am Vormittag zutrittsberechtigt, so bekommt aber ein Transponder mit Zeitzone „Immer“ dennoch ganztägig Zutritt.
Zeitgesteuerte Rechtevergabe: Zeitzone der Gruppe	■ Wird diese Zeitzone vergeben, gilt sie für alle Türen, an denen die Transpondergruppe berechtigt ist. ■ Die Transpondergruppe muss über einen Programmierauftrag berechtigt werden.

In Offline-Systemen werden keine Data on Transponder-Lizenz, Online-Produkte oder Funkkomponenten zum Betrieb benötigt. Zur Aktualisierung und zum Auslesen der Daten ist das Programmiergerät die Schnittstelle zwischen KeyManager und den Türen und ggf. Transpondern. Der Datenaustausch wird „manuell“ durch Ablaufen der Türen und eine berührungslose Datenübertragung ermöglicht. Anpassungen wie z. B. geänderte Zutrittsrechte müssen auf diesem Weg übertragen werden. Neben der Programmierfunktion ist für die Wartung ein Auslesen der Serviceparameter der Türen möglich.

3.6.1.3 Zutrittsberechtigungen in Online-Systemen (nonDoT und DoT)

Im Online-System werden die Daten vom BKS KeyManager in Echtzeit über ein externes Peripheriegerät z. B. das EBK FM an die Türen gesendet.

Der sichere Datenaustausch vom BKS KeyManager wird durch die Anbindung von Funkwandmodulen über Netzwerk wie z. B. eine bestehende LAN-Infrastruktur und die weitere Übertragung zur Tür über Funk ermöglicht.

Änderungen der Schließberechtigungen müssen nicht „manuell“ mit dem Programmiergerät in der Tür programmiert werden, sondern werden automatisch über Funk übertragen.

Grundlage eines solchen Online-Systems ist die Verwendung von Online-Produkten.

3.6.2 Effiziente Reihenfolge bei Vergabe der Zutrittsberechtigungen

Bei der Vergabe der Zutrittsberechtigungen kann durch die Reihenfolge in der Vorgehensweise die Effizienz bei Vergabe von Zutrittsberechtigungen beeinflusst werden. Wir empfehlen folgende Reihenfolge. Die Vergabe erfolgt in der Ansicht „Listenmenü“ wechseln Sie ggf. zu dieser Ansicht.

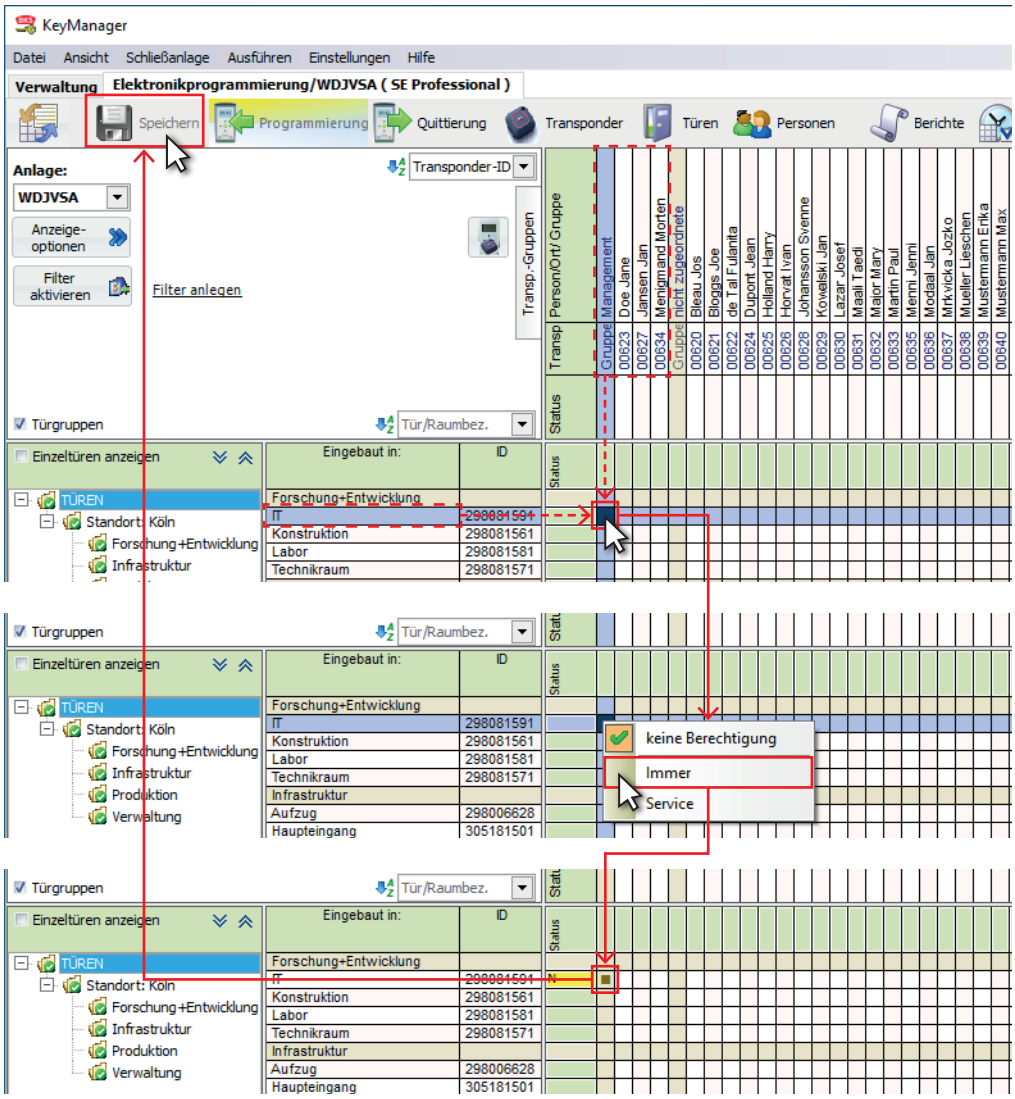
- Definition und Anlegen von Transpondergruppen für eine Personengruppe mit den gleichen Zutrittsberechtigungen.
  - Durch „Hinzufügen“ Transpondergruppen anlegen.
  - Mit „Zuordnung bearbeiten“ den Gruppen die Transponder zuordnen, welche durch die Gruppenzugehörigkeit eine Zutrittsberechtigung erhalten sollen.
- Vergabe der Gruppenberechtigungen
  - Durch „Berechtigungen“ den Transpondergruppen die Türen zuweisen, zu denen die Gruppe eine Zutrittsberechtigung haben soll und evtl. über „Zeitzone“ die Art dieser Berechtigung festlegen.
- Optional Definition und Anlegen von Türgruppen zur Übersichtlichkeit
- Vergabe von besonderen Berechtigungen zum Zutritt, z. B. Zeitzonen, Tagesfreigaben etc.
- Vergabe der Einzelberechtigungen für Transponder und deren Personen unter anderem auch zur Ergänzung der Berechtigungen der Transpondergruppen
  - In der Berechtigungsmatrix einzelnen Transpondern durch Auswahl eines Schnittpunkts und dem Kontextmenü „Transponder-Recht“ die Zutrittsberechtigung zu einzelnen Türen zuweisen.
- Programmierung
  - *Data on Transponder-Anlagen (DoT)*: Programmierung der Türen mit Transpondergruppenrechten und der Transponder mit Einzelrechten.
  - *Offline- oder Online-Anlage (nonDoT)*: Programmierung der Türen
- Quittierung

3.6.3 Berechtigung von Transpondergruppen/Gruppenberechtigungen

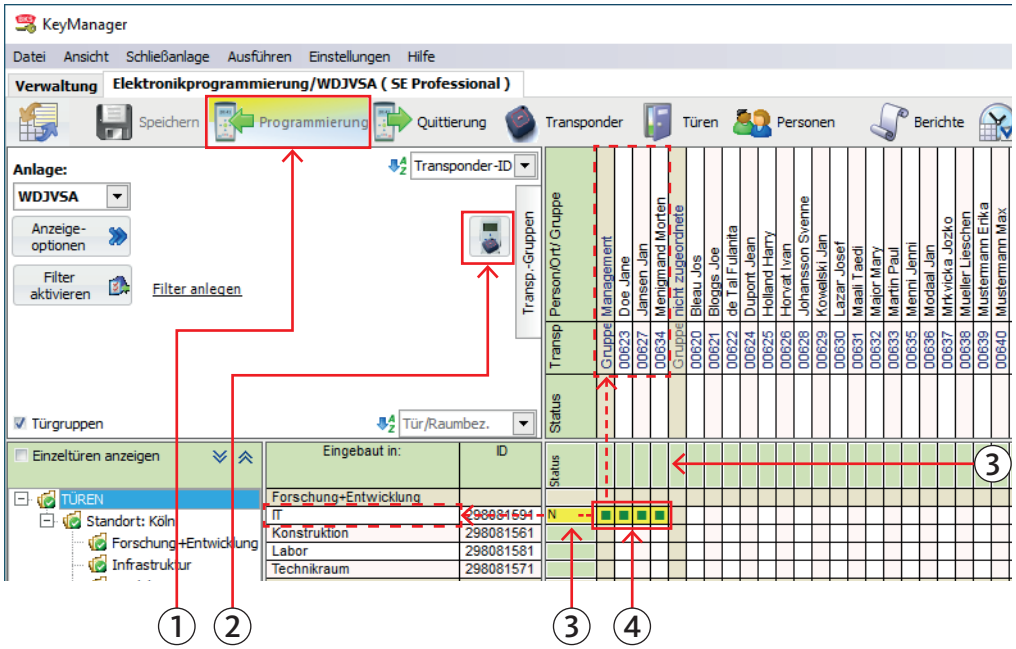
3.6.3.1 Gruppenberechtigungen im Transponder (DoT-Anlagen)

In Data on Transponder-Anlagen (DoT) vergeben Sie die Zutrittsberechtigungen der Transpondergruppen zu den Türen direkt in der in der Berechtigungsmatrix. Die Berechtigung wird anschließend in den Transponder als Berechtigung zur Gruppe und initial als Gruppenrecht in der Tür programmiert. Zum Erstellen einer Gruppenberechtigung in der Matrix befolgen Sie folgende Schritte.

- Markieren Sie in der Berechtigungsmatrix das Quadrat im Schnittpunkt der Spalte der gewünschten Transpondergruppe und der Zeile der gewünschten Tür mit der linken Maustaste.
- Öffnen Sie das Kontextmenü zum Quadrat mit der rechten Maustaste.
- Wählen Sie im Kontextmenü die Berechtigung mit der linken Maustaste aus. In diesem Beispiel wurde die Berechtigung „Immer“ ausgewählt. Die Auswahl einer Zeitzone z. B. „Service“ ist auch möglich. Gruppenrechte können nur für ganze Gruppe vergeben oder entfernt werden.
- Drücken Sie auf den Button „Speichern“. Dadurch wird automatisch allen Mitgliedern der Gruppe das Zutrittsrecht zugewiesen



Nach dem Speichern wird Ihnen der aktuelle Status der Programmierungen angezeigt:



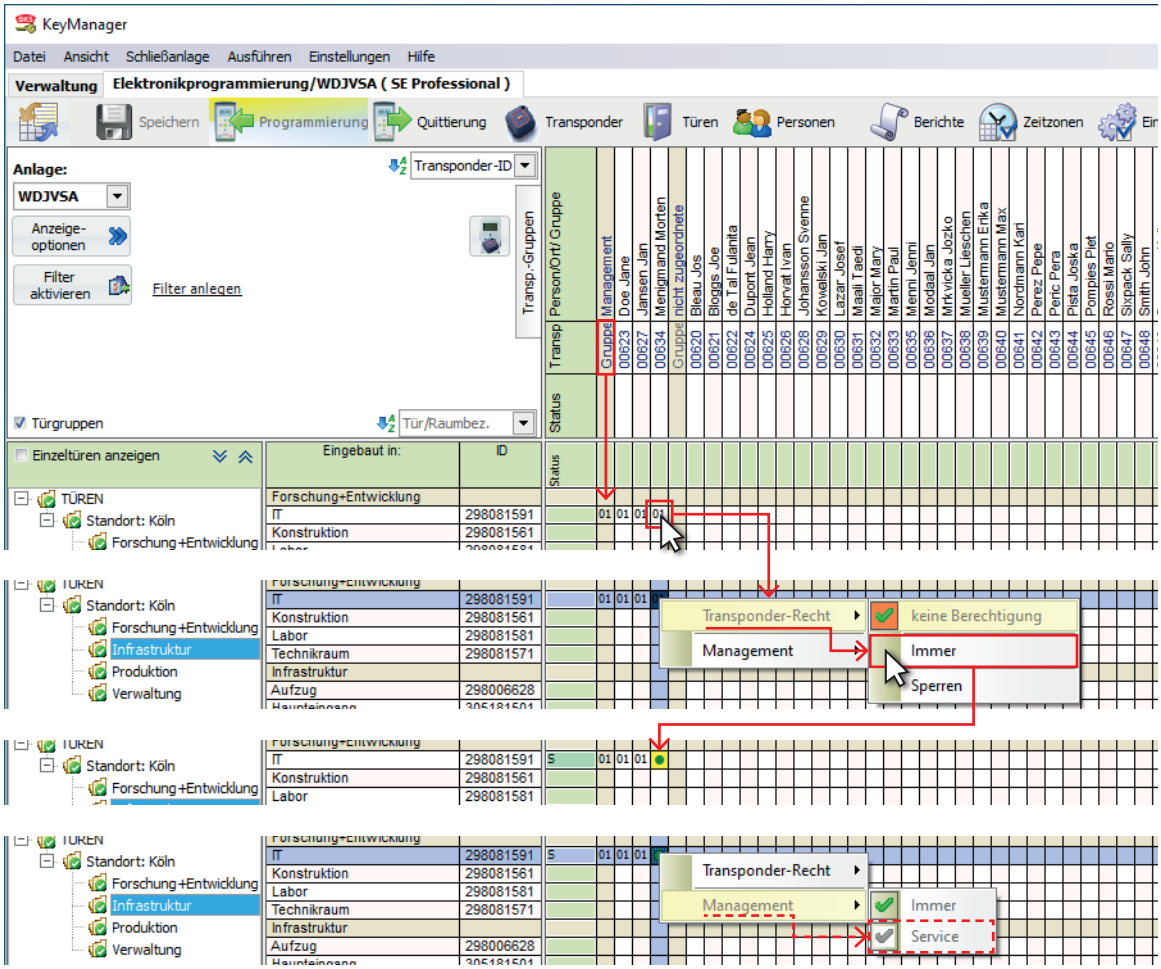
Wesentliche Bestandteile des Hauptbildschirms „Berechtigungsmatrix“.

Nr.	Beschreibung
1.	Sobald die Programmierung von mindestens einer Tür oder Zutrittspunkt erforderlich ist, wird der Button „Programmierung“ im Hauptmenü gelb hinterlegt.
2	Button zum „Programmierung der Transponder“ (nur DoT-Anlagen).
3.	In der Spalte „Status“ ist für jede Tür/Zutrittspunkt einzeln zu erkennen, ob eine Programmierung erforderlich ist. In der Zeile „Status“ (nur DoT-Anlagen) ist für jeden Transponder/Person einzeln zu erkennen, ob eine Programmierung erforderlich ist.
a.	Statusfeld: Leer -> Keine Programmierung erforderlich.
b.	Statusfeld: „N“ + Gelb -> Programmierung erforderlich und noch nicht auf Programmiergerät übertragen.
c.	Statusfeld: „S“ + Grün -> Programmierung erforderlich, bereits auf Programmiergerät übertragen jedoch noch nicht quittiert. Weitere Symbole siehe Kapitel 3.5.5 [90]
4.	Berechtigungen werden in der Berechtigungsmatrix angezeigt.
a.	Matrixfeld: Leer -> Keine Berechtigung.
b.	Matrixfeld: Punkt|Quadrat -> Transponder ist immer berechtigt.
c.	Matrixfeld: Gelb -> Farbe zeigt je Berechtigung an, dass die Übertragung der Änderungen der Berechtigungen auf ein Programmiergerät noch aussteht.
d.	Matrixfeld: Grün -> Farbe zeigt je Berechtigung an, dass die Berechtigungen auf ein Programmiergerät übertragen und noch nicht quittiert wurden.
e	Matrixfeld: Zahl -> Transponder ist zu einer bestimmten Zeitzone berechtigt. Weitere Symbole siehe Kapitel 3.5.5 [90].

Die Transpondereinzelberechtigung hat immer Priorität vor der Transpondergruppenberechtigung. In einer Transpondergruppe kann ein einzelner Transponder eine abweichende Berechtigung zur restlichen Gruppe durch die Vergabe einer Einzelberechtigung erhalten. In diesem Fall erlischt das Gruppenrecht und das Transponder-Recht ist für die Zutrittsberechtigung gültig.

In Beispiel unten hat die Transpondergruppe „Management“ die Berechtigung Zeitzone „01“ für die Transponder dieser Gruppen gültig. Dem einzelnen Transponder wird zusätzlich das Transponder-Recht „Immer“ zugewiesen, wodurch dieses das Gruppenrecht ungültig macht. Durch Auswahl des Transponder-Rechts „Sperren“ würde die Zutrittsberechtigung des Transponders trotz Gruppenberechtigung für die Tür gesperrt. In der Darstellung in der Berechtigungsmatrix ist das Gruppenrecht und die Zeitzone „01“ in Grau dargestellt, um dies zu unterstreichen. Das aktive Transponder-Recht „Immer“ wird dagegen mit grünem Haken und in Schwarz angezeigt.

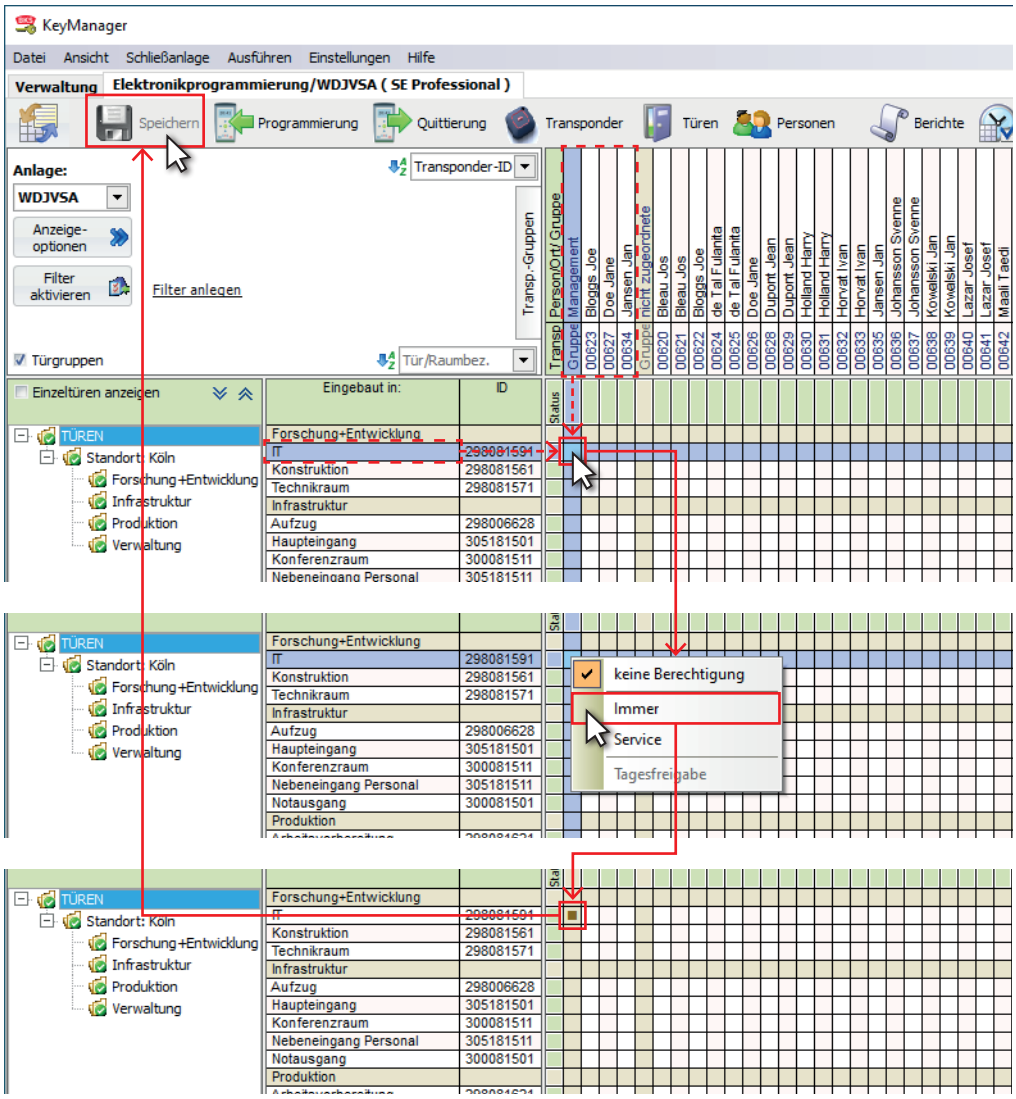
Auf diesem Weg ist es möglich, einem einzelnen Transponder eine abweichende Zutrittsberechtigung von der restlichen Transpondergruppe zu vergeben.



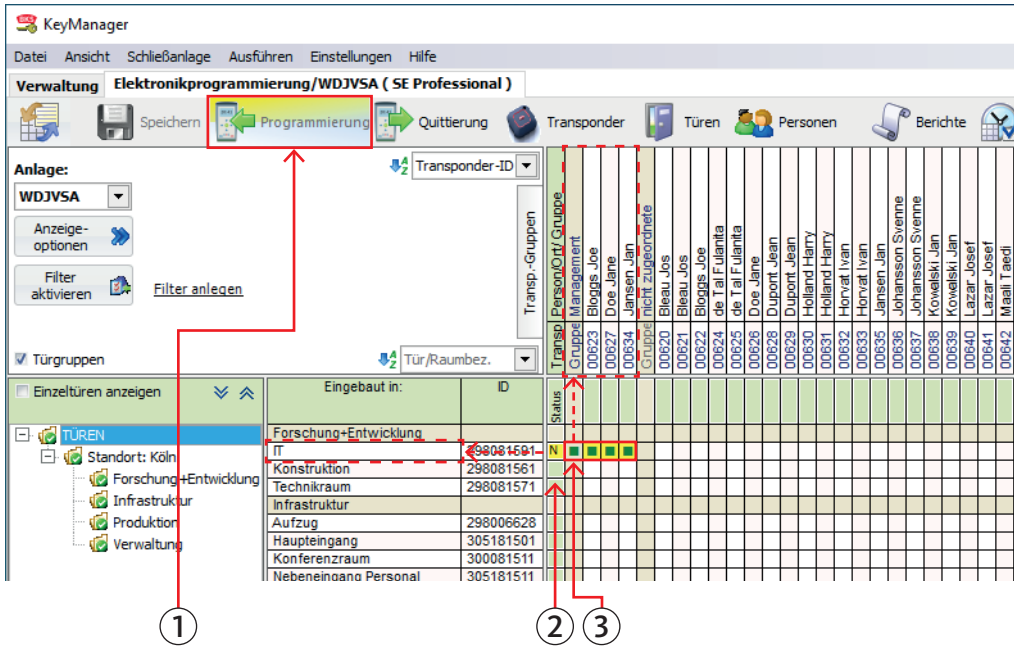
3.6.3.2 Gruppenberechtigungen in der Tür (nonDoT-Anlagen)

In Data on Transponder-Anlagen (DoT) vergeben Sie die Zutrittsberechtigungen der Transpondergruppen zu den Türen direkt in der in der Berechtigungsmatrix. Die Berechtigung wird anschließend in die Tür als Gruppenrecht programmiert. Zum Erstellen einer Gruppenberechtigung in der Matrix befolgen Sie folgende Schritte.

- Markieren Sie in der Berechtigungsmatrix das Quadrat im Schnittpunkt der Spalte der gewünschten Transpondergruppe und der Zeile der gewünschten Tür mit der linken Maustaste.
- Öffnen Sie das Kontextmenü zum Quadrat mit der rechten Maustaste.
- Wählen Sie im Kontextmenü die Berechtigung mit der linken Maustaste aus. In diesem Beispiel wurde die Berechtigung „Immer“ ausgewählt. Die Auswahl einer Zeitzone z. B. „Service“ ist auch möglich. Die optionale Tagesfreigabe kann an dieser Stelle erst aktiviert werden, wenn die Tagesfreigabe vorher in den Einstellungen der Tür aktiv gemacht wurde.
- Drücken Sie auf den Button „Speichern“. Dadurch wird automatisch allen Mitgliedern der Gruppe das Zutrittsrecht zugewiesen



Nach dem Speichern wird Ihnen der aktuelle Status der Programmierungen angezeigt:



Wesentliche Bestandteile des Hauptbildschirms „Berechtigungsmatrix“.

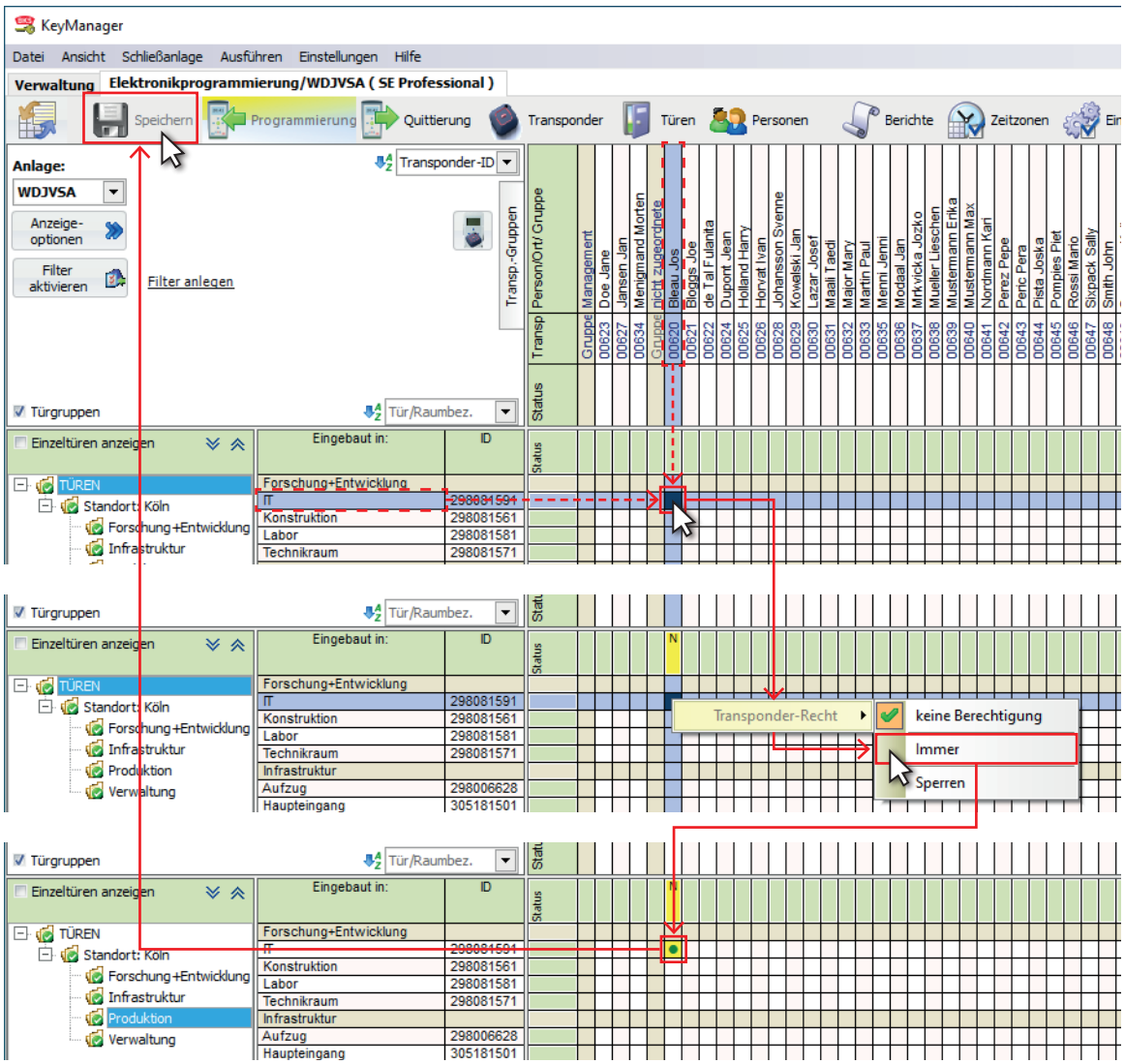
Nr.	Beschreibung
1.	Sobald die Programmierung von mindestens einer Tür oder Zutrittspunkt erforderlich ist, wird der Button „Programmierung“ im Hauptmenü gelb hinterlegt.
2.	In der Spalte „Status“ ist für jede Tür/Zutrittspunkt einzeln zu erkennen, ob eine Programmierung erforderlich ist.
a.	Statusfeld: Leer -> Keine Programmierung erforderlich.
b.	Statusfeld: „N“ + Gelb -> Programmierung erforderlich und noch nicht auf Programmiergerät übertragen.
c.	Statusfeld: „S“ + Grün -> Programmierung erforderlich, bereits auf Programmiergerät übertragen jedoch noch nicht quittiert. Weitere Symbole siehe Kapitel 3.5.5 [90]
3.	Berechtigungen werden in der Berechtigungsmatrix angezeigt.
a.	Matrixfeld: Leer -> Keine Berechtigung.
b.	Matrixfeld: Punkt|Quadrat -> Transponder ist immer berechtigt.
c.	Matrixfeld: Gelb -> Farbe zeigt je Berechtigung an, dass die Übertragung der Änderungen der Berechtigungen auf ein Programmiergerät noch aussteht.
d.	Matrixfeld: Grün -> Farbe zeigt je Berechtigung an, dass die Berechtigungen auf ein Programmiergerät übertragen und noch nicht quittiert wurden.
e	Matrixfeld: Zahl -> Transponder ist zu einer bestimmten Zeitzone berechtigt. Weitere Symbole siehe Kapitel 3.5.5 [90].

3.6.4 Berechtigung von Transpondern

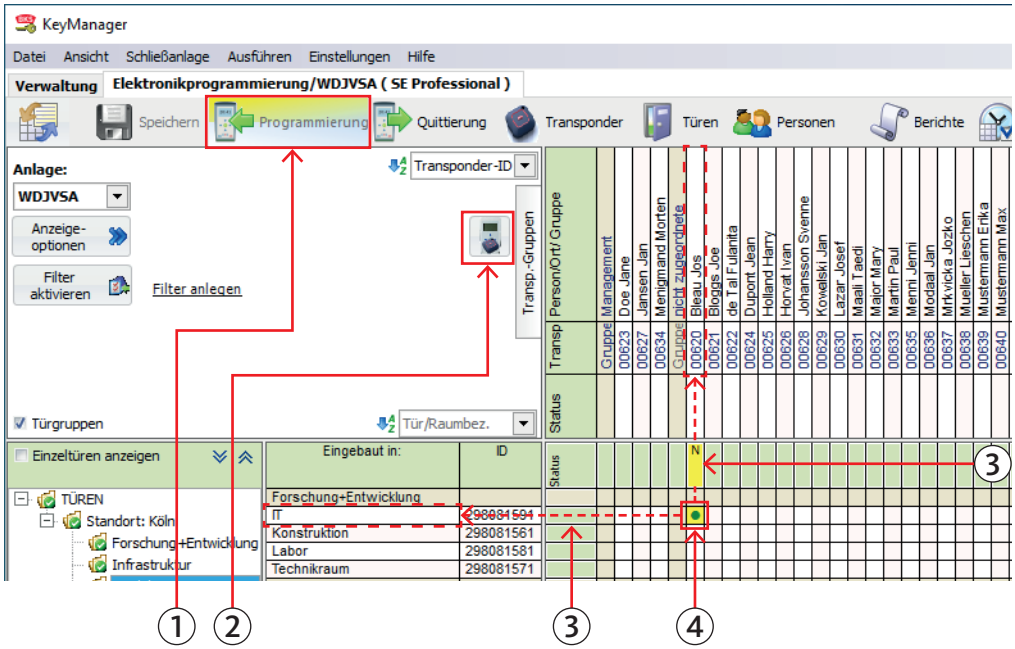
3.6.4.1 Einzelberechtigung im Transponder, Transponder-Recht (DoT-Anlagen)

In Data on Transponder-Anlagen (DoT) vergeben Sie die Zutrittsberechtigungen der einzelnen Transponder direkt in der in der Berechtigungsmatrix. Die Berechtigung wird anschließend in den Transponder und initial in der Tür programmiert. Zum Erstellen einer Einzelberechtigung in der Matrix befolgen Sie folgende Schritte.

- Markieren Sie in der Berechtigungsmatrix das Quadrat im Schnittpunkt der Spalte des gewünschten Transponders und der Zeile der gewünschten Tür mit der linken Maustaste.
- Öffnen Sie das Kontextmenü zum Quadrat mit der rechten Maustaste.
- Wählen Sie im Kontextmenü die Berechtigung mit der linken Maustaste aus. In diesem Beispiel wurde die Berechtigung „Immer“ ausgewählt. Einzelne Transponder, die zu einer Gruppe gehören, können mit der Auswahl „Sperren“ für eine Tür gesperrt werden, ohne das andere Transponder in der Gruppe davon betroffen sind. In der Matrix ist die Kennzeichnung ist ein rotes Minus-Zeichen.
- Drücken Sie auf den Button „Speichern“.



Nach dem Speichern wird Ihnen der aktuelle Status der Programmierungen angezeigt:



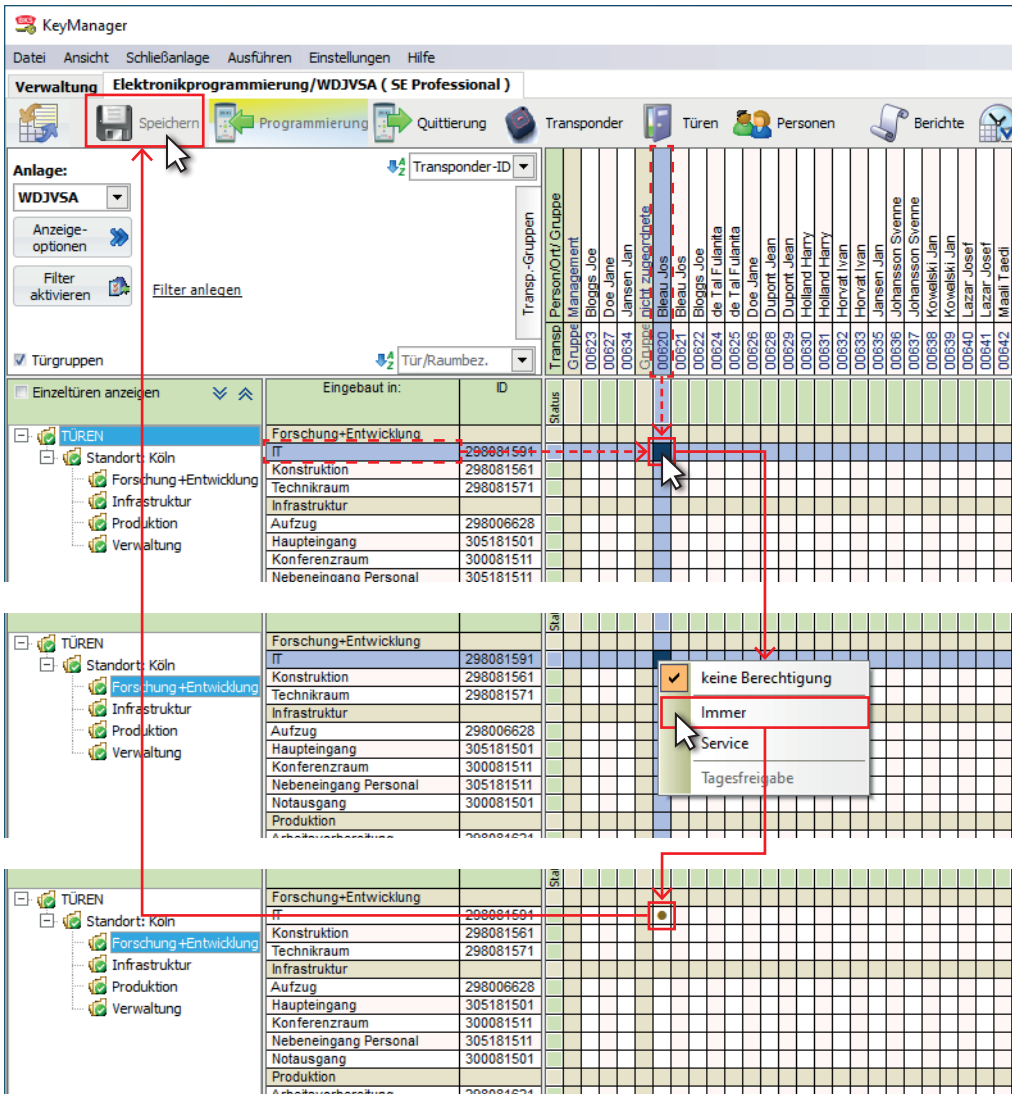
Wesentliche Bestandteile des Hauptbildschirms „Berechtigungsmatrix“.

Nr.	Beschreibung
1.	Sobald die Programmierung von mindestens einer Tür oder Zutrittspunkt erforderlich ist, wird der Button „Programmierung“ im Hauptmenü gelb hinterlegt.
2	Button zum „Programmierung der Transponder“ (nur DoT-Anlagen).
3.	In der Spalte „Status“ ist für jede Tür/Zutrittspunkt einzeln zu erkennen, ob eine Programmierung erforderlich ist. In der Zeile „Status“ (nur DoT-Anlagen) ist für jeden Transponder/Person einzeln zu erkennen, ob eine Programmierung erforderlich ist.
a.	Statusfeld: Leer -> Keine Programmierung erforderlich.
b.	Statusfeld: „N“ + Gelb -> Programmierung erforderlich und noch nicht auf Programmiergerät übertragen.
c.	Statusfeld: „S“ + Grün -> Programmierung erforderlich, bereits auf Programmiergerät übertragen jedoch noch nicht quittiert. Weitere Symbole siehe Kapitel 3.5.5 [90]
4.	Berechtigungen werden in der Berechtigungsmatrix angezeigt.
a.	Matrixfeld: Leer -> Keine Berechtigung.
b.	Matrixfeld: Punkt|Quadrat -> Transponder ist immer berechtigt.
c.	Matrixfeld: Gelb -> Farbe zeigt je Berechtigung an, dass die Übertragung der Änderungen der Berechtigungen auf ein Programmiergerät noch aussteht.
d.	Matrixfeld: Grün -> Farbe zeigt je Berechtigung an, dass die Berechtigungen auf ein Programmiergerät übertragen und noch nicht quittiert wurden.
e	Matrixfeld: Zahl|Minus-Zeichen-> Transponder ist zu einer bestimmten Zeitzone berechtigt oder gesperrt. Weitere Symbole siehe Kapitel 3.5.5 [90].

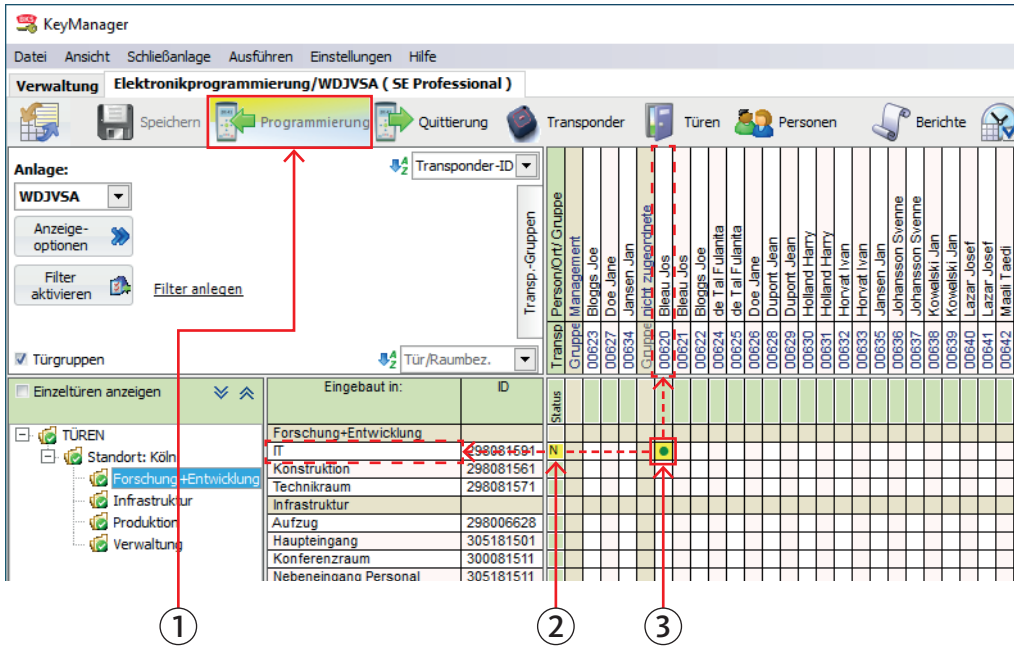
3.6.4.2 Einzelberechtigungen in der Tür (nonDoT-Anlagen)

In On-und Offline-Anlagen (nonDoT) vergeben Sie die Zutrittsberechtigungen der einzelnen Transponder direkt in der in der Berechtigungsmatrix. Die Berechtigung wird anschließend in die Tür als Zutrittsrecht programmiert. Zum Erstellen einer Einzelberechtigung in der Matrix befolgen Sie folgende Schritte.

- Markieren Sie in der Berechtigungsmatrix das Quadrat im Schnittpunkt der Spalte des gewünschten Transponders und der Zeile der gewünschten Tür mit der linken Maustaste.
- Öffnen Sie das Kontextmenü zum Quadrat mit der rechten Maustaste.
- Wählen Sie im Kontextmenü die Berechtigung mit der linken Maustaste aus. In diesem Beispiel wurde die Berechtigung „Immer“ ausgewählt. Die Auswahl einer Zeitzone z. B. „Service“ ist auch möglich. Über die Auswahl „keine Berechtigung“ wird die Tür gesperrt. Die optionale Tagesfreigabe kann an dieser Stelle erst aktiviert werden, wenn die Tagesfreigabe vorher in den Einstellungen der Tür und Transponder aktiv gemacht wurde.
- Drücken Sie auf den Button „Speichern“.



Nach dem Speichern wird Ihnen der aktuelle Status der Programmierungen angezeigt:



Wesentliche Bestandteile des Hauptbildschirms „Berechtigungsmatrix“.

Nr.	Beschreibung
1.	Sobald die Programmierung von mindestens einer Tür oder Zutrittspunkt erforderlich ist, wird der Button „Programmierung“ im Hauptmenü gelb hinterlegt.
2.	In der Spalte „Status“ ist für jede Tür/Zutrittspunkt einzeln zu erkennen, ob eine Programmierung erforderlich ist.
a.	Statusfeld: Leer -> Keine Programmierung erforderlich.
b.	Statusfeld: „N“ + Gelb -> Programmierung erforderlich und noch nicht auf Programmiergerät übertragen.
c.	Statusfeld: „S“ + Grün -> Programmierung erforderlich, bereits auf Programmiergerät übertragen jedoch noch nicht quittiert. Weitere Symbole siehe Kapitel 3.5.5 [90]
3.	Berechtigungen werden in der Berechtigungsmatrix angezeigt.
a.	Matrixfeld: Leer -> Keine Berechtigung.
b.	Matrixfeld: Punkt|Quadrat -> Transponder ist immer berechtigt.
c.	Matrixfeld: Gelb -> Farbe zeigt je Berechtigung an, dass die Übertragung der Änderungen der Berechtigungen auf ein Programmiergerät noch aussteht.
d.	Matrixfeld: Grün -> Farbe zeigt je Berechtigung an, dass die Berechtigungen auf ein Programmiergerät übertragen und noch nicht quittiert wurden.
e	Matrixfeld: Zahl|Minus-Zeichen-> Transponder ist zu einer bestimmten Zeitzone berechtigt oder gesperrt. Weitere Symbole siehe Kapitel 3.5.5 [90].

3.6.5 Berechtigung durch Zeitzonen und/oder Sondertagen

Zeitzonen und Sondertage sind eine differenziertere Methode, die Zutrittsberechtigungen anzulegen im Gegensatz zu den im vorherigen Kapitel beschriebenen „Ja/Nein“-Rechten.

Zeitzonen sind begrenzte Berechtigungszeiträume, welche auch an mehreren Tagen und auch an Sondertagen gelten können. Während der Zeitzone haben die Transponder/-gruppen eine Zutrittsberechtigung zu den über die Matrix zugeordneten Türen bzw. Zutrittspunkten. Außerhalb des zeitlichen Intervalls der Zeitzonen besteht keine Zutrittsberechtigung. Ausgenommen sind Berechtigungen durch eine GHS-Berechtigung (siehe 4.2.7 [186]) oder durch eine Einzelberechtigung (siehe vorherige Kapitel).

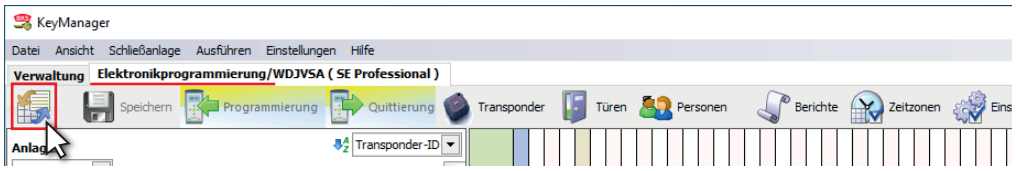
Sondertage werden genutzt, um an bestimmten Tagen die vorhandenen Zutrittsrechte Außerkraft zusetzen. Während der Sondertage haben nur die über die Matrix speziell ausgewählte Transponder/-gruppen zu den zugeordneten Türen eine Berechtigung. Andere Berechtigungen haben keine Gültigkeit. Ausgenommen sind Berechtigungen durch eine GHS-Berechtigung, siehe 4.2.7 [186].

- Vor der Vergabe der Berechtigung müssen Sie zuerst die Zeitzonen und Sondertage wie im Kapitel 4.7 [243] beschrieben festlegen.

Weitere Informationen zur Einrichtung von Zeitzonen als Berechtigung finden Sie in den Kapiteln „Transponder ausgeben“ siehe Kapitel 4.2.2 [164] und „Einstellungen des Zutrittspunkts“ siehe Kapitel 4.3.2 [208].

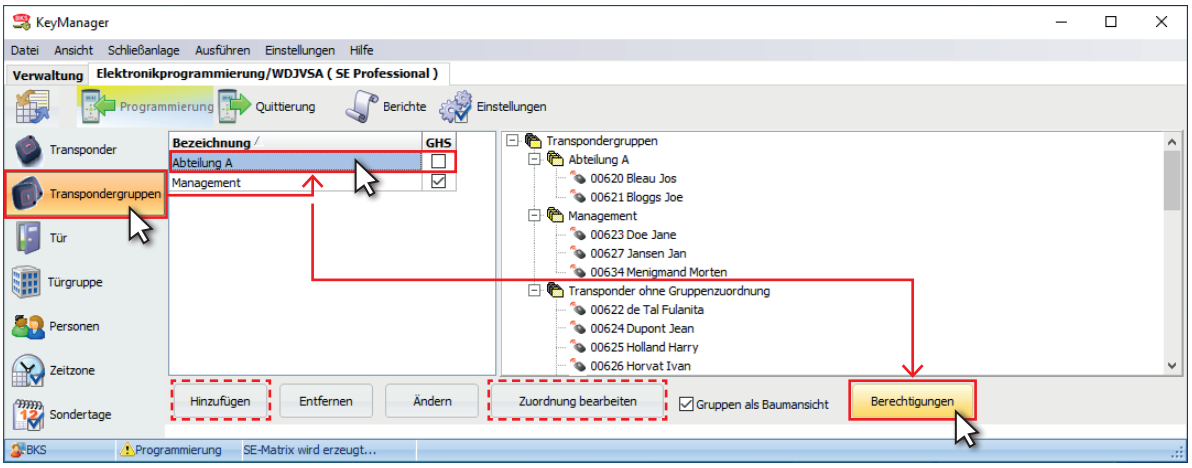
Durch Verwendung einer Data on Transponder-Anlage (DoT) oder einer Offline- oder Online-Anlage (nonDoT) kommt es zu Unterschieden bei der Vergabe der Berechtigungen.

3.6.5.1 Zeitzonen für Transpondergruppen



Die Vergabe erfolgt in der Ansicht „Listenmenü“ wechseln Sie ggf. zu dieser Ansicht.

- Drücken Sie auf die Schaltfläche „Transpondergruppen“.
- Wählen Sie die Transpondergruppe aus, welche die Berechtigung für die Zeitzone erhalten soll. Die Zeitzone kann auch Sondertage enthalten.



Zur Erstellung einer neuen Gruppe drücken Sie auf „Hinzufügen“. Über den Button „Zuordnung bearbeiten“ ist es möglich, einer Gruppe neue bzw. weitere Transponder hinzuzufügen. Weitere Vorgehensweise siehe Kapitel 4.2.7 [186].

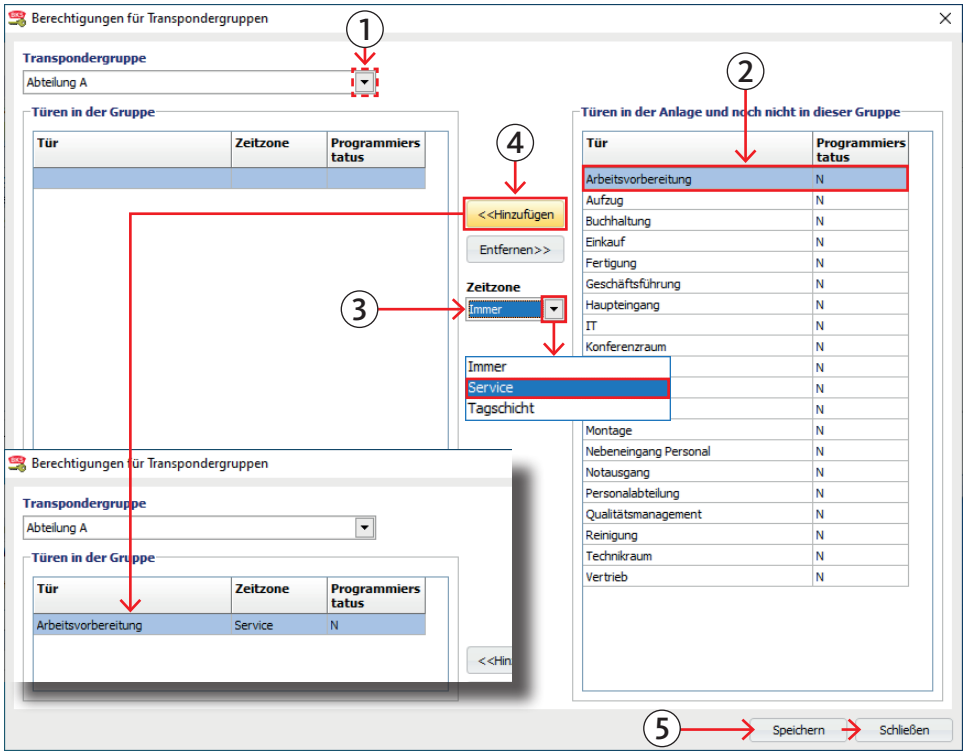
- Drücken Sie auf den Button „Berechtigungen“.

Definieren Sie über die folgenden Schritte die Berechtigungen.

- Über das Dropdown-Menü (1) ist das Wechseln der Transpondergruppe vor oder während der Bearbeitung möglich.
- Wählen Sie in die Tür (2) aus, welche zur Transpondergruppe hinzugefügt werde soll.
- Legen Sie mit dem Dropdown-Menü (3) die Zeitzone (oder Immer) fest und dadurch welche Berechtigung für die Tür (1) gelten soll.

Bei Erstellung der Zeitzone ist die Berechtigung für Sondertage durch das Hinzufügen der Sondertage zur Zeitzone zu berücksichtigen, falls es gewünscht ist, während der Zeitzone an Sondertagen Zutritt zuhaben.

- Drücken Sie auf den Button (4) „Hinzufügen und fügen die Tür zur Transpondergruppe (1) hinzu.
- Beenden Sie den Dialog durch „Speichern“ und „Schließen“

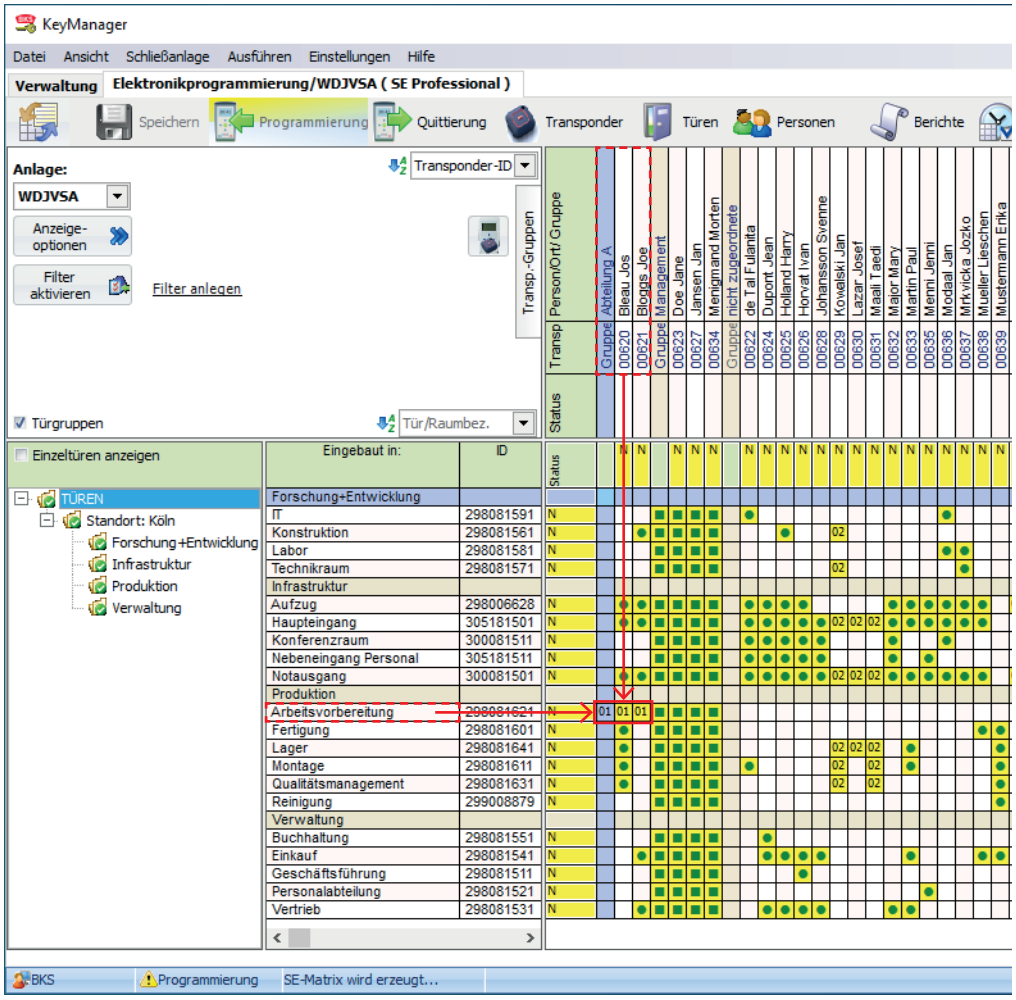


- Folgende Berechtigungen werden nun in der Matrix dargestellt, welche exemplarisch durch die vorherigen Schritte erstellt worden.

Alle Transponder der Transpondergruppe erhalten nach dem Beenden des Dialogs die Zutrittsberechtigung für die gewählten Türen mit der jeweils im Dropdown ausgesuchten Zeitzone, z. B. die Anzeige „01“ für die Zeitzone „Service“. Ausgenommen sind Transponder, welche schon vorher über die Einzelberechtigung eines Transponders eine Zutrittsberechtigung bekommen haben.

Eine Einzelberechtigung hat immer Priorität vor den Gruppenberechtigungen und muss ggf. über das Kontextmenü der Einzelberechtigung beim „Transponder-Recht“ auf „keine Berechtigung“ gesetzt werden, um den Transponder die Rechte der Transpondergruppe zuzuweisen.

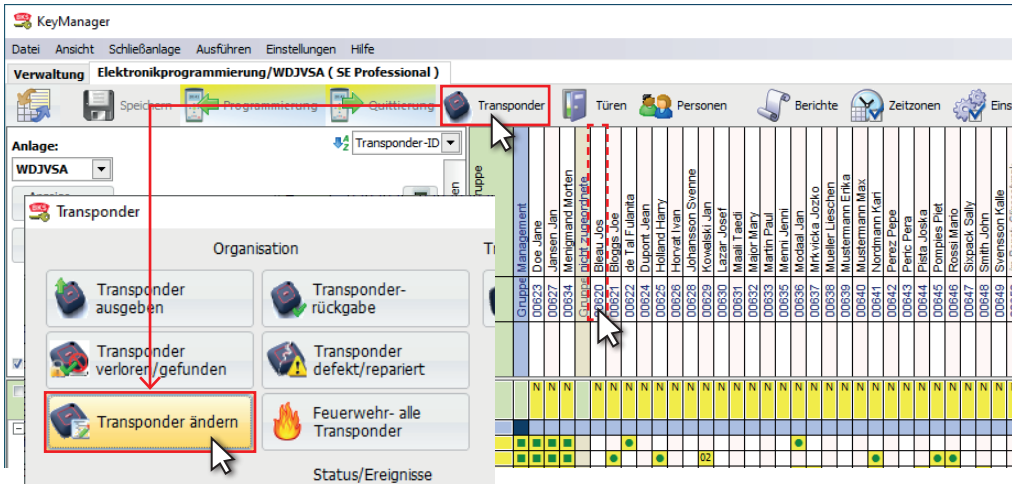
Die Änderungen der Berechtigungen müssen vor dem Wirksamwerden in der Türe bzw. den Zutrittspunkten programmiert werden.

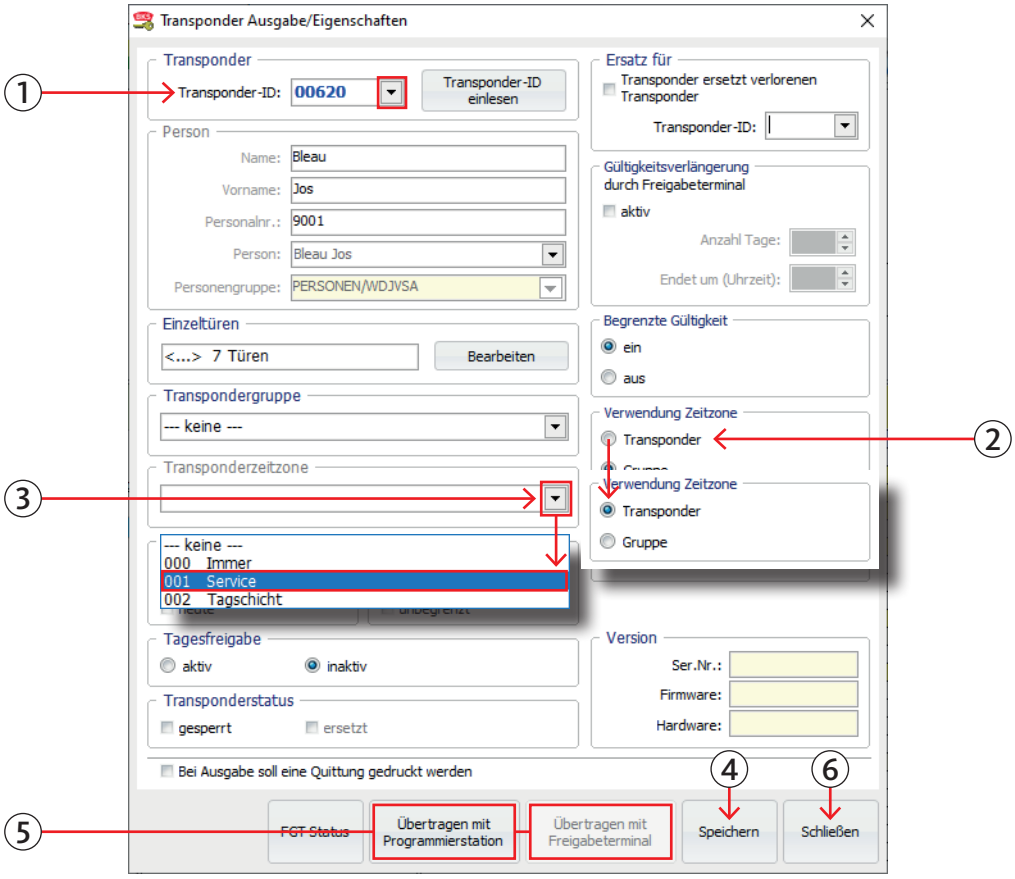


3.6.5.2 Zeitzonen für einzelne Transponder in DoT-Anlagen

- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Transponder“ und im Transponder-Fenster auf den Button „Transponder ändern“.

Alternativ können Sie im Kopf der Matrix durch einen doppelten Mausklick auf die Nummer des Transponders oder das Feld des Personennamens den Dialog öffnen.

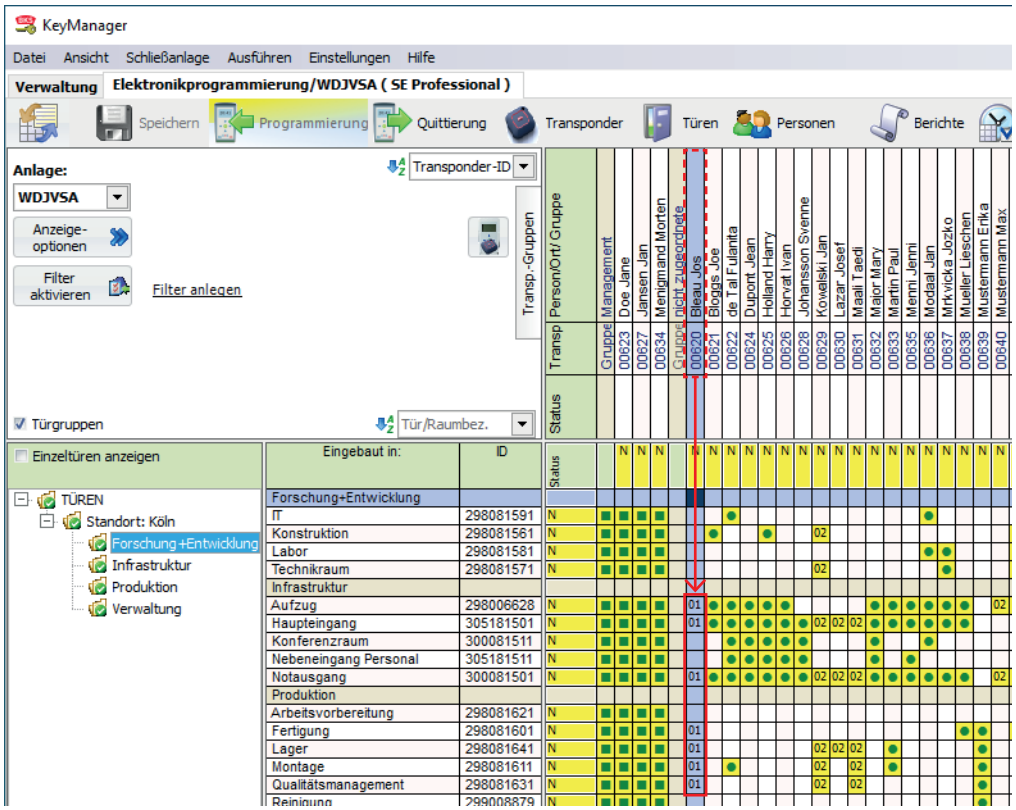




- Wählen Sie über das Dropdown-Menü (1) den gewünschten Transponder aus. Alternativ kann man den gewünschten Transponder über das Programmiergerät durch das Auslesen auswählen, falls der Transponder physisch vorhanden ist. Nach einem Doppelklick auf einen Transponder in der Matrix ist dieser Transponder vorausgewählt.
- Setzen Sie die „Verwendete Zeitzone“ (2) durch Aktivierung der Checkbox „Transponder“.
- Legen Sie mit dem Dropdown-Menü (3) die Zeitzone (z. B. „001 Service“) fest, welche nach der Vergabe der Berechtigung in der Matrix für diesen Transponder gelten soll.

Bei Erstellung der Zeitzone ist die Berechtigung für Sondertage durch das Hinzufügen der Sondertage zur Zeitzone zu berücksichtigen, falls es gewünscht ist, während der Zeitzone an Sondertagen Zutritt zuhaben.

- Drücken Sie auf den Button „Speichern“ (4).
- Vor dem Wirksamwerden muss die Zeitzone auf den Transponder übertragen werden. Drücken Sie auf den Button „Übertragung mit Programmierstation“ (5) bei Verwendung eines Programmiergeräts zur Übertragung oder auf den Button „Übertragung mit Freigabeterminal“ (5), wenn der Transponder bei der nächsten Präsentation am Freigabeterminal mit den Daten programmiert werden soll.
- Beenden Sie den Dialog „Schließen“ (6).



3.6.5.3 Zeitzonen für einzelne Transponder in einer nonDoT-Anlagen

Die Vergabe erfolgt in der „Berechtigungsmatrix“, wechseln Sie ggf. zu dieser Ansicht.

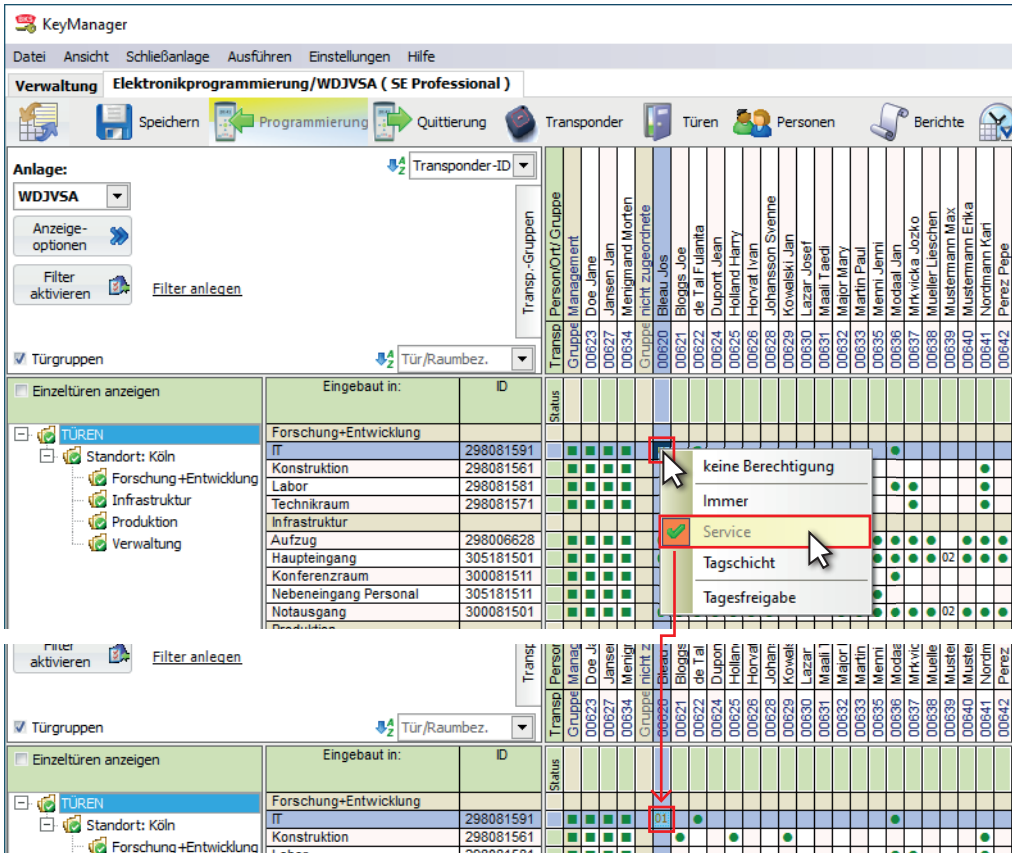
- Wählen Sie in der Matrix den Schnittpunkt der Spalte des Transponders und der Zeile der Tür aus, für welche Sie die Berechtigung der Zeitzone vergeben wollen.

Bei Erstellung der Zeitzone ist die Berechtigung für Sondertage durch das Hinzufügen der Sondertage zur Zeitzone zu berücksichtigen, falls es gewünscht ist, während der Zeitzone an Sondertagen Zutritt zuhaben.

- Öffnen Sie im Quadrat des Schnittpunkts das Kontextmenü mit der rechten Maustaste.
- Wählen Sie im Kontextmenü mit der linken Maustaste die Zeitzone zur Vergabe der Berechtigung aus.

Nach der Auswahl der Berechtigung wird für die Zeitzone „Service“ nach Abschluss des Dialogs im Quadrat der Matrix ein „01“ angezeigt.

- Vor dem Wirksamwerden muss die Zeitzone mit dem Programmiergerät auf die Tür bzw. den Zutrittspunkt übertragen werden.



3.6.6 Berechtigung über Tagesfreigaben

Die Tagesfreigabe ist eine weitere Berechtigungsform, bei der die Zutrittsberechtigung zur Tür nach Freischaltung durch einen berechtigten Transponder weiter, solange die Tagesfreigabe besteht, aktiv bleibt. Der Zeitraum und die Funktionsweise der Tagesfreigabe ist vom Modus abhängig.

Je Zutrittspunkt kann wahlweise nur ein Modus eingestellt werden. Folgende Tagesfreigabe-Funktionen stehen zur Auswahl: „Manuell“, „Halbautomatisch“ oder „Automatisch“.
Weiter Erläuterungen finden Sie in den folgenden Unterkapiteln.

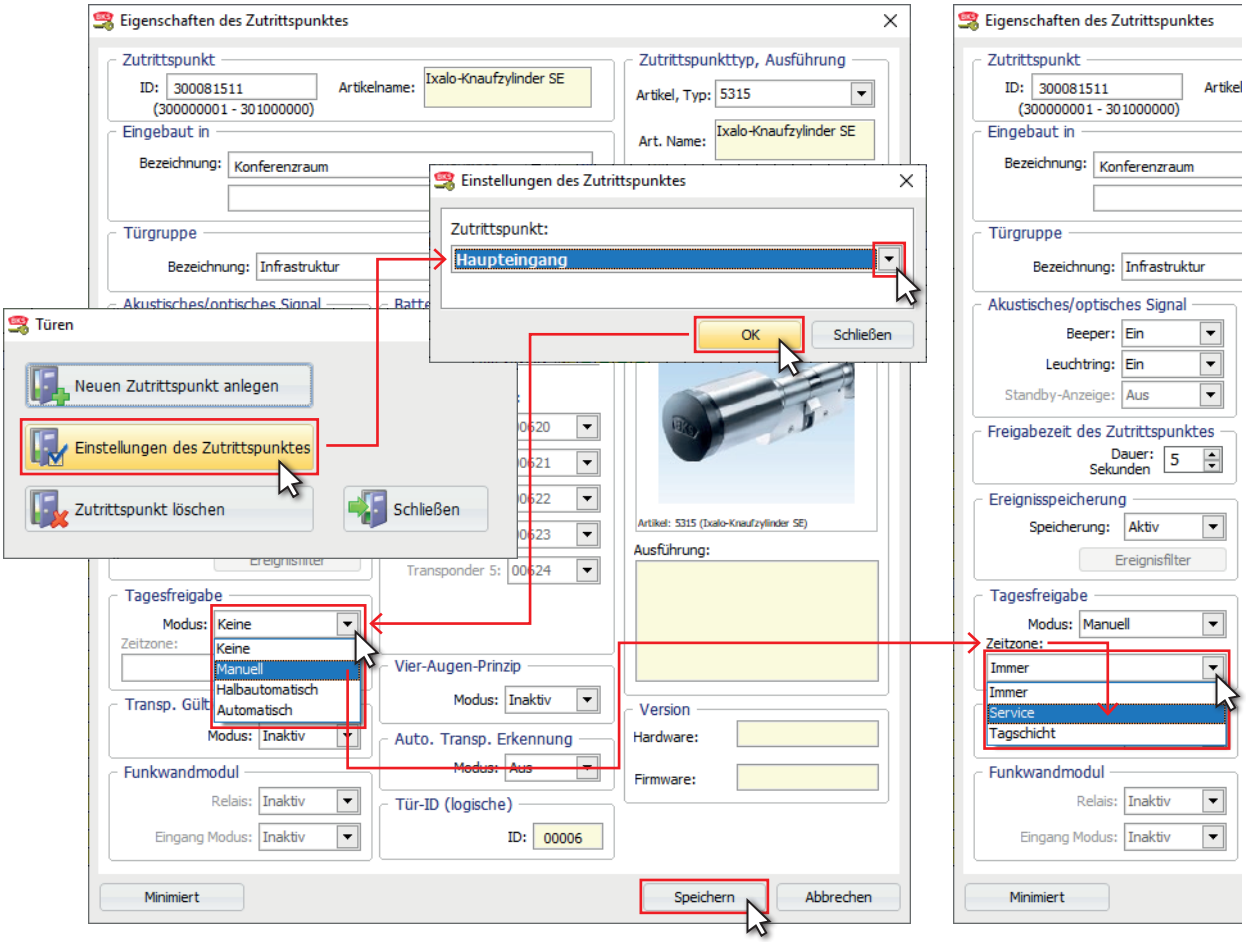
Nach Freischaltung der Funktion in der betroffenen Tür und ggf. Transponder kann die Berechtigung „Tagesfreigabe“ über die Berechtigungsmatrix, den Transpondern und Türen wie eine normale Berechtigung zugeordnet werden.

HINWEIS

Die Tagesfreigabefunktion verkürzt unabhängig von Modus und Länge der Freigabe die Lebensdauer der Batterien der Zutrittspunkte nicht.
Die Tagesfreigabe-Funktion ist nicht mit dem janus SE-Zylinder kompatibel und bei diesem auch nicht aktivierbar.

Aktivierung der Tagesfreigabe in einer Data on Transponder-Anlage (DoT).

- Drücken Sie in der Berechtigungsmatrix auf den Menüpunkt „Türen“ und im Weiteren den Button „Einstellungen des Zutrittspunktes“.
- Wählen Sie im Dropdown-Menü den gewünschten Zutrittspunkt aus. Drücken Sie zur Bestätigung auf „OK“.



Die Option zur Aktivierung der Tagesfreigabe befindet sich im Feld „Tagesfreigabe“

- Wählen Sie im Dropdown-Menü „Modus“ die Funktionalität der Tagesfreigabe aus. Folgende Möglichkeiten stehen zur Auswahl: Manuell | Halbautomatisch | Automatisch. Keine deaktiviert die Funktion der Tagesfreigabe.

Weitere Beschreibung zu den Eigenschaften der drei Modi in den folgenden Unterkapiteln.

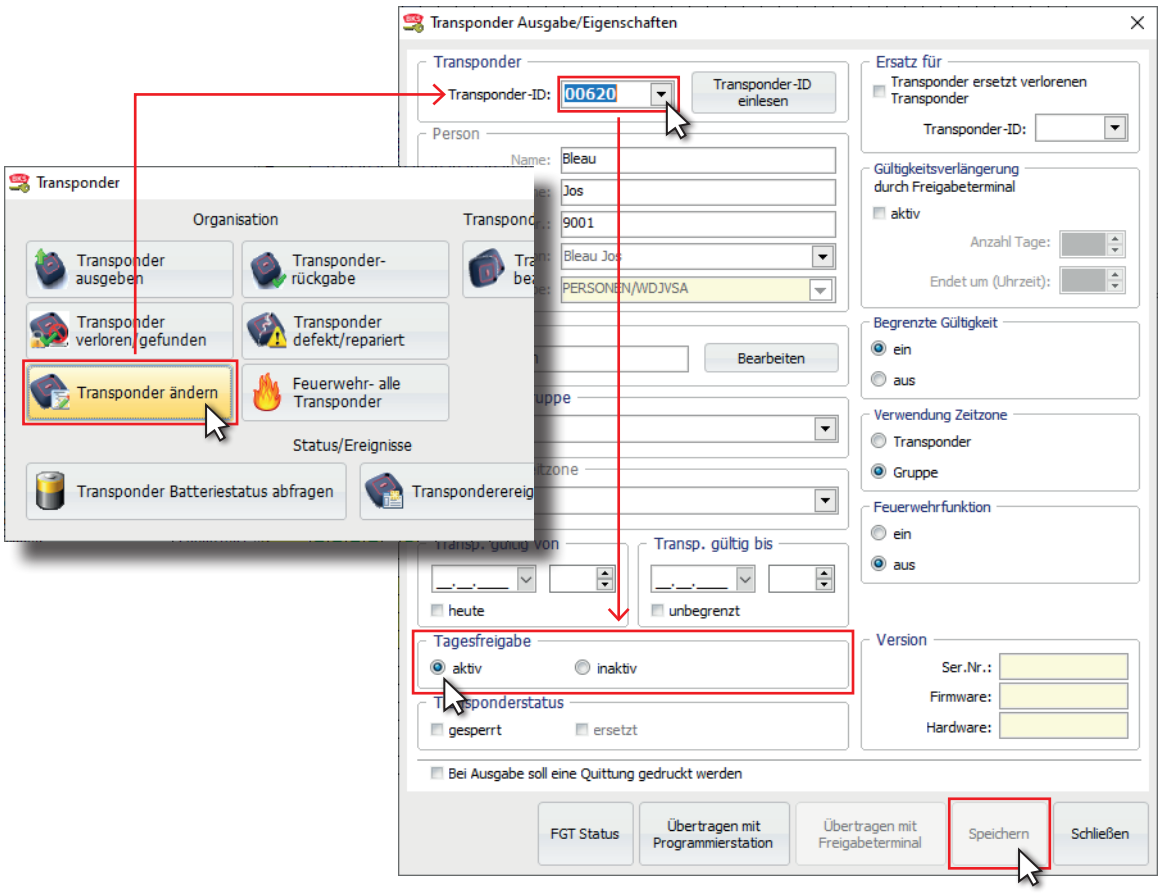
- Legen Sie über das Dropdown-Menü „Zeitzone“ die Zeitzone fest, während der die Tagesfreigabe aktivierbar bzw. aktiviert werden soll.
- Drücken Sie auf den Button „Speichern“ zum Beenden des Dialogs.

Wenn Sie in den Eigenschaften des Zutrittspunkts die Tagesfreigabe auf Manuell oder Halbautomatisch eingestellt haben sind die folgenden Schritt erforderlich.

- Drücken Sie in der Berechtigungsmatrix auf den Menüpunkt „Transponder“ und im Weiteren den Button „Transponder ändern“.
- Wählen Sie im Dropdown-Menü den gewünschten Transponder aus.

Die Option zur Aktivierung der Tagesfreigabe befindet sich im Feld „Tagesfreigabe“

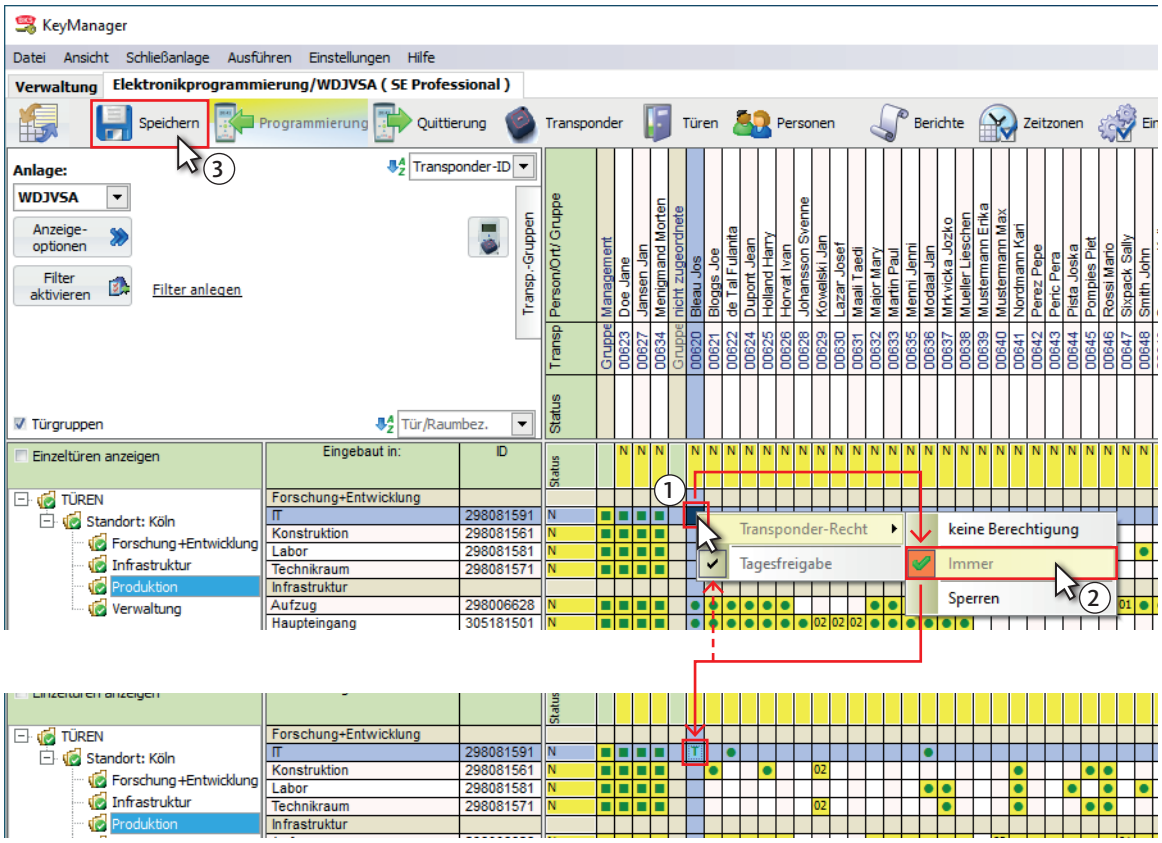
- Aktivieren Sie die Checkbox „aktiv“, um die Tagesfreigabe einzuschalten.
- Drücken Sie auf den Button „Speichern“ zum Beenden des Dialogs.



Zur Aktivierung der vorherigen Einstellungen im Menü „Türen“ und „Transponder“ ist die Berechtigungsmatrix zu verwenden.

- Wählen Sie in der Matrix über den Schnittpunkt der Zeile die Tür|Zutrittspunkt und in der Spalte den Transponder|Person, der die Tür öffnen soll, aus.
- Öffnen Sie im Quadrat zu diesem Schnittpunkt das Kontextmenü mit der rechten Maustaste.
- Wählen Sie im Kontextmenü über das Untermenü „Transponder-Recht“ die Berechtigung „Immer“ oder die gewünschte Zeitzone aus. Mit der linken Maustaste können Sie z. B. „Immer“ auswählen und die Tagesfreigabe für die Tür und Transponder aktivieren.

Die aktivierte Tagesfreigabe wird in der Matrix mit einem „T“ symbolisiert. Beim Öffnen des Kontextmenüs zu diesem Schnittpunkt ist der Menüpunkt „Tagesfreigabe“ mit einem Haken gekennzeichnet.



Aktivierung der Tagesfreigabe in einer Offline- oder Online-Anlage (nonDoT).

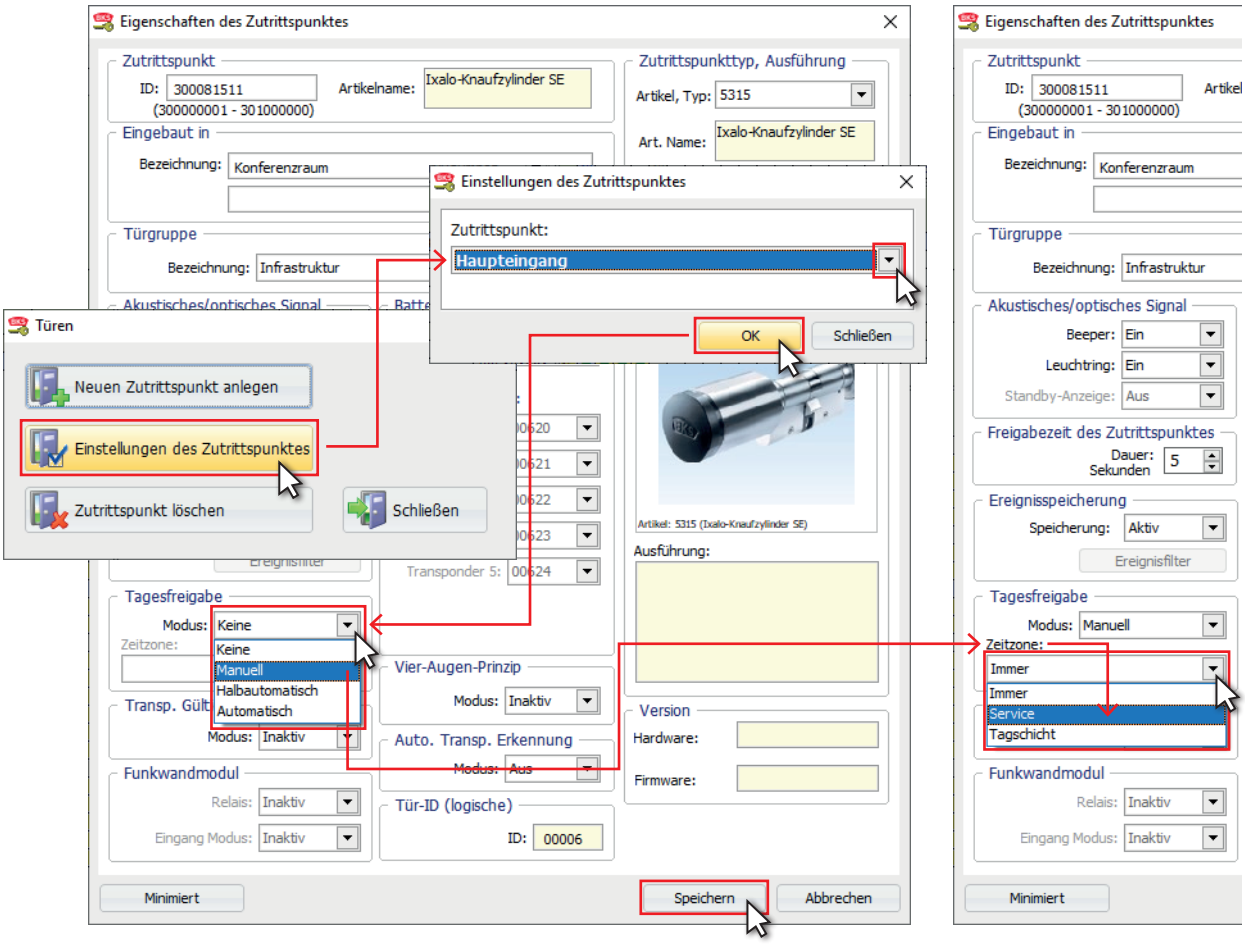
- Drücken Sie in der Berechtigungsmatrix auf den Menüpunkt „Türen“ und im Weiteren den Button „Einstellungen des Zutrittspunktes“.
- Wählen Sie im Dropdown-Menü den gewünschten Zutrittspunkt aus. Drücken Sie zur Bestätigung auf „OK“.

Die Option zur Aktivierung der Tagesfreigabe befindet sich im Feld „Tagesfreigabe“

- Wählen Sie im Dropdown-Menü „Modus“ die Funktionalität der Tagesfreigabe aus. Folgende Möglichkeiten stehen zur Auswahl: Manuell | Halbautomatisch | Automatisch. Keine deaktiviert die Funktion der Tagesfreigabe.

Weitere Beschreibung zu den Eigenschaften der drei Modi in den folgenden Unterkapiteln.

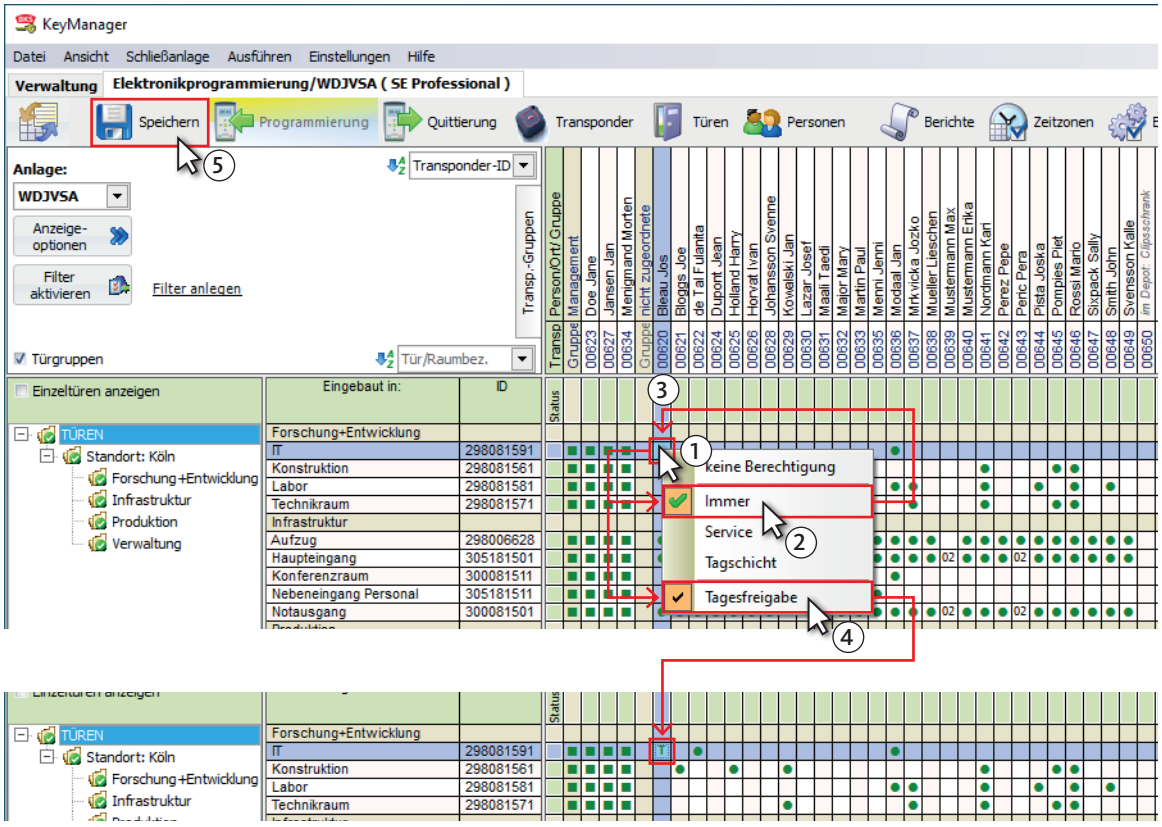
- Legen Sie über das Dropdown-Menü „Zeitzone“ die Zeitzone aus, während der die Tagesfreigabe aktivierbar sein soll.
- Drücken Sie auf den Button „Speichern“ zum Beenden des Dialogs.



Zur Aktivierung der vorherigen Einstellungen im Menü „Türen“ ist die Berechtigungsmatrix zu verwenden.

- Wählen Sie in der Matrix über den Schnittpunkt der Zeile die Tür|Zutrittspunkt und in der Spalte den Transponder|Person, der die Tür öffnen soll, aus.
- Öffnen Sie im Quadrat zu diesem Schnittpunkt das Kontextmenü mit der rechten Maustaste.
- Wählen Sie im Kontextmenü die Berechtigung „Immer“ oder die gewünschte Zeitzone aus. Mit der linken Maustaste können Sie z. B. „Immer“ auswählen und um für den Transponder die Zutrittsberechtigung zu dieser Tür zu aktivieren.
- Öffnen Sie das Kontextmenü im Quadrat zum Schnittpunkt erneut mit der rechten Maustaste.
- Wählen Sie im Kontextmenü den Menüpunkt „Tagesfreigabe“ aus und aktivieren diesen mit der linken Maustaste.

Die aktivierte Tagesfreigabe wird in der Matrix mit einem „T“ symbolisiert.



3.6.6.1 Tagesfreigabe-Modus „Manuell“ (Toggle-Modus)

Die Tagesfreigabe-Funktion „Manuell“ wird durch die Präsentation eines berechtigten Transponders mit Tagesfreigabe am Zutrittspunkt manuell gestartet. Die Zutrittsberechtigung ist während der Aktivierung dauerhaft freigeschaltet und der Zutrittspunkt frei begehbar.

Die Tagesfreigabe kann nur gestartet werden, während eine Zutrittsberechtigung des Transponders zum Zutrittspunkt besteht. Ist die Berechtigung „Immer“ in der Berechtigungsmatrix gesetzt worden, kann die Tagesfreigabe beliebig gestartet werden. Wurde die Berechtigung „Zeitzone“ vergeben, ist ein Start der Tagesfreigabe nur innerhalb des Berechtigungszeitraums der Zone möglich. Die Deaktivierung ist aber auch außerhalb der Zeitzone möglich.

Die Beendigung der Tagesfreigabe ist nur manuell möglich. Der Transponder muss erneut am Zutrittspunkt präsentiert werden, wodurch die Tagesfreigabe deaktiviert und der Zutrittspunkt gesperrt wird.

Außerhalb des Zeitraums der Tagesfreigabe können an Zutrittspunkten mit aktiviertem Modus „Manuell“ alle Transponder normal verwendet werden und gewähren je nach ihrer Berechtigung Zutritt.

Ein Anwendungsbeispiel wäre die Tür zu einem Betriebsraum, in dem Arbeiten von einer externen Firma durchgeführt werden sollen. Vor Arbeitsbeginn würde durch den Hausmeister die Zutrittsberechtigung manuell auf Tagesfreigabe gesetzt werden, um den externen Kräften einen unbegrenzten Zugang zu dem Raum zu gewähren. Nach Abschluss der Arbeiten würde der Hausmeister die Tagesfreigabe manuell wieder beenden und die Zutrittsberechtigung sperren.

Voraussetzung für die Tagesfreigabe „Manuell“

- Bei der Türe|Zutrittspunkt ist in den Eigenschaften im Feld Tagesfreigabe im Dropdown-Menü „Modus“ der Menüpunkt „Manuell“ ausgewählt (bei DoT und nonDoT-Anlagen erforderlich).
- In den Eigenschaften des Transponders muss die Checkbox Tagesfreigabe auf „aktiv“ gesetzt sein (nur bei DoT-Anlagen erforderlich).
- In der Berechtigungsmatrix muss im Schnittpunkt von Transponder und Tür ein „T“ stehen.

Start der Tagesfreigabe „Manuell“

- Betätigen Sie den Button des Transponders und halten ihn gedrückt bis eine doppelte Bestätigung der Freigabe vom Zutrittspunkt erfolgt und die Tagesfreigabe deaktiviert ist.
- Bei Transpondern mit einer Firmware-Version kleiner 3.35 wird die Tagesfreigabe durch einen einfachen Tastendruck aktiviert.

HINWEIS **Die Firmware-Version des Transponders können Sie über das Programmiergerät (Menü SE / Transponderinfo) auslesen.**

Ende der Tagesfreigabe „Manuell“

- Betätigen Sie den Button des Transponders und halten ihn gedrückt bis eine doppelte Bestätigung der Freigabe vom Zutrittspunkt erfolgt und die Tagesfreigabe deaktiviert ist.
- Bei Transpondern mit einer Firmware-Version kleiner 3.35 wird die Tagesfreigabe durch einen einfachen Tastendruck deaktiviert.

3.6.6.2 Tagesfreigabe-Modus „Halbautomatisch“

Die Tagesfreigabe-Funktion „Halbautomatisch“ wird durch die Präsentation eines berechtigten Transponders mit Tagesfreigabe am Zutrittspunkt manuell gestartet. Die Zutrittsberechtigung ist während der Aktivierung dauerhaft freigeschaltet und der Zutrittspunkt frei begehbar.

Die Tagesfreigabe kann nur gestartet werden, während eine Zutrittsberechtigung des Transponders zum Zutrittspunkt besteht. Das heißt, nur während des Berechtigungszeitraums der in der Berechtigungsmatrix gesetzten „Zeitzone“ kann die Tagesfreigabe mit einem Transponder der Tagesfreigabe berechtigt ist, gestartet werden.

Die Beendigung der Tagesfreigabe wird halb-automatisch ausgeführt. Außerhalb der in der Berechtigungsmatrix gesetzten „Zeitzone“ wird die Tagesfreigabe automatisch deaktiviert und der Zutrittspunkt gesperrt. Alternativ ist es aber auch möglich, mit einem Transponder die Tagesfreigabe manuell zu deaktivieren und den Zutrittspunkt zu sperren.

Außerhalb des Zeitraums der Tagesfreigabe können an Zutrittspunkten mit aktiviertem Modus „Halbautomatisch“ alle Transponder normal verwendet werden und gewähren je nach ihrer Berechtigung Zutritt.

Ein Anwendungsbeispiel wäre die Tür zu einem Seminarraum, bei der vom Seminarleiter morgens manuell die Zutrittsberechtigung auf Tagesfreigabe gesetzt wird, um den Teilnehmen tagsüber unbegrenzten Zugang zu gewähren und abends automatisch zur eingestellten Zeit automatisch die Zutrittsberechtigung zu sperren.

Voraussetzung für die Tagesfreigabe „Halbautomatisch“

- Bei der Türe|Zutrittspunkt ist in den Eigenschaften im Feld Tagesfreigabe im Dropdown-Menü „Modus“ der Menüpunkt „Halbautomatisch“ ausgewählt (bei DoT und nonDoT-Anlagen erforderlich).
- In den Eigenschaften des Transponders muss die Checkbox Tagesfreigabe auf „aktiv“ gesetzt sein (nur bei DoT-Anlagen erforderlich).
- In der Berechtigungsmatrix muss im Schnittpunkt Transponder und Tür ein „T“ stehen

Start der Tagesfreigabe „Halbautomatisch“

- Betätigen Sie den Button des Transponders und halten ihn gedrückt bis eine doppelte Bestätigung der Freigabe vom Zutrittspunkt erfolgt und die Tagesfreigabe deaktiviert ist.
- Bei Transpondern mit einer Firmware-Version kleiner 3.35 wird die Tagesfreigabe durch einen einfachen Tastendruck aktiviert.

HINWEIS **Die Firmware Version des Transponders können Sie über das Programmiergerät (Menü SE / Transponderinfo) auslesen.**

Ende der Tagesfreigabe „Halbautomatisch“

- Automatisch mit Ende der Zeitzone.
- Betätigen Sie den Button des Transponders und halten ihn gedrückt bis eine doppelte Bestätigung der Freigabe vom Zutrittspunkt erfolgt und die Tagesfreigabe deaktiviert ist.
- Bei Transpondern mit einer Firmware-Version kleiner 3.35 wird die Tagesfreigabe durch einen einfachen Tastendruck deaktiviert.

3.6.6.3 Tagesfreigabe-Modus „Automatisch“

Die Tagesfreigabe-Funktion „Automatisch“ wird durch die Zeitzone automatisch gestartet. Während des durch die Zeitzone vorgegebenen Zeitraums ist die Zutrittsberechtigung dauerhaft freigeschaltet und der Zutrittspunkt frei begehbar.

Die Tagesfreigabe wird automatisch durch die Zeitzone gestartet und auch beendet. Außerhalb der Zeitzone ist die Tagesfreigabe deaktiviert. Es sind keine Transponder für die Tagesfreigabe im Modus „Automatisch“ notwendig.

Außerhalb des Zeitraums der Tagesfreigabe können an Zutrittspunkten mit aktiviertem Modus „Automatisch“ alle Transponder normal verwendet werden und gewähren je nach ihrer Berechtigung Zutritt.

Ein Anwendungsbeispiel wäre eine stark frequentierte Haupteingangstüre, zu welcher Personen ohne Zutrittsberechtigung oder ohne Transponder während eines bestimmten Zeitraums einen Zutritt erhalten sollen. Außerhalb der Geschäftszeiten oder in den Pausen, wenn der Empfang nicht besetzt ist, soll die Tür verschlossen sein und nur von berechtigten Personen passierbar sein.

Voraussetzung für die Tagesfreigabe „Automatisch“

- Bei der Türe|Zutrittspunkt ist in den Eigenschaften im Feld Tagesfreigabe im Dropdown-Menü „Modus“ der Menüpunkt „Automatisch“ ausgewählt (bei DoT und nonDoT-Anlagen erforderlich).

Start der Tagesfreigabe „Automatisch“

- Automatisch mit Beginn der Zeitzone.

Ende der Tagesfreigabe „Automatisch“

- Automatisch mit Ende der Zeitzone.

3.6.7 Gültigkeitsverlängerung der Zutrittsberechtigung über Freigabeterminal (DoT-Anlagen)

3.6.7.1 DoT-Anlage mit FGT und Gültigkeitsverlängerung

In Data on Transponder-Anlagen (DoT), die mit Freigabeterminals (FGT) betrieben werden, ist die Verwendung der relativen Gültigkeit der Transponder eine Praktik, die Türen und den BKS Key-Manager über eine regelmäßige Datenübertragung zu vernetzen. Gegenüber Onlinesystemen mit direkter Vernetzung durch Verkabelung und Funkverbindung werden die Daten z. B. Änderungen der Berechtigungen automatisch an das FGT übertragen und der Transponder wird zum Überträger beim weiteren Zusammenspiel der Komponenten der Schließanlage.

Damit eine regelmäßige Datenübertragung ohne eine direkte Vernetzung gewährleistet ist, verlieren die Transponder nach Ablauf der Gültigkeit ihre Berechtigungen, wodurch sie gezwungen sind, kontinuierlich über das Aufsuchen eines FGTs die Gültigkeit zu verlängern. Mit jeder Gültigkeitsverlängerung am FGT werden die aktuellen Programmierdaten an die Transponder übertragen. Während der Begehung der Schließanlage übertragen die Transponder auf diesem Weg die Daten zu den Türen. Die Daten aus den Türen werden auf selben Weg zurück zur Quittierung übertragen.

Wurde die Gültigkeitsverlängerung mithilfe der FGTs aktiviert, muss die Gültigkeit der Transponder nach dem Ende des festgelegten Zeitraums verlängert werden. Dieser Zeitraum wird über die Anzahl an Tagen bis zum Ablauf der Gültigkeit und der Uhrzeit am Tag des Ablaufens festgelegt. Der Transponder verliert nach Ablauf der Gültigkeit automatisch alle Zutrittsberechtigungen. Durch das Einbuchen an einem FGT wird der Zeitraum neu gestartet und der Transponder erlangt seine Gültigkeit und die Zutrittsberechtigungen zurück.

Die Verwendung der relativen Gültigkeit ist besonders wie oben beschrieben in Verbindung mit einem FGT geeignet. Eine aufwendigere Möglichkeit ist, die Gültigkeit des Transponders mit dem Programmiergerät zu verlängern. Diese Möglichkeit sollte aber nur als Provisorium genutzt werden.

In Ihrer Schließanlage können Sie spezielle Türen von der relativen Gültigkeit ausschließen. Ein Transponder mit abgelaufener Gültigkeit hat dann trotz abgelaufener Gültigkeit zu dieser speziellen Tür eine Zutrittsberechtigung, wenn vor Ablauf der Gültigkeit eine Berechtigung bestanden hat. Über die Funktion „Transpondergültigkeit ignorieren“ im Kapitel 4.3.1 [202] kann eine Tür von der Regel der Gültigkeitsverlängerung ausgenommen werden. So können Sie eine Tür, die sich räumlich vor dem FGT befindet wie z. B. eine Schranke, die außerhalb vor dem FGT des Haupteingangs liegt, trotzdem passierbar machen.

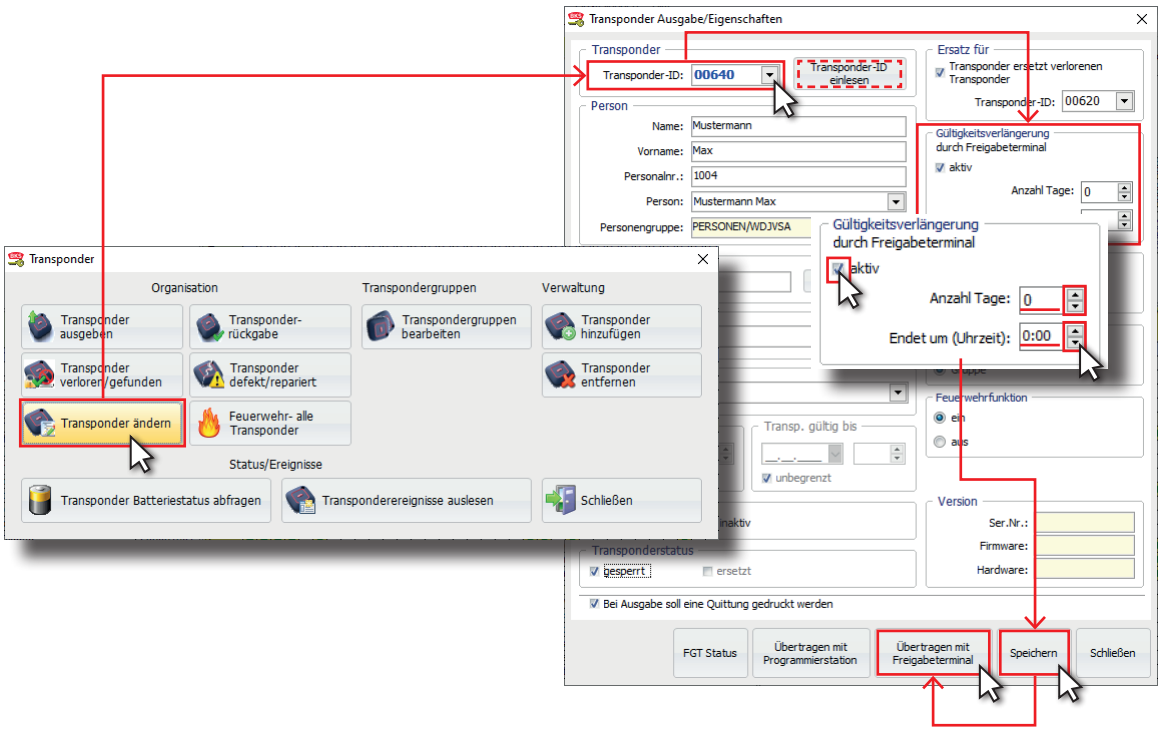
Bei Verlust eines Transponders ist abzuwägen, ob der Aufwand für das Programmieren einer Sperre in allen Türen mit Zutrittsberechtigung gerechtfertigt ist oder ob es für die Sicherheit ausreichend ist, dass der verlorene Transponder nur noch den restlichen Gültigkeitszeitraum berechtigt ist. Ein verlorener Transponder kann durch das Auslaufen lassen der Gültigkeit gesperrt werden. Hierbei ist abzuwägen, ob die Anlagensicherheit nicht gefährdet wird, wenn der verlorene Transponder den restlichen Gültigkeitszeitraum eine Zutrittsberechtigung hat. Dabei ist zu beachten, dass die Möglichkeit der Verlängerung des Gültigkeitszeitraums in der Berechtigungsmatrix durch das Sperren des Transponders auszuschließen ist.

3.6.7.2 Gültigkeitsverlängerung aktivieren

Zur Aktivierung dieser Funktion folgen Sie den weiteren Schritten dieses Abschnitts.

- Drücken Sie in der Berechtigungsmatrix auf den Menüpunkt „Transponder“ und im Weiteren den Button „Transponder ändern“ oder „Transponder ausgeben“.
- Wählen Sie im Dropdown-Menü den gewünschten Transponder aus. Alternativ können Sie den Transponder mit dem Programmiergerät einlesen.
- Aktivieren Sie die Checkbox „aktiv“ im Feld „Gültigkeitsverlängerung durch Freigabeterminal“.
- Legen Sie den Zeitraum fest, nachdem die Gültigkeit abläuft und der Transponder seine Gültigkeit verlieren soll.
  Im Feld „Anzahl der Tage“ geben Sie die Zeitspanne ein und
  im Feld „Endet um (Uhrzeit)“ einen Zeitpunkt am Tag des Ablaufens.
  Die Eingabe ist über das Textfeld oder über die Tasten rechts neben dem Textfeld möglich.
- Drücken Sie auf den Button „Speichern“.
- Drücken Sie auf den Button „Übertragen mit Freigabeterminal“.

Alternativ ist auch eine manuelle Übertragung der Daten auf den Transponder über den Button „Übertragen mit Programmierstation“ direkt vor Ort möglich, z. B. im Rahmen der Einrichtung und Ausgabe eines neuen Transponders.



3.6.7.3 Status der Gültigkeitsverlängerung in Berechtigungsmatrix

In der Berechtigungsmatrix wird nach dem Start der Übertragung zum Freigabeterminal (FGT) der aktuelle Status der Übertragung durch eine Meldung angezeigt. Mit folgenden Statusmeldungen wird der Fortschritt der Übertragung angezeigt.
(Abbildungen des Status zur Vereinfachung ohne Batterieanzeige)

Anzeige eines **neutralen Transponderstatus**, hier z. B. von einem Neuen oder ordnungsgemäß quittierten Transponder.
→Gültigkeitsverlängerung aktivieren und Zeitraum vergeben sowie speichern.

N

Nach dem **Speichern der Gültigkeitsverlängerung** im Fenster „Transponder Ausgabe/Eigenschaften“ wird der Status durch ein „N“ auf gelben Hintergrund symbolisiert.
→Starten der Übertragung zum Freigabeterminal.

O

Während der **Übertragung** der Daten vom BKS KeyManager **zum Freigabeterminal** wird der Status durch ein „O“ auf grünem Hintergrund symbolisiert.
→Übertragung ggf. abwarten.

S

Ist die **Übertragung zum Freigabeterminal abgeschlossen**, wird der Status durch ein „S“ auf grünem Hintergrund symbolisiert.
→Die Daten stehen jetzt zur Abholung durch den Transponder bereit.

Zur **Programmierung** vom **Transponder** wird der geänderte Transponder am FGT eingebucht. Die Daten werden vom FGT zum Transponder übertragen. Der Status wird nur durch einen grauen Hintergrund nach erfolgreicher Übertragung symbolisiert.
→Im Transponder ist die Gültigkeitsverlängerung aktiviert und der Transponder verliert ohne erneute verlängernde Programmierung nach Ablauf des Zeitraums seine Gültigkeit.

Wenn der Speicher im FGT nicht mehr ausreicht, um die Programmierinformation abzulegen, werden die Daten im Direktmodus übertragen. Dies bedeutet, dass die Programmierdaten ohne Zwischenspeicherung zum FGT übertragen werden. Die Übertragung startet in diesem Fall erst, wenn der Transponder am FGT gebucht wird und sich in Kommunikation mit dem FGT befindet.

D

Nach dem Speichern wird der **Direktmodus** durch die Statusmeldung „D“ angezeigt.
→Die Daten stehen im BKS KeyManager zur Abholung durch den Transponder am FGT bereit.

Zur **Programmierung** vom **Transponder** wird der geänderte Transponder am FGT eingebucht. Die Daten werden vom BKS KeyManager über das FGT zum Transponder übertragen. Der Status wird nur durch einen grauen Hintergrund nach erfolgreicher Übertragung symbolisiert.
→Im Transponder ist die Gültigkeitsverlängerung aktiviert.

3.6.8 Zutrittsberechtigung entziehen/sperren

Die über den BKS KeyManager erteilten Zutrittsberechtigungen der Personen bzw. deren Transponder zu den Türen können über verschiedene Funktionen diesen wieder entzogen werden.

Dabei können die Zutrittsberechtigungen zu den Türen der Schließanlage über verschiedene Funktionen wieder entzogen werden. Für die Auswahl der richtigen Funktion beachten Sie die folgenden Kapitel dieses Abschnitts.

Auch ist bei der Umsetzung zu beachten, dass nicht nur in der Matrix die Sperre verhängt wird, sondern auch eine Übertragung zu den Zutrittspunkten der Schließanlage stattfindet. Erst danach ist die Sperre wirksam.

HINWEIS

Wird ein Transponder über eine dieser Funktionen gesperrt, dann hat dies die Programmierung der betroffenen Zutrittspunkte zur Folge. Ein nur in der Matrix gesperrter Transponder kann die Türen weiterhin öffnen (Ausnahme bilden eine Online-Anlage oder die Funktion „Ersatz für“ in Verbindung mit einer DoT-Anlage mit EBK).

Der Aufwand der Programmierung kann je nach Größe der Schließanlage und Anzahl der betroffenen Teile der Anlage stark variieren. Das Sperren einer Zutrittsberechtigung von einem Transponder für eine Tür erzeugt einen vergleichsweise geringen Aufwand gegenüber dem Verlust eines Transponders mit einer GHS-Gruppenberechtigung. Letztere hat Zutritt zu allen Türen, wodurch zum Sperren des Transponders alle Türen programmiert werden müssen.

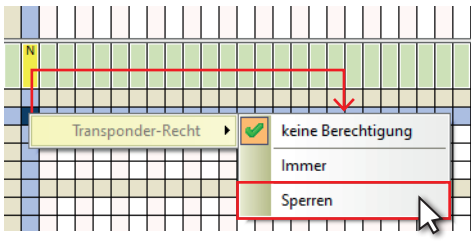
Im Detail können Sie eine Sperre für Transponder oder deren Gruppen zu einer Tür über die Berechtigungsmatrix oder für alle Türen eines Transponders über das Menü Transponder einrichten. Folgen Sie der Beschreibung der weiteren Kapitel dieses Abschnitts.

3.6.8.1 Sperren über die Berechtigungsmatrix

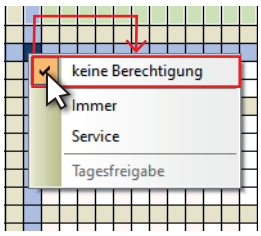
Diese Funktionalität der Berechtigungsmatrix dient zum Sperren der Berechtigung eines Transponders oder einer Gruppe zu einer Tür und kann gezielt eine Berechtigung zu entziehen.

- Sperren der Berechtigung einer Transpondergruppe zur Tür
  - Folgen Sie der Anleitung im Kapitel 3.6.3 [112]
  - Auswahl von „Sperren“ bzw. „keine Berechtigung“ im Quadrat des Schnittpunkts Transpondergruppe/Tür sperrt alle Transponder der Gruppe, ausgenommen sind Transponder mit einer vorhandenen Einzelberechtigung
  - Transponder der Gruppe mit einer Einzelberechtigung können wie im nächsten Punkt beschrieben gesperrt werden
- Sperren der Einzelberechtigung eines Transponders zu einer Tür
  - Folgen Sie der Anleitung im Kapitel 3.6.4 [117]
  - Auswahl von „keine Berechtigung“ im Quadrat des Schnittpunkts Transponder/Tür sperrt den Transponder, ausgenommen sind Transponder in einer DoT-Anlage mit einem vorhandenen Transpondergruppenrecht
  - Bei einem vorhandenen Transpondergruppenrecht wird durch Auswahl von „Sperren“ im Quadrat des Schnittpunkts Transponder/Tür der Transponder in DoT-Anlagen gesperrt

[DoT]

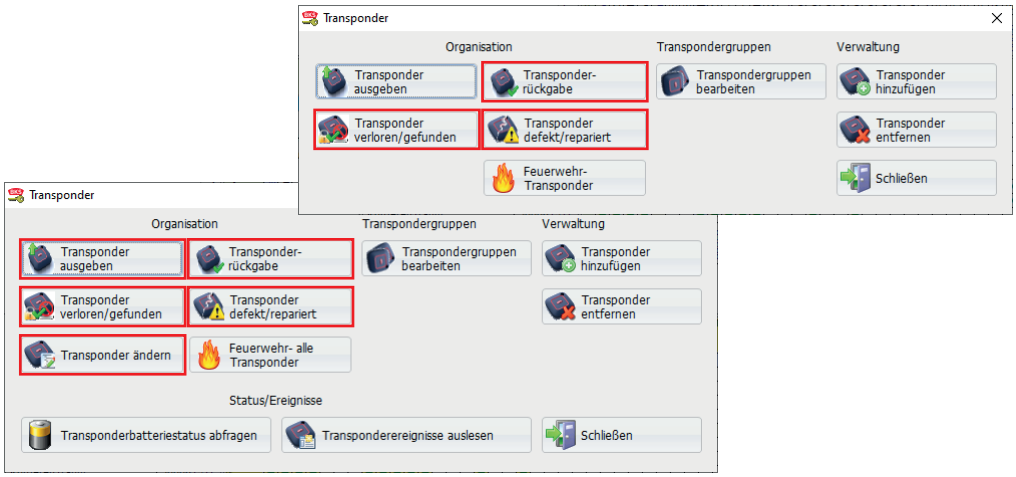


[nonDot]



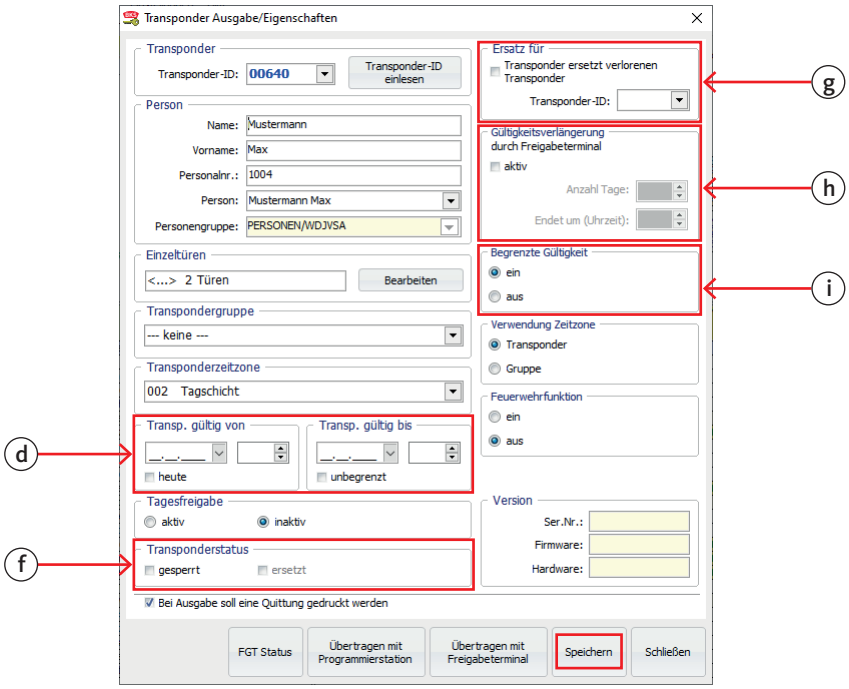
3.6.8.2 Sperren über das Menü Transponder

Die Menüpunkte des Transpondermenüs können zum Sperren aller Zutrittsberechtigungen eines gewählten Transponders genutzt werden, siehe Kapitel 4.2 [160]. Dadurch ist es Ihnen möglich, z. B. bei Verlust, Defekt oder Austausch eines Transponders etc., diesem Transponder alle Zutrittsberechtigungen in der Anlage zu entziehen.

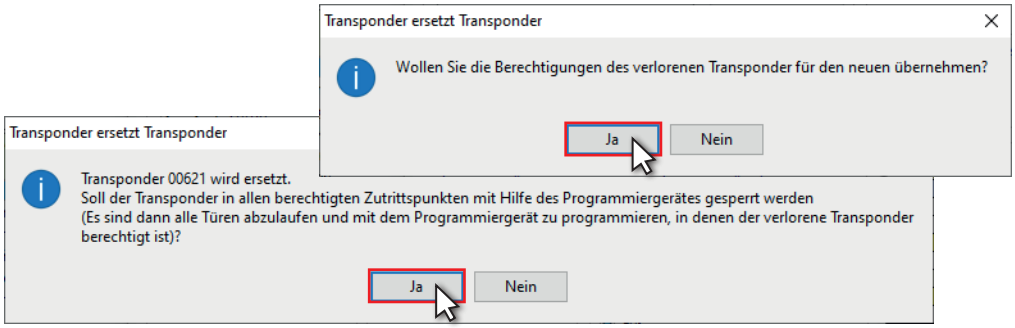


- Menüpunkt „Transponder verloren/gefunden“
  - Folgen Sie der Anleitung im Kapitel 4.2.4 [177], um den Transponders als Verloren zu kennzeichnen
  - Sperren Sie die Zutrittsberechtigungen des verlorenen Transponders wie in Kapitel 4.2.4.2 [178] beschrieben
- Menüpunkt „Transponder defekt/repariert“
  - Folgen Sie der Anleitung im Kapitel 4.2.5 [181] und Kennzeichnen den Transponder als Defekt
  - Aktivieren Sie die Checkbox im Fenster bzw. Dialog „Wollen Sie dem Transponder sperren?“ zum Sperren aller Zutrittsberechtigungen des Transponders
- Menüpunkt „Tranponderrückgabe“
  - Folgen Sie der Anleitung im Kapitel 4.2.3 [175] zur Rückgabe des Transponders
  - Aktivieren Sie die Checkbox „Berechtigungen bei Rückgabe Löschen“ im Fenster „Transponderrückgabe“ zum Sperren aller Zutrittsberechtigungen des Transponders

Die folgenden Einstellungen sind nur in einer Data on Transponder-Anlage (DoT) möglich.



- Ersetzen eines Transponders durch einen anderen Transponder und Sperrung des ersetzten Transponders → Menüpunkt „Transponder ausgeben“ oder „Transponder ändern“ (nur bei DoT-Anlagen)
  - Folgen Sie der Anleitung im Kapitel 4.2.2 [164] zum Ersetzen und Sperren des Transponders
  - Aktivieren Sie im Feld (g) „Ersatz für“ die Checkbox „Transponder ersetzt verlorenen Transponder“
  - Wählen Sie im Feld „Ersatz für“ über das Dropdown-Menü „Transponder-ID“ den zu ersetzenden Transponder aus
  - Drücken Sie auf den Button „Speichern“
  - Drücken Sie im nächsten Fenster auf den Button „Ja“, damit alle Zutrittspunkte, in denen der zu ersetzende Transponder eine Zutrittsberechtigung hat, für diesen gesperrt werden
  - Im darauf folgenden Fenster können Sie die Berechtigungen durch Drücken auf Button „Ja“ für den neuen Transponder übernehmen.



- Zeitraum festlegen, nach der die Gültigkeit verlängert werden muss. Erfolgt keine Verlängerung, wird der Transponder gesperrt → Menüpunkt „Transponder ausgeben“ oder „Transponder ändern“ (nur bei DoT-Anlagen)
  - Folgen Sie der Anleitung im Kapitel 3.6.7 [135]
  - Aktivieren Sie im Feld (h) „Gültigkeitsverlängerung durch Freigabeterminal“ die Checkbox „aktiv“
  - Geben Sie den Zeitraum, nach dem der Transponder gesperrt werden soll, in die Felder „Anzahl der Tage“ und „Endet um (Uhrzeit)“ ein
  - Eine Gültigkeitsverlängerung ist durch eine Programmierung der Transponder mit dem Programmiergerät möglich, aber umständlicher als bei Verwendung eines Freigabeterminals
- Start und Ende der Gültigkeit festlegen, außerhalb dieses Zeitraums oder Zeitpunkts ist der Transponder gesperrt → Menüpunkt „Transponder ausgeben“ oder „Transponder ändern“ (nur bei DoT-Anlagen)
  - Folgen Sie der Anleitung im Kapitel 4.2.2 [164]
  - Aktivieren Sie im Feld (i) „Begrenzte Gültigkeit“ die Checkbox „ein“
  - Geben Sie einen Zeitpunkt im Feld „Transp. gültig bis“ ein, nachdem der Transponder gesperrt sein soll
  - Geben Sie einen Zeitpunkt im Feld „Transp. gültig von“ ein, vor dem der Transponder gesperrt sein soll
- Transponder über den Transponderstatus in den Zustand gesperrt versetzen → Menüpunkt „Transponder ausgeben“ oder „Transponder ändern“ (nur bei DoT-Anlagen)
  - Folgen Sie der Anleitung im Kapitel 4.2.2 [164] zum Sperren aller Berechtigungen
  - Aktivieren Sie im Feld (f) „Transponderstatus“ die Checkbox „gesperrt“ um den Transponder zu sperren

3.6.8.3 Sperren und Ersetzen mit einem anderen Transponder (DoT)

In Data on Transponder-Anlagen (DoT) mit Freigabeterminal verfügt die Funktion „Ersatz für“ eine zusätzliche Erweiterung. Es besteht die Möglichkeit, dass Sie in Ihrer Schließanlage einen Transponder durch einen anderen Transponder ersetzen können und den Ersatztransponder so zu programmieren, dass dieser beim Begehen der Türen eine Sperre für die Zutrittsberechtigung des ersetzten Transponders in die Türen programmiert.

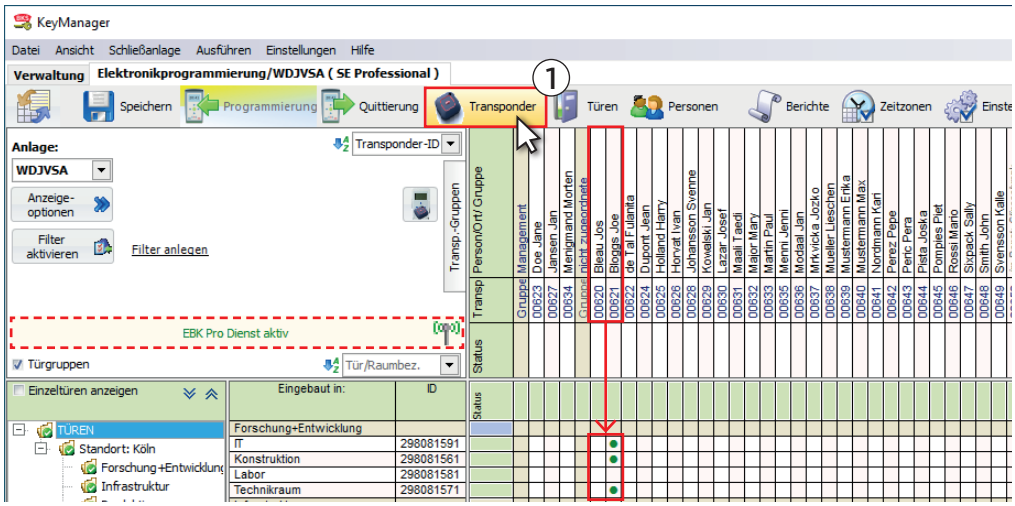
Die Programmierung des neuen Transponders kann beim Eintritt durch das Einbuchen an einem Freigabeterminal erfolgen. Der Transponder bzw. dessen Person sperrt durch das normale Begehen der Zutrittspunkte den ersetzten Transponder. Das aufwendige Ablaufen der Türen mit einem Programmiergerät durch die Benutzer des BKS KeyManagers kann dadurch entfallen. Schlecht besuchte oder sicherheitsrelevante Türen sollten aber protokolliert mit dem Programmiergerät gesperrt werden. Der ersetzte Transponder könnte sonst ohne die Programmierung der Sperre in den Türen diese weiterhin öffnen.

HINWEIS **Dieser Funktion steht nur bei einer Data on Transponder-Anlage (DoT) zur Verfügung.**

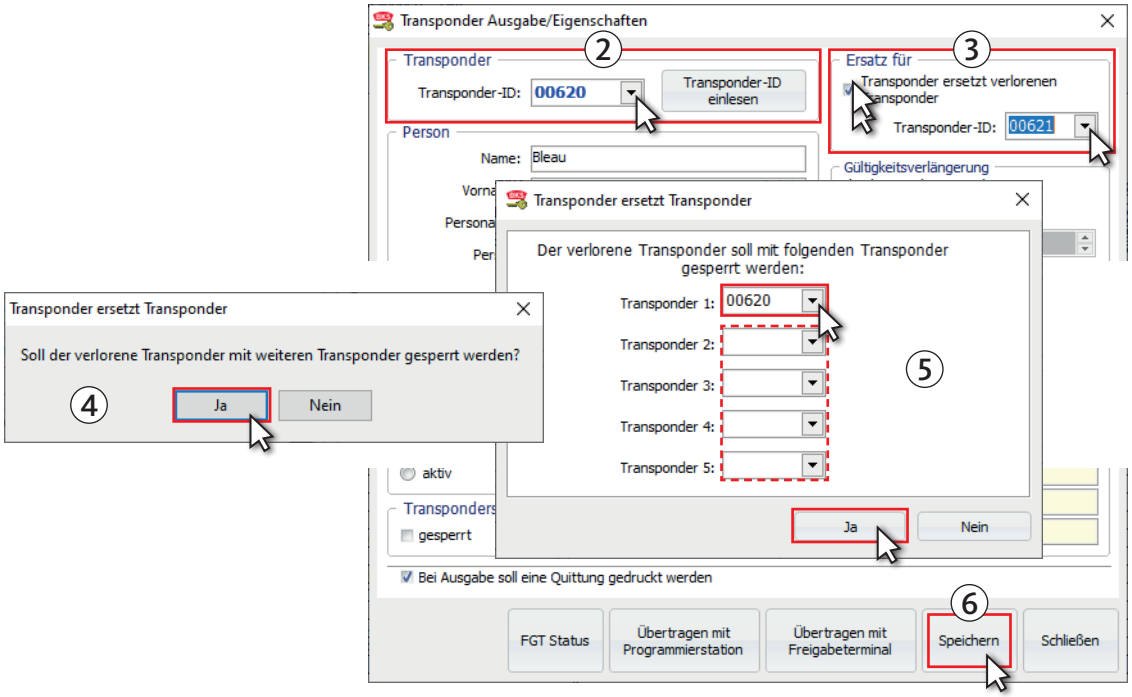
Mit der Funktion „Ersatz für“ können Sie den ersetzten Transponder sperren und in der Matrix als „Ersetzt“ kennzeichnen. Dem neuen Transponder können Sie die Berechtigungen des ersetzten zuweisen und wie ober beschrieben zum Sperren der Zutrittsberechtigungen verwenden.

Zum Ersetzen eines z. B. verlorenen Transponders durch einen Neuen, der diesen auch sperrt, folgen Sie der Beschreibung.

- (1) Drücken Sie auf die Schaltfläche Transponder im Menü und öffnen das Fenster „Transponder“
- Öffnen Sie durch Drücken auf die Menüpunkte „Transponder ausgeben“ oder „Transponder ändern“ das Fenster „Transponder Ausgabe/Eigenschaften“
  (ohne Abbildung beachten Sie hierzu die Anleitung im Kapitel 4.2.2 [164] bzw. 4.2.8 [189]).

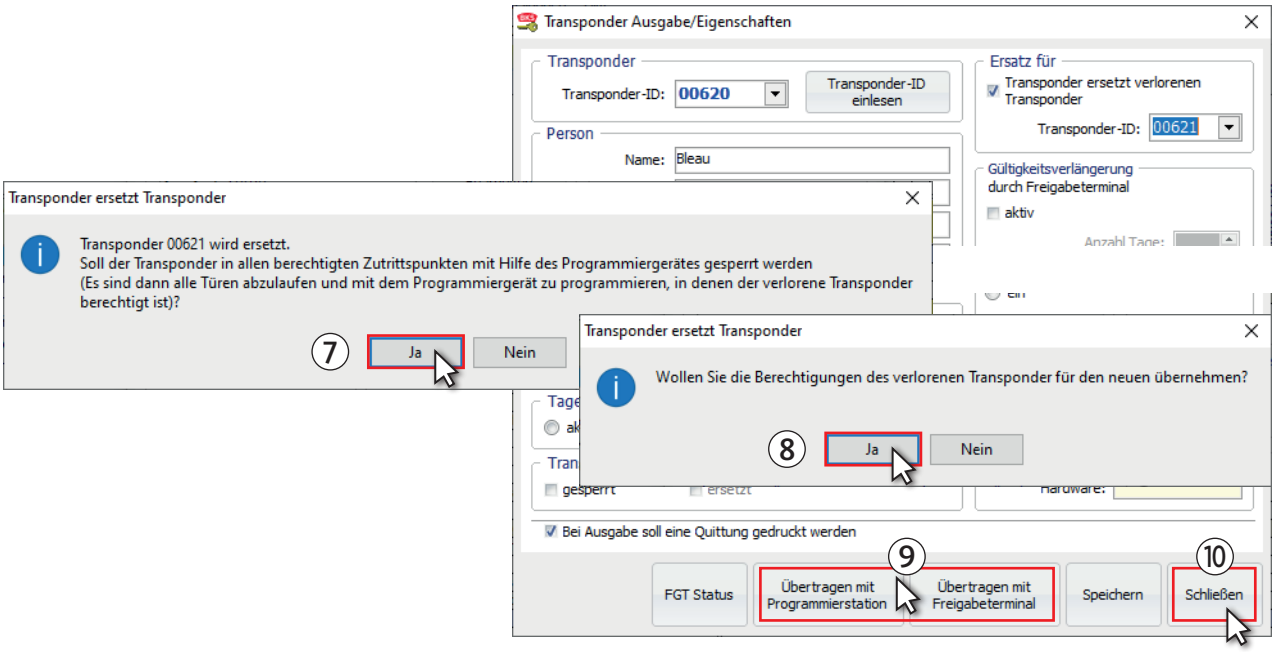


- (2) Wählen Sie im Dropdown-Menü den für den Ersatz vorgesehenen oder neuen Transponder aus. Alternativ können Sie auch über den Button „Transponder-ID einlesen“ den Transponder mit dem Programmiergerät einlesen.
- (3) Aktivieren Sie im Feld „Ersatz für“ die Checkbox „Transponder ersetzt verlorenen Transponder“ und wählen anschließend im Dropdown-Menü „Transponder ID“ den Transponder aus, der ersetzt werden soll.
- (4) Drücken Sie auf den Button „Ja“; um weitere Transponder auszuwählen; mit denen der zu ersetzende Transponder gesperrt werden soll. Drücken Sie auf den Button „Nein“, wenn nur mit dem gewählten Transponder gesperrt werden soll.
- (5) Wählen Sie in den fünf Dropdown-Menüs jeweils einen Transponder aus, mit denen die Zutrittsberechtigungen des zu ersetzenden Transponders gesperrt werden sollen.
- (6) Drücken Sie auf den Button „Speichern“.

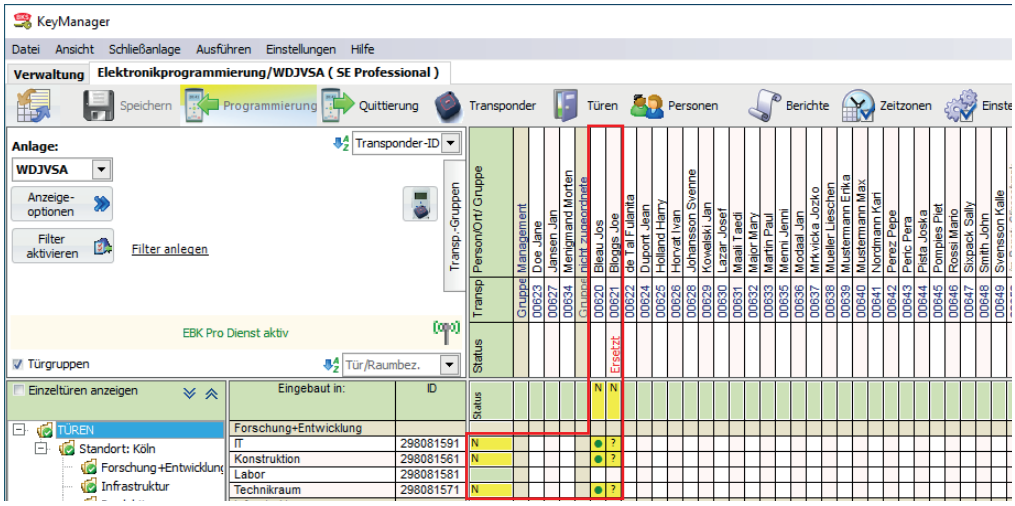


- (7) Drücken Sie auf den Button „Ja“, um zusätzlich einen Programmierauftrag zu generieren. Die Sperrung wird nochmals beim nächsten Ablaufen der zu sperrenden Türen protokolliert zu den Türen übertragen. Über die Quittierung wird sichergestellt, dass keine Tür vergessen wurde zu programmieren. Alternativ können Sie auf das Ablaufen mit dem Programmiergerät verzichten, indem Sie auf den Button „Nein“ drücken und die Programmierung nur über die gewählten Transponder übertragen lassen.

- (8) Zur Übernahme der Berechtigungen des ersetzten Transponders auf den Neuen drücken Sie auf den Button „Ja“. Beim Übernehmen werden die vorhandenen Berechtigungen gelöscht. Soll der neue Transponder seine Berechtigungen behalten, dann drücken Sie auf den Button „Nein“.
- (9) Drücken Sie auf den Button „Übertragen mit Freigabeterminal“, um die Programmierdaten an die Freigabeterminals zu übermitteln. Bei der nächsten Präsentation eines gewählten Transponders wird dieser programmiert. Öffnen Sie mit diesem Transponder die Türen, werden diese gleichzeitig für den ersetzten Transponder gesperrt. Alternativ können Sie auf den Button „Übertragen mit Programmierstation“ drücken, um das Programmiergerät zu verwenden.
- (10) Drücken Sie auf den Button „Schließen“.



Der Status des ersetzten Transponders und seiner Berechtigungen wurden auf „Ersetzt“ und „?“ gesetzt. In diesem Beispiel sind die Berechtigungen an den neuen Transponder vom Ersetzten übernommen worden.

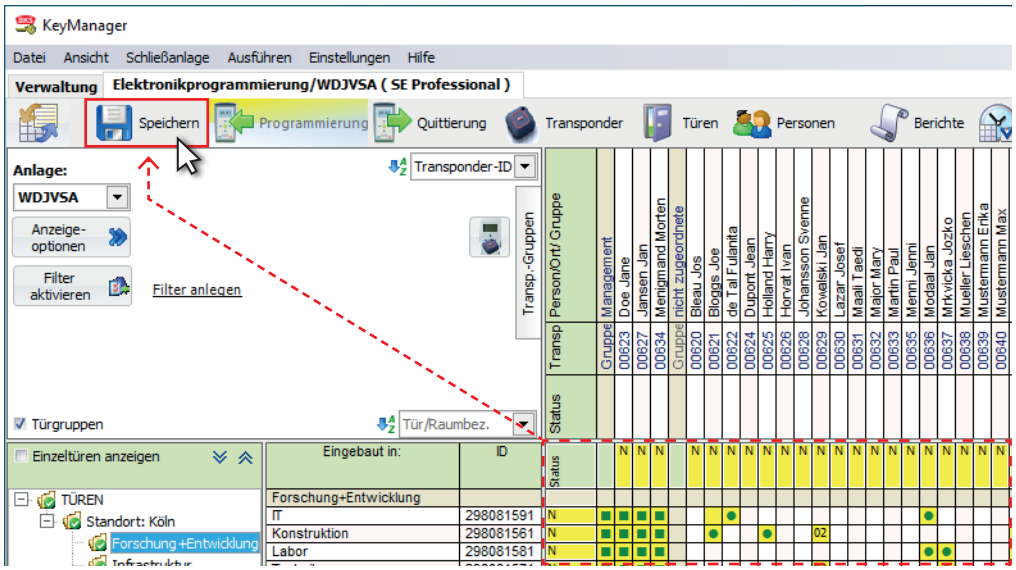


3.7 Speichern

Nach der Vergabe der Zutrittsberechtigungen, bevor Sie im nächsten Schritt die Rechte an die Transponder und Zutrittspunkte übermitteln, ist die Matrix in der Datenbank zu speichern. Nach dem Speichern wird der Button ausgegraut und ist bis eine neue Änderung in der Matrix vorgenommen wurde nicht auswählbar.

Je nach Aufwand und Dauer der Berechtigungsvergabe ist es ratsam, während der Überarbeitung sowie nach Abschluss der Arbeiten die Berechtigungsmatrix durch Speichern in die Datenbank zu übernehmen. Dieses gilt im Besondern bei der Arbeit an Client-Arbeitsplätzen, um möglichen Datenverlusten z. B. durch Netzwerkprobleme vorzubeugen.

- Drücken Sie auf den Button „Speichern“.



- Fahren Sie mit der Programmierung der Komponenten und Übertragung der Änderungen, die Sie in der Berechtigungsmatrix vorgenommen haben, fort.

In **Data on Transponder Anlagen (DoT) mit Freigabeterminals (FGT)** und in **Online-Anlagen** wird je nach Einrichtung beim Speichern eine manuelle oder automatische Übertragung der Daten zu den FGTs und/oder zu den online Zutrittspunkten gestartet.

Eine Programmierung und Quittierung mit dem Programmiergerät der in der Berechtigungsmatrix geänderten Daten ist dadurch bei diesen beiden Anlagentypen nicht notwendig.

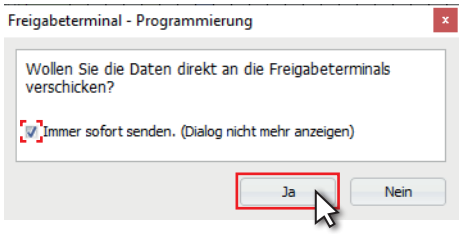
3.7.1 Speichern in DoT-Anlagen mit FGTs und Übertragung der Daten

In Data on Transponder-Anlagen (DoT) mit Freigabeterminals (FGT) werden Sie nach dem Drücken des Buttons „Speichern“ in einem Dialog gefragt, ob die Daten zu den verbundenen FGTs übertragen werden sollen. Die eigentliche Programmierung der Transponder wird nach diesem Schritt beim Einbuchen des Transponders am FGT vollzogen. Die Programmierung der Transponder durch das Programmiergerät ist dadurch nicht erforderlich.

Das Fenster „Freigabeterminal - Programmierung“ öffnet sich initial beim Speichern oder falls keine automatische Übertragung gewünscht wird bei jedem Speichern.

- Aktivieren Sie die Checkbox „Immer sofort senden“, wenn Sie eine automatische Übertragung der Daten zu den FGTs beim Speichern wünschen. Das Fenster wird nach Aktivierung beim Speichern nicht mehr angezeigt.
- Drücken Sie auf den Button „Ja“ um die Übertragung zu den FGTs zu starten.

Wenn Sie eine Übertragung der Daten zu einem späteren Zeitpunkt wünschen, drücken Sie auf den Button „Nein“.



Durch die Übertragung wechselt die Anzeige des Status in den Zeilen- und Spaltenüberschriften der Berechtigungsmatrix, siehe Kapitel 3.5.5 [90].

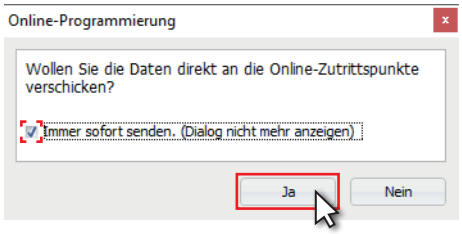
3.7.2 Speichern in Online-Anlagen und Übertragung der Daten

In Online-Anlagen können Sie optional die Daten durch Drücken auf den Button „Speichern“ automatisch im Hintergrund zu den mit dem BKS KeyManager online verbundenen Türen übertragen.

Das Fenster „Online-Programmierung“ öffnet sich initial beim Speichern oder falls keine automatische Übertragung gewünscht wird bei jedem Speichern.

- Aktivieren Sie die Checkbox „Immer sofort senden“, wenn Sie eine automatische Übertragung der Daten zu den Türen beim Speichern wünschen. Das Fenster wird nach Aktivierung beim Speichern nicht mehr angezeigt.
- Drücken Sie auf den Button „Ja“ um die Übertragung zu den online verbundenen Türen zu starten.

Wenn Sie eine Übertragung der Daten zu einem späteren Zeitpunkt wünschen, drücken Sie auf den Button „Nein“.



Eine Programmierung der Online-Türen mit dem Programmiergerät ist dadurch nicht erforderlich. Durch die Übertragung wechselt die Anzeige des Status in den Zeilen- und Spaltenüberschriften der Berechtigungsmatrix, siehe Kapitel 3.5.5 [90].

3.8 Programmierung

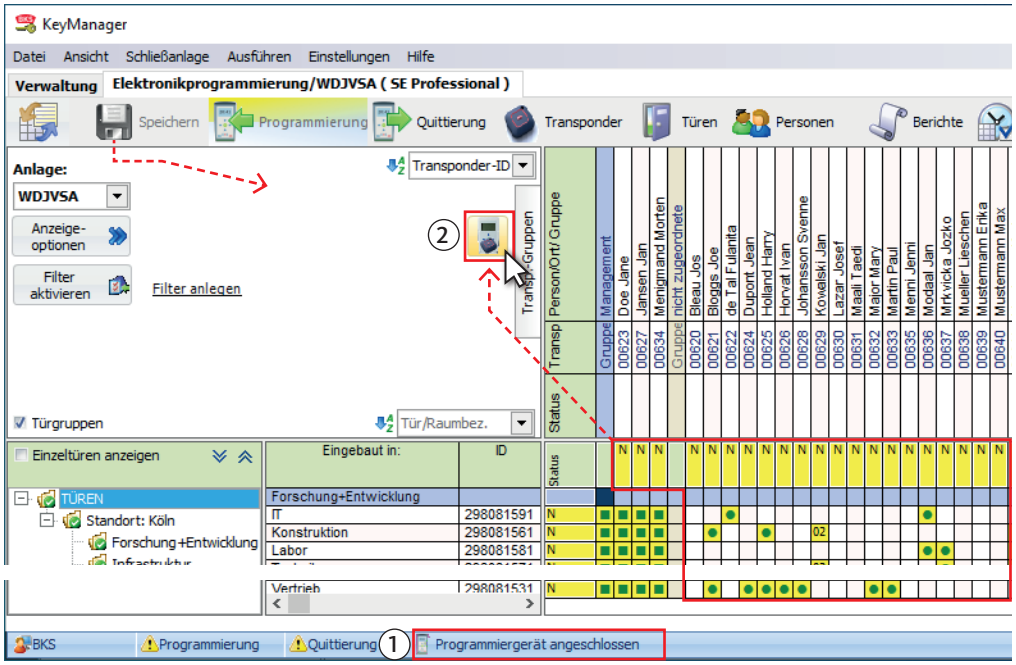
3.8.1 Programmierung der Transponder (DoT-Anlagen)

Die den Transponder betreffenden Einstellungen und Änderungen in der Berechtigungsmatrix müssen bei Data on Transponder-Anlagen (DoT-Anlagen) auf den Transponder programmiert werden. Die Programmierung kann direkt in der Matrix über den Button (2) gestartet werden. Zur Übertragung ist ein verbundenes Programmiergerät notwendig.

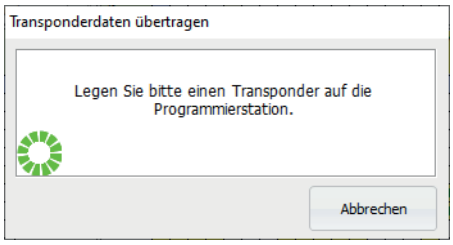
Alternativ kann die Programmierung der Transponder auch über das Menü „Transponder“ gestartet werden, siehe Kapitel 4.2.2 [164].

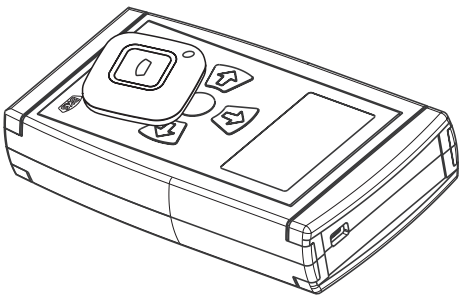
Die Transponder können auch optional über ein Freigabeterminal (FGT) programmiert werden. Hierzu ist eine entsprechende Online-Konfiguration erforderlich, siehe Kapitel 5.7 [293].

- Verbinden Sie das Programmiergerät und den Computer mit einem USB-Kabel und warten, bis die Verbindung bestätigt ist und das verbundene Programmiergerät in der Statuszeile angezeigt wird.
- Drücken Sie auf den Button (2) mit dem Symbol für das Einlesen mit dem Programmiergerät, um den Vorgang zu starten.



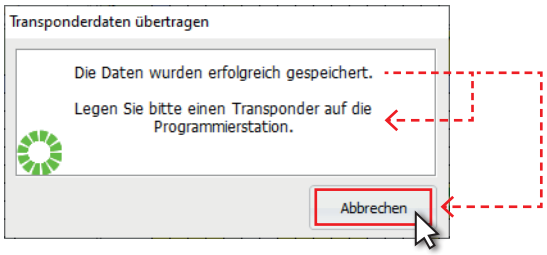
- Legen Sie den einzulesenden Transponder auf das Programmiergerät.



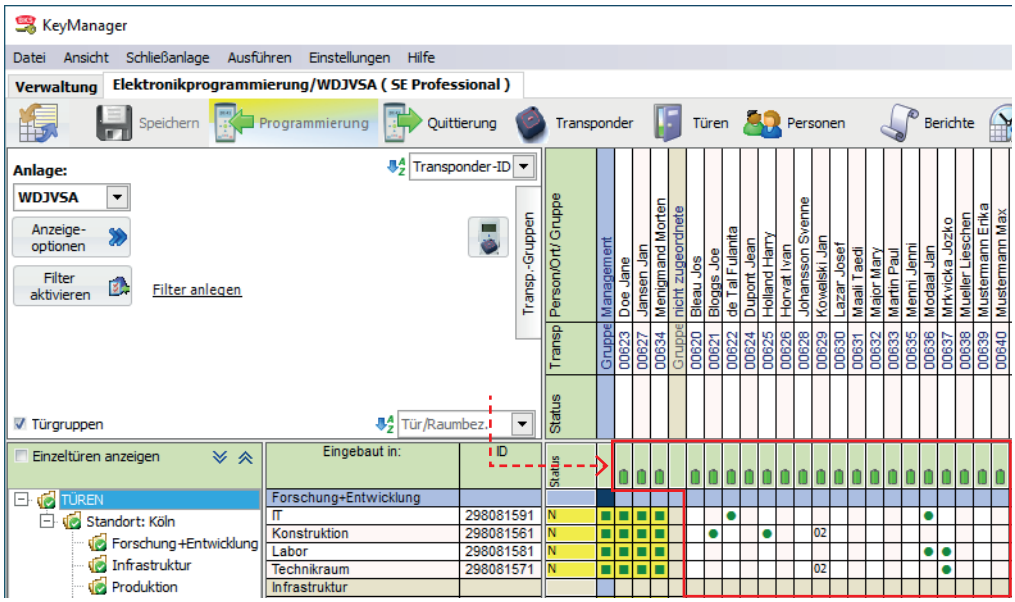


Die Daten werden zum Transponder übertragen und mit der Anzeige „Die Daten wurden erfolgreich gespeichert“ wird der Vorgang abgeschlossen. Entfernen Sie den Transponder nicht vom Programmiergerät, bis der Vorgang beendet ist. Sollte die Übertragung nach dem Auflegen des Transponders nicht starten, können Sie den Transponder mit einem Tastendruck aufwecken.

- Verwenden Sie weitere Transponder, legen Sie diese auf das Programmiergerät und wiederholen das Programmieren, bis auf allen Transponder die Daten übertragen worden sind.
- Drücken Sie auf den Button „Abbrechen“ zum Beenden.



Der Status der Transponder wechselt von der gelb unterlegten Kennzeichnung „N“ zu der grünen Spaltenanzeige für die erfolgreiche Programmierung und der Anzeige bzw. Aktualisierung des Ladezustands der Batterien des Transponders.



3.8.1.1 Programmierung der Transponder über FGT (DoT-Anlagen)

In Data on Transponder-Anlagen (DoT) mit Freigabeterminals (FGT) werden in der Regel die Daten beim „Speichern“ zu den verbundenen FGTs übertragen und die Transponder beim Einbuchen am FGT programmiert. Beachten Sie hierzu die Anleitung im Kapitel 3.7.1 [146].

Die Programmierung der Transponder mit dem Programmiergerät ist weiterhin möglich, aber durch die Übertragung über das FGT nicht erforderlich.

3.8.2 Programmierung der Transponder (nonDoT-Anlagen)

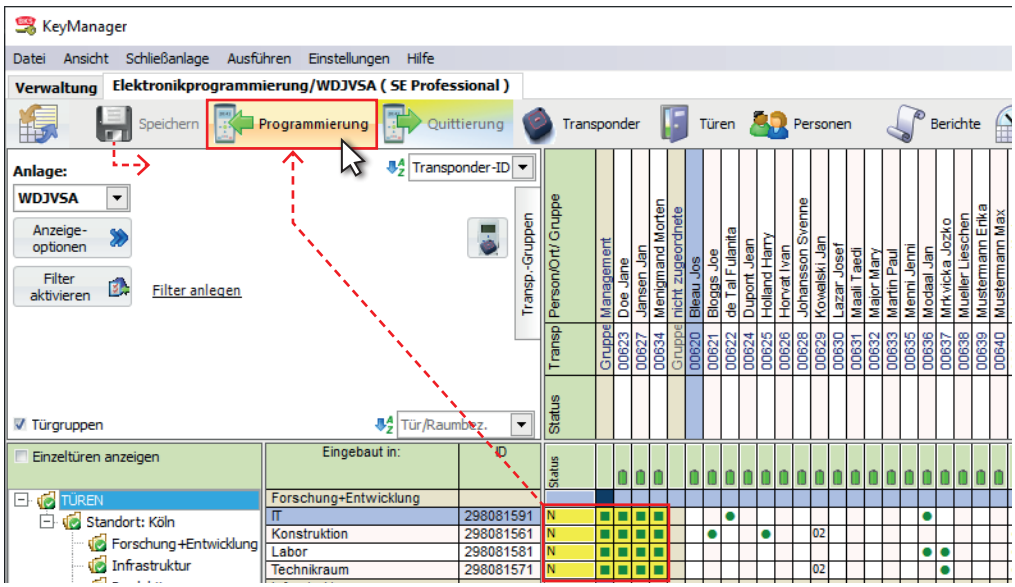
Eine Programmierung der Transponder in Online- und Offline-Schließanlagen (nonDoT) ist im Rahmen der Zutrittsberechtigung nicht möglich. Bei diesen Anlagen werden keine Berechtigungen auf dem Transponder gespeichert, wodurch die Programmierung entfällt.

Als Konsequenz ist eine Programmierung der Transponder nur bei der Funktion „Feuerwehrtransponder“ aus den Menüs der Grundfunktionen siehe Kapitel 4.2.9 [194] erforderlich.
Führen Sie die Programmierung im Rahmen dieser Funktionen aus.

3.8.3 Programmierung der Türen/Zutrittspunkte

Die geänderten Berechtigungen müssen auf ein Programmiergerät gespeichert werden, um auf die Zutrittspunkte übertragen zu werden.

- Drücken Sie auf den Button „Programmierung“ im Hauptmenü.



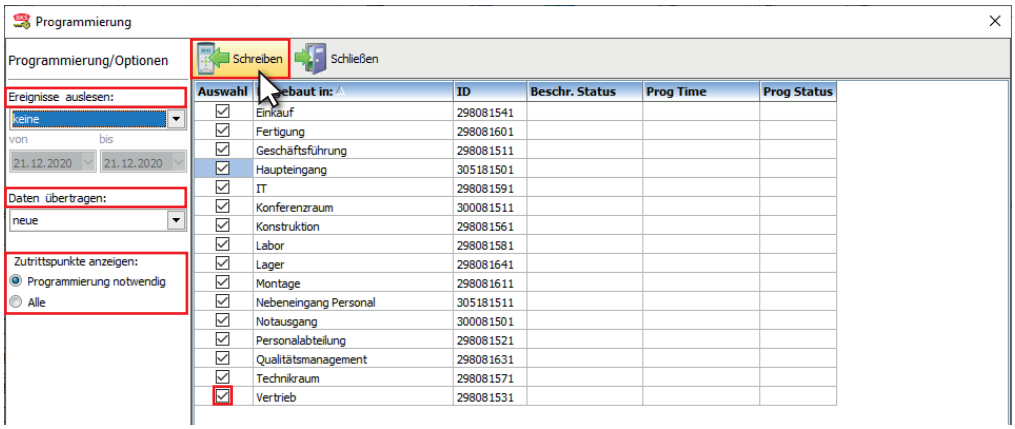
Im Fenster „Programmierung“ wird in Abhängigkeit der Einstellungen, eine Liste mit den zur Programmierung notwendigen Zutrittspunkten angezeigt. Über „Zutrittspunkte anzeigen“ können Sie Einstellen, dass entweder „Alle“ oder die zur „Programmierung notwendigen“ Zutrittspunkte angezeigt werden.

Optional ist es möglich, durch Deaktivierung der Checkbox bestimmte Zutrittspunkte bei der Übertragung auf das Programmiergerät auszulassen. Weitere Einschränkungen sind durch die Auswahl der Menüpunkte „Neue“, „Alle“ oder „für definierten Zeitraum“ unter den Dropdown-Menüs „Ereignisse auslesen“ und „Daten übertragen“ möglich.

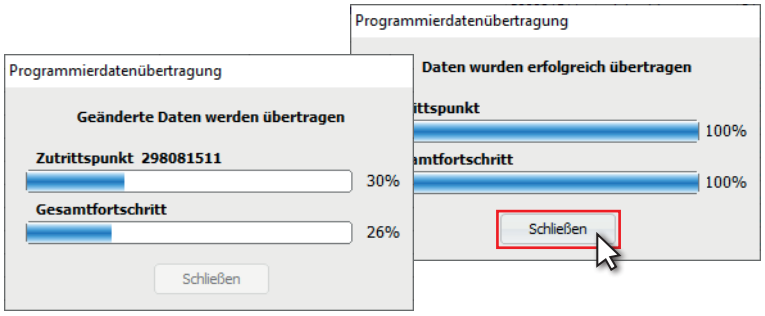
HINWEIS

Bei der ersten Programmierung während der Inbetriebnahme sind die Zutrittspunkte mit der Option „Alle“ bzw. allen Daten zu programmieren.

- Drücken Sie auf den Button „Schreiben“, um die Daten auf das angeschlossene Programmiergerät zu übertragen.



Die Daten werden auf das Programmiergerät übertragen.

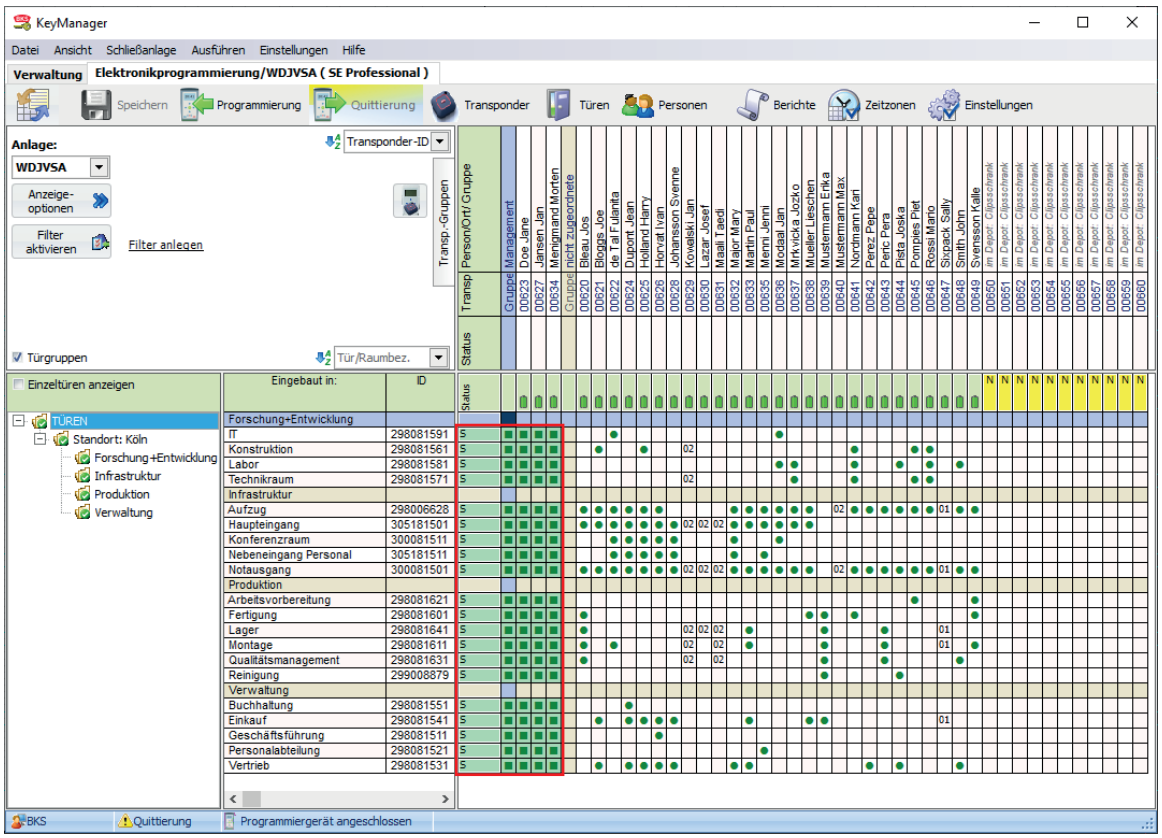


- Drücken Sie auf den Button „Schließen“ oder warten, bis sich nach wenigen Sekunden der Dialog schließt.

Der Status der Zutrittspunkte ist von „N“ auf „S“ gewechselt. Die Berechtigungen in der Berechtigungsmatrix sind von Gelb auf Grün gewechselt. Nach der Übertragung auf die Türen|Zutrittspunkte und der Quittierung am Computer wird der Status farblos für keine Programmierung erforderlich angezeigt.

In einer Online-Anlage wechselt der Status der Türen von Gelb auf farblos, wenn die Programmierung automatisch online übertragen wurde.

In Data on Transponder-Anlagen (DoT) sind die Einzelrechte an die Transponder gebunden und die Änderungen der Berechtigungen der Türen werden nicht programmiert. Allerdings müssen Türen, in denen Transpondergruppen berechtigt sind, programmiert werden. Der Status wechselt erst nachdem die Programmierdaten auf das Programmiergerät übertragen wurden, von Gelb auf Grün in der Matrix.



3.8.4 Türen mit Programmiergerät programmieren

Vor dem Programmieren empfiehlt es sich, eine Laufliste mit sämtlichen Türen, für die ein Programmierauftrag im Programmiergerät vorliegt, zu erstellen bzw. auszudrucken. Die Erstellung des Berichts „Laufliste“ wird im Kapitel 4.6.2 [231] beschrieben.

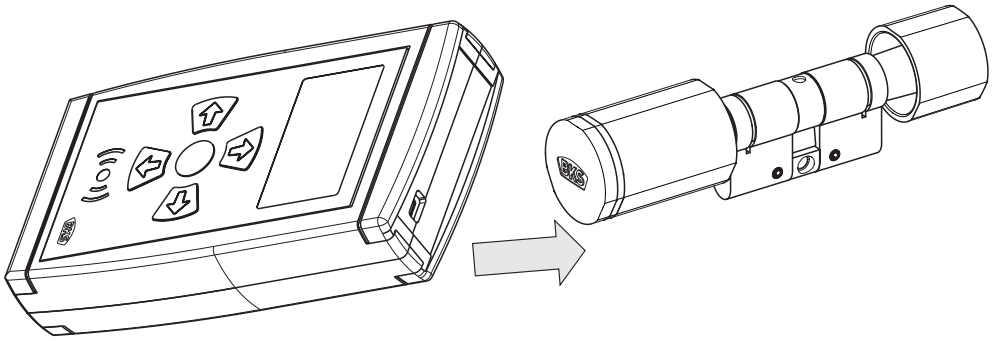
- Programmieren Sie die Zutrittspunkte.

Beim Programmiervorgang wird die Uhr des Zutrittspunkts mit der des Programmiergerätes synchronisiert.

HINWEIS

Wählen Sie im Menü Ihres Programmiergeräts den Punkt „SE“ -> „Programmieren“ aus. Halten Sie das Programmiergerät vor einen Zutrittspunkt z. B. einem Zylinder Ihrer Schließanlage. Nachdem die Programmierung abgeschlossen ist, können Sie den Vorgang an weiteren Zutrittspunkten wiederholen. Achten Sie darauf, dass unter dem Menüpunkt „SE“ -> „Anlage wählen“ im Programmiergerät die richtige Anlage ausgewählt ist.

```
WDJVSA        31.07 09:06
▶ Programmieren          >
  Zutrittspunkt-Info     >
  Karten/Tag-Info        >
  Anlage wählen          >
  Laufliste              >
  Ereignisse lesen
```



```
ID              300000014
Initialisierung        Ok
Berechtigungen         ⌛5%
```

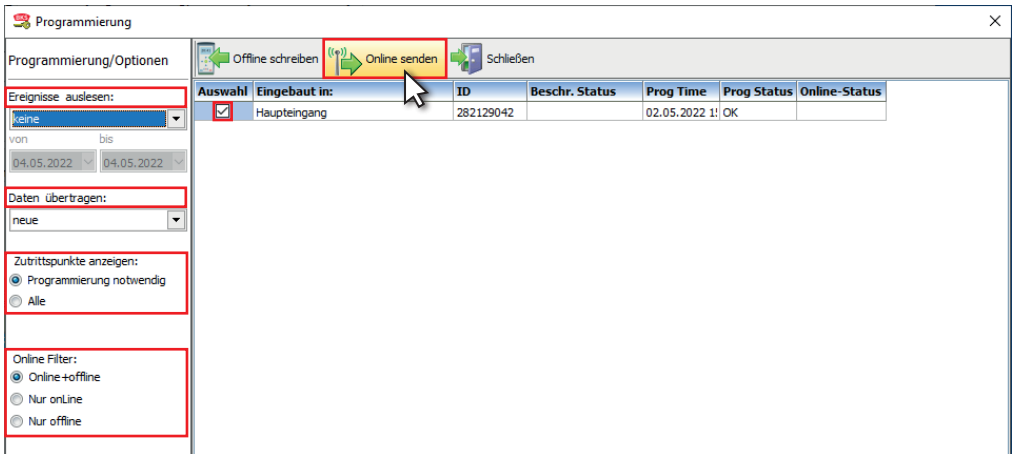
```
Programmierung
beendet
```

3.8.5 Programmierung der Türen in Online-Anlagen

In Online-Anlagen werden die Daten für die Programmierung direkt und bequem vom BKS KeyManager über Funk zu den online angeschlossenen Türen übertragen. Ein Ablaufen dieser Türen mit dem Programmiergerät ist überflüssig. Wir Empfehlen die Option der automatischen Übertragung beim Speichern der Berechtigungsmatrix zu aktivieren, siehe Online-Konfiguration im Kapitel 5.7.4 [323].

Die direkte Übertragung der Daten zu den Türen wird im Dialog im Fenster „Programmierung“ gestartet. In der rechten Spalte des Fensters wird eine Liste der zu programmierenden Türen angezeigt. Es besteht die Möglichkeit, wie bei der im vorigen Kapitel beschriebenen Übertragung zum Programmiergerät die Anzahl der Türen und die zu übertragene Datenmenge zu begrenzen.

- Drücken Sie auf den Button „Programmierung“ im Hauptmenü und öffnen das Fenster.
- Optional können Sie in der rechten Spalte die angezeigten Türen und Datenmenge über die Auswahlfelder einschränken.
- Drücken Sie auf den Button „Online senden“, um die Daten an die Türen zu übertragen.



Voraussetzung für die Übertragung beim Speichern ist die Einrichtung der Anlage in der Online-Konfiguration und entsprechender Installation der Zutrittspunkte, siehe Kapitel 5.7 [293].

Durch die Übertragung wechselt die Anzeige des Status in den Zeilen- und Spaltenüberschriften der Berechtigungsmatrix vom oben abgebildeten gelb unterlegten Status „N“ auf den Status „grau“ ohne Buchstaben für eine erfolgreiche Übertragung und Quittierung, siehe Kapitel 3.5.5 [90].

3.9 Quittierung

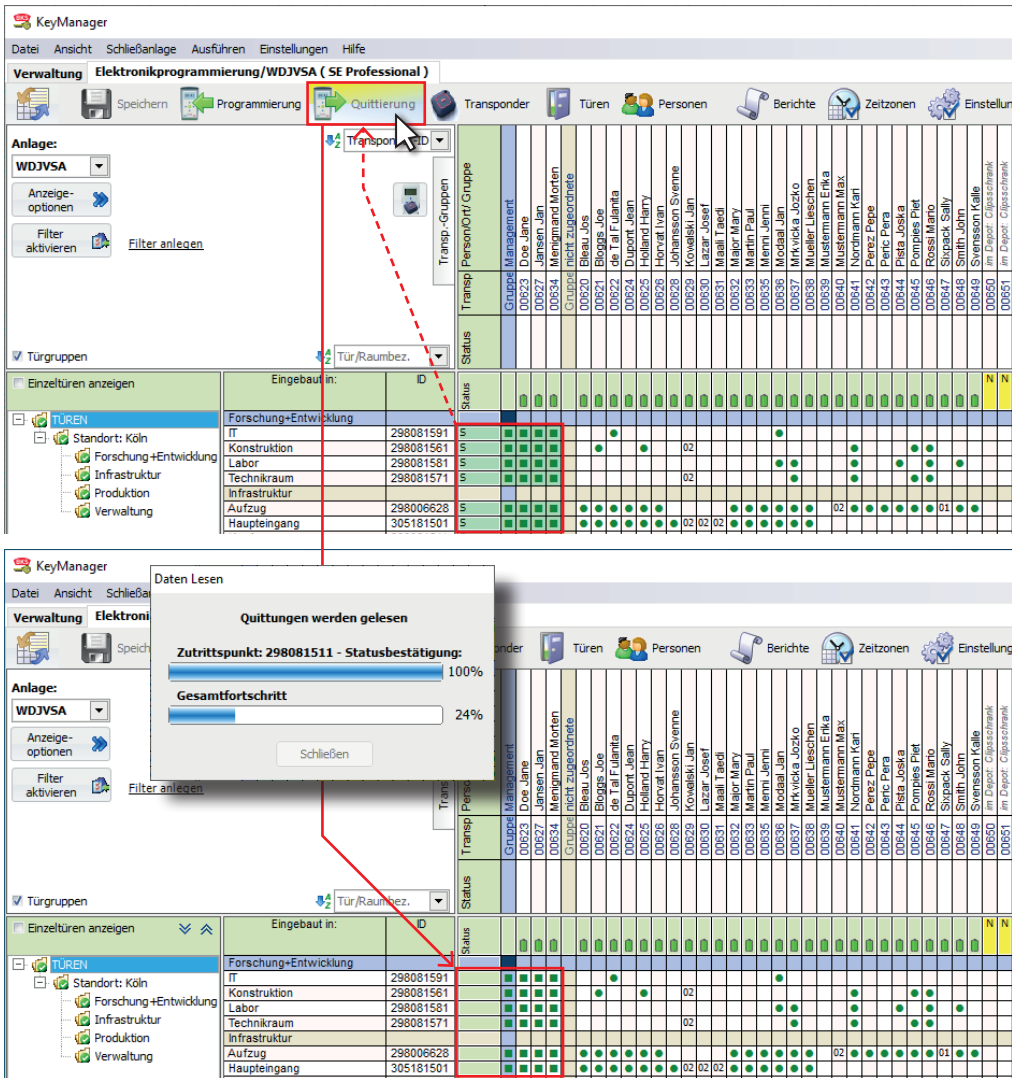
Durch die Quittierung werden die Daten im BKS KeyManager mit den Daten in den Komponenten über das Programmiergerät synchronisiert. Der BKS KeyManager erhält eine Rückmeldung über den Status der Programmierungen. Bei der Quittierung werden auch die ausgelesenen Ereignisse und Berichte der Türen in den BKS KeyManager eingelesen. Zum Abschluss der Quittierung werden die Symbole des Programmierstatus in der Berechtigungsmatrix aktualisiert.

- Verbinden Sie das Programmiergerät und den Computer mit einem USB-Kabel.

Warten Sie ab, bis die Verbindung bestätigt ist und das verbundene Programmiergerät in der Statuszeile angezeigt wird.

- Die Quittierung sollte automatisch starten. Falls diese nicht starten sollte, drücken Sie auf den Button „Quittierung“ und starten dadurch das Einlesen der Daten bzw. Rückmeldung vom Programmiergerät.

Nach der Quittierung wird die Anzeige des Status in den Zeilen- und Spaltenüberschriften sowie in den Quadraten der Berechtigungsmatrix aktualisiert, siehe Kapitel 3.5.5 [90].



3.9.1 Quittierung Anlagen in DoT-Anlagen mit FGT

In Data on Transponder-Anlagen (DoT) mit Freigabeterminals (FGT) werden die Ereignisse der Türen beim Zutritt an den Transponder übertragen. Durch das Buchen des Transponders am FGT werden die Daten zum BKS KeyManager übertragen. Bei der Programmierung der Transponder mit dem FGT wird die Quittierung direkt durchgeführt.

Die Quittierung der Programmierung der Türen wird vom Programmiergerät eingelesen.

3.9.2 Quittierung in Online-Anlagen

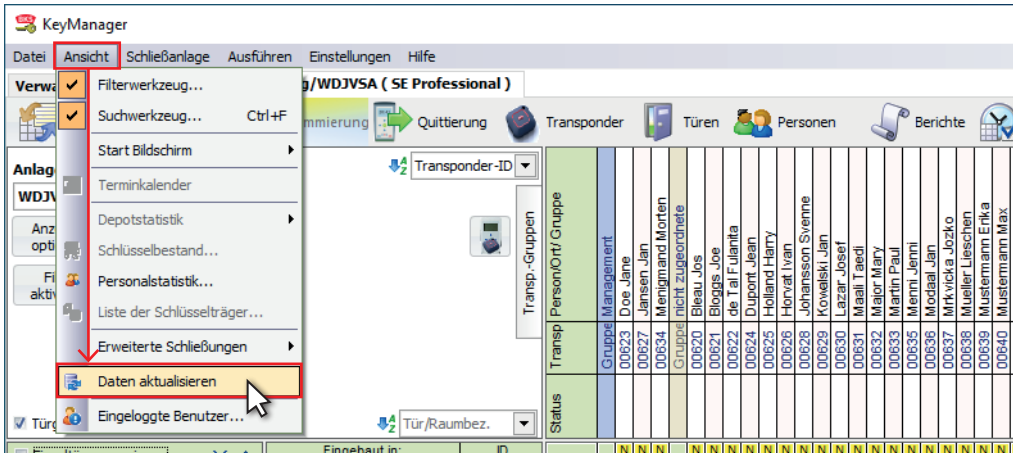
In Online-Anlagen wird die Quittierung der Programmierung der Türen während der Programmierung dieser automatisch über die Online-Verbindung ausgeführt. Die Synchronisation wird automatisch beim Speichern oder Programmieren durchgeführt. Eine separate Quittierung der Türen ist nicht nötig.

3.10 Daten aktualisieren

Der BKS Keymanager aktualisiert die Matrix während des Betriebs in der Regel automatisch. Änderungen werden in der Darstellung aktuell angezeigt. Sollte dieser Prozess durch Überschneidungen von Prozessen nicht ausgeführt werden, kann mit der Funktion "Daten aktualisieren", die Matrix manuell aktualisiert werden.

Bei der parallelen Bearbeitung durch mehrere Benutzer beim Client-Server-Betrieb kann es notwendig werden, den Bildschirminhalt manuell zu aktualisieren. Im Normalfall erhält der Benutzer aber eine Meldung, das Daten von anderen Nutzern verändert wurden und kann die Aktualisierung bestätigen.

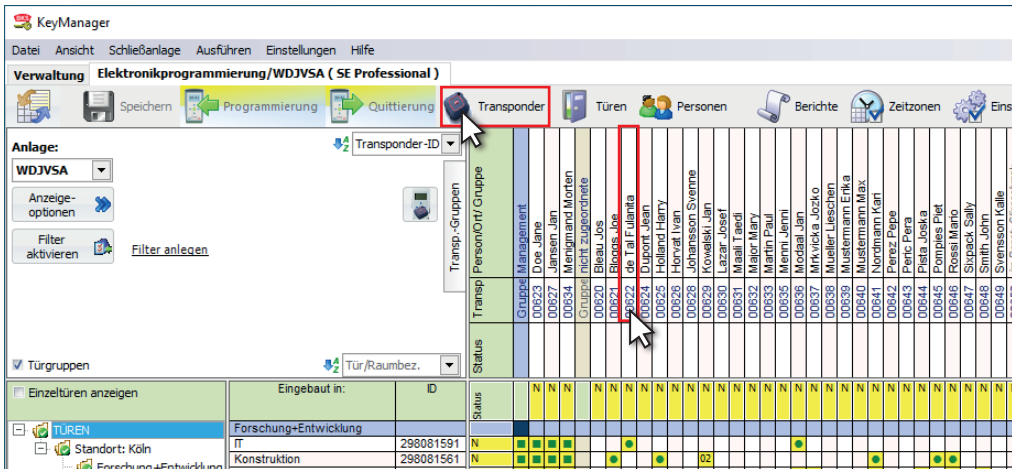
- Wählen Sie über das Dropdown-Menü „Ansicht“ den Menüpunkt „Daten aktualisieren“ aus.



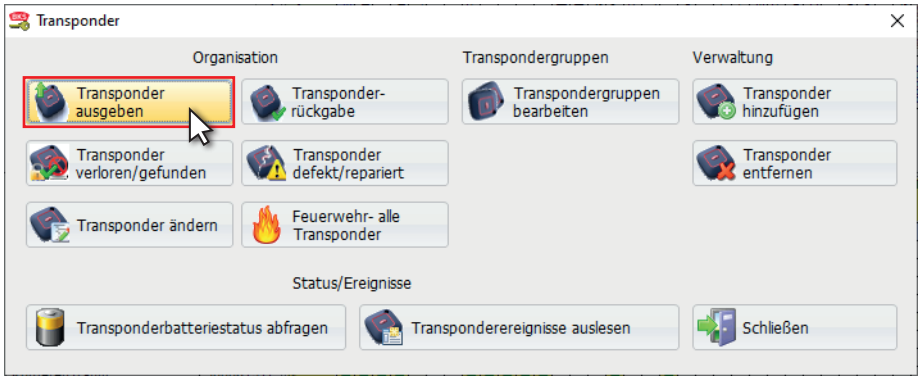
3.11 Transponder an Personen ausgeben und programmieren (DoT)

Mit der Funktion „Transponder an Personen ausgeben“ wird der Transponder an die jeweiligen Personen ausgegeben. In der Matrix und den Ereignissen wird die Person sowie der Transponder entsprechend angezeigt.

- Wählen Sie in der Hauptansicht der Matrix mit einem doppelten Mausklick die Nummer eines Transponders oder das leere Feld des Personennamens aus.



- Alternativ Drücken Sie im Hauptmenü den Menüpunkt „Transponder“ und im Fenster „Transponder“ den Button „Transponder ausgeben“.



Bei Data on Transponder-Anlagen (DoT) werden die Einzelberechtigungen auf den Transpondern gespeichert. Wenn der Stand der Daten auf dem Transponder nicht aktuell ist, muss der Transponder vor der Ausgabe programmiert werden. Im Fenster „Transponder Ausgabe/Eigenschaften“ können Sie die für die Ausgabe des Transponders notwendigen Schritte ausführen.

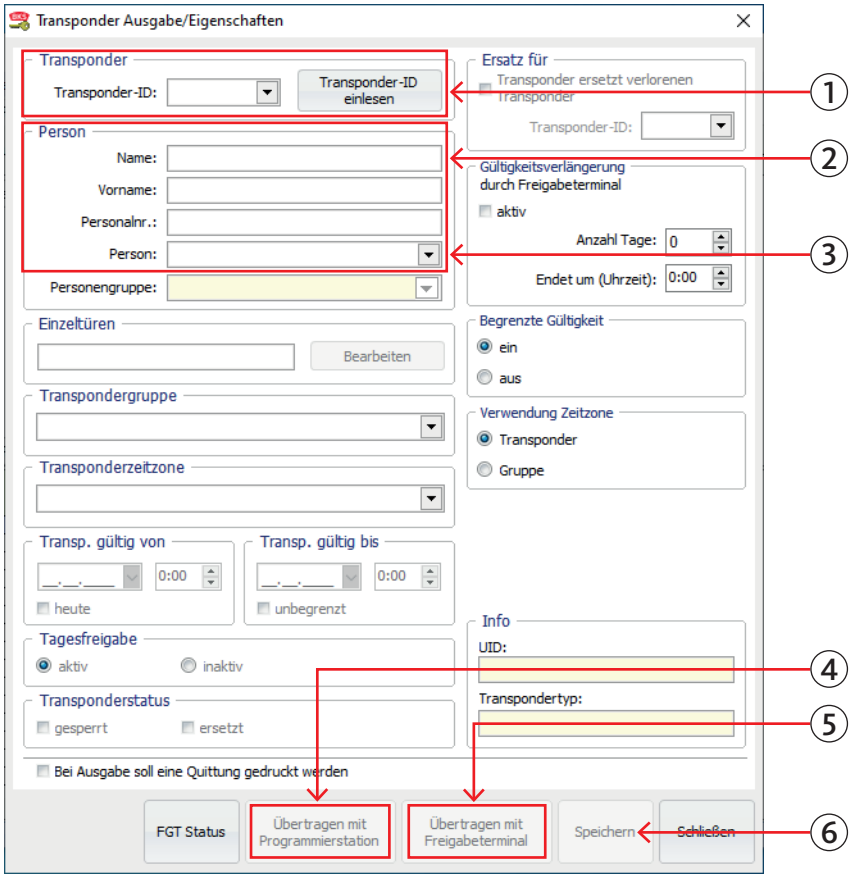
➔ (5) Die Daten können automatisch durch entsprechende Auswahl bei der Einrichtung des Freigabeterminals oder manuell mit dem Button „Übertragen mit Freigabeterminal“ auf den Transponder gespeichert werden.

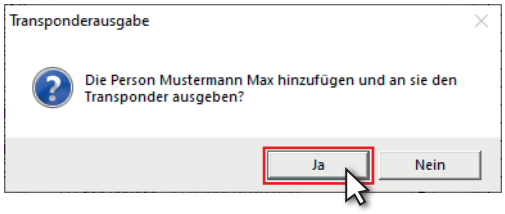
➔ (4) Das Programmiergerät kann ebenfalls zur Datenübertragung verwendet werden. Durch Drücken des Buttons „Übertragen mit Programmierstation“ wird der Vorgang gestartet.

- (1) Der gewählte Transponder wird im Feld „Transponder-ID:“ angezeigt. Alternativ kann über das Dropdown-Menü ein Transponder ausgewählt oder durch Drücken des Buttons „Transponder-ID einlesen“ der Transponder eingelesen werden.
- (3) Wählen Sie über das Dropdown-Menü im Feld „Person“ die Person aus, welche dem Transponder zugeordnet werden soll. (2) Ist diese Person nicht auf der Liste vorhanden, können Sie manuell die Felder der Personendaten ausfüllen und eine neue Person anlegen.

Über die Option „Bei Transponderausgabe soll eine Quittung gedruckt werden“ legen Sie fest, ob ein Formular zur Transponderausgabe gedruckt werden soll.

- (6) Drücken Sie den Button „Speichern“ und im nächsten Fenster auf „Ja“, um Eingaben zu sichern.





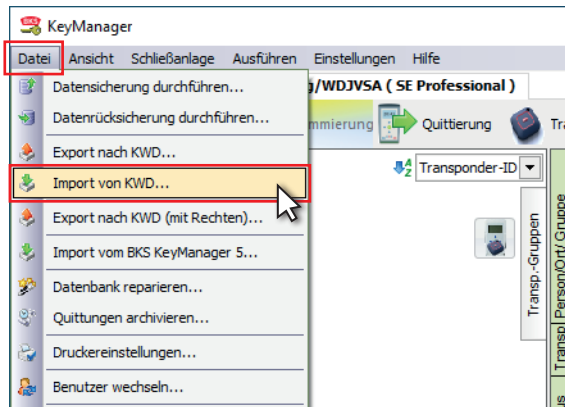
4. Grundfunktionen des BKS KeyManagers

Nachdem Sie Ihre Schließanlage angelegt haben, kann diese mit den folgenden Grundfunktionen weiter eingerichtet werden. Richten Sie Ihre Zutrittsmedien, Zutrittspunkte, berechtigte Personen und Ihr Berichtswesen individuell weiter ein.

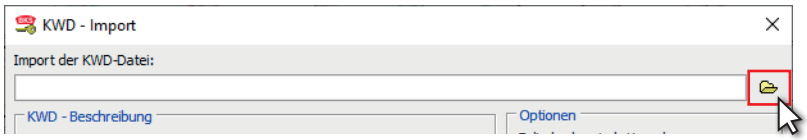
4.1 Hinzufügen neuer Komponenten durch Import der KWD-Datei

Nach dem Erwerb weiterer Zutrittspunkte können Sie diese mit der Funktion Import KWD-Datei der Schließanlage hinzufügen. Dadurch entfällt ein manuelles Hinzufügen. Eine passende KWD-Datei kann über Ihren Vertriebspartner bezogen werden.

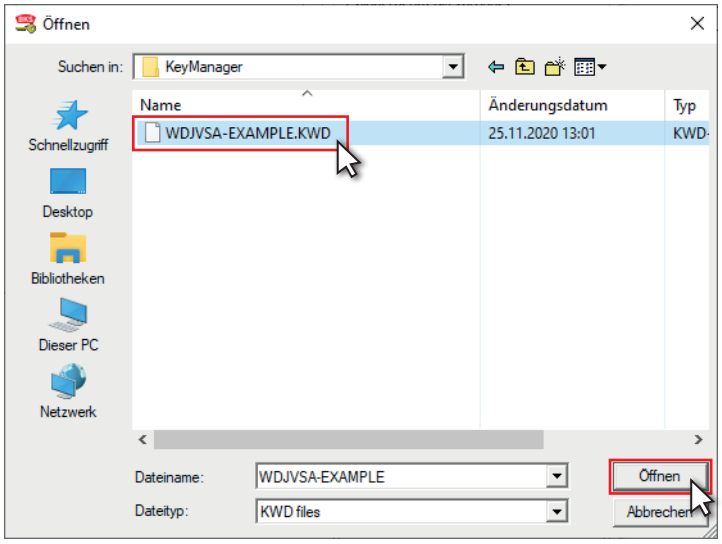
- Öffnen Sie in der Menüleiste das Dropdown-Menü „Datei“ und wählen den Menüpunkt „Import von KWD ...“ aus.



- Drücken Sie auf das Verzeichnissymbol für „KWD-Datei öffnen“.

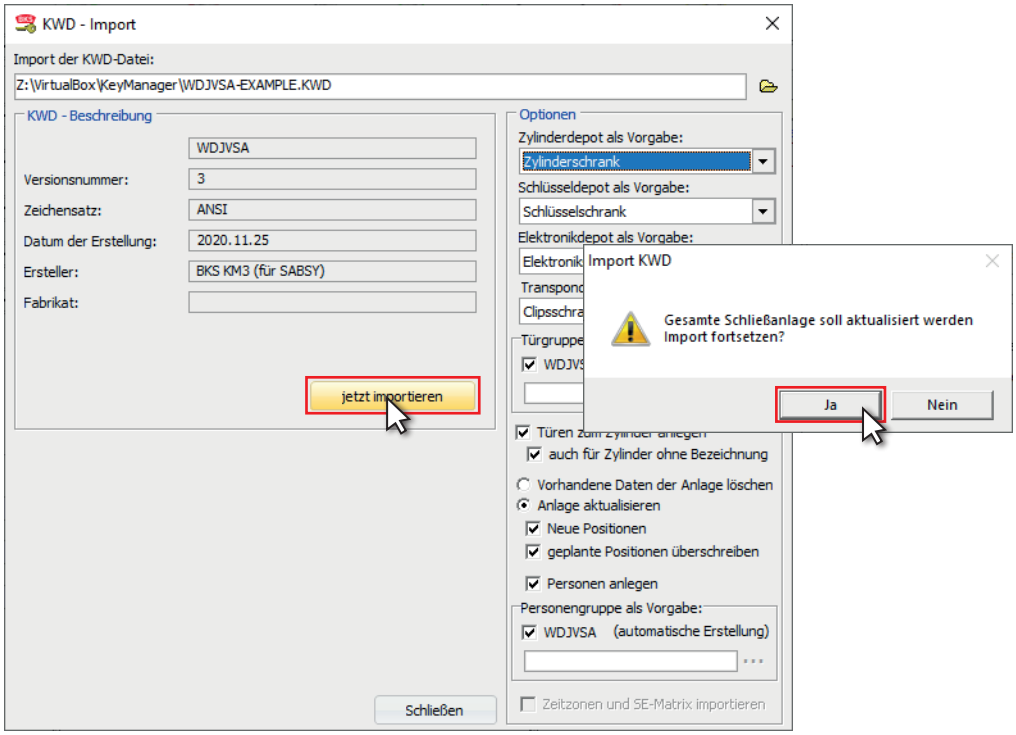


- Navigieren Sie zur KWD-Datei, wählen diese aus und drücken auf den Button „Öffnen“.

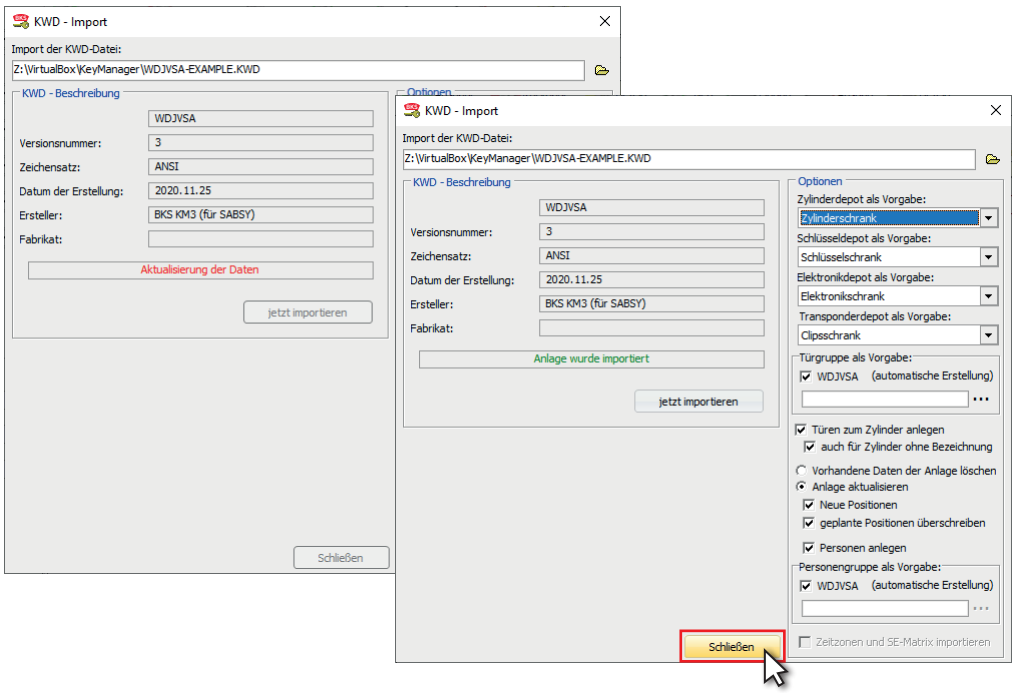


Überprüfen Sie die Importoptionen und passen diese ggf. an.

- Starten Sie die Aktualisierung mit „jetzt importieren“ und bestätigen den Dialog mit „Ja“.



- Nach erfolgreichem Import drücken Sie auf den Button „Schließen“.

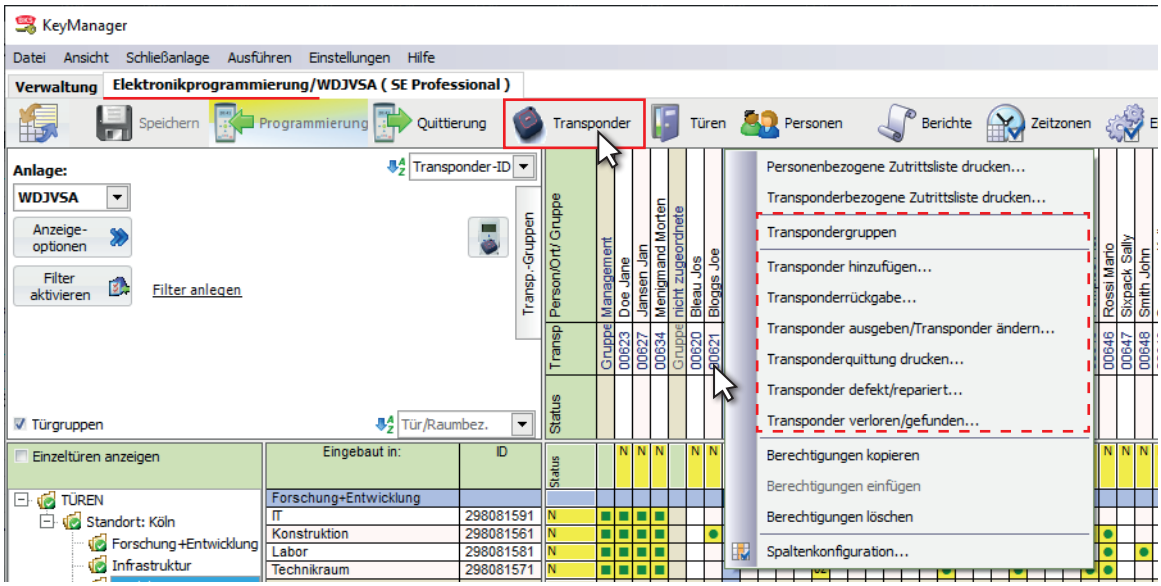


4.2 Transponder

Das Transponder-Menü kann über verschiedene Wege erreicht werden.

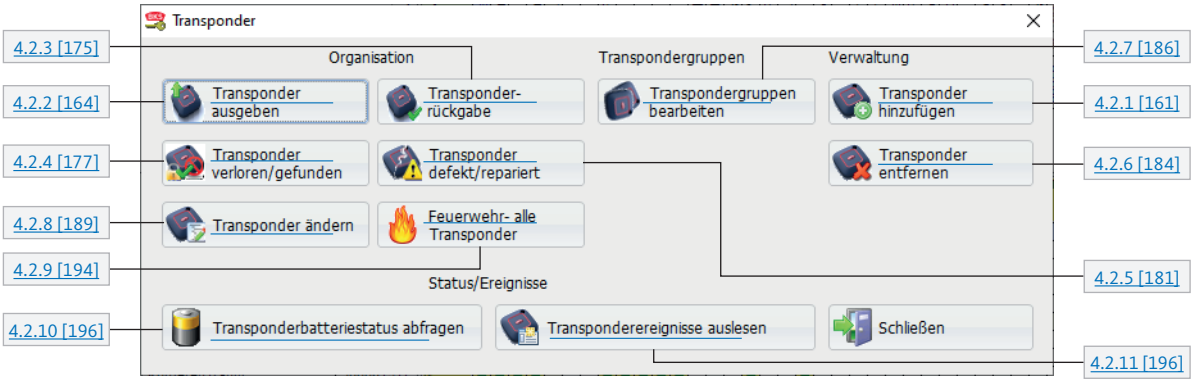
- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Transponder“.

Einige Funktionen des Transponder-Menüs können durch Auswahl eines Transponders in der Matrix mit der rechten Maustaste aufgerufen werden. Wählen Sie im Kontextmenü die Funktion aus, die für den gewählten Transponder gestartet werden soll.



Im Transponder Menü lassen sich die folgenden Funktionen aufrufen. Diese können Variieren.

→ Fenster „Transponder“ für eine Data on Transponder-Anlage (DoT).

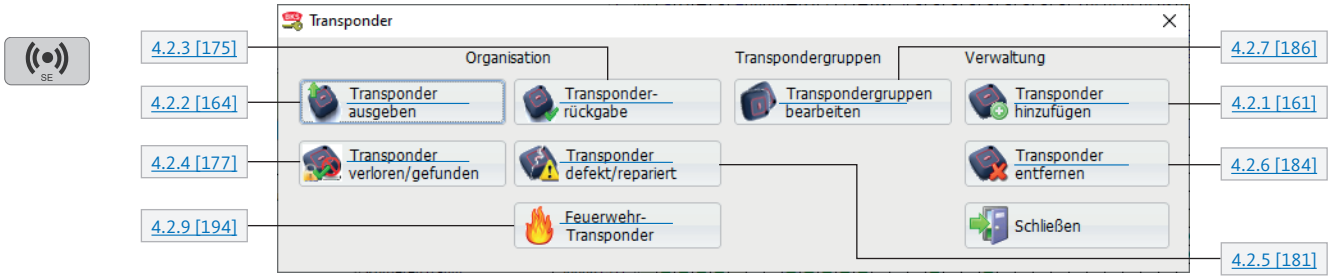


HINWEIS

Beim Ausführen der Funktionen des Transponder-Menüs können je nach Anlagentyp verschiedene Funktionen zur Verfügung stehen.

Der Transponder kann mit einem Programmiergerät (SXPG) [B 5971 00x1] automatisch eingelesen werden. Um diese Funktion nutzen zu können, müssen Sie das Programmiergerät mit Ihrem Computer verbinden. Der Status des Geräts wird nach einer erfolgreichen Verbindung in der Fußzeile des BKS KeyManagers als „Programmiergerät angeschlossen“ angezeigt werden. Diese Alternative steht in der Regel bei einer „nonDoT“-Anlage nicht zur Verfügung. Die Ausnahme bildet die Funktion „Feuerwehrtransponder“.

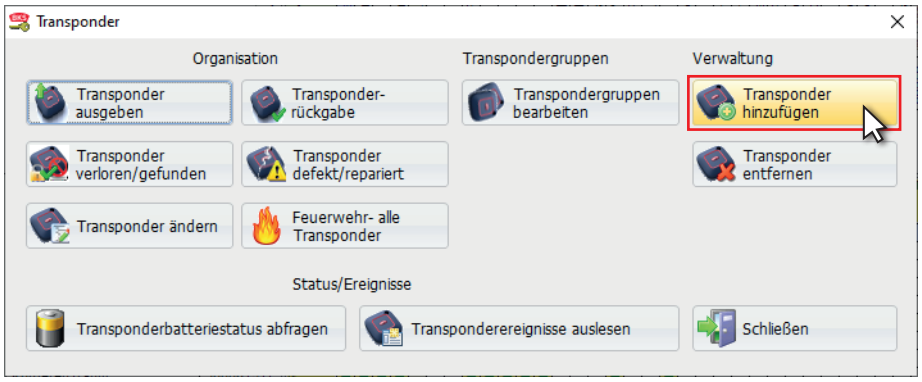
→ Fenster „Transponder“ für eine Offline- oder Online-Anlage (nonDoT).



4.2.1 Transponder hinzufügen

Mit der Funktion „Transponder hinzufügen“ können weitere Transponder manuell im BKS KeyManager angelegt werden.

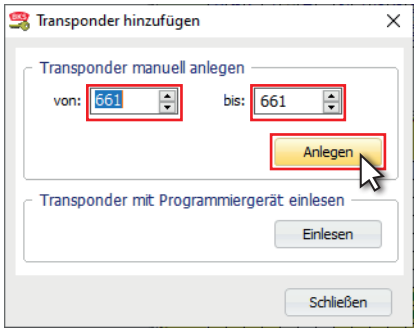
- Drücken Sie auf den Button „Transponder hinzufügen“.

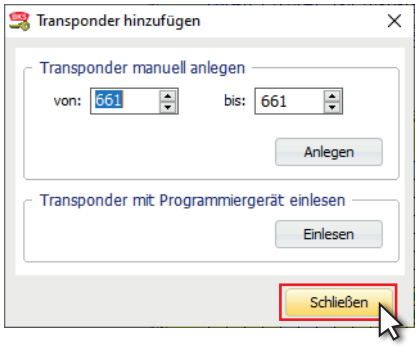


- Geben Sie den Bereich der Transponder-IDs ein, welche hinzugefügt werden sollen. Drücken Sie den Button „Anlegen“ zum Hinzufügen.

Als Beispiel wurde der Transponder mit der ID 661 im BKS KeyManager angelegt. Die Transponder-ID ist auf dem Transponder zu finden.

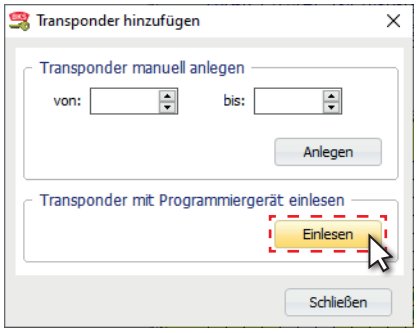
- Beenden Sie das Hinzufügen und drücken auf den Button „Schließen“.



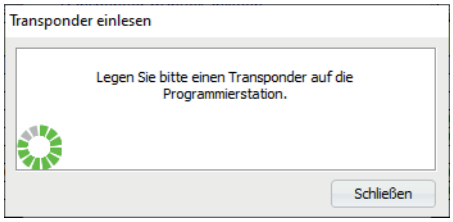


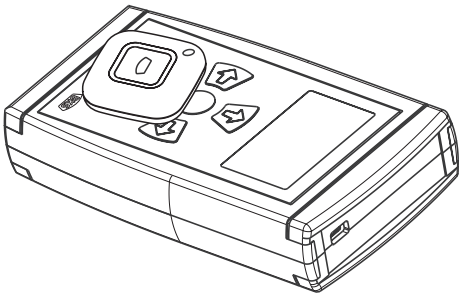
Alternativ kann der Transponder automatisch mit einem Programmiergerät eingelesen werden. Verbinden Sie das Programmiergerät und den Computer mit einem USB-Kabel und warten, bis die Verbindung bestätigt ist.

- Drücken Sie auf den Button „Einlesen“, um den Vorgang zu starten.



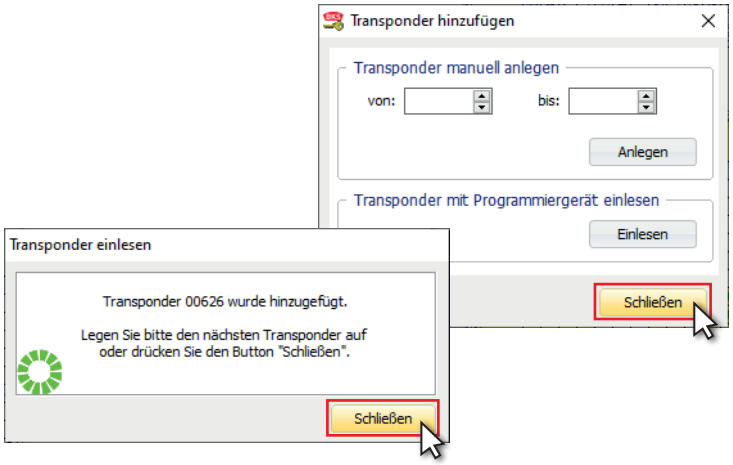
- Legen Sie den einzulesenden Transponder auf das Programmiergerät.





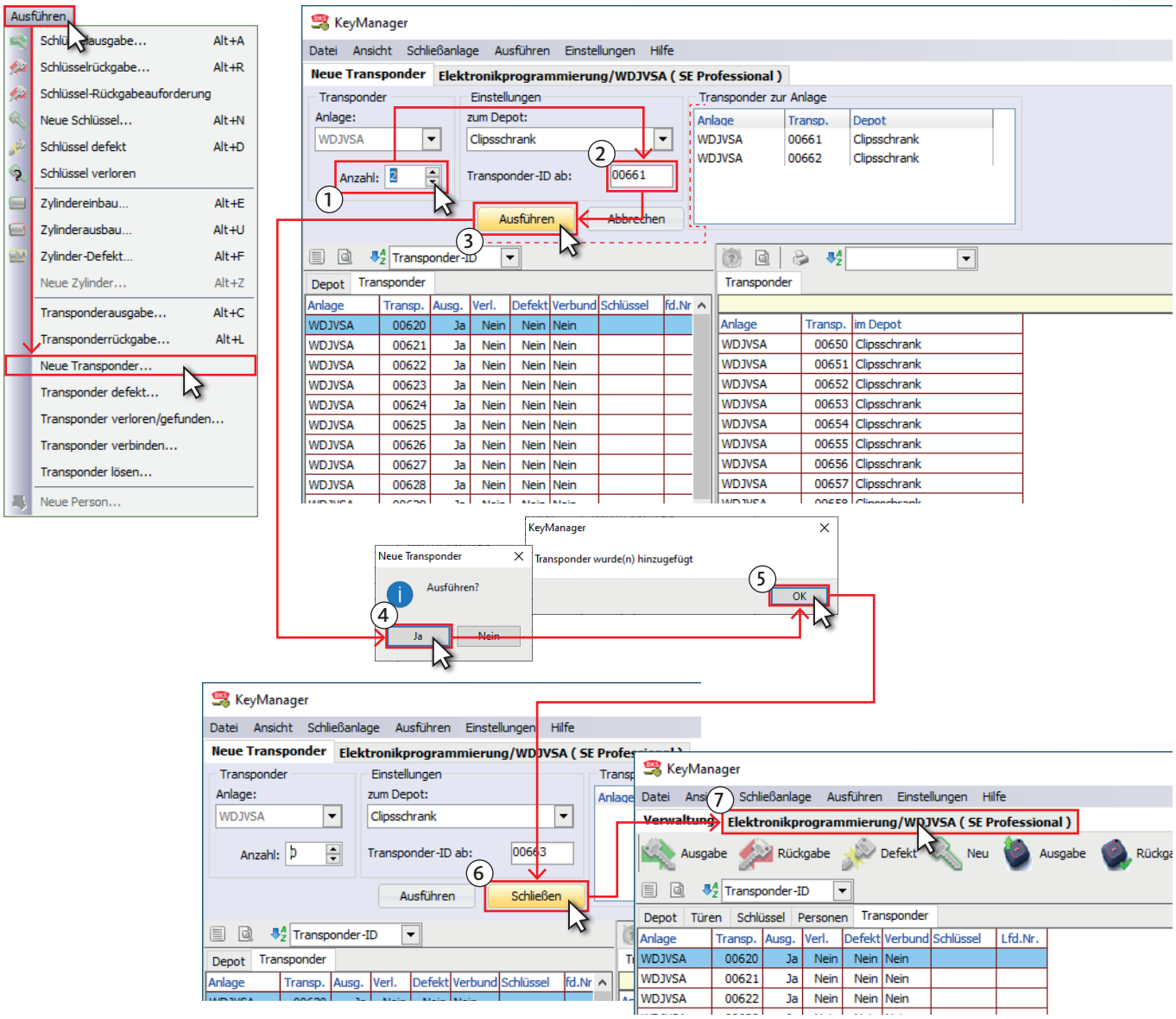
Der neue Transponder wird im BKS KeyManager angelegt.

- Drücken Sie in den beiden Fenstern jeweils den Button „Schließen“ zum Beenden.



4.2.1.1 Neue Transponder (Verwaltungsmodul)

- Geben Sie die Anzahl der Transponder ein, die hinzugefügt werden sollen. Tragen Sie die Transponder-ID des ersten Transponders in das Feld ein. Drücken Sie auf den Button „Ausführen“.
- Folgen Sie den Schritten der Abbildung.

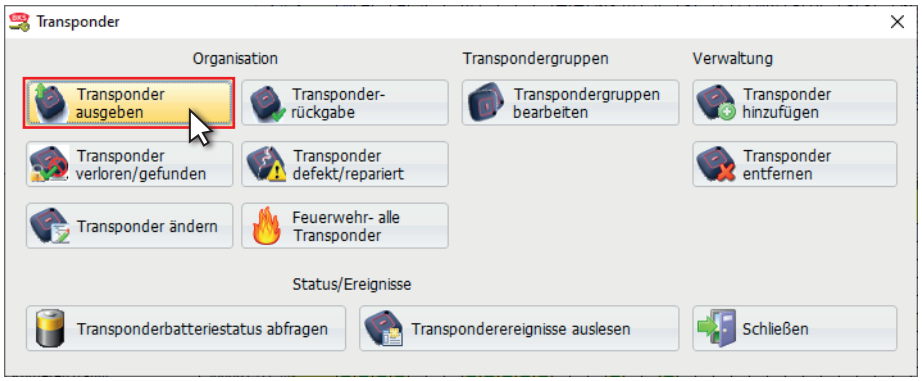


4.2.2 Transponder ausgeben

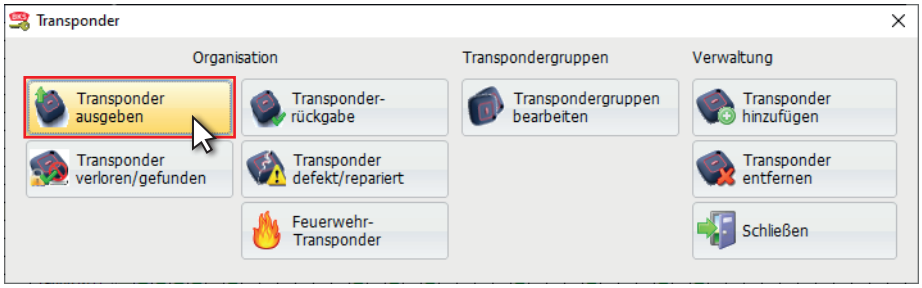
Mit der Funktion „Transponder an Personen ausgeben“ wird der Transponder an eine Person ausgegeben. In der Matrix und den Ereignissen wird diese Person und der Transponder dann miteinander verbunden und zusammen angezeigt. Beachten Sie die Beschreibung im Kapitel 4.2.8 [189].

- Drücken Sie auf den Button „Transponder ausgeben“.

DoT-Anlage, siehe Kapitel 4.2.2.1 [165]

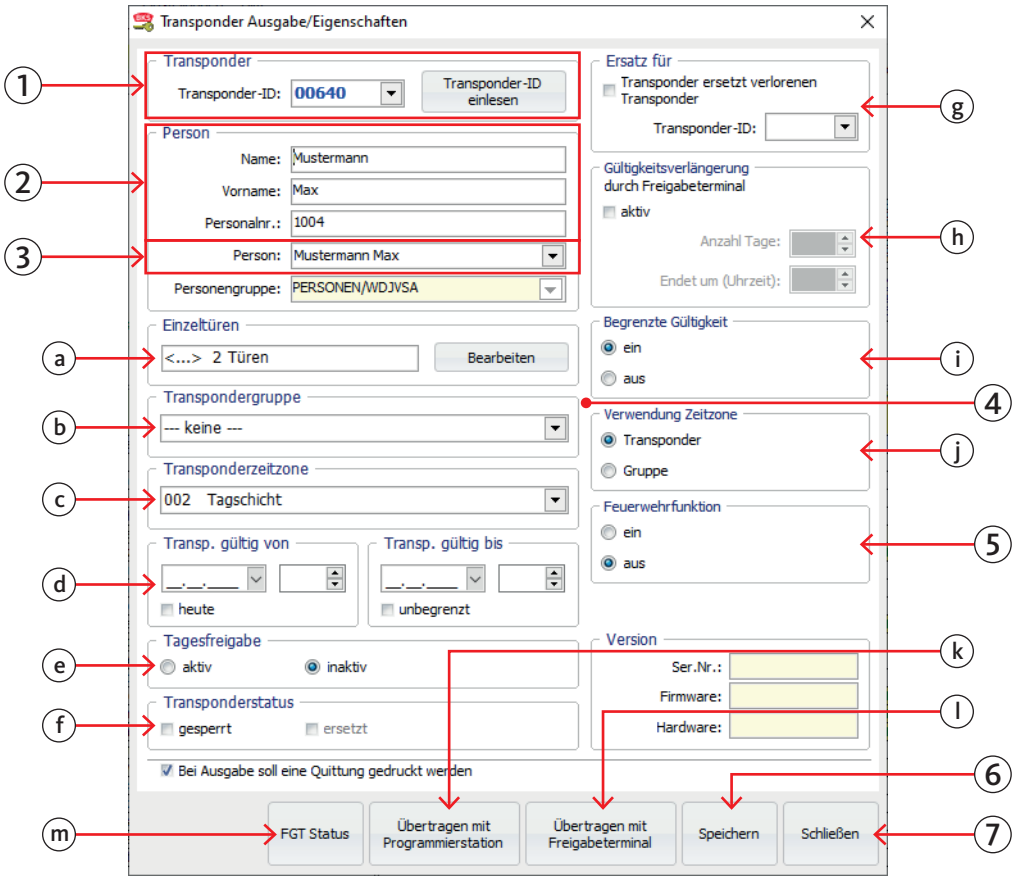


nonDoT-Anlage, siehe Kapitel 4.2.2.2 [172]

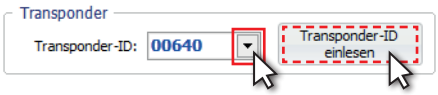


HINWEIS **Der Dialog kann auch durch einen Doppelklick auf einen Transponder im Spaltenkopf der Matrix geöffnet werden (nur bei DoT).**

4.2.2.1 Transponder ausgeben in DoT-Anlagen

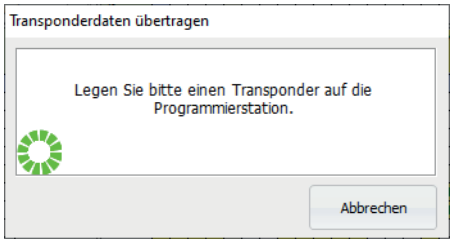


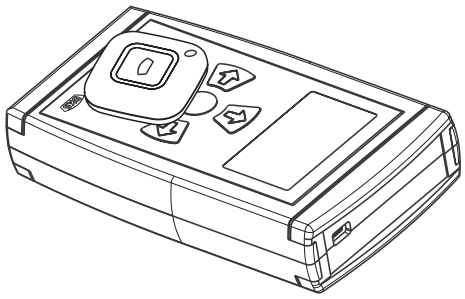
- (1) Im Feld Transponder wählen Sie im Dropdown-Menü die ID des Transponders aus, der ausgegeben werden soll.



Alternativ können Sie den Button „Transponder-ID einlesen“ drücken und mit dem Programmiergerät den Transponder einlesen.

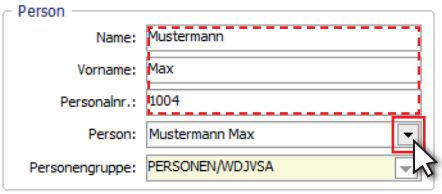
- Verbinden Sie das Programmiergerät und den Computer mit einem USB-Kabel und warten, bis die Verbindung bestätigt ist und das verbundene Programmiergerät in der Statuszeile angezeigt wird.
- Legen Sie den einzulesenden Transponder auf das Programmiergerät.





- (3) Im Feld Person wählen Sie im Dropdown-Menü die Person aus, die mit dem Transponder verbunden werden soll.

(2) Alternativ können Sie eine neue Person anlegen. Füllen Sie hierzu die Felder mit den entsprechenden Daten zur Person aus.



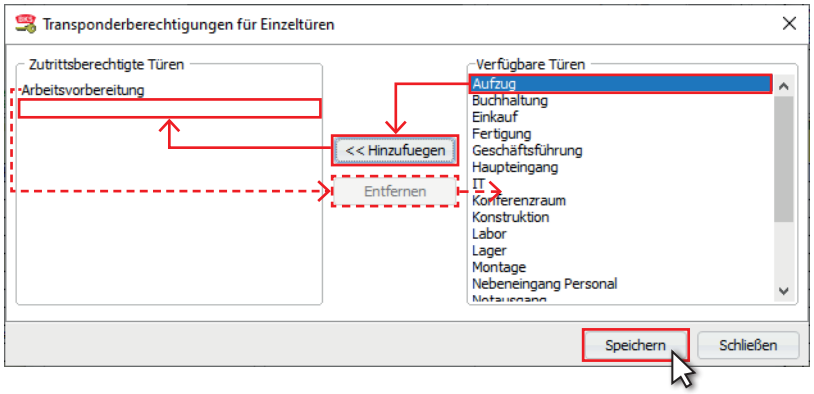
(a) Im Feld Einzeltüren können Sie dem Transponder eine Zutrittsberechtigung zu einzelnen Türen der Anlage erteilen. Diese Funktion kann je nach Einstellung und der Firmware der Transponder auf 8 Türen pro Transponder begrenzt sein.

- Drücken Sie auf den Button „Bearbeiten“ zur Vergabe der Berechtigungen.

- Wählen Sie in der Spalte „Verfügbare Türen“ eine Tür aus, zu welcher der Transponder berechtigt werden soll.
- Drücken Sie auf den Button „<< Hinzufügen“.

Die Tür wird in die Spalte „Zutrittsberechtigte Türen“ verschoben und der Transponder ist zutrittsberechtigt zu dieser Tür nach der Programmierung. Wiederholen Sie das Auswählen und Hinzufügen, um den Transponder zu weiteren Türen zu berechtigen.

- Zum Entfernen der Berechtigung zu einer Tür bzw. aus der Spalte „Zutrittsberechtigte Türen“ wählen Sie die gewünschte Tür aus und drücken auf den Button „Entfernen“.
- Drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern.



(j)+(b) Im Feld „Verwendung Zeitzone“ können Sie den Einzelberechtigungen eine Zeitzone zuweisen. Im Feld „Transponderzeitzone“ suchen Sie eine Zone in der Dropdown-Liste aus. Die Einzelberechtigung hat Priorität und überschreibt die Berechtigung durch die Gruppe.

- Aktivieren Sie die Checkbox „Transponder“ im Feld „Zeitzone“.
- Wählen Sie im Dropdown-Menü „Transponderzeitzone“ eine Zeitzone aus.

(j)+(c) Wahlweise oder ergänzend können Sie im Feld „Verwendung Zeitzone“ dem Transponder die Berechtigungen einer Transpondergruppe zuweisen. Im Feld „Transponderzeitzone“ suchen Sie eine Transpondergruppe in der Dropdown-Liste aus.

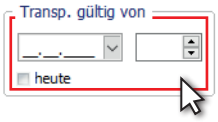
- Aktivieren Sie die Checkbox „Gruppe“ im Feld „Zeitzone“.
- Wählen Sie im Dropdown-Menü „Transpondergruppe“ eine Zeitzone aus.

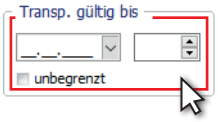
(i)+(d) Im Feld „Begrenzte Gültigkeit“ können Sie diese Funktion aktivieren und in den Feldern „Transp. gültig bis“ und „Transp. gültig von“ einen Zeitraum für die Gültigkeit festlegen. Außerhalb des Zeitraums ist der Transponder deaktiviert.

Die Eingabe des Zeitraums kann geführt über die Dropdown-Menüs bzw. Tasten oder manuell durch Eingabe erfolgen. Setzen Sie die Checkbox „heute“, um das aktuelle Datum und Uhrzeit ohne weitere Einstellung zu setzen.

Über die Checkbox „heute“ können Sie den Start-Zeitpunkt unkompliziert auf das aktuelle Datum und Uhrzeit setzen und über die Checkbox „unbegrenzt“ eine endlose Gültigkeit festlegen.

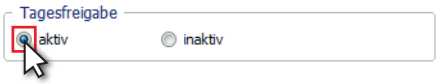
- Aktivieren Sie die Checkbox „ein“ im Feld „Begrenzte Gültigkeit“.
- Geben Sie einen Start-Zeitpunkt im Feld „Transp. gültig von“ und einen Endzeitpunkt im Feld „Transp. gültig bis“ ein.





(e) Im Feld „Tagesfreigabe“ können Sie die Funktion Tagesfreigabe für den Transponder aktivieren.

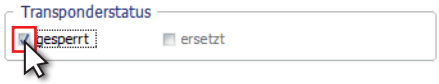
- Aktivieren Sie die Checkbox „aktiv“ im Feld „Tagesfreigabe“.
- Beachten Sie zur Einrichtung, dass die Tagesfreigabe auch in der Tür eingerichtet werden muss. Die komplette Beschreibung der Tagesfreigabe finden Sie im Kapitel 3.6.6 [127].



(f) Im Feld „Transponderstatus“ wird Ihnen angezeigt, ob der Transponder gesperrt und/oder ersetzt wurde. Über die Checkbox können Sie den Transponder in den Zustand gesperrt versetzen.

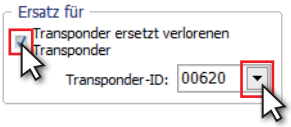
Diese Funktion sollten Sie nur nutzen, wenn der Transponder für Sie verfügbar ist. Bei einem defekten oder verlorenem Transponder verwenden Sie bitte den entsprechenden Menüpunkt im Transpondermenü, siehe Kapitel 4.2.6 [184] bzw. 4.2.5 [181].

- Aktivieren Sie die Checkbox „gesperrt“ im Feld „Transponderstatus“ , um den Transponder zu deaktivieren.



(g) Im Feld „Ersatz für“ können Sie einen anderen Transponder durch den gerade ausgewählten Transponder ersetzen. Im Dialog können Sie auswählen, ob der zu ersetzende Transponder gesperrt werden soll und der neue (ausgewählte) Transponder die Berechtigungen des Ersetzten übernehmen soll, wodurch evtl. vorhandene Berechtigungen im gewählten Transponder gelöscht werden.

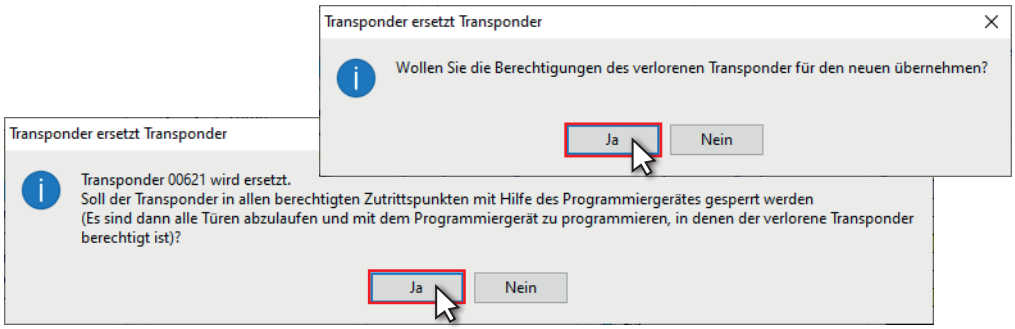
- Aktivieren Sie die Checkbox „Transponder ersetzt verlorenen Transponder“
- Wählen Sie über das Dropdown-Menü „Transponder-ID“ den zu ersetzenden Transponder aus.



In Data on Transponder-Anlagen mit Freigabeterminal verfügt die Funktion „Ersatz für“ eine zusätzliche Erweiterung. Beachten Sie hierzu die Anleitung im Kapitel 3.6.8.3 [142].

Nachdem Drücken des Buttons „Speichern“ werden Sie noch zu folgenden Eingaben aufgefordert, um das Ersetzen des Transponders abzuschließen.

- Drücken Sie im nächsten Fenster auf den Button „Ja“, damit alle Zutrittspunkte, in denen der zu ersetzende Transponder eine Zutrittsberechtigung hat, für diesen gesperrt werden.
- Im darauf folgenden Fenster können Sie die Berechtigungen durch Drücken auf Button „Ja“ für den neuen Transponder übernehmen.



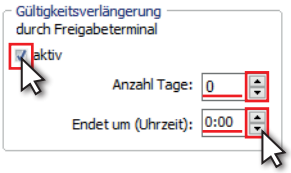
(h) Im Feld „Gültigkeitsverlängerung durch Freigabeterminal“ legen Sie einen Zeitraum fest, nachdem die Gültigkeit des Transponders verlängert werden muss. Dieser Zeitraum wird über die Anzahl an Tagen bis zum Ablauf der Gültigkeit und der Uhrzeit am Tag des Ablaufens festgelegt. Der Transponder verliert nach Ablauf der Gültigkeit automatisch alle Zutrittsberechtigungen. Durch das Buchen an einem Freigabeterminal wird der Zeitraum neu gestartet und der Transponder erlangt seine Gültigkeit und die Zutrittsberechtigungen zurück.

Diese relative Gültigkeit ist besonders in Verbindung mit einem Freigabeterminal geeignet, eine regelmäßige Datenübertragung zwischen dem BKS KeyManager und den verschiedenen Komponenten der Schließanlage herzustellen, ohne diese direkt zu vernetzten. Eine aufwendige Möglichkeit ist, die Gültigkeit des Transponders mit dem Programmiergerät zu verlängern.

Ein verlorener Transponder kann durch das auslaufen lassen, der Gültigkeit gesperrt werden. Hierbei ist abzuwägen, ob die Anlagensicherheit nicht gefährdet wird, wenn der verlorene Transponder den restlichen Gültigkeitszeitraum weiterhin eine Zutrittsberechtigung hat. Dabei ist zu beachten, dass die Möglichkeit der Verlängerung des Gültigkeitszeitraums in der Berechtigungsmatrix durch das Sperren des Transponders auszuschließen ist.

Eine ausführlichere Beschreibung der Gültigkeitsverlängerung mit Freigabeterminal finden Sie im Kapitel 3.6.7 [135].

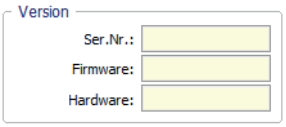
- Aktivieren Sie die Checkbox „aktiv“ im Feld „Gültigkeitsverlängerung durch Freigabeterminal“.
- Legen Sie den Zeitraum fest, nachdem die Gültigkeit abläuft und der Transponder seine Gültigkeit verlieren sein soll.
  Im Feld „Anzahl der Tage“ geben Sie die Zeitspanne ein und
  im Feld „Endet um (Uhrzeit)“ einen Zeitpunkt am Tag des Ablaufens.
  Die Eingabe ist über das Textfeld oder über die Tasten rechts neben dem Textfeld möglich.



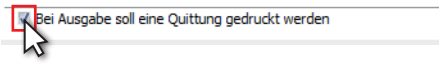
(5) Im Feld „Feuerwehrfunktion“ können Sie die Energiesparfunktion im Transponder aktivieren. Eine Beschreibung zur Feuerwehrfunktion finden Sie im Kapitel 4.2.9 [194].

- Aktivieren Sie die Checkbox „ein“ im Feld „Feuerwehrfunktion“.

Im Feld „Version“ wird Ihnen nach dem Auslesen des Transponders die aktuelle Hardware- und Firmware Version sowie die Seriennummer des gewählten Transponders angezeigt.

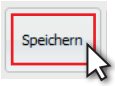


- Wenn zur Ausgabe des Transponders eine Quittung ausgedruckt werden soll, aktivieren Sie die Checkbox „Bei Ausgabe soll eine Quittung gedruckt werden“.



(6) Nachdem Sie alle gewünschten Eingaben im Fenster „Transponder Ausgeben“ gemacht haben, müssen diese in die Datenbank übernommen und gespeichert werden.

- Drücken Sie auf den Button „Speichern“.

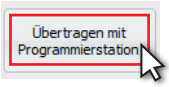


In der Berechtigungsmatrix werden neue Transponder oder Transponder, bei denen die Eigenschaften verändert wurden, mit dem Status „N“ und einem gelben Hintergrund angezeigt.
Ist die Online-Einstellung „Geänderte Transponderrechte immer sofort an die Freigabeterminals senden“ aktiv, wird der Status „N“ übersprungen und direkt gesendet. Der Status „O“ oder „S“ wird während bzw. nach der Übertragung angezeigt.
(Abbildung des Status zur Vereinfachung ohne Batterieanzeige)

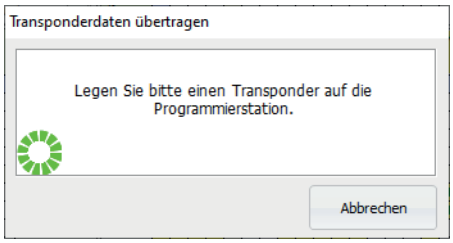
Die gespeicherten Änderungen des Transponders müssen im nächsten Schritte über ein Programmiergerät (k) oder über die Freigabeterminals (l) zum Transponder übertragen werden.

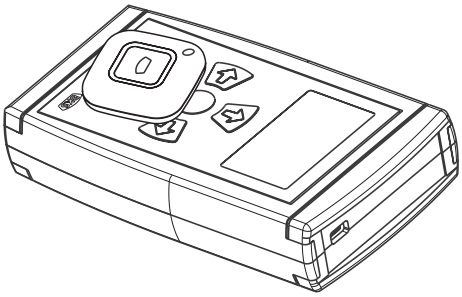
(k) Zur Übertragung der Daten über ein Programmiergerät folgen Sie den nächsten Schritten.

- Drücken Sie auf den Button „Übertragen mit Programmierstation“.



- Verbinden Sie das Programmiergerät und den Computer mit einem USB-Kabel und warten, bis die Verbindung bestätigt ist und das verbundene Programmiergerät in der Statuszeile angezeigt wird.
- Legen Sie den einzulesenden Transponder auf das Programmiergerät.

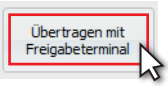




In der Berechtigungsmatrix wird die erfolgreiche Übertragung der Daten mit einem grauen Hintergrund in der Farbe der Statuszeile angezeigt. Der Buchstabe „N“ verschwindet.
(Abbildung des Status ohne Batterieanzeige)

(l) Zur Übertragung der Daten über ein Freigabeterminal folgen Sie den nächsten Schritten.

■ Drücken Sie auf den Button „Übertragen mit Freigabeterminal“.



In der Berechtigungsmatrix wird nach dem Start der Übertragung zum Freigabeterminal (FGT) der aktuelle Status der Übertragung durch folgende Meldungen angezeigt.
(Abbildungen des Status zur Vereinfachung ohne Batterieanzeige)

Während der Übertragung der Daten vom BKS KeyManager zum FGT wird der Status „O“ angezeigt.

Die erfolgreiche Übertragung aller Daten wird durch den Status „S“ und einen grünen Hintergrund angezeigt. Die Daten stehen jetzt zur Abholung durch den Transponder bereit.

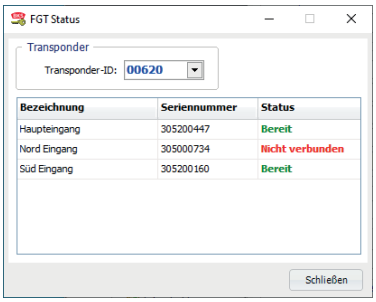
Wird der ausgegebene oder geänderte Transponder am FGT eingebucht, werden diese Daten zum Transponder übertragen und die Ereignisse vom Transponder ausgelesen.
Zur Quittierung der erfolgreichen Übertragung wird der Status durch einen grauen Hintergrund angezeigt. Der Buchstabe „S“ verschwindet.

Wenn der Speicher im FGT (ohne Pro) nicht mehr ausreicht, um die Programmierinformation abzulegen, werden die Daten im Direktmodus übertragen. Dies bedeutet, dass die Programmierdaten ohne Zwischenspeicherung auf dem FGT übertragen werden. Die Übertragung startet in diesem Fall erst, wenn der Transponder am FGT eingebucht wird und sich in Kommunikation mit dem FGT befindet.

Der Direktmodus wird durch die Statusmeldung „D“ angezeigt. Nach erfolgreicher Übertragung der Daten zum Transponder wird der Status „D“ nicht mehr angezeigt und verschwindet.
Status „D“ nur bei alten FGTs (ohne Pro).

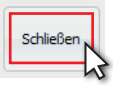
(m) Der Status der Übertragung zu den einzelnen FGTs kann zur Problemfindung abgefragt werden. Hierbei wird die Aktualität der Programmierdaten des jeweils gewählten Transponders auf den verschiedenen FGTs der Schließanlage ermittelt. Kommt es zu Differenzen z. B. durch das Offline-Gehen von FGTs während der Übertragung, können die Daten durch ein erneutes „Übertragen zum Freigabeterminal“ (l) aktualisiert werden.

■ Drücken Sie auf den Button „FGT Status“ zum Start der Abfrage.

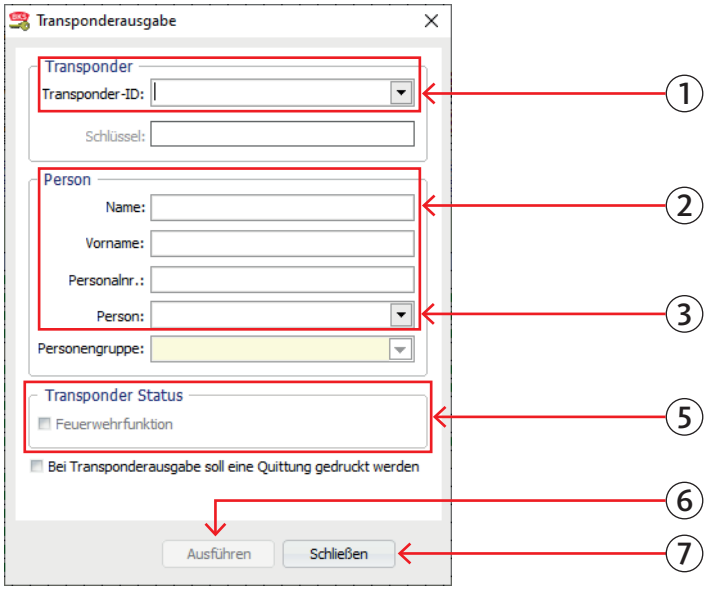


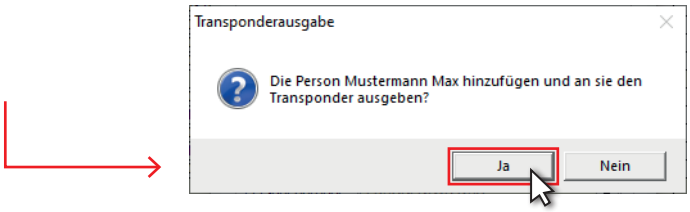
(7) Zum Beenden des Dialogs schließen Sie das Fenster „FGT Status“.

■ Drücken Sie auf den Button „Schließen“.

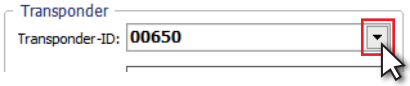


4.2.2.2 Transponder ausgeben in nonDoT-Anlagen



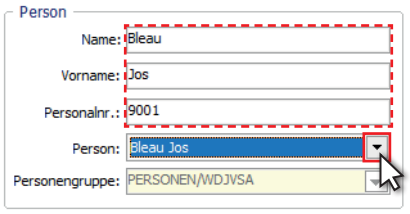


- (1) Im Feld Transponder wählen Sie im Dropdown-Menü die ID des Transponders aus, der ausgegeben werden soll.



- (3) Im Feld Person wählen Sie im Dropdown-Menü die Person aus, die mit dem Transponder verbunden werden soll.

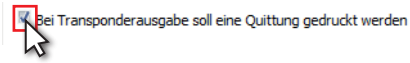
(2) Alternativ können Sie eine neue Person anlegen. Füllen Sie hierzu die Felder mit den entsprechenden Daten zur Person aus.



(5) Im Feld „Feuerwehrfunktion“ können Sie die Energiesparfunktion im Transponder aktivieren. Eine Beschreibung zur Feuerwehrfunktion finden Sie im Kapitel 4.2.9 [194].

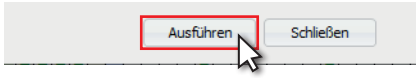
- Aktivieren Sie die Checkbox „Feuerwehrfunktion“.

- Wenn zur Ausgabe des Transponders eine Quittung ausgedruckt werden soll, aktivieren Sie die Checkbox „Bei Transponderausgabe soll eine Quittung gedruckt werden.



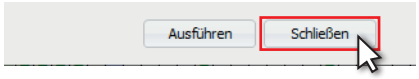
(6) Zum Beenden des Dialogs schließen Sie das Fenster „Transponder Ausgabe“.

- Drücken Sie auf den Button „Ausführen“ und Bestätigen die Ausgabe des Transponders im nächsten Fenster durch Drücken des Buttons „Ja“.



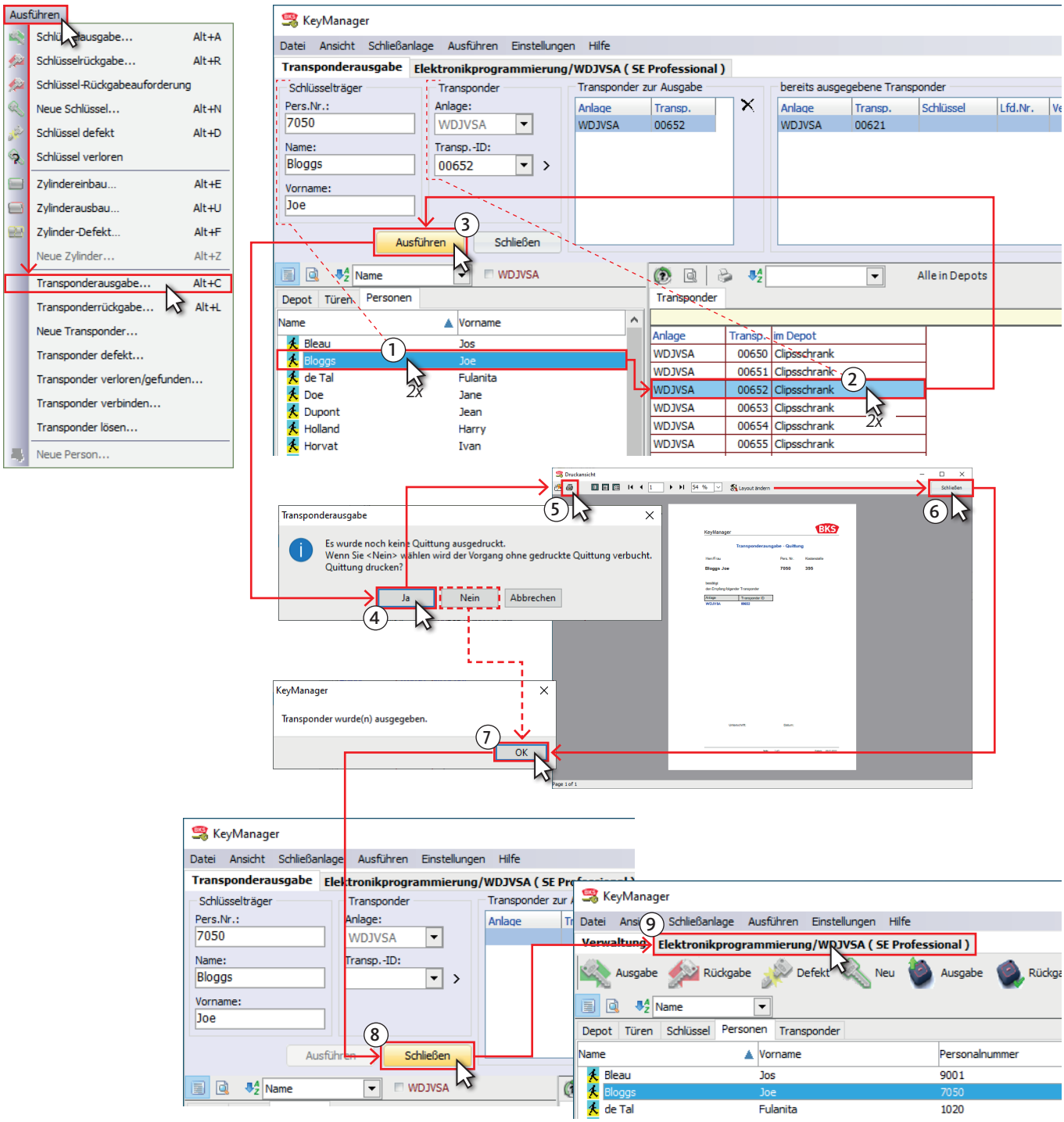
(7) Zum Beenden des Dialogs schließen Sie das Fenster „Transponder Ausgabe“.

- Drücken Sie auf den Button „Schließen“.



4.2.2.3 Transponderausgabe (Verwaltungsmodul)

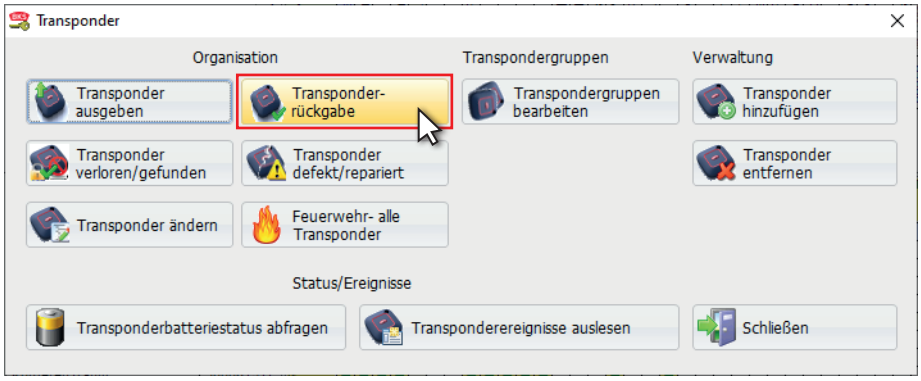
- Wählen Sie die Person und den Transponder, die verbunden werden sollen, mit einem Doppelklick aus und drücken auf Ausführen.
- Folgen Sie den Schritten der Abbildung.



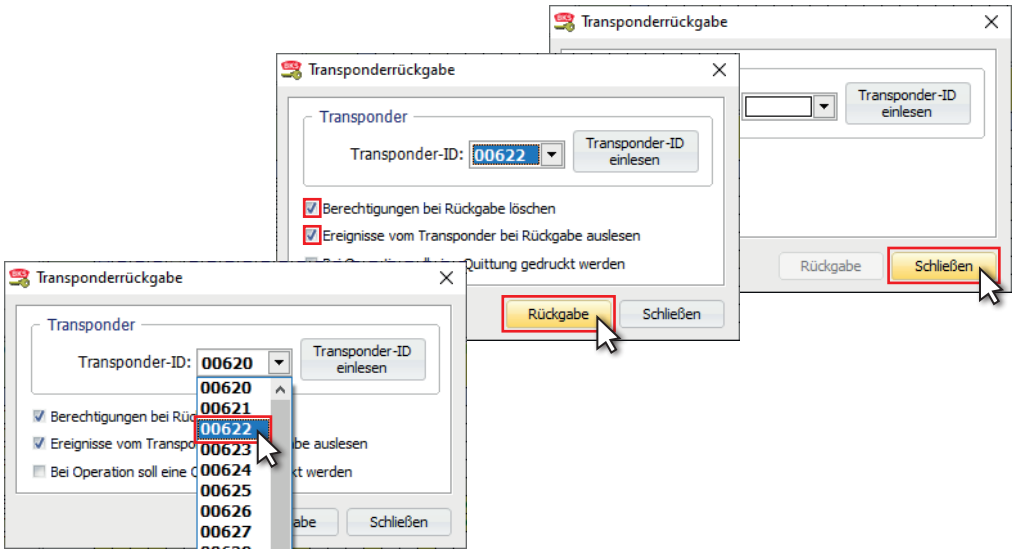
4.2.3 Transponderrückgabe

Mit der Funktion „Transponderrückgabe“ ist es möglich, einen ausgegebenen Transponder wieder zurückzunehmen.

- Drücken Sie auf den Button „Transponderrückgabe“.

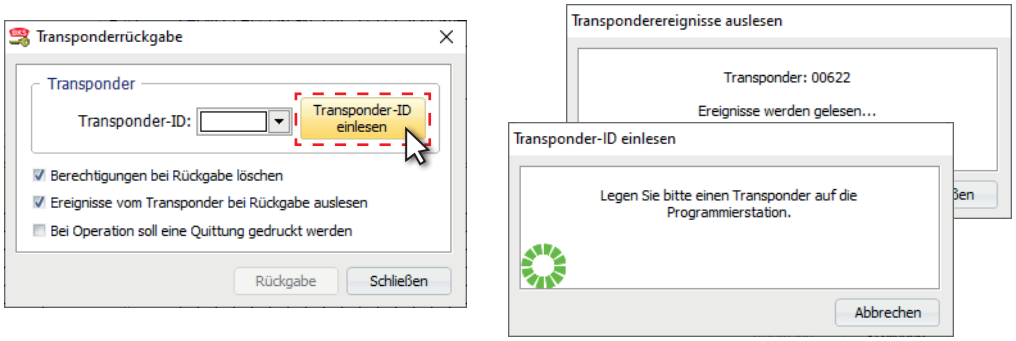


- Wählen Sie im Dropdown-Menü die ID des Transponders aus der zurückgegeben werden soll.
- Drücken Sie auf „Rückgabe“ und „Schließen“ zum Beenden des Vorgangs.



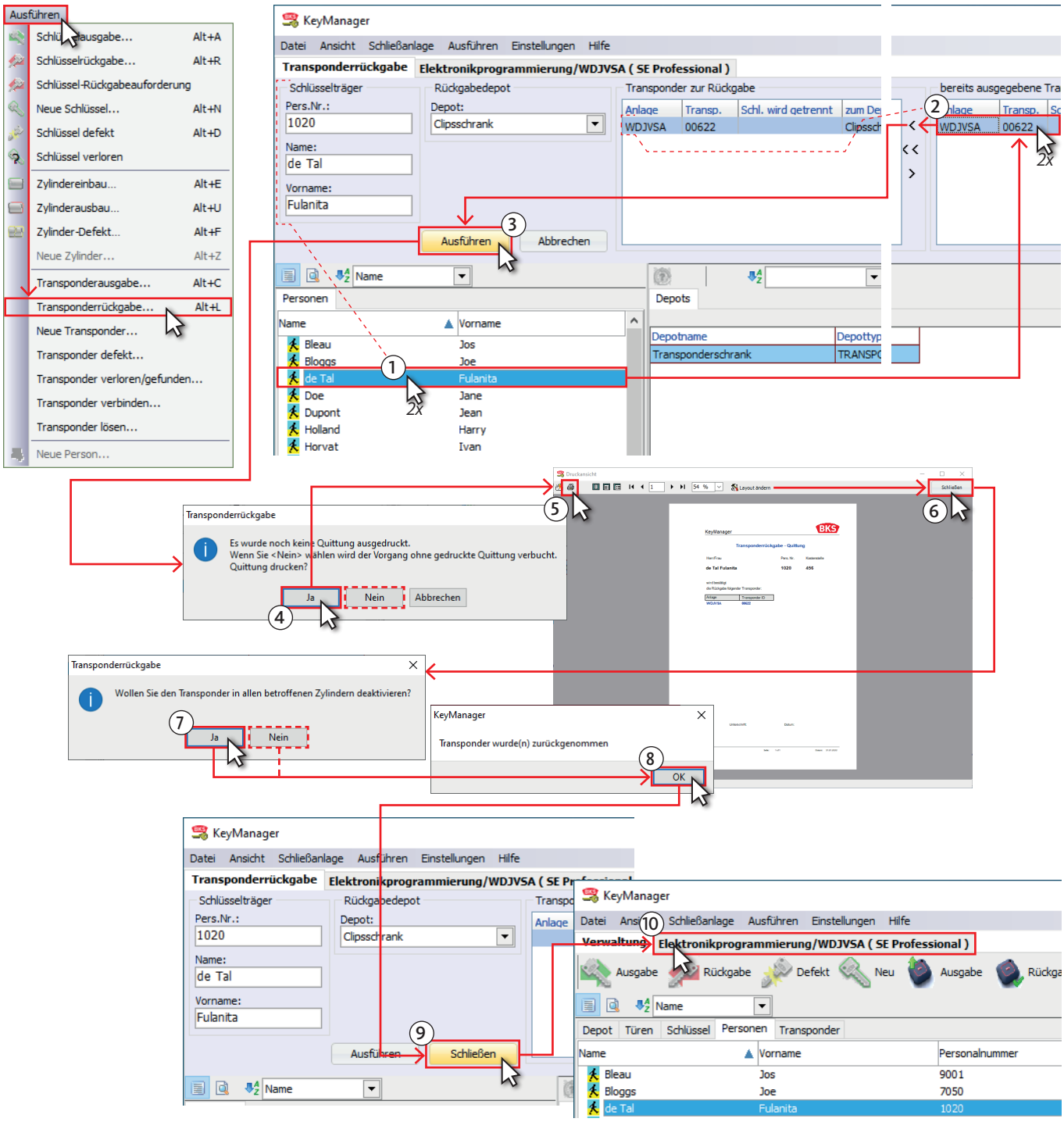
Alternativ können Sie den Button „Transponder-ID einlesen“ drücken und mit dem Programmiergerät den Transponder einlesen.

- Drücken Sie auf den Button „Transponder-ID einlesen“.



4.2.3.1 Transponderrückgabe (Verwaltungsmodul)

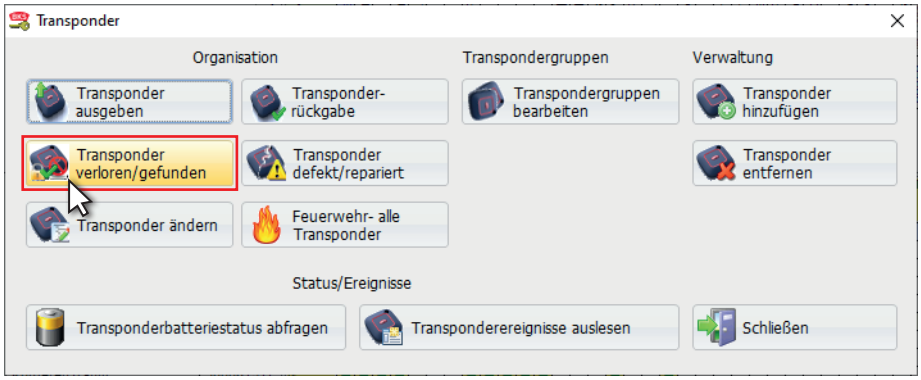
- Wählen Sie den Transponder und die Person, von der dieser zurückgeben werden soll, mit einem Doppelklick aus und drücken auf Ausführen.
- Folgen Sie den Schritten der Abbildung.



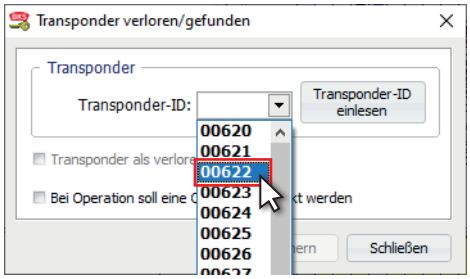
4.2.4 Transponder verloren/gefunden

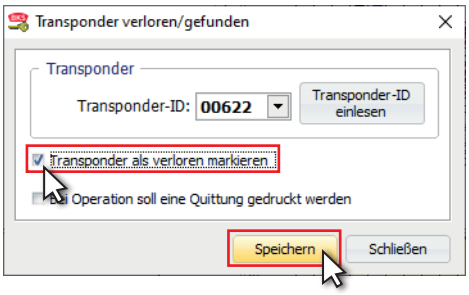
Mit der Funktion „Transponder verloren/gefunden“ werden Transponder im BKS KeyManager als verloren markiert. In diesem Menü kann auch ein als verloren gesetzter Transponder in den Status „gefunden“ zurückgesetzt werden. Dadurch wird die Kennzeichnung „verloren“ zurückgenommen.

- Drücken Sie auf den Button „Transponder verloren/gefunden“.



- Wählen Sie im Dropdown-Menü die ID des verlorenen Transponders aus.
- Aktivieren Sie die Checkbox „Transponder als verloren markieren“. Drücken Sie auf „Speichern“.





4.2.4.1 Transponder als Verloren markieren, aber die Berechtigungen nicht sperren

- Drücken Sie zum Markieren des Transponders als Verloren auf den Button „Abbrechen“. Die Checkbox zum Sperren des Transponders darf in diesem Fall **nicht** aktiviert werden.
- Drücken Sie zum Beenden auf „Schließen“.

4.2.4.2 Transponder als Verloren markieren und den Zutritt zu den Türen sperren

- Aktivieren Sie die Checkbox, das der betroffene Transponder in allen zutrittsberechtigten Zutrittspunkten gesperrt werden soll.
- Drücken Sie zum Beenden auf „Schließen“.

ACHTUNG

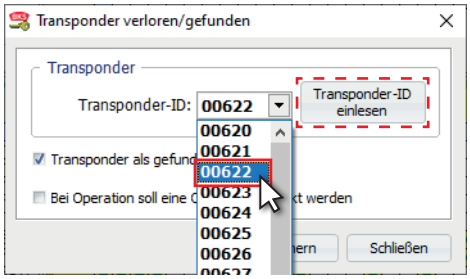
Wenn Sie diese Option wählen, wird pro Zutrittspunkt ein Programmierjob erzeugt, mit dem die Zutrittsberechtigung für den verlorenen Transponder entzogen wird. Wenn Sie sich dagegen entscheiden, behält der verlorene Transponder sämtliche Berechtigungen und kann missbräuchlich weiter verwendet werden.

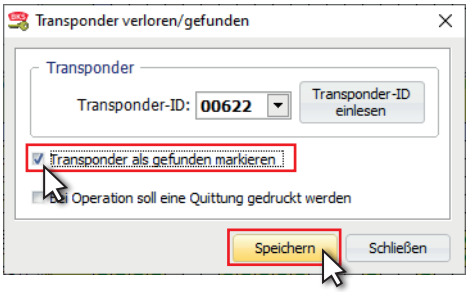
Beim Ausgeben eines neuen Transponders können Sie über die Option „Transponder ersetzt verlorenen Transponder“ den Verlorenen ersetzen und dessen Berechtigungen übernehmen, siehe Kapitel 4.2.2 [164]. Diese Option steht nur bei Data on Transponder-Anlagen (DoT) zur Verfügung.

4.2.4.3 Verlorener Transponder ist gefunden worden

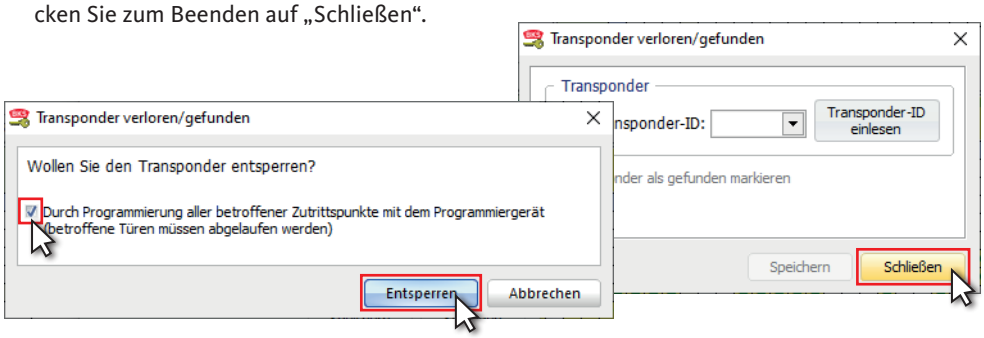
Wird ein verlorener Transponder wiedergefunden, kann dieser durch Entfernen der Markierung „verloren“ in der Schließanlage wieder reaktiviert werden.

- Wählen Sie im Dropdown-Menü die ID des als verloren zu markierenden Transponders aus. Alternativ kann der Transponder automatisch über ein mit dem Computer verbundenes Programmiergerät eingelesen werden. Drücken Sie auf den Button „Transponder-ID einlesen“.
- Aktivieren Sie die Checkbox „Transponder als gefunden markieren“. Drücken Sie zur Bestätigung auf „Speichern“.



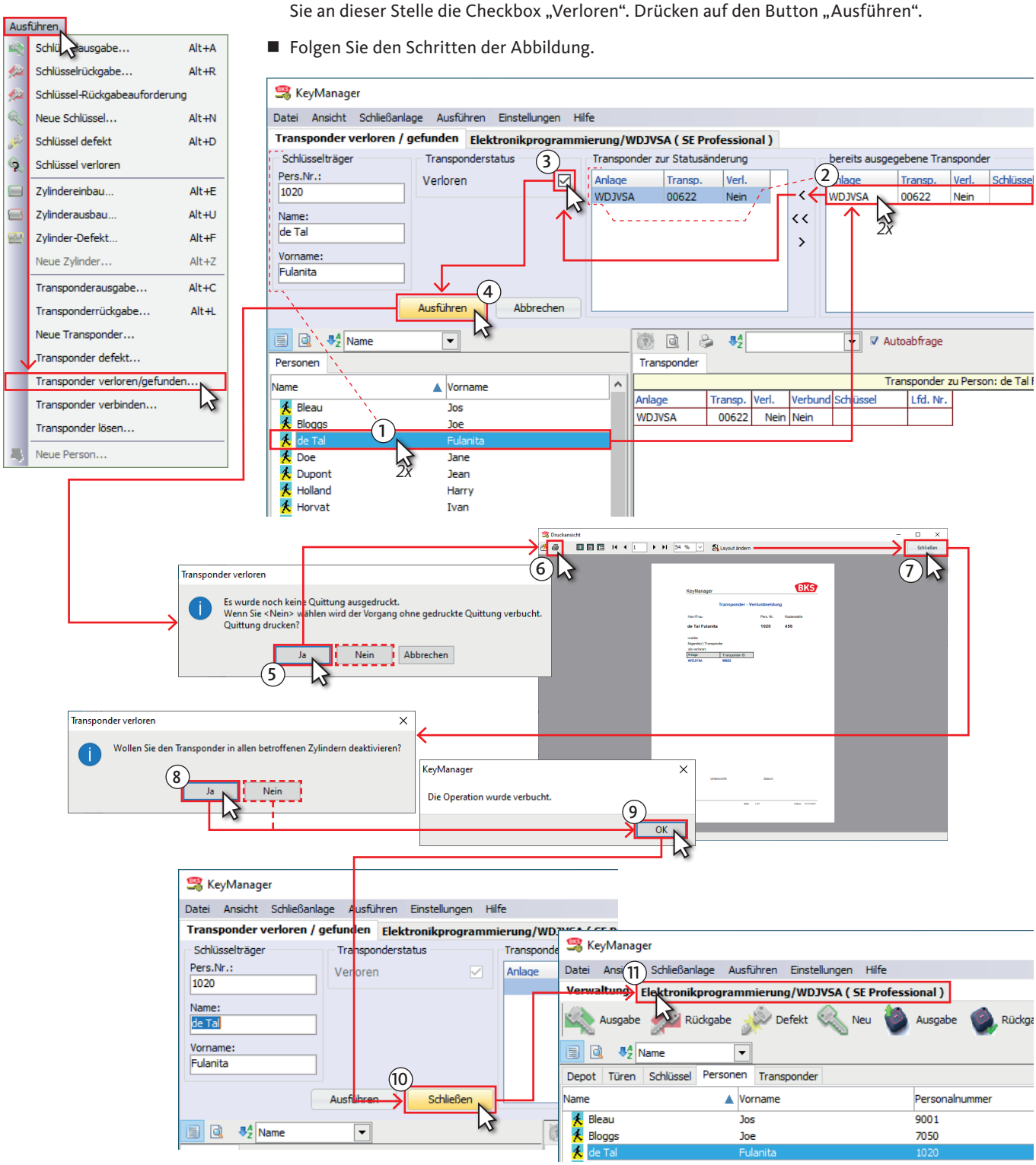


- Aktivieren Sie die Checkbox um die Berechtigungen zu den Zutrittspunkten zu entsperren. Drücken Sie zum Beenden auf „Schließen“.



4.2.4.4 Transponder verloren/gefunden (Verwaltungsmodul)

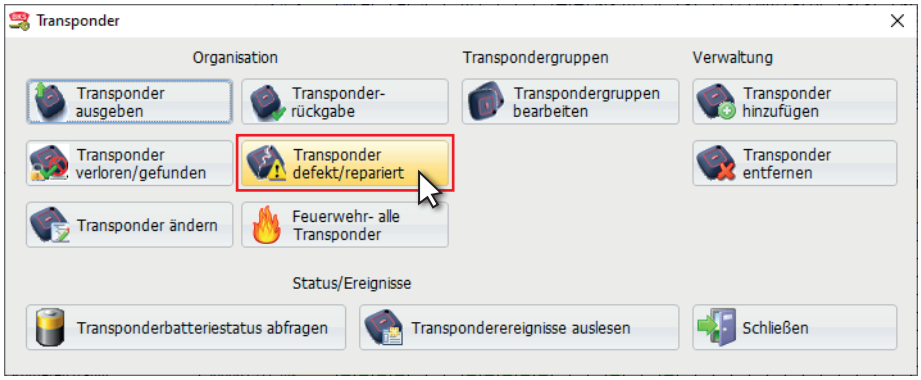
- Wählen Sie die Person, deren Transponder als verloren bzw. gefunden gebucht werden soll und den betreffenden Transponder mit einem Doppelklick aus.
- Aktivieren Sie die Checkbox „Verloren“. Ist der Transponder Gefundenen worden, deaktivieren Sie an dieser Stelle die Checkbox „Verloren“. Drücken auf den Button „Ausführen“.
- Folgen Sie den Schritten der Abbildung.



4.2.5 Transponder defekt/repariert

Transponder, die in Folge eines Defekts nicht mehr ausgegeben oder zur Rechtevergabe verwendet werden sollten, können mit der Funktion „Transponder defekt/repariert“ im BKS KeyManager als defekt markiert werden.

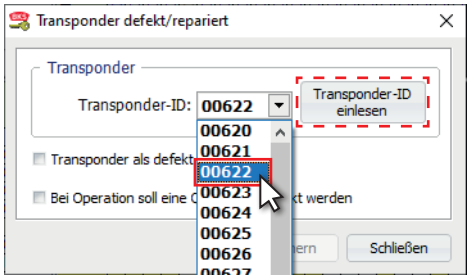
- Drücken Sie den Button „Transponder defekt/repariert“.

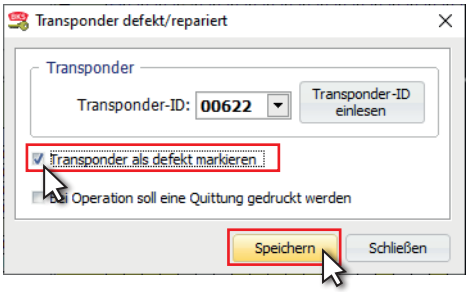


- Wählen Sie im Dropdown-Menü die ID des defekten Transponders aus.

Alternativ können Sie den Button „Transponder-ID einlesen“ drücken. Lesen Sie mit dem Programmiergerät den Transponder ein.

- Aktivieren Sie die Checkbox „Transponder als defekt markieren“. Drücken Sie auf „Speichern“.

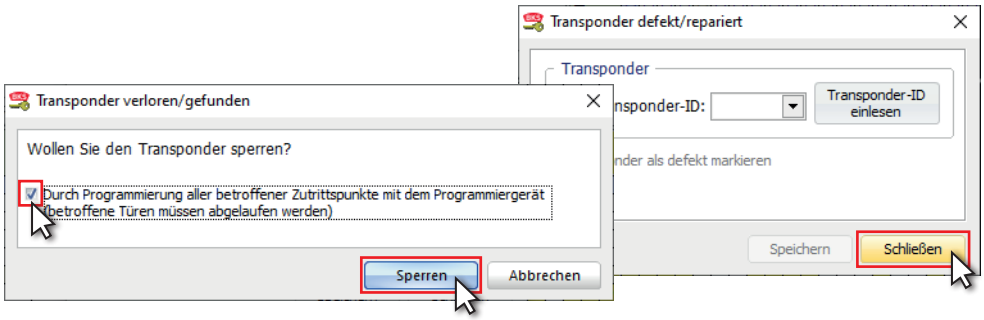




- Aktivieren Sie die Checkbox, das der betroffene Transponder in allen zutrittsberechtigten Zutrittspunkten gesperrt werden soll. Drücken Sie zum Beenden auf „Schließen“.

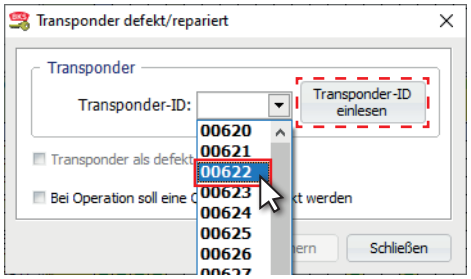
ACHTUNG

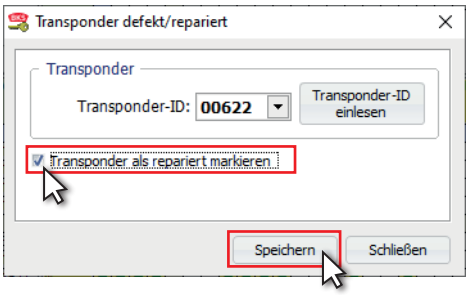
Wenn Sie diese Option wählen, wird pro Zutrittspunkt ein Programmierjob erzeugt, mit dem die Zutrittsberechtigung für den defekten Transponder entzogen wird. Wenn Sie sich dagegen entscheiden, behält der verlorene Transponder sämtliche Berechtigungen und kann missbräuchlich weiter verwendet werden.



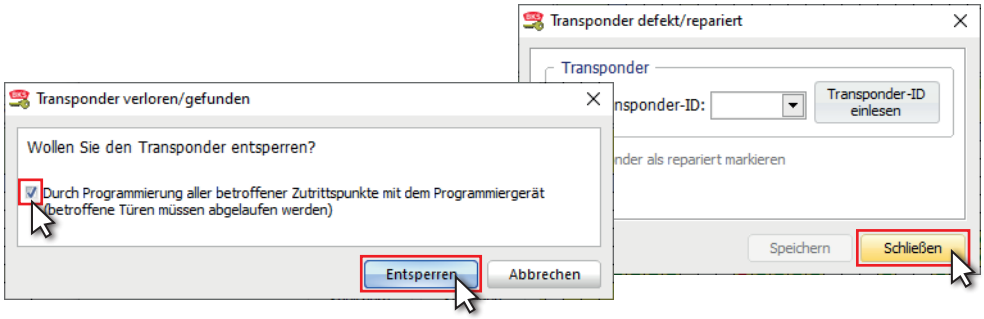
Kann ein defekter Transponder repariert werden, ist es möglich, diesen durch Entfernen der Markierung „defekt“ in der Schließanlage zu reaktivieren.

- Wählen Sie im Dropdown-Menü die ID des als repariert zu markierenden Transponders aus. Alternativ kann der Transponder automatisch über ein mit dem Computer verbundenes Programmiergerät eingelesen werden. Drücken Sie auf den Button „Transponder-ID einlesen“.
- Aktivieren Sie die Checkbox „Transponder als repariert markieren“ und drücken zur Bestätigung auf „Speichern“.





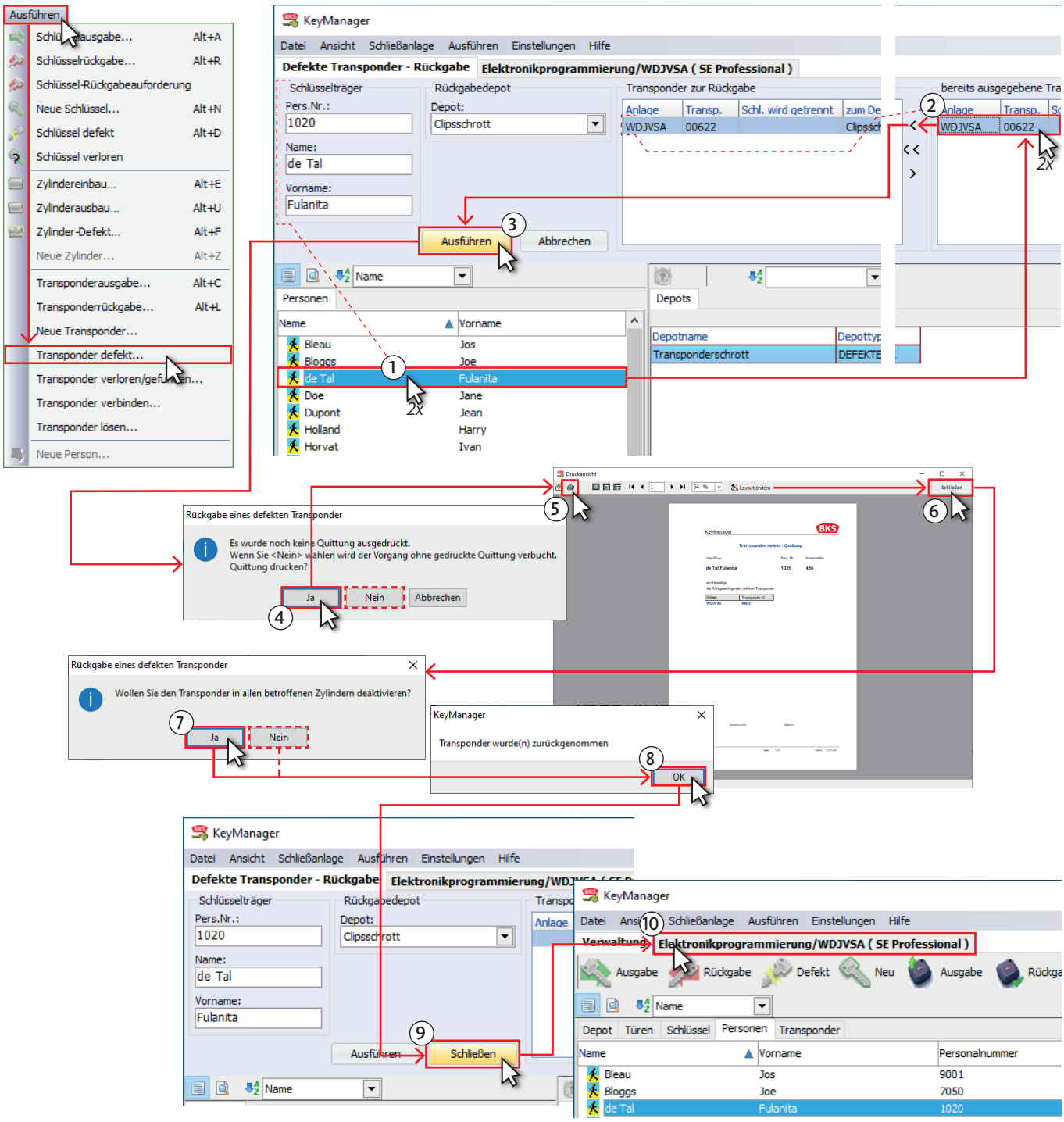
- Aktivieren Sie die Checkbox, um die Berechtigungen zu den Zutrittspunkten zu entsperren und drücken zum Beenden auf „Schließen“.



Beim Ausgeben eines neuen Transponders können Sie über die Option „Transponder ersetzt verlorenen Transponder“ den Defekten ersetzen und dessen Berechtigungen übernehmen, siehe Kapitel 4.2.2 [164]. Diese Option steht nur bei Data on Transponder-Anlagen (DoT) zur Verfügung.

4.2.5.1 Transponder defekt (Verwaltungsmodul)

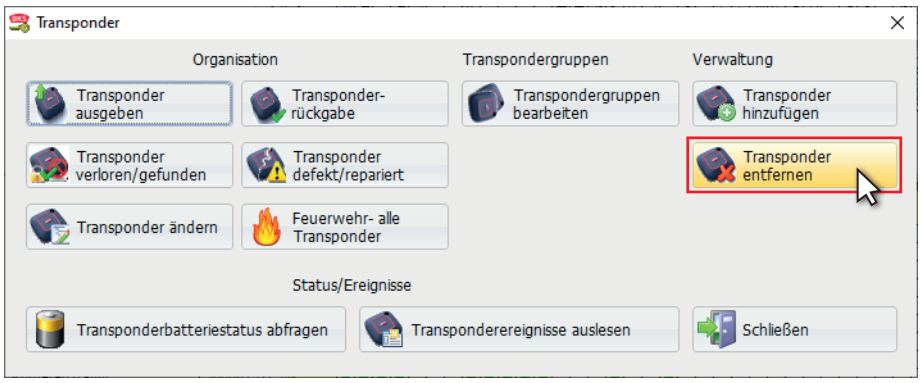
- Wählen Sie die Person, deren Transponder als defekt zurückgebucht werden soll und den betreffenden Transponder mit einem Doppelklick aus. Drücken Sie auf den Button „Ausführen“.
- Folgen Sie den Schritten der Abbildung.



4.2.6 Transponder entfernen

Mit der Funktion „Transponder entfernen“, werden defekte Transponder aus dem BKS KeyManager gelöscht. Der Transponder muss zuvor als „Defekt“ gekennzeichnet werden, siehe Kapitel 4.2.5 [181].

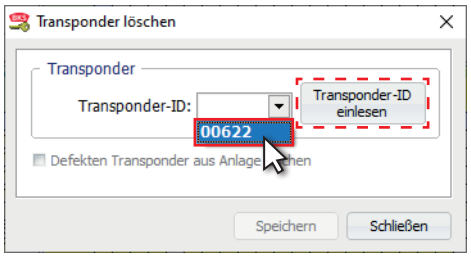
- Drücken Sie den Button „Transponder entfernen“.



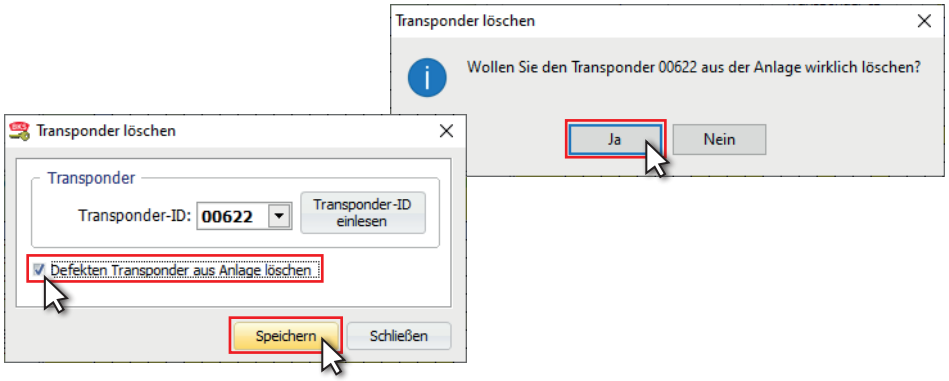
- Wählen Sie im Dropdown-Menü die ID des defekten Transponders aus.

Alternativ kann der Transponder automatisch über ein mit dem Computer verbundenes Programmiergerät eingelesen werden.

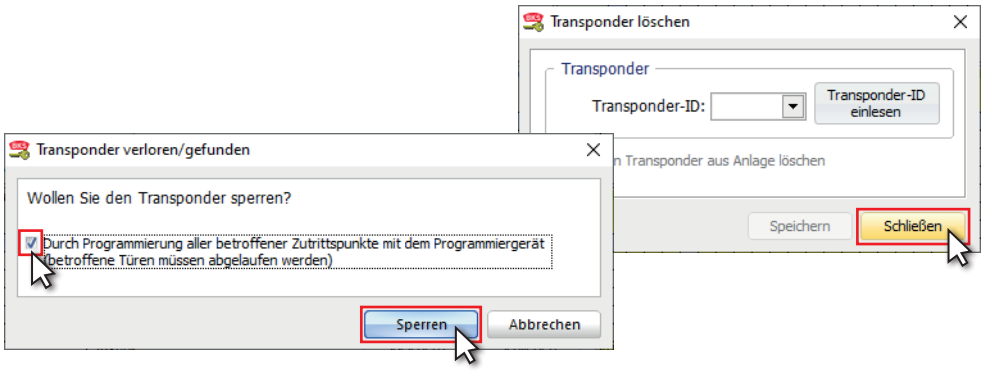
- Drücken Sie auf den Button „Transponder-ID einlesen“.



- Aktivieren Sie die Checkbox „Defekten Transponder aus der Anlage löschen“. Drücken Sie zum Beenden in beiden Fenstern auf „Speichern“ und „Ja“.



- Aktivieren Sie die Checkbox, das der betroffene Transponder in allen zutrittsberechtigten Zutrittspunkten gesperrt werden soll. Drücken Sie zum Beenden auf „Schließen“.



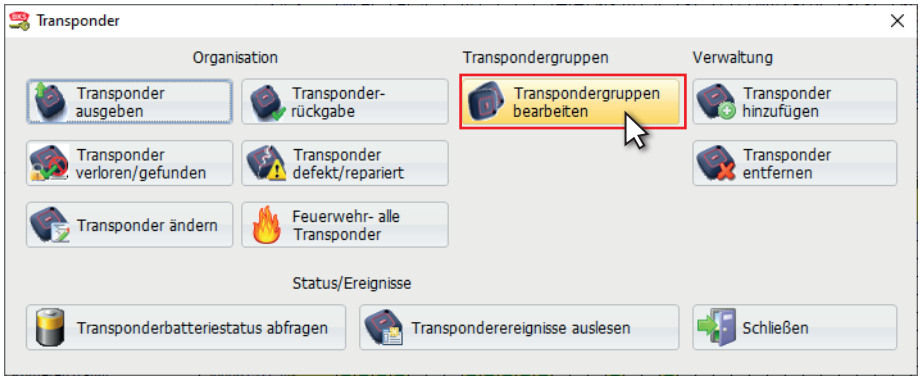
ACHTUNG

Wenn Sie diese Option wählen, wird pro Zutrittspunkt ein Programmierjob erzeugt, mit dem die Zutrittsberechtigung für den gelöschten Transponder entzogen wird. Wenn Sie sich dagegen entscheiden, behält der verlorene Transponder sämtliche Berechtigungen und kann missbräuchlich weiter verwendet werden.

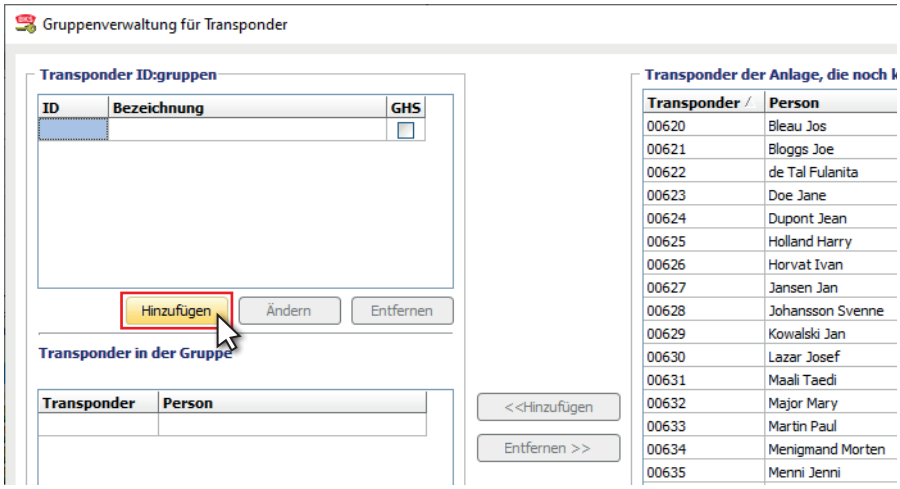
4.2.7 Transpondergruppen (DoT)

In einer Schließanlage haben häufig mehrere Transponder bzw. deren Besitzer die gleichen Zutrittsberechtigungen. Um diese Berechtigungen nicht jeweils einzeln pflegen zu müssen, empfiehlt es sich, solche Rechte über Transpondergruppen festzulegen. Neue Transponder mit den gleichen Rechten müssen dann nur noch einer vorhandenen Gruppe zugeordnet werden. Die Rechtevergabe zu jedem einzelnen Zutrittspunkt kann dann entfallen, weil der Transponder automatisch die Rechte der Gruppe bekommt. Bei der Programmierung in der Matrix des BKS KeyManagers können mit einem Mausklick die Rechte des gewählten Zutrittspunkts für die gesamte Gruppe festlegen werden.

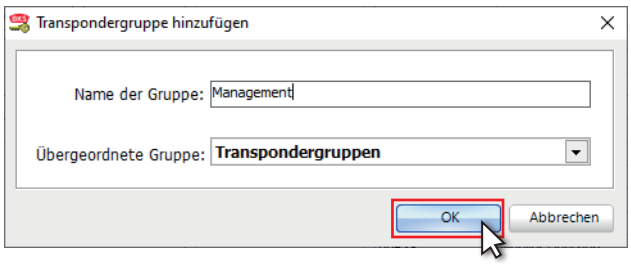
- Drücken Sie den Button „Transpondergruppen bearbeiten“.



- Drücken Sie auf den Button „Hinzufügen“, um die Transpondergruppe einzurichten.



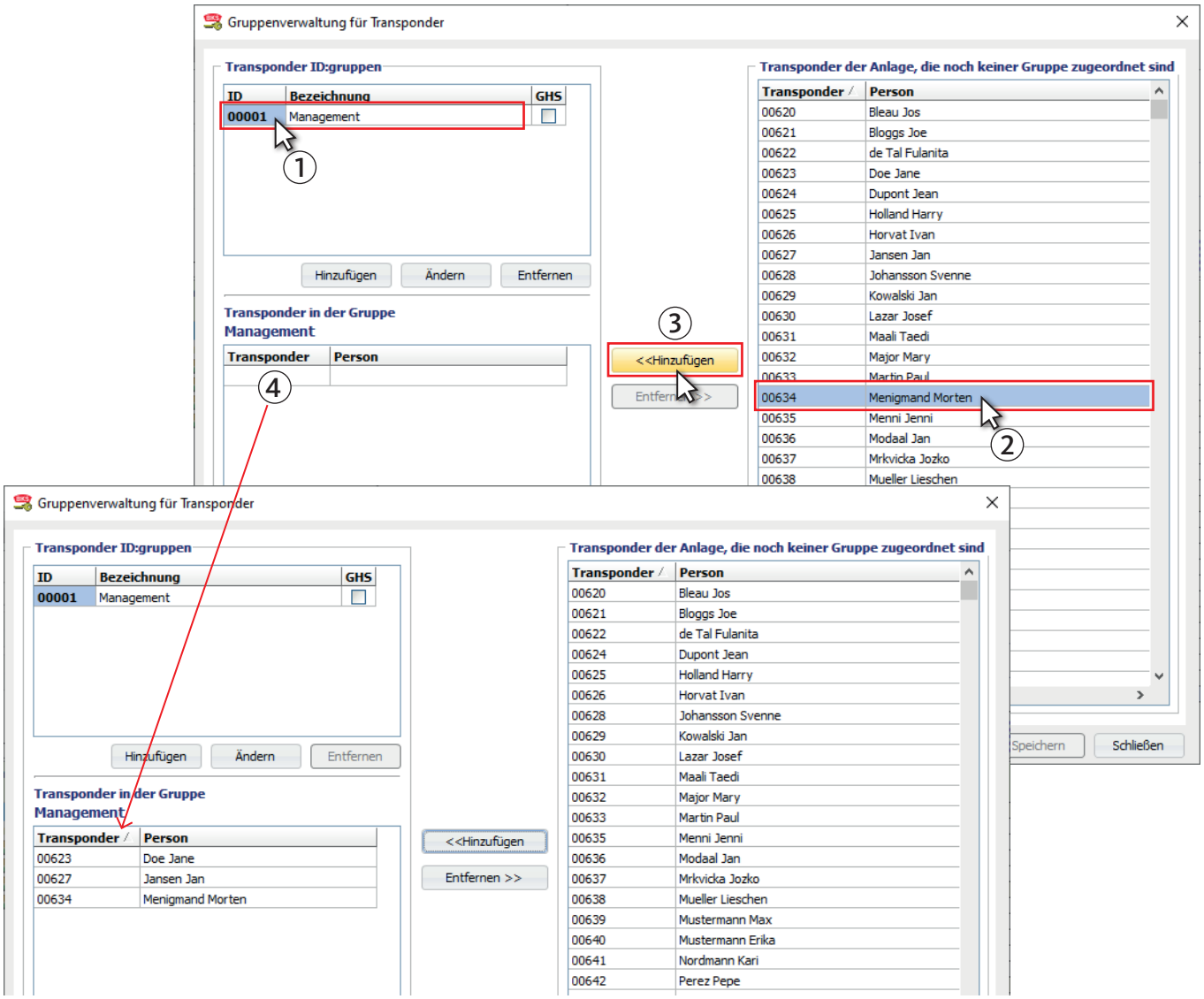
- Geben Sie den für die Gruppe gewünschten Namen ein. Drücken Sie zur Bestätigung auf „OK“.



Diese Transponder-Gruppe ist jetzt im Inventar der Schließanlage und es können ihr Transponder bzw. Personen zugeordnet werden.

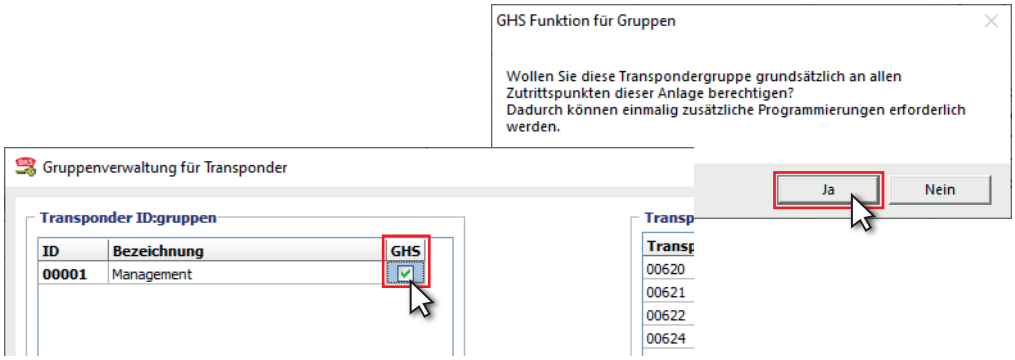
Das Fenster „Gruppenverwaltung für Transponder“ ist in drei Bereiche unterteilt:
– Liste der Gruppen.
– Übersicht der zur Gruppe zugeordneten Transponder bzw. Personen.
– Übersicht der Transponder bzw. Personen, die keiner Gruppe zugeordnet sind.

- Wählen Sie in der Übersicht „Transponder-Gruppe“ eine Gruppe zur Bearbeitung aus.
- Markieren Sie den gewünschten Transponder bzw. Person im rechten Teil der Ansicht.
- Drücken Sie auf den Button „<<Hinzufügen“ und der gewählte Transponder bzw. Person wird in die Gruppe verschoben. Ein Doppelklick auf den Transponder bzw. Person hat den gleichen Effekt.
- Wiederholen Sie den Vorgang und ergänzen die Gruppe um weitere Transponder bzw. Personen mit den gleichen Zutrittsberechtigungen.

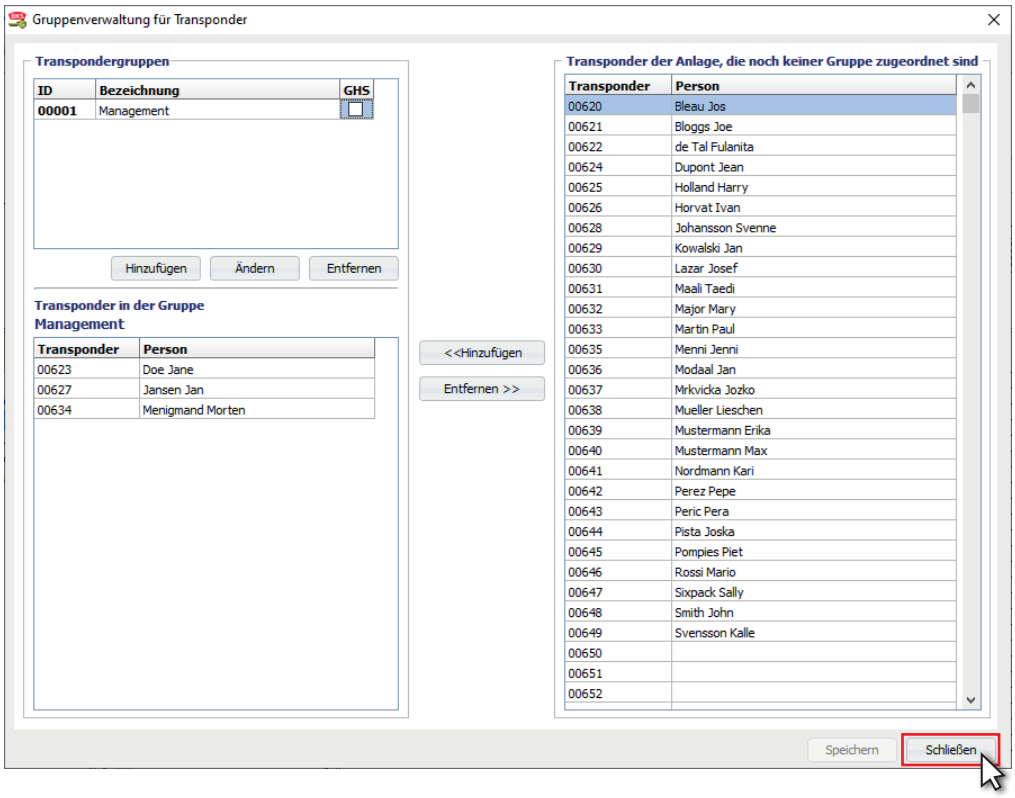


In der Liste der Gruppen ist es möglich, das Attribut „GHS“ (Generalhauptschlüssel) für diese Transponder-Gruppe zu aktivieren. Jeder Transponder dieser Gruppe bekommt dadurch automatisch Zutritt zu jedem Zutrittspunkt der Anlage. In der Matrix „Elektronikprogrammierung“ werden die Gruppenmitglieder mit einem Quadrat für die Zeitzone „Immer“ gekennzeichnet.

- Aktivieren Sie für eine Gruppe, die immer die Berechtigung zu einem Zutritt haben soll, die Checkbox „GHS“ und drücken zur Bestätigung auf „Ja“.



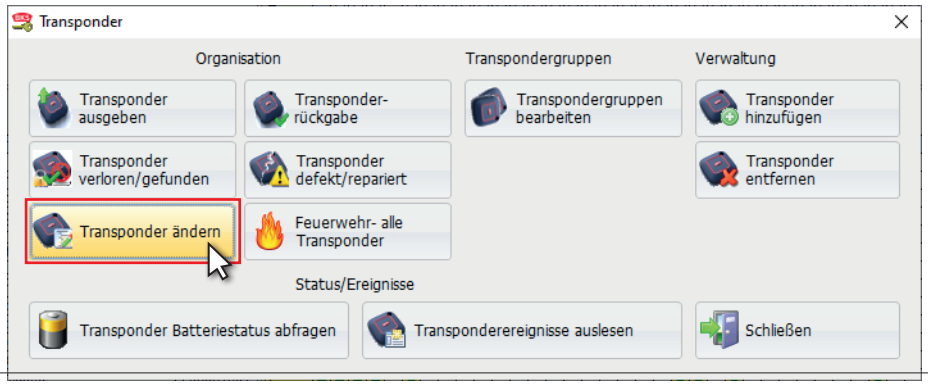
- Drücken Sie auf den Button „Schließen“ zum Beenden der Gruppenverwaltung der Transponder.



4.2.8 Transponder ändern

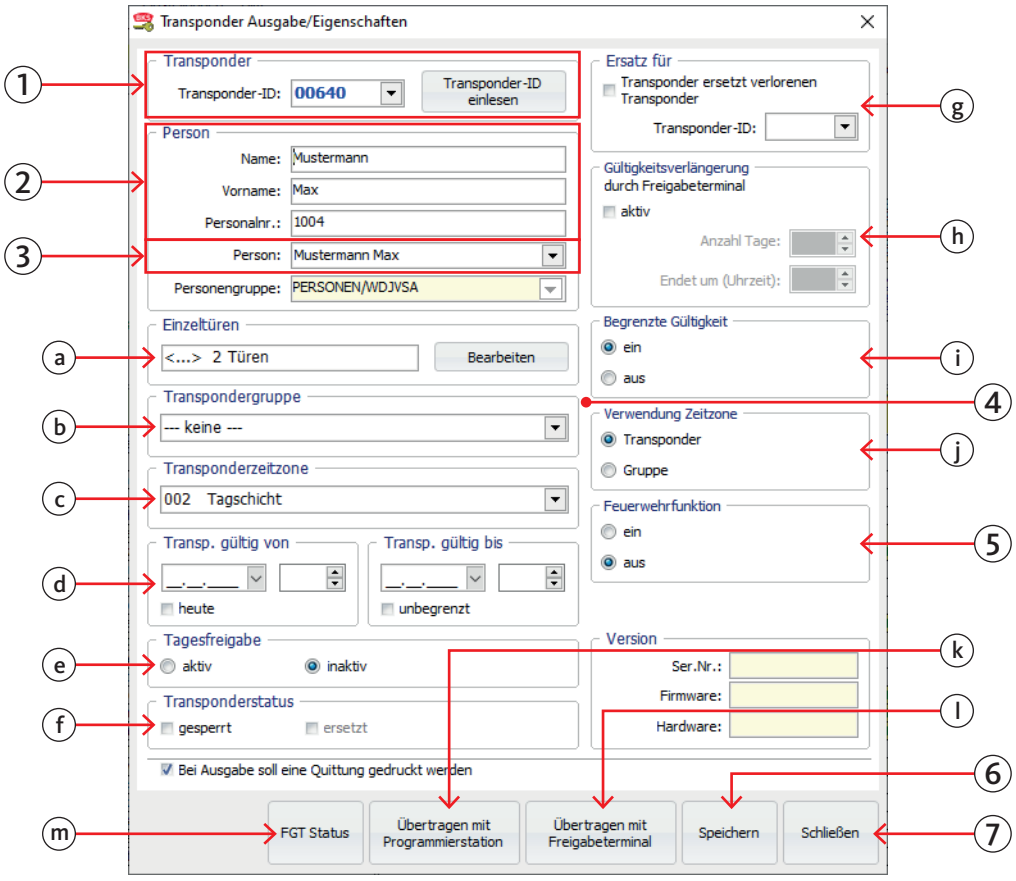
Mit der Funktion „Transponder ändern“ können bei einer DoT-Schließanlage die Einstellungen des Transponders verändern. Die Beschreibung zu den einzelnen Einstellungen finden Sie sind im Kapitel 4.2.2 [164]. Bei Einlesen des Transponders über ein Programmiergerät wird zu diesen Einstellungsmöglichkeiten auch der Batteriestatus (nur bei DoT) abgefragt und in der Matrix angezeigt.

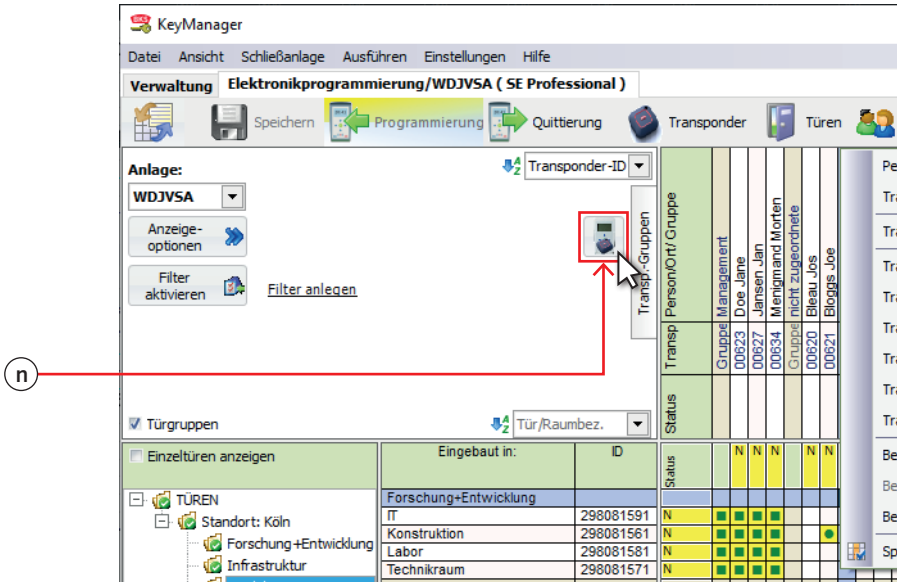
- Drücken Sie den Button „Transponder ändern“.



HINWEIS **Der Dialog kann alternativ durch einen Doppelklick auf einen Transponder im Spaltenkopf der Matrix geöffnet werden (nur bei DoT).**

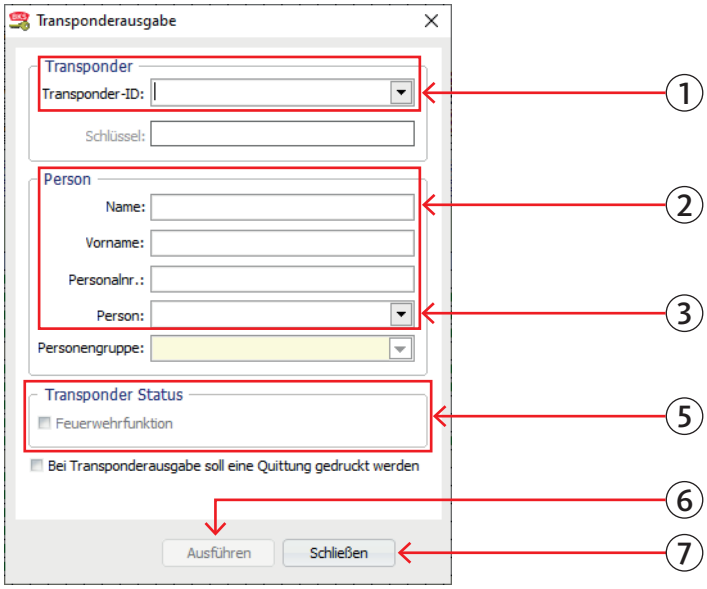
Menü bei einer Data on Transponder-Anlage (DoT)

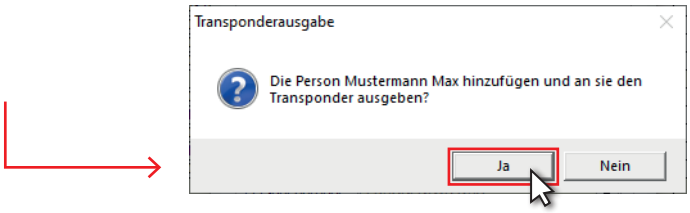




(Menü bei einer DoT-Anlage)

(Menü bei einer nonDoT-Anlage)





Folgende Eingaben können bei der Einrichtung oder Überarbeitung des Transponders in den Eingabefeldern des Fensters „Transponderausgabe“ bearbeitet werden:

Nr.	Eingabe	Beschreibung
1	Transponder	Der gewählte Transponder wird im entsprechenden Feld angezeigt. Bei leerem Auswahlfeld kann über das Dropdown-Menü ein Transponder ausgewählt oder durch Drücken des Buttons „Transponder-ID einlesen“, der Transponder über das Programmiergerät eingelesen werden.
2	Person	Eingabe-/Auswahlfelder für die Person an welche der Transponder ausgegeben werden soll. Ist diese Person nicht auf der Dropdown-Liste (3) vorhanden, können Sie manuell die Felder der Personendaten ausfüllen und so eine neue Person anlegen.
3	Personenliste	Wählen Sie im Dropdown-Menü der Personenliste die Person aus, zu welcher der Transponder zugeordnet und ausgegeben werden soll.
4	Konfiguration (nur DoT)	Konfiguration des Transponders mit den in der „Data on Transponder“-Schließanlage (DoT) vorhandenen Berechtigungen und Auswahlmöglichkeiten.

HINWEIS

Bei einer DoT-Schließanlage werden die Einzelberechtigungen auf den Transpondern gespeichert. Aus diesem Grund werden bei DoT-Schließanlagen die Transponder programmiert.

a b c	Zutrittsberechtigung	Bestimmen Sie die Zutrittsberechtigungen durch Auswahl der Einzeltüren (a) und/oder über die Rechte der Tranpondergruppen (b) sowie der Zeitzonen (c) der Transponder. Wählen Sie mit „Bearbeiten“ die Einzeltüren bzw. über die Dropdown-Menüs die Gruppen oder Zeitzonen aus. In der Hierarchie haben die Rechte der Transponder immer Priorität vor den Rechten der Gruppe.
d	Gültigkeitsdauer	Mit der absoluten Gültigkeitsdauer des Transponders wird eine Limitierung der Verwendung durch die Festlegung eines fixen Zeitraums der Gültigkeit festgelegt.
e	Tagesfreigabe	Die Funktion Tagesfreigabe wird im Transponder durch Aktivierung der Checkbox „aktivieren“ freigeschaltet. Ist im Zutrittspunkt ebenfalls die Funktion Tagesfreigabe aktiviert und der Transponder berechtigt, wird bei Präsentation mit einem langen Druck auf den Button des Transponders am Zutrittspunkt eine dauerhafte Berechtigung zum Zutritt erteilt. Diese ist bis zum Widerruf oder Ablauf der Berechtigungszeitzone im Modus „Halbautomatisch“ beim nächsten Präsentieren mit einem langen Druck auf den Transponder gültig. Ein kurzer Druck löst eine Kurzzeitfreigabe aus.
f	Transponderstatus (sperren)	Der Transponder verliert durch Aktivierung des Transponderstatus „gesperrt“ alle Zutrittsberechtigungen. Der Transponderstatus gesperrt betrifft den Transponder selbst. Der Transponder muss hierzu programmiert werden. Diese Funktion ist z. B. bei Verlust des Transponders zu aktivieren. Die Checkbox „ersetzt“ wird markiert, nachdem der Transponder ersetzt (g) wurde.

Nr.	Eingabe	Beschreibung
g	Ersatz für	Ein verlorener Transponder kann durch den aktuell gewählten Transponder ersetzt werden. Wählen Sie die ID des zu ersetzenden Transponders aus. Die Rechte des ersetzten Transponders können übernommen werden und ersetzen die vorhandenen Rechte. Die Berechtigungen des ersetzten Transponders können gesperrt werden. Bei aktiven FGT und vorher gesperrten (f) zu ersetzenden Transponder kann die Sperrung auch mit Hilfe von Transpondern übertragen werden.
h	Gültigkeits-verlänge-rung durch Freigabe-terminal	Die relative Gültigkeit des Transponders wird durch Aktivierung der Checkbox „aktiv“ und setzen eines Intervalls wirksam. Bis zum Ablauf dieses Zeitraums ist der Transponder gültig und muss, um diese weiterhin zu behalten, an einem Freigabeterminal eingebucht werden, um das Intervall neu zu starten. Nach Ablauf des Zeitraums ohne Gültigkeitsverlängerung verliert der Transponder seine Berechtigungen und muss vor erneuter Verwendung an den Zutrittspunkten durch Präsentation am Freigabeterminal wieder aktiviert werden.
i	Begrenzte Gültigkeit	Mit der begrenzten Gültigkeit wird die in (d) festgelegte absolute Gültigkeit aktiviert/deaktiviert.
j	Verwendung Zeitzone	Durch die Aktivierung der Checkbox „Transponder“ ist die Verwendung der Transponderzeitzone (c) möglich. Wird die Checkbox „Gruppe“aktiviert ist die Transponderzeitzone (c) nicht mehr auswählbar.
k	Übertragen mit Program-mierstation	Die im Fenster „Transponder Ausgabe/Eigenschaften“ eingegebenen Daten können mit dem Programmiergerät auf den Transponder übertragen werden. Durch Drücken des Buttons „Übertragen mit Programmierstation“ wird der Transponder mit dem Programmiergerät programmiert.
l	Übertragen mit Freigabe-terminal	Wenn der BKS KeyManager über eine Netzwerk-/Onlineverbindung mit dem Freigabeterminal (FGT) verbunden ist, können mit dem Button „Übertragen mit Freigabeterminal“ die eingegebenen Daten zum FGT übertragen werden. Bei der ersten Übertragung kann im Online-Menü die automatische Übertragung aktiviert werden, wodurch die Daten mit dem Speichern automatisch an das FGT übertragen werden. Im zweiten Schritt werden beim Buchen des Transponders am FGT die Daten zum Transponder übertragen.
m	FGT Status	Funktion zur Ermittlung der Aktualität der Programmierdaten des jeweils gewählten Transponders auf den verschiedenen FGTs der Schließanlage. Anzeige zur Ermittlung von Differenzen z. B. durch das Offline-Gehen von FGTs während der Übertragung. Aktualisierung der Daten durch erneutes „Übertragen zum Freigabeterminal“ (l).
n	Datenübertra-gung	Alternativ kann die Übertragung der Daten über das Programmiergerät mit diesem Button aus der Matrixansicht gestartet werden, siehe Kapitel 3.8.1 [147].

Nr.	Eingabe	Beschreibung
5	Feuerwehr-funktion	Die Feuerwehrfunktion zum Energiesparen kann bei einer DoT-Schließanlage mit der Checkbox im Transponder aktiviert werden. Bei einer nonDoT-Schließanlage dient die Checkbox nur zur Anzeige, ob beim Transponder die Feuerwehrfunktion aktiv ist.
6	Speichern, Ausführen	Drücken Sie den Button „Speichern“ bzw. „Ausführen“ und im nächsten Fenster auf „Ja“, um Eingaben zu sichern.
7	Schließen	Geben Sie weitere Transponder aus oder schließen das Fenster. Bestätigen Sie zum Beenden mit „Ja“.

Über die Option „Bei Transponderausgabe soll eine Quittung gedruckt werden“, legen Sie fest, ob ein Formular zur Transponderausgabe gedruckt werden soll.

4.2.9 Feuerwehr-Transponder

Mit der Funktion „Feuerwehr-Transponder“ wird die Energiesparfunktion im Transponder aktiviert. Ist die „Feuerwehr-Funktion“ aktiv, reagiert der Transponder nicht auf Wecksignale von anderen Geräten.

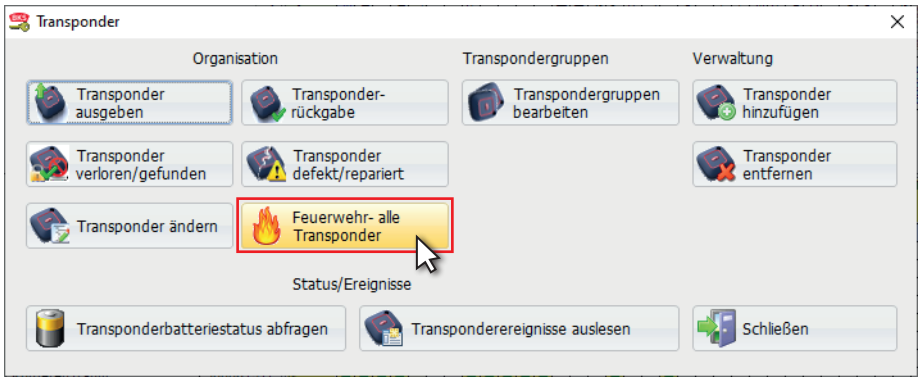
HINWEIS

Wird ein Transponder in einem Feuerwehrdepot aufbewahrt, dann sollte bei diesem Transponder die Feuerwehrfunktion im BKS KeyManager aktiviert werden.

Die Spannung der Batterie muss regelmäßig alle 6 Monate überprüft werden.

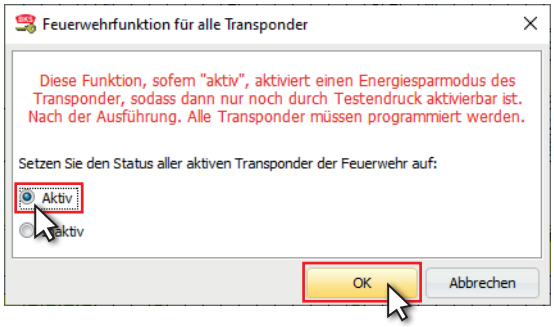
Durch einen Druck auf die Taste wird der Transponder eingeschaltet und kann Funktionen ausführen. Dadurch ist dieser Betriebsmodus sehr energiesparend.

- Drücken Sie auf den Button „Feuerwehr-Transponder“ (**DoT-Anlage**).



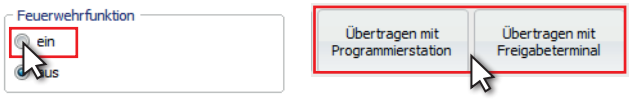
Im Fenster „Feuerwehrfunktion für alle Transponder“ kann diese Funktion in allen aktiven Transpondern aktiviert werden.

- Aktivieren Sie die Checkbox „Aktiv“ und drücken auf den Button „OK“.
- Im Weiteren ist zur Aktivierung der Funktion eine Programmierung der Transponder notwendig.

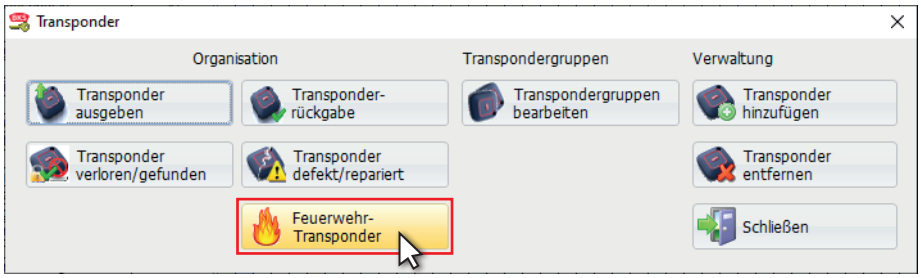


Alternativ kann die Feuerwehrfunktion in einzelnen Transponder aktiviert werden. Beachten Sie die Hinweise in Kapitel 4.2.2 [164] und Folgen der Beschreibung.

- Ergänzend zur Beschreibung wählen Sie den gewünschten Transponder aus. Aktivieren Sie im Bereich Feuerwehrfunktion die Checkbox „ein“ und starten durch Drücken des Buttons „Übertragen mit ...“ die Programmierung.



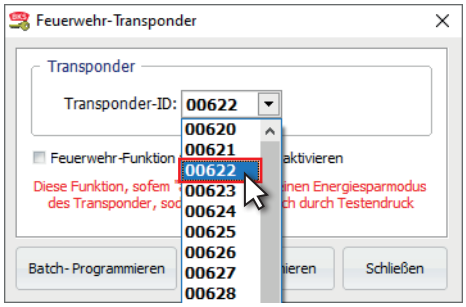
■ Drücken Sie auf den Button „Feuerwehr-Transponder“ (**nonDoT-Anlage**).

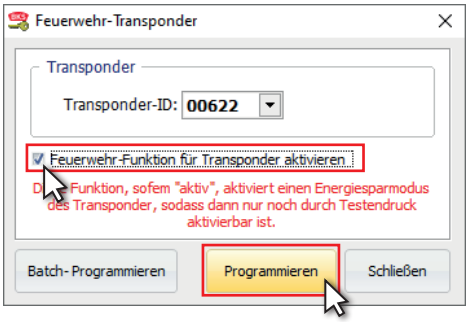


HINWEIS **Diese Funktion ist bei Transpondern ab der Firmware-Version 3.34 möglich.**

■ Wählen Sie im Dropdown-Menü die ID vom späteren Feuerwehr-Transponder aus.

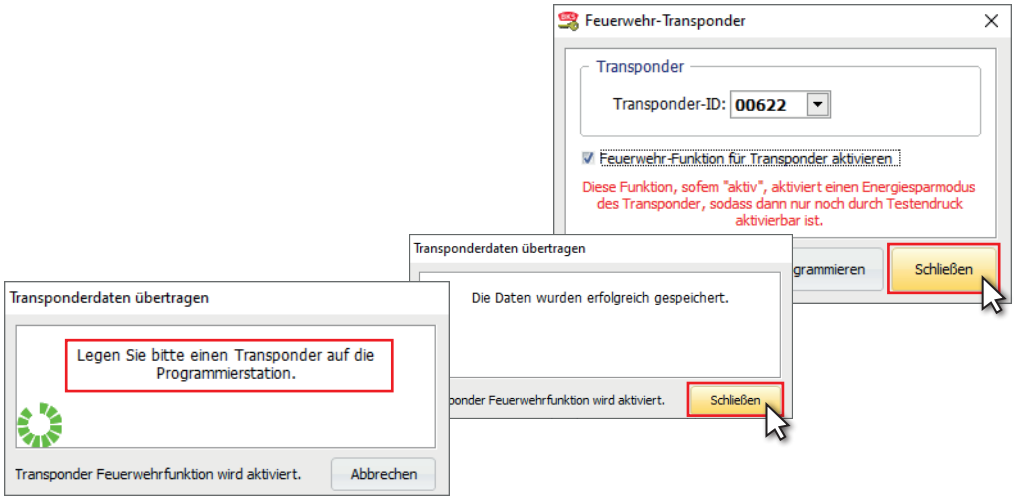
■ Aktivieren Sie die Checkbox „Feuerwehr-Funktion für Transponder aktivieren“. Drücken Sie auf den Button „Programmieren“. Alternativ können Sie mehrere Transponder mit dem Button „Batch-Programmieren“ nacheinander auflegen und programmieren.





Nachdem Sie den Transponder auf das Programmiergerät gelegt haben, werden die Konfigurationsdaten zum Transponder übertragen.

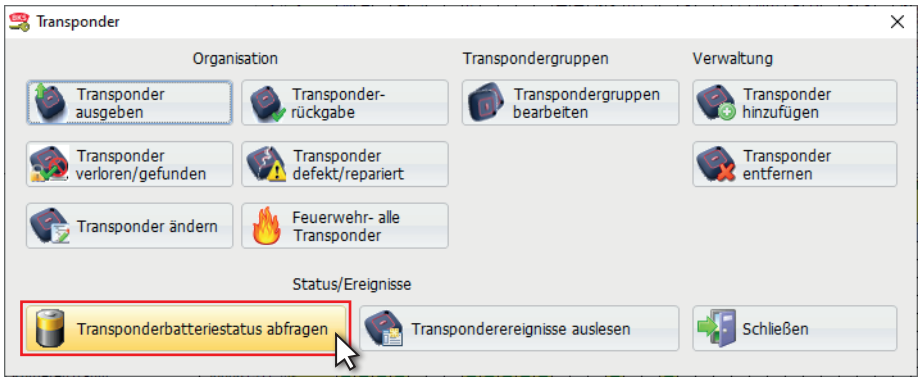
■ Drücken Sie zum Beenden in beiden Fenstern jeweils auf den Button „Schließen“.



Falls die Funktion „Feuerwehr-Transponder“ wieder deaktiviert werden soll, kann im gleichen Menü der Haken in der Checkbox „Feuerwehr-Funktion für Transponder aktivieren“ herausgenommen werden. Zum Programmieren muss jetzt die Taste des Transponders betätigt werden, damit der Transponder mit dem Programmiergerät kommunizieren kann.

4.2.10 Batteriestatus der Transponder abfragen (DoT)

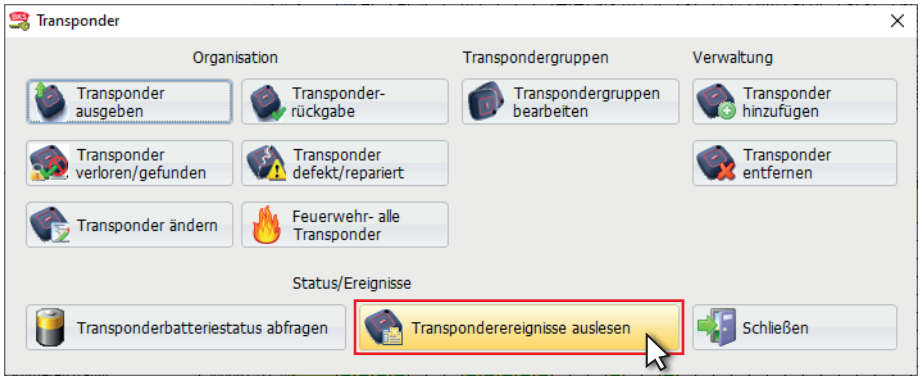
- Drücken Sie den Button „Transponderbatteriestatus abfragen“ und legen den Transponder zum Auslesen auf das Programmiergerät.



Der Batteriestatus wird Ihnen im folgenden Fenster und für dieses Auslesen in der Matrix der Schließanlage als Batterie-Symbol angezeigt.

4.2.11 Ereignisse aus den Transpondern lesen

- Drücken Sie den Button „Transponderereignisse auslesen“ und legen den Transponder zum Auslesen auf das Programmiergerät.



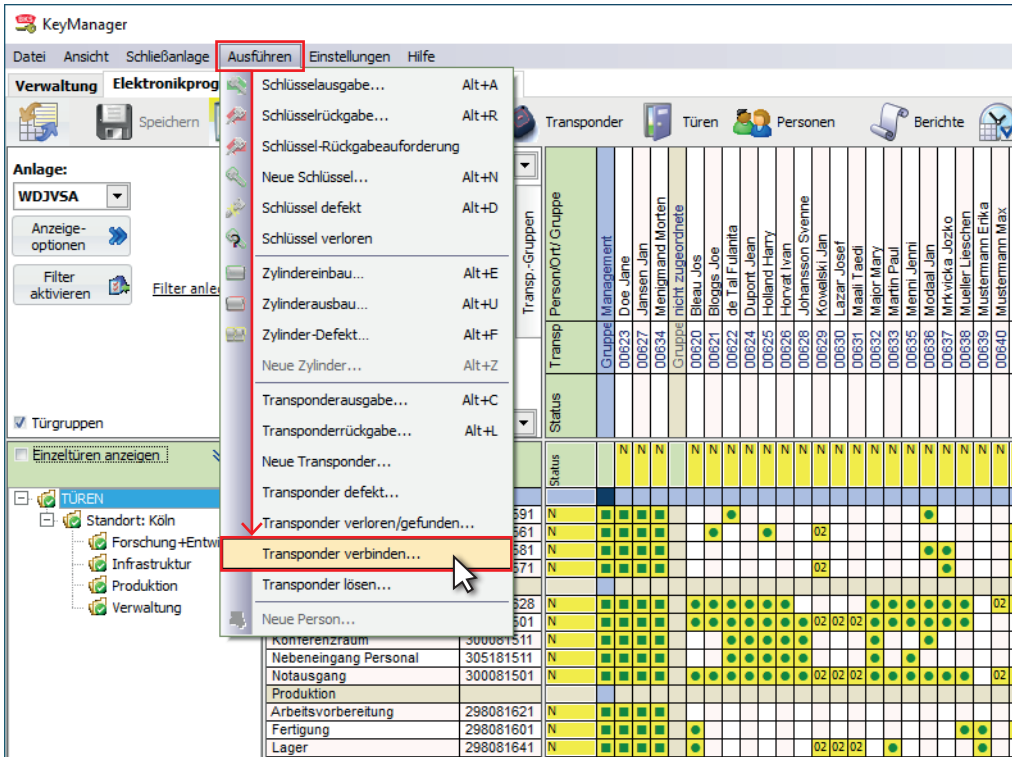
Die ausgelesenen Ereignisse können im Berichtemenü angezeigt werden, siehe Kapitel 4.6 [224].

4.2.12 Transponder mit mechanischen Schlüsseln verbinden

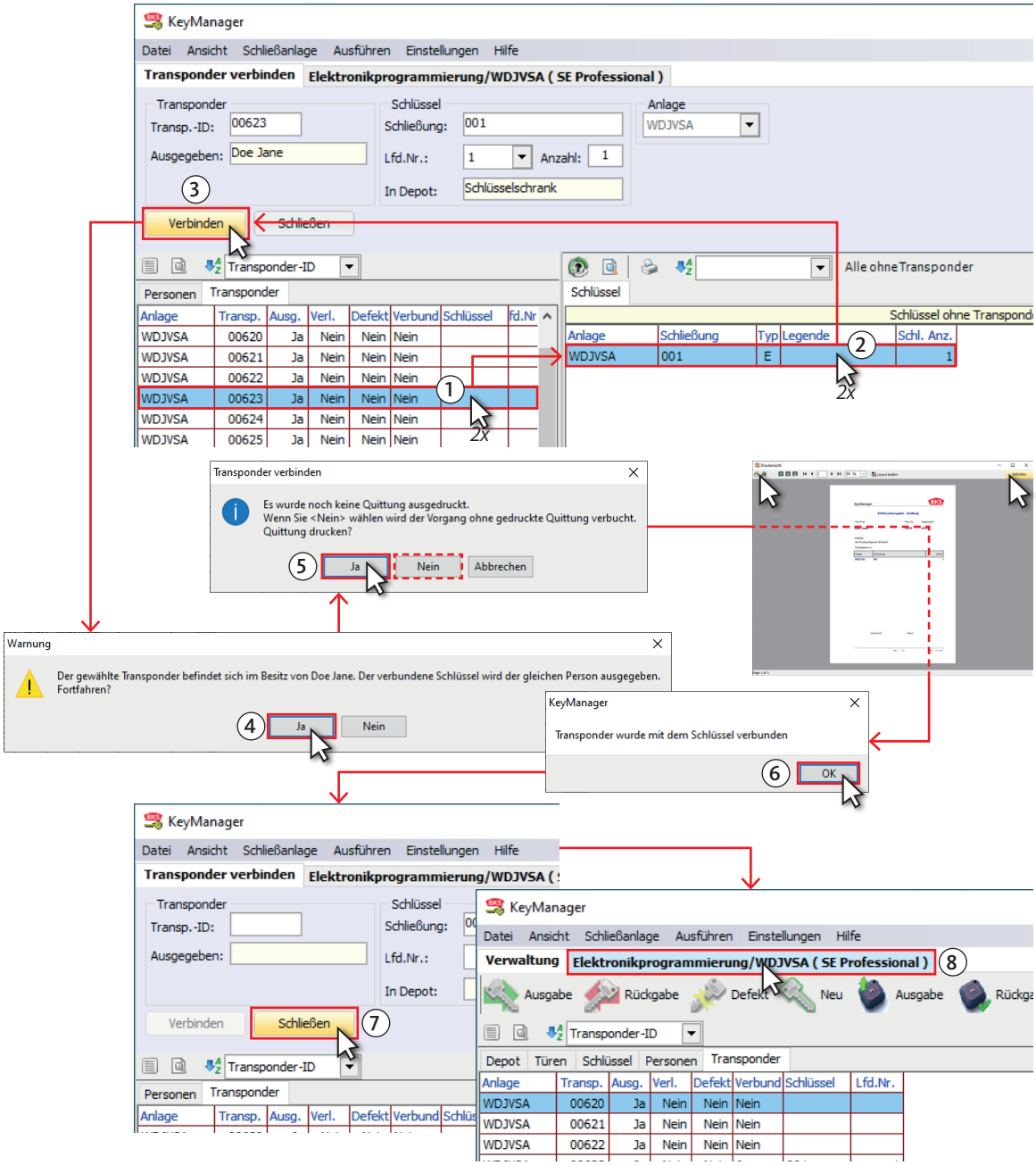
Die Transponder und die mechanischen Schlüssel der aktuellen BKS Schließanlagen-Serien können Sie zu einer Einheit zusammenbauen. Zum Zusammenbau von Transponder und Schlüssel muss zunächst die Unterschale des Transponders entfernt werden. Verwenden Sie zum Öffnen des Transponders das Öffnungswerkzeug B 5380 0002. Legen Sie den Schlüssel passend in die vorgesehene Kontur bzw. Aussparung in der Schlüsselaufnahmeschale ein und klipsen die Schale mit dem Schlüssel an die Stelle der Unterschale auf den Transponder. Je nach Bauform des Schlüssels ist eine Schlüsselaufnahme für symmetrische (B 5380 0102) und asymmetrische Schlüsselserien (B 5380 0103) zu verwenden.

Mit der Funktion „Transponder verbinden“ wird die mechanische Verbindung in der Schließanlage nachvollzogen und der Transponder mit dem Schlüssel auch im BKS KeyManager miteinander Verbunden. Sind Transponder und Schlüssel als Einheit zur Schließanlage geliefert worden, können Sie mithilfe der KWD-Datei diese als verbundene Einheit zur Anlage hinzufügen, siehe Kapitel 7.3.1 [367].

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Ausführen“ und wählen den Menüpunkt „Transponder verbinden ...“ aus.



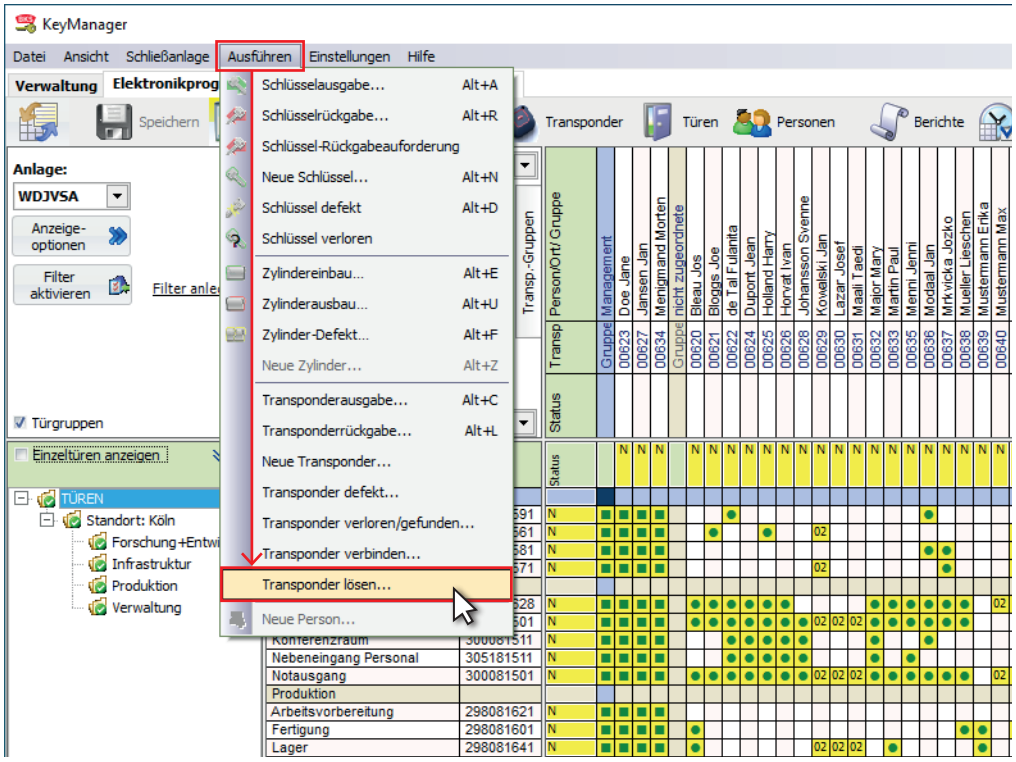
- Wählen Sie jeweils mit einem Doppelklick den Transponder und den Schlüssel, die miteinander verbunden werden sollen, in der Liste aus.
- Drücken Sie auf den Button „Verbinden“.
- Bestätigen Sie mit dem Button „Ja“ die Ausgabe des Schlüsseltransponders an die mit dem Transponder verbundene Person. Der Button „Nein“ führt zum Abbruch.
- Drücken Sie auf den Button „Ja“ zum Ausdruck einer Quittung für die Ausgabe bzw. auf „Nein“ für keine Quittung.
- Zur Bestätigung drücken Sie auf den Button „OK“. Zurück zur Berechtigungsmatrix gelangen Sie durch Drücken auf den Button „Schließen“ und das Register „Elektronikprogrammierung“.



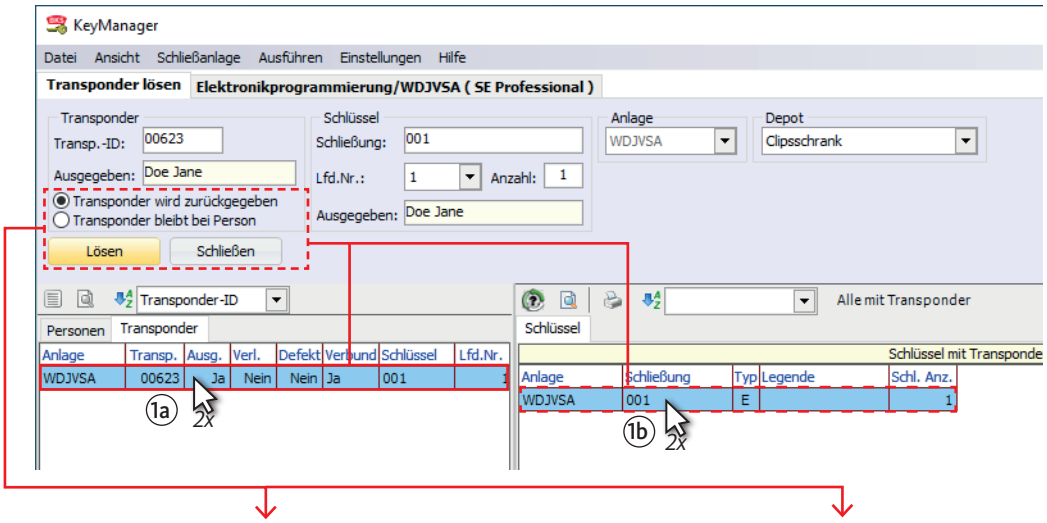
4.2.13 Verbindung Transponder mit mechanischen Schlüsseln lösen

Mit der Funktion „Transponder lösen“ heben Sie in der Schließanlage des BKS KeyManagers die Verbindung zwischen Transponder und mechanischen Schlüssel wieder auf.

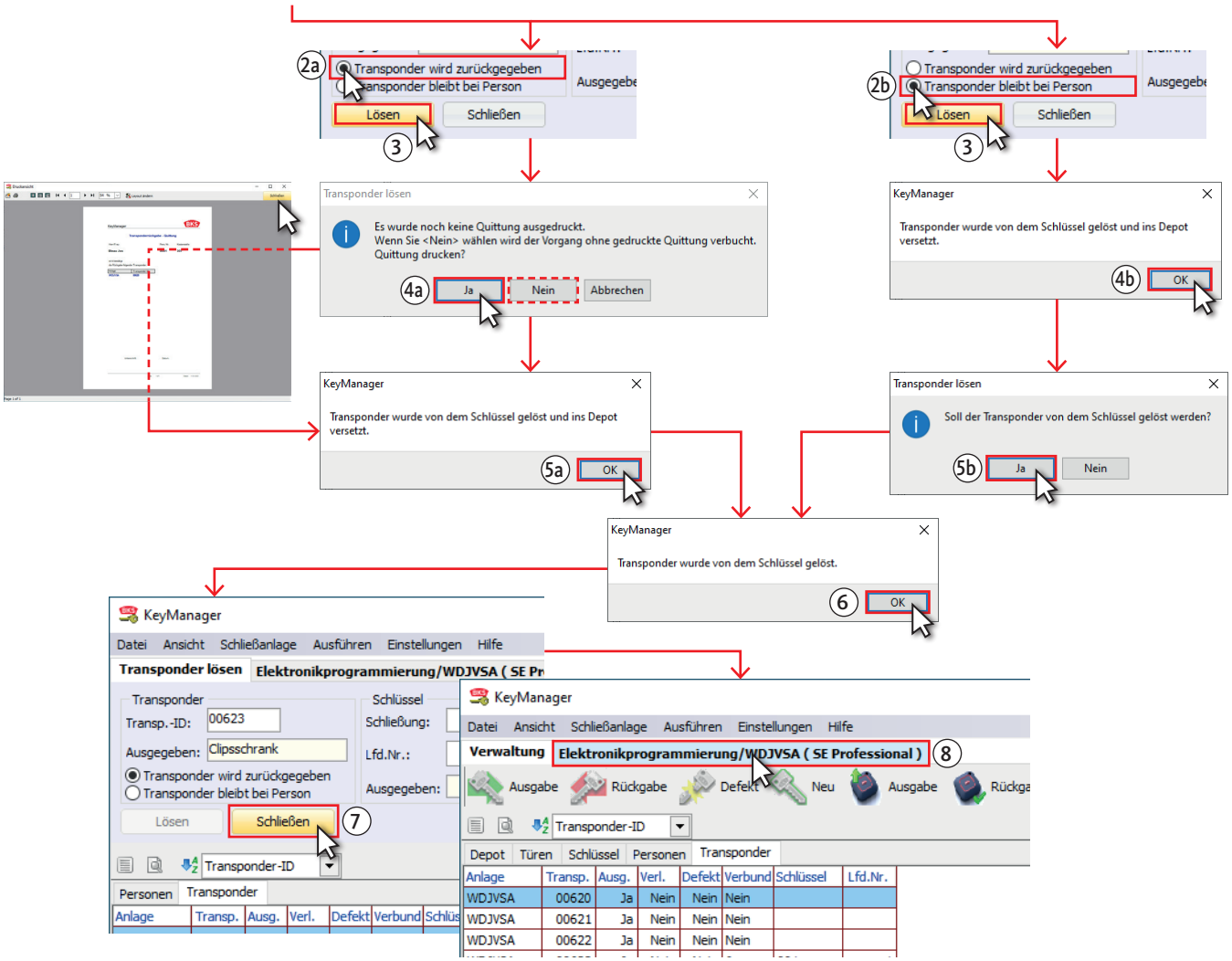
- Öffnen Sie in der Menüleiste das Dropdown-Menü „Ausführen“ und wählen den Menüpunkt „Transponder lösen ...“ aus.



- (1a) Wählen Sie mit einem Doppelklick in der Liste der Transponder den Transponder aus, der vom Schlüssel gelöst werden soll.
  (1b) Alternativ kann in der Liste der Schlüssel mit einem Doppelklick der Schlüssel von der zu lösenden Verbindung ausgewählt werden.



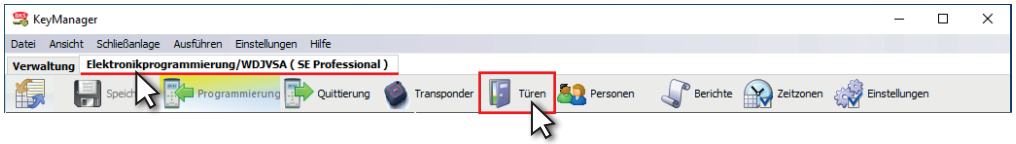
- Wählen Sie eine der beiden Checkboxen aus und legen den weiteren Verbleib des Transponders und Schlüssels nach dem Lösen der Verbindung fest.
  (2a) Die Checkbox „Transponder wird zurückgegeben“ ist zu wählen, wenn Transponder und Schlüssel getrennt und auch die Verbindung zur Person gelöst werden sollen. Die Option kann z, B. bei Rückgabe und Einlagerung verwendet werden.
  (2b) Die Checkbox „Transponder bleibt bei Person“ ist auszuwählen, wenn nur der Schlüssel zurückgegeben werden soll und der Transponder bei der Person verbleibt. Die Option kann z, B. für den Austausch des Schlüssels im Transponder verwendet werden.
- Drücken Sie auf den Button „Lösen“ (3).
- (4a) Drücken Sie auf den Button „Ja“ zum Ausdruck einer Quittung für die Rückgabe bzw. auf „Nein“ für keine Quittung. Der Button „Abbrechen“ führt zum Abbruch.
  (4b) Drücken Sie auf den Button „OK“ und bestätigen die Rückgabe des Schlüssels.
- (5a) Drücken Sie auf den Button „OK“ und bestätigen die Trennung und Rückgabe des Transponders und Schlüssels.
  (5b) Drücken Sie auf den Button „Ja“ und lösen die Verbindung. Der Button „Nein“ führt zum Abbruch.
- Zur Bestätigung drücken Sie auf den Button „OK“ (6). Zurück zur Berechtigungsmatrix gelangen Sie durch Drücken auf den Button „Schließen“ und das Register „Elektronikprogrammierung“.



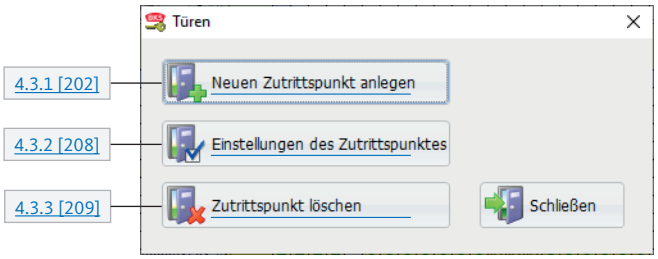
4.3 Türen/Zutrittspunkte

Das Menü „Türen“ kann über verschiedene Wege erreicht werden. Eine Möglichkeit ist der Aufruf über die horizontale Menüleiste und durch drücken auf den Menüpunkt „Türen“.

- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Türen“.

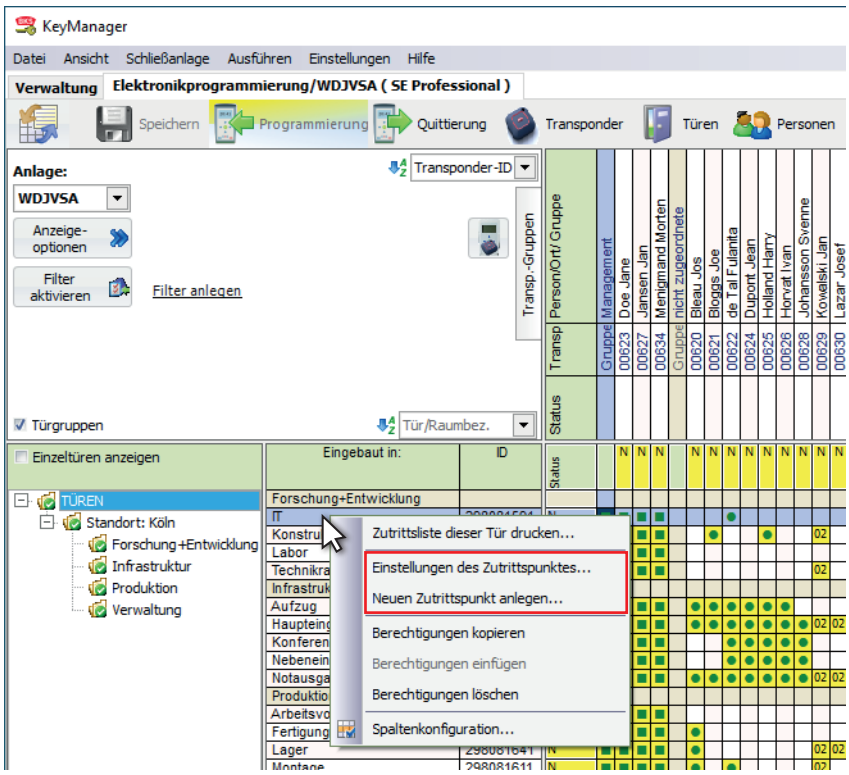


Im Menü „Türen“ lassen sich die folgenden Funktionen aufrufen.



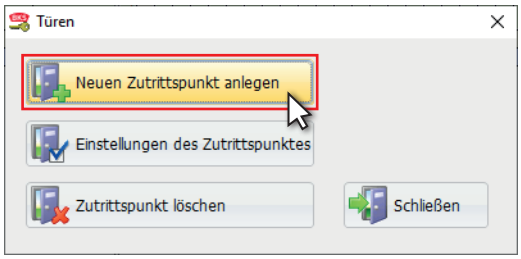
Alternativ können diese Funktionen teilweise über das Kontextmenü aufgerufen werden.

- Drücken Sie mit der rechten Maustaste auf die Zeile der zu editierenden Tür unter der Spalte „Eingebaut in:“. Es öffnet sich wie unten dargestellt das Kontextmenü.



4.3.1 Anlegen neuer Türen/Zutrittspunkte

- Zur Erstellung eines neuen Zutrittspunkts drücken Sie den Button „Neuen Zutrittspunkt anlegen“.



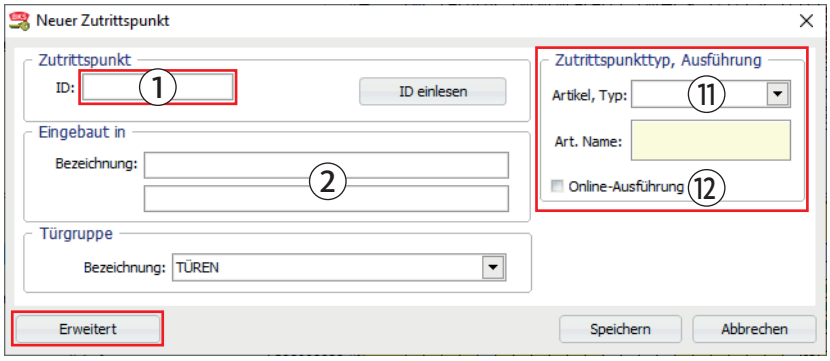
Die Erstellung eines neuen Zutrittspunkts in der Schließanlage wird im folgenden Dialog beschrieben. Die Felder „ID“ mit der Seriennummer und „Bezeichnung“ („Eingebaut in“) sind Pflichtfelder und müssen ausgefüllt werden.

Das nachfolgend abgebildete minimierte Fenster bietet die Möglichkeit, die Zutrittspunkte mit Standardparametern anzulegen. Wird das erweiterte Fenster angezeigt, können Sie durch Drücken des Buttons „Minimiert“ zur minimierten Ansicht wechseln.

- Geben Sie die Seriennummer des neuen Geräts (z. B. Zylinder, Schloss etc.) im Feld „ID“ ein.

Beachten Sie das die Felder „Zutrittspunkttyp, Ausführung“ (auch Online-Ausführung) nur beim Anlegen editiert werden können und später gesperrt sind.

Minimierter Dialog:

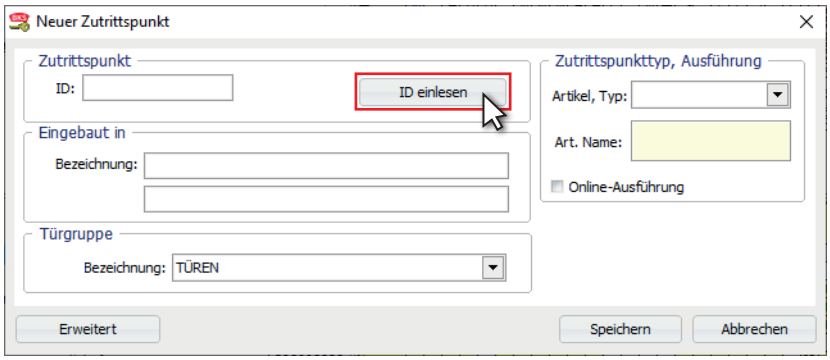


Das Fenster „Neuer Zutrittspunkt“ ist oben im minimierten Dialog abgebildet. Dort können die Standardparameter eingegeben werden. Für eine ausführlichere Ansicht wechseln Sie in den erweiterten Dialog. Hier können weitere Einstellungen und Änderungen für die Funktionen und Eigenschaften des Zutrittspunkts vorgenommen werden.

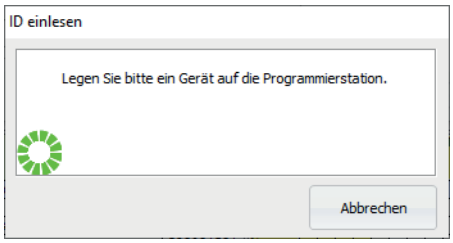
- Drücken Sie den Button „Erweitert“. Erläuterungen siehe „Erweiterter Dialog:“ auf Seite 205.

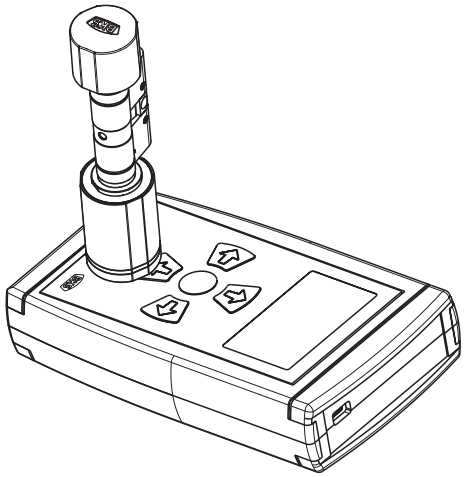
Alternativ kann der Zutrittspunkt mit einem Programmiergerät (SXPG) [B 5971 00x1] automatisch eingelesen werden. Verbinden Sie das Programmiergerät und den Computer mit einem USB-Kabel und warten, bis die Verbindung bestätigt ist.

- Drücken Sie auf den Button „ID einlesen“, um den Vorgang zu starten.



- Legen Sie den Zutrittspunkt, der eingelesen werden soll, auf das Programmiergerät.





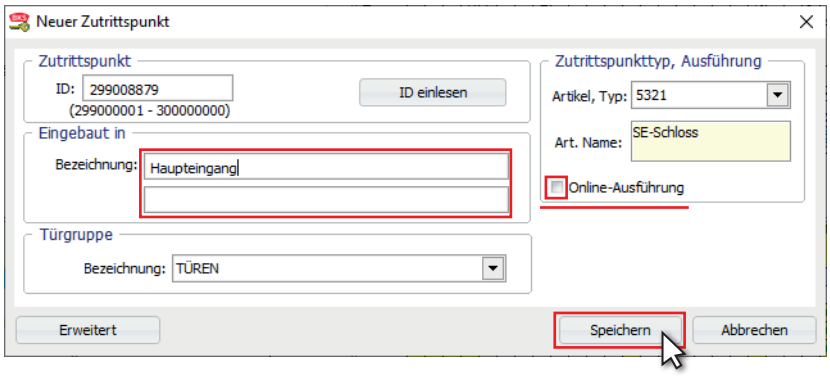
Der neue Zutrittspunkt wird angelegt.

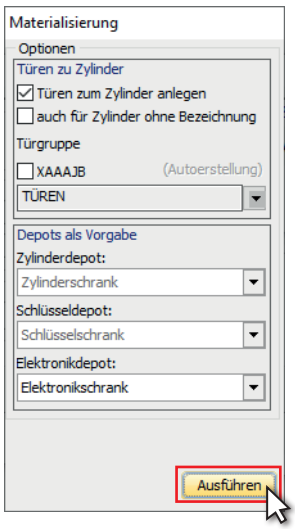
- Überprüfen Sie die Felder „Zutrittspunkttyp, Ausführung“ und ergänzen ggf. die Angaben zum Zutrittspunkt.
- Tragen Sie in das Feld „Bezeichnung“ den Namen, Einbauort, Standort etc. des Zutrittspunktes ein. Der Zutrittspunkt wird dadurch besser in der Berechtigungsmatrix auffindbar. Der Artikel-Typ wird automatisch mit der ID gepflegt.

HINWEIS

Bei onlinefähigen (Funk-) Produkten aktivieren Sie die Checkbox „Online-Ausführung“.
→ Diese Einstellung kann nur beim Anlegen editiert werden und ist später gesperrt.

- Drücken Sie auf den Button „Speichern“ zum Sichern der Eingabe.



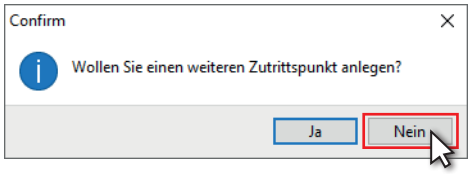


Nach dem Speichern wird der neu angelegte Zutrittspunkt materialisiert. Das ist die Zuordnung des Zutrittspunkts (z. B. Zylinder) zu einer Tür. Im System werden dadurch Türen zum Zylinder angelegt.

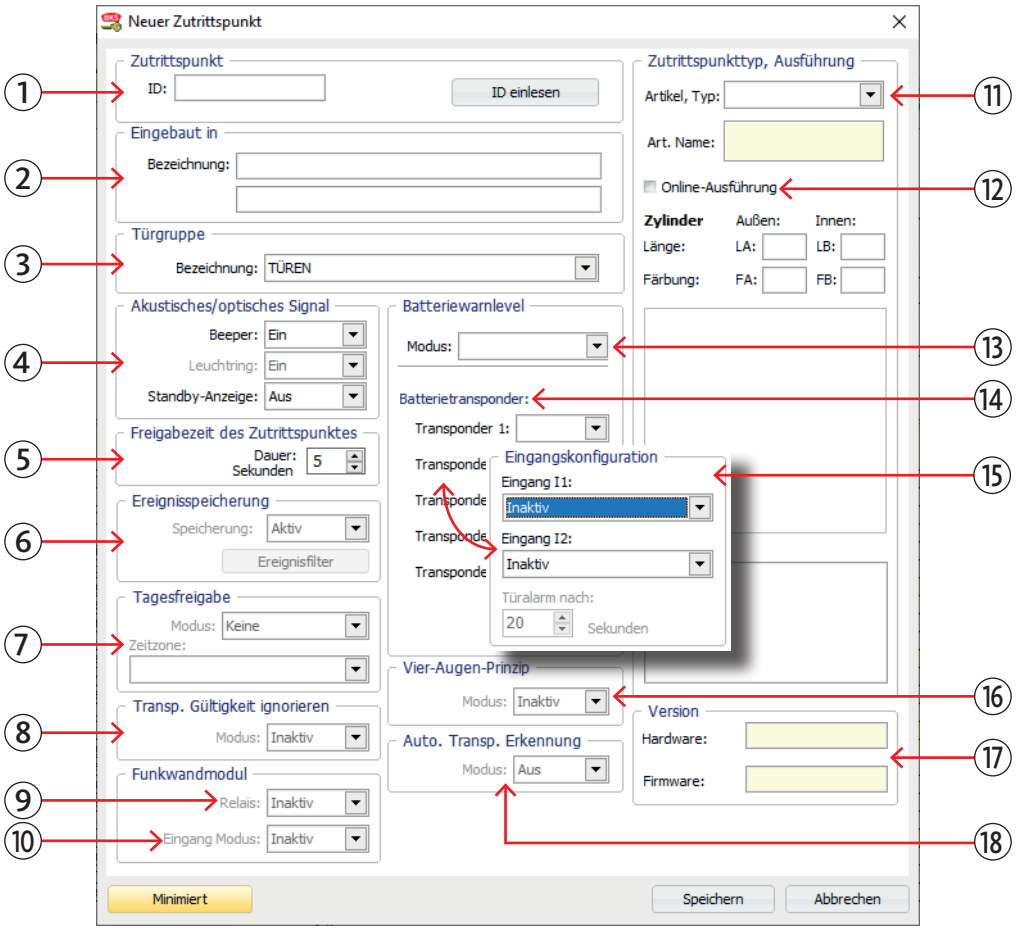
- Übernehmen Sie die Voreinstellung und drücken Sie „Ausführen“, um fortzufahren.

Im nächsten Fenster können Sie auswählen, ob ein weiterer Zutrittspunkt zur Schließanlage hinzugefügt werden soll.

- Drücken Sie auf den Button „Ja“, um einen weiteren Zutrittspunkt anzulegen.
- Drücken Sie auf den Button „Nein“, um den Assistenten zu beenden.

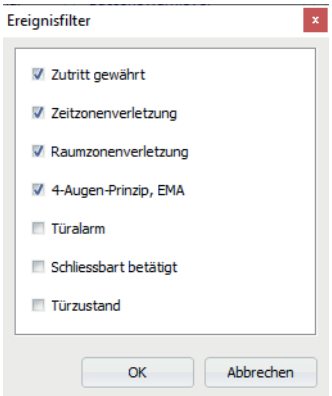


Erweiterter Dialog:



Folgende Eingaben können bei der Einrichtung oder Überarbeitung des Zutrittspunkts in den Eingabefeldern des Fensters bearbeitet werden:

Nr.	Eingabe	Beschreibung
1	ID	Dieses Eingabefeld ist für Seriennummer oder ID des Zutrittspunkts. Alternativ kann mit dem Button „ID einlesen“, die ID des Zutrittspunkts über ein Programmiergerät eingelesen werden. Die ID ist nach dem Speichern geschützt und nicht mehr editierbar. Eine nachträgliche Änderung der ID ist durch markieren und aufheben des Schutzes mit der Tastenkombination **„Strg“ + „Alt“ + „I“** möglich.
2	Eingebaut in	Die Tür-/Raumbezeichnung dient der Identifikation und wird in den verschiedenen Ansichten angezeigt.
3	Türgruppe	Zuordnung des Zutrittspunkts zu einer Türgruppe. Die Türgruppen ermöglicht eine Gliederung oder Ordnung der Anlage bzw. Unteranlage.
4	Akustisches Signal	Ein- oder Ausschalten des akustischen Signals bei Zutritten durch Setzen von „ein“ oder „aus“.

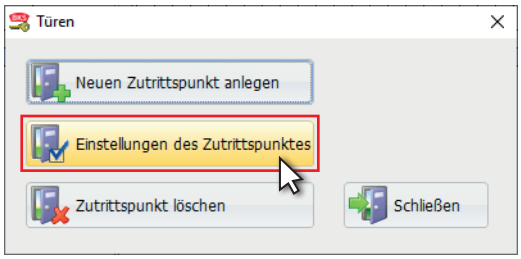
Nr.	Eingabe	Beschreibung
5	Freigabezeit des Zutritts-punkts	Einstellung der Freigabedauer des Zutrittspunkts (max. 240 s)
6	Ereignis-speicherung	*Aktiv:* Speicherung der Zutrittsereignisse des Zutrittspunkts mit Transponder-ID. *Aktiv ohne ID:* Anonyme Speicherung der Zutrittsereignisse ohne Transponder-ID. *Inaktiv:* keine Speicherung von Zutritten. *Ereignisfilter:* Einstellung, welche Ereignistypen der Zutrittspunkt lokal speichert. 
7	Tagesfreigabe	„Manuell“ ermöglicht die Freischaltung des Zugangs zu einem Zutrittspunkt ohne Abfrage der Berechtigung und ohne einen fest definierten Zeitraum bis zur Sperrung (Toggle-Funktion). Durch langen Tastendruck auf einen berechtigten Transponder wird ein Freigabeintervall gestartet und beendet. „Halbautomatisch“ ist eine Mischung aus manueller Tagesfreigabe, die innerhalb des zeitlichen Rahmens einer automatischen Tagesfreigabe gestartet und beendet werden kann. Nach Ablauf des Freigabeintervalls (Zeitzone) wird der Zutrittspunkt gesperrt. Die Aktivierung einer Tagesfreigabe außerhalb der Zeitzone ist nicht möglich. „Automatisch“ bedeutet, dass der Zutrittspunkt zeitgesteuert automatisch innerhalb der gewählten Zeitzone freigegeben und nach Ablauf des Zeitraums wieder gesperrt wird. Während des Freigabezeitraums ist der Zutrittspunkt ohne Abfrage der Berechtigung begehbar.
8	Transponder-gültigkeit ignorieren	Wenn diese Funktion aktiviert wird, werden die Gültigkeitsverlängerungen über Data on Transponder (DoT) durch das Freigabeterminal bei der Berechtigungsprüfung vom Zutrittspunkt nicht berücksichtigt. Dies kann erforderlich sein, wenn ein Zutrittspunkt, wie z. B. eine Parkschranke geöffnet werden soll, bevor die Gültigkeit am Freigabeterminal verlängert wird.
9	Relais im Wandmodul*	Bei einem erfolgreichen Zutritt wird ein Ausgang des zugeordneten SE-Funkmoduls Unterputz (SE FM UP) für 5 s geschaltet. * Nur in Verbindung mit Onlinezylinder und SE FM UP. Zusätzlich wird die Online Lizenz benötigt.
10	Eingang Wand-modul*	Wenn Sie diese Funktion aktivieren, ist die Zutrittssperre über den Eingang des Wandmoduls aktiv (EMA-aktiv). Diese Funktion ist in Kombination mit einer Einbruchmeldeanlage (EMA) sinnvoll. Ist die Einbruchmeldeanlage scharf und der Eingang gesetzt, haben alle Transponder (auch die berechtigten) keinen Zutritt mehr. * Nur in Verbindung mit Onlinezylinder und SE FM UP. Zusätzlich wird die Online Lizenz benötigt.

Nr.	Eingabe	Beschreibung
11	Artikeltyp	Artikeltyp (nur beim Anlegen editierbar, nachträglich ist keine Änderung möglich)
12	Online-Ausführung	Onlinefähiger Artikel mit Funkmodul (nur beim Anlegen editierbar, nachträglich ist keine Änderung möglich)
13	Batterie-warnlevel	Auswahl zwischen Modus „Sicherheit“ und „Komfort“ für das Verhalten eines janus SE-Zylinders im Batteriewarnlevel 2 (Aufforderung zum Wechseln der Batterie).
14	Batterie-transponder	Auswahl der Transponder, die im Batteriewarnlevel 2 schließen dürfen. Speziell für Zutrittspunkte, bei denen das Batteriewarnlevel 2 nicht über das SXPG zurückgesetzt werden kann.
15	Eingangs-konfiguration	Hier kann die Funktion des Schalteingangs eines Wandlesers kompakt eingestellt werden. *Inaktiv:* Der Eingang ist ohne Funktion. *Türkontakt:* Wird nach einem Zutritt die Tür nicht nach Ablauf der eingestellten Zeit geschlossen, so ertönt ein akustischer Alarm. *Kurzzeitfreigabe:* Das Freigabe-Relais wird für die eingestellte Freigabe-Dauer angesteuert. *Freigabe solange aktiv:* Solange der Eingang aktiv ist, wird das Freigabe-Relais angesteuert. *Zutritte gesperrt:* Wenn der Eingang aktiv ist, werden auch berechtigte Transponder abgewiesen.
16	4-Augen-Prinzip	Ist diese Funktion aktiv, müssen zur Freigabe des Zutrittspunkts zwei zugangsberechtigte Transponder innerhalb von 10 s vor den Zutrittspunkt gehalten werden.
17	Version	Anzeige von Hardware und Firmware-Version vom gewählten Zutrittspunkt
18	Automatische Transponder-erkennung	Diese Funktion ermöglicht den Zutritt an einem SE-Zutrittspunkt, ohne dass die Taste am Transponder gedrückt werden muss. Diese Funktion ist nicht bei aktivierter „Feuerwehr-Funktion“ des Transponders möglich.

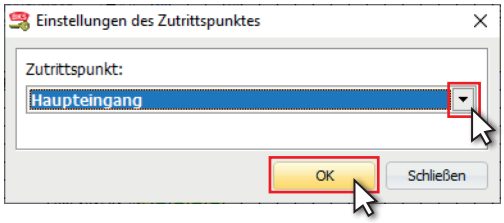
- Drücken Sie auf den Button „Speichern“ zum beenden des Dialogs.

4.3.2 Einstellungen Türen/Zutrittspunkte

- Für die Bearbeitung der Einstellungen eines vorhandenen Zutrittspunkts drücken Sie den Button „Einstellungen des Zutrittspunktes“.

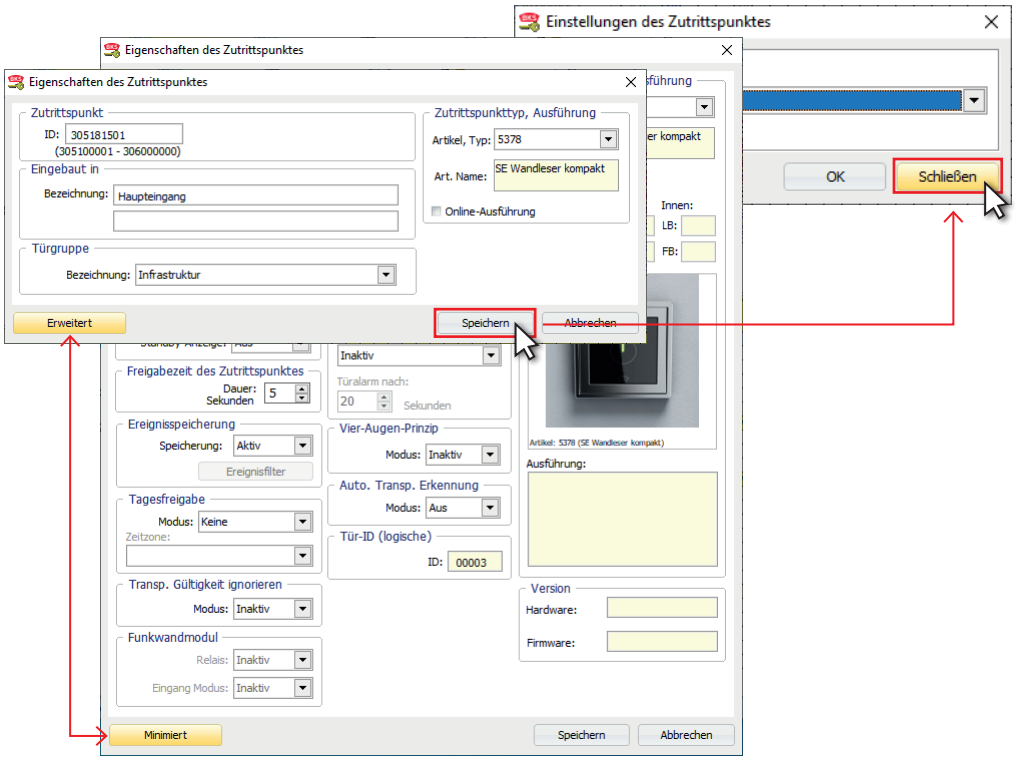


- Wählen Sie im Dropdown-Menü den gewünschten Zutrittspunkt aus. Drücken Sie zur Bestätigung auf „OK“.



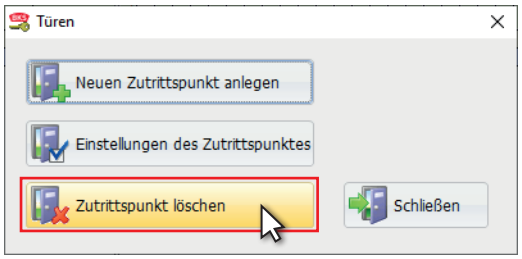
Bei der Überarbeitung der Einstellungen des Zutrittspunkts im Fenster Eigenschaften beachten Sie die Beschreibung des vorherigen Kapitels. Eine Änderung hat in den meisten Fällen zur Folge, dass der Zutrittspunkt neu programmiert werden muss.

- Drücken Sie nach Änderung der Eigenschaften auf den Button „Speichern“ und „Schließen“, um den Dialog zu beenden.



4.3.3 Türen/Zutrittspunkte löschen

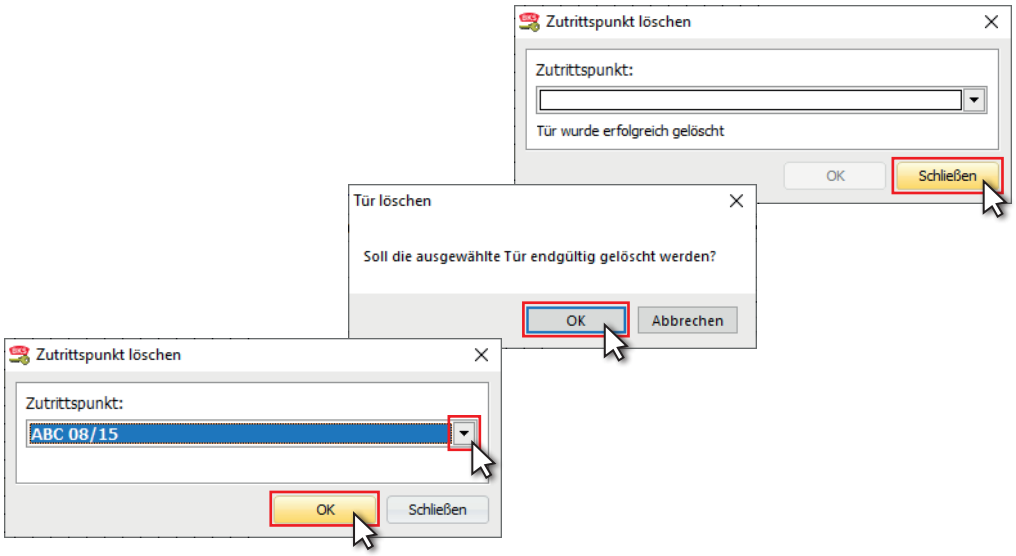
- Drücken Sie auf den Button „Zutrittspunkt löschen“ zum Starten des Dialogs zum Löschen eines vorhandenen Zutrittspunkts.



- Wählen Sie im Dropdown-Menü den zu löschenden Zutrittspunkt aus. Drücken Sie zur Bestätigung auf den Button „OK“.

Mit dem Löschen des Zutrittspunkts (Tür) wird das zugewiesene Produkt z. B. der eingebaute Zylinder in das Elektronik-Depot gebucht. Dadurch ist Seriennummer frei und das Produkt kann in einer anderen Tür weiterverwendet werden.

- Drücken Sie auf den Button „Schließen“ zum Beenden des Dialogs.



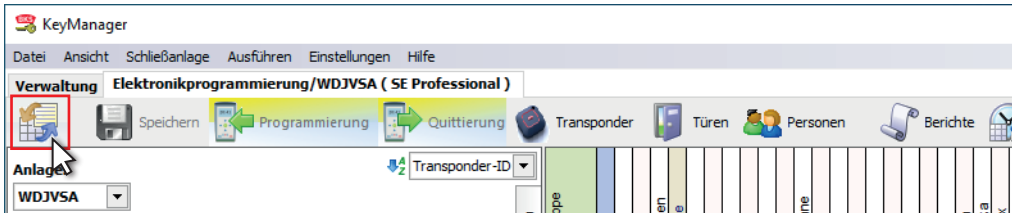
4.3.4 Berechtigungen zu Türen/Zutrittspunkte

Mit dieser Funktion können die zuvor erstellten Transpondergruppen für den Zugang zur ausgewählten Tür die Berechtigung erhalten oder die vorhandene Rechte entzogen werden.

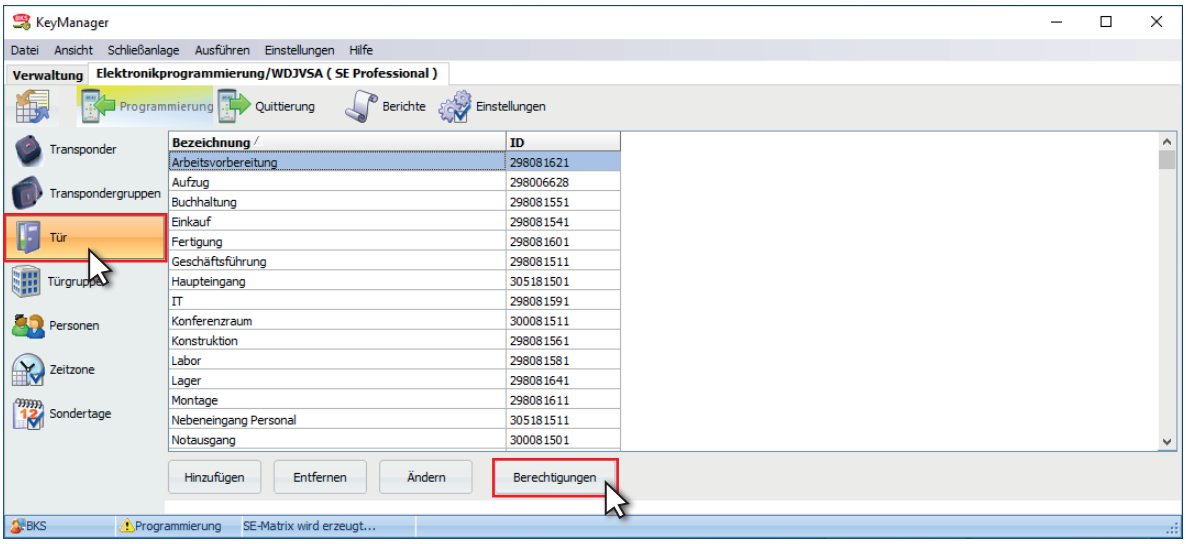
Für das Aufrufen der weiteren Menüs ist es erforderlich, die Ansicht des BKS KeyManager umzustellen. Wechseln Sie von der beim Programmstart gezeigten Berechtigungsmatrix in das Listenmenü.

- Drücken Sie auf den Button mit dem Symbol „Listenmenü anzeigen“.

Die Darstellung Listenansicht kann durch Drücken dieses Buttons jetzt mit der Funktion „SE-Matrix anzeigen“, auf die Berechtigungsmatrix zurückgewechselt werden.



- Drücken Sie auf die Schaltfläche „Tür“ und unter der zugehörigen der Listenansicht auf den Button „Berechtigungen“.



- (1) Öffnen Sie das Dropdown-Menü „Tür“ und wählen eine Tür für die Rechtevergabe aus.

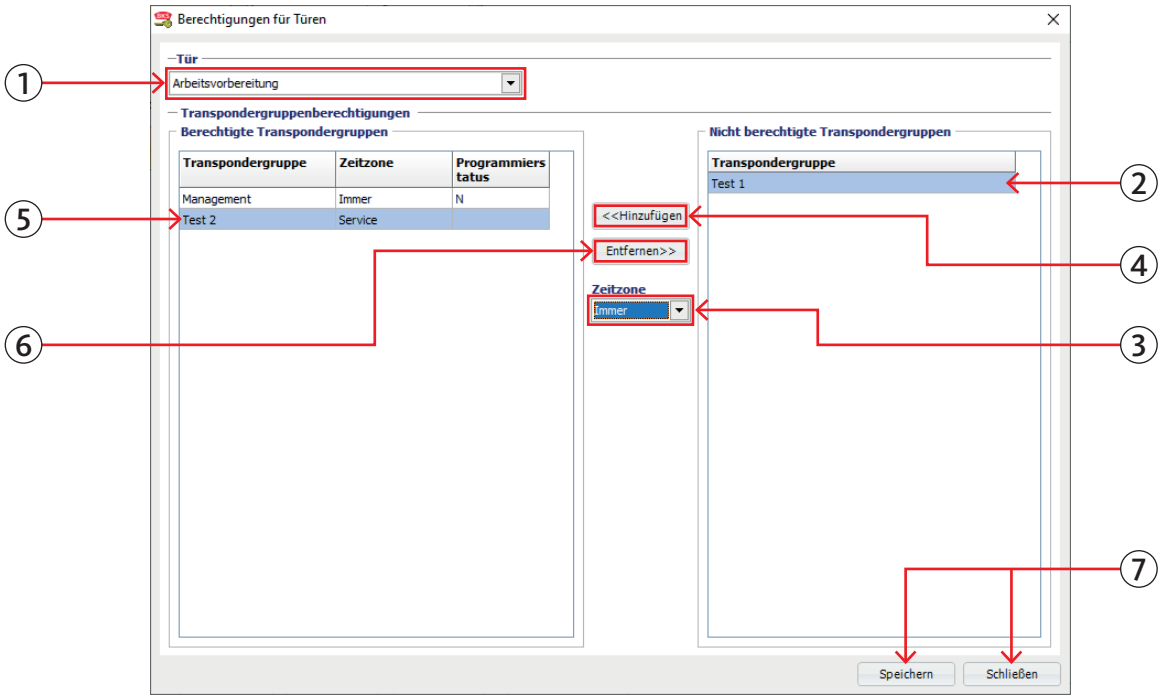
Transpondergruppen gewähren Sie die Berechtigung zu dieser Tür durch die folgenden Schritte.

- (2) Auswahl der Transpondergruppe in der Spalte der nicht berechtigten Transpondergruppen.
- (3) Einstellung der Zeitzone, die für die Berechtigung gelten soll.
- (4) Drücken Sie den Button „Hinzufügen“ und die Transpondergruppe wird zur linken Spalte zu den berechtigten Gruppen verschoben.
- (5) Auswahl einer Transpondergruppe in der linken Spalte der berechtigten Transponder.
- (6) Drücken Sie den Button „Entfernen“ und die Transpondergruppe wird zur rechten Spalte zu den nicht Berechtigten verschoben.

Die Berechtigung wird durch das Verschieben der Transpondergruppe von der linken Spalte der berechtigten Transpondergruppen in die rechte Spalte der nicht Berechtigten entfernt.

Transpondergruppen mit der Berechtigung „GHS“ (Generalhauptschlüssel) können nicht in die rechte Spalte der nicht berechtigten Gruppen verschoben werden.

- (7) Zum Beenden des Dialogs „Berechtigungen für Türen“ drücken Sie auf den Button „Speichern“ und „Schließen“.



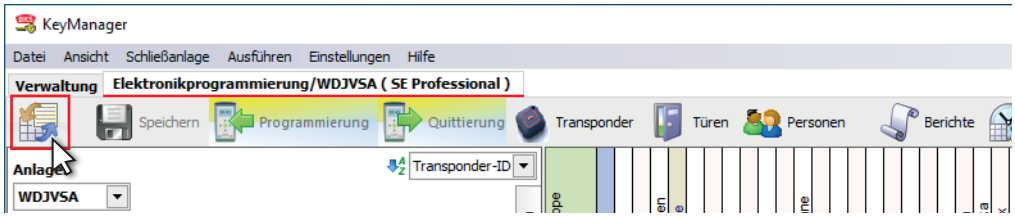
4.4 Türgruppen (Gruppen von Zutrittspunkten)

Im BKS KeyManager können Sie die Türen zur besseren Übersichtlichkeit und für eine komfortablere Bearbeitbarkeit zu Türgruppen zusammenfassen. Diese Funktion ermöglicht die Strukturierung in einen Verzeichnisbaum mit ober- und untergeordneten Türgruppen. Je nach Ihren Anforderungen ist es möglich, eine individuelle Benennung der Gruppierung z. B. nach der Infrastruktur wie Standort, Gebäude, Etage etc. und/oder nach der Organisation wie Geschäftsbereich, Abteilungen etc. zu erstellen. Das Menü „Türgruppe“ ist Teil des Listenmenüs.

Für das Aufrufen der weiteren Menüs ist es erforderlich, die Ansicht des BKS KeyManager umzustellen. Wechseln Sie von der beim Programmstart gezeigten Berechtigungsmatrix in das Listenmenü.

- Drücken Sie auf den Button mit dem Symbol „Listenmenü anzeigen“.

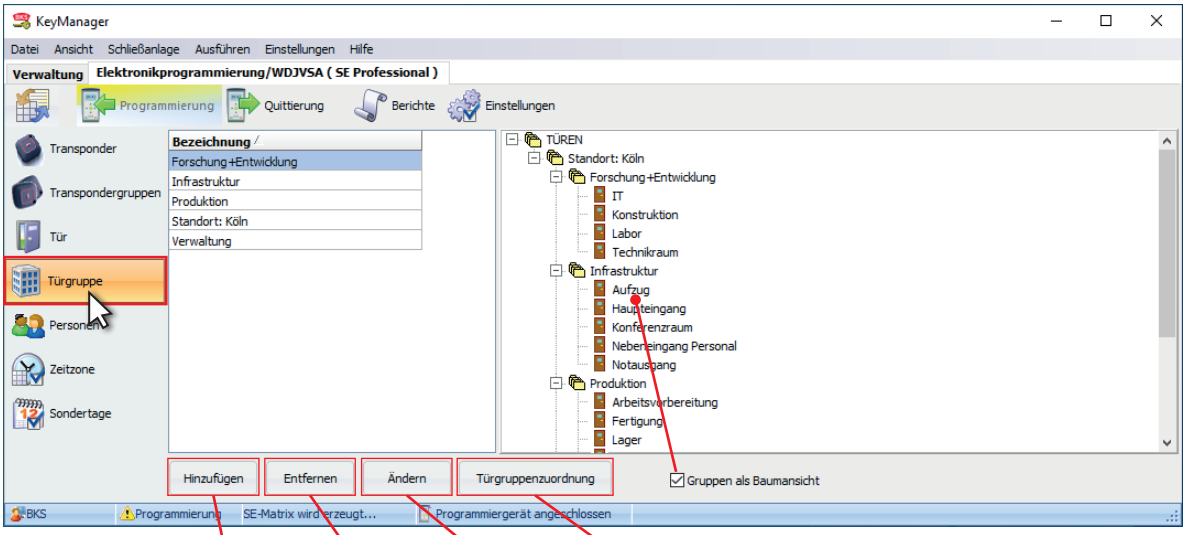
Die Darstellung Listenansicht kann durch Drücken dieses Buttons jetzt mit der Funktion „SE-Matrix anzeigen“, auf die Berechtigungsmatrix zurückgewechselt werden.



- Drücken Sie auf die Schaltfläche „Türgruppe“.

Das Anlegen neuer Türgruppen, die Bearbeitung oder das Löschen der vorhandenen Gruppen sowie die Zuordnung der Türen zu den Zutrittspunkten ist in dieser Listenansicht möglich. Verwenden Sie die entsprechenden Buttons in der Spalte unter der Liste.

- Aktivieren Sie die Checkbox „Gruppen als Baumansicht“ zur zusätzlichen Darstellung der Türen und Türgruppen in einem Verzeichnisbaum.



Die Beschreibung der Funktion und die weiteren Schritte finden Sie im zugehörigen Kapitel.

4.4.1 Seite 213

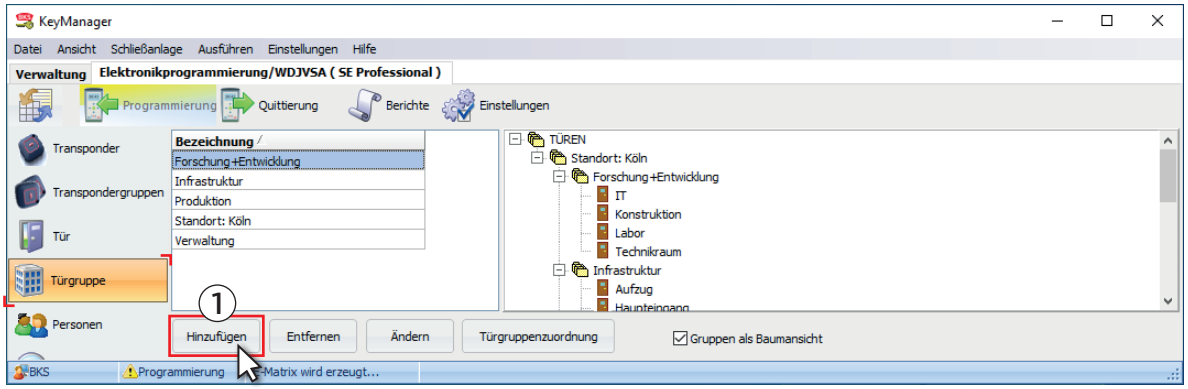
4.4.2 Seite 213

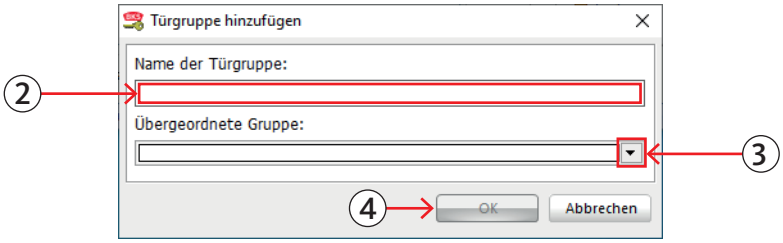
4.4.3 Seite 214

4.4.4 Seite 214

4.4.1 Türgruppen hinzufügen

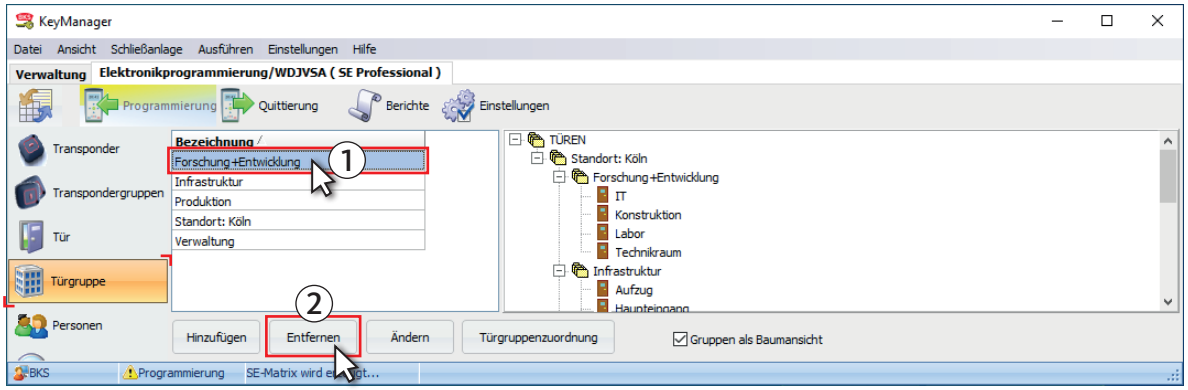
- Drücken Sie den Button „Hinzufügen“ (1) und geben im Feld (2) einen Namen für die neu zu erstellende Türgruppe ein.
- Über das Dropdown-Menü (3) ist eine übergeordnete Türgruppe auszuwählen, unter der die neue Gruppe geführt wird. Beenden Sie die Eingabe und drücken auf den Button „OK“ (4).

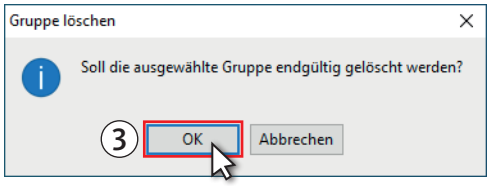


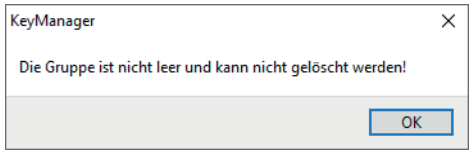


4.4.2 Türgruppen entfernen

- Wählen Sie in der Spalte „Bezeichnung“ die zu entfernende Türgruppe (1) aus. Es können nur leere Türgruppen ohne zugeordnete Türen gelöscht werden.
- Drücken Sie den Button „Entfernen“ (2) zum Löschen der ausgewählten Gruppe. Beenden Sie die Eingabe und drücken auf den Button „OK“ (3).

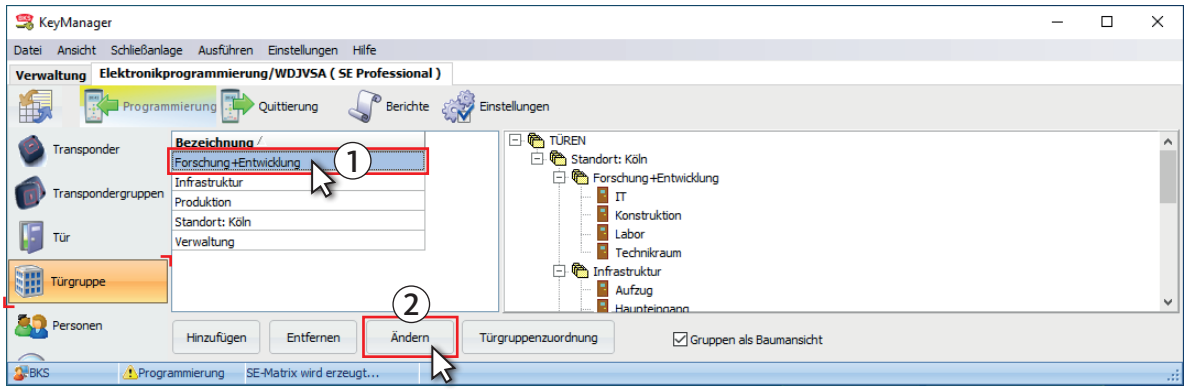


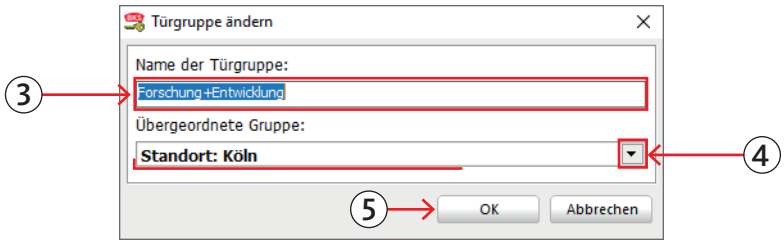




4.4.3 Türgruppen ändern

- Wählen Sie in der Spalte „Bezeichnung“ die Türgruppe (1), die geändert werden soll, aus.
- Drücken Sie den Button „Ändern“ (2) und editieren die Türgruppe in den folgenden Optionen.
  – Überarbeitung des Namens der Türgruppe über das Feld (3).
  – Auswahl einer anderen übergeordneten Türgruppe im Dropdown-Menü (4).
- Beenden Sie die Eingabe und drücken auf den Button „OK“ (5).

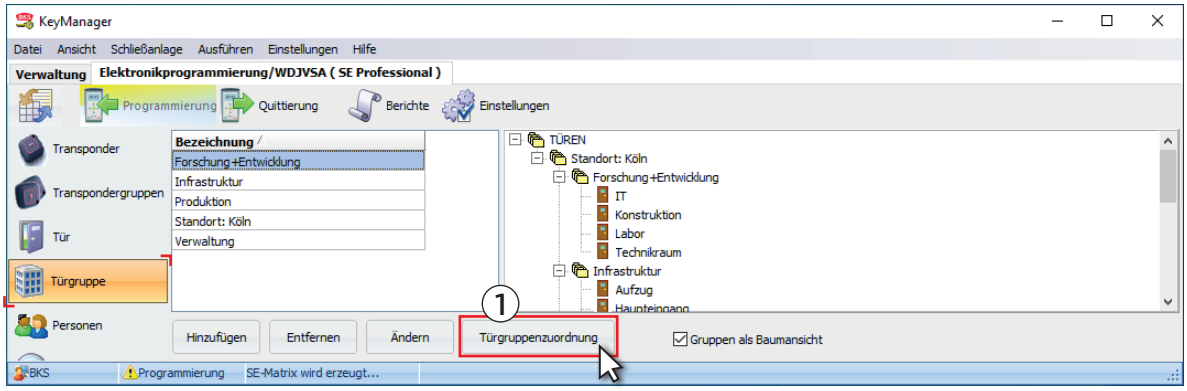




4.4.4 Zuordnung der Türgruppen

- Drücken Sie den Button „Türgruppenzuordnung“ (1).

Die existenten Türen im Schließsystem können im folgenden Dialog zu einer Türgruppe zugeordnet werden. Dabei wird ein Verzeichnisbaum erstellt bzw. gepflegt.



Im Feld (A) erhalten Sie eine Übersicht der vorhandenen Türgruppen.

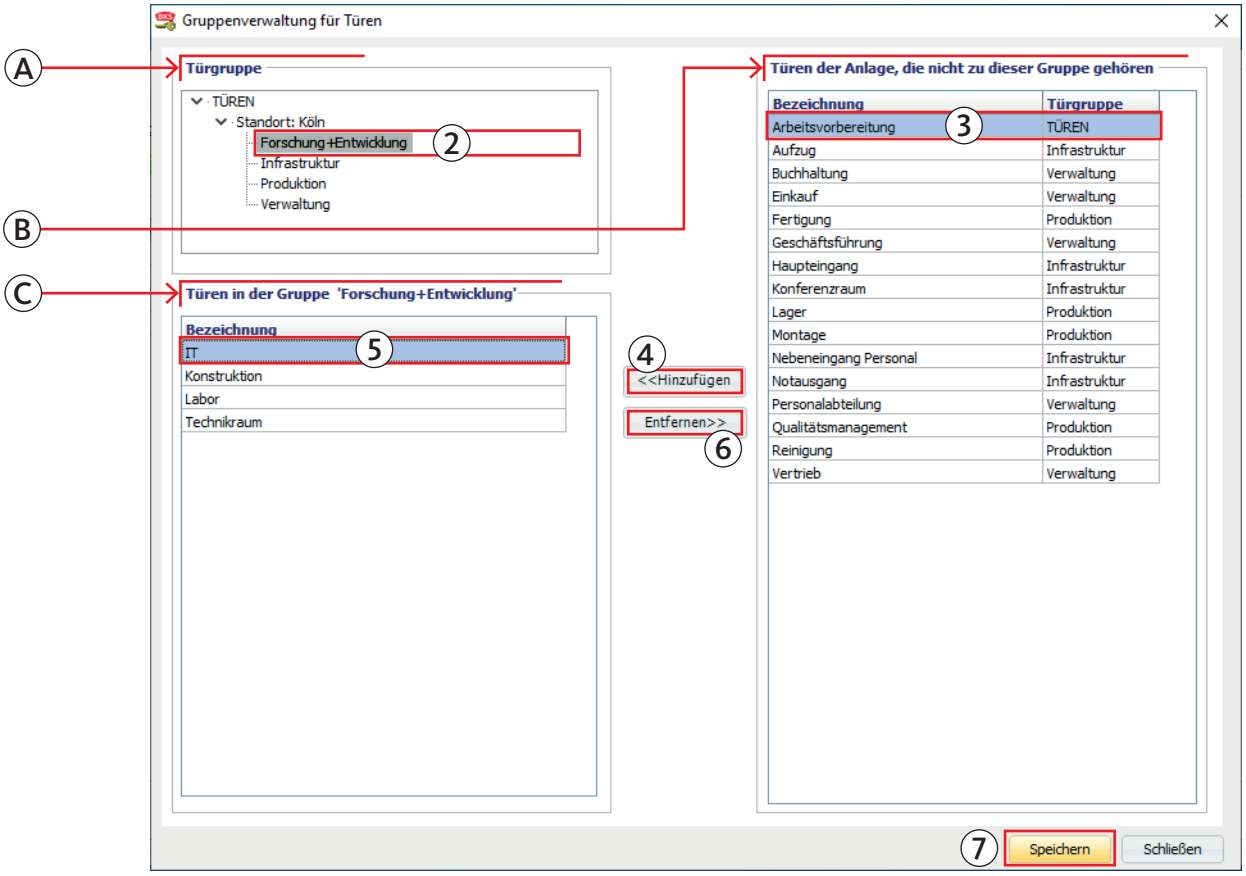
- Wählen Sie eine Türgruppe (2) aus, für die im Weiteren die Zuordnung ausgeführt werden soll.

Die Türen, welche zur gewählten Türgruppe zugeordnet werden können, stehen im Feld (B). Eine Tür kann aber immer nur einer Türgruppe angehören bzw. zugeordnet werden.

- Wählen Sie eine Tür (3) aus, die der markierten Türgruppe (2) hinzugefügt werden soll.
- Drücken Sie auf den Button „<< Hinzufügen“ (4) und die Tür wird in Feld (C) verschoben.

Im Feld (C) werden alle Türe die der in Feld (A) gewählten Türgruppe zugeordneten sind, angezeigt. An dieser Stelle können auch Türen aus der gewählten Gruppe entfernt werden.

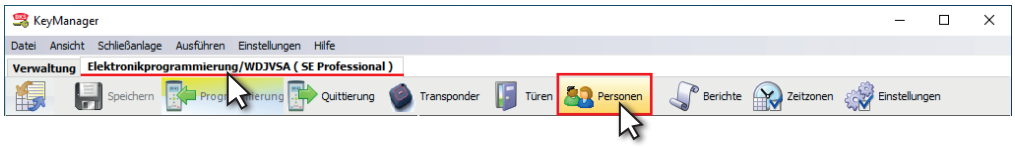
- Wählen Sie eine Tür (5) aus, die aus der markieren Türgruppe (2) entfernt werden soll.
- Drücken Sie auf den Button „Entfernen >>“ (6) und die Tür wird in Feld (B) verschoben.
- Beenden Sie den Dialog und drücken auf den Button „Speichern“ (7).



4.5 Personen

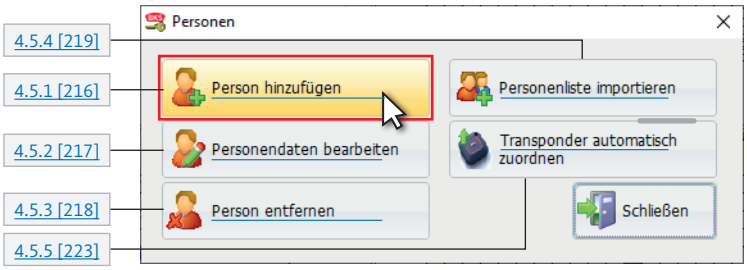
Mit dem Menü „Personen“ können Sie Personen hinzufügen, bearbeiten und löschen. Zusätzlich können Personenstammdaten über die Importfunktion eingelesen werden. Mit der Funktion „Transponder automatisch zuordnen“, können freie Transponder und Personen ohne Transponder automatisch zugeordnet werden.

- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Personen“.



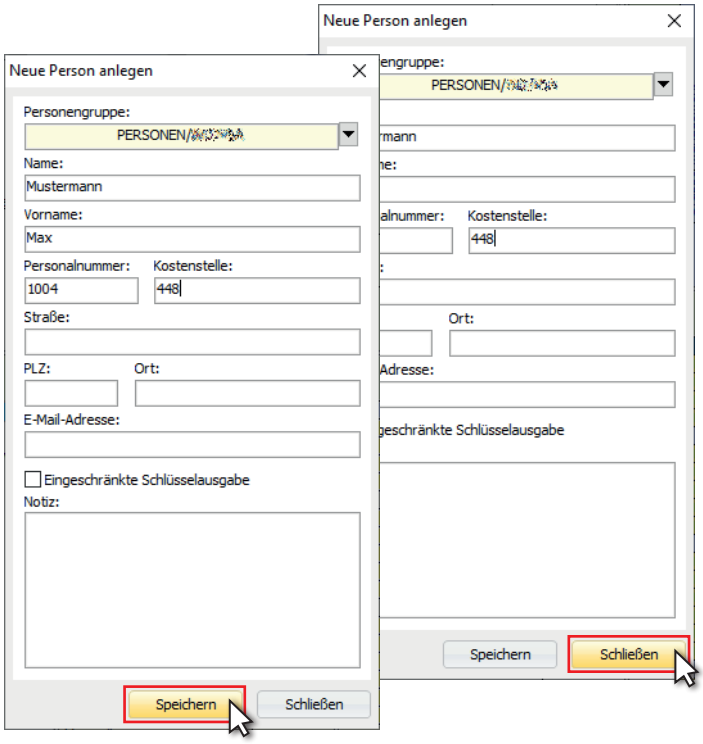
4.5.1 Personen hinzufügen

- Drücken Sie auf den Button „Person hinzufügen“.



Füllen Sie die Felder mit den entsprechenden Daten zur Person aus.

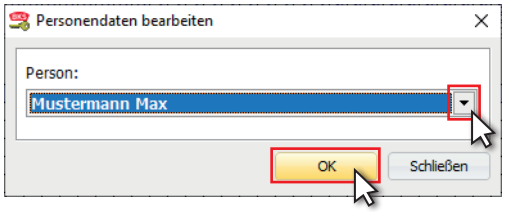
- Drücken Sie auf „Speichern“ zum Sichern der Eingabe und auf „Schließen“, um den Dialog zu beenden.



4.5.2 Personen bearbeiten

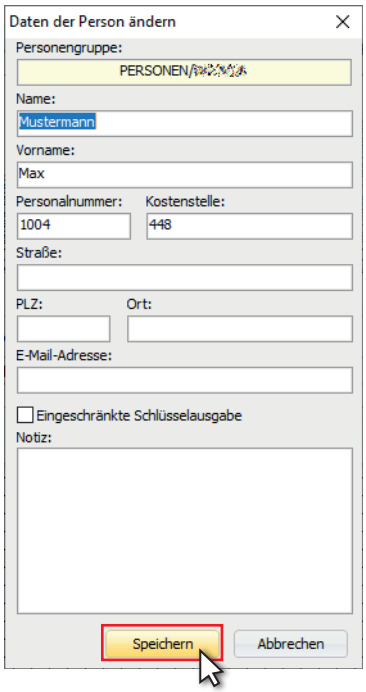
- Drücken Sie auf den Button „Personendaten bearbeiten“.

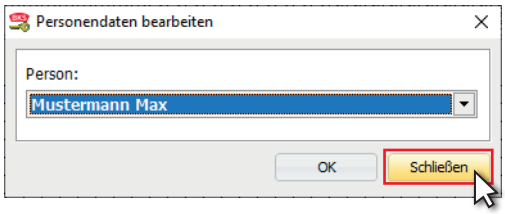
- Wählen Sie im Dropdown-Menü die zu editierende Person aus. Drücken Sie zur Bestätigung auf den Button „OK“.



Im Fenster „Daten der Person ändern“, sind die gewünschten Änderungen und Korrekturen in die betreffenden Felder einzutragen.

- Drücken Sie auf „Speichern“ zum Sichern der Eingabe und auf „Schließen“, um den Dialog zu beenden.

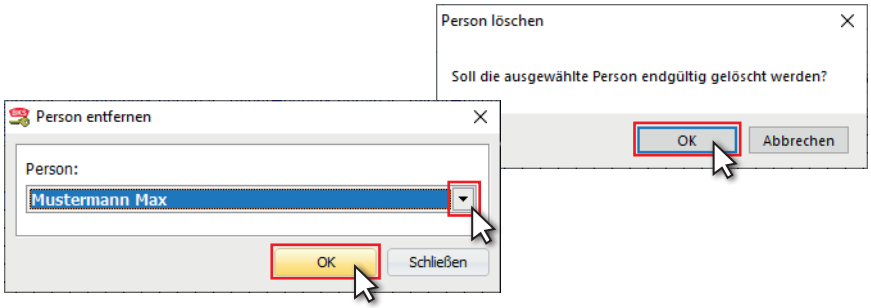




4.5.3 Personen entfernen

- Drücken Sie auf den Button „Personendaten entfernen“.

- Wählen Sie im Dropdown-Menü die Person, die gelöscht werden soll, aus.
- Drücken Sie zum Löschen dieser Person in den beiden Fenstern jeweils auf den Button „OK“.



4.5.4 Personenlisten importieren

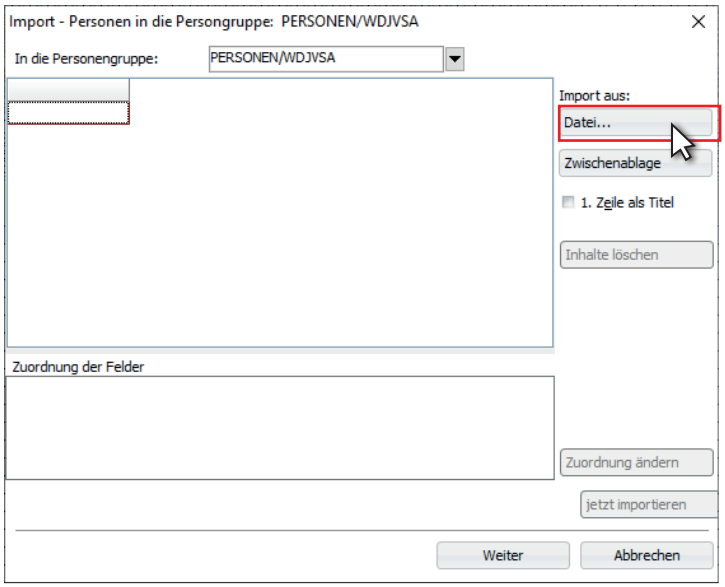
Es kann eine Personenliste für die Schließanlage geladen werden. Die Personenliste können Sie über eine CSV-Datei (*.CSV) importieren.

HINWEIS **Achten Sie darauf, dass die CSV-Datei auf eine „UTF-8“-Codierung eingestellt ist, weil es keinen allgemeinen Standard für das Dateiformat CSV gibt!**

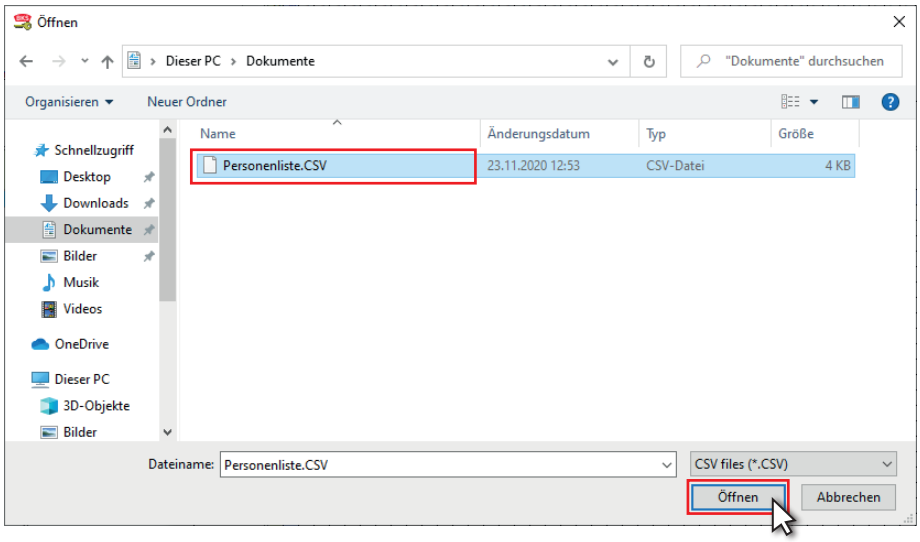
- Drücken Sie auf den Button „Personenliste importieren“.

Nach der Auswahl „Personenliste importieren“ öffnet sich folgender Dialog.

- Drücken Sie auf den Button „Datei ...“ in der Spalte „Import aus:“ des Fensters.

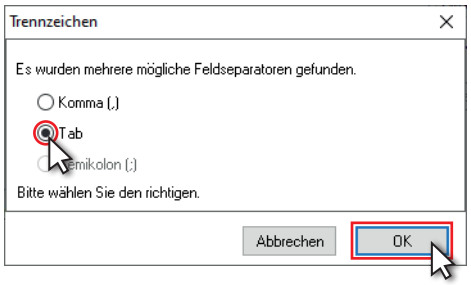


- Navigieren Sie mit dem Dateibrowser zur Personenliste. Die Datei muss im CSV-Format (*.CSV) vorliegen.
- Drücken Sie auf den Button „Öffnen“, um den Import zu starten.



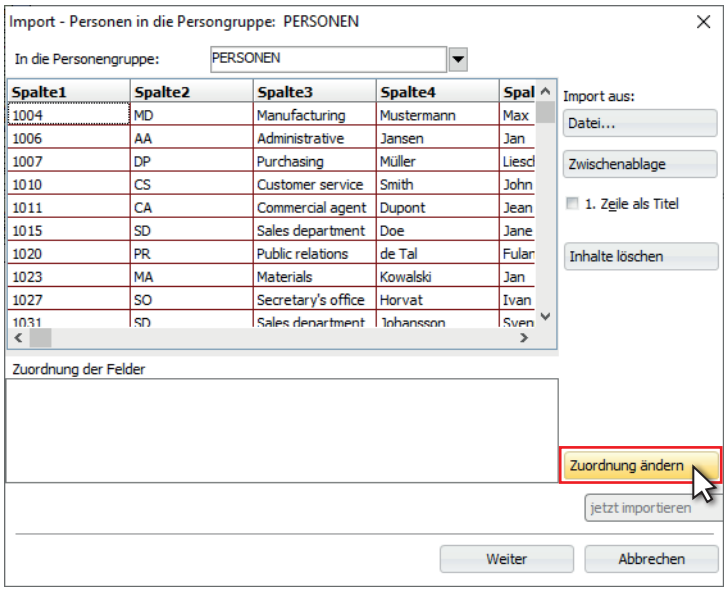
Optional wird, wenn mehrere Trennzeichen in der CSV-Datei gefunden wurden, folgendes Fenster zur Auswahl der zu verwendenden Trennzeichen geöffnet.

- Aktivieren Sie die Checkbox mit den zur CSV-Datei passenden Trennzeichen.



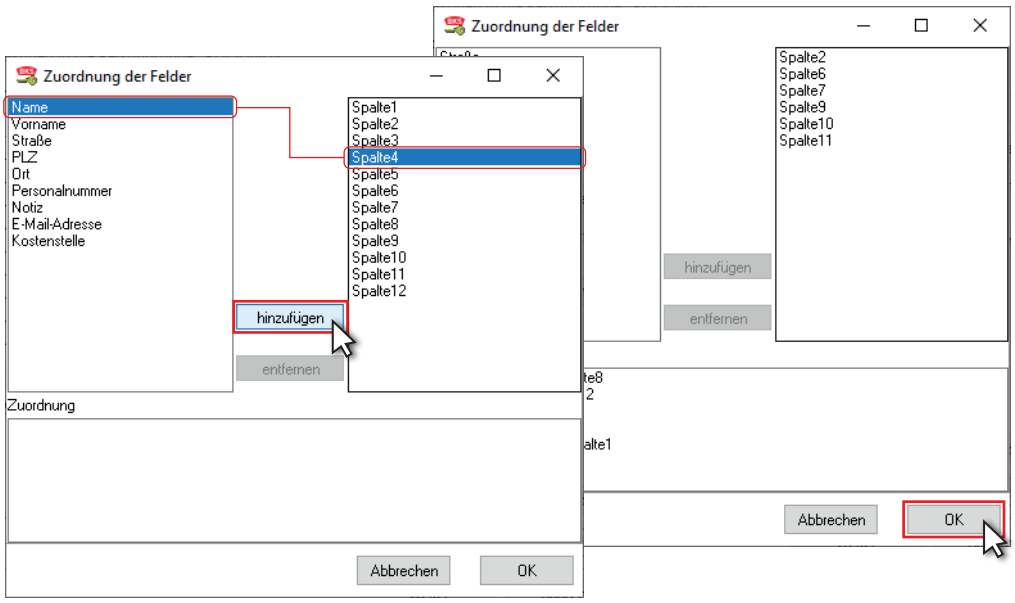
Zur Übersicht wird Ihnen die importierte Personenliste angezeigt. Die Spalten der Personenliste sind den Feldern des BKS KeyManagers zuzuweisen.

- Drücken Sie auf den Button „Zuordnung ändern“.

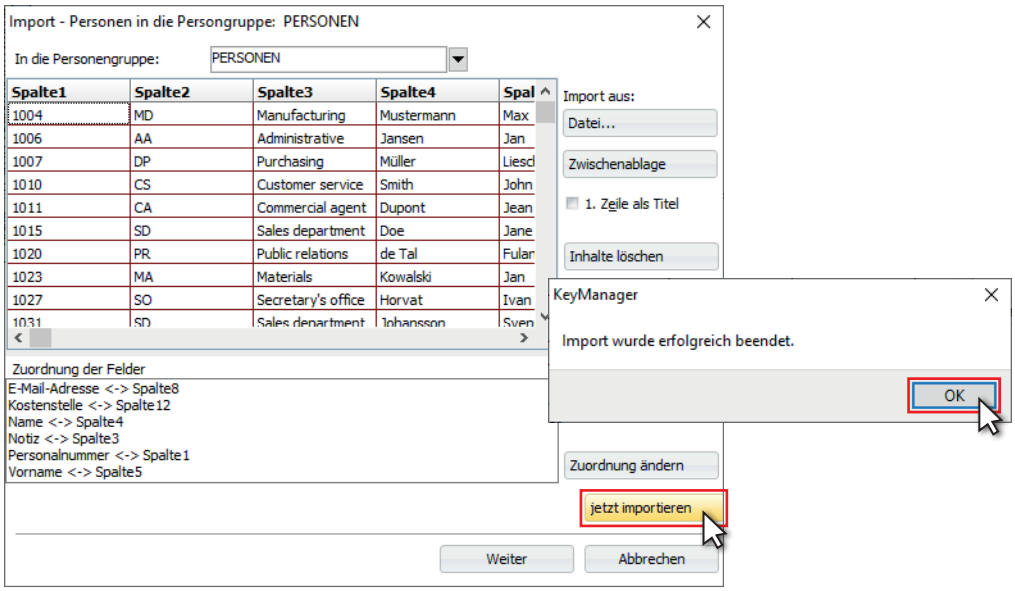


Ordnen Sie im Fenster „Zuordnung der Felder“ die personenbezogenen Daten der dazugehörigen Spalte zu. Zum Beispiel „Name“ und „Spalte 4“.

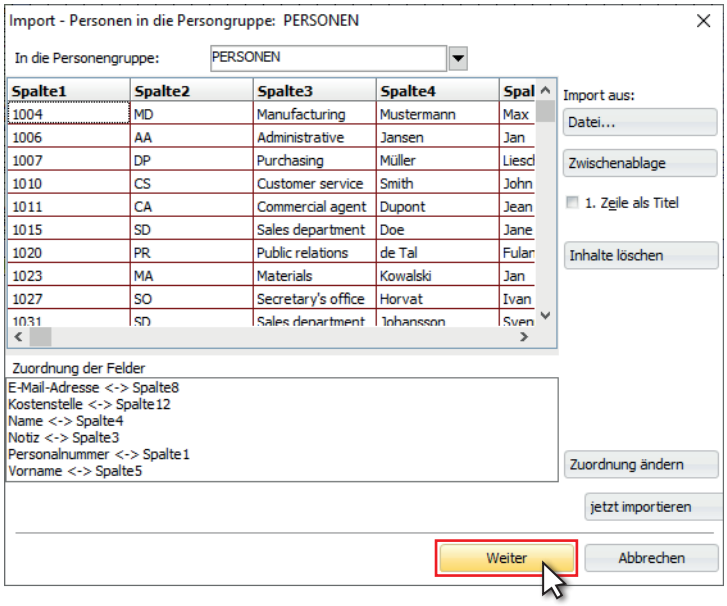
- Wählen Sie „hinzufügen“ aus und stellen Sie die Zuordnung her.
- Nach der Zuordnung der Spalten der Personenliste mit den Feldern des BKS KeyManagers fahren Sie mit „jetzt importieren“ fort.
- Beenden Sie die Zuordnung und drücken auf den Button „OK“.



- Lesen Sie die Personenliste mit „jetzt importieren“ ein und drücken zur Bestätigung auf den Button „OK“.



- Drücken Sie auf den Button „Weiter“, um die Zuordnung abzuschließen.



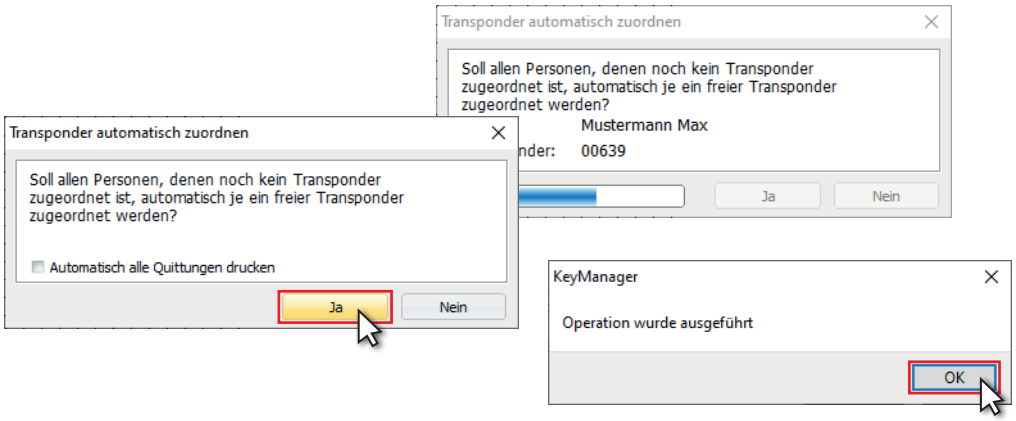
4.5.5 Transponder automatisch zuordnen

Mit der automatischen Zuordnung der Transponder wird allen Personen, die noch keinen Transponder zugewiesen bekommen haben, ein Transponder zugeordnet. Hierdurch werden Personen, die mittels CSV-Datei importiert wurden, automatisch einem Transponder zugeordnet.

- Drücken Sie auf den Button „Transponder automatisch zuordnen“.

Allen Personen, die noch keinen Transponder haben, kann automatisch ein Transponder zugeordnet werden. Bei Ausgabe von mehreren Transpondern kann dies eine große Zeitersparnis sein.

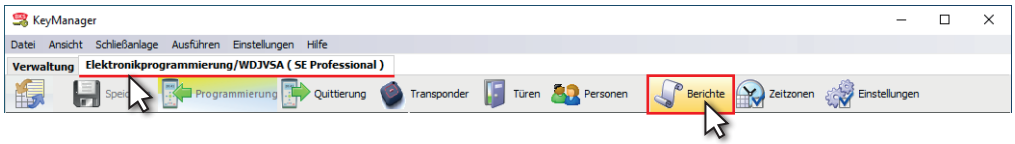
- Drücken Sie auf den Button „Ja“, um die Zuordnung zu starten.



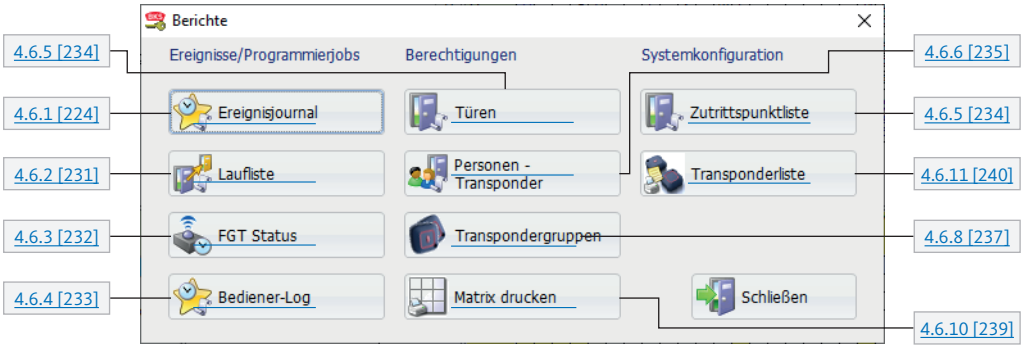
4.6 Berichte

Im Menü „Berichte“ können zu verschiedenen Funktionen des BKS KeyMangers Berichte erzeugt und gedruckt werden. Der Menüpunkt „Bediener-Log“ ist erst ab einer Professional-Lizenz und die „Transponderliste“ mit einer „DoT“-Lizenz (Data on Transponder) verfügbar. Die Datenbasis der Berichte wird beim Auslesen des Programmiergeräts automatisch an den BKS KeyManager übertragen.

- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Berichte“.



Im Berichte-Menü lassen sich die folgende Funktionen aufrufen.

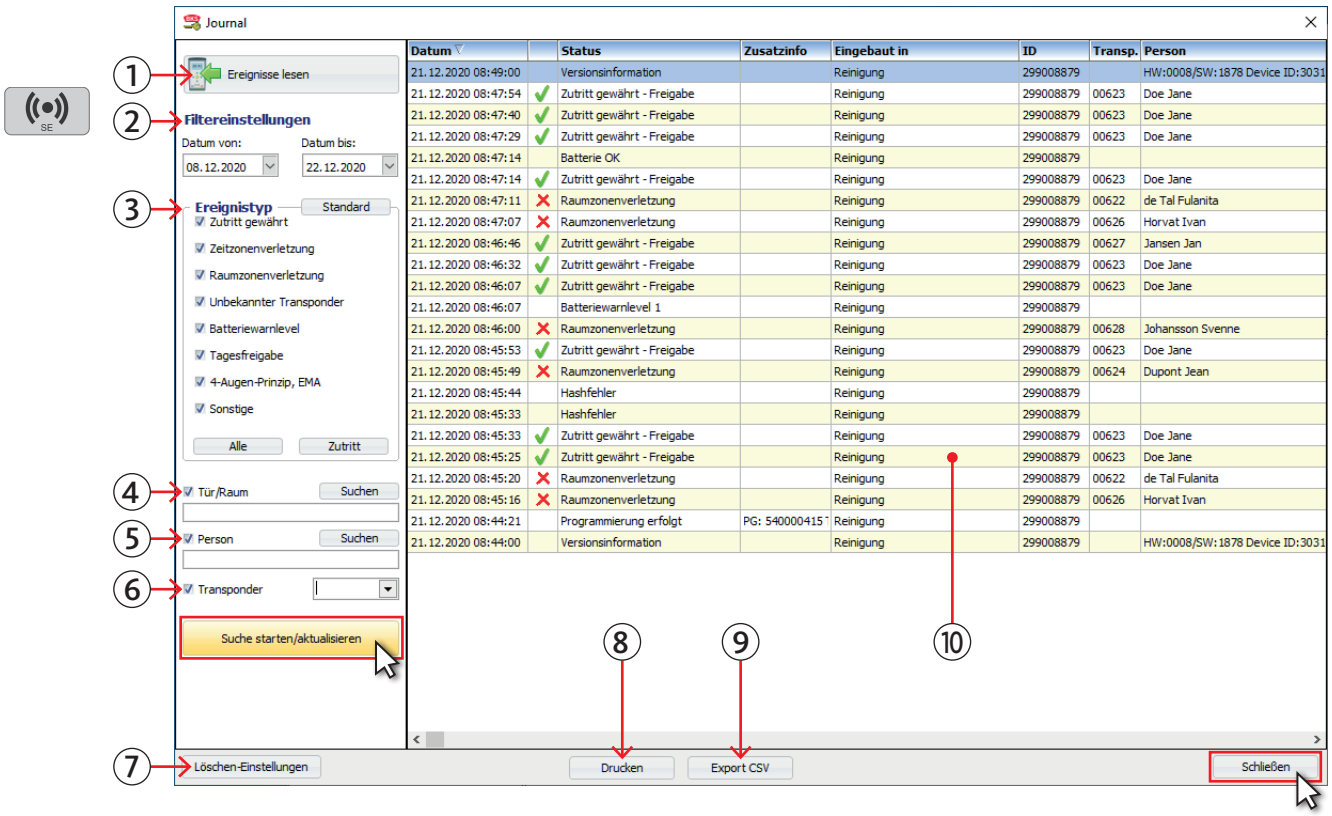


4.6.1 Ereignisjournal

Im Bericht „Ereignisjournal“ werden alle aus den Komponenten ausgelesenen Ereignisse angezeigt. Das Journal bietet nähere Informationen zu den Personen, Transpondern und den Zutrittspunkten an.

Das Journal besteht aus verschiedenen Informationen und kann komplett oder gefiltert dargestellt werden. Zur besseren Übersichtlichkeit kann die Anzeige über die verschiedenen Filtereinstellungen in der linken Leiste der Journalanzeige nach Ihren Wünschen angepasst werden. Das Ereignisjournal gibt Ihnen eine Übersicht der berechtigten Zutritte und der Zutrittsversuche mit nicht berechtigten Transpondern in einer übersichtlich aufgelisteten Ansicht.

- Drücken Sie auf den Button „Ereignisjournal“, um zum Bericht zu gelangen.

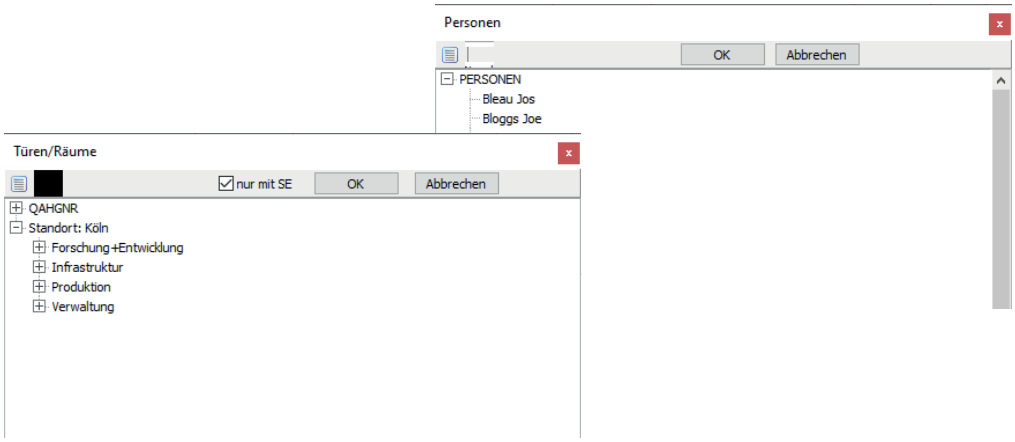


Nr.	Beschreibung
1.	Der Button öffnet ein Fenster zur Auswahl der Ereignisse und Zutrittspunkte, die bei der Programmierung berücksichtigt werden sollen und der Option zum Ein- und Auslesen der Ereignisse für die gewählten Zutrittspunkte.
2.	Filtereinstellung für einen gewünschten Zeitraum, innerhalb dessen die Ereignisse gesucht und in der Ereignisliste (10) angezeigt werden sollen.
3.	Selektion der Ereignisse nach Ereignistyp über die Auswahl „Standard|Erweitert“, „Alle“, „Zutritt“ oder eine manuelle Auswahl.
4.	Filter zur Suche nach Ereignissen von einer bestimmten Tür.
5.	Filter zur Suche nach Ereignissen von einer bestimmten Person.
6.	Filter zur Suche nach Ereignissen von einem bestimmten Transponder.
7.	Einstellung, nach welchem Zeitraum die Ereignisse gelöscht werden sollen.
8.	Ausgabe der Ereignisse als druckbare Liste z. B. zur Erstellung einer PDF oder Ausdruck.
9.	Export der Ereignisse in eine CSV-Datei.
10.	Ereignisliste mit den Ereignissen nach den links gesetzten Filtereinstellungen.

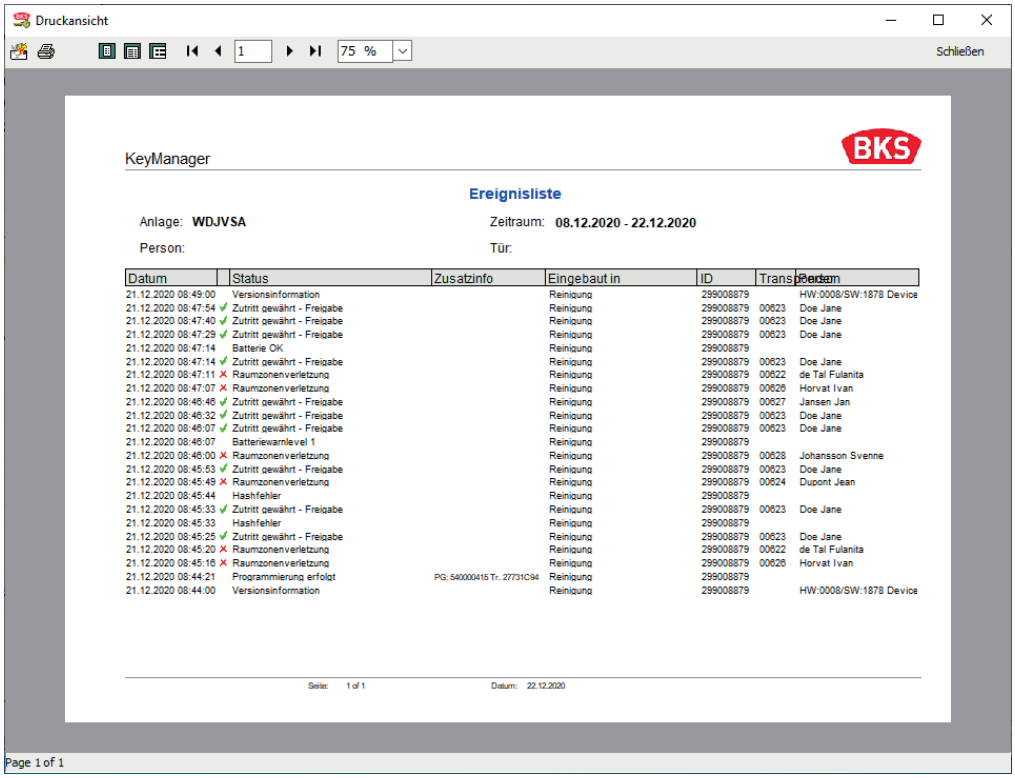
Die Ergebnisliste (10) kann durch Auswahl der Suchparameter in den Filtereinstellungen (2) bis (6) eingeschränkt werden. Die Anzahl der Einträge in der Liste kann individuell für eine bessere Übersichtlichkeit auf Ihre Bedürfnisse reduziert werden.

■ Drücken Sie auf den Button „Suche starten/aktualisieren“, um eine Ergebnisliste zu erzeugen.

Mit den Filterfunktionen (4) bis (6) ist es möglich, die Auswahl der gezeigten Ereignisse auf bestimmte Zutrittspunkte und Personen zu begrenzen.



Mit dem Button „Drucken“ (8) kann die Ereignisliste über einen Drucker ausgegeben oder als PDF gespeichert werden.



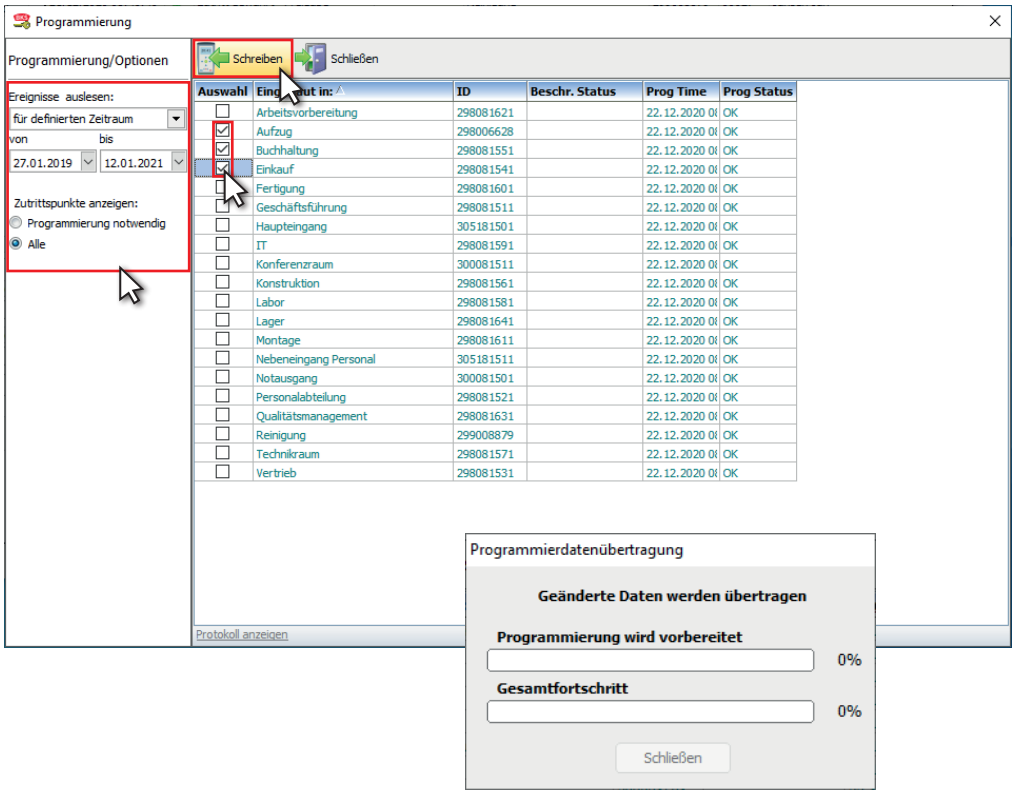
- Drücken Sie den Button „Ereignisse lesen“ (1), um die Ereignisse für die gewählten Zutrittspunkte ein- und auszulesen. Es öffnet sich das Fenster „Programmierung“.

Wählen Sie unter „Programmierung/Optionen“ aus, welche Ereignisse und Zutrittspunkte bei der Programmierung berücksichtigt werden sollen. Mit dem Dropdown-Menü „Ereignisse auslesen“, bestimmen Sie, welche Daten ausgelesen werden sollen. Dadurch werden „keine“, „neue“ oder „alle“ Ereignisse sowie auch die „über einen definierten Zeitraum“ stattgefundenen Ereignisse ausgelesen. Über „Zutrittspunkte anzeigen“ kann die Anzahl der Zutrittspunkte auf „Alle“ gesetzt oder durch die Auswahl „Programmierung notwendig“ auf diese beschränkt werden. Es werden nur Ereignisse nach diesen Parametern abgefragt.

Durch Aktivierung der Checkboxen in der Spalte Auswahl legen Sie fest, aus welchen Zutrittspunkten die Ereignisse ausgelesen werden sollen. Über Kontextmenü über der Spalte „Auswahl“ können Sie auch „Alle“ markieren.

- Drücken Sie auf den Button „Schreiben“ und der Programmierjob zum Auslesen der Ereignisse wird auf das Programmiergerät übertragen. Alternativ kann in Online-Schließanlagen über den Button „Online senden“ das Auslesen gestartet werden, siehe Kapitel 3.8.5 [153].

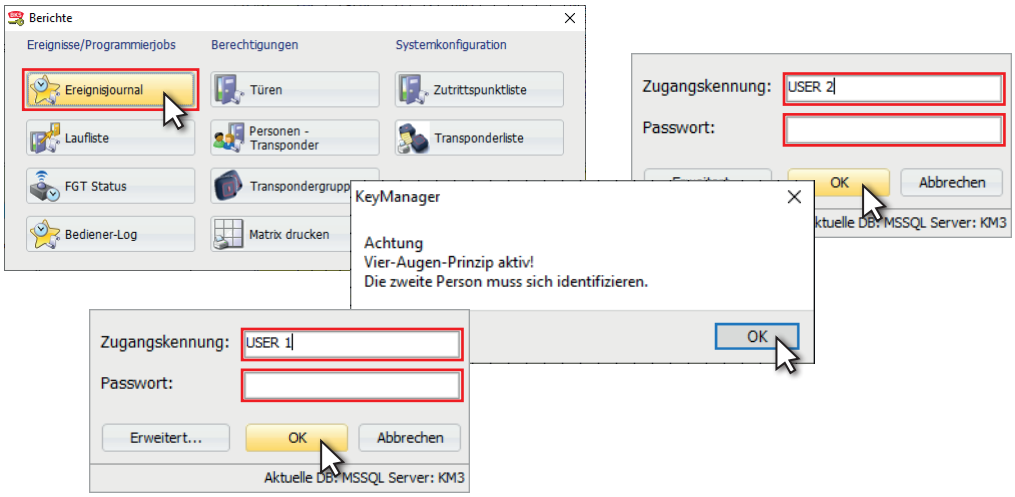
Diesen Programmierjob führen Sie durch das Auslesen der Zutrittspunkte mit dem Programmiergerät im nächsten Schritt aus. Anschließend schließen Sie das Programmiergerät erneut an Ihrem Computer an, um die neuen übermittelten Ereignisse auszulesen und im Journal anzuzeigen.



4.6.1.1 Sicherheitsstufen beim Zugriff auf die Ereignisjournale

Der Zugriff auf den Bericht „Ereignisjournal“ ist nur Benutzern mit dem entsprechenden Recht zum Lesen möglich. Über zwei Sicherheitsstufen können weitere Einschränkungen zum Zugang erfolgen.

Die erste Sicherheitsstufe ermöglicht nur einen Zugriff auf das Ereignisjournal, nachdem sich ein berechtigter Benutzer erneut mit Benutzernamen und Passwort einloggt hat. In der zweiten Sicherheitsstufe muss sich noch zusätzlich ein weiterer Benutzer mit Berechtigung anmelden, um den Zugriff freizuschalten.

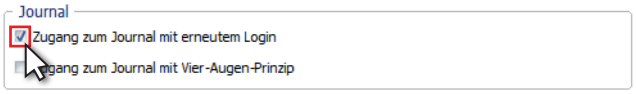


Die Sicherheitsstufen sind über das Menü „Einstellungen“ auszuwählen, siehe Kapitel 5.1.1.2 [260].

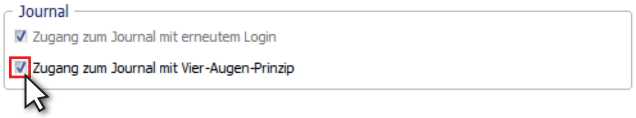
- Aktivieren Sie die jeweiligen Checkboxen.

➔ **Uneingeschränkter Zugriff auf das Ereignisjournal.**
Wird keine Checkbox aktiviert, können berechtigte Benutzer ohne eine weitere Authentifizierung die Berichte einsehen.

➔ **Zugriff auf das Ereignisjournal mit aktiviertem erneutem Login.**
Wird diese Option gewählt, ist für den Zugriff auf das Ereignisjournal die erneute Eingabe der Zugangskennung und Passwort von einem berechtigten Benutzer erforderlich.
Zur Berechtigung benötigt der Benutzer das Recht „Ereignisjournal“.



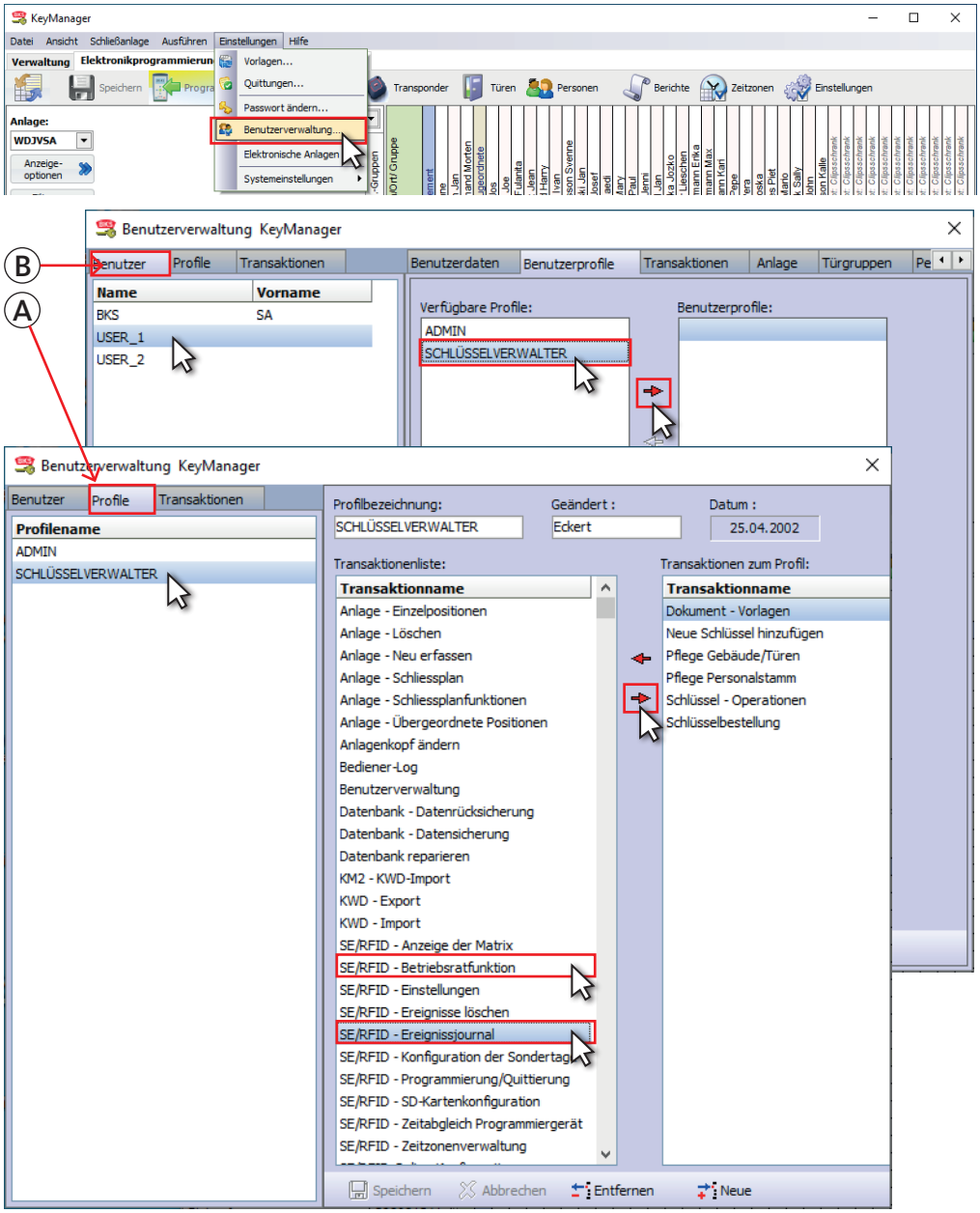
➔ **Zugriff auf das Ereignisjournal mit aktiviertem 4 Augen Prinzip .**
Bei Aktivierung dieser Option ist der Zugriff auf das Ereignisjournal nur noch möglich, wenn zwei berechtigte Benutzer sich authentifizieren.
Beide Benutzer müssen im BKS KeyManager für die Transaktion „Ereignisjournal“ berechtigt worden sein. Diese Berechtigung ist über die Benutzerverwaltung des BKS KeyManagers zu gewähren.



- Legen Sie die Berechtigungen der Benutzer über die Benutzerverwaltung fest, siehe Kapitel 6 [339].

In der Benutzerverwaltung können die Rechte der Transaktionen nur von Administratoren vergeben werden. Zum Einstellen der Benutzerrechte befolgen Sie folgende Schritte.

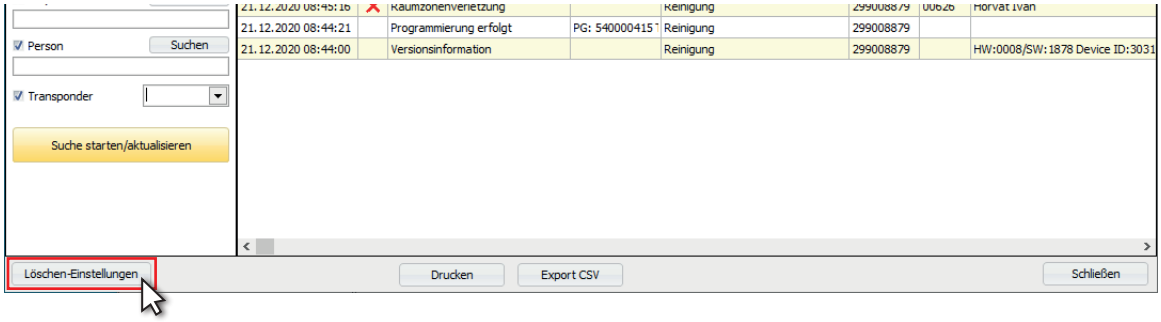
- (A) Beginnen Sie mit der Auswahl eines bestehenden Profils oder erstellen ein neues Profil. Markieren Sie eine aus den verfügbaren Transaktionen eine Transaktion aus und weisen diese mit dem „Pfeil“ dem markierten Profil zu.
- (B) Wählen Sie einen Benutzer aus oder erstellen einen neuen Benutzer. Weisen Sie diesem mit dem „Pfeil“ aus den verfügbaren Profilen ein Profil zu.



4.6.1.2 Löschung von personenbezogenen Daten

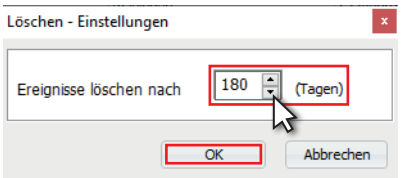
Die personenbezogenen Daten lassen sich unter anderem auch um dem Datenschutz einzuhalten, löschen. Neben dem direkten Löschen von Personen im Menü „Personen“ ist es auch möglich, die im Ereignisjournal gespeicherten personenbezogenen Daten zu löschen. Hierdurch werden die Einträge des Ereignisjournals nach einem Zeitraum automatisch gelöscht.

- Zur Bearbeitung dieses Zeitraums, nachdem die Daten gelöscht werden, drücken Sie in der Fußzeile des Journals auf den Button „Löschen-Einstellungen“.



Als Grundeinstellung ist der Zeitraum auf 180 Tage voreingestellt. Dieser kann noch Ihren Vorgaben im Eingabefeld geändert werden. Ältere Ereignisse werden automatisch inklusive der personenbezogenen Daten gelöscht und sind nicht mehr im Ereignisjournal sichtbar.

- Geben Sie einen Wert in Tagen ein.



4.6.2 Laufliste

Der Bericht „Laufliste“ ermöglicht eine Druckansicht aller Türen, für die ein Programmierauftrag im Programmiergerät vorliegt.

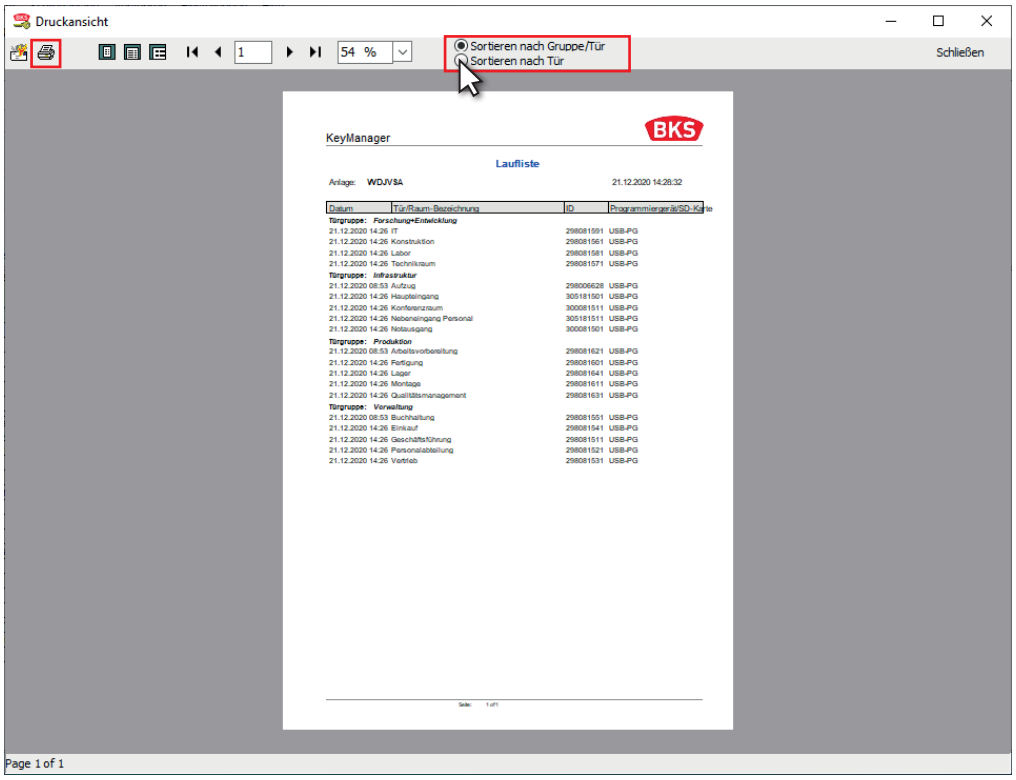
- Drücken Sie auf den Button „Laufliste“, um zum Bericht zu gelangen.

Alternativ ist es möglich, die Laufliste im Display des Programmiergeräts anzusehen.

Die Sortierung der Laufliste kann zwischen der Sortierung nach Türgruppen und nach Türen gewählt werden.

- Aktivieren Sie zur Auswahl der gewünschten Sortierung eine Checkbox.

Die Druckvorschau der Laufliste kann über den Button mit dem Druckersymbol ausgedruckt werden.



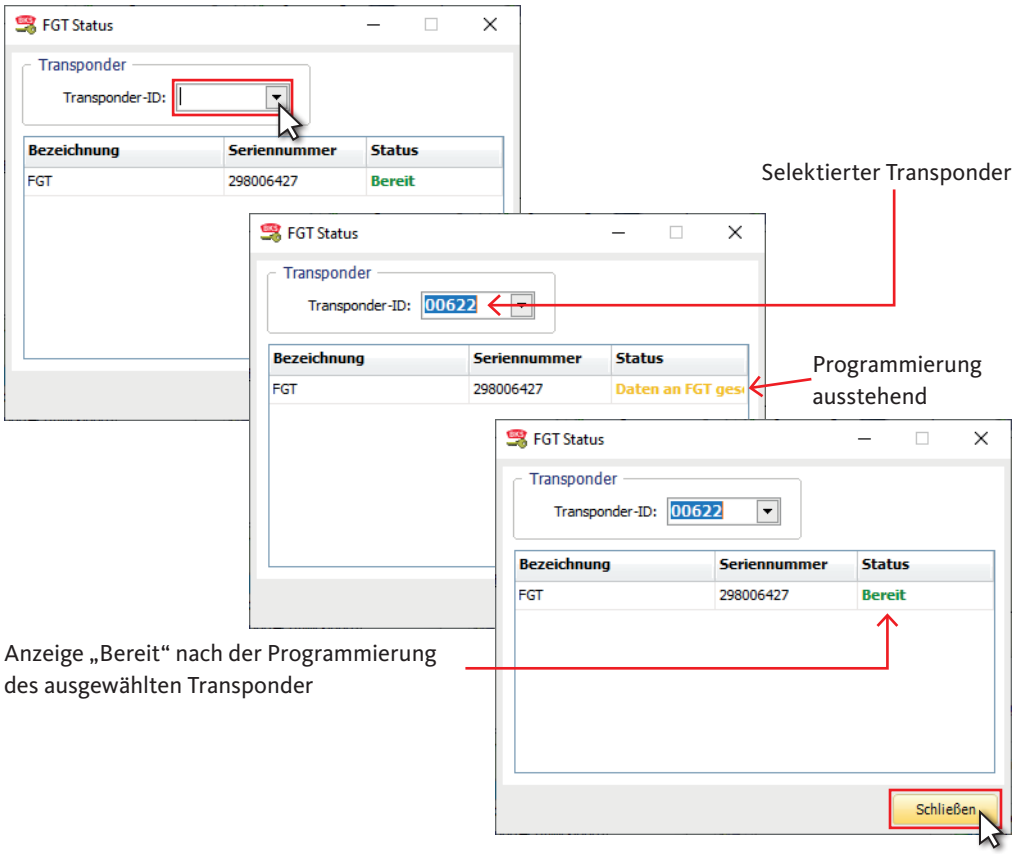
4.6.3 Status der Freigabeterminals (FGT Status)

Der Bericht „FGT Status“ zeigt den Status der Programmierjobs für die verfügbaren Freigabeterminals (FGT) an. Es wird für den ausgewählten Transponder angezeigt, welche Programmierjobs übertragen wurden oder bei keinem ausgewählten Transponder die verbundenen FGTs.

- Drücken Sie auf den Button „FGT Status“, um zum Bericht zu gelangen.

- Wählen Sie über das Dropdown-Menü einen Transponder aus.

Der Status der FGTs zur Programmierung des ausgewählten Transponders werden angezeigt. Bei der Fehlersuche infolge eines nicht übertragenden Programmierjobs kann das FGT, zu dem keine Übertragung stattgefunden hat, mit dieser Funktion lokalisiert werden.



4.6.4 Bediener-Log

Wichtige Aktionen der Bediener werden in der Datenbank protokolliert. Im Bericht „Bediener-Log“ können diese Ereignisse aufgerufen und angezeigt werden. Diese Funktion ist ab einer Professional-Lizenz freigeschaltet.

■ Drücken Sie auf den Button „Bediener-Log“, um zum Bericht zu gelangen.

Die im „Bediener-Log“ angezeigten Einträge können über die Filtereinstellungen (1) eingeschränkt werden. Über die folgenden Einstellungen kann die Ansicht gefiltert werden.

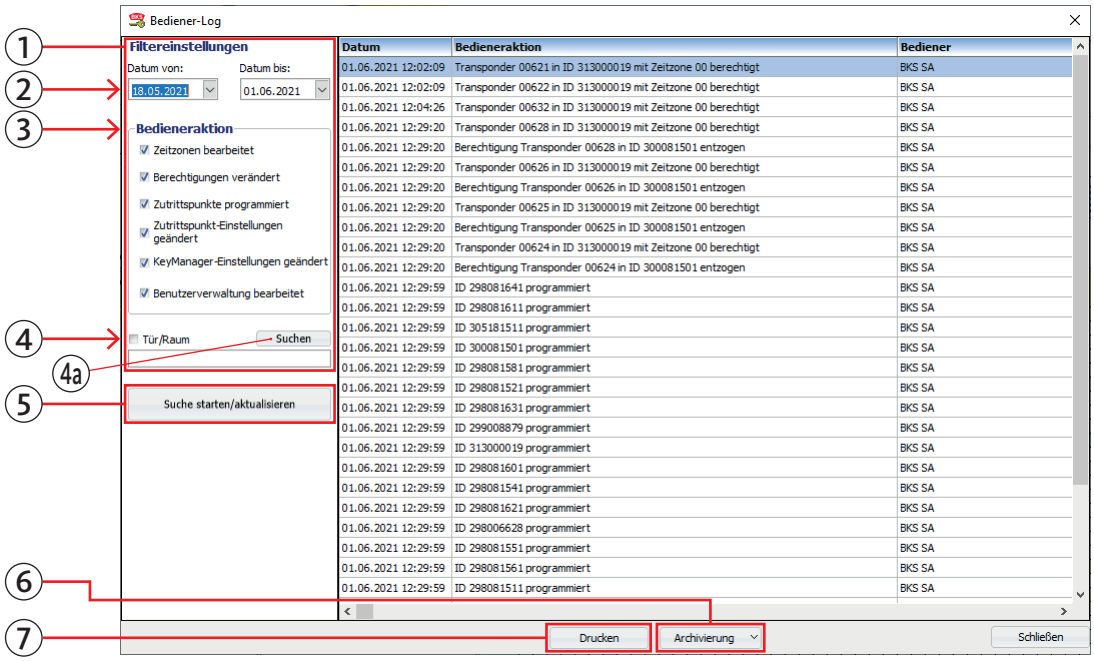
– Nach dem Zeitraum (2), in der die Aktionen stattfanden.

– Die Bediener-Aktion (3) ist durch Aktivierung der Checkbox auswählbar.

– Die Beschränkung auf die Tür/Raum (4) ist durch Aktivierung der Checkbox möglich. Die Tür kann durch Eingabe des Namens oder über den Button „Suche“ (4a) mit Auswahl der Tür über eine Liste gewählt werden.

■ Drücken Sie auf den Button (5), um die Filtereinstellungen anzuwenden.

Das Bediener-Log kann über den Button „Drucken“ (7) ausgegeben oder zur „Archivierung“ (6) über das Dropdown-Menü „Archivdatei für gewählte Aktionen erzeugen“ in eine ZIP-Datei gespeichert werden. Diese kann mit dem Dropdown-Menü „Archivdatei wieder einspielen“ geladen werden.



4.6.5 Berechtigungen der Türen/Zutrittspunkte

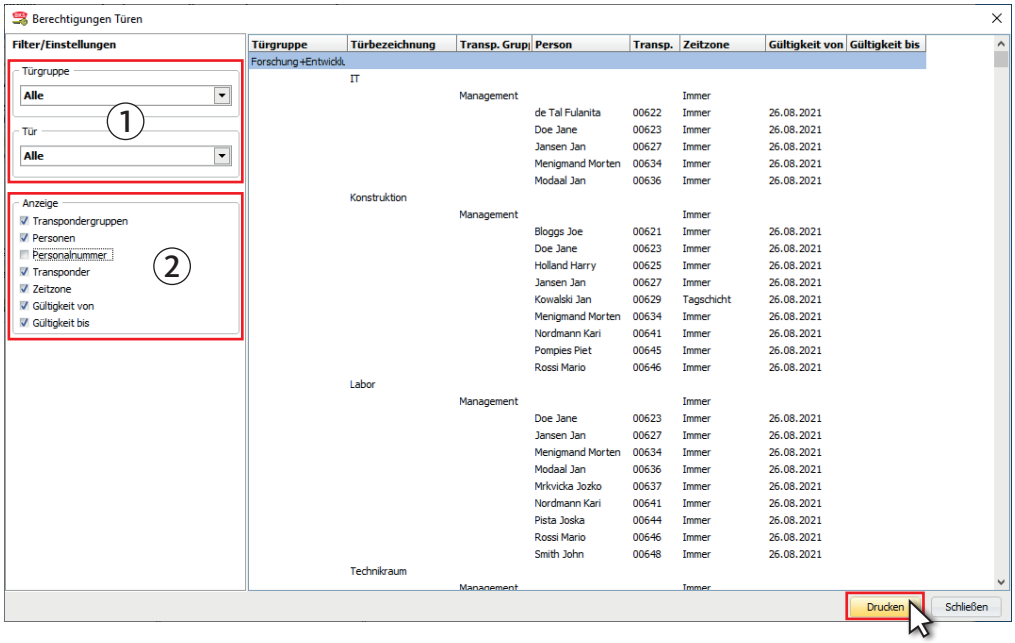
Der Bericht „Türen“ bietet eine Übersicht, welche Transponder (bzw. Personen) und Transpondergruppen jeweils zu den Türen bzw. Zutrittspunkten zutrittsberechtigt sind und welche Zutrittsberechtigung oder Zeitzone der Transponder bzw. die Person hat. Der Bericht ist nach Türen sortiert und die Ansicht kann durch die Filtereinstellung auf die von Ihnen gewünschte Tür oder Türgruppe und Parameter beschränkt werden.

- Drücken Sie auf den Button „Türen“, um zum Bericht zu gelangen.

Mit folgenden Filtereinstellungen kann die Ansicht des Berichts angepasst werden.

- (1) Anzahl der Türen auf eine Türgruppe und/oder Tür begrenzen durch die Auswahl im Pulldown-Menü.
- (2) Spalten in der Ansicht ein- oder ausblenden durch Aktivieren der Checkboxen.

Der Button „Drucken“ ruft eine Druckansicht auf. Diese kann gedruckt oder gespeichert werden.



4.6.6 Berechtigungen der Transponder und Personen

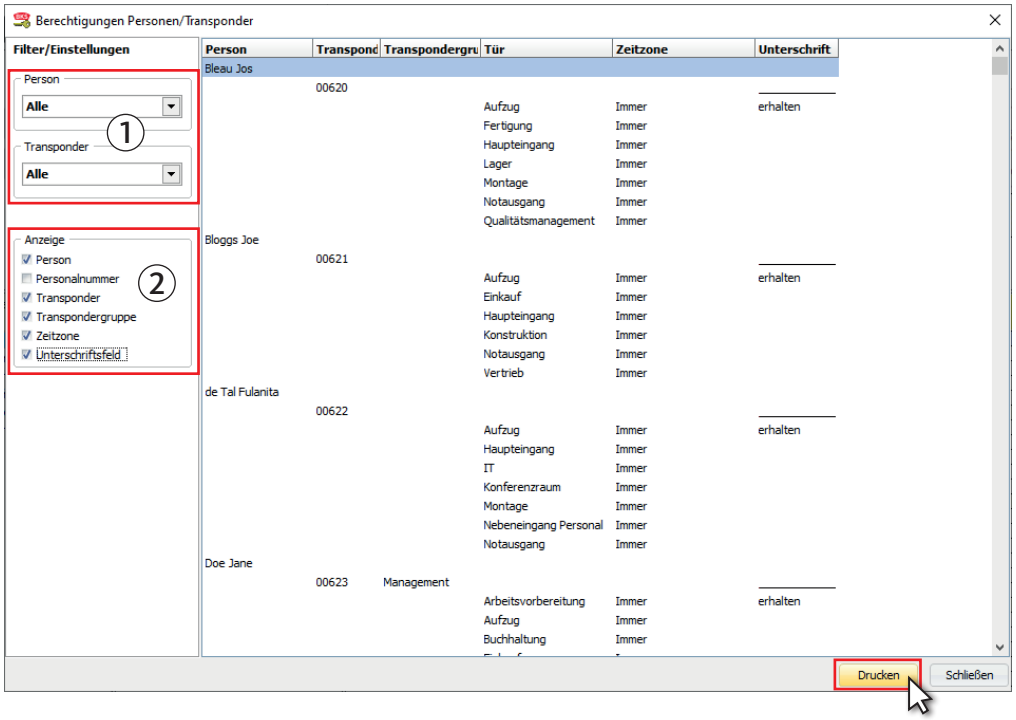
Der Bericht „Personen-Transponder“ bietet eine Übersicht, zu welchen Türen bzw. Zutrittspunkten die Transponder bzw. Personen einen Zutritt haben. Der Bericht ist nach Transponder bzw. Personen sortiert und die Ansicht kann durch die Filtereinstellung auf die von Ihnen gewünschte Person/Transponder und Parameter beschränkt werden.

- Drücken Sie auf den Button „Personen-Transponder“, um zum Bericht zu gelangen.

Mit folgenden Filtereinstellungen kann die Ansicht des Berichts angepasst werden.

- (1) Anzahl der Personen auf eine Person und/oder Transponder begrenzen durch die Auswahl im Pulldown-Menü.
- (2) Spalten in der Ansicht ein- oder ausblenden durch Aktivieren der Checkboxen.

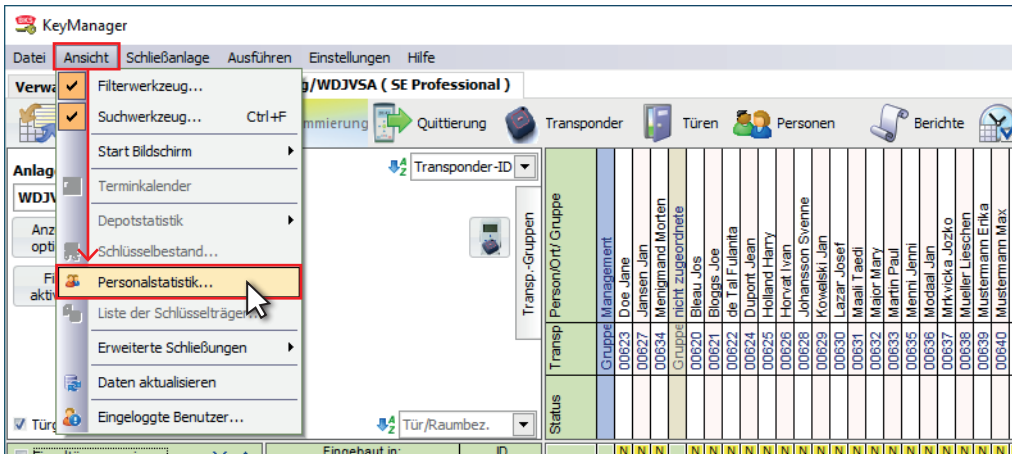
Der Button „Drucken“ ruft eine Druckansicht auf. Diese kann gedruckt oder gespeichert werden.



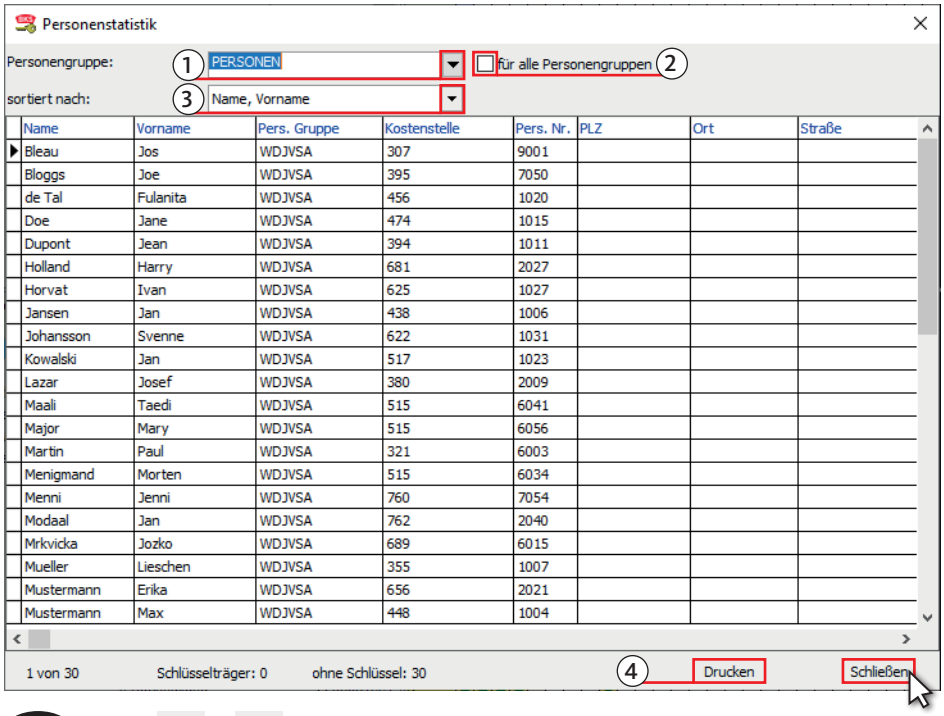
4.6.7 Anzeige der Personenliste, Personalstatistik

Mit dieser Funktion können Sie einen Bericht erstellen, der Ihnen eine Übersicht der Personen gibt, die in Ihrer Datenbank oder den ausgewählten Schließanlagen enthalten sind. Die Stammdaten der Personen werden in der Liste ebenfalls aufgeführt.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Ansicht“ und wählen den Menüpunkt „Personalstatistik ...“ aus.



- (1) Die Anzahl der in der Liste angezeigten Personen kann auf eine Personengruppe beschränkt werden. Wählen Sie im Dropdown-Menü die Schließanlagen aus. Die zu den gewählten Anlagen-gehörenden Personen werden in der Liste angezeigt. (2) Setzen Sie in der Checkbox „für alle Personengruppen“ einen Haken, um alle Personen der Datenbank angezeigt zu bekommen.
- (3) Einstellung nach welchen Kriterien die Liste der Personen sortiert wird. Wählen Sie im Dropdown-Menü eine der Sortieroptionen aus.
- (4) Starten Sie den Dialog zum Ausdruck der angezeigten Personenliste.

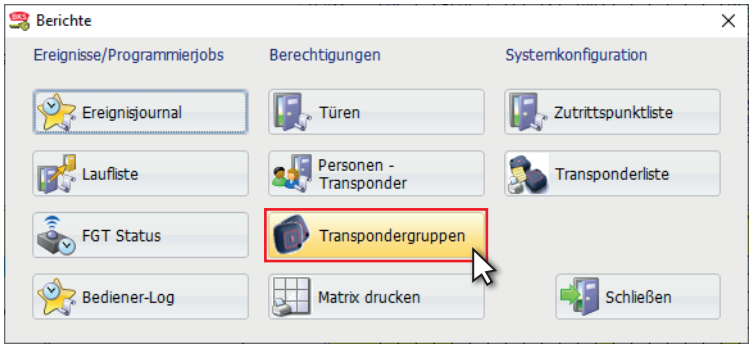


Name	Vorname	Pers. Gruppe	Kostenstelle	Pers. Nr.	PLZ	Ort	Straße
Bleau	Jos	WDJVSA	307	9001			
Bloggs	Joe	WDJVSA	395	7050			
de Tal	Fulanita	WDJVSA	456	1020			
Doe	Jane	WDJVSA	474	1015			
Dupont	Jean	WDJVSA	394	1011			
Holland	Harry	WDJVSA	681	2027			
Horvat	Ivan	WDJVSA	625	1027			
Jansen	Jan	WDJVSA	438	1006			
Johansson	Svenne	WDJVSA	622	1031			
Kowalski	Jan	WDJVSA	517	1023			
Lazar	Josef	WDJVSA	380	2009			
Maali	Taedi	WDJVSA	515	6041			
Major	Mary	WDJVSA	515	6056			
Martin	Paul	WDJVSA	321	6003			
Menigmand	Morten	WDJVSA	515	6034			
Menni	Jenni	WDJVSA	760	7054			
Modaal	Jan	WDJVSA	762	2040			
Mrkvicka	Jozko	WDJVSA	689	6015			
Mueller	Lieschen	WDJVSA	355	1007			
Mustermann	Erika	WDJVSA	656	2021			
Mustermann	Max	WDJVSA	448	1004			

4.6.8 Transpondergruppen (Berechtigungen)

Der Bericht „Transpondergruppen“ bietet eine Übersicht, welche Türen bzw. Zutrittspunkte von den Transpondergruppen zutrittsberechtigt sind, welche Zeitzone oder Zutrittsberechtigung der Gruppe zur Tür besteht und welche Transponder bzw. Personen zur Transpondergruppe gehören und dadurch berechtigt sind. Der Bericht ist nach Transpondergruppen sortiert und die Ansicht kann durch die Filtereinstellung auf die von Ihnen gewünschte Transpondergruppe und Parameter beschränkt werden.

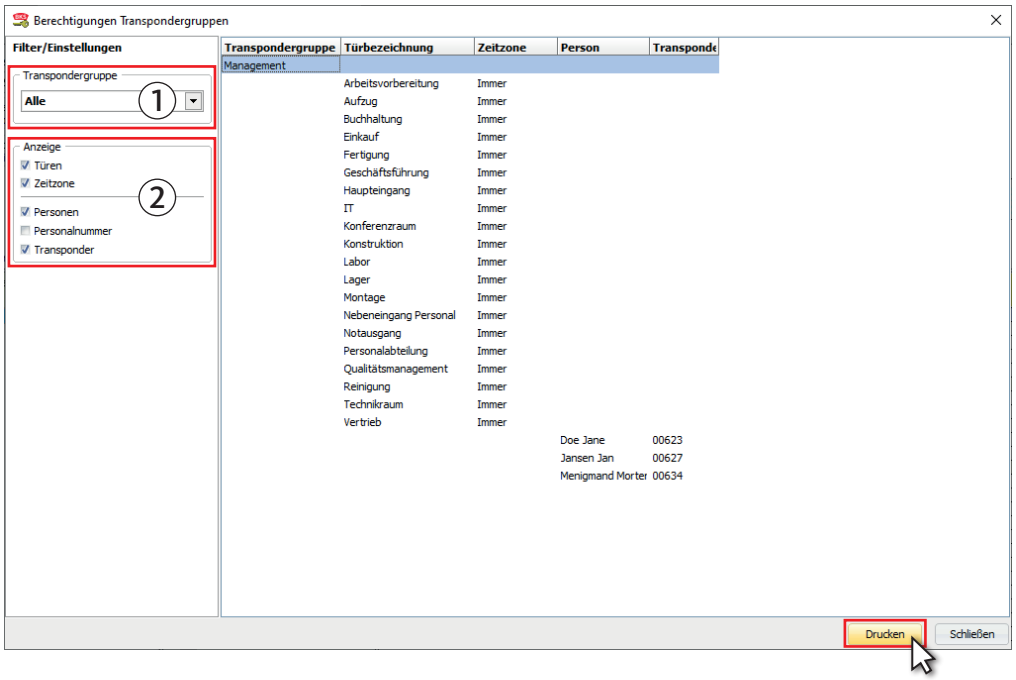
- Drücken Sie auf den Button „Personen-Transponder“, um zum Bericht zu gelangen.



Mit folgenden Filtereinstellungen kann die Ansicht des Berichts angepasst werden.

- (1) Anzahl der Transpondergruppen auf eine Gruppe begrenzen durch die Auswahl im Pulldown-Menü.
- (2) Spalten in der Ansicht ein- oder ausblenden durch Aktivieren der Checkboxen.

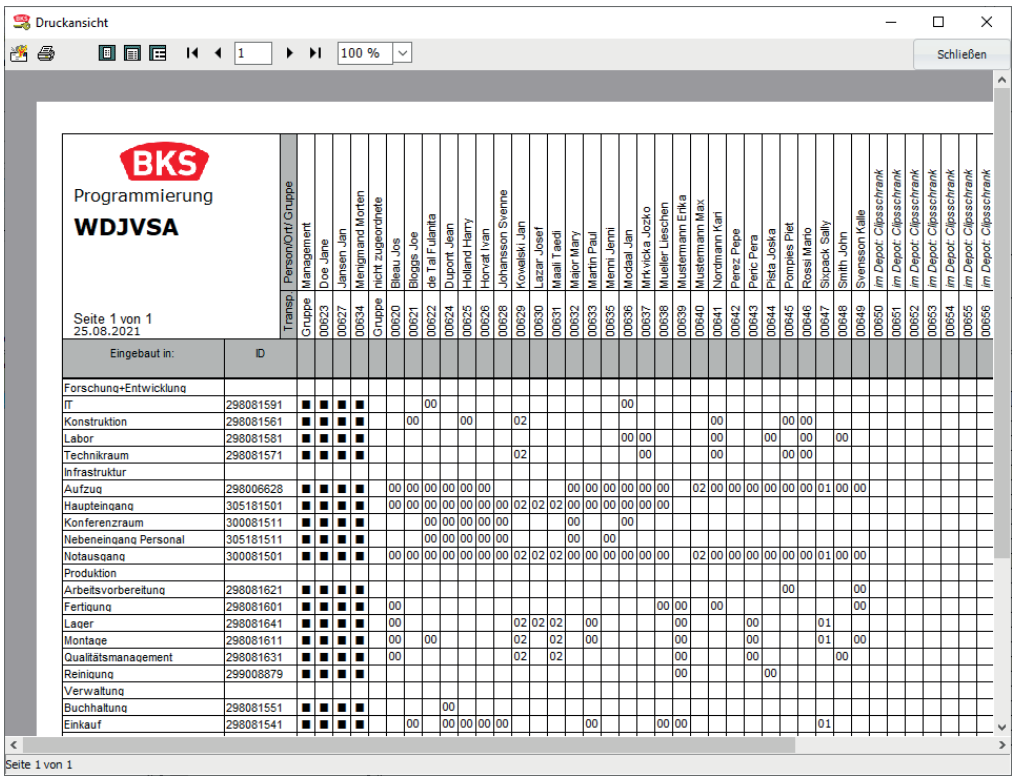
Der Button „Drucken“ ruft eine Druckansicht auf. Diese kann gedruckt oder gespeichert werden.



4.6.9 Matrix ausdrucken (Berechtigungen)

- Drücken Sie auf den Button „Matrix drucken“, um zum Bericht zu gelangen.

Mit dieser Funktion gelangen Sie zur Ansicht des momentan aktuellen Stands Ihrer Schließanlage. Diese Darstellung kann als Momentaufnahme der Berechtigungsmatrix ausgedruckt werden.



4.6.10 Zutrittspunktliste (Konfiguration)

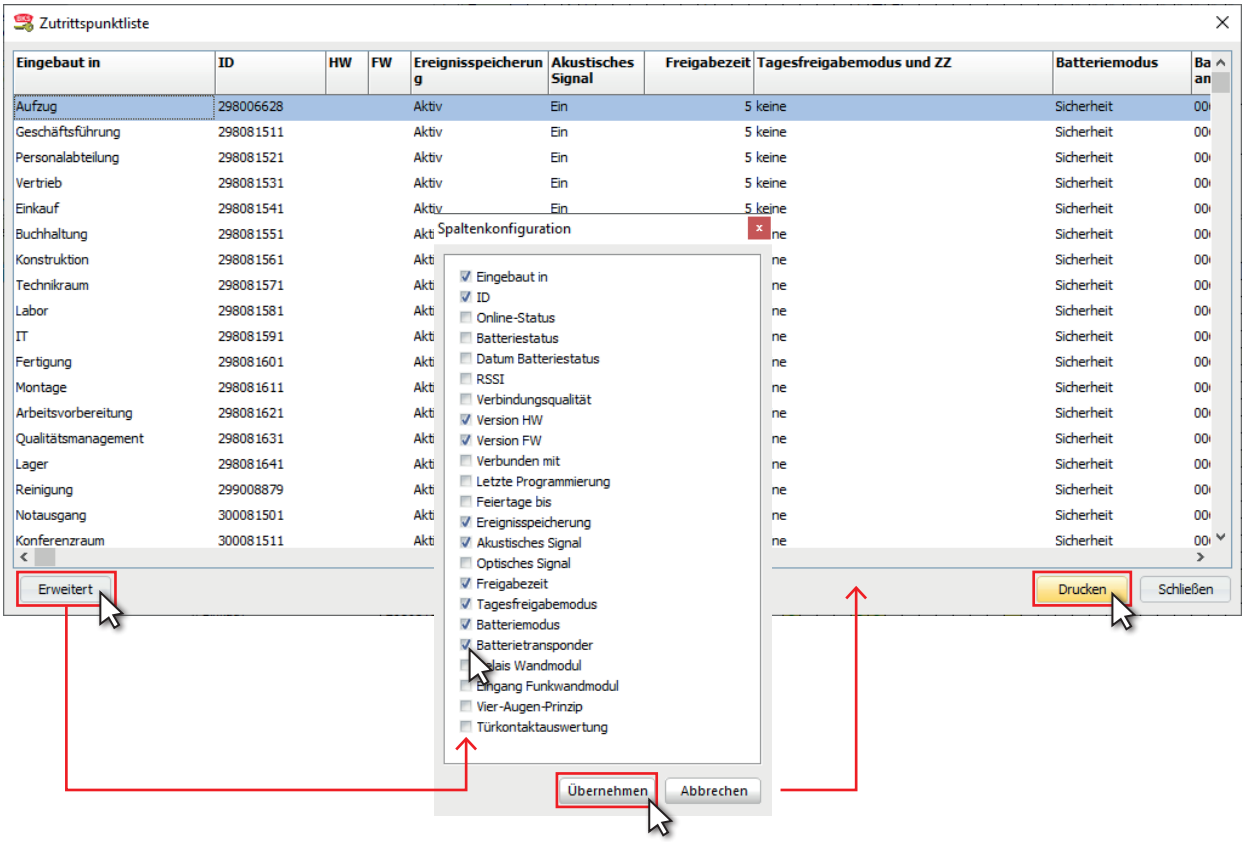
Der Bericht „Zutrittspunktliste“ ist eine Übersicht des aktuellen Status aus der Systemkonfiguration der Zutrittspunkte bzw. Türen in Ihrem Schließsystem. Hierbei werden zu jedem Zutrittspunkt die Einstellungen aufgelistet. Es lässt sich so ein Protokoll über die aktuelle Konfiguration der Zutrittspunkte erstellen, um z. B. bei einer Übergabe den Istzustand festzuhalten.

- Drücken Sie auf den Button „Zutrittspunktliste“, um zum Bericht zu gelangen.

Mit folgenden Filtereinstellungen kann die Ansicht des Berichts angepasst werden.

- Drücken Sie auf den Button „Erweitert“, um die Spaltenkonfiguration zu starten.
- Aktivieren oder deaktivieren Sie die Checkboxen, um weitere Informationen in den Spalten des Berichts ein- oder auszublenden. Drücken Sie auf den Button „Übernehmen“.

Der Button „Drucken“ ruft eine Druckansicht auf. Diese kann gedruckt oder gespeichert werden.



4.6.11 Transponderliste (Konfiguration)

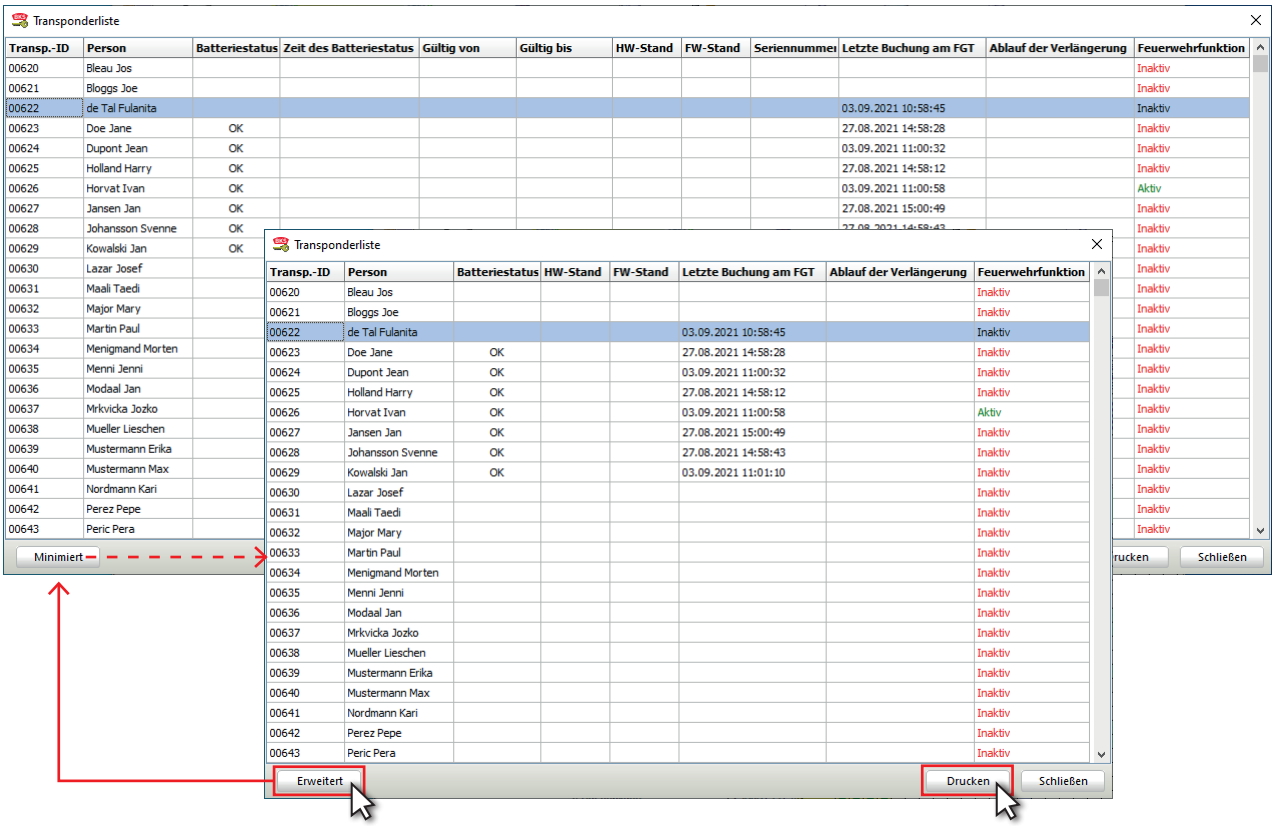
Der Bericht „Transponderliste“ ist eine Übersicht der Transponder und Personen in Ihrem Schließsystem mit dem aktuellen Status und Konfiguration. Hierbei werden zu jedem Transponder die Einstellungen aufgelistet. Es lässt sich so eine Übersicht über die aktuelle Konfiguration und den Status der Transponder erstellen.

- Drücken Sie auf den Button „Transponderliste“, um zum Bericht zu gelangen.

Die Transponderliste wird mit reduzierter Spaltenanzahl („Minimiert“) angezeigt.

- Drücken Sie auf den Button „Erweitert“, um alle verfügbaren Eigenschaften des Transponders anzuzeigen und in den Spalten der Transponderliste darzustellen.

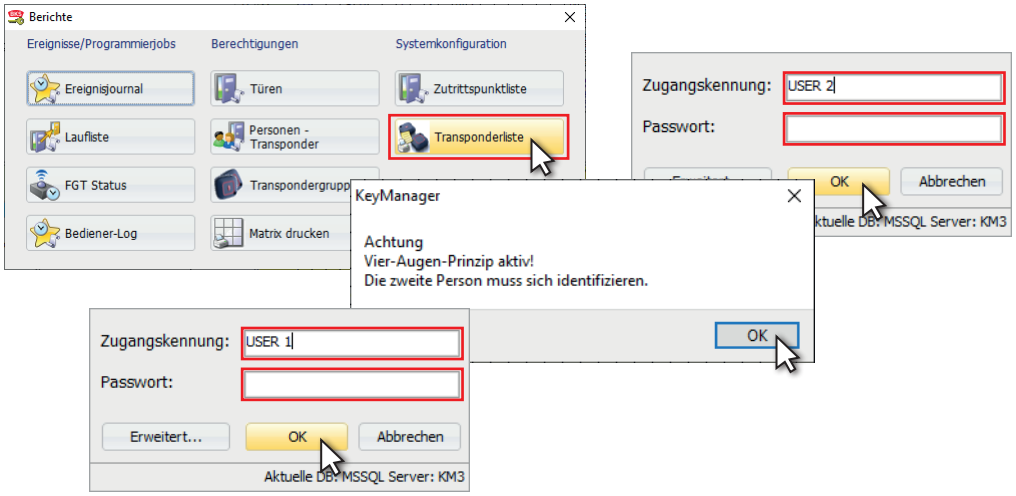
Der Button „Drucken“ ruft eine Druckansicht auf. Diese kann gedruckt oder gespeichert werden.



4.6.11.1 Sicherheitsstufen beim Zugriff auf die Transponderliste

Der Zugriff auf den Bericht „Transponderliste“ ist nur für Benutzer mit entsprechendem Recht zum Lesen dieses möglich. Über zwei Sicherheitsstufen können weitere Einschränkungen zum Zugang erfolgen.

Die erste Sicherheitsstufe ermöglicht nur einen Zugriff auf die Transponderliste, nachdem sich ein berechtigter Benutzer erneut mit Benutzernamen und Passwort eingeloggt hat. In der zweiten Sicherheitsstufe muss sich noch zusätzlich ein weiterer Benutzer mit Berechtigung anmelden, um den Zugriff freizuschalten.

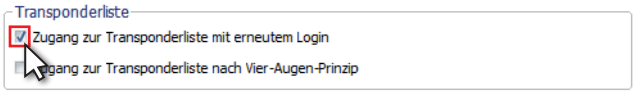


Die Sicherheitsstufen sind über das Menü „Einstellungen“auszuwählen, siehe Kapitel 5.1.1.2 [260].

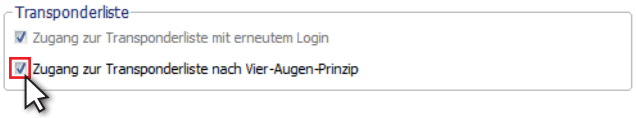
- Aktivieren Sie die jeweiligen Checkboxen.

➔ **Uneingeschränkter Zugriff auf die Transponderliste.**
Wird keine Checkbox aktiviert, können berechtigte Benutzer ohne eine weitere Authentifizierung die Berichte einsehen.

➔ **Zugriff auf die Transponderliste mit aktiviertem erneutem Login.**
Wird diese Option gewählt, ist für den Zugriff auf das Transponderliste die erneute Eingabe der Zugangskennung und Passwort von einem berechtigten Benutzer erforderlich.



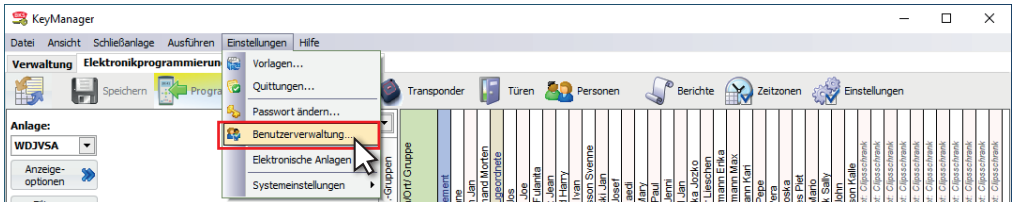
➔ **Zugriff auf die Transponderliste mit aktiviertem 4 Augen Prinzip.**
Bei Aktivierung dieser Option ist der Zugriff auf das Transponderliste nur noch möglich, wenn zwei berechtigte Benutzer sich authentifizieren.
Beide Benutzer müssen im BKS KeyManager für die Transaktion „Ereignisjournal“ berechtigt worden sein. Diese Berechtigung ist über die Benutzerverwaltung des BKS KeyManagers zu gewähren.

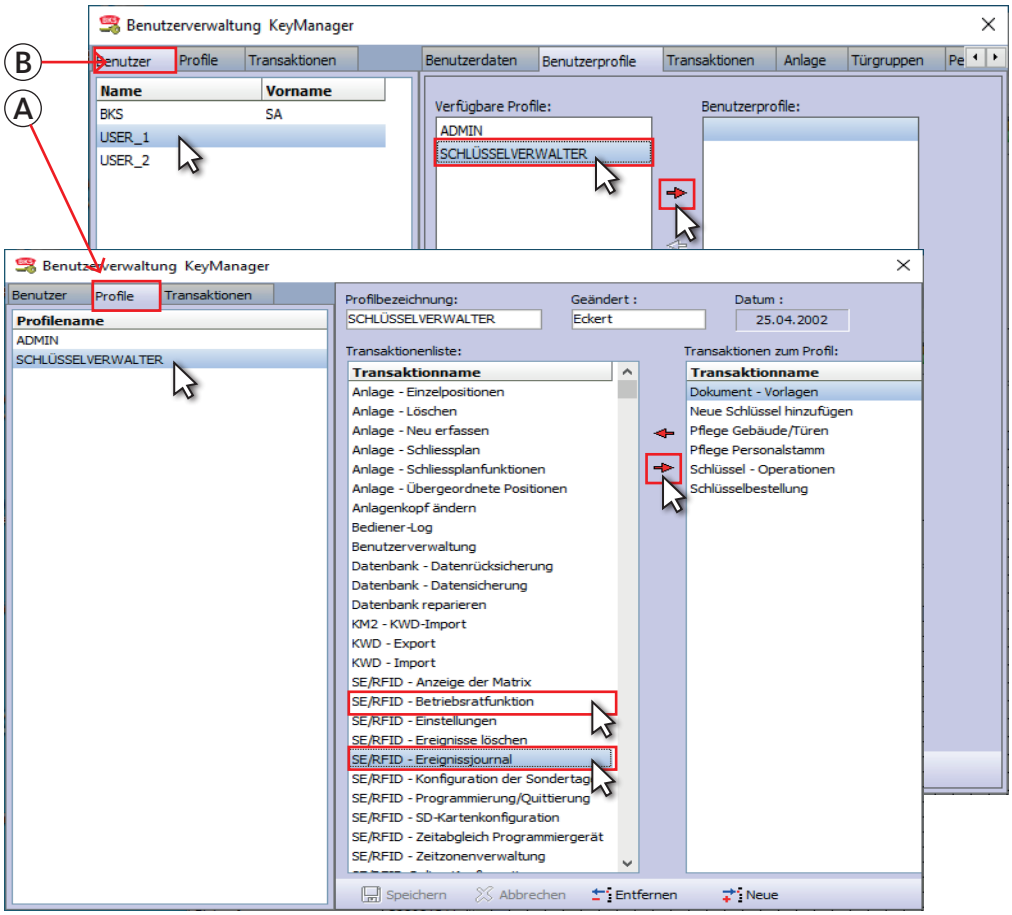


- Legen Sie die Berechtigungen der Benutzer über die Benutzerverwaltung fest, siehe Kapitel 6 [339].

In der Benutzerverwaltung können die Rechte der Transaktionen nur von Administratoren vergeben werden. Zum Einstellen der Benutzerrechte befolgen Sie folgende Schritte.

- (A) Beginnen Sie mit der Auswahl eines bestehenden Profils oder erstellen ein neues Profil. Markieren Sie eine aus den verfügbaren Transaktionen eine Transaktion aus und weisen diese mit dem „Pfeil“ dem markierten Profil zu.
- (B) Wählen Sie einen Benutzer aus oder erstellen einen neuen Benutzer. Weisen Sie diesem mit dem „Pfeil“ aus den verfügbaren Profilen ein Profil zu.



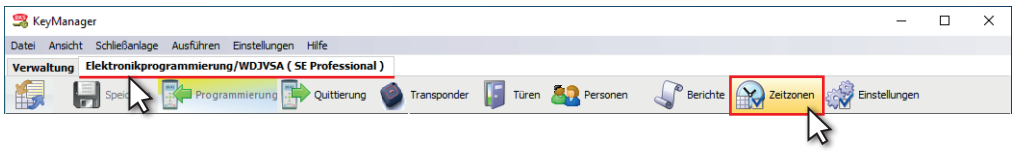


4.7 Zeitzonen und Sondertage für Zutrittsberechtigungen

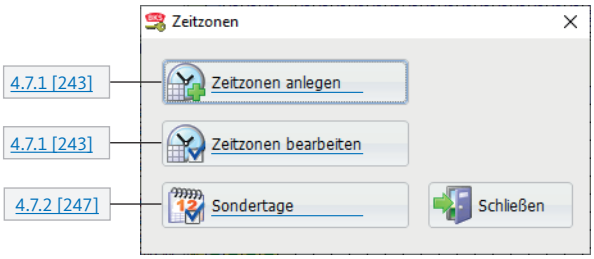
Das Menü „Zeitzonen“ bietet Ihnen die Möglichkeit, die Berechtigungen von Transpondern bzw. Personen zu den Türen bzw. Zutrittspunkten genauer zu definieren. Hierdurch werden die beiden im BKS KeyManager standmäßig vorhandenen Berechtigungen, „Ja/Nein“-Rechte bzw. „ständiger Zutritt“ oder „kein Zutritt“ um einen bestimmten Zeitbereich, innerhalb der eine Berechtigung besteht, erweitert.

Mit der Funktion „Zeitzonen“ werden Intervalle festgelegt, während dessen eine zeitlich beschränkte Zutrittsberechtigung besteht. Diese Zeitzonen können bei der Vergabe der Berechtigungen den Personen, Transpondern und Zutrittspunkten zugeordnet werden, um diesen für den festgelegten Zeitraum eine Berechtigung zum Zutritt zu gewähren.

- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Zeitzonen“.



Im Menü „Zeitzonen“ lassen sich die folgenden Funktionen aufrufen.



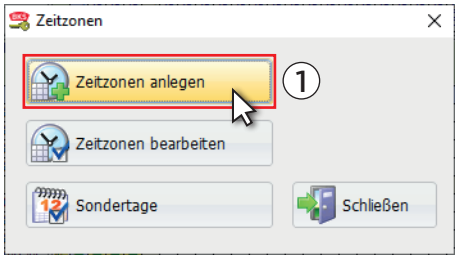
HINWEIS

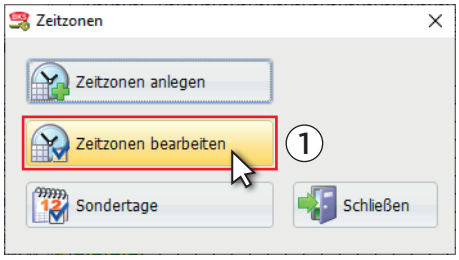
Die Zeitzone 000 für einen „Immer“-Zugang ist grundsätzlich vorhanden und kann nicht verändert oder gelöscht werden.
Es können in einer Anlage max. 128 Zeitzonen und pro Tag max. 4 Intervalle angelegt werden.

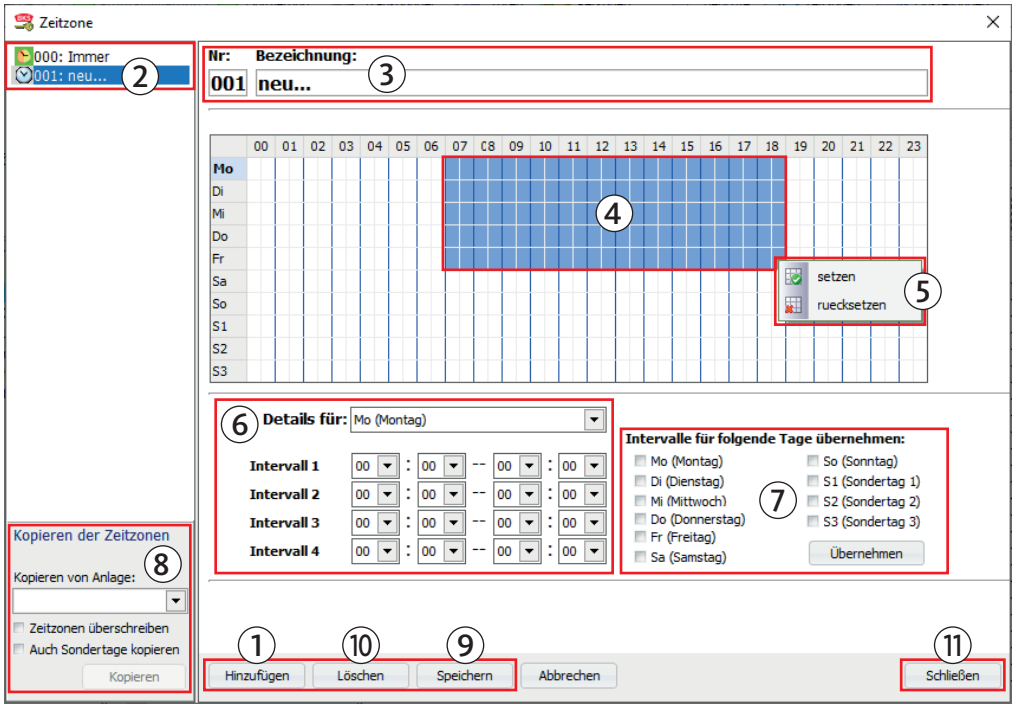
4.7.1 Einrichtung und Bearbeitung der Zeitzonen

In diesem Menü werden die gewünschten Zeitzonen definiert, während dessen die Berechtigung zu einem zeitlich eingeschränkten Zutritt besteht.

- Drücken Sie den Button „Zeitzone anlegen“ oder „Zeitzonen bearbeiten“ zum Anlegen bzw. Bearbeiten einer Zeitzone.





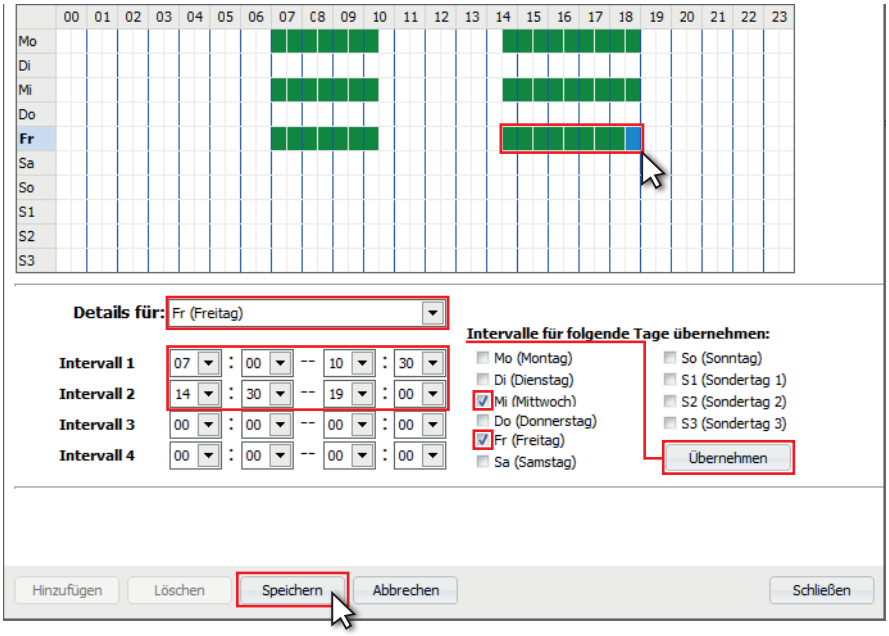


Im Fenster „Zeitzone“ sind folgende Eingaben zur Einrichtung oder Überarbeitung möglich:

Nr.	Eingabe	Beschreibung
1	Hinzufügen	Button zum Anlegen oder Bearbeiten einer neuen Zeitzone.
2	Auswahl	Liste zur Übersicht und Auswahl der zu überarbeitenden Zeitzone.
3	Bezeichnung	Feld zur Eingabe des neuen Namens der Zeitzone oder zum Editieren.
4	Zeitzonenfeld	Matrix Tag/Uhrzeit, in der die Zutrittsberechtigungen als grüne Balken angezeigt werden. Die Sondertage (S1 bis S3) erteilen eine Zutrittsberechtigung für die im Kapitel 4.7.2 [247] festgelegte und zugewiesene Sondertage.
5	Berechtigung	Nach dem Erstellen einer Auswahl (Feld ziehen mit der Maus) in der Matrix werden Sie zum Setzen der Berechtigung über ein Dropdown-Menü aufgefordert. Durch Setzen wird die Zeitzone aktiviert bzw. mit Rücksetzen die Berechtigung entfernt. Pro Tag sind nur 4 Intervalle möglich.
6	Intervall	Manuelle Eingabe der Zeitintervalle für jeweils den unter "Details für:" angezeigten Tag.
7	Übernahme	Übernahme der manuell konfigurierten Intervalle eines Tages für die zur Übernahme ausgewählten Tage.
9	Import	Die Zeitzonen von einer anderen Anlage kopieren und einfügen.
10	Speichern	Die Zeitzone speichern.
11	Löschen	Ausgewählte Zeitzone löschen.
12	Schließen	Dialog beenden.

Beim Anlegen einer Neuen oder Bearbeiten einer vorhandenen Zeitzone für die zeitlich begrenzte Zutrittsberechtigung sind die folgenden Punkte zu beachten.

- Zum Anlegen einer neuen Zeitzone ist im Feld „Bezeichnung“ (3) der Name für die neue Zeitzone einzutragen.
- Drücken Sie auf den Button „Hinzufügen“ (1) und fahren mit der Bearbeitung fort.
- Zur Bearbeitung einer Zeitzone wählen Sie die gewünschte Zone in der Liste (2) aus.
- Der Name bzw. die Bezeichnung der Zeitzone kann im Feld (3) geändert werden.
- Die Zeitzone ist zeitlich durch Intervalle und Tage festzulegen, an denen eine zeitliche Berechtigung für den Zutritt besteht. Die Intervalle lassen sich sowohl für die Wochentage von Montag bis Sonntag wie auch für die Sondertage S1 bis S3 vergeben. Es sind maximal vier Intervalle pro Tag möglich.
  - In der Matrix Tag/Uhrzeit können Sie Intervalle in Balkenform (4) für eine Zeitzone erstellen. Durch die Auswahl eines oder mehrerer Felder durch Auswählen und Ziehen mit der Maus wird ein Balken für ein Intervall grafisch erstellt. Nach dem „setzen“ (5) im Kontextmenü wird der Balken grün angezeigt. Diesen Schritt können Sie wiederholen, um weitere Balken zu erstellen oder durch „Rücksetzen“ (5) im Kontextmenü vorhandene Balken löschen.
  - Die Intervalle (6) lassen sich auch händisch durch Eintragen der Daten anlegen. Wählen Sie mit „Details für:“ den gewünschten Tag aus und tragen die Anfangs– und Endzeiten für die Intervalle ein. Wiederholen Sie diesen Vorgang um weitere Tage zu pflegen.
  - Mit „Übernehmen“ (7) lassen sich auch Intervalle von einem Tag auf weitere Tage kopieren. Nach der Erstellung der Intervalle für einen Tag können Sie für das Übernehmen im Dialog die Checkboxen der Tage aktivieren, für welche die Intervalle übernommen werden sollen. Abschließend drücken Sie den Button „Übernehmen“, um die Intervalle zu setzen.

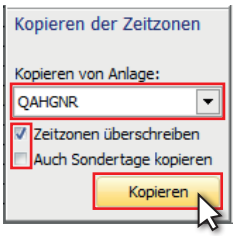


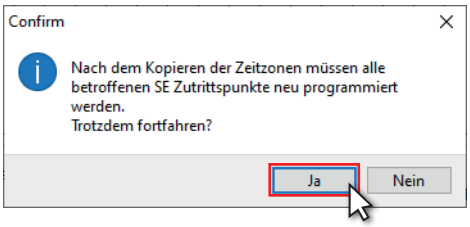
Zur Veranschaulichung wurde hier montags, mittwochs und freitags in der Zeit von 7:00–10:00 Uhr und von 14:30–19:00 Uhr eine Zeitzone erstellt. An Sondertagen besteht keine Berechtigung.
Die Zeitzone steht in der Berechtigungsmatrix für die weitere Vergabe von Zutrittsberechtigungen zur Verfügung.

- Drücken Sie auf den Button „Speichern“ (9), um die neu erstellte bzw. überarbeitete Zeitzone zu sichern.

Bei Verwaltung von mehreren Schließanlagen im BKS KeyManager können bereits in anderen Anlagen vorhandene Zeitzonen in die aktuelle Schließanlage kopiert werden.

- Importieren Sie mit „Kopieren der Zeitzonen“ (8) die Zonen in Ihre aktuelle Anlage.
- – Wählen Sie im Dropdown-Menü die Anlage, von der die Zeitzonen importiert werden sollen, aus.
  - Für die Optionen zum Überschreiben vorhandener Zeitzonen und zum Import von Sondertagen aktivieren Sie ggf. die Checkboxen.
  - Drücken Sie den Button „Kopieren“ und zur Bestätigung auf „Ja“.





Eine gewählte Zeitzone kann durch Drücken des Buttons „Löschen“ (11) wieder entfernt werden.

- Drücken Sie auf den Button „Schließen“ (12) und beenden den Dialog.

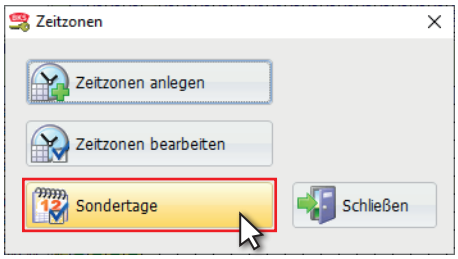
4.7.2 Einrichten und Bearbeiten der Sondertage

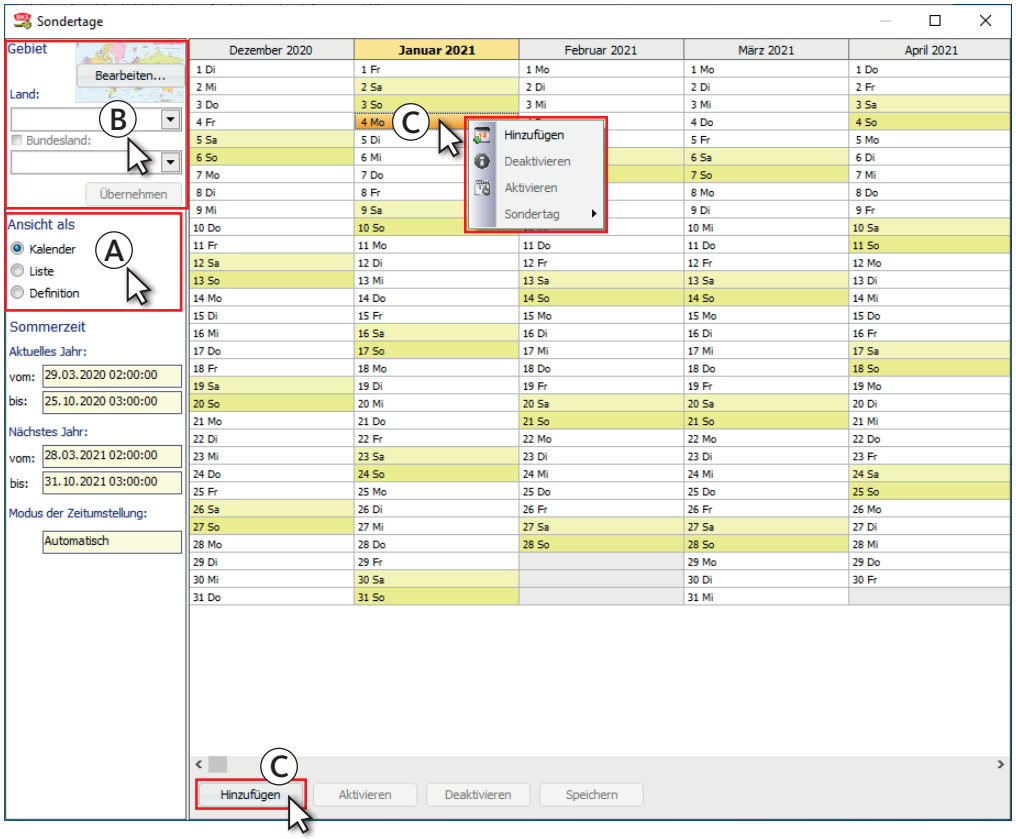
Sondertage sind eine den allgemeinen Wochentagen übergeordnete Spezifizierung für besondere Ereignisse oder Feiertage. Die in den Zeitzonen angelegten Intervalle für die Zutrittsberechtigung von Wochentagen gelten nicht an den Sondertagen. Die Zutrittsberechtigung für Sondertage muss in der Zeitzone gesondert erteilt werden oder falls keine erteilt wird, besteht an Sondertagen kein Zutritt, auch wenn für den betreffenden Wochentag eine Berechtigung besteht.

Zum Beispiel ist in einem Unternehmen eine Zeitzone für eine Zutrittsberechtigung an den Arbeitstagen von Montag bis Freitag eingerichtet worden. Am Ostermontag soll die Firma aber geschlossen bleiben und auch kein Personal vor Ort sein. Um dem Personal an diesem Tag den Zutritt zu verwehren, kann man diesen Tag als Sondertag festlegen und mit anderen Zutrittsrechten versehen, ohne die Zutrittsberechtigung der allgemeinen Wochentage zu beeinflussen.

Um eine größere Variabilität zu haben, können die Sondertage in drei Sondertagsklasse von S1 bis S3 unterteilt werden. Sie können aber auch problemlos in nur einer Sondertagsklasse verbleiben.

- Drücken Sie den Button „Sondertage“ zur Einrichtung oder Bearbeitung dieser.



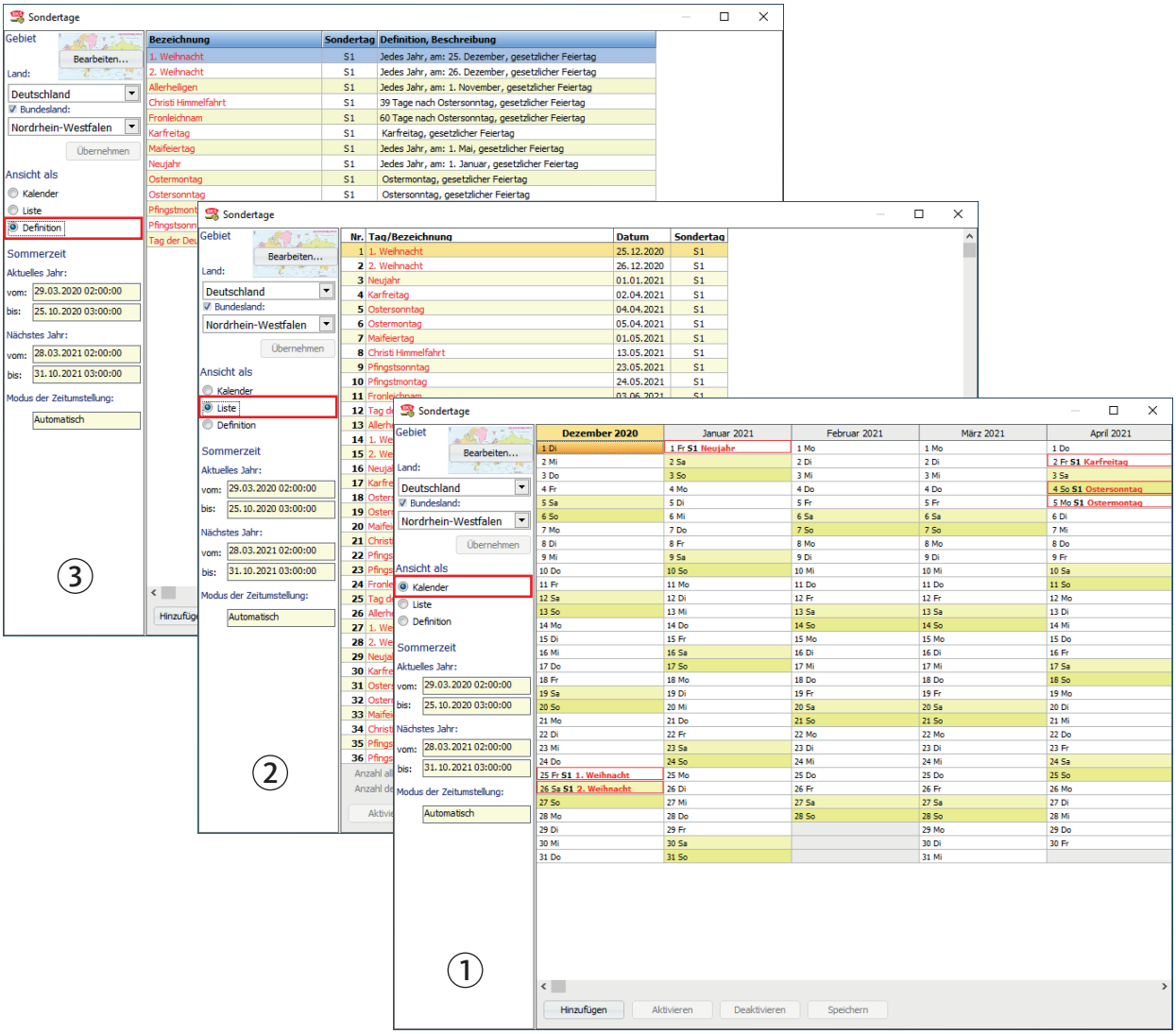


4.7.2.1 Auswahl der Ansicht der Sondertage (A)

Im Feld "Ansicht als" kann die Darstellung der Sondertage frei gewählt werden. Wählen Sie eine der drei folgenden Möglichkeiten aus.

- (1) Kalenderansicht (klassische Übersicht nach Monaten und Tagen)
- (2) Listenansicht (Tabellarische Darstellung der Sondertage)
- (3) Definitionsliste (Listenansicht mit zusätzlicher Beschreibung)

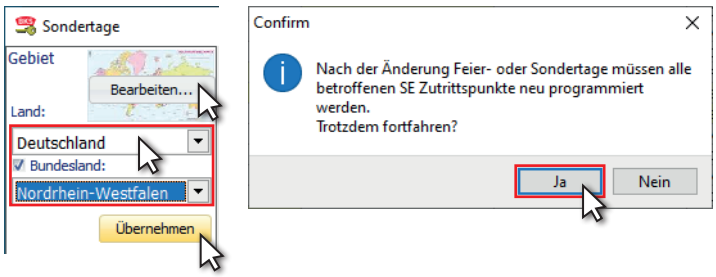
Die Einstellung der Klassifizierung der Sondertage nach S1 bis S3 kann nur in Listenansichten und der Definitionsliste vorgenommen werden.



4.7.2.2 Sondertage aus den Vorlagen importieren (B)

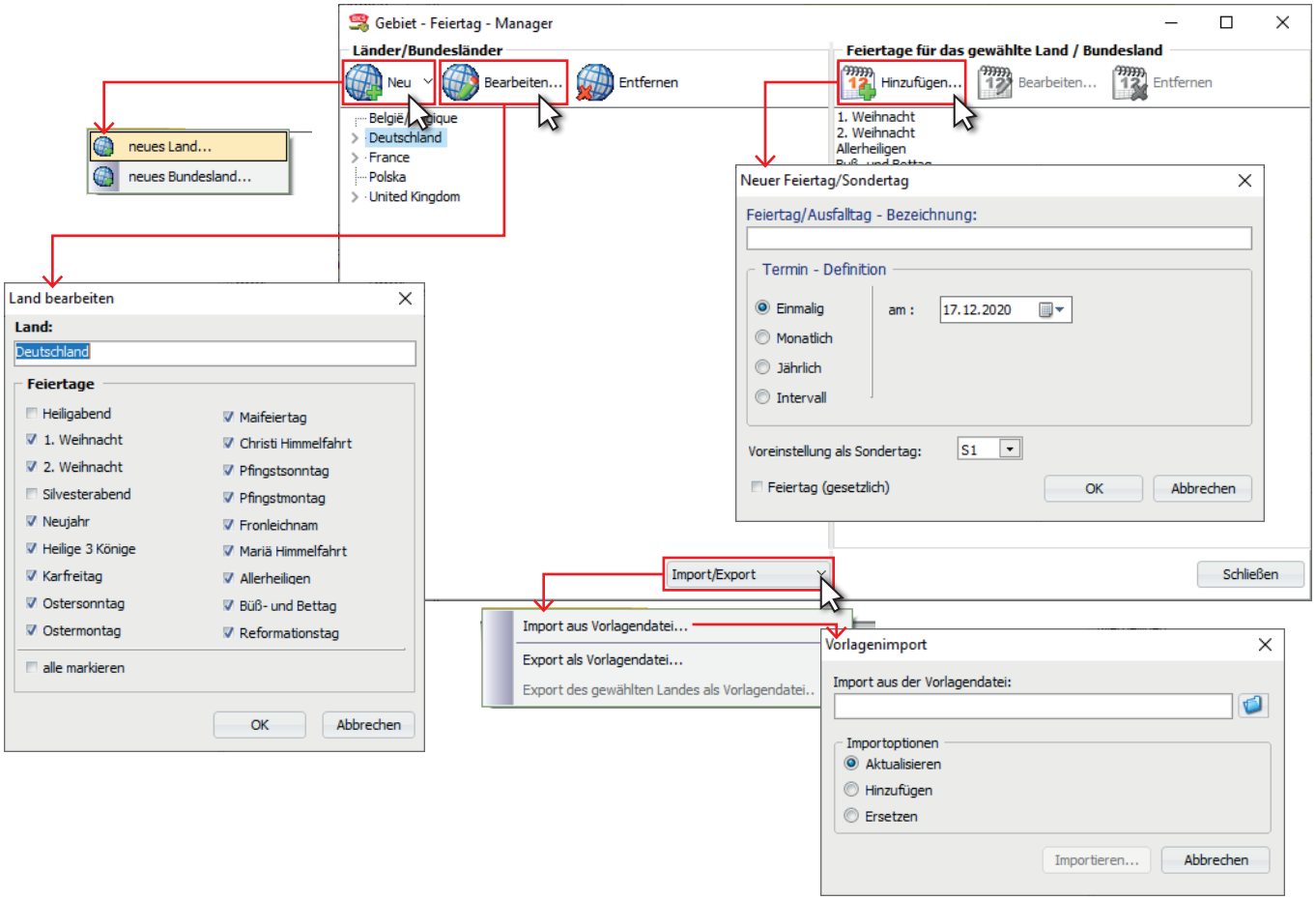
Die Feiertage für Deutschland und die der unterstützten Landessprachen sind im BKS KeyManager als Vorlage der Sondertage enthalten.

- Zum Importieren einer Vorlage wählen Sie ein gewünschtes "Land" aus. Zur feineren Auswahl kann durch Aktivierung der Checkbox ein Bundesland z. B. Nordrhein-Westfalen gewählt werden.
- Drücken Sie auf den Button „Übernehmen“, um die Feiertage in die Sondertage zu übernehmen. Bestätigen Sie den Hinweis mit „Ja“ und Programmieren die Zutrittspunkte. Spielen Sie die neue Programmierung (mit allen Daten) auf die Zutrittspunkte auf.



Mit dem Feiertagsmanager können Sie die vorhandenen landesspezifischen Vorlagen bearbeiten sowie eine Vorlage für ein neues Land manuell hinzufügen.

- Drücken Sie auf den Button „Bearbeiten“ und öffnen den Feiertagsmanager.



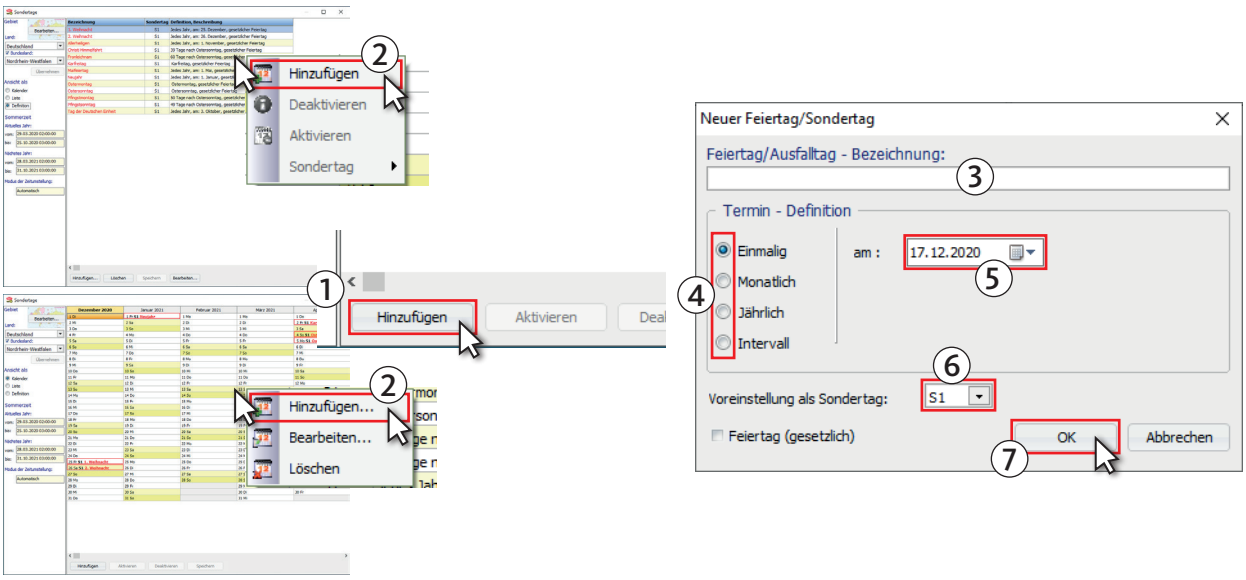
Im Feiertag-Manager können die Vorlagen editiert werden. Es ist möglich, dass Länder hinzugefügt oder bearbeitet werden sowie Feiertage anlegt oder geändert werden können.

- Drücken Sie auf den jeweiligen Button, um eine der folgenden Funktionen aufzurufen:
  - → „Neu“ zum Anlegen eines neuen Landes.
  - → „Bearbeiten ...“ zur Bearbeitung eines vorhandenen Landes.
  - → „Hinzufügen ...“ ermöglicht einen neuen Feiertag für das ausgewählte Land zu erstellen.
  - → „Import/Export“ zum Import einer neuen Vorlagendatei (*.KM3) in den Feiertag-Manager oder Export vorhandener Feiertage in eine Vorlagendatei für ein oder alle Länder.

Nach dem „Schließen“ des Feiertag-Managers können Sie mit dem Button „Übernehmen“ die neuen Feiertage der Vorlage im Fenster „Sondertage“ einfügen.

4.7.2.3 Zusätzliche Sondertage hinzufügen (C) oder bearbeiten

Zum Hinzufügen eines Sondertages können Sie in der Ansicht „Kalender“ oder „Definition“ den Dialog über den Button „Hinzufügen ...“ (1) oder über das Kontextmenü (2) starten.



- Drücken Sie auf den Button „Hinzufügen ...“ (1). Das Fenster „Neuer Feiertag/Sondertag“ wird geöffnet.
- Geben Sie in das Feld „Bezeichnung“ (3) einen Namen für den anzulegenden Sondertag an.
- Wählen Sie eine Checkbox (4) für die Wiederholung des Termins aus.

Durch diese Auswahl wird festgelegt, ob es sich um einen einmaligen Sondertag, einen monatlich oder jährlich wiederkehrenden Sondertag oder einem einmaligen Intervall handelt. Das Intervall wird nur durch das Start- und Enddatum festgelegt. Dadurch müssen nicht alle Tage einzeln im Zutrittspunkt gespeichert werden. Ein Beispiel sind Ferien an Schulen.

- Machen Sie weitere Angaben (5) zum Sondertag. Der Sondertag ist durch Datum, Gültigkeitsdauer sowie das Enddatum des Intervalls zu definieren.

Das Dropdown-Menü Voreinstellung (6) legt die Klassifizierung des Sondertages fest. Ordnen Sie den Sondertag den Klassen „S1“ bis „S3“ zu. Die Einstellung „S0“ bedeutet keinen Sondertag. Die Klasse können Sie später beim Einrichten der Zeitzonen verwenden.

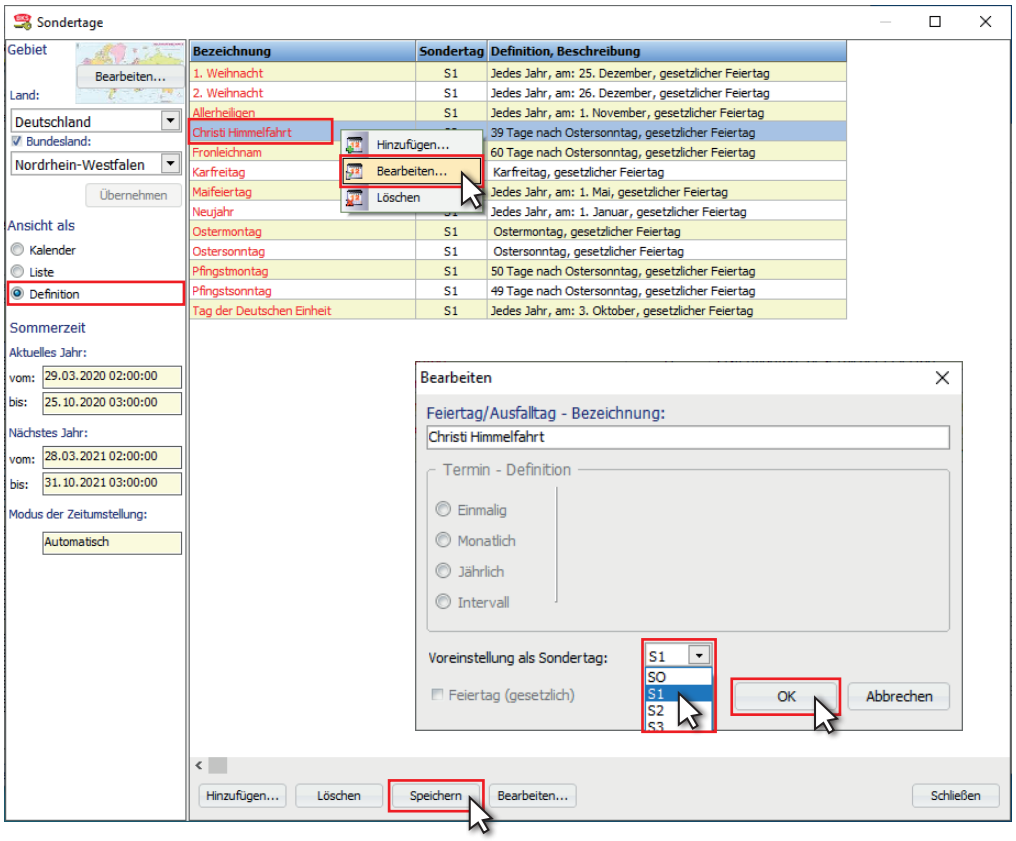
- Drücken Sie auf den Button „OK“ (7) zum Beenden der Eingabe und im Fenster „Sondertage“ auf den Button „Speichern“, um die Eingabe zu sichern.

Die übernommenen Sondertage werden Ihnen in den drei Ansichten Kalender, Liste und Definition angezeigt. In der Ansicht Kalender ist die Einstellung der Klasse nicht möglich.

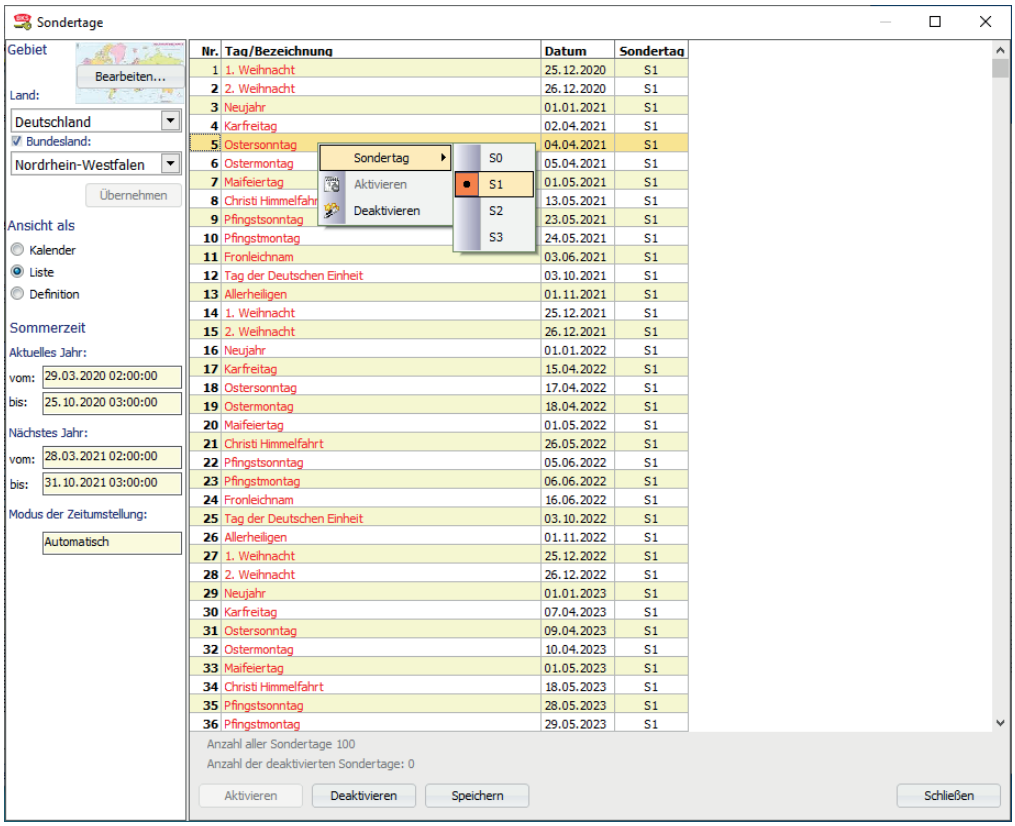
HINWEIS

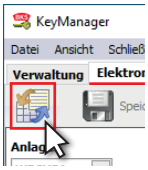
Grundsätzlich gilt für alle im BKS KeyManager eingerichteten Sondertage, dass die gewünschten Zutrittsberechtigungen durch die Klassifizierung S1 bis S3 in der Zeitzone nur aktiv wird, wenn diese explizit mit dem Programmiergerät auf die Zutrittspunkte übertragen wurde. Bei dieser Übertragung werden immer die nächsten 50 Sondertage übermittelt, wodurch vor Ablauf des letzten Sondertags die Zutrittspunkte immer wieder aktualisiert werden müssen. Bei vorhandenen Zeitzonen mit Klassifizierung wird ohne gepflegte Sondertage der Zutritt von der Schließanlage verweigert.

- In der Ansicht „Definition“ können Sie durch Auswahl des entsprechenden Sondertages mit der rechten Maustaste das Kontextmenü (2) öffnen. Drücken Sie auf „Bearbeiten ...“.
- Im Fenster „Bearbeiten“ kann die Einstellung der Klassifizierung geändert werden (S0 = kein Sondertag oder S1 bis S3 für jeweils eine Klasse).
- Drücken Sie auf den Button „OK“ und „Speichern“, um den Dialog zu beenden.



- In der Ansicht „Liste“ können Sie durch Auswahl eines Sondertags mit der rechten Maustaste das Kontextmenü „Sondertag“ öffnen.
- Die Einstellung Klassifizierung lässt sich im Dropdown-Menü ändern (S0 = kein Sondertag oder S1 bis S3).
  In diesem Menü ist eine Deaktivierung bzw. Aktivierung ebenfalls möglich.
- Drücken Sie den Button „Speichern“, um den Dialog zu beenden.

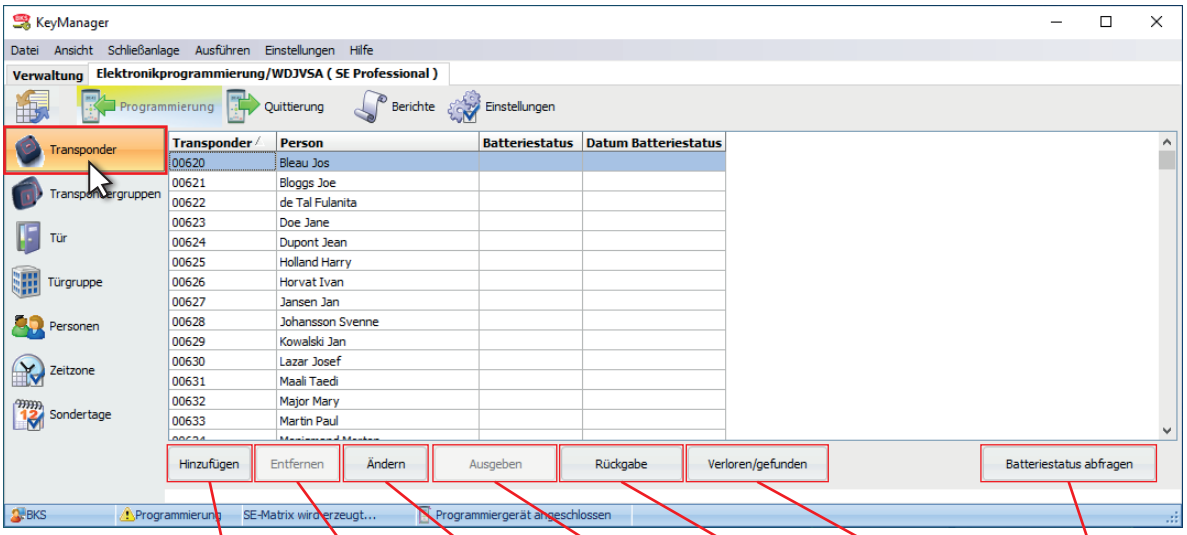




4.8 Listenmenü

4.8.1 Transponder (Listenansicht)

- Drücken Sie auf die Schaltfläche „Transponder“ und wählen ggf. einen Transponder aus. Betätigen Sie den Button mit der gewünschten Funktion.

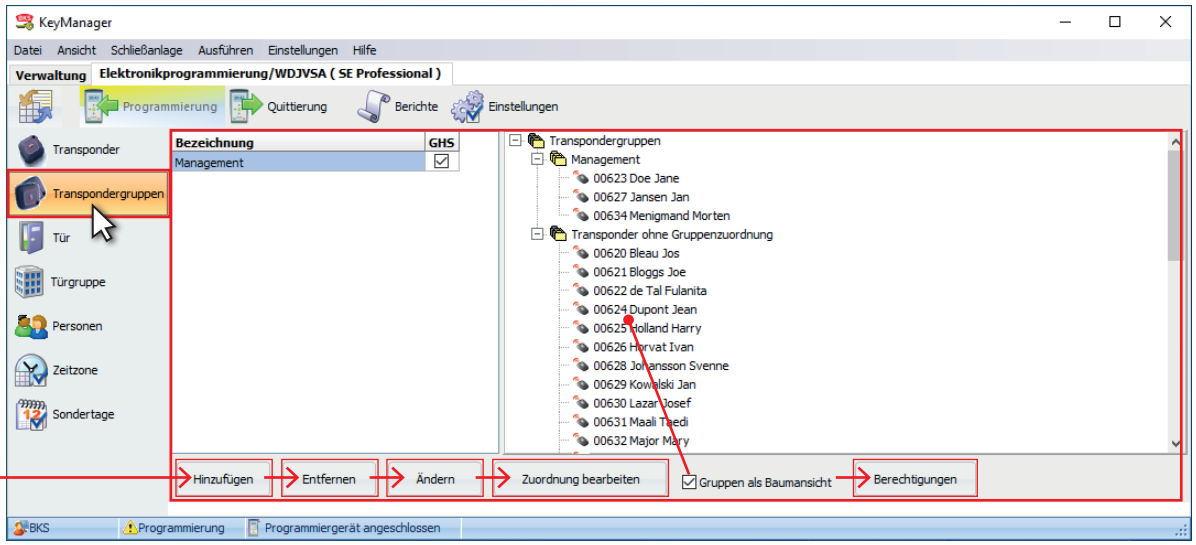


Die Beschreibung der Funktion und die weiteren Schritte finden Sie im zugehörigen Kapitel.

4.2.1	4.2.6	4.2.8	4.2.2	4.2.3	4.2.4	4.2.10
Seite 161	Seite 184	Seite 189	Seite 164	Seite 175	Seite 177	Seite 196

4.8.2 Transpondergruppen (Listenansicht)

- Drücken Sie auf die Schaltfläche „Transpondergruppen“ und wählen ggf. eine Gruppe aus. Betätigen Sie den Button mit der gewünschten Funktion.



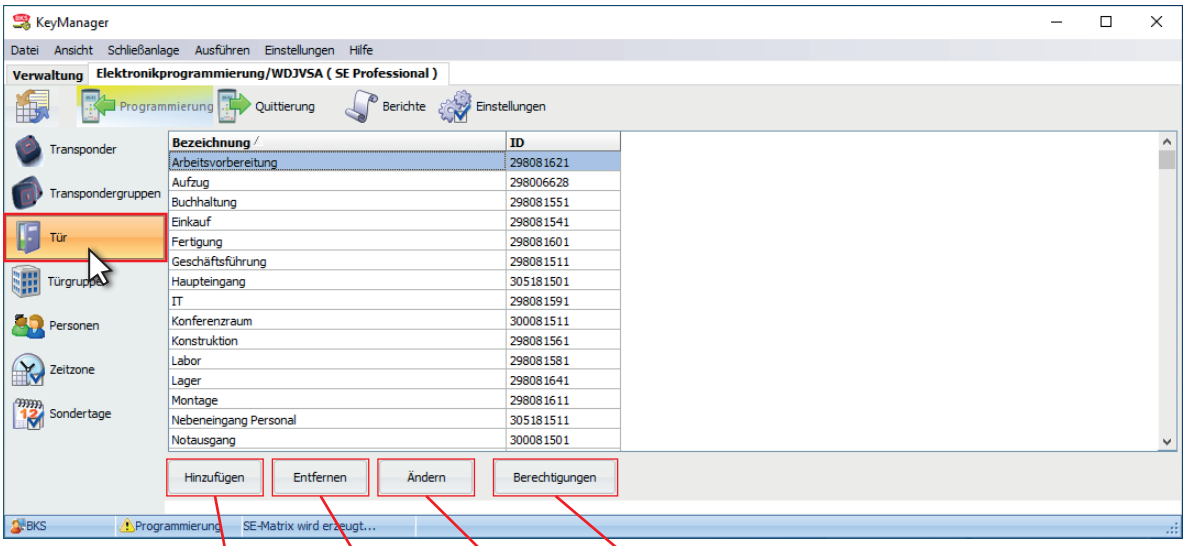
Die Beschreibung der Funktion und die weiteren Schritte finden Sie im zugehörigen Kapitel.

4.2.7

Seite 186

4.8.3 Türen/Zutrittspunkten (Listenansicht)

- Drücken Sie auf die Schaltfläche „Tür“ und wählen eine Tür aus.
  Betätigen Sie den Button mit der gewünschten Funktion.

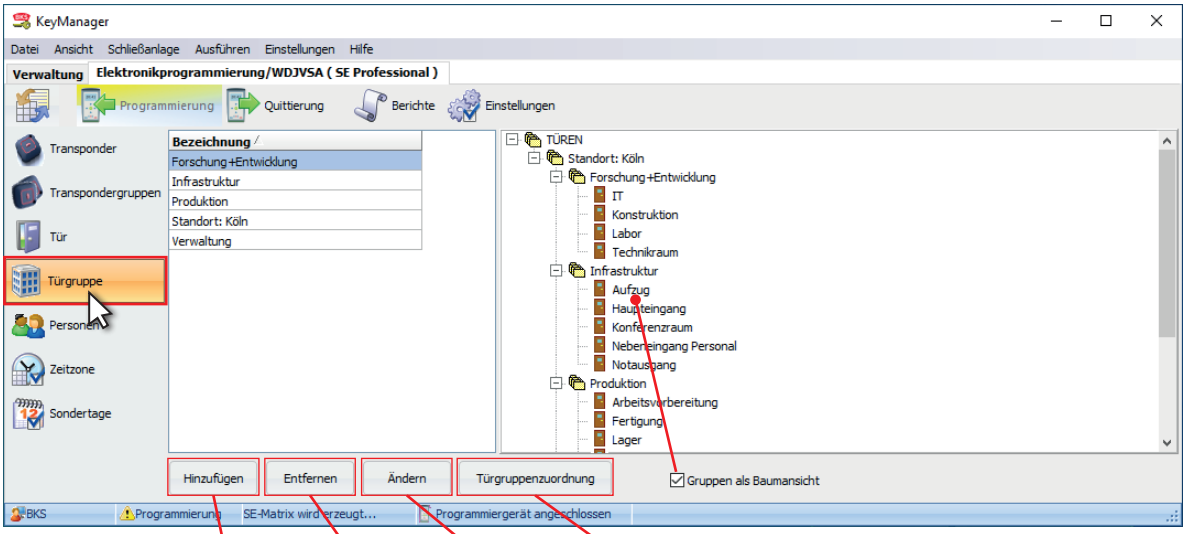


Die Beschreibung der Funktion und die weiteren Schritte finden Sie im zugehörigen Kapitel.

4.3.1 Seite 202
4.3.3 Seite 209
4.3.2 Seite 208
4.3.4 Seite 210

4.8.4 Türgruppen/Gruppen von Zutrittspunkten

- Drücken Sie auf die Schaltfläche „Türgruppe“ und wählen ggf. eine Gruppe aus.
  Betätigen Sie den Button mit der gewünschten Funktion.

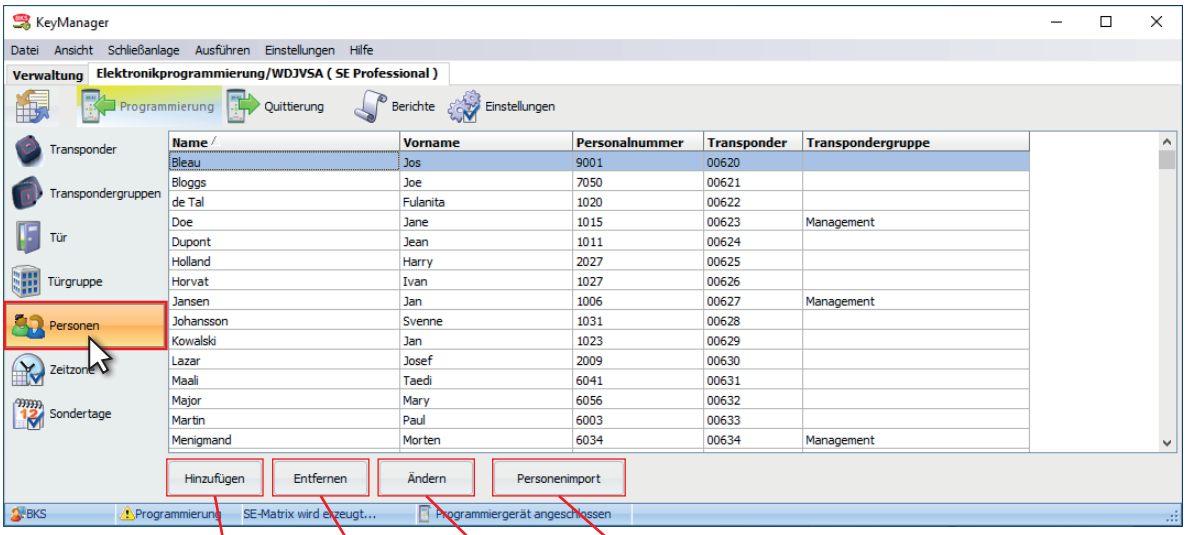


Die Beschreibung der Funktion und die weiteren Schritte finden Sie im zugehörigen Kapitel.

4.4.1 Seite 213
4.4.2 Seite 213
4.4.3 Seite 214
4.4.4 Seite 214

4.8.5 Personen (Listenansicht)

- Drücken Sie auf die Schaltfläche „Personen“ und wählen ggf. eine Person aus. Betätigen Sie den Button mit der gewünschten Funktion.



Die Beschreibung der Funktion und die weiteren Schritte finden Sie im zugehörigen Kapitel.

4.5.1 Seite 216

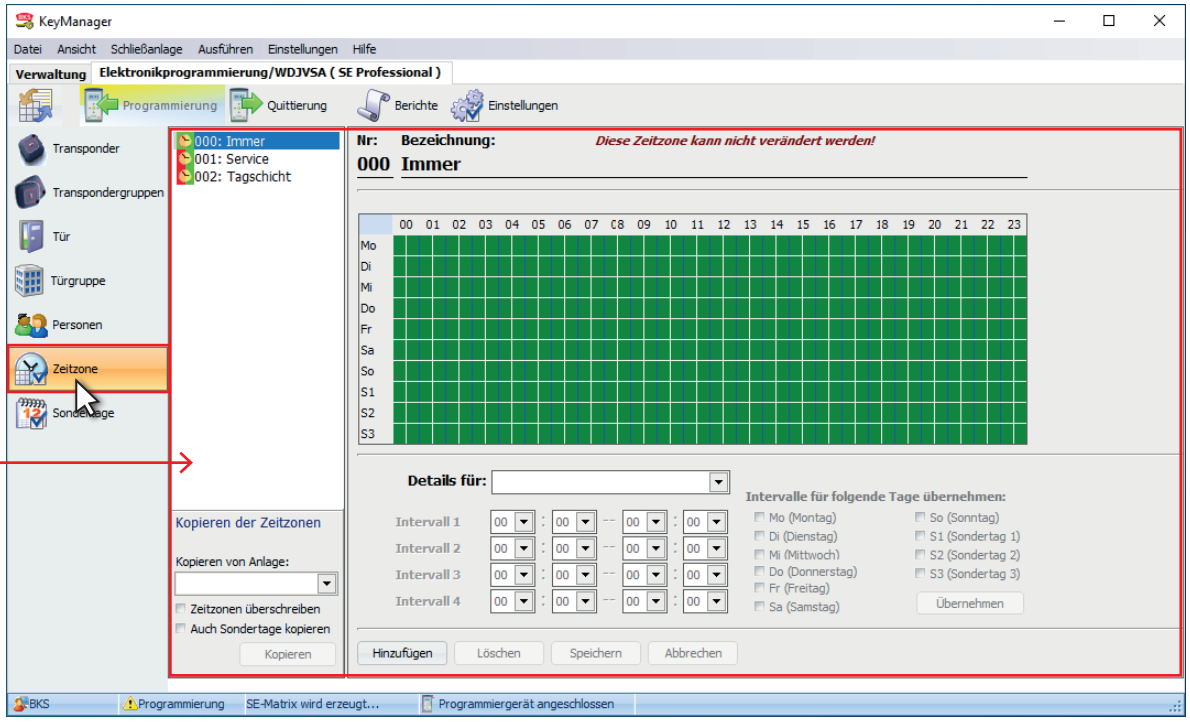
4.5.3 Seite 218

4.5.2 Seite 217

4.5.4 Seite 219

4.8.6 Zeitzonen (Listenansicht)

- Drücken Sie auf die Schaltfläche „Zeitzone“ und wählen ggf. eine Zone aus. Betätigen Sie den Button mit der gewünschten Funktion.

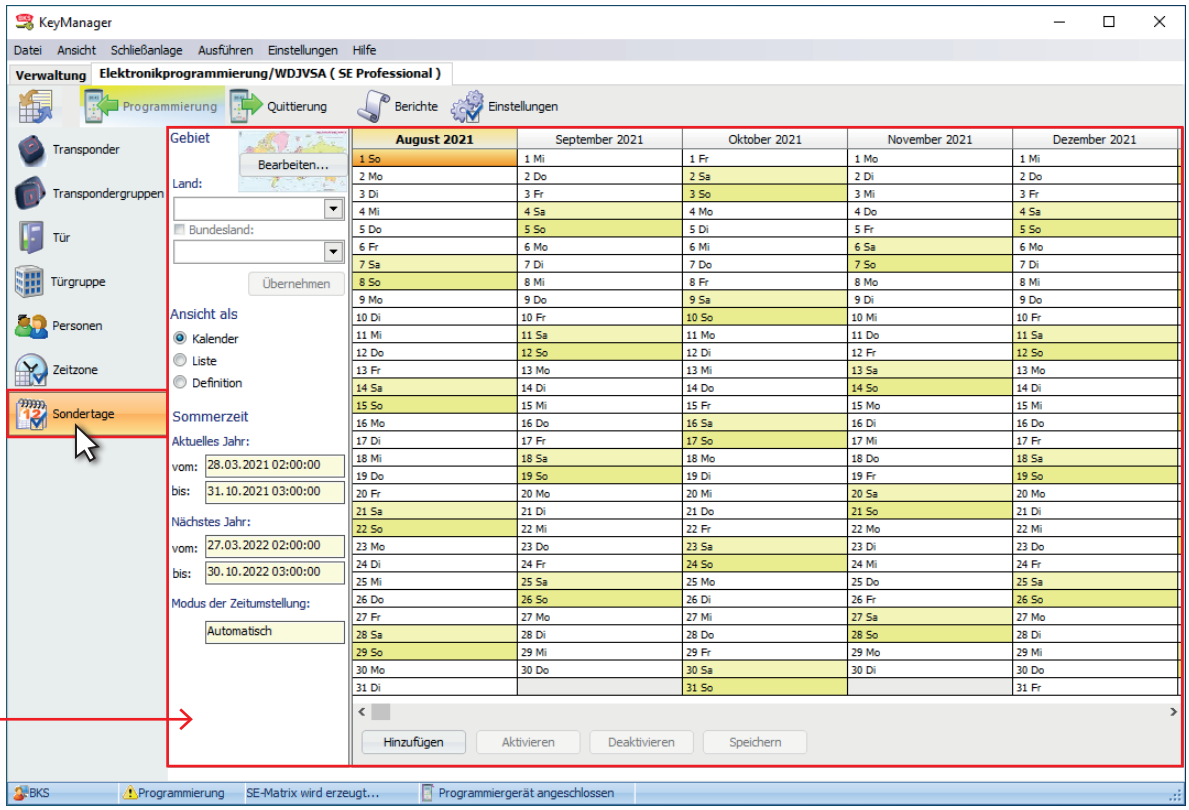


Die Beschreibung der Funktion und die weiteren Schritte finden Sie im zugehörigen Kapitel.

4.7 Seite 243

4.8.7 Sondertage (Listenansicht)

- Drücken Sie auf die Schaltfläche „Sondertag“ und wählen ggf. einen Tag aus. Betätigen Sie den Button mit der gewünschten Funktion.



Die Beschreibung der Funktion und die weiteren Schritte finden Sie im zugehörigen Kapitel.

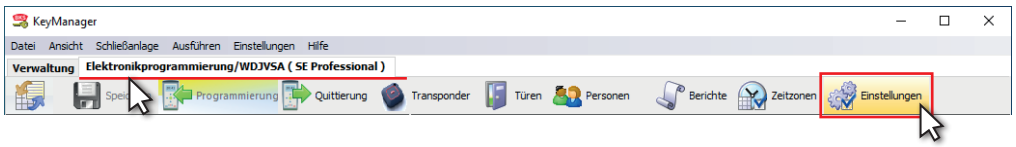
4.7.2

Seite 247

5. Einstellungen

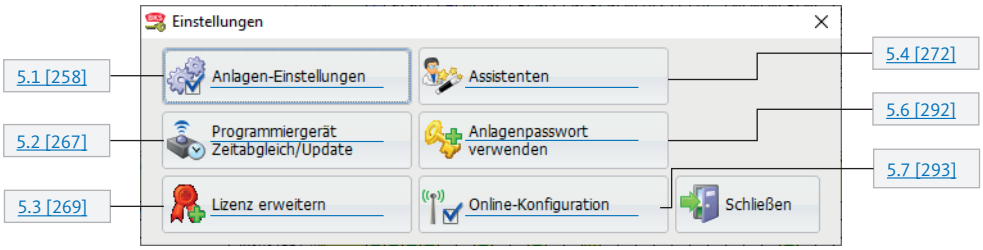
Das Menü „Einstellungen“ des Hauptmenüs bietet Ihnen die Möglichkeit, grundlegende Eigenschaften der Schließanlage bzw. Einstellungen für die Verwaltung des BKS KeyManagers einzurichten.

- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Einstellungen“.

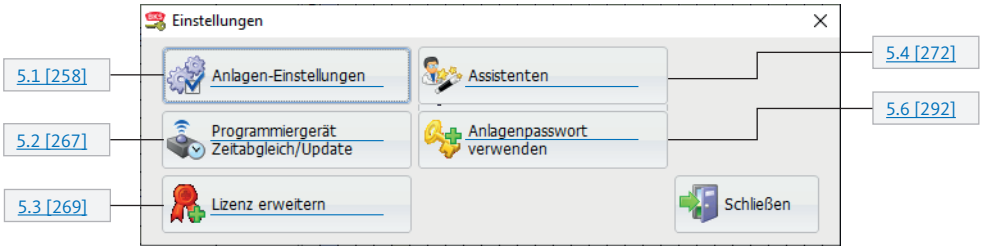


Im Menü „Einstellungen“ lassen sich die folgenden Funktionen aufrufen. Diese können je nach Typ der Schließanlage variieren.

→ Fenster „Einstellungen“ für eine Data on Transponder-Anlage (DoT) oder Online-Anlage (nonDoT).

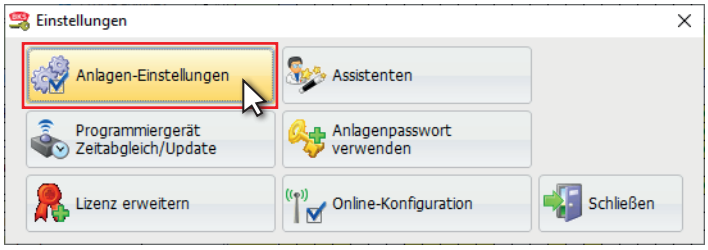


→ Fenster „Einstellungen“ für eine Offline-Anlage (nonDoT).



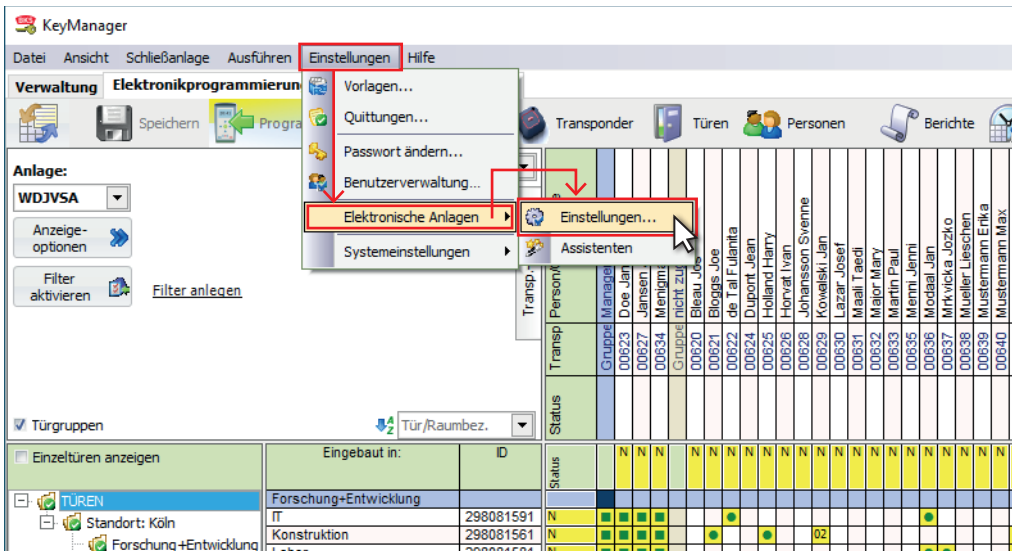
5.1 Anlagen-Einstellungen

- Drücken Sie auf den Button „Anlagen-Einstellungen“, um Änderungen in den Einstellungen der Schließanlage und des BKS KeyManagers vorzunehmen.



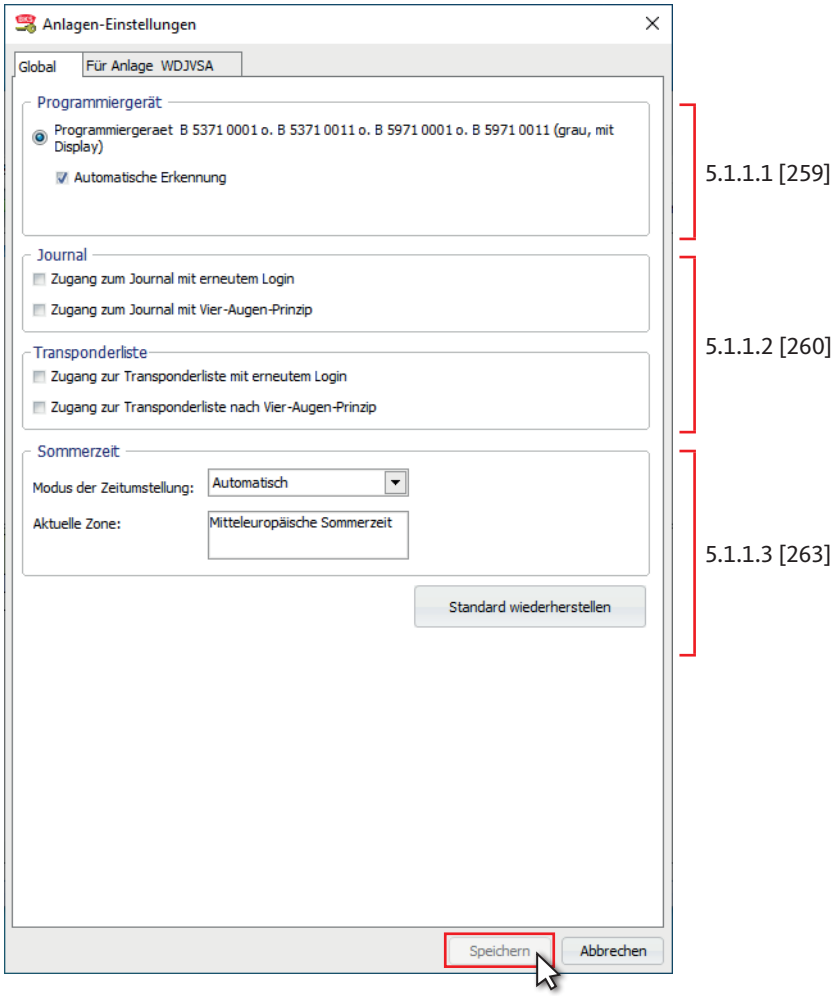
Alternativ kann das Fenster Anlagen-Einstellungen über die Menüleiste aufgerufen werden.

- Drücken Sie in der Menüleiste auf „Einstellungen“, wählen das Dropdown-Menü „Elektronische Anlagen“ aus und drücken auf den Menüpunkt „Einstellungen ...“.



5.1.1 Globale Einstellungen der Anlage

Im Register „Global“ des Fensters „Anlagen-Einstellungen“ können verschiedene Einstellungen zu den Komponenten durchgeführt werden. Eine ausführlichere Beschreibung zur jeweiligen Einstellung finden Sie in dem rechts daneben aufgeführten Kapitel.



Der Button „Standard wiederherstellen“ setzt alle Einstellungen wieder auf die Werkseinstellung zurück.

- Drücken Sie auf den Button „Speichern“, um die Bearbeitung zu beenden.

5.1.1.1 Programmiergerät

Aktivieren Sie die Checkbox entsprechend dem von Ihnen verwendeten Programmiergerät.

- Auswahl für das *graue* Programmiergerät: B 5971 0001 oder B 5971 0011.
  - Datenübertragung über USB und Direktanschluss am Computer.
  - Dialog zur SD-Kartenverwaltung ist bei Auswahl dieses Geräts nicht mehr sichtbar.

5.1.1.2 Sicherheitsstufen beim Zugriff auf Ereignisjournal und Transponderliste

Der Zugriff auf die Berichte Ereignisjournal und Transponderliste ist nur für Benutzer mit entsprechendem Recht zum Lesen dieser möglich. Über zwei Sicherheitsstufen können weitere Einschränkungen zum Zugang erfolgen.

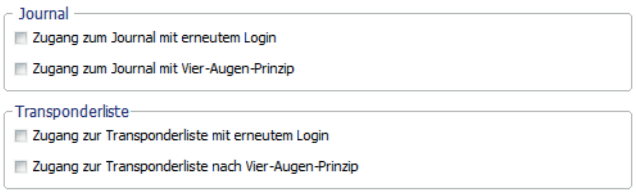
Die erste Sicherheitsstufe ermöglicht nur einen Zugriff auf diese Berichte nachdem, sich ein berechtigter Benutzer erneut mit Benutzernamen und Passwort einloggt hat. In der zweiten Sicherheitsstufe muss sich noch zusätzlich ein weiterer Benutzer mit Berechtigung anmelden, um den Zugriff freizuschalten.

Die Berechtigungen der Benutzer wie im Kapitel 6 [339] beschrieben zu vergeben.

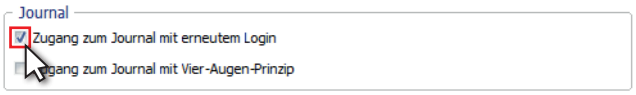
- Aktivieren Sie die jeweiligen Checkboxen.

Folgende Sicherheitsstufen sind nach Ihren Einstellungen möglich.

➔ Uneingeschränkter Zugriff auf die Berichte.
Wird keine Checkbox aktiviert, können berechtigte Benutzer ohne eine weitere Authentifizierung die Berichte einsehen.



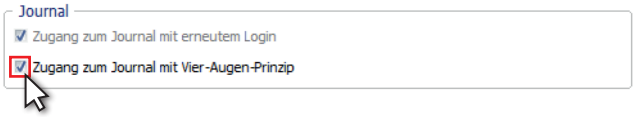
➔ Zugriff auf das Ereignisjournal mit aktiviertem erneutem Login.
Wird diese Checkbox aktiviert, ist der Zugriff auf das Ereignisjournal nur noch möglich, wenn sich ein berechtigter Benutzer durch seine Zugangskennung und Passwort authentifiziert.



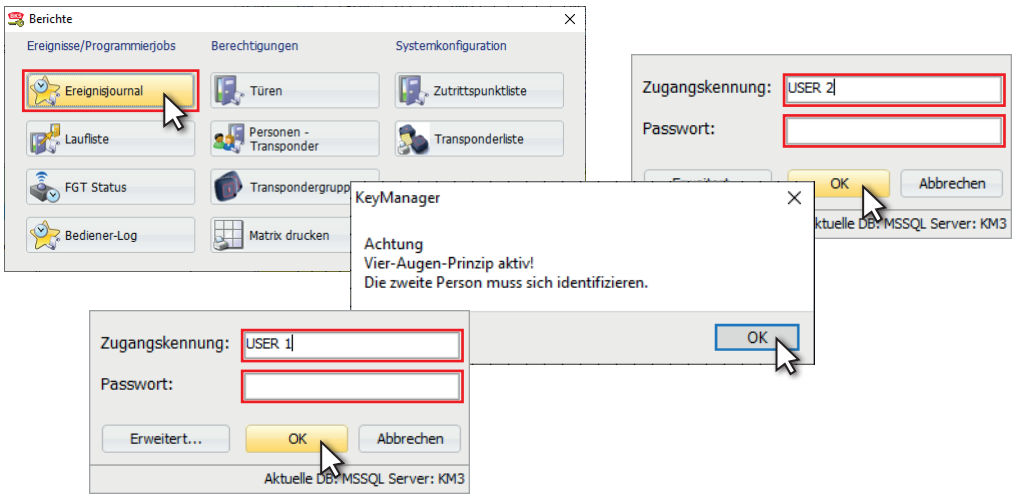
Nach dem Speichern der Einstellungen werden Sie beim Öffnen des Ereignisjournals aufgefordert, sich mit Benutzernamen und Passwort einzuloggen. Erst nach erfolgreicher Anmeldung wird der Zugriff auf das Ereignisjournal gewährt.

➔ **Zugriff auf das Ereignisjournal mit aktiviertem 4 Augen Prinzip.**
Wird diese Checkbox aktiviert, ist der Zugriff auf das Ereignisjournal nur noch möglich, wenn sich zwei berechtigte Benutzer durch ihre Zugangskennung und Passwort authentifizieren.

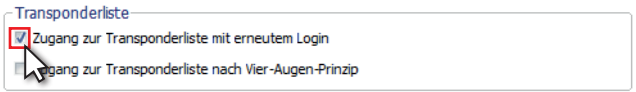
Beide Benutzer müssen im BKS KeyManager für die Transaktion „Ereignisjournal“ berechtigt worden sein. Diese Berechtigung ist über die Benutzerverwaltung des BKS KeyManagers zu gewähren.



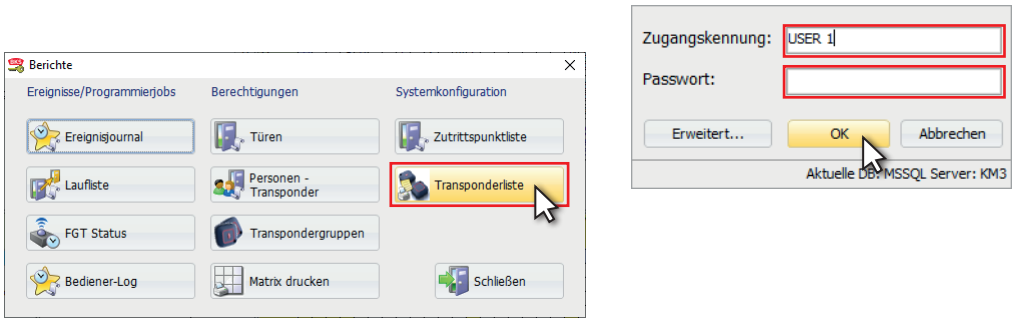
Nach dem Speichern der Einstellungen werden diese zwei Benutzer beim Öffnen der Ereignisjournals aufgefordert, sich mit Benutzernamen und Passwort einzuloggen. Erst nach beiden erfolgreichen Anmeldungen wird der Zugriff auf das Ereignisjournal gewährt.



➔ **Zugriff auf die Transponderliste mit aktiviertem erneutem Login.**
Wird diese Checkbox aktiviert, ist der Zugriff auf die Transponderliste nur noch möglich, wenn sich ein berechtigter Benutzer durch seine Zugangskennung und Passwort authentifiziert. Die Transponderliste wird nur bei einer DoT-Anlage angezeigt.

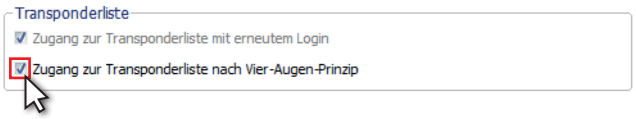


Nach dem Speichern der Einstellungen werden Sie beim Öffnen der Transponderliste aufgefordert, sich mit Benutzernamen und Passwort einzuloggen. Erst nach erfolgreicher Anmeldung wird der Zugriff auf die Transponderliste gewährt.

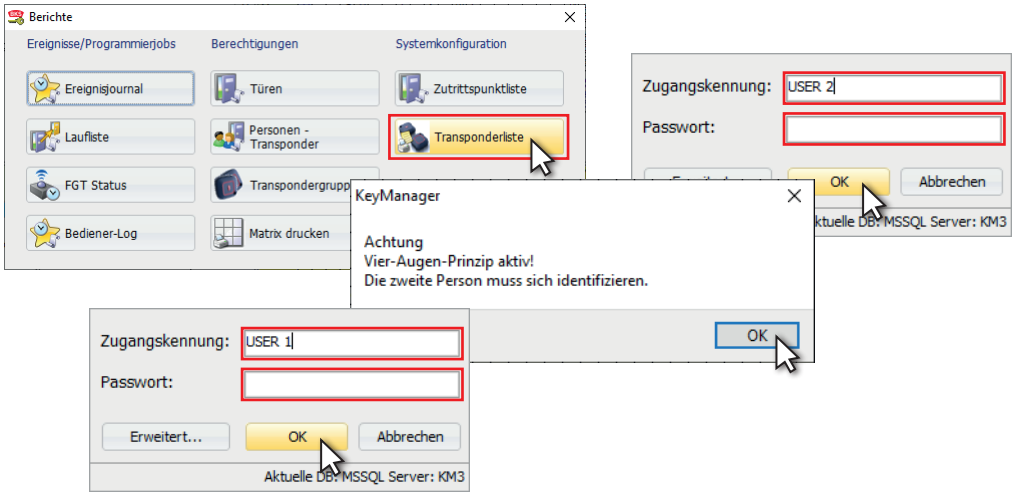


➔ Zugriff auf die Transponderliste mit aktiviertem 4 Augen Prinzip.
Wird diese Checkbox aktiviert, ist der Zugriff auf die Transponderliste nur noch möglich, wenn sich zwei berechtigte Benutzer durch ihre Zugangskennung und Passwort authentifizieren.

Beide Benutzer müssen im BKS KeyManager für die Transaktion „Ereignisjournal“ berechtigt worden sein. Diese Berechtigung ist über die Benutzerverwaltung des BKS KeyManagers zu gewähren.



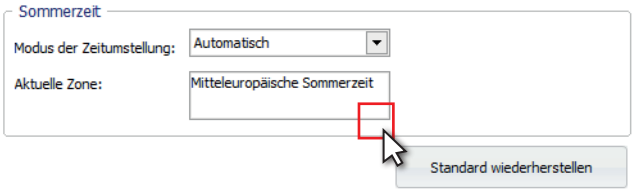
Nach dem Speichern der Einstellungen werden diese zwei Benutzer beim Öffnen der Transponderliste aufgefordert, sich mit Benutzernamen und Passwort einzuloggen. Erst nach beiden erfolgreichen Anmeldungen wird der Zugriff auf die Transponderliste gewährt.



5.1.1.3 Sommerzeit

Die Umstellung von Winterzeit auf Sommerzeit und zurück zur Winterzeit wird über die folgenden Einstellungen vorgenommen.

HINWEIS **Wir empfehlen, den Modus der Zeitumstellung auf die Einstellung „Automatisch“ zu stellen bzw. die Einstellung beizubehalten.**

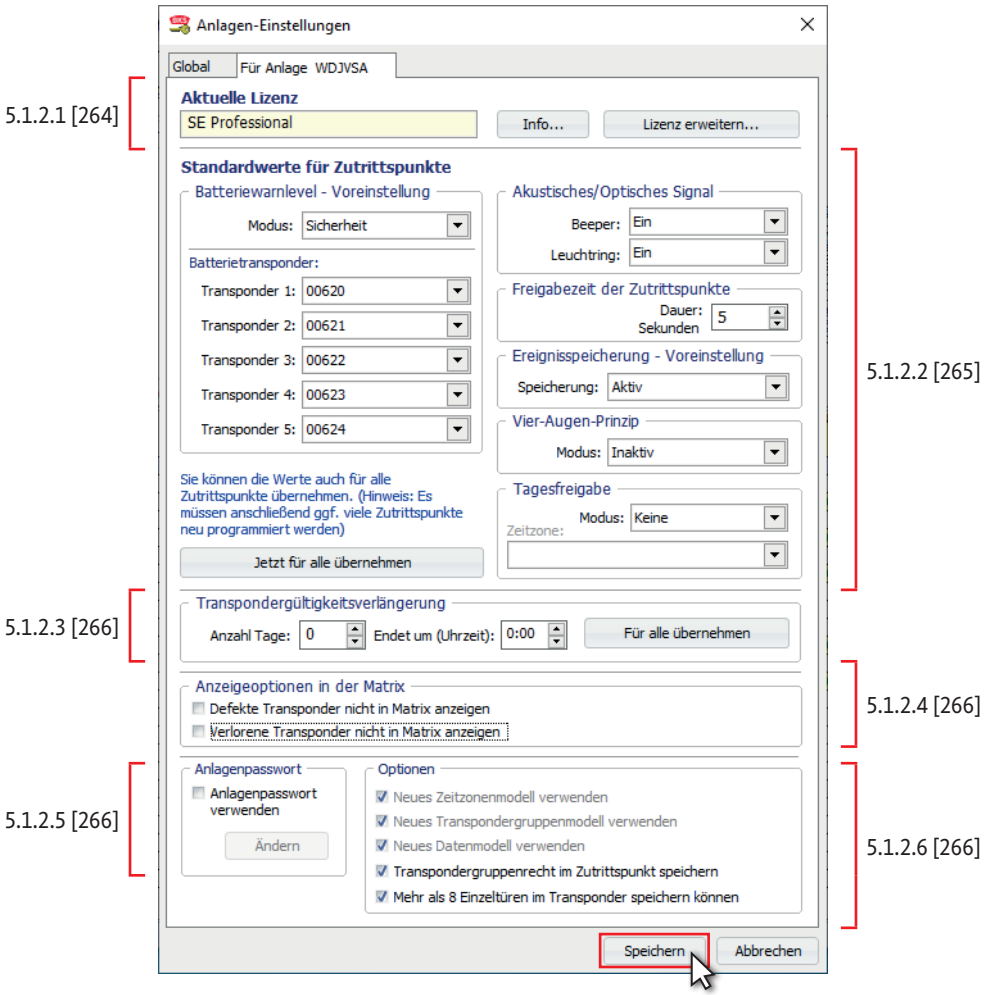


Wählen Sie im Dropdown-Menü eine der folgenden zwei Möglichkeiten für die Zeitumstellung aus.

- „Automatisch“ schaltet die Zutrittspunkte und das Programmiergerät automatisch zwischen Sommer- und Winterzeit um. Die Berechnung der Umschalttermine erfolgt nach einem internen Algorithmus im Zutrittspunkt/Programmiergerät. Die Termine werden Ihnen im oberen Teil des Fensters angezeigt.
- „Aus“ deaktiviert die automatische Umstellung auf die Sommerzeit. Es erfolgt keine Zeitumstellung. Die Zeit wird dauerhaft nach der Winterzeit angezeigt.

5.1.2 Standardeinstellungen für die ausgewählte Anlage

Im Register „Für Anlage ...“ des Fensters „Anlagen-Einstellungen“ ist es möglich, die verschiedenen Einstellungen zur ausgewählten Schließanlage (hier: WDJVSA) vorzunehmen. Eine ausführlichere Beschreibung zur jeweiligen Einstellung finden Sie in den neben der Einstellung aufgeführten Kapitel.



5.1.2.1 Aktuelle Lizenzen

Dieses Feld zeigt die aktuell verwendeten (Haupt-) Lizenz der Schließanlage an und bietet die Möglichkeit, diese zu erweitern.

- Drücken Sie auf den Button „Info“, um eine Liste mit allen in der Schließanlage geladenen Lizenzen anzuzeigen.
- Drücken Sie auf den Button „Lizenz erweitern“, um weitere Lizenzen der Schließanlage hinzuzufügen.

  → Wählen Sie die Checkbox „Lizenz laden“ und drücken auf den Button „Durchsuchen ...“, um mit dem Dateibrowser eine neue Lizenz zuladen.

  → Durch Aktivierung der Checkbox „Ich möchte meine Lizenz erweitern“, können Sie im weiteren Dialog eine Lizenz per E-Mail oder auf einer SD-Karte anfordern. Füllen Sie bitte mindestens die Felder „Persönliche Angaben“ und „Lizenz“ aus. Wählen Sie ein „Registrierungsformular“ zur Übermittlung aus.

5.1.2.2 Standardwerte für Zutrittspunkte

Batteriewarnlevel-Modus
Das Batteriewarnlevel der Zutrittspunkte arbeitet im Modus „Sicherheit“, wodurch der Zutritt je nach Batteriewarnlevel verzögert oder gesperrt wird. Nur bei den 5302 und 5303 janus-Zylindern | SE gibt es die Möglichkeit, auch in den Modus „Komfort“ zu wechseln.

Der Zutrittspunkt schaltet nach Zustand der Batterien in eins der folgenden Batteriewarnlevel.

- **Warnlevel 1** wird bei sinkender Kapazität zum Ende der Lebensdauer aktiviert. Dadurch wird nach Berechtigung des Zutritts durch Präsentieren des Transponders eine Zeitverzögerung von 10 Sekunden bei jedem Zutritt gestartet.
- **Warnlevel 2** wird kurz vor Lebensende der Batterie aktiviert und sperrt den Zutrittspunkt für alle Transponder.

Das Batteriewarnlevel 2 wird nur selten erreicht, weil um diesen Level zu erreichen, vorher einige tausend Personen im Warnlevel 1 eine Zutrittsverzögerung von 10 Sekunden je Zutritt in Kauf nehmen mussten, wodurch die Batterie erfahrungsgemäß kurzfristig gewechselt wird.
Bei Zutrittspunkten im Warnlevel 2 muss mit dem Programmiergerät das Batteriewarnlevel zurückgesetzt werden, um die Transponder für den Austausch der Batterien zum Zutritt zu berechtigen wenn die Tür verschlossen ist.

Der Modus des Batteriewarnlevels kann nur beim janus-Zylinder | SE über das Dropdown-Menü gewechselt werden.

- Modus „Sicherheit“ sperrt den Zutritt im Batteriewarnlevel 2.
- Modus „Komfort“ ermöglicht einen Zutritt in Batteriewarnlevel 2 mit dem zum janus-Zylindern | SE passenden mechanischen Schlüssel.

Batterietransponder
In aktuellen Schließanlagen wird das Batteriewarnlevel mit dem Programmiergerät zurückgesetzt. Bei Altanlagen werden automatisch die ersten fünf Transponder als Batterietransponder festgelegt, welche das Batteriewarnlevel der Zutrittspunkte zurücksetzen können.

- In den Dropdown-Menüs können Sie auch andere Transponder auswählen.

Akustisches/optisches Signal
Die Zutrittspunkte können bei berechtigtem oder nicht berechtigtem Zutrittsversuch diesen je nach Bauart akustisch/optisch signalisieren.

- Im Dropdown-Menü können Sie den Beeper/Leuchtring ein- oder ausschalten.

Ereignisspeicherung – Voreinstellung
- „Aktiv“ – alle Zutrittsereignisse werden im Zutrittspunkt gespeichert.
- „Aktiv ohne ID“ – alle Zutrittsereignisse werden ohne Transponder-IDs gespeichert.
- „Inaktiv“ – es werden keine Zutrittsereignisse gespeichert.

Vier-Augen-Prinzip

- „Aktiv“ – zwei berechtigte Transponder müssen kurz hintereinander buchen, um einen Zutritt zu erhalten.
- „Inaktiv“ – ein berechtigter Transponder erhält (alleine) Zutritt.

Drücken Sie auf den Button „Jetzt für alle übernehmen“, um die Einstellungen für alle Zutrittspunkte der Anlage zu festzulegen.

HINWEIS **Eine Änderung in den Einstellungen hat zur Folge, dass für alle betroffenen Zutrittspunkte ein Programmierjob erzeugt wird.**

5.1.2.3 Gültigkeitsverlängerung der Transponder

Die relative Gültigkeit für alle Transponder wird aktiviert durch setzen einer Frist und Programmierung. Die Transponder behalten dadurch solange ihre Gültigkeit, wie sie innerhalb der Frist durch Präsentation am Freigabeterminal die Laufzeit neu starten und so die Gültigkeit verlängern. Bei Ablauf der Frist verlieren die Transponder die Zutrittsrechte. Die Frist muss am Freigabeterminal durch Einbuchen reaktiviert werden.

- Geben Sie die Frist der Verlängerung und drücken auf den Button „Für alle übernehmen“.

5.1.2.4 Anzeigeoptionen in der Matrix

- Aktivieren Sie die jeweilige Checkbox, damit defekte oder verlorene Transponder in der Matrix angezeigt werden.

5.1.2.5 Anlagenpasswort verwenden

Das Anlagenpasswort dient zum Schutz vor missbräuchliche Programmierung der Zutrittspunkte. Ist das Anlagenpasswort aktiviert worden, werden Sie vor jeder Programmierung der Zutrittspunkte zur Eingabe des Passworts aufgefordert. Eine Programmierung ist nur mit gültigem Passwort möglich.

- Aktivieren Sie die Checkbox „Anlagenpasswort verwenden“. Geben Sie im weiteren Dialog das aktuelle und zweimal neue Passwort ein.
- Drücken auf den Button „Speichern“ und „Ändern“. Das Anlagenpasswort ist aktiviert.

5.1.2.6 Optionen

Die Checkboxen geben Auskunft über das verwendete Daten- und Zeitmodell der Schließanlage. Um die nachfolgenden Funktionen speziell für Altanlagen nutzbar zu machen, kann über die Einstellmöglichkeiten die Kompatibilität in Abhängigkeit der verwendeten Version der Hard- und Firmware angepasst werden, um z. B. die Nutzung älterer Transponder oder Zutrittspunkte zu ermöglichen.

Neues Zeitzonenmodell verwenden.
Ab der Version 4 des BKS KeyManagers haben die Zeitzonen standardmäßig eine Auflösung von 15 Minuten. In früheren Versionen hatten die Zeitzonen eine Auflösung von 5 Minuten. Ist die Checkbox aktiviert, wird das neue Zeitzonenmodell verwendet.

Neue Transpondergruppen verwenden.
Ab der Version 4 des BKS KeyManagers kann ein Transponder nur einer Transpondergruppe zugeordnet sein. In früheren Versionen konnte ein Transponder mehreren Gruppen angehören. Ist die Checkbox aktiviert, wird das neue Transpondergruppenmodell verwendet.

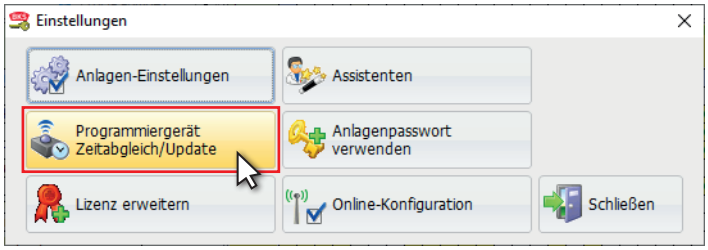
Neues Datenmodell verwenden.
Ab der Version 4 des BKS KeyManagers können Zutrittspunkte und Transponder im neuen Datenmodell verwaltet werden.

Transpondergruppen-Berechtigung im Zutrittspunkt speichern.
In einer DoT-Schließanlage werden die Rechte der Transpondergruppe standardmäßig als Transpondergruppen-ID im Zutrittspunkt abgelegt. Ist die Checkbox nicht aktiviert, werden sämtliche Transpondergruppenrechte für die einzelnen Türen auf den Transponder gespeichert und nicht im Zutrittspunkt. Die Zutrittspunkte müssen dadurch seltener programmiert werden. Die Transponder sind jedoch jetzt häufiger und mit einer längeren Programmierzeit zu programmieren. Voraussetzung für das Speichern der Gruppenrechte auf dem Transponder ist mindestens eine Firmware-Version 3.2 der Transponder.

Mehr als 8 Einzeltüren im Transponder speichern können.
Diese Option ist ab dem BKS KeyManager 4.2 und Transponder-Firmware 3.2 möglich. Hier werden die Berechtigungen als Tür-ID im Transponder abgelegt. Wird diese Option zusätzlich ausgewählt, lassen sich mehr als 8 Einzeltüren auf einem Transponder speichern.

5.2 Programmiergerät

■ Drücken Sie auf den Button „Programmiergerät Zeitabgleich/Update“.

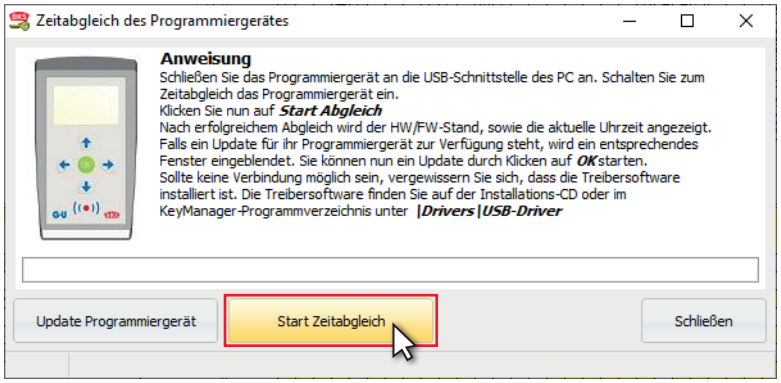


5.2.1 Zeitabgleich Programmiergerät

Diese Funktion ermöglicht einen manuellen Zeitabgleich zwischen dem Programmiergerät und Ihrem Computer. Je nach verwendeten Programmiergerät wird eins der folgenden Fenster angezeigt. Beim Programmiergerät Professional wird bei jeder Programmierung automatisch ein Zeitabgleich durchgeführt.

Dialog für Programmiergerät Professional B 5971 00x1.

■ Drücken sie auf den Button „Start Zeitabgleich“.



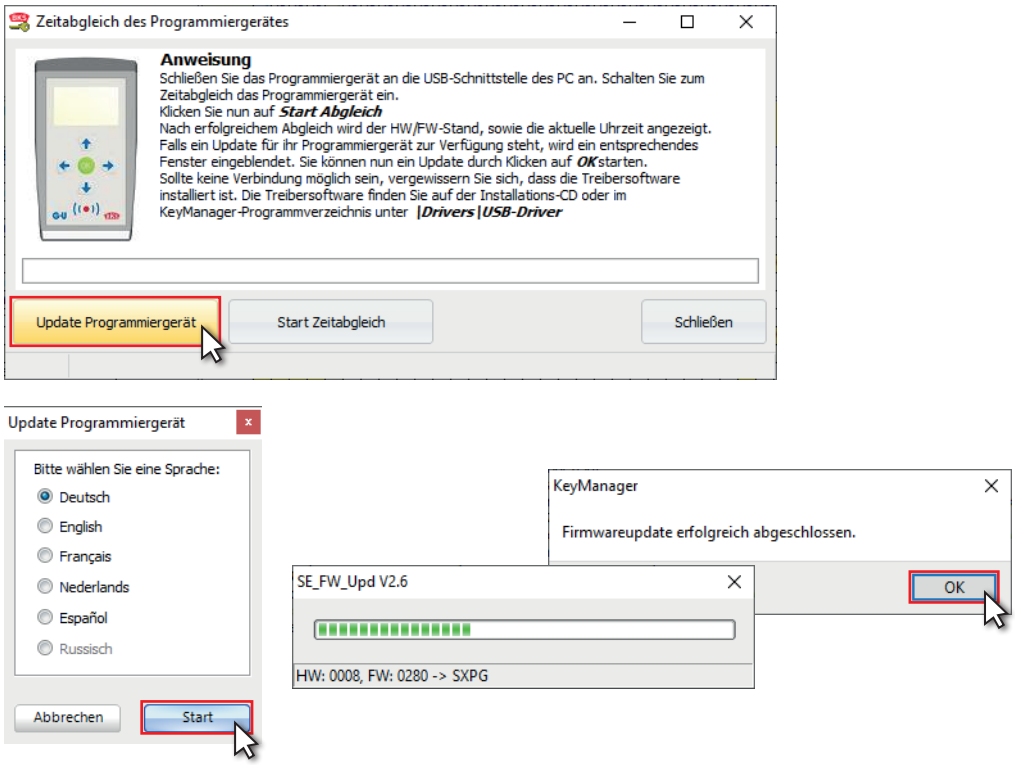
5.2.2 Update Programmiergerät

Im BKS KeyManager ist eine Update-Funktion für das Programmiergerät Professional integriert. Sollte ein Update für das Programmiergerät zur Verfügung stehen, wird automatisch nach Anschluss des Programmiergeräts an den Computer und Verbindungsanzeige im BKS KeyManager ein Dialog für das Update gestartet. Wenn z. B. nach einem fehlerhaften Update das Programmiergerät nicht angezeigt wird, kann mit dem Menü „Programmiergerät Zeitabgleich/Update“ das Update manuell gestartet werden.

Mit der aktuellsten Version des BKS KeyManagers wird Ihnen auch immer die aktuellste Software für das Programmiergerät zur Verfügung gestellt. Über das Pulldown-Menü „Hilfe“ wird unter dem Menüpunkt „Auf Online-Updates prüfen ...“ die aktuellste Version des BKS KeyManagers bereitgestellt. Während der Installation wird die neuste Software für das Programmiergerät Professional in den BKS KeyManager geladen.

- Starten Sie das Update des Programmiergeräts durch Auswahl des Buttons „Update Programmiergerät“.
- Wählen Sie die Sprache aus und beginnen mit „Start“ das Update. Mit „OK“ wird das Fenster geschlossen.

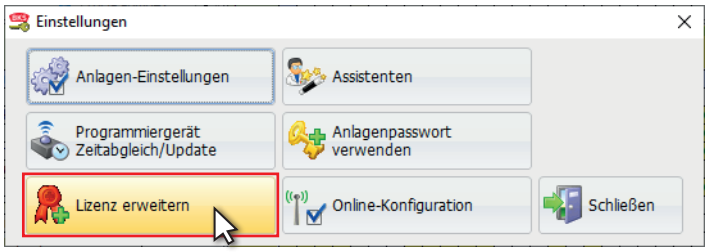
HINWEIS **Während der Übertragung des Updates darf das Programmiergerät und der BKS KeyManager nicht verwendet werden. Warten Sie ab, bis das Update erfolgreich abgeschlossen ist.**



5.3 Lizenzen erweitern

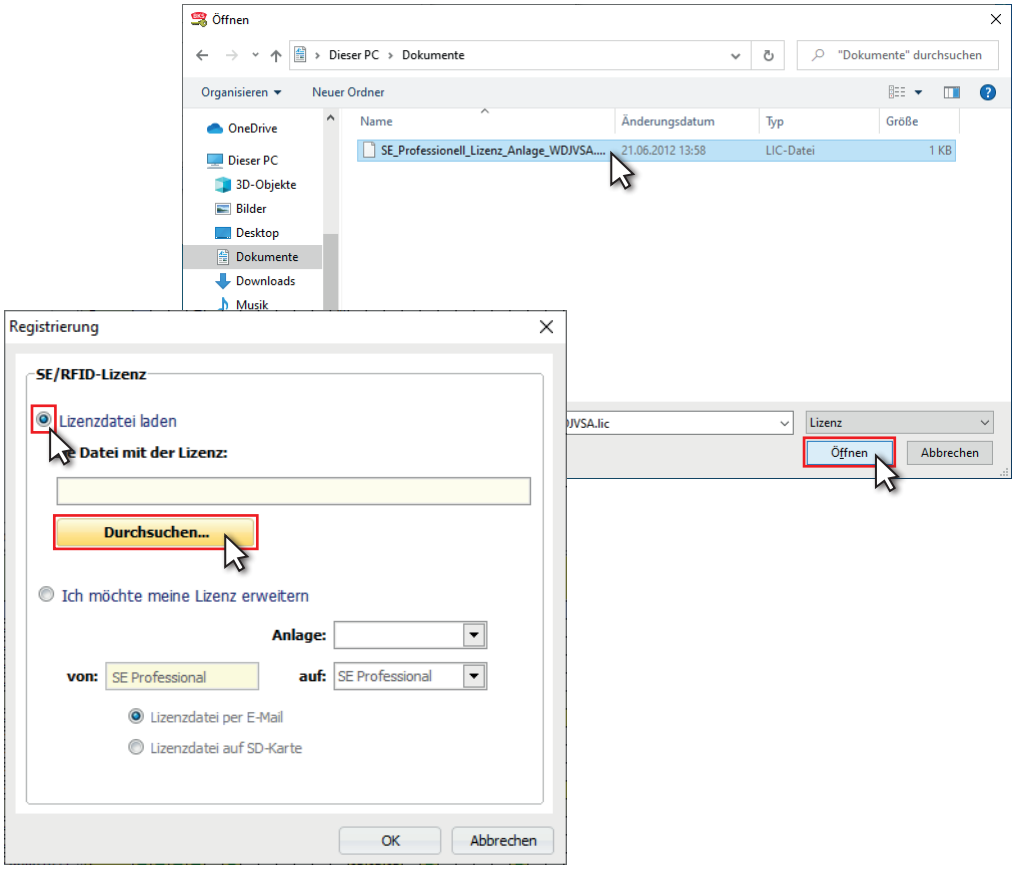
Die Funktion „Lizenz erweitern“ bietet die Möglichkeit, die Schließanlage um neue Funktionalitäten und/oder weitere Benutzer, Transponder und Zutrittspunkte durch das Hinzufügen von Lizenzen zu erweitern.

- Drücken Sie auf den Button „Lizenz erweitern“.



Im Fenster „Registrierung“ können Sie neue Lizenzen auswählen und ins System laden.

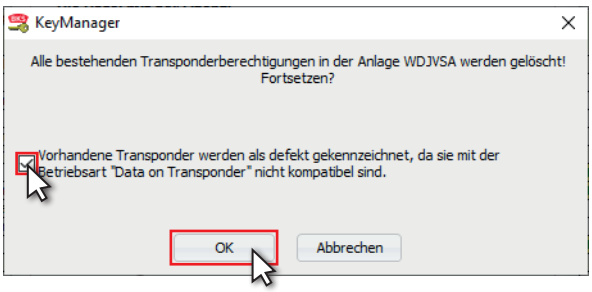
- Aktivieren Sie die Checkbox „Lizenz laden“ und drücken Sie auf den Button „Durchsuchen ...“.
- Navigieren Sie mit dem Dateibrowser zur Lizenzdatei (*.lic) und drücken auf den Button „Öffnen“. Die Lizenzdatei wird geladen und geprüft.



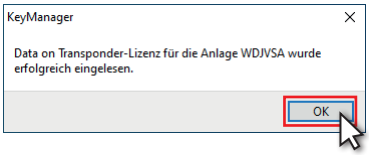
Durch das Erweitern der Lizenz kann das Berechtigungssystem der Schließanlage von Offline- oder Online-Anlage (nonDoT) auf eine Data on Transponder-Anlage (DoT) geändert werden. Allerdings ist dieses Erweitern nicht anders herum von DoT auf nonDoT möglich. Durch das Laden einer DoT-Lizenz wird in einer bestehenden nonDoT-Anlage eine Umstellung des Rechtesystems vollzogen. Dadurch werden die Zutrittsberechtigungen von den in der Anlage vorhandenen Transpondern zu den Türen unwiderruflich aus der Matrix entfernt. Die Berechtigungen und ggf. auch die Transponder müssen nach der Erweiterung neu angelegt werden.

Aus diesem Grund werden Sie beim Laden der DoT-Lizenz in einer nonDoT-Anlage extra auf diesen Umstand hingewiesen.

- Aktivieren Sie die Checkbox zur Kennzeichnung aller Transponder in der Anlage als defekt, wenn die Transponder nicht mit DoT kompatibel sind. Die deaktivierten Transponder können direkt gelöscht werden oder kompatible Transponder bei Bedarf wieder aktiviert werden.
- Deaktivieren Sie die Checkbox, wenn die Transponder in der Anlage verbleiben sollen und als DoT-Transponder verwendet werden sollen.
- Drücken sie auf den Button „OK“ zum Laden der Lizenz.



- Drücken Sie zum Fertigstellen in den beiden weiteren Fenstern auf den Button „OK“.



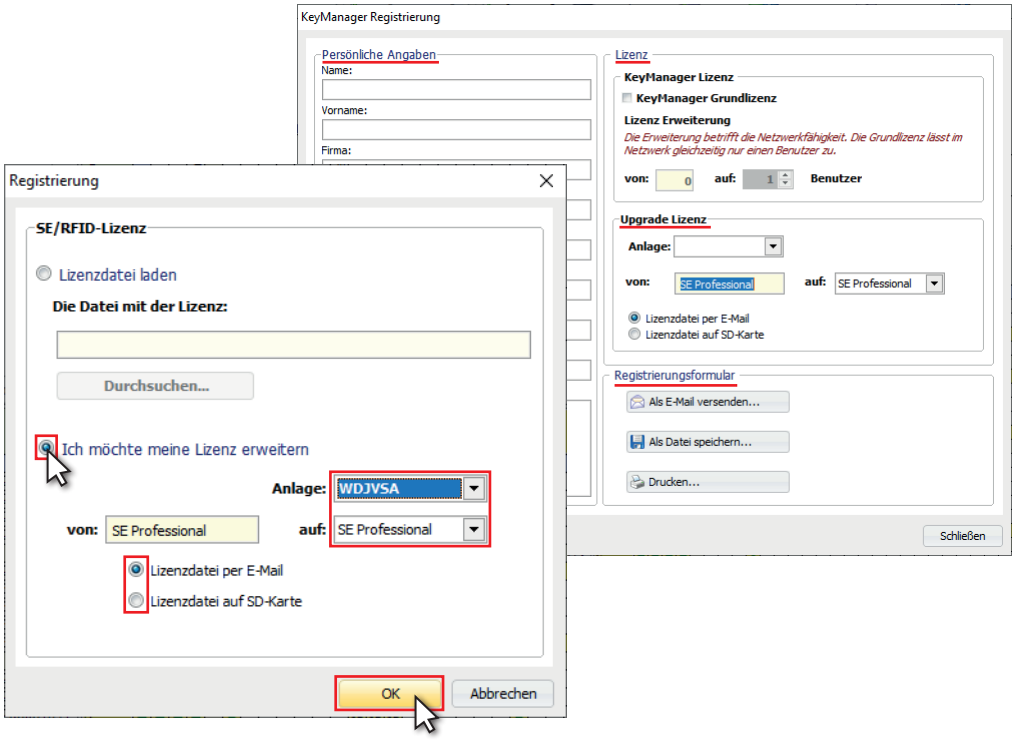
Im Fenster „Registrierung“ gibt es die Möglichkeit, eine Lizenzerweiterung anzufordern.

- Aktivieren Sie die Checkbox „Ich möchte meine Lizenz erweitern“.
- Wählen Sie in den Dropdown-Menüs Ihre Anlage und die gewünschte Lizenz aus.
- Entscheiden Sie sich über die Checkboxen für die Art der Übermittlung. Wählen Sie die Übermittlung der Lizenzdatei per E-Mail oder SD-Karte aus und drücken auf den Button „OK“.

Füllen Sie die Felder im Fenster “KeyManager Registrierung“ zu den Bereichen „Persönliche Angaben“, „Lizenz“ und „Upgrade Lizenz“ aus.

- Drücken Sie im Bereich „Registrierungsformular“ auf den entsprechenden Button für die Bestellung.

Das aus Ihren Angabe generierte Formular können Sie per E-Mail versenden, als Datei abspeichern oder ausdrucken, um es z. B. per Fax zu versenden.



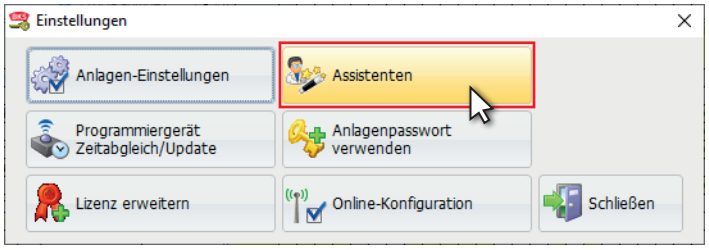
HINWEIS **Bewahren Sie Ihre Lizenz-Dateien an einem sicheren Ort auf, der für Dritte nicht zugänglich ist.**

- Drücken Sie auf den Button „Schließen“.

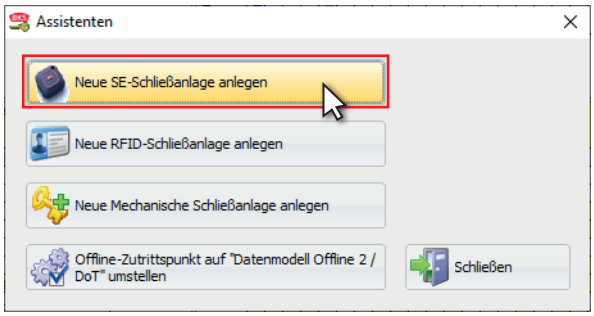
5.4 Inbetriebnahme-Assistent

Mit dem Inbetriebnahme-Assistenten richten Sie eine neue Schließanlage im BKS KeyManager ein.

- Drücken Sie auf den Button „Assistenten“ im Menü Einstellungen.

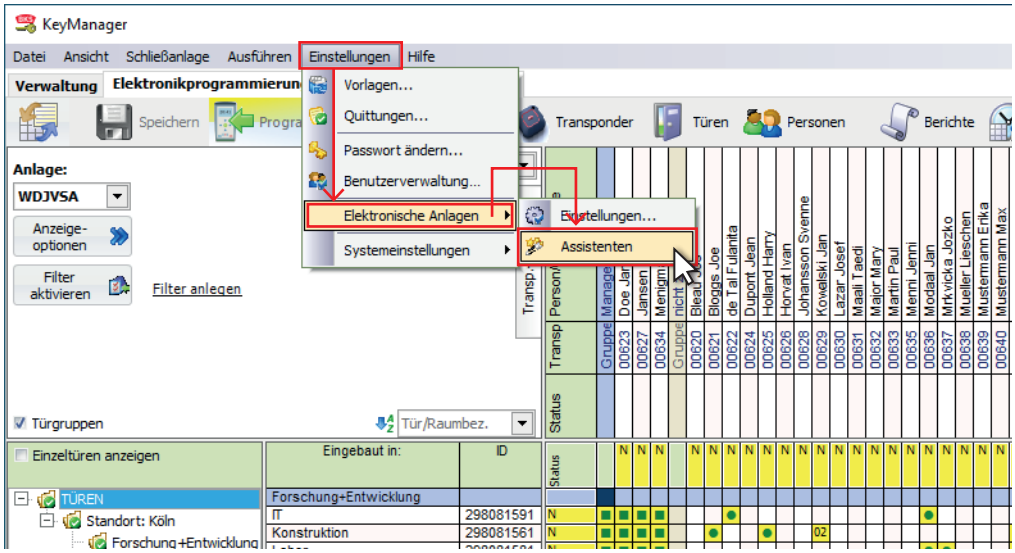


- Starten Sie den Inbetriebnahme-Assistenten manuell und drücken auf den Button „Neue SE -Schließanlage anlegen“ und beginnen mit dem Anlegen.



Alternativ kann das Fenster „Anlagen-Einstellungen“ über die Menüleiste aufgerufen werden.

- Drücken Sie in der Menüleiste auf „Einstellungen“, wählen das Dropdown-Menü „Elektronische Anlagen“ aus und drücken auf den Menüpunkt „Assistenten“.

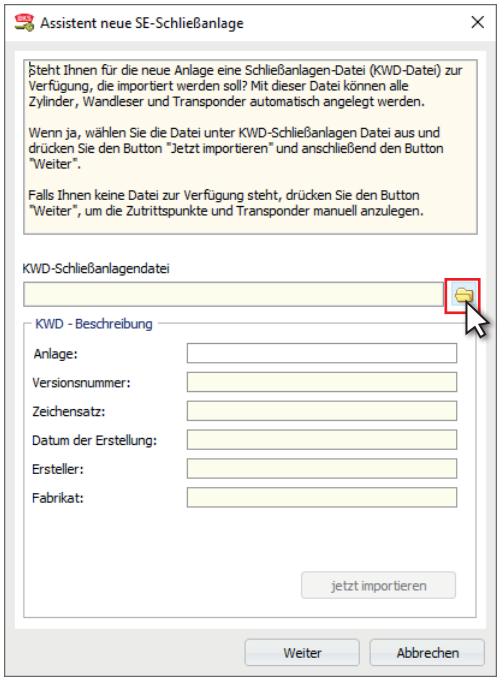


5.4.1 Schließanlage mit der Schließanlagendatei anlegen

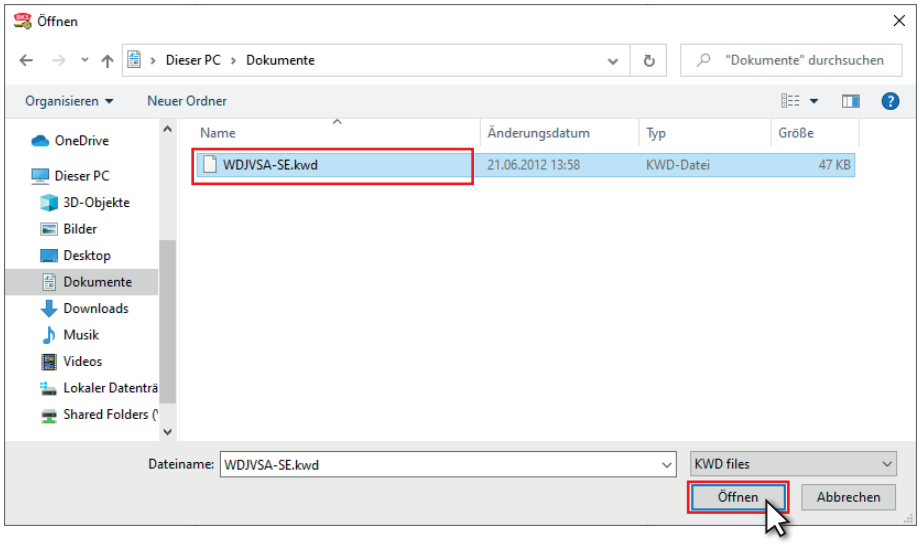
Die von Ihnen verwendeten Produkte können durch den Import der Schließanlagen-Datei der Schließanlage hinzugefügt werden. Der Inhalt dieser KWD-Datei (*.KWD) bildet die verwendeten Komponenten in der Schließanlage ab. Der BKS KeyManager legt diese durch den Import der KWD-Datei in der Schließanlage an.

Bei diesem Vorgang werden sowohl mechanische und elektromechanische Zylinder als auch alle Schlüssel und Transponder angelegt und mit Eigenschaften wie z. B. der Türbezeichnung, in die der Zylinder eingebaut ist, versehen.

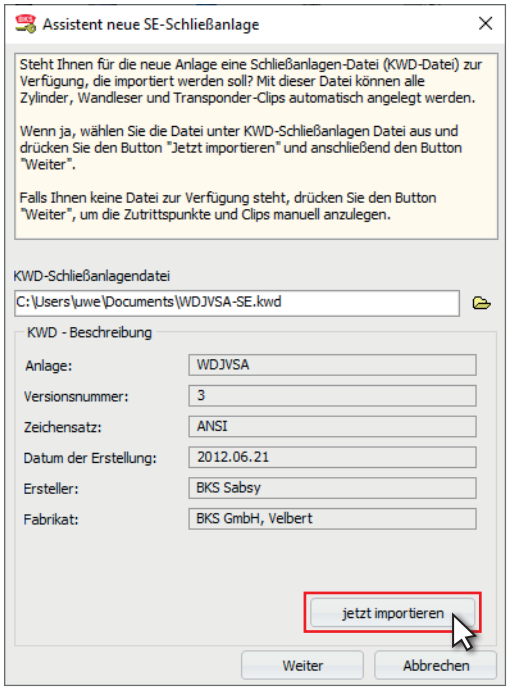
- Drücken Sie auf das Verzeichnissymbol.

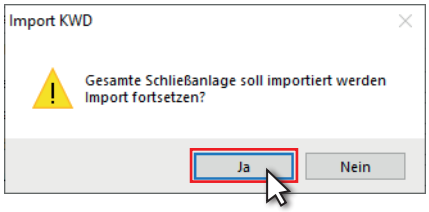


- Navigieren Sie mit dem Dateibrowser zur Schließanlagendatei (*.KWD) und drücken Sie auf den Button „Öffnen“.

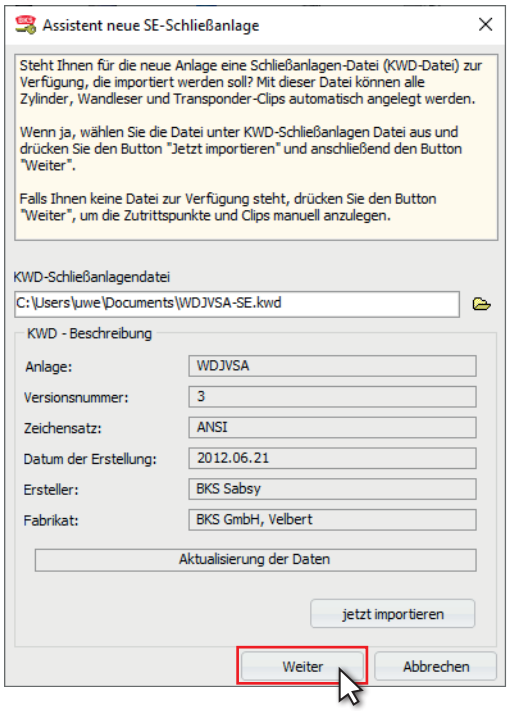


- Drücken Sie auf den Button „jetzt importieren“ und zur Bestätigung auf „Ja“.





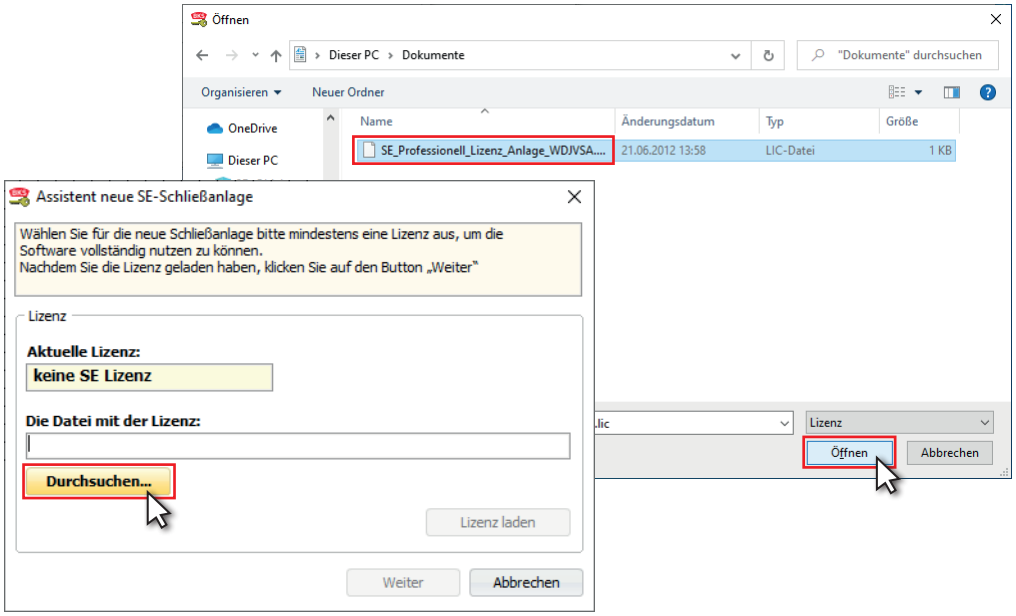
- Mit dem Button „Weiter“ gelangen Sie zum Import der Lizenzen.



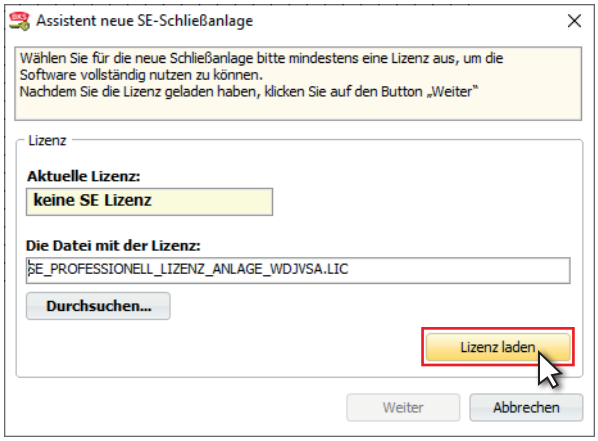
5.4.1.1 Lizenzen der Schließanlage hinzufügen

Zur Nutzung des BKS KeyManagers wird eine Lizenz benötigt. Laden Sie die Lizenzen für Ihre Schließanlage in den BKS KeyManager. Die Lizenzdateien enden mit der Bezeichnung „.lic“.

- Drücken Sie auf den Button „Durchsuchen ...“ und öffnen den Dateibrowser.
- Wählen Sie die Lizenzdatei aus und laden diese mit dem Button „Öffnen“ in den BKS KeyManager.

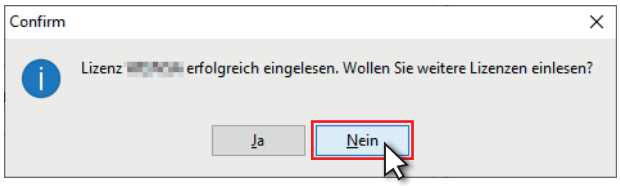


- Drücken Sie auf den Button „Lizenz laden“, um den BKS KeyManager zu lizenzieren.



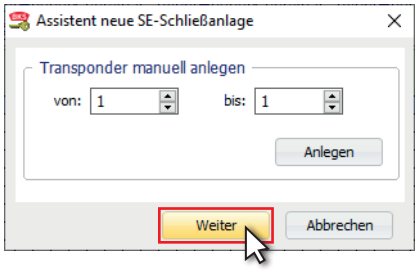
Im nächsten Fenster können Sie auswählen, ob eine weitere Lizenzierung durchgeführt werden soll.

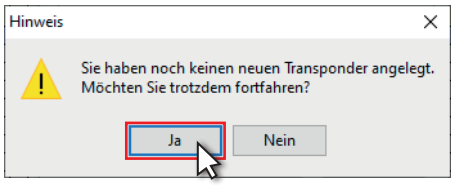
- Drücken Sie auf den Button „Ja“, um eine weitere Lizenz zu laden.
- Drücken Sie auf den Button „Nein“, um fort zu fahren.



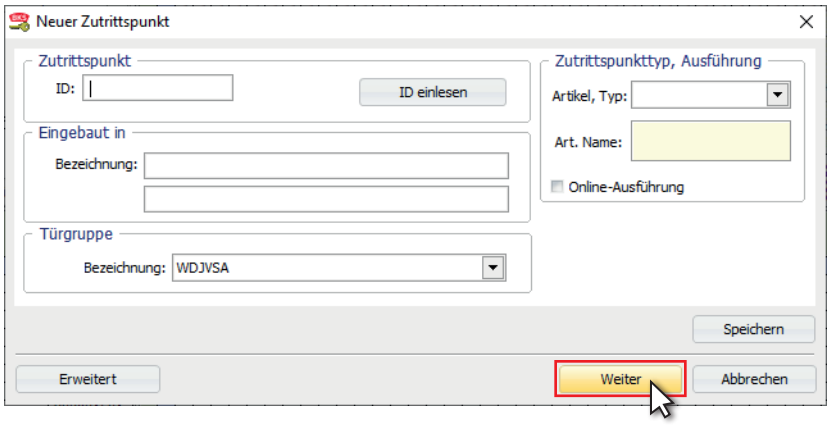
Die Transponder und Zutrittspunkte worden bereits über die KWD-Datei der Anlage hinzugefügt.

- Drücken Sie auf den Button „Weiter“ und zur Bestätigung auf „Ja“.





- Drücken Sie auf den Button „Weiter“.

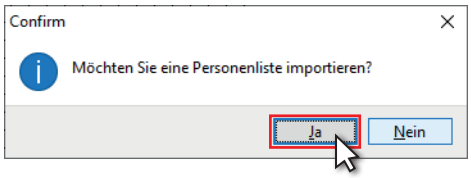


5.4.1.2 Personenlisten der Schließanlage hinzufügen

Es kann eine Personenliste für die Schließanlage geladen werden. Die Personenliste können Sie über eine CSV-Datei (*.CSV) importieren.

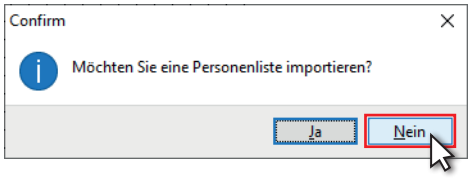
HINWEIS **Achten Sie darauf, dass die CSV-Datei auf eine „UTF-8“-Codierung eingestellt ist, weil es keinen allgemeinen Standard für das Dateiformat CSV gibt!**

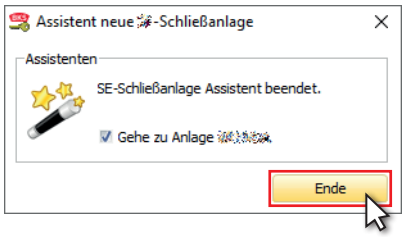
- Drücken Sie auf den Button „Ja“, um eine Personenliste zu importieren.



Sie können auch den Import zu einem späteren Zeitpunkt durchführen, wenn Ihnen keine Personenliste zur Verfügung steht. In diesem Fall ist der Assistent zu beenden.

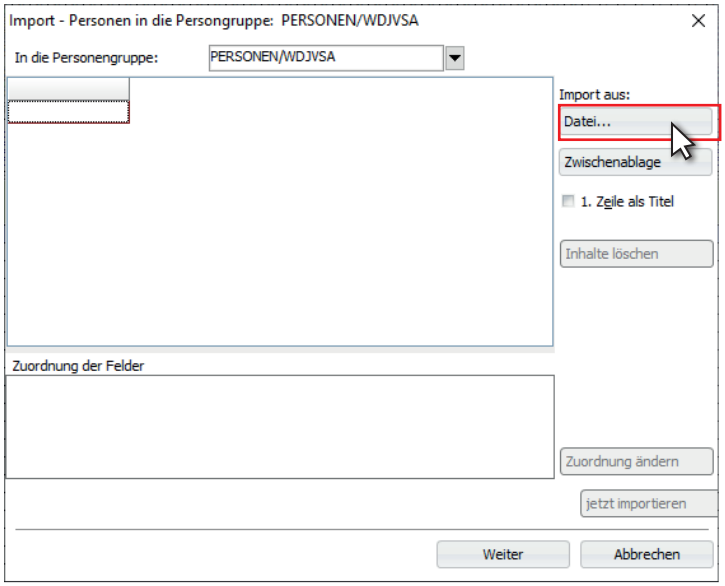
- Drücken Sie auf den Button „Nein“, um die Anlage der Schließanlage zu beenden, ohne eine Personenliste zu importieren.
- Wechseln Sie mit „Ende“ zu der neu angelegten Schließanlage.



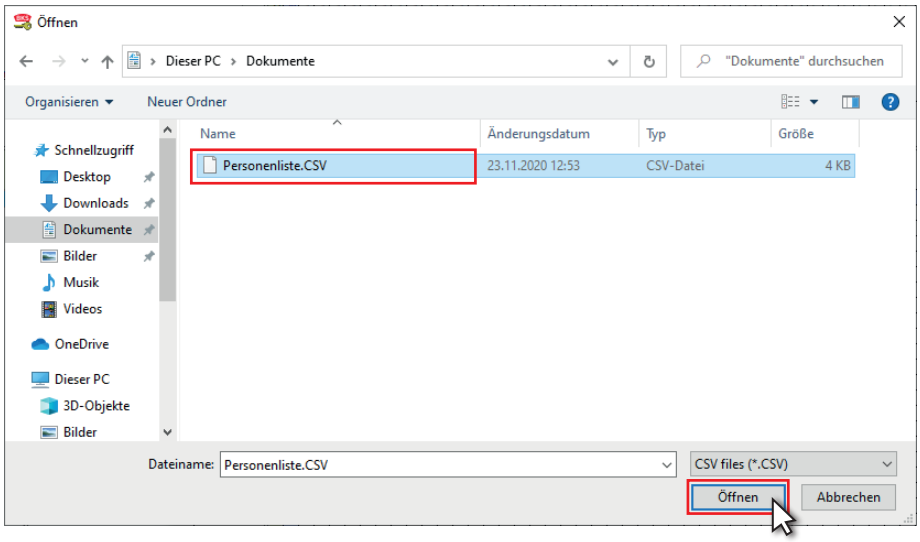


Nach der Auswahl „Personenliste importieren“ öffnet sich folgender Dialog.

- Drücken Sie auf den Button „Datei ...“ in der Spalte „Import aus:“ des Fensters.

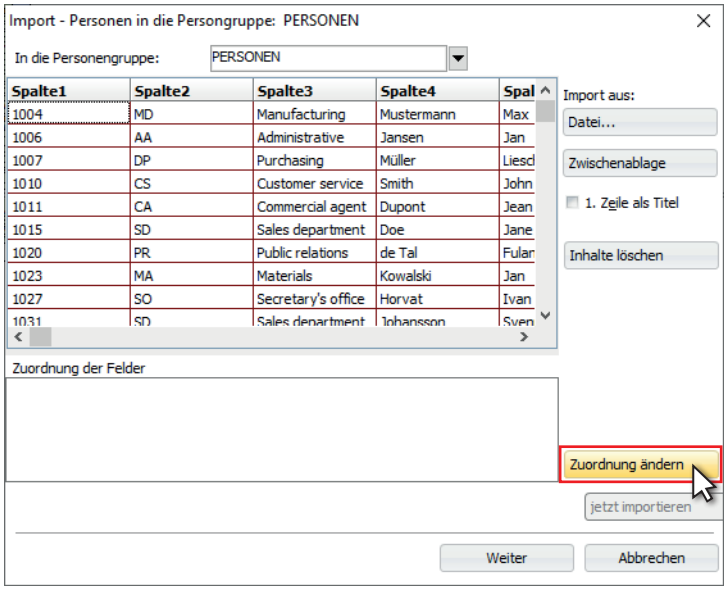


- Navigieren Sie mit dem Dateibrowser zur Personenliste. Die Datei muss im CSV-Format (*.CSV) vorliegen.
- Drücken Sie auf den Button „Öffnen“, um den Import zu starten.



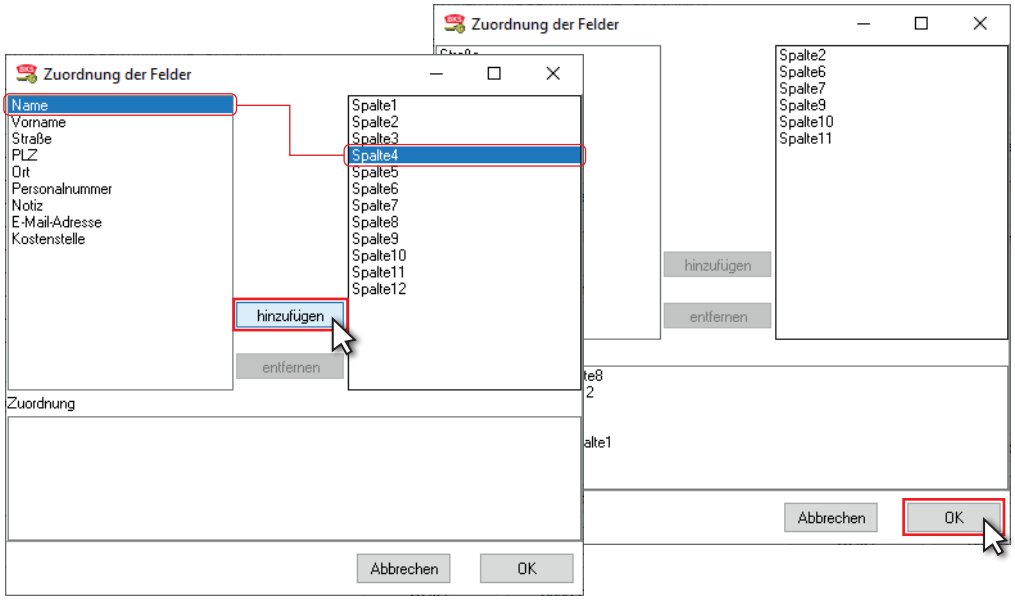
Zur Übersicht wird Ihnen die importierte Personenliste angezeigt. Die Spalten der Personenliste sind den Feldern des BKS KeyManagers zuzuweisen.

- Drücken Sie auf den Button „Zuordnung ändern“.

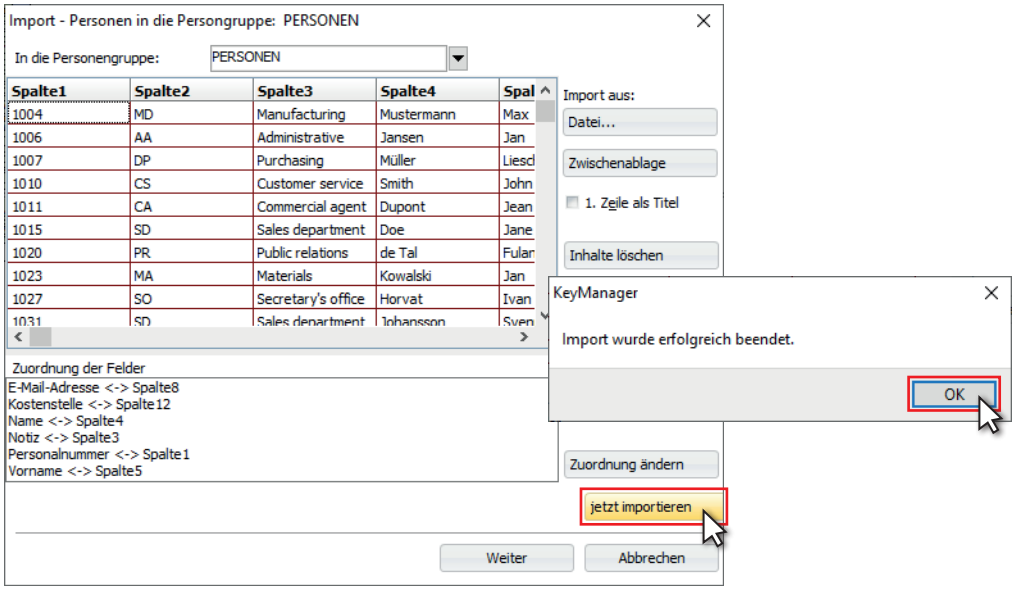


Ordnen Sie im Fenster „Zuordnung der Felder“ die personenbezogenen Daten der dazugehörigen Spalte zu. Zum Beispiel „Name“ und „Spalte 4“.

- Wählen Sie „hinzufügen“ aus und stellen Sie die Zuordnung her.
- Nach der Zuordnung der Spalten der Personenliste mit den Feldern des BKS KeyManagers fahren Sie mit „jetzt importieren“ fort.
- Beenden Sie die Zuordnung und drücken auf den Button „OK“.



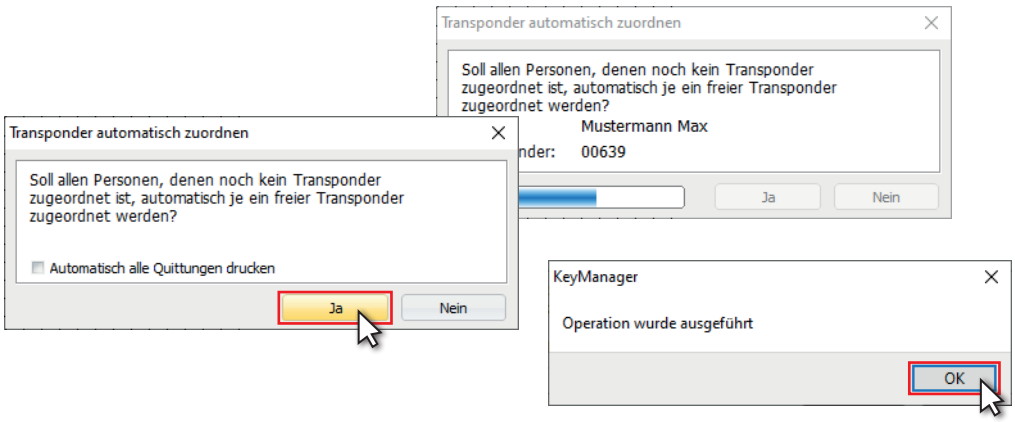
- Lesen Sie die Personenliste mit „jetzt importieren“ ein und drücken zur Bestätigung auf den Button „OK“.



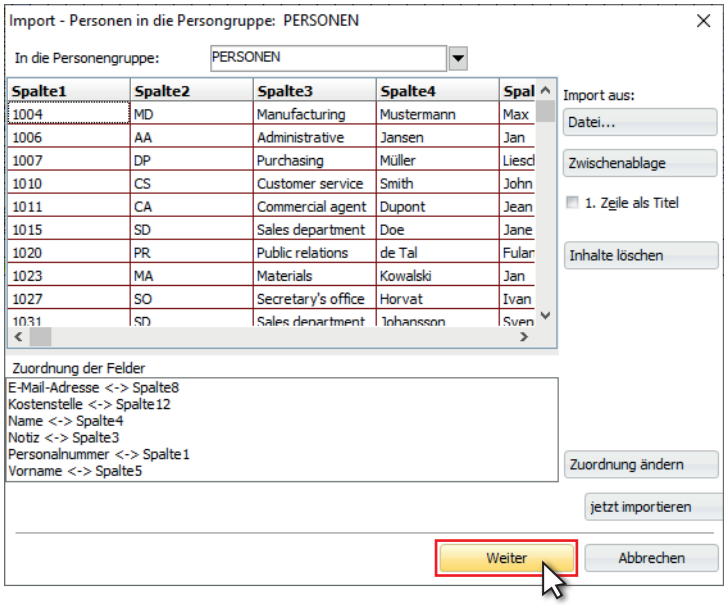
5.4.1.3 Automatische Transpondervergabe

Allen Personen, die noch keinen Transponder haben, kann automatisch ein Transponder zugeordnet werden. Bei Ausgabe von mehreren Transpondern kann dies eine große Zeitersparnis sein.

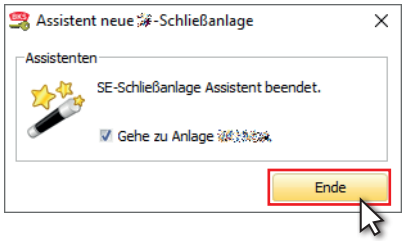
- Drücken Sie auf den Button „Ja“, um die Zuordnung zu starten.



- Drücken Sie auf den Button „Weiter“, um die Zuordnung abzuschließen.

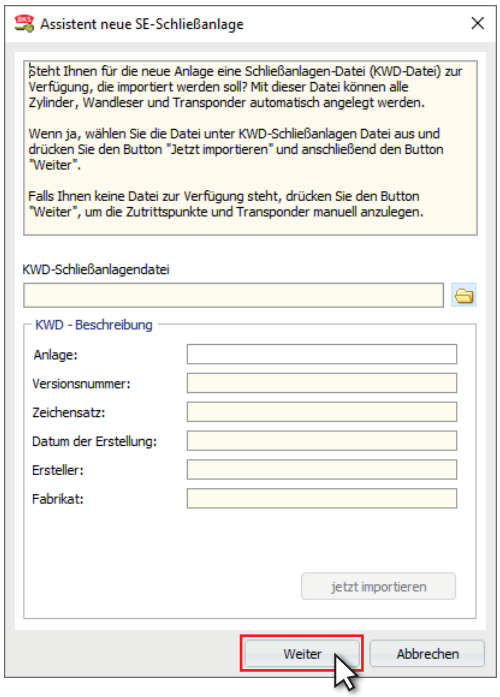


- Zum Beenden des Assistenten drücken Sie auf den Button „Ende“ und schließen Sie den Assistenten der Schließanlage ab.



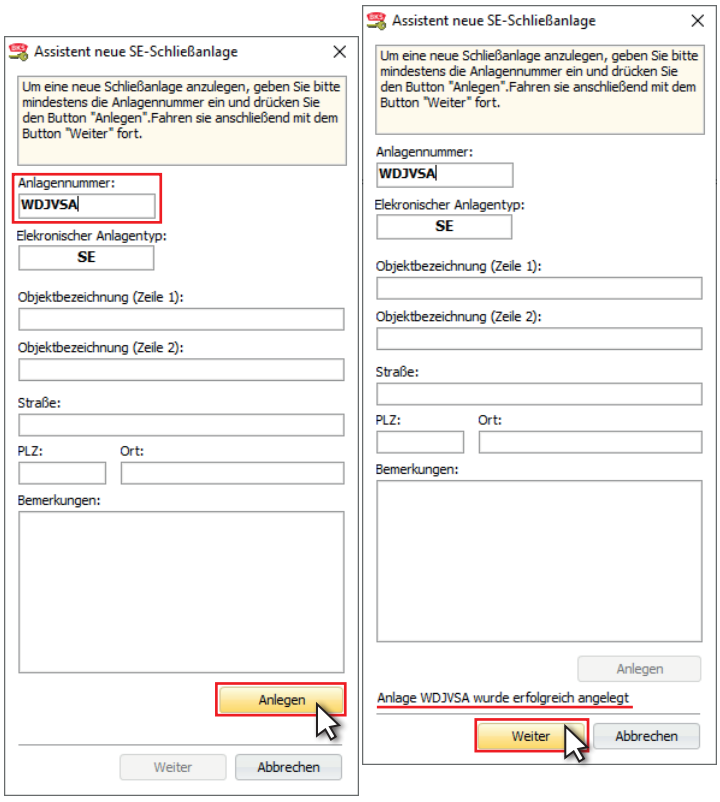
5.4.2 Schließanlage anlegen (ohne Schließanlagendatei)

Nach dem Start des Inbetriebnahme-Assistenten können die von Ihnen verwendeten Produkte auch manuell in der Schließanlage angelegt werden.



- Drücken Sie auf den Button „Weiter“.

Der Assistent startet das Fenster mit der Abfrage der erforderlichen Daten. Sie werden aufgefordert, die mechanischen und mechatronischen Komponenten der Schließanlage manuell einzugeben.



- Geben Sie die 6-stellige Anlagennummer im entsprechenden Feld ein.

Diese finden Sie auch auf Ihren Produkten z. B. Zylinder, Transponder etc. .

Die weiteren Angaben Objektbezeichnung und Adresse sind optional.

- Drücken Sie auf den Button „Anlegen“.

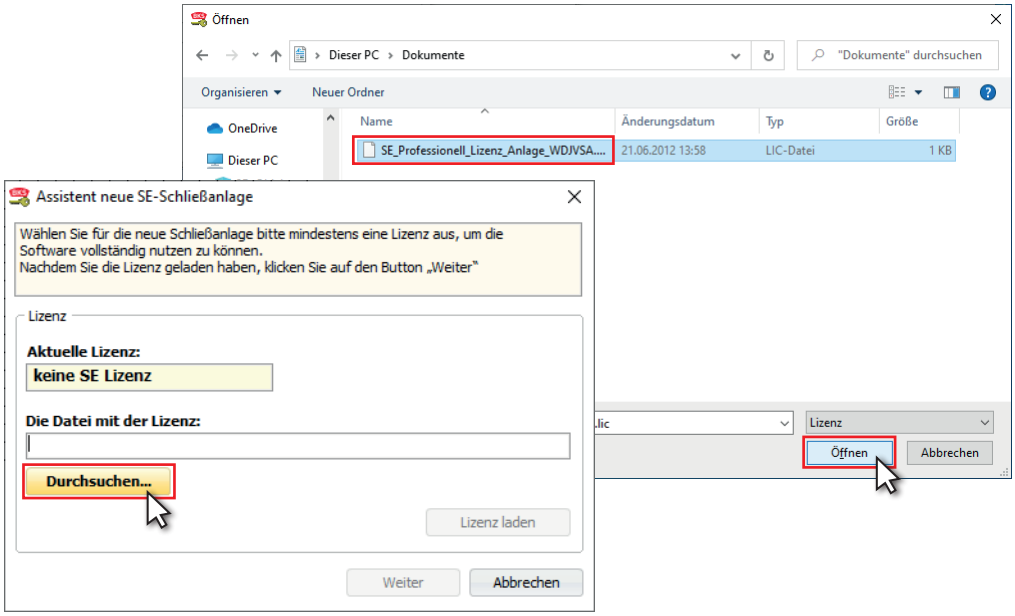
Wenn die Anlage erfolgreich angelegt wurde, erhalten Sie eine Bestätigung unterhalb des Buttons.

- Drücken Sie auf den Button „Weiter“ zum Fortfahren.

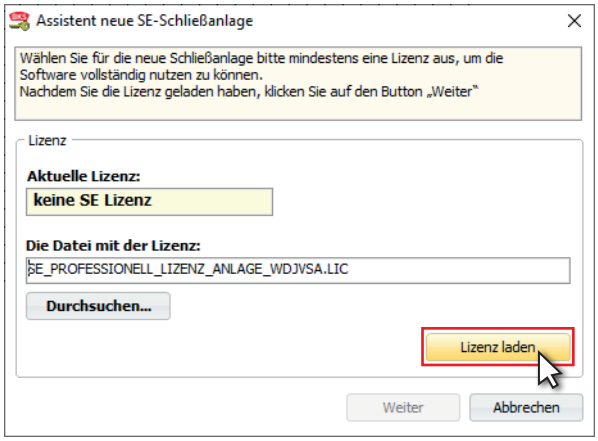
5.4.2.1 Lizenzen der Schließanlage hinzufügen

Zur Nutzung des BKS KeyManagers wird eine Lizenz benötigt. Laden Sie die Lizenzen für Ihre Schließanlage in den BKS KeyManager. Die Lizenzdateien enden mit der Bezeichnung „.lic“.

- Drücken Sie auf den Button „Durchsuchen ...“ und öffnen den Dateibrowser.
- Wählen Sie die Lizenzdatei aus und laden diese mit dem Button „Öffnen“ in den BKS KeyManager.

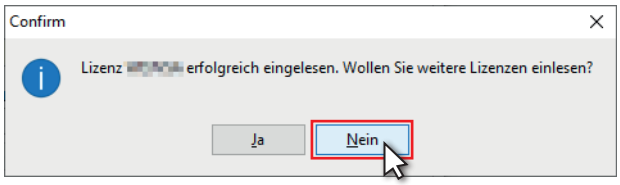


- Drücken Sie auf den Button „Lizenz laden“, um den BKS KeyManager zu lizenzieren.



Im nächsten Fenster können Sie auswählen, ob eine weitere Lizenzierung durchgeführt werden soll.

- Drücken Sie auf den Button „Ja“, um eine weitere Lizenz zu laden.
- Drücken Sie auf den Button „Nein“, um fort zu fahren.

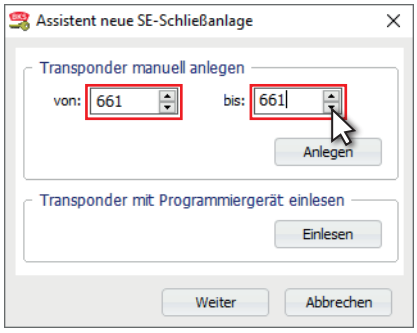


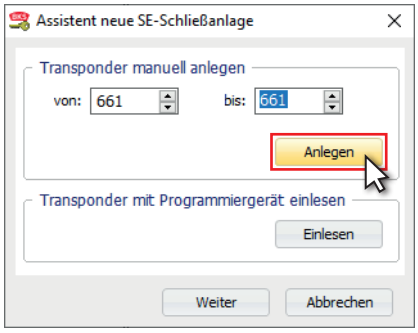
5.4.2.2 Transponder der Schließanlage hinzufügen

- Geben Sie den Bereich der Transponder-IDs ein, welche hinzugefügt werden sollen. Drücken Sie den Button „Anlegen“ zum Hinzufügen.

Als Beispiel wurde der Transponder mit der ID 661 im BKS KeyManager angelegt. Die Transponder-ID ist auf dem Transponder zu finden.

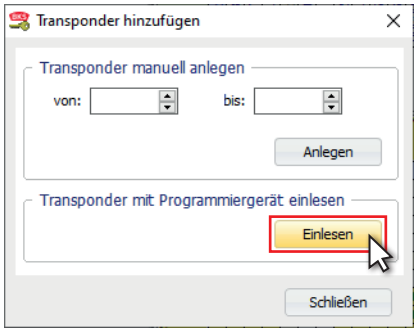
- Drücken Sie auf den Button „Anlegen“.



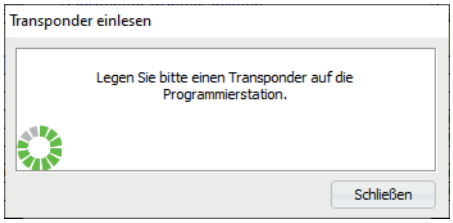


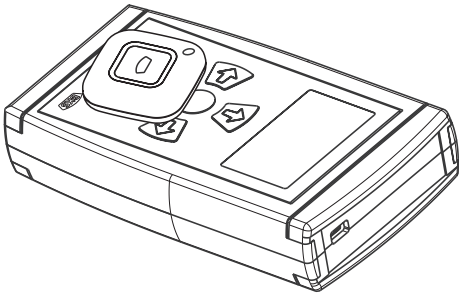
Alternativ kann der Transponder automatisch mit einem Programmiergerät eingelesen werden. Verbinden Sie das Programmiergerät und den Computer mit einem USB-Kabel und warten, bis die Verbindung bestätigt ist.

- Drücken Sie auf den Button „Einlesen“, um den Vorgang zu starten.



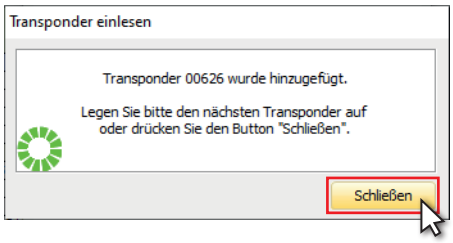
- Legen Sie den einzulesenden Transponder auf das Programmiergerät.



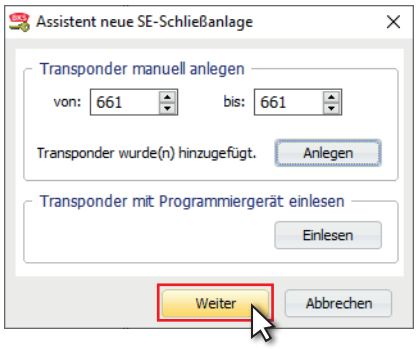


Der neue Transponder wird im BKS KeyManager angelegt.

- Legen Sie ggf. weitere Transponder auf das Programmiergerät.
- Drücken Sie auf den Button „Schließen“.



- Beenden Sie das Hinzufügen und drücken auf den Button „Schließen“.



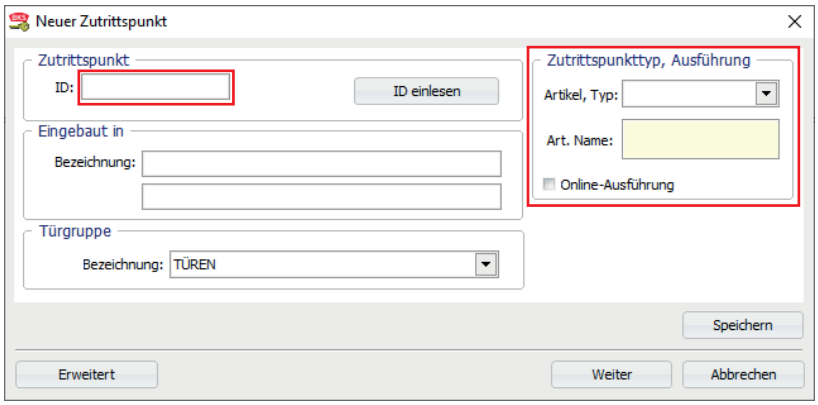
5.4.2.3 Zutrittspunkte der Schließanlage hinzufügen

Die Erstellung eines neuen Zutrittspunkts in der Schließanlage wird im folgenden Dialog beschrieben. Die Felder „ID“ mit der Seriennummer und „Bezeichnung“ („Eingebaut in“) sind Pflichtfelder und müssen ausgefüllt werden.

Das nachfolgend abgebildete minimierte Fenster bietet die Möglichkeit, die Zutrittspunkte mit Standardparametern anzulegen. Wird das erweiterte Fenster angezeigt, können Sie durch Drücken des Buttons „Minimiert“ zur minimierten Ansicht wechseln.

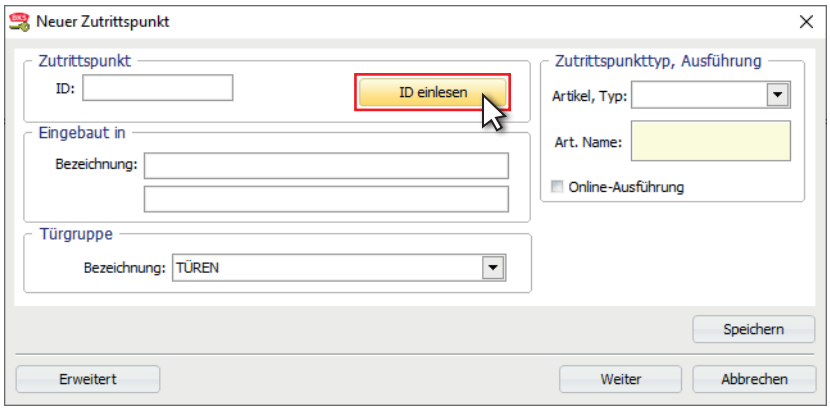
- Geben Sie die Seriennummer des neuen Geräts (z. B. Zylinder, Schloss etc.) im Feld „ID“ ein.

Beachten Sie das die Felder „Zutrittspunkttyp, Ausführung“ (auch Online-Ausführung) nur beim Anlegen editiert werden können und später gesperrt sind.

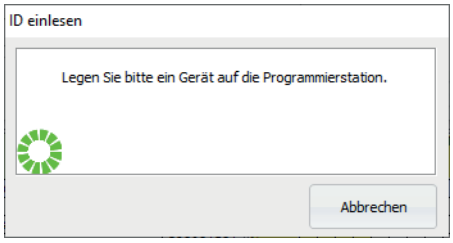


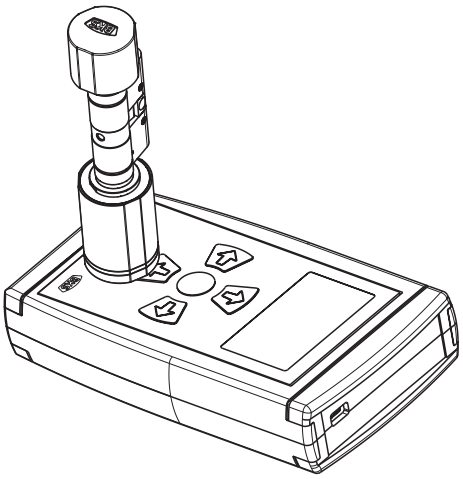
Alternativ kann der Zutrittspunkt mit einem Programmiergerät (SXPG) [B 5971 00x1] automatisch eingelesen werden. Verbinden Sie das Programmiergerät und den Computer mit einem USB-Kabel und warten, bis die Verbindung bestätigt ist.

- Drücken Sie auf den Button „ID einlesen“, um den Vorgang zu starten.



- Legen Sie den Zutrittspunkt, der eingelesen werden soll, auf das Programmiergerät.





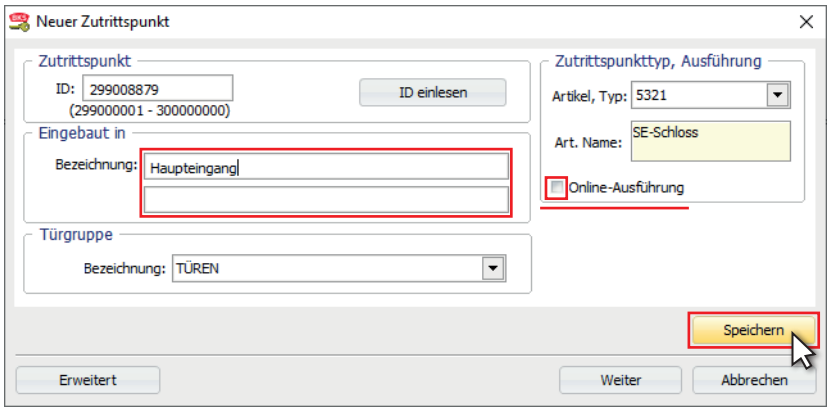
Der neue Zutrittspunkt wird angelegt.

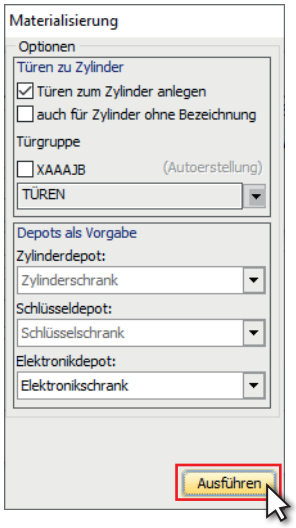
- Überprüfen Sie die Felder „Zutrittspunkttyp, Ausführung“ und ergänzen ggf. die Angaben zum Zutrittspunkt.
- Tragen Sie in das Feld „Bezeichnung“ den Namen, Einbauort, Standort etc. des Zutrittspunktes ein. Der Zutrittspunkt wird dadurch besser in der Berechtigungsmatrix auffindbar. Der Artikel-Typ wird automatisch mit der ID gepflegt.

HINWEIS

Bei onlinefähigen (Funk-) Produkten aktivieren Sie die Checkbox „Online-Ausführung“.
→ Diese Einstellung kann nur beim Anlegen editiert werden und ist später gesperrt.

- Drücken Sie auf den Button „Speichern“ zum Sichern der Eingabe.



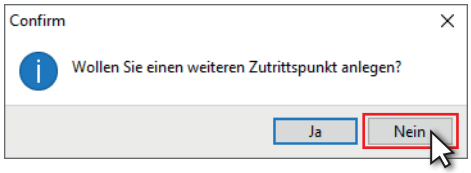


Nach dem Speichern wird der neu angelegte Zutrittspunkt materialisiert. Das ist die Zuordnung des Zutrittspunkts (z. B. Zylinder) zu einer Tür. Im System werden dadurch Türen zum Zylinder angelegt.

- Übernehmen Sie die Voreinstellung und drücken Sie „Ausführen“, um fortzufahren.

Im nächsten Fenster können Sie auswählen, ob ein weiterer Zutrittspunkt zur Schließanlage hinzugefügt werden soll.

- Drücken Sie auf den Button „Ja“, um einen weiteren Zutrittspunkt anzulegen.
- Drücken Sie auf den Button „Nein“, um den Assistenten zu beenden.

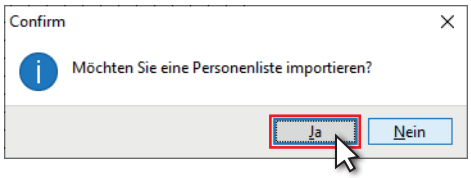


5.4.2.4 Personenliste der Schließanlage hinzufügen

Es kann eine Personenliste für die Schließanlage geladen werden. Die Personenliste können Sie über eine CSV-Datei (*.CSV) importieren.

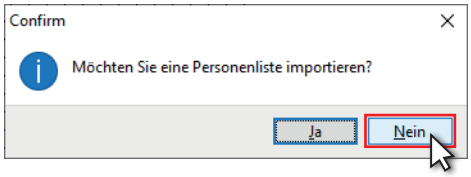
HINWEIS **Achten Sie darauf, dass die CSV-Datei auf eine „UTF-8“-Codierung eingestellt ist, weil es keinen allgemeinen Standard für das Dateiformat CSV gibt!**

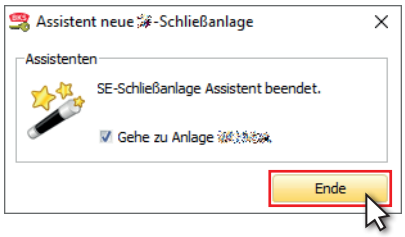
- Drücken Sie auf den Button „Ja“, um eine Personenliste zu importieren.



Sie können auch den Import zu einem späteren Zeitpunkt durchführen, wenn Ihnen keine Personenliste zur Verfügung steht. In diesem Fall ist der Assistent zu beenden.

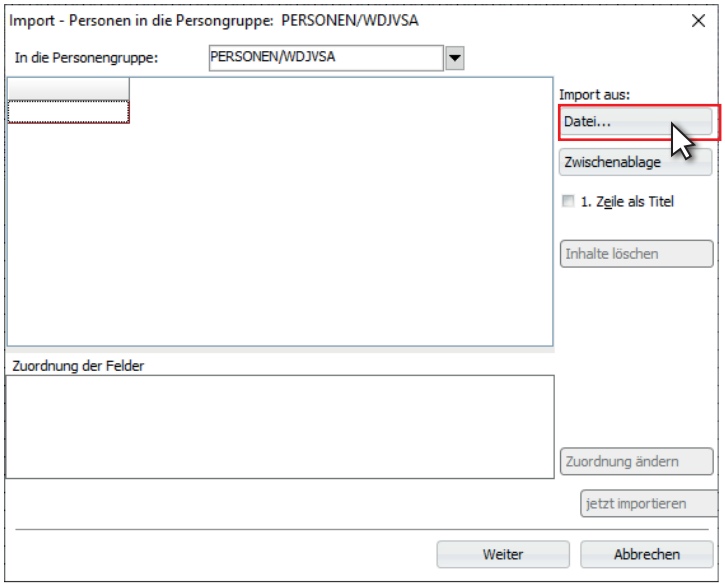
- Drücken Sie auf den Button „Nein“, um die Anlage der Schließanlage zu beenden, ohne eine Personenliste zu importieren.
- Wechseln Sie mit „Ende“ zu der neu angelegten Schließanlage.



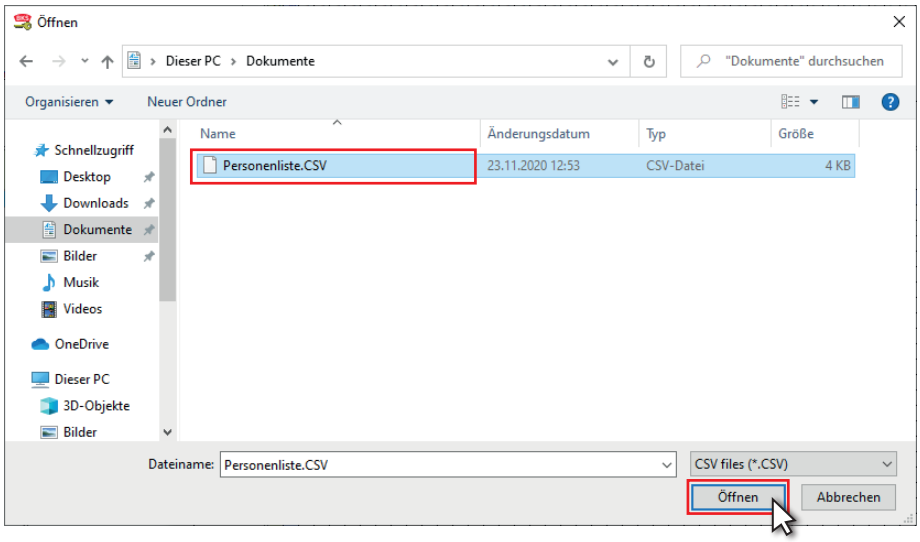


Nach der Auswahl „Personenliste importieren“ öffnet sich folgender Dialog.

- Drücken Sie auf den Button „Datei ...“ in der Spalte „Import aus:“ des Fensters.

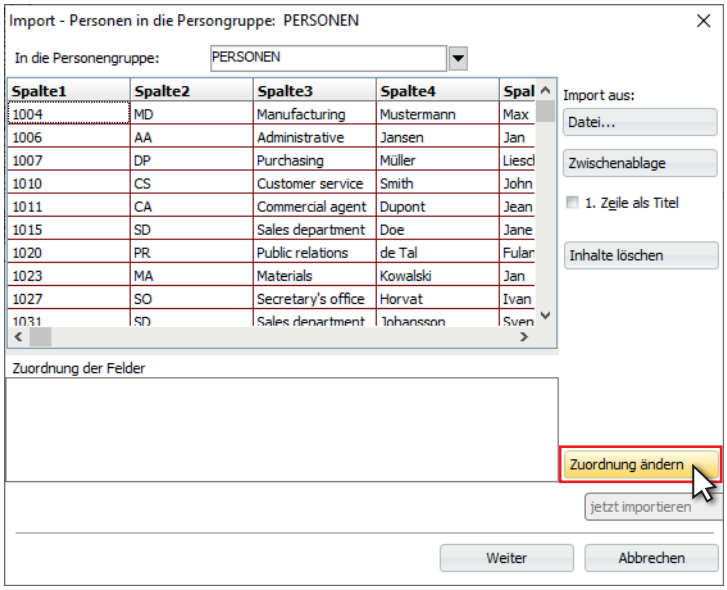


- Navigieren Sie mit dem Dateibrowser zur Personenliste. Die Datei muss im CSV-Format (*.CSV) vorliegen.
- Drücken Sie auf den Button „Öffnen“, um den Import zu starten.



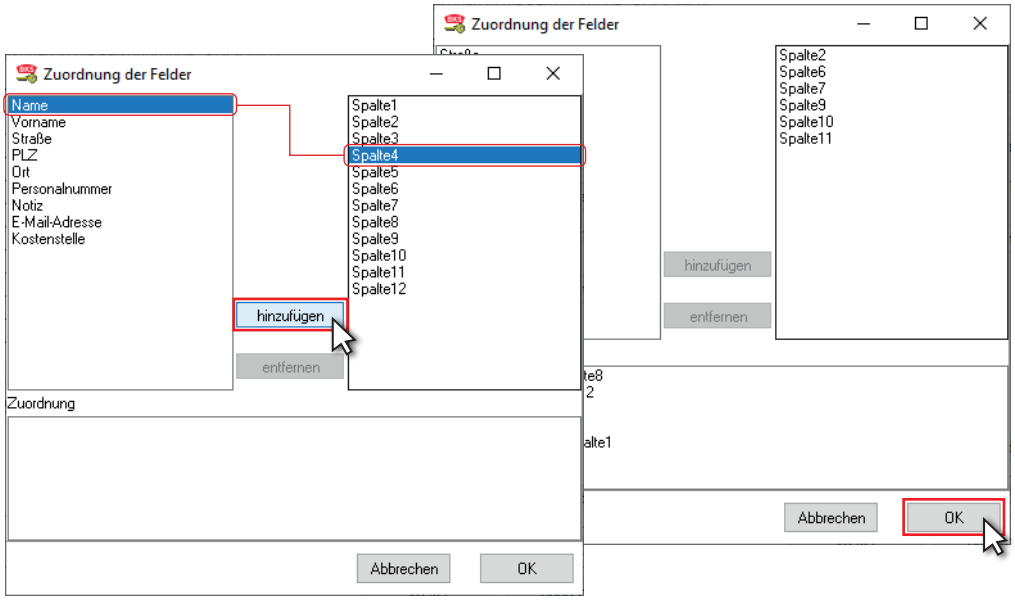
Zur Übersicht wird Ihnen die importierte Personenliste angezeigt. Die Spalten der Personenliste sind den Feldern des BKS KeyManagers zuzuweisen.

- Drücken Sie auf den Button „Zuordnung ändern“.

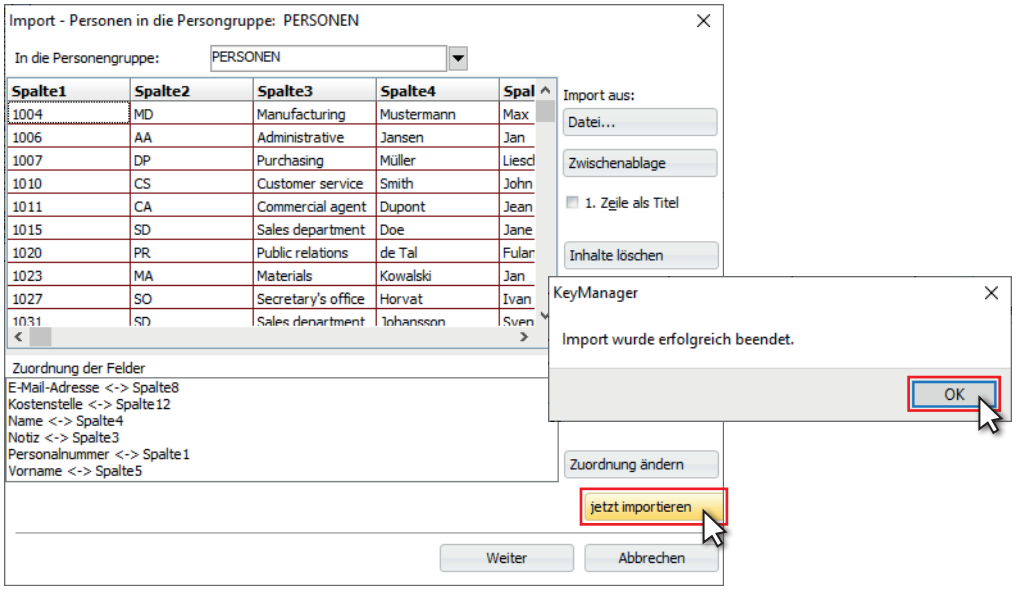


Ordnen Sie im Fenster „Zuordnung der Felder“ die personenbezogenen Daten der dazugehörigen Spalte zu. Zum Beispiel „Name“ und „Spalte 4“.

- Wählen Sie „hinzufügen“ aus und stellen Sie die Zuordnung her.
- Nach der Zuordnung der Spalten der Personenliste mit den Feldern des BKS KeyManagers fahren Sie mit „jetzt importieren“ fort.
- Beenden Sie die Zuordnung und drücken auf den Button „OK“.



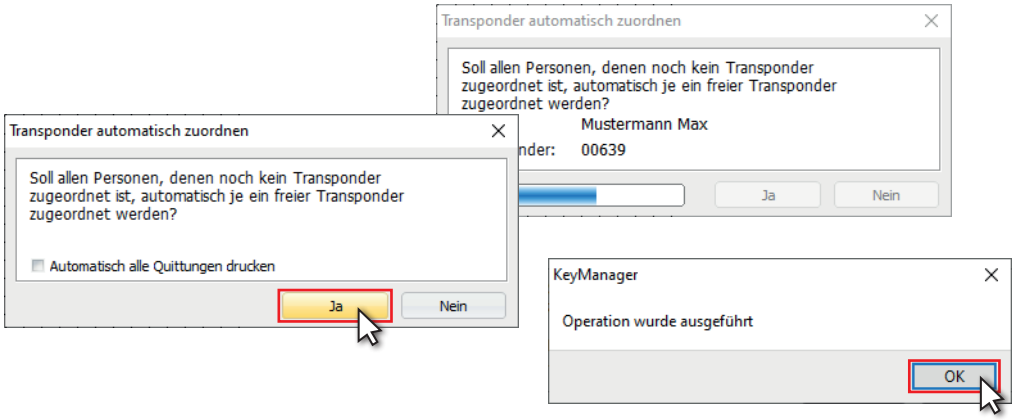
- Lesen Sie die Personenliste mit „jetzt importieren“ ein und drücken zur Bestätigung auf den Button „OK“.



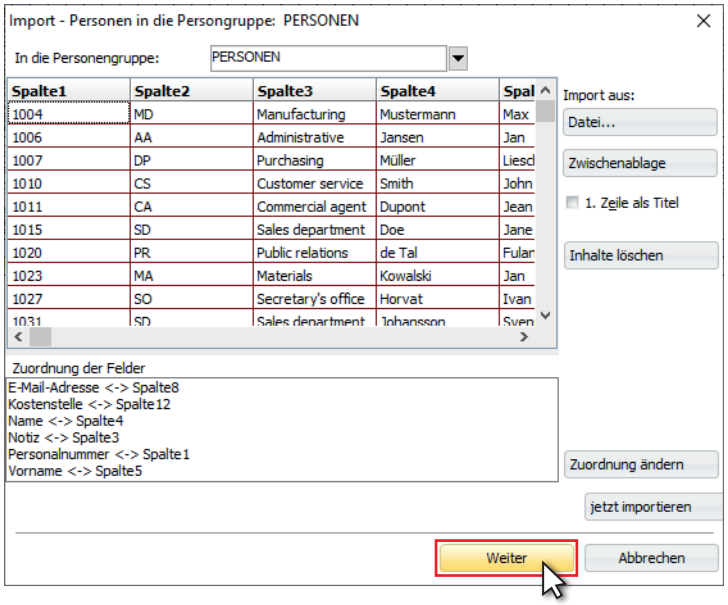
5.4.2.5 Automatische Transpondervergabe

Allen Personen, die noch keinen Transponder haben, kann automatisch ein Transponder zugeordnet werden. Bei Ausgabe von mehreren Transpondern kann dies eine große Zeitersparnis sein.

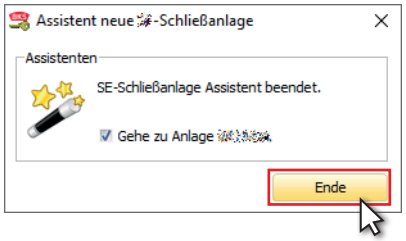
- Drücken Sie auf den Button „Ja“, um die Zuordnung zu starten.



- Drücken Sie auf den Button „Weiter“, um die Zuordnung abzuschließen.



- Zum Beenden des Assistenten drücken Sie auf den Button „Ende“ und schließen Sie den Assistenten der Schließanlage ab.



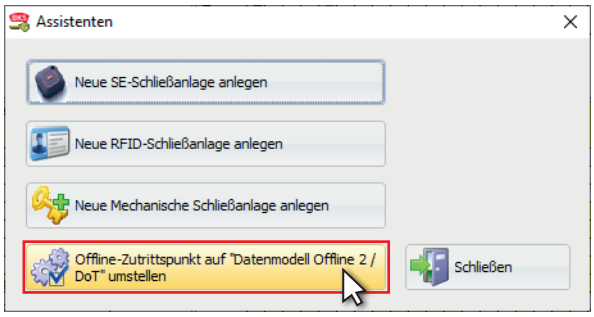
5.5 Offline Zutrittspunkte mit altem Datenmodell auf das Neue umstellen

Zutrittspunkte, die noch auf dem alten „Datenmodell Offline 1“ basieren, können nicht in Schließanlagen mit dem „Datenmodell Offline 2 / DoT“ verwendet werden. Die Kompatibilität kann durch die Umstellung des Zutrittspunkts auf das neue Datenmodell hergestellt werden.

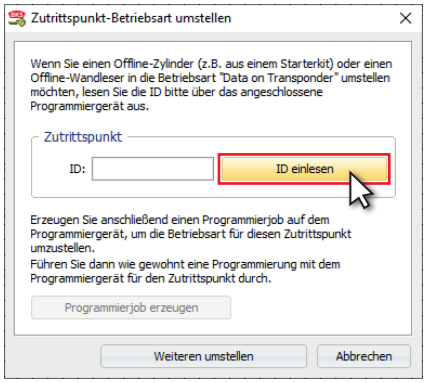
ACHTUNG

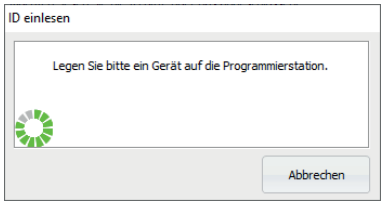
Das Umstellen ändert das Datenmodell und alle Daten im Zutrittspunkt werden gelöscht.
→ Eine Umstellung zurück in das Datenmodell Offline 1 ist nicht möglich!

- Drücken Sie auf den Button „Offline-Zutrittspunkt auf „Datenmodell Offline 2 / DoT“ umstellen“, um den Vorgang zu starten.

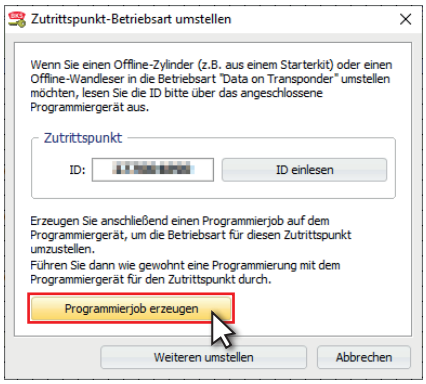


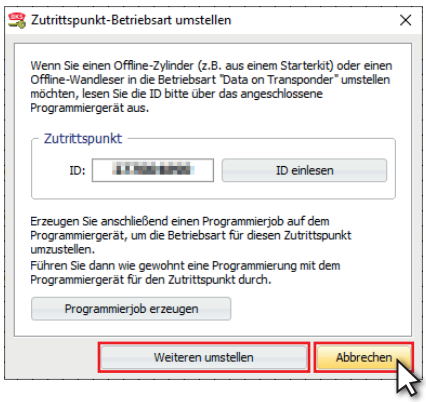
- Drücken Sie auf den Button „ID“ einlesen“ und legen den Zutrittspunkt auf das verbundene Programmiergerät.





- Drücken Sie auf den Button „Programmierjob erzeugen“ und auf „Abbrechen“ zum Beenden oder auf „weitere Umstellen“.





Übertragen Sie den Programmierjob mit Funktion „Programmieren“ des Hauptmenüs auf das Programmiergerät. Senden Sie die Daten vom Programmiergerät zum Zutrittspunkt zur Umstellung.

5.6 Anlagenpasswort festlegen

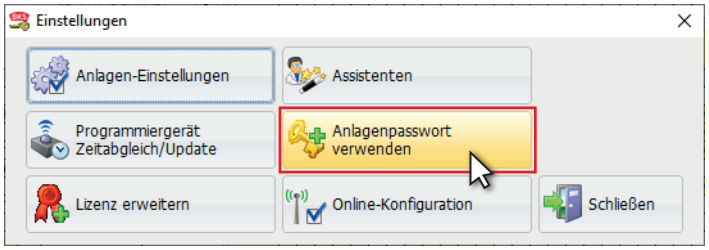
Mit der Funktion „Anlagenpasswort verwenden“, können Sie ein Anlagenpasswort für Ihre Schließanlage anlegen bzw. ein vorhandenes ändern. Durch die Definition eines Anlagenpasswortes können Sie die Programmieraufträge zusätzlich zum Benutzerprofil durch ein individuelles Passwort absichern. Eine nicht autorisierte Programmierung wird so verhindert.

HINWEIS

Bei Verlust des Anlagenpasworts ist ein Rücksetzen des Passworts nicht möglich. Kontaktieren Sie den Service der Firmengruppe Gretsch-Unitas und senden nach Absprache die Zutrittspunkte ein.

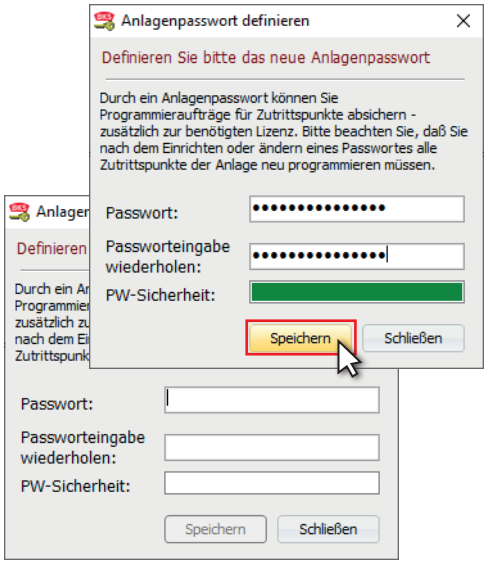
Wenn ein Passwort neu definiert oder geändert wird, müssen sämtliche Zutrittspunkte der Anlage neu programmiert werden. Idealerweise sollte ein Passwort vor der Erstprogrammierung der Zutrittspunkte definiert werden.

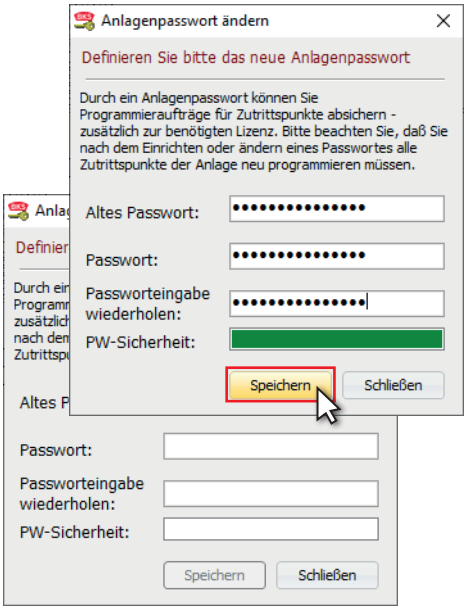
- Drücken Sie den Button „Anlagenpasswort verwenden“ im Menü Einstellungen.



Im folgenden Fenster werden Sie aufgefordert, ein Passwort einzugeben. Ist ein Passwort schon einmal vergeben worden, müssen Sie vor der Neueingabe zuerst das alte Passwort eingeben.

Das Passwort muss aus mindestens 8 Zeichen bestehen. Die Sicherheit des Passworts wird durch die Verwendung von Klein- und Großbuchstaben sowie von Zahlen und Sonderzeichen erhöht.





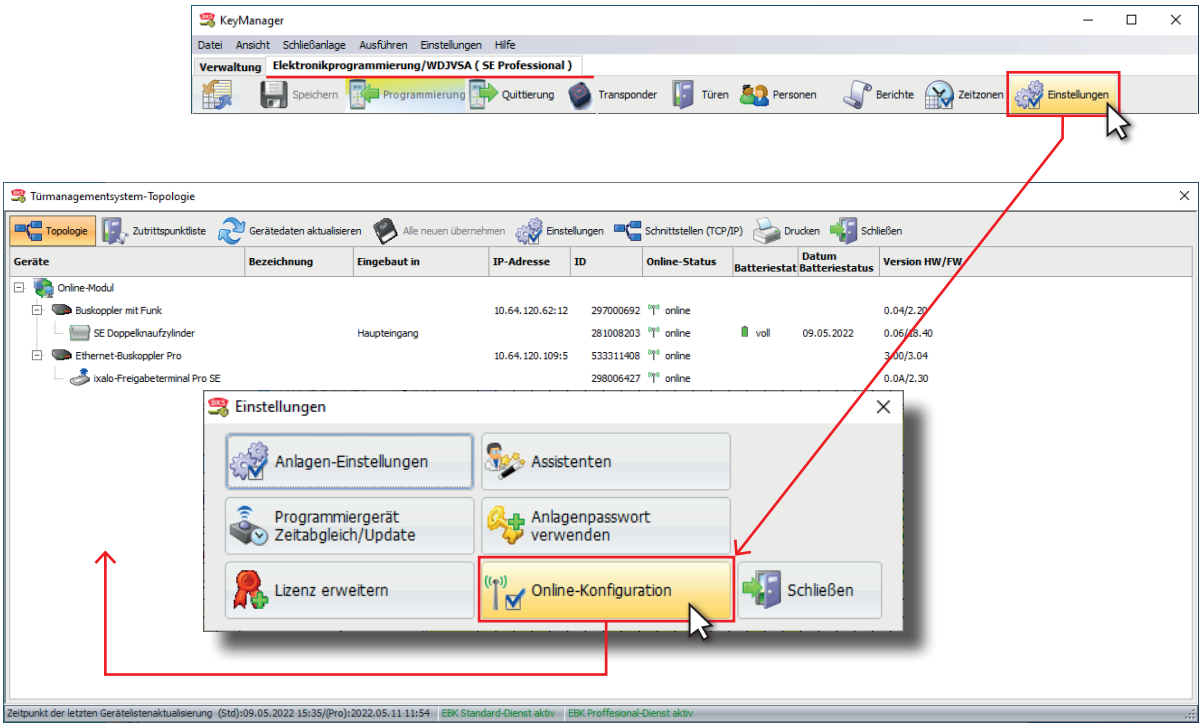
Die Sicherheitsstufe des Passworts wird ihnen als farbiger Balken angezeigt.
Ab Sicherheitsstufe gelb können Sie das Passwort mit „Speichern“ übernehmen.

5.7 Online-Konfiguration

Zum Betreiben des Online-Moduls sind der Online-Dienst und/oder der EBK Pro-Dienst notwendig, um die Daten vom BKS KeyManager an die online angebundenen Zutrittspunkte oder Freigabeterminals über Ethernetbuskoppler übermitteln zu können. Den Status des Online-Dienstes können Sie wie im Kapitel 5.7.1 [293] beschrieben prüfen und ggf. Korrekturen durchführen. Zur Einrichtung des Online-Moduls dient das Menü „Online-Konfiguration“.

Der Online-Dienst und diese Online-Konfiguration steht Ihnen erst zur Verfügung, wenn Sie in Ihrer Schließanlage eine Data on Transponder- und/oder Online-Lizenz geladen haben, siehe 5.3 [269].

- Wählen Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ den Menüpunkt „Einstellungen“ aus.
- Drücken Sie auf den Button „Online-Konfiguration“.



5.7.1 Systemstatus der Dienste überprüfen

In der Online-Konfiguration des BKS KeyManagers können zwei Dienste konfiguriert werden. Je nach Aufbau Ihrer Anlage sind das folgende Dienste.

- **KeyManager Online**-Dienst für Online-Anlagen oder Data on Transponderanlage mit Freigabeterminal
- **EBK Pro**-Dienst für Data on Transponderanlage mit Freigabeterminal Pro / Freigabeterminal 2 Pro

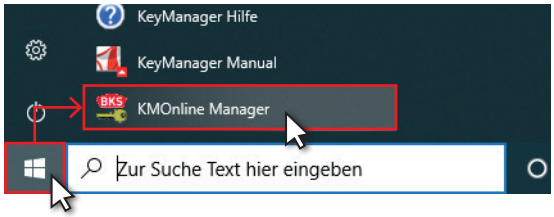
Vor der Konfiguration der Dienste sollten Sie sich einen Überblick über den Systemstatus und die Einbindung bzw. die Verbindung zu den verschiedenen Komponenten des BKS KeyManagers verschaffen.

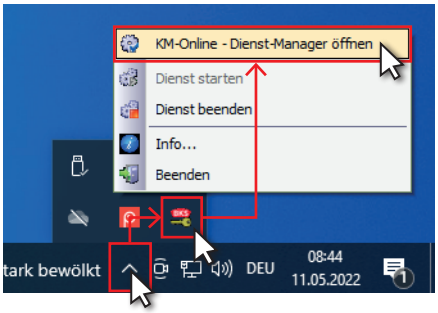
In den Einstellungen der Datenbank können Sie festlegen, auf welche Datenbank die Dienste zugreifen soll. Sollte Sie eine eigene kompatible Datenbank verwenden, können Sie diese über die Einstellungen einbinden. Bei Client-Server Installationen wird der Online- oder EBK Pro-Dienst nur auf dem Server benötigt.

5.7.1.1 Systemstatus mit dem KeyManager Online-Service Manager

Voraussetzung für dieses Tool ist, dass bei der Installation des BKS KeyManagers auch das Online-Modul installiert wurde. Falls Sie nur den EBK Pro-Dienst installiert haben, verwenden Sie bitte das EBK Pro Server Config-Tool.

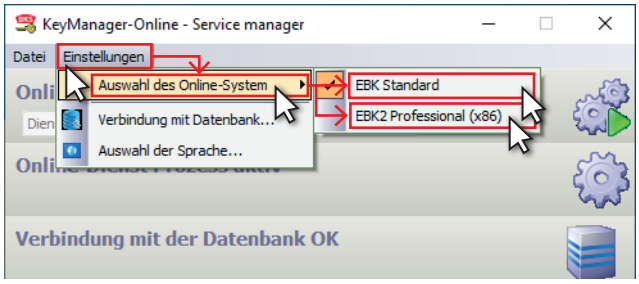
- Öffnen Sie das Windows-Startmenü und drücken auf den Programmpunkt „KeyManager Online-Service Manager“ im Ordner „BKS“.
- Drücken Sie auf das Symbol des KeyManager Online-Service Managers in der Taskleiste. Falls das Symbol ausgeblendet ist, öffnen Sie mit der rechten Maustaste das Kontextmenü und Drücken auf den Menüpunkt „KM-Online - Dienst-Manager öffnen“.





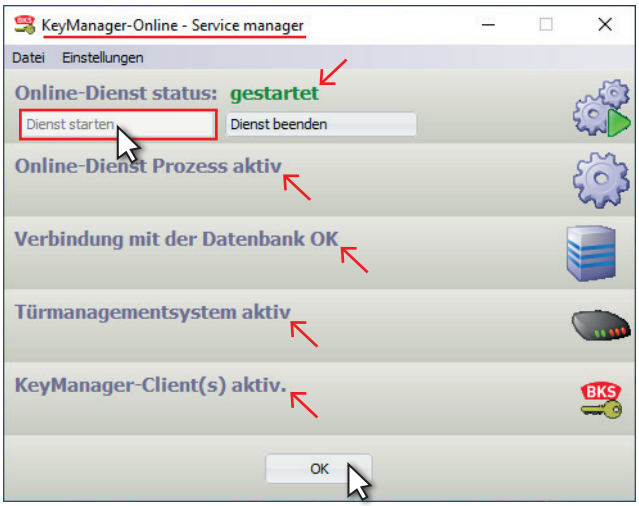
Im Fenster des KeyManager Online-Service Managers erhalten Sie einen Überblick über den Status.

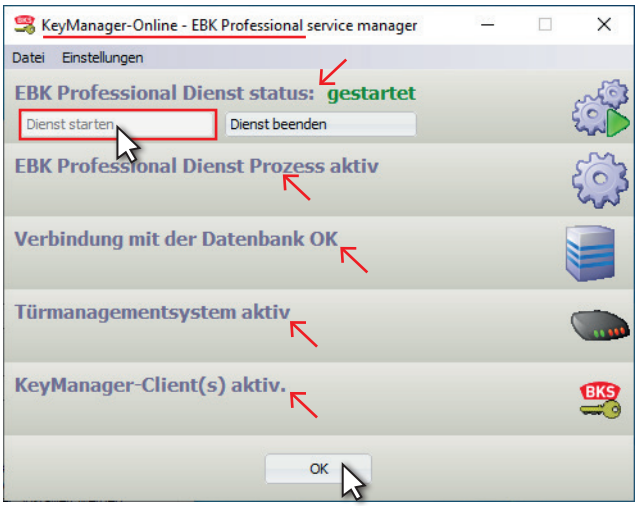
- Wechseln Sie über das Dropdown-Menü „Einstellungen“ dem Menüpunkt „Auswahl des Online-Systems“ zum Dienst „EBK Standard“ für den Online-Dienst oder „EBK2 Professional“ für den EBK-Pro-Dienst.



Der für Ihre Anwendung benötigte Dienst muss gestartet und aktiv sein. Die Verbindung zu den Komponenten des Programms müssen OK oder aktiv sein.

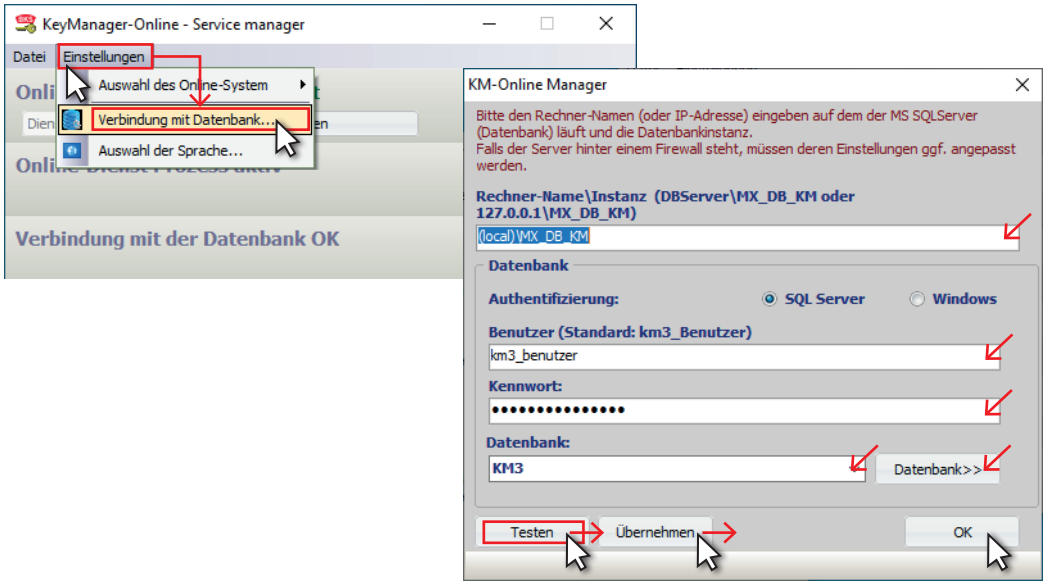
- Starten Sie ggf. den Dienst über den Button „Dienst starten“.





Die Datenbankverbindung kann im Fenster „Einstellungen“ konfiguriert werden. Bei einer Client-Server-Anlage wird der Online- und EBK Pro-Dienst nur auf dem Server benötigt.

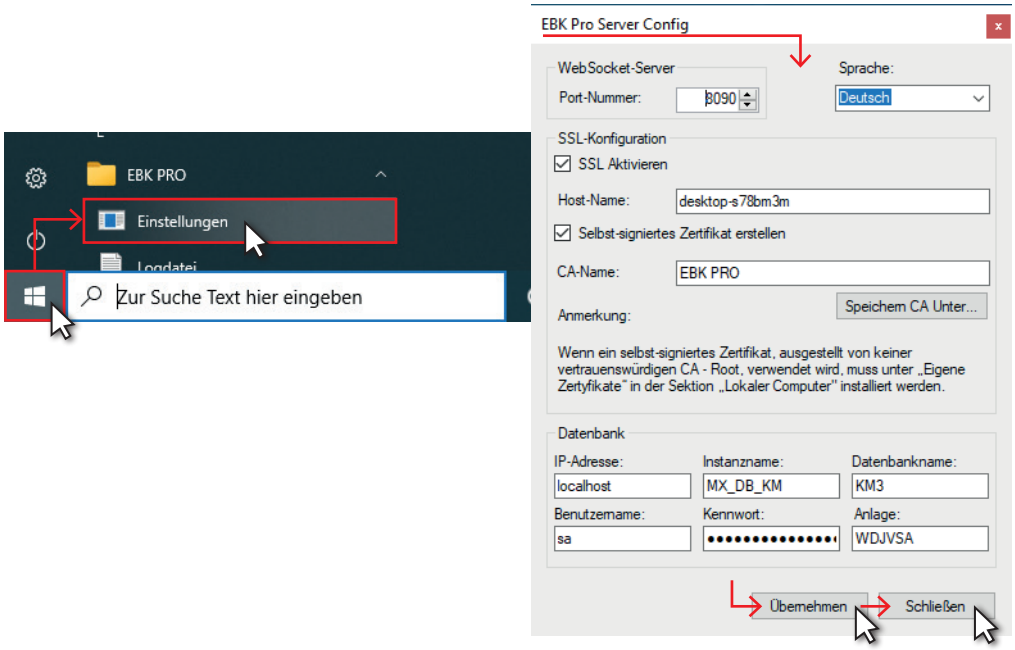
- Öffnen Sie das Dropdown-Menü „Einstellungen“ und drücken auf den Menüpunkt „Verbindung mit Datenbank“.
- Im Fenster „KM-Online Manager“ können Sie eine andere vorhandene Datenbank mit dem BKS KeyManager verknüpfen. Wir empfehlen, die mit dem BKS KeyManager installierte Datenbank zu verwenden und keine Änderung vorzunehmen. Füllen Sie zum Ändern der Datenbank die entsprechenden Felder aus. Überprüfen Sie mit dem Button „Testen“ die Verbindung zur Datenbank.



5.7.1.2 Datenbank konfigurieren mit dem EBK Pro Server Config

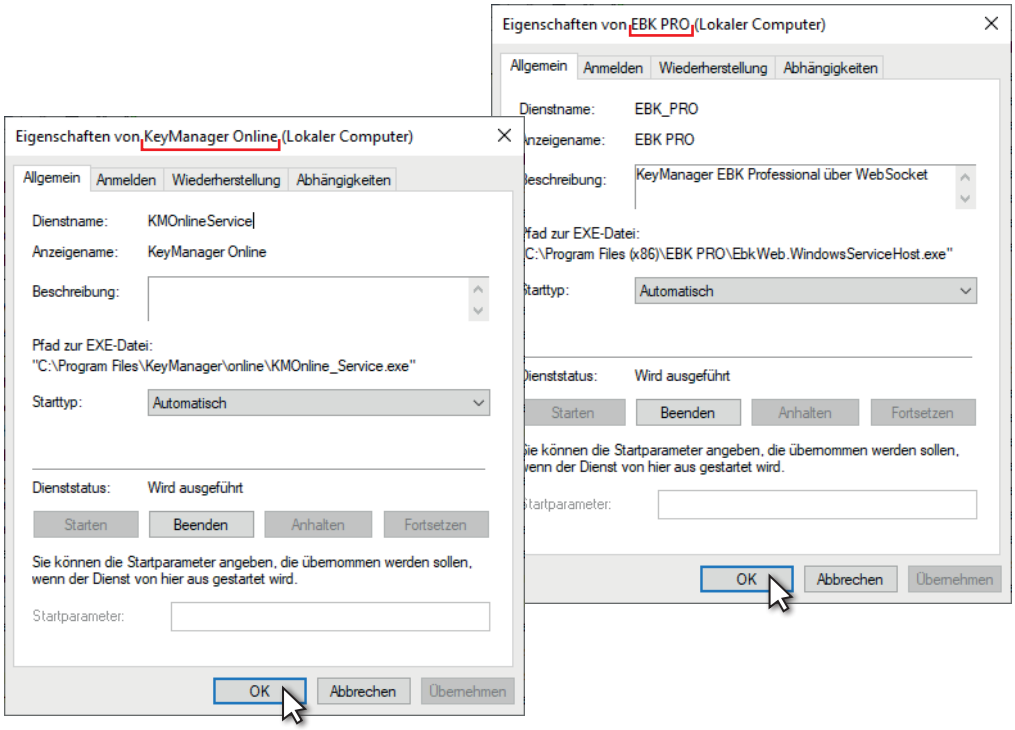
Sollten Sie nur den EBK Pro-Dienst nutzen, verwenden Sie bitte das EBK Pro Server Config-Tool zur Konfiguration der Datenbank.

- Öffnen Sie das Windows-Startmenü und drücken auf den Programmpunkt „Einstellungen“ im Ordner „EBK Pro“.



5.7.1.3 Anzeige des Dienstes in Windows

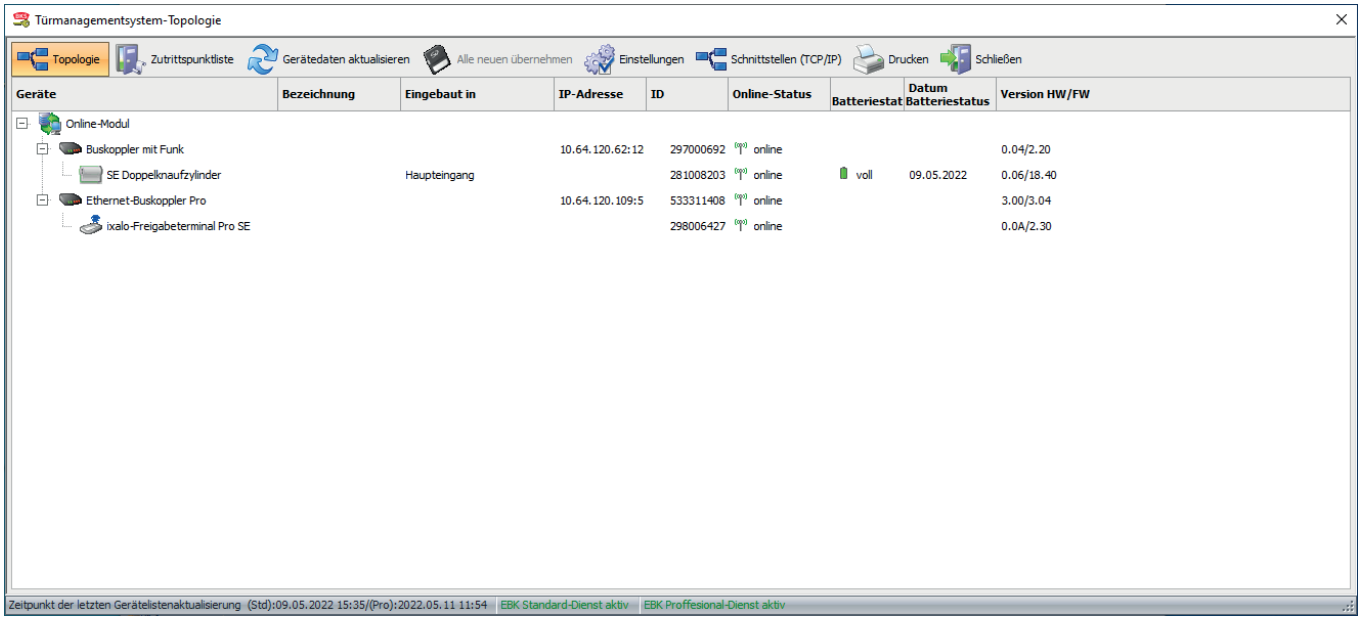
- Die Dienste können Sie alternativ auch in der App „Dienste“ von Windows aufrufen.



5.7.2 Funktionen Online-Konfiguration

Mit den Funktionen der Online-Konfiguration können Sie die verschiedenen Modelle des Ethernet-buskopplers (EBK, EBK FM, EBK Pro und EBK 2 Pro) im Netzwerk identifizieren und einer Liste der Topologie angezeigt bekommen. Bei der Einrichtung der Ethernetbuskoppler im Netzwerk können Sie die online angebunden Zutrittspunkte und angeschlossenen Freigabeterminals in der Topologie konfigurieren.

Zur Konfiguration stehen Ihnen die folgenden Menüpunkte zur Verfügung.
Für die in der Topologie gelisteten Komponenten können Sie über die jeweiligen Kontextmenüs weitere Einstellungen vornehmen.

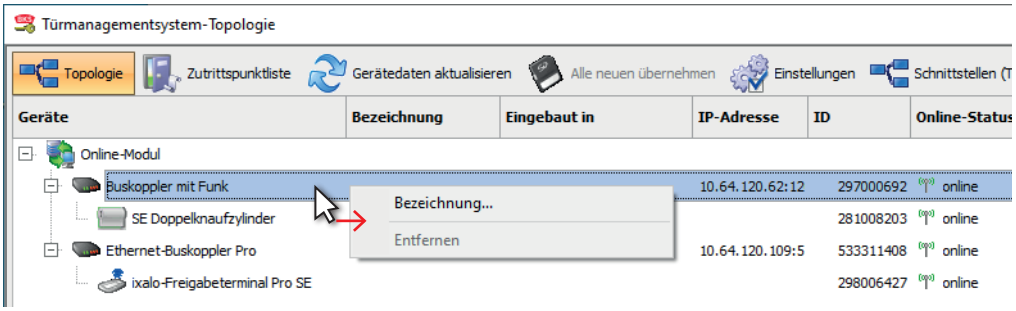


5.7.2.1 Topologie

Die einzelnen in der Liste aufgeführten Komponenten lassen sich über ein Kontextmenü, welches sich zu jedem Listeneintrag mit der rechten Maustaste aufgerufen lässt, editieren.

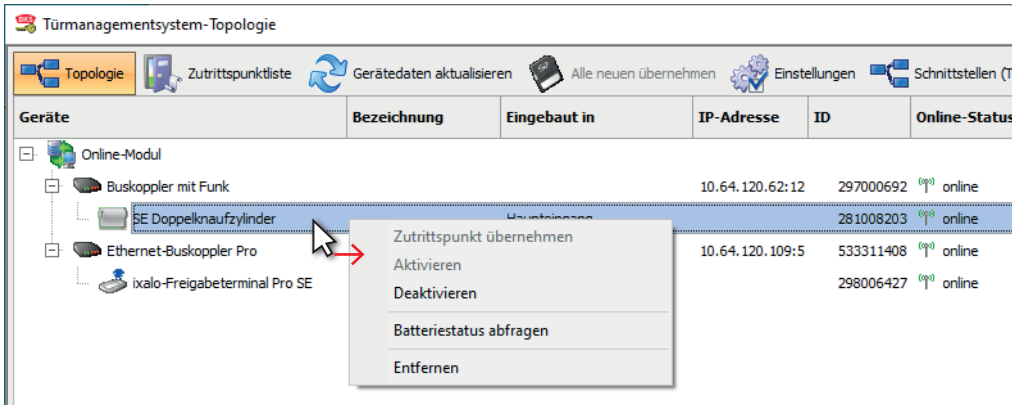
Kontextmenü für Ethernet-Buskoppler (EBK), Ethernet-Buskoppler Funkmodul (EBK FM)

- Menüpunkt „Bezeichnung“ ändern oder vergeben Sie einen Namen für das EBK/EBK FM.
- Menüpunkt „Entfernen“ zum Löschen des EBK/EBK FM aus dem Onlinesystem. Das EBK/EBK FM muss hierzu ohne verbundene Zutrittspunkte sein.



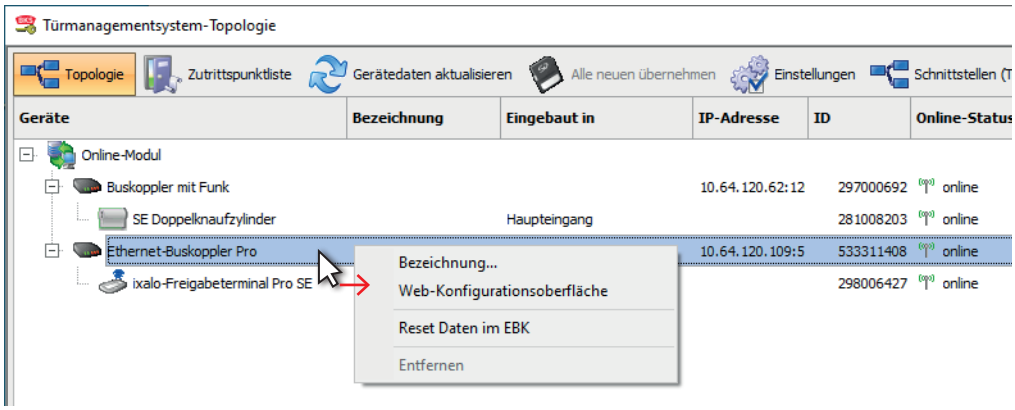
Kontextmenü für einen online verbundenen Zutrittspunkt

- Menüpunkt „Zutrittspunkt übernehmen“, um einen vom System neu gefundenen Zutrittspunkt in das Onlinesystem zu übernehmen.
- Menüpunkt „Aktivieren“ / „Deaktivieren“, um den Zutrittspunkt online oder offline zusetzen.
- Menüpunkt „Batteriestatus abfragen“ zur Aktualisierung des Batteriestaus.
- Menüpunkt „Entfernen“ zum endgültigen Löschen des Zutrittspunkts aus dem Onlinesystem. Der Zutrittspunkt muss vorher im Menü „Schnittstellen“ gelöscht werden.



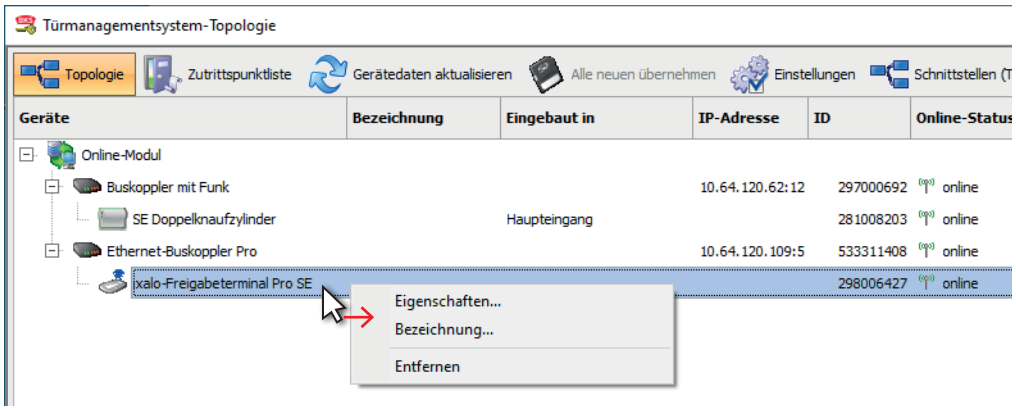
Kontextmenü für EBK Pro (Ethernet-Buskoppler Pro) und EBK 2 Pro

- Menüpunkt „Bezeichnung“ ändern oder vergeben Sie einen Namen für das EBK.
- Menüpunkt „Web-Konfigurationsoberfläche“ ist zum Öffnen der Oberfläche zur Einrichtung des EBK Pro / EBK 2 Pro im Web-Browser.
- Menüpunkt „Reset Daten im EBK“ leert den Speicher im EBK Pro / EBK 2 Pro.
- Menüpunkt „Entfernen“ zum Löschen des EBK aus dem Onlinesystem. Das EBK muss hierzu ohne verbundene Zutrittspunkte/Freigabeterminals sein.



Kontextmenü für ein Freigabeterminal (FGT)

- Im Menüpunkt „Eigenschaften“ können Sie die Einstellungen der Übertragung und somit der beim Buchen des Transponders gesendeten Daten anpassen. Details siehe weitere Beschreibung.
- Menüpunkt „Bezeichnung“ ändern oder vergeben Sie einen Namen für das FGT.
- Verwenden Sie den Menüpunkt „Entfernen“ zum Löschen des Freigabeterminal Pro‘s aus dem Onlinesystem. Trennen Sie im nächsten Schritt die Verkabelung zum EBK Pro. Nach einem Reboot vom EBK Pro wird sonst das FGT Pro wieder verbunden und erscheint in der Topologie.



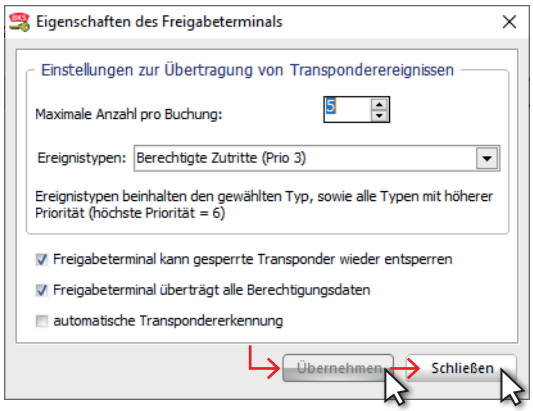
In den Einstellungen zur Übertragung der Transponderereignisse können Sie den Umfang der übertragenen Daten festlegen. Hierbei gilt es, den Komfort bei der Übertragung von vielen Ereignissen und den Datenschutz, durch welchen so wenig wie möglich Daten gespeichert werden sollen, mit Ihren Firmenrichtlinien in Einklang zu bringen.

- Legen Sie fest, wie viele Ereignisse bei einer Buchung zum Transponder übertragen werden sollen. Grundsätzlich sind max. 25 Ereignisse pro Buchung möglich.
- Im Dropdown-Menü „Ereignistypen“ wählen Sie aus, welche Art der Ereignisse bei der Buchung übertragen werden sollen. Die Ereignisse sind in Prioritätsstufen unterteilt, dabei schließt die niedrigste Priorität alle höheren Prioritäten mit ein. Bei der höchsten „Prio 6“ werden nur wichtige Systemereignisse übertragen. Bei „Prio 3“ werden neben den berechtigten Zutritten auch die Ereignisse der anderen Prioritätsstufen übertragen.

Durch Aktivieren der folgenden Checkboxen können Sie weitere Einstellungen festlegen.

- Die aktivierte Checkbox „Transponder kann gesperrte Transponder wieder entsperren“ ermöglicht es, dass gesperrte Transponder nach dem Entsperren und senden eines Programmierauftrags an das FGT bei der Buchung am FGT entsperrt. Bei Deaktivierung werden gesperrte Transponder nicht vom FGT entsperrt.
- Mit aktivierter Checkbox „Freigabeterminal überträgt alle Berechtigungsdaten“ werden Änderungen der Zutrittsberechtigungen oder der Transpondereigenschaften übertragen. Der Transponder wird beim Buchen am FGT programmiert.
- Die deaktivierte Checkbox „automatische Transpondererkennung“ schaltet die Funktion aus, durch welche die Transponder auch ohne eine Betätigung des Druckknopfs beim Vorhalten am FGT eine Buchung auslösen.

- Drücken Sie nach einer Änderung auf den Button „Ändern“ und anschließend auf „Schließen“.



HINWEIS

Wenn die Anzahl der Zutritte und Ereignisse, die beim Buchen an den Zutrittspunkten auf dem Transponder gespeichert werden, dessen Kapazität übersteigen, werden unabhängig von den Einstellungen des FGTs nicht alle Daten von den Zutrittspunkten an die Freigabeterminals zum BKS KeyManager übertragen. Die Zutritte und Ereignisse können jedoch jederzeit bei Bedarf mit dem Programmiergerät aus den verschiedenen Zutrittspunkten ausgelesen und zum BKS KeyManager übertragen werden.

5.7.2.1.1 Darstellung der Topologie

In der Anzeige der Topologie werden alle Komponenten des Online-Dienstes in einer Baumstruktur dargestellt. Die Spalten stellen weitere Informationen zu den Komponenten bereit.

- Spalte „Geräte“
  – Übersicht der Netzwerkstruktur der verschiedenen Geräte
- Spalte „Bezeichnung“
  – Bezeichnung der Komponente durch eine vom Benutzer frei wählbare Benennung
- Spalte „Eingebaut in“
  – Bezeichnung des Zutrittspunkt. Die wurde beim Anlegen des Zutrittspunkts festgelegt
- Spalte „IP-Adresse“
  – IP-Adresse der Online-Komponenten
- Spalte „ID“
  – Seriennummer der jeweiligen Online-Komponente
- Spalte „online-Status“ mit folgenden Meldungen
  – online — Online-Komponente ist verbunden und online
  – nicht aktiv — Online-Komponente ist deaktiviert worden
  – unbekannt — Status unbekannt
  – nicht verbunden — es ist keine (Funk-)Kommunikation mit der Online-Komponente möglich
  – nicht gefunden — es ist keine Netzwerk-Kommunikation zur Online-Komponente möglich
- Spalte „Batteriestatus“ und „Datum Batteriestatus“
  Visualisierung der Kapazität der Batterie zum angegebenen Zeitpunkt
  – voll — Funk-Komponente meldet keinen Batteriewarnlevel
  – halbvoll — Funk-Komponente meldet Batteriewarnlevel 1, baldiger Austausch der Batterie notwendig
  – leer — Funk-Komponente meldet Batteriewarnlevel 2, sofortiger Austausch der Batterie notwendig

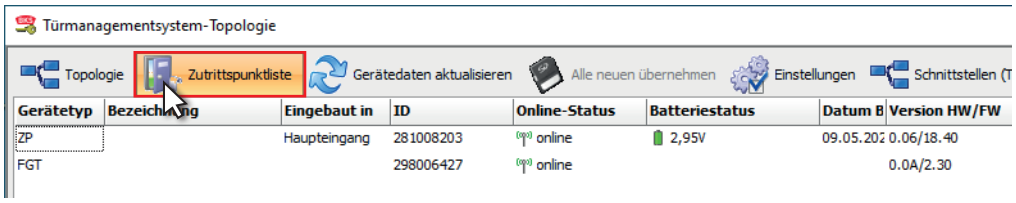
Durch Drücken der Tastenkombination „Strg“ + „Alt“ + „O“ werden die Spalte „RSSI“ und „Bewertung“ eingeblendet. Diese visualisieren die Funk-Übertragungs-Qualität zwischen EBK FM / SE FM und Funk-Zutrittspunkt.

- Spalte „RSSI“ und „Bewertung“
  - sehr gut — sehr gute Verbindungsqualität
  - gut — gute Verbindungsqualität
  - OK — Verbindungsqualität akzeptabel
  - gering — geringe Signalstärke, ändern Sie ggf. die Ausrichtung der Funkantenne und/oder die Position des EBK FM / SE FM
- Spalte „Version HW/FW“
  - Hardware- und Firmwareversion der Online-Komponenten

5.7.2.2 Zutrittspunktliste

In der Zutrittspunktliste werden Ihnen nur die vorhandenen Online-Zutrittspunkte in einer Liste dargestellt.

- Aufrufen der Kontextmenüs analog der Bearbeitung der Zutrittspunkte in der Topologie.

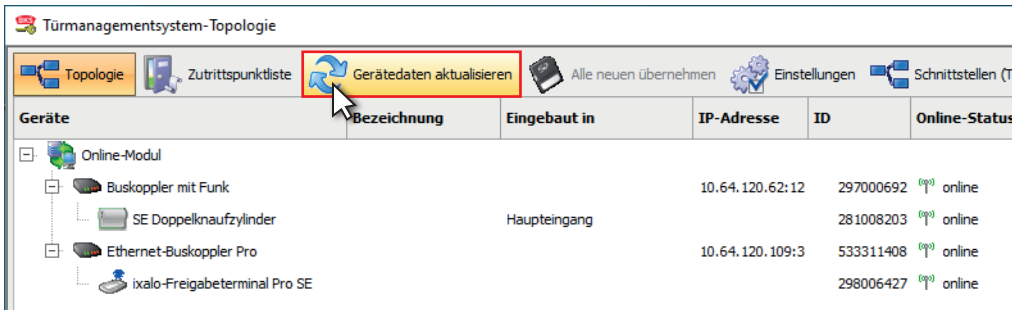


Anstelle der Spalte „Batteriestatus“ wird die „Batteriespannung“ angezeigt. Um herauszufinden, an welchen Zutrittspunkten ein Batteriewechsel fällig wird, können Sie die Zutrittspunkte nach der Batteriespannung sortieren lassen.

Eine andere Möglichkeit ist die Sortierung der Funk-Zutrittspunkte nach dem RSSI-Wert, um z. B. die Zutrittspunkte mit der ungünstigsten Funk-Verbindungen herauszufinden. Dabei gilt es zu beachten, dass je kleiner der Betrag des RSSI-Wertes ist, umso besser ist die Funkverbindung.

5.7.2.3 Gerätedaten aktualisieren

- Drücken Sie auf den Button „Gerätedaten aktualisieren“ für ein Update der Liste.



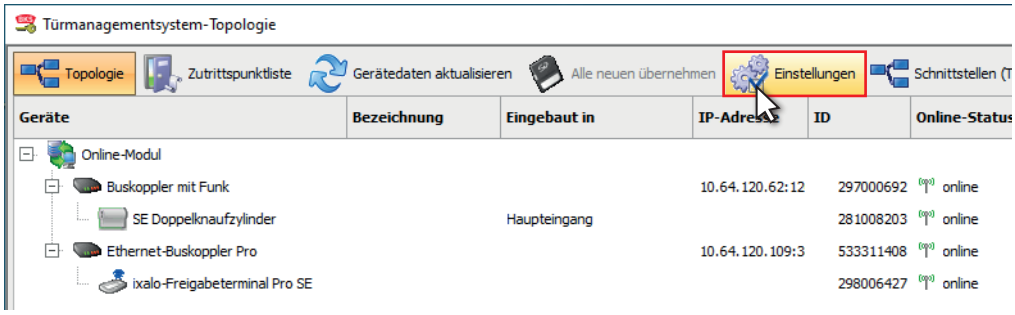
5.7.2.4 Gerätedaten aktualisieren

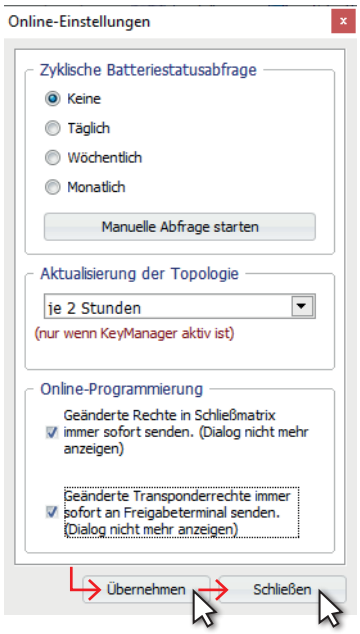
Über diese Funktion werden neue Ethernetbuskoppler und/oder online angebundene Zutrittspunkte, welche über das Menü „Schnittstellen“ erkannt bzw. hinzugefügt wurden, in die Topologie übernommen. Ausgenommen hiervon sind die EBK Pro-Modelle.

- Drücken Sie auf den Button „Alle neuen übernehmen“ zur Aktivierung in der Anlage.

5.7.2.5 Einstellungen

- Drücken Sie auf den Button „Einstellungen“ zum Öffnen des Fensters Online-Einstellungen.





- Durch Aktivieren einer der Checkboxen legen Sie die Abstände zwischen den Abfragen des Batteriestatus fest bzw. durch Auswahl von „Keine“ deaktivieren Sie die Abfrage.
- Drücken Sie auf den Button „Manuelle Abfrage starten“, um bei Bedarf den Batteriestatus zu aktualisieren.
- Wählen Sie im Dropdown-Menü „Aktualisierung der Topologie“ einen Zeitraum, nach der die Liste der in der Topologie angezeigten Komponenten aktualisiert wird.
- Im Feld Online-Programmierung können Sie festlegen, das die Daten der Änderungen in der Berechtigungsmatrix durch das Drücken des Menüpunkts „Speichern“ sofort an die online verbundenen Zutrittspunkte und/oder Freigabeterminals übertragen werden. Durch Aktivierung der Checkboxen werden die Daten beim Speichern automatisch übertragen. Sind die Checkboxen deaktiviert, haben Sie die Möglichkeit, über einen Button oder Dialog die Datenübertragung manuell zu starten.

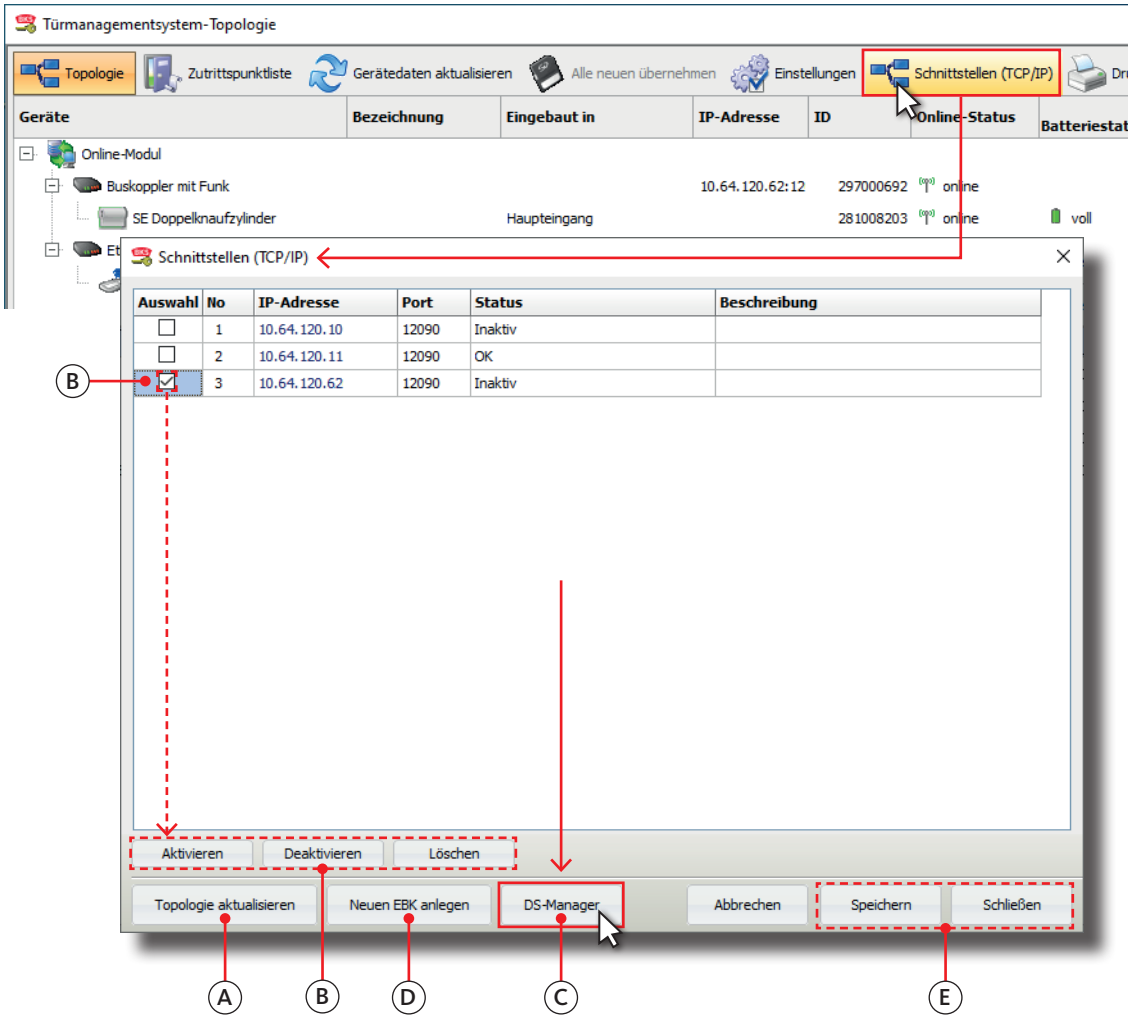
ACHTUNG **Jede Abfrage von Daten kostet Energie – die Lebensdauer der Batterie wird durch eine zyklische Datenabfrage reduziert.**

5.7.2.6 Schnittstellen (TCP/IP)

Die angeschlossenen Ethernetbuskoppler (EBK/EBK FM) werden erst in der Topologie angezeigt, wenn die TCP/IP-Verbindung eingerichtet worden ist. Die TCP/IP-Verbindung zwischen EBK/EBK FM und BKS KeyManager wird über das Menü „Schnittstellen (TCP/IP)“ eingerichtet.

- Drücken Sie auf den Button „Schnittstellenverwaltung (TCP/IP)“ zum Einrichten der TCP/IP-Verbindungen.

Menü der Schnittstellenverwaltung (TCP/IP) für den Online-Dienst (EBK/EBK FM)
Zur Verwendung in der Topologie müssen die Ethernetbuskoppler in der Liste im Fenster Schnittstellen über die Identifizierung angezeigt und aktiviert werden.



Die EBK/EBK FM müssen im Netzwerk identifiziert und für die jeweilige Netzwerkinfrastruktur eingerichtet werden. Mit der App „DS-Manager“ haben Sie die Möglichkeit, nach Geräten zu suchen, die nicht im Fenster Schnittstellen aufgeführt sind.

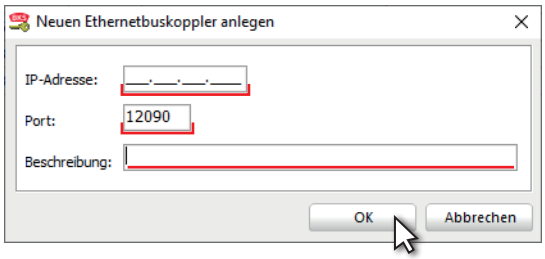
- (A) Zur Aktualisierung der in der Liste angezeigten Schnittstellen verwenden Sie den Button „Topologie aktualisieren“. In der Liste werden die identifizierten und neu hinzugefügten Ethernetbuskoppler (EBK/EBK FM) angezeigt.

- (B) Die Bearbeitung der Schnittstellen in dieser Liste können Sie mit den Buttons der folgenden Funktionen ausführen.
  - Wählen Sie im ersten Schritt ein EBK/EBK FM zur Bearbeitung aus.
  - Zur „Aktivierung“ eines EBK/EBK FM drücken Sie auf den gleichnamigen Button und fügen den Ethernetbuskoppler in die Liste der Schnittstellen ein.
  - Zur „Deaktivierung“ drücken Sie auf den gleichnamigen Button und die Verbindung zum EBK/EBK FM wird deaktiviert.
  - Drücken Sie auf den Button „Löschen“, um den gewählten Ethernetbuskoppler aus der Liste der Schnittstellen zu entfernen. Erst nach diesem Schritt kann das EBK/EBK FM endgültig in der Topologie (im Fenster Türmanagementsystem) gelöscht werden.

Wird in der Topologie ein EBK/EBK FM als offline angezeigt und bleibt dieser Zustand trotz Aktivierung der Schnittstellen bestehen, können Sie durch Löschen der Schnittstellen und das Identifizieren im DS-Manager das EBK/EBK FM wieder online setzen.

- (C) Die App „DS-Manager“ ist zum Auffinden und zum Identifizieren der EBK/EBK FM in Ihrem Netzwerk bestimmt. Neue EBK/EBK FM oder Geräte, zu denen die Verbindung verloren gegangen ist, können über den DS-Manager auf diesem Weg zur Liste der Schnittstellen hinzugefügt werden, siehe Kapitel 5.7.2.6.1 [305].

- (D) Optional besteht die Möglichkeit, ein EBK/EBK FM manuell im System anzulegen, wenn z. B. aufgrund der Netzwerkarchitektur die Geräte mit dem DS-Manager nicht identifiziert werden können. Ein Beispiel hierfür ist die Verwendung eines Gateways, um ein EBK/EBK FM, welches in einem anderen Netzwerksegment angeschlossen ist, nutzbar zu machen.
  In diesem Fällen verwenden Sie zum Anlegen den Button „Neuen EBK anlegen“, um manuell ein EBK oder EBK FM über die Eingabe der IP-Adresse, Port und Beschreibung der Liste der Schnittstellen hinzuzufügen.



- (E) Drücken Sie nach der Identifikation und Aktivierung der Ethernetbuskoppler auf den Button „Speichern“, um die Änderungen in die Topologie (im Fenster Türmanagementsystem) zu übernehmen. Zum „Schließen“ des Fensters drücken Sie auf den gleichnamigen Button.

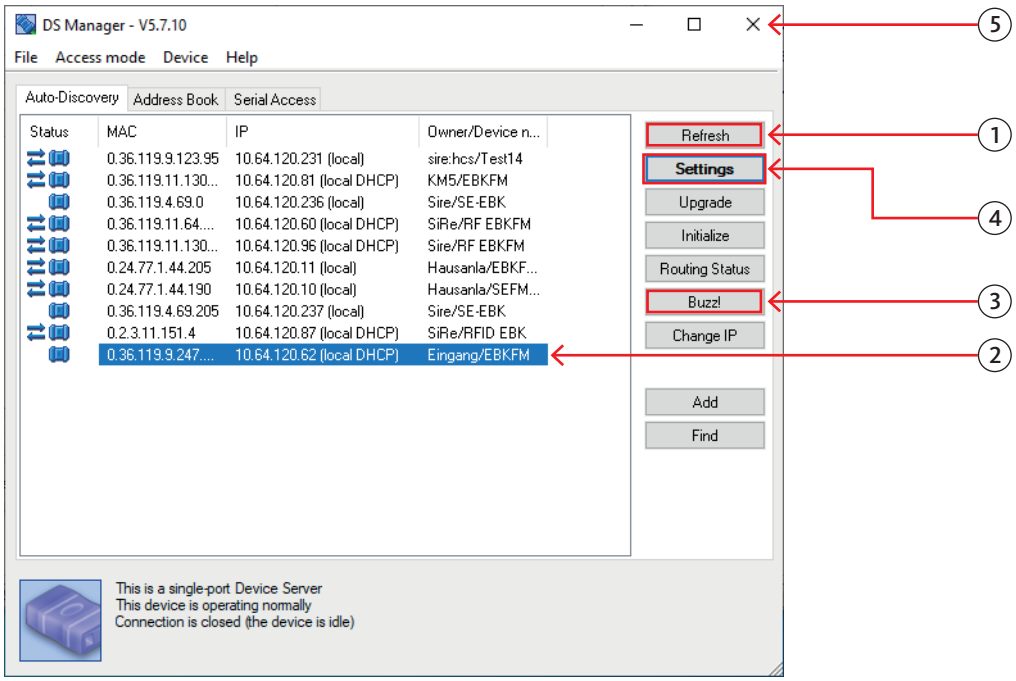
5.7.2.6.1 DS-Manager

Im separaten Fenster „DS-Manager“ wird Ihnen eine Liste der erreichbaren Schnittstellen und den damit verbundenen EBK/EBK FM angezeigt. Es werden auch Schnittstellen angezeigt, die nicht in der Topologie aufgeführt sind. Hierzu werden die Geräte anhand eines TCP/IP-Bausteins in Ihrem Netzwerk gesucht. Damit Sie die nicht angezeigten EBK/EBK FM in die Topologie übernehmen können, ist es erforderlich, dass Sie die Geräte mit dem DS-Manager identifizieren und einrichten.

Je nach Aufbau des Netzwerks ist es möglich, dass ein EBK/EBK FM sich in einem anderen Netzwerksegment befindet und die Verbindung zum Online-Dienst z. B. über ein Gateway ermöglicht wurde. In dieser Konstellation muss das EBK/EBK FM über den Button (D) „Neuen EBK anlegen“ manuell eingerichtet werden

- Zum Öffnen der App drücken Sie auf den Button „DS-Manager“ (C).
- Sollte die Firewall Ihres Windows den Zugriff auf den DS-Manager blockieren, drücken Sie bitte in diesem Dialog auf den Button „Zugriff zulassen“.

Menü des DS-Managers für den Online-Dienst (EBK/EBK FM)



Richten Sie die EBK/EBK FM bzw. die Schnittstellen zur späteren Verwendung in der Topologie im „DS-Manager“ ein. Vor der Einrichtung ist es erforderlich, dass Sie Geräte identifizieren.

- (1) Der Button „Refresh“ aktualisiert die Liste der Schnittstellen. Sollte das zu identifizierende Gerät nicht angezeigt werden, können Sie über diesen Button die Liste der Schnittstellen aktualisieren. Überprüfen Sie ggf. die Anschlüsse und die Erreichbarkeit des Geräts, falls es nicht angezeigt wird.
- (2) Wählen Sie die Schnittstelle des zu identifizierenden EBK/EBK FM aus.

- (3) Zur Überprüfung der richtigen Zuordnung bzw. ob die markierte Schnittstelle und das zu identifizierende EBK/EBK FM zusammengehören, drücken Sie auf den Button „Buzz“. Die LEDs am RJ45-Netzwerkanschluss des EBK/EBK FM leuchten dadurch kurzzeitig auf. Hierdurch wird die Lokalisierung bei mehreren Geräten erleichtert.
- (4) Die gewählte Schnittstelle ist im nächsten Schritt zu Konfigurieren. Drücken Sie auf den Buttons „Settings“. Die weitere Beschreibung entnehmen Sie Kapitel 5.7.2.6.2 [306].
- (5) Schließen Sie das Fenster über den Button „X“ in der linken Kopfzeile.

5.7.2.6.2 Settings im DS-Managers

- Wählen Sie eine Schnittstelle im DS-Manager aus und Drücken Sie auf den Button „Settings“.
- Überprüfen Sie die Einstellungen und drücken auf den Button „OK“

Die Einstellungen der Settings sind voreingestellt. Optional können Sie im Register Network folgende Einstellungen bei Bedarf anpassen.

Register Network

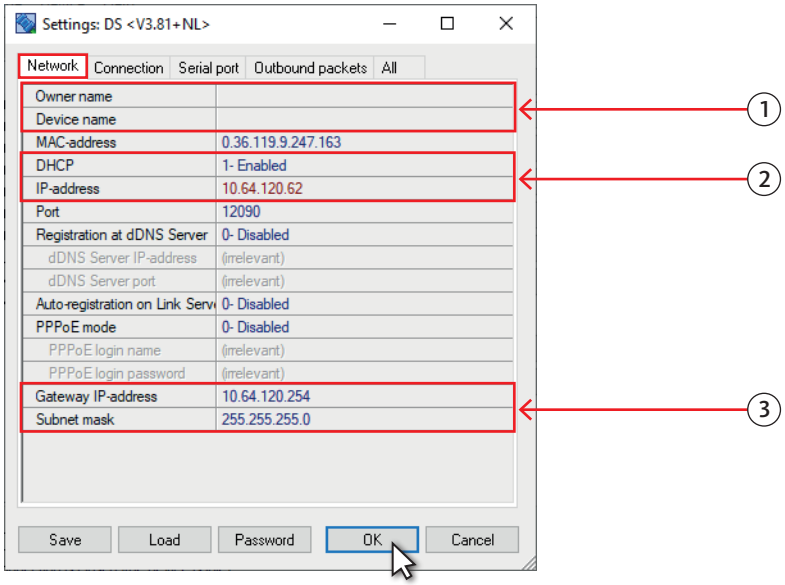
(1) Angaben zum EBK/EBK FM in den Feldern „Owner name:“ und „Device Name:“.

(2) Manuelle Konfiguration der Netzwerkeinstellungen

– Protokoll:	0 - kein DHCP
	1 - DHCP wird verwendet
– IP-Adresse:	manuelle Eingabe der Adresse
– Port:	12090
	Der Netzwerkport 12090 sollte verwendet werden.

(3) Erweiterte Netzwerkeinstellungen

– Gateway IP-adress: / Subnet mask:

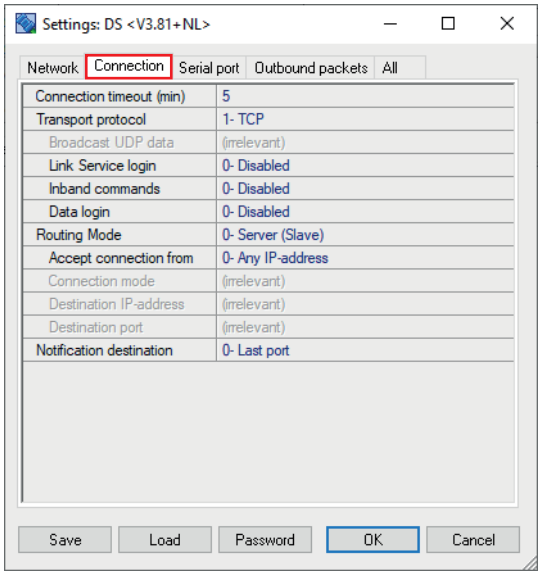


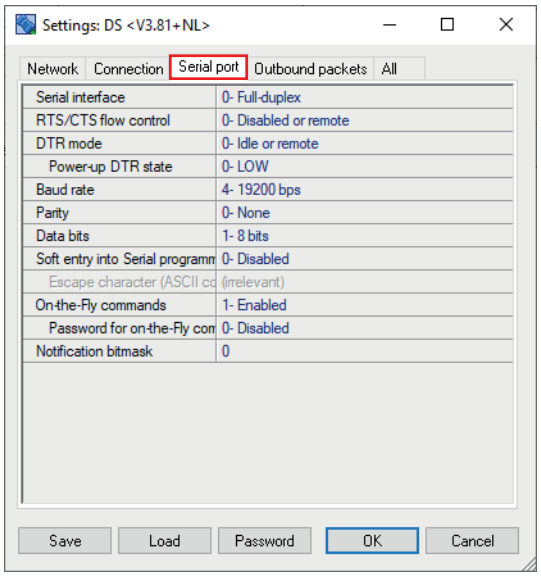
Register Connection | Serial Port | Outbound packets | All

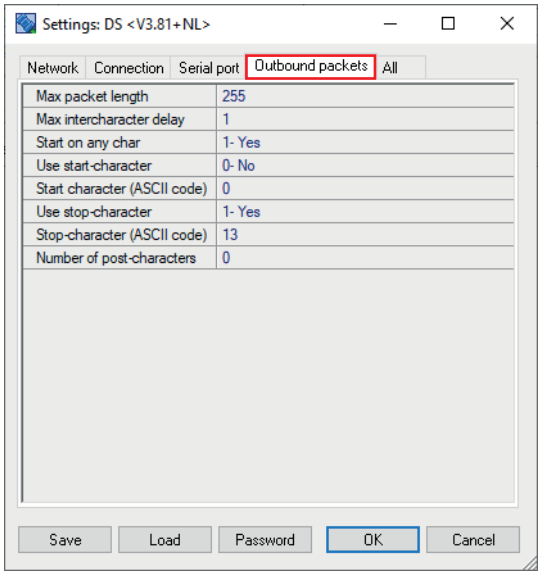
In den weiteren Registern des Menüs „Settings“ sind die Einstellungen vordefiniert. Mithilfe der folgenden Abbildungen können Sie ggf. Änderungen auf die vordefinierten Einstellungen zurückstellen. Im Register „All“ erhalten Sie eine Übersicht als Zusammenfassung, um alle Inhalte der Register in einer Ansicht zu haben.

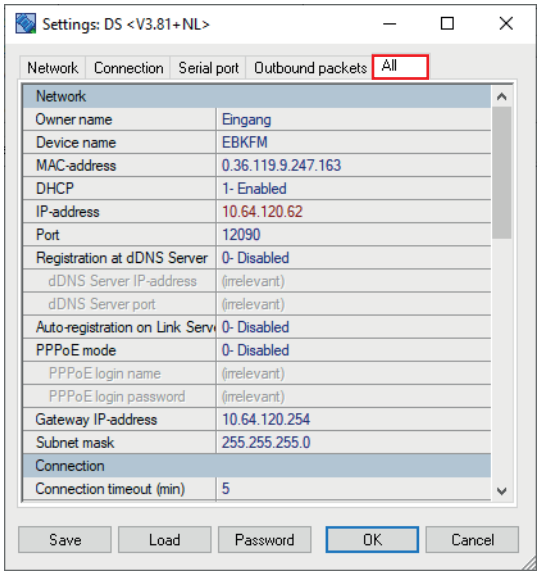
HINWEIS

Die Einstellungen der folgenden Register sind vordefiniert und sollten nicht bzw. aus einem triftigen Grund verändert werden. Wenn z. B. der Ethernetbuskoppler nicht in der Topologie aktivierbar sein sollte, könnte die Fehlerbehebung das Ändern der Einstellungen in die der unten abgebildeten Register sein.





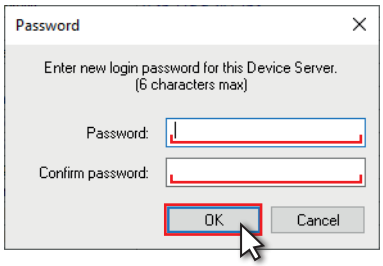




Optional können Sie den unbefugten Zugriff auf die Einstellungen des Menüs „Settings“ zur gewählten Schnittstelle/Gerät durch die Vergabe eines Passworts verhindern.

■ Drücken Sie hierzu auf den Button „Password“.

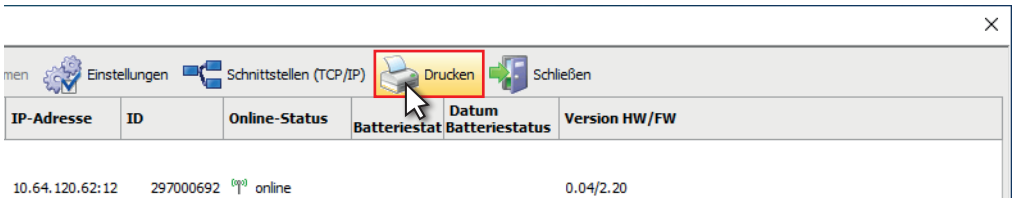
HINWEIS **Nach Festlegung des Passworts sind Änderungen in den Settings nur mit einer Authentifizierung durch das Passwort möglich. Das Passwort ist im Nachhinein nicht mehr veränderbar.**



5.7.2.7 Drucken und Schließen der Online-Konfiguration

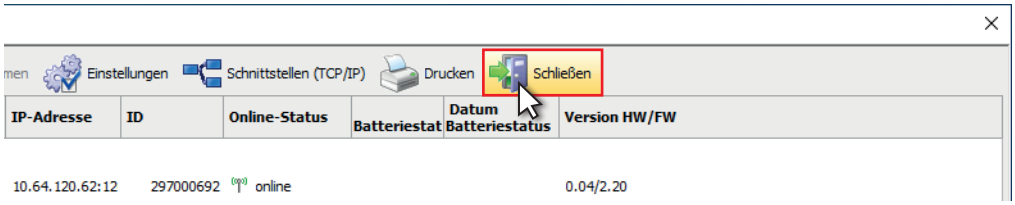
Ausdruck der Liste Topologie der online verbundenen Komponenten mit Status

■ Drücken Sie auf den Button „Drucken“.



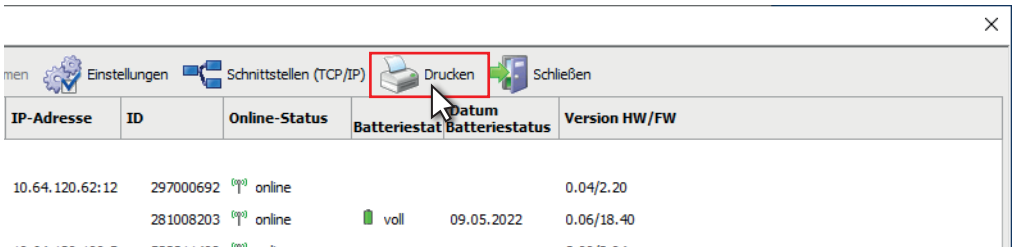
Beenden der Online-Konfiguration

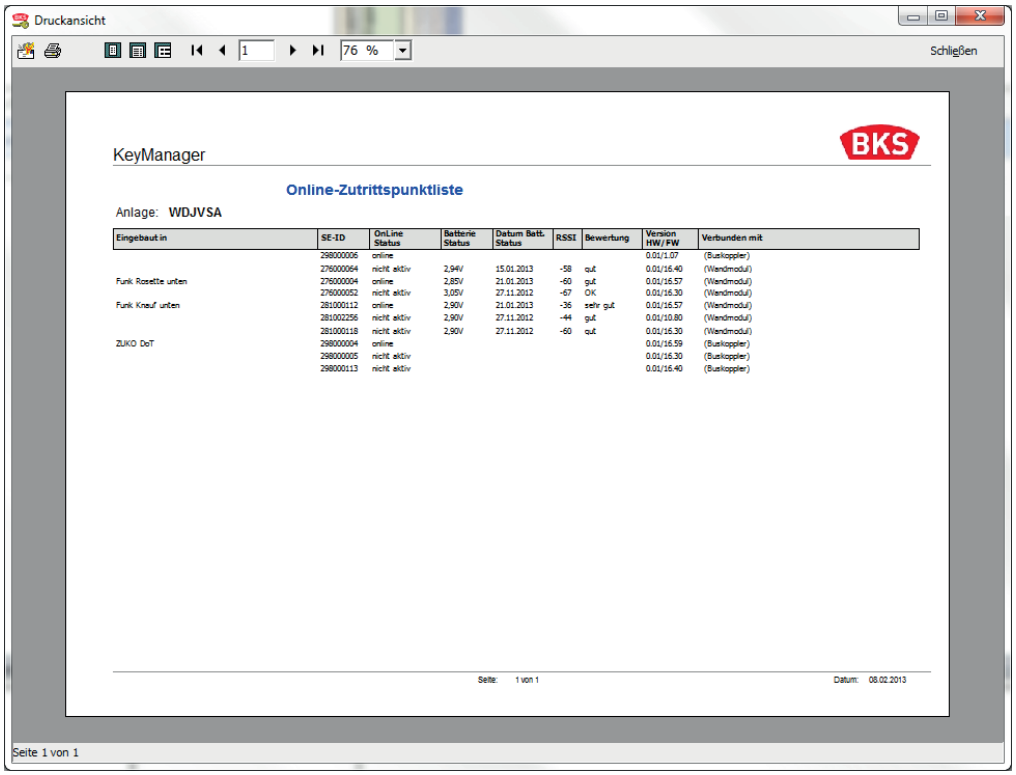
■ Drücken Sie auf den Button „Schließen“.



5.7.2.7.1 Druckansicht

- Drücken Sie auf den Button „Drucken“, um von der aktuell gezeigten Liste einen Ausdruck zu erstellen.



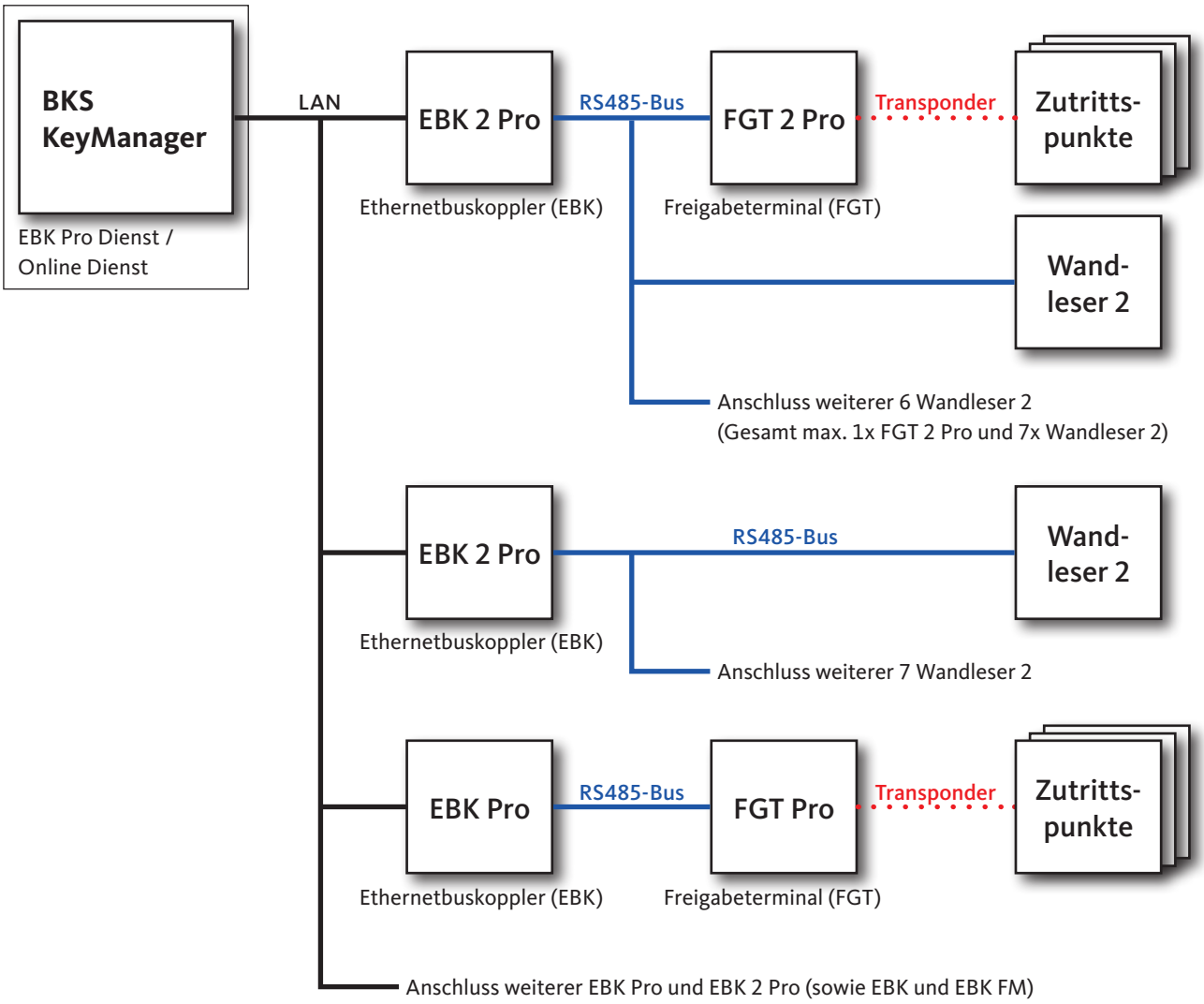


5.7.3 Konfiguration einer Data on Transponder-Anlage (DoT) mit Freigabeterminal (FGT)

Voraussetzung der Einbindung der Online-Komponenten in die Schließanlage des BKS KeyManagers ist die Einrichtung in der Online-Konfiguration. Über die Topologie und den weiteren Funktionen wird der EBK Pro-Dienst dabei zur Vernetzung der Ethernetbuskoppler und Freigabeterminals mit dem BKS KeyManager eingerichtet.

- Ein kombinierter Betrieb von EBK, EBK FM, EBK Pro und EBK 2 Pro ist möglich!
- Der EBK Pro-Dienst und der Online-Dienst können parallel betrieben werden!

5.7.3.1 Systemübersicht DoT-Anlage mit FGT



- Freigabeterminal 2 Professional (FGT 2 Pro)
  - Beim Buchen des Transponders werden die Zutrittsberechtigungen aktualisiert und Ereignisse im Transponder ausgelesen
  - Optional verfügt das FGT 2 Pro über die Funktion „Wandleser-Modul“. Nach Aktivierung dieser wird die Zutrittsberechtigung abgefragt und der Transponder öffnet bei entsprechender Berechtigung den Zugangspunkt per Schaltkontakt

- Wandleser 2
  - Die Zutrittskontrolle öffnet einen Zugangspunkt per Schaltkontakt beim Buchen eines berechtigten Transponders.

Anschlussoptionen FGT 2 Pro, Wandleser 2
- Anschlussoption bei Installation in einem sicheren Bereich ist der direkte Anschluss der Steuerung des Zutrittspunkts an den Relaiskontakten
- Anschlussoption bei Installation in einem ungeschützten Bereich ist die sichere Übertragung über den RS485-Bus zu einem im gesicherten Bereich installierten ixalo Relaismodul

- Freigabeterminal Professional (FGT Pro)
  - Beim Buchen des Transponders werden die Zutrittsberechtigungen aktualisiert und Ereignisse im Transponder gespeichert.

5.7.3.2 Installation für eine DoT-Anlage mit FGT

Wir empfehlen die Verwendung der folgenden Installationsvariante des BKS KeyManagers, um eine DoT-Anlage mit FGT zu verwalten.

- Einzelplatz- und Serverversion mit Microsoft SQL Server
  - Folgen Sie der Anleitung im Kapitel 2.2 [18]

- Ethernetbuskoppler Professional-Dienst (EBK Pro-Dienst)
  - Folgen Sie der Anleitung im Kapitel 2.8 [57]

Alternativ ist beim Client/Server-Betrieb folgende Installationsvariante zu wählen.

- Clients der Netzwerkversion
  - Folgen Sie der Anleitung im Kapitel 2.3 [32]

- Server der Netzwerkversion
  - Folgen Sie der Anleitung im Kapitel 2.5 [47]

  Ethernetbuskoppler Professional-Dienst (EBK Pro-Dienst)
  - Folgen Sie der Anleitung im Kapitel 2.8 [57]

Installationsparameter
Während der Installation werden Sie im Dialog durch die Installation geführt. Folgende Parameter sollten bei der Installation gesetzt werden.

- In der Auswahl des Setuptypes aktivieren Sie die Checkbox „SE-Online-Modul installieren“, um den KeyManager Online-Service Manager mit in die Installation einzuschließen

- Bei der Verbindungseinstellung des EBK Professional-Dienst ist im Feld „Anlage:“ die Anlagenbezeichnung der Schließanlage (zu finden z. B. auf Ihrer Sicherungskarte) einzugeben.

5.7.3.3 Erforderliche Lizenz-Erweiterung der Schließanlage (DoT mit FGT)

Die Schließanlage benötigt die folgenden Lizenzen, um als DoT-Anlage mit FGT betrieben werden zu können.

- SE-Lizenz Free, Standard oder Professional
- SE-Lizenz Data on Transponder
- Wird in der Anlage die Kombination EBK (ohne Pro) mit Wandleser eingesetzt, wird eine SE-Lizenz Online zum Betrieb benötigt

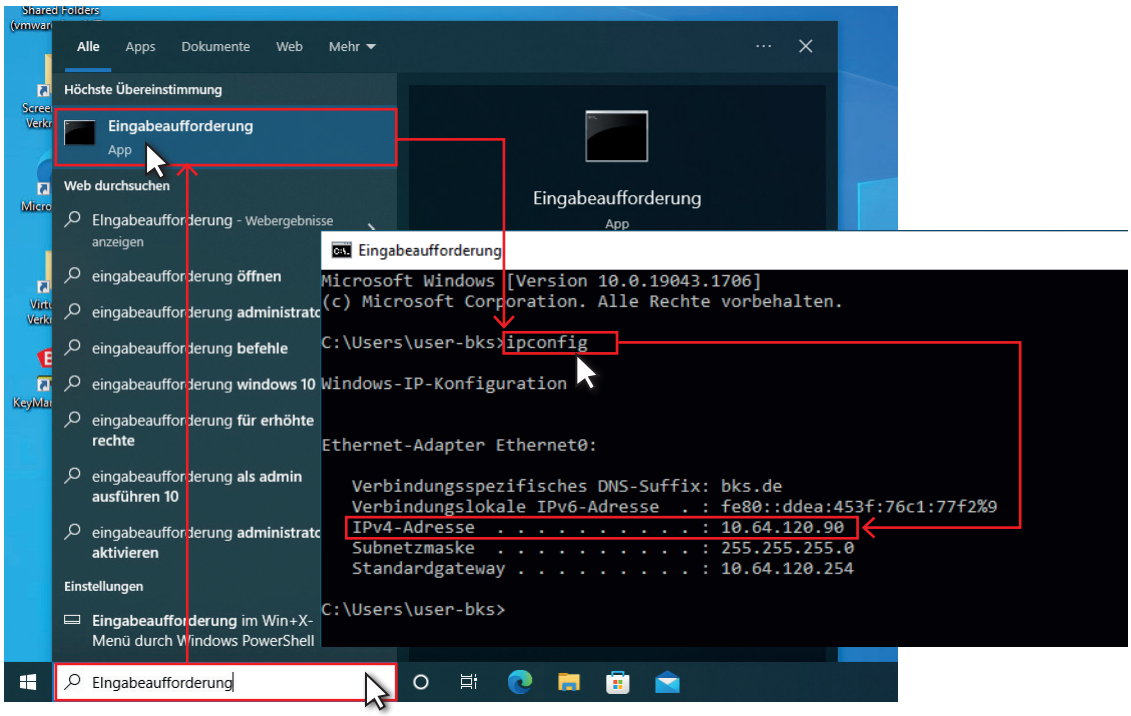
Während des Anlegens der Schließanlage werden Sie, wie im Kapitel 5.4 [272] beschrieben, im Dialog aufgefordert die Lizenzen zu laden.
Wurde dieser Schritt bei der Einrichtung übersprungen oder sollen in einer vorhandenen Schließanlage die erforderlichen Lizenzen nachträglich erweitert bzw. geladen werden, folgen Sie der Anweisung im Kapitel 5.3 [269].

- Lesen Sie die erforderlichen Lizenzen nacheinander ein.

5.7.3.4 Identifikation der IP-Adresse des BKS KeyManagers

Zur Einrichtung des Ethernetbuskopplers benötigen Sie die IP-Konfiguration des Computers, auf dem der BKS KeyManager installiert ist bzw. beim Client/Server-Betrieb die IP-Konfiguration des Servers.

- Öffnen Sie die App „Eingabeaufforderung“ über das Feld „Suche“. Geben Sie zum Starten im Eingabefeld „Eingabeaufforderung“ ein und drücken die „Enter-Taste“.
  Alternativ startet die App über die Tastenkombination „Windows-Taste“ und „r“, der Eingabe von „cmd“ im Feld „Ausführen“ sowie der „Enter-Taste“.
- Geben Sie den Befehl „ipconfig“ in der Zeile ein und drücken die „Enter-Taste“.
- Notieren Sie sich die angezeigte IP-Adresse von der Zeile „IPv4-Adresse:“ und ggf. die weitere IP-Konfiguration.



5.7.3.5 Systemstatus des EBK Pro-Dienstes

Zum Betreiben des Online-Moduls sind der Online-Dienst und/oder der EBK Pro-Dienst notwendig, um die Daten vom BKS KeyManager an die online angebundenen Zutrittspunkte oder Freigabeterminals über Ethernetbuskoppler übermitteln zu können. Den Status des Online-Dienstes können Sie wie im Kapitel 5.7.1 [293] beschrieben prüfen und ggf. Korrekturen durchführen. Zur Einrichtung des Online-Moduls dient das Menü Online-Konfiguration.

HINWEIS

Überprüfen Sie den Systemstatus des EBK Pro-Dienstes im Online-Service Managers. Der EBK Pro-Dienst muss „gestartet“ und in allen Instanzen „aktiv“ bzw. „OK“ sein. Folgen Sie der Anleitung im Kapitel 5.7.1.1 [294] .

5.7.3.6 Konfiguration der Ethernetbuskoppler und Freigabeterminals

Vor der Einrichtung im BKS KeyManager müssen die Online-Komponenten ordnungsgemäß in der Schließanlage installiert werden. Für den Einbau und die Verkabelung beachten Sie die jeweils zum Produkt gehörende Anleitung. Schließen Sie die Komponenten erst nach vollendeten Einbau an die Spannungsversorgung an.

Die Online-Komponenten müssen für die elektronische Schließanlage in einem eigenen Netzwerk (z. B. VLAN) zur Verfügung stehen. Hierbei ist zu beachten, das sich alle Komponenten im gleichen Netzwerksegment befinden und eine eigene IP-Adresse haben bzw. diese zugewiesen wurde.

Das Netzwerk inklusive Firewalls, Switches, Virenscanner etc. ist so zu konfigurieren, dass die Kommunikation über die unten angegebenen Ports jederzeit möglich ist. Das Netzwerk sollte zur Sicherheit ausschließlich für das elektronische Schließsystem verwendet werden.

Online-Komponenten	**Anleitung | Datenblatt**
EBK Pro	C59501172
FGT Pro	C59501171
EBK 2 Pro	C59501267 C59501285
FGT 2 Pro	C59501267
Wandleser 2	C59501203
Relaismodul	C59501258
EBK	C59501138
EBK FM	C59501138
FGT	C59501152

Die Online-Komponenten werden erst nach der Einrichtung für die Schließanlage in der Topologie angezeigt. Das EBK Pro und EBK 2 Pro verfügen hierzu über einen integrierten Webserver zur Konfiguration der Systemeinstellungen.

Im Auslieferungszustand sind die Ethernetbuskoppler folgendermaßen konfiguriert.

EBK/EBK FM	DHCP ein
EBK Pro	DHCP ein, Fallback 192.168.0.10
EBK 2 Pro	DHCP off, IP 192.168.0.10

5.7.3.6.1 Konfiguration des EBK 2 Pro

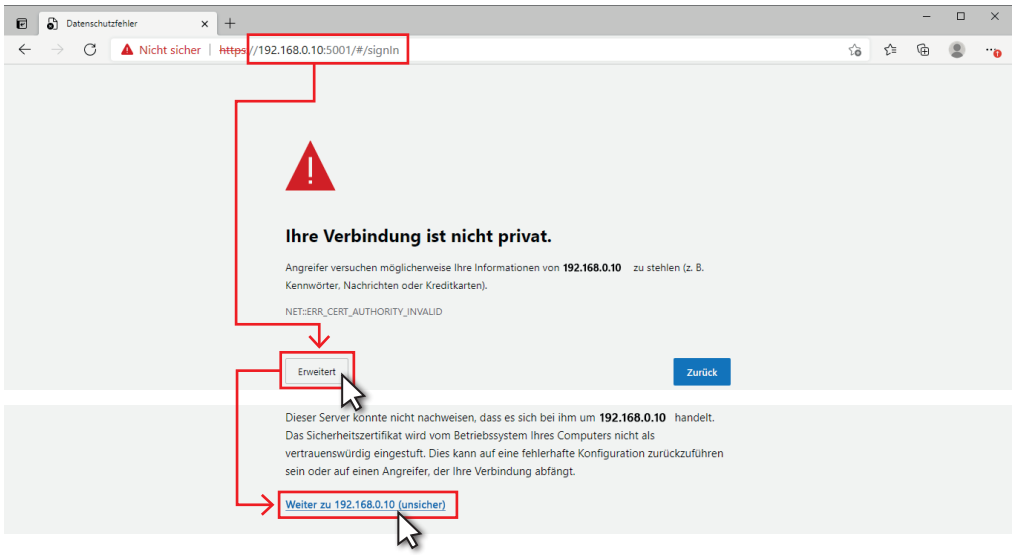
Erstinbetriebnahme und Inbetriebnahme mit fester IP

Für die Erstinbetriebnahme ist eine IP-Adresse voreingestellt. Geben Sie diese oder die Ihnen bekannte feste IP-Adresse des EBK 2 Pro in die Adresszeile Ihres Webbrowsers ein. Sollten Sie die feste IP-Adresse bei der Konfiguration ändern, ist es ratsam, die neue IP zu dokumentieren.
Bei Ersteinbetriebnahme geben Sie die folgende Adresse ein.

- https://192.168.0.10:5001/#/signIn

Beim ersten Aufruf des Webservers wird Ihnen eine Sicherheitsmeldung angezeigt.

- Drücken Sie auf den Button „Erweitert“ und den Link „weiter zu ... (unsicher)“, um zur Anmeldung zu gelangen.

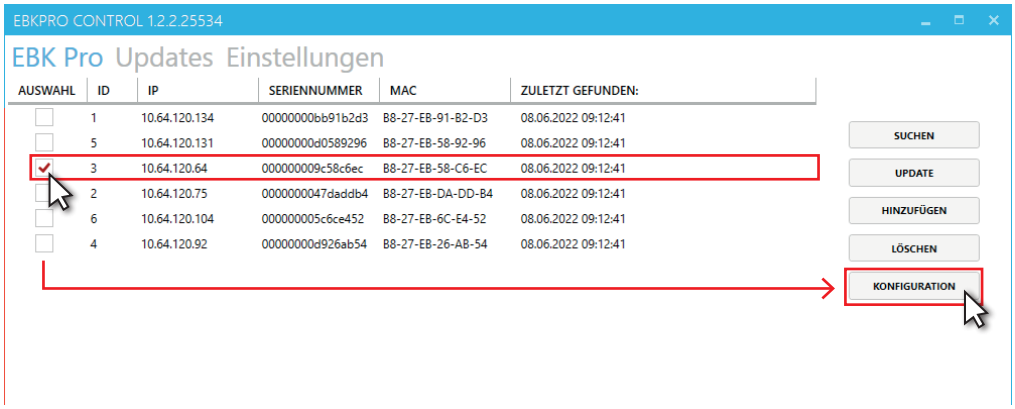


Inbetriebnahme im Netzwerk mit DHCP-Server

Um die unbekannte IP-Adresse eines EBK 2 Pro z. B. in einem Netzwerk mit DHCP-Server zu ermitteln, können Sie die App „EBK Pro Control“ verwenden. In diesem Fall können Sie die App über unseren Support anfragen.

Nach dem Start der App wird im Netzwerk nach verfügbaren EBK 2 Pro gesucht.

- Wählen Sie das zu konfigurierende EBK 2 Pro in der Liste aus und drücken auf den Button „Konfiguration“.



Anmeldung auf dem Webbrowser

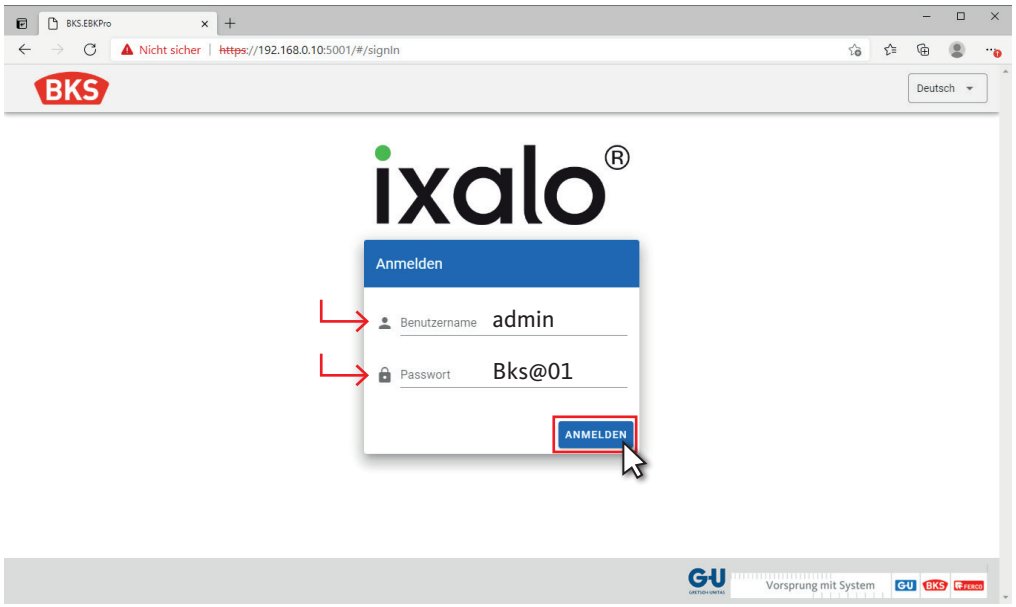
- Für die Anmeldung nutzen Sie die folgenden Daten.

  Login: admin

  Passwort: Bks@01

Ändern Sie ggf. unter dem Register „Benutzerdaten“ die Daten zur Authentifizierung.

- Drücken Sie auf den Button „Anmelden“.

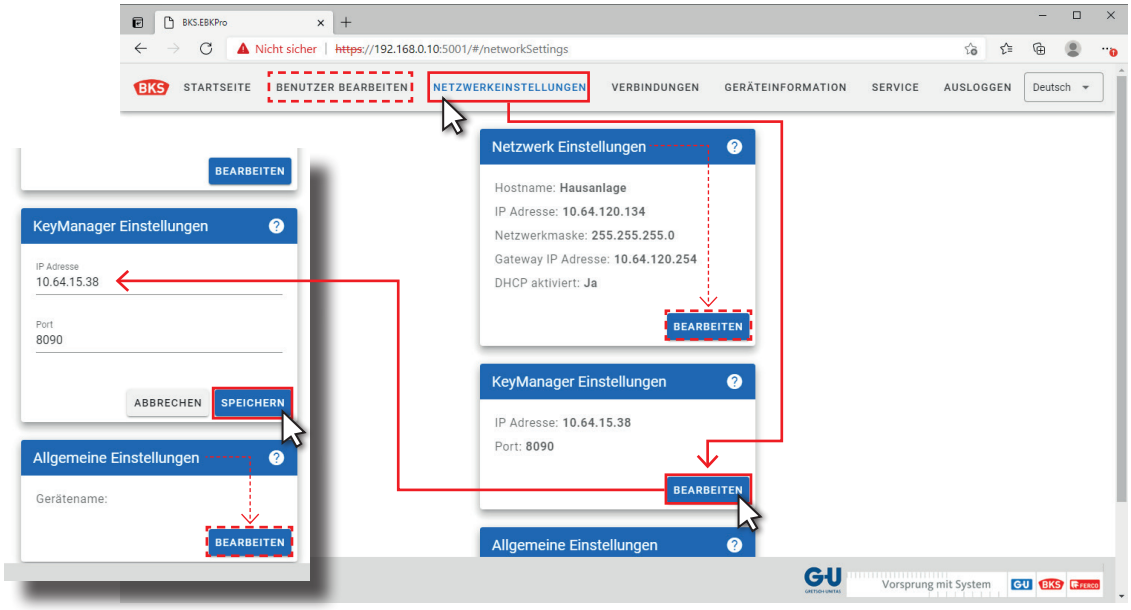


- Wählen Sie das Register „Netzwerkeinstellungen“ aus. Scrollen Sie die Ansicht zu den Eingabezeilen.
- Im Feld „KeyManager Einstellungen“ geben Sie im Feld „KeyManager-Server-IP“ die wie im Kapitel 5.7.3.4 [312] beschrieben ermittelte IP-Adresse ein. Drücken Sie auf „Bearbeiten“ und nach der Eingabe auf „Speichern“, um die Änderungen zu übernehmen.
- Im Feld „Allgemeine Einstellungen“ können Sie optional für das EBK Pro einem Namen vergeben, um die Zuordnung zu erleichtern. Drücken Sie auf „Bearbeiten“ und nach der Eingabe auf „Speichern“, um die Änderungen zu übernehmen.

Sollten die Gegebenheiten Ihres Netzwerks es erforderlich machen, die Funktion DHCP in der entsprechenden Checkbox zu deaktivieren, ist auch die IP-Adresse von Ihnen manuell einzutragen.

Die physikalische Adresse (MAC) sowie die Seriennummer werden nur angezeigt und können nicht verändert werden.

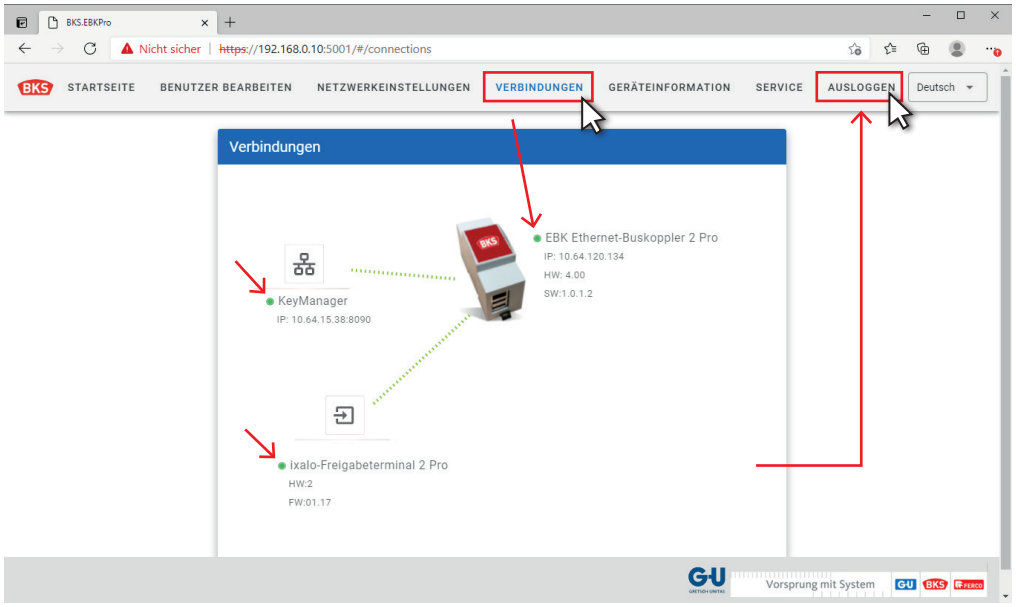
- Im Feld „Allgemeine Einstellungen“ können Sie optional die Netzwerkeinstellungen anpassen, wenn der DHCP-Dienst deaktiviert werden soll. Drücken Sie auf „Bearbeiten“ und nach der Eingabe auf „Speichern“, um die Änderungen zu übernehmen.



■ Wählen Sie das Register „Verbindungen“ aus.

Überprüfen Sie in dieser Ansicht den Status der Verbindungen zwischen dem EBK 2 Pro und den angeschlossenen Komponenten. Wird eine Verbindung z. B. als „kein Gerät verbunden“ angezeigt, sollten Sie zu den betreffenden Abschnitt der Konfiguration wechseln und die Einstellungen korrigieren.

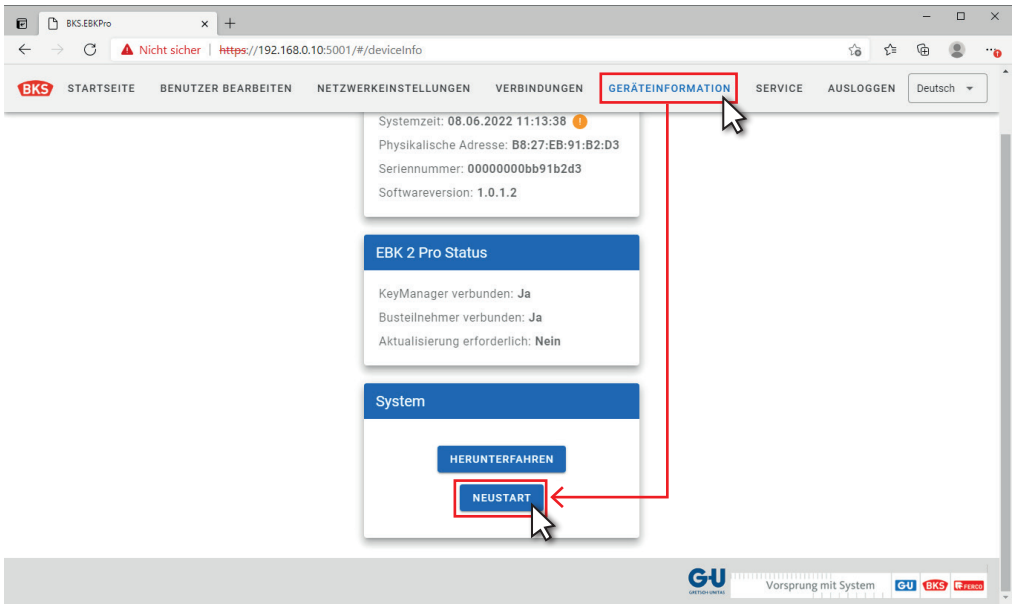
■ Drücken Sie auf den Button „Ausloggen“ zum Verlassen des EBK-Webbrowsers.



Wird trotz korrekter Eingaben und Anschluss zwischen den Komponenten keine Verbindung aufgebaut, kann ein Neustart des EBK 2 Pro evtl. dieses Problem beheben.

■ Wählen Sie das Register „Geräteinformationen“ aus. Scrollen Sie die Ansicht zur Zeile „System“.

■ Drücken Sie auf den Button „Neustart“.



5.7.3.6.2 Konfiguration des EBK Pro

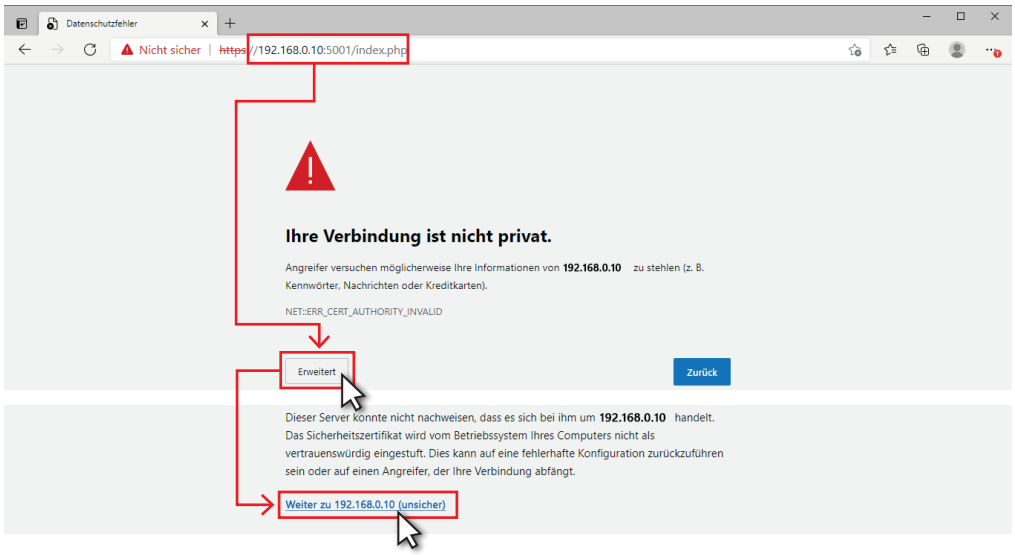
Erstinbetriebnahme und Inbetriebnahme mit fester IP

Für die Erstinbetriebnahme ist eine IP-Adresse voreingestellt. Geben Sie diese oder die Ihnen bekannte feste IP-Adresse des EBK Pro in die Adresszeile Ihres Webbrowsers ein. Sollten Sie die feste IP-Adresse bei der Konfiguration ändern, ist es ratsam, die neue IP zu dokumentieren.
Bei Ersteinbetriebnahme geben Sie die folgende Adresse ein.

- https://192.168.0.10/index.php

Beim ersten Aufruf des Webservers wird Ihnen eine Sicherheitsmeldung angezeigt.

- Drücken Sie auf den Button „Erweitert“ und den Link „weiter zu ... (unsicher)“, um zur Anmeldung zu gelangen.

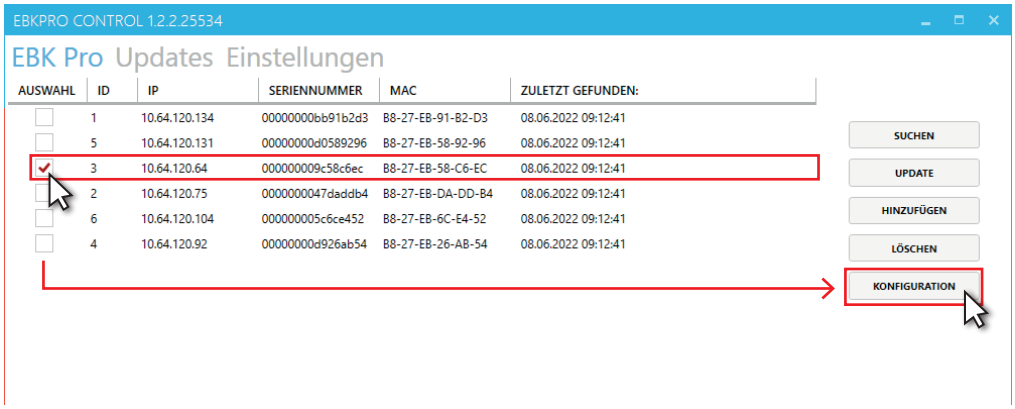


Inbetriebnahme im Netzwerk mit DHCP-Server

Um die unbekannte IP-Adresse eines EBK Pro z. B. in einem Netzwerk mit DHCP-Server zu ermitteln, können Sie die App „EBK Pro Control“ verwenden. In diesem Fall können Sie die App über unseren Support anfragen.

Nach dem Start der App wird im Netzwerk nach verfügbaren EBK Pro gesucht.

- Wählen Sie das zu konfigurierende EBK Pro in der Liste aus und drücken auf den Button „Konfiguration“.



Anmeldung auf dem Webbrowser

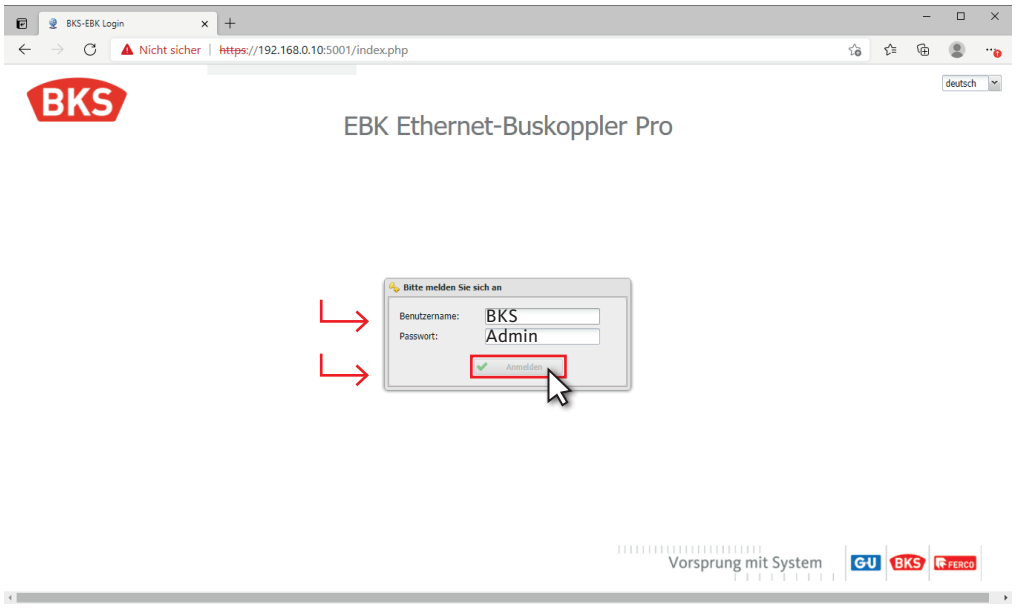
- Für die Anmeldung nutzen Sie die folgenden Daten.

  Benutzername: BKS

  Passwort: Admin

Ändern Sie ggf. unter dem Register „Benutzer“ die Daten zur Authentifizierung.

- Drücken Sie auf den Button „Anmelden“.



- Wählen Sie das Register „Einstellungen“ aus. Scrollen Sie die Ansicht zu den Eingabezeilen.
- Geben Sie im Feld „KeyManager-Server-IP“ die wie im Kapitel 5.7.3.4 [312] beschrieben ermittelte IP-Adresse ein.
- Optional können Sie für das EBK Pro einem Namen vergeben.

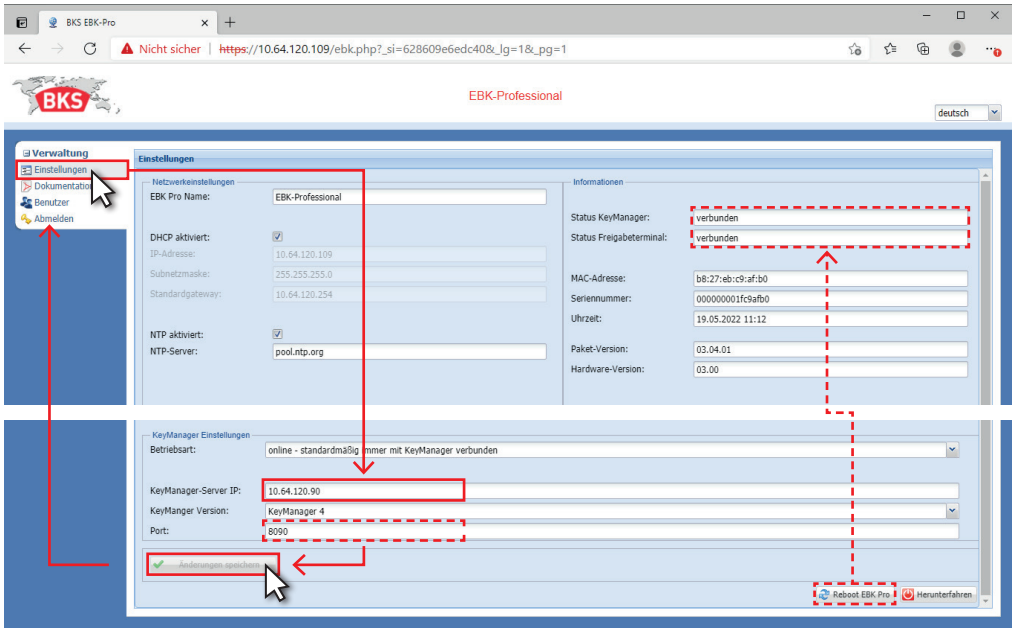
Sollten die Gegebenheiten Ihres Netzwerks es erforderlich machen, die Funktion DHCP in der entsprechenden Checkbox zu deaktivieren, ist auch die IP-Adresse von Ihnen manuell einzutragen.

Die physikalische Adresse (MAC) sowie die Seriennummer werden nur angezeigt und können nicht verändert werden.

- Drücken Sie auf den Button „Änderungen speichern“.

Das Feld „Status KeyManager“ und „Status Freigabeterminal“ zeigt den aktuellen Zustand der Verbindung an. Wechselt die Anzeige trotz korrekter Eingaben und Anschluss nicht auf „verbunden“, kann ein Neustart des EBK Pro evtl. dieses Problem beheben.

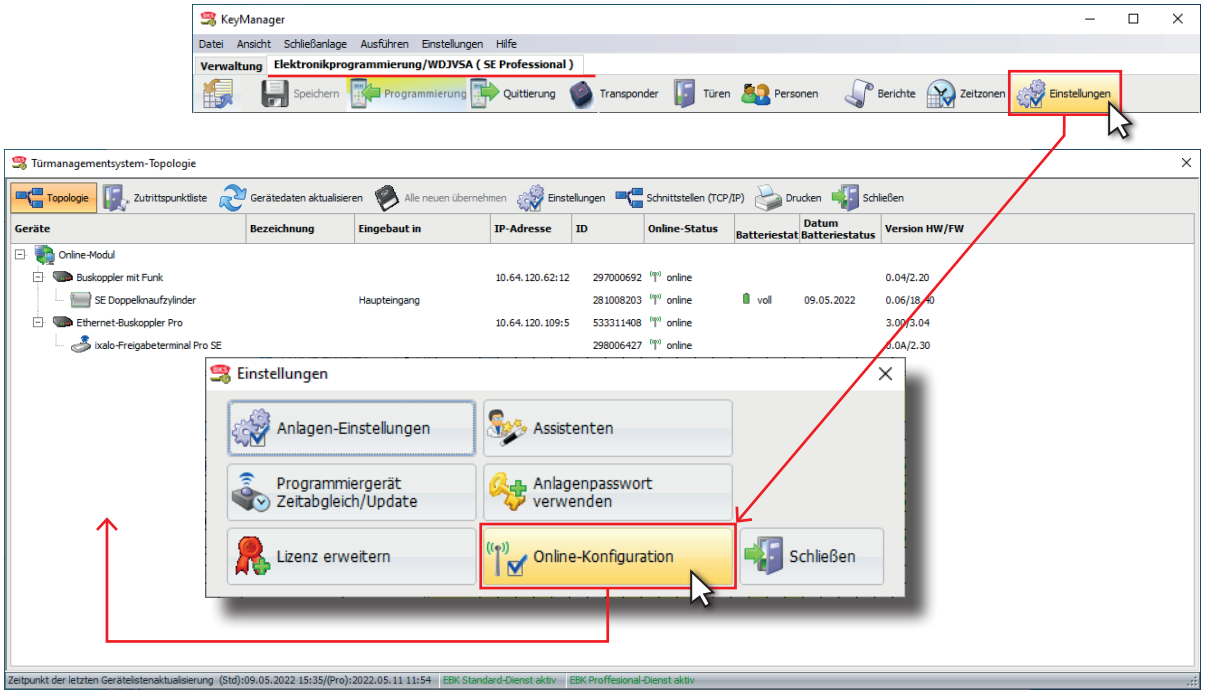
- Drücken Sie für den Neustart auf den Button „Reboot EBK Pro“.



5.7.3.6.3 Freigabeterminal (FGT), Wandleser 2 und Ixalo Relaismodul

In der Topologie des Online-Dienstes werden die in der Schließanlage vorhanden Online-Komponenten angezeigt. Im Weiteren können diese konfiguriert werden.

- Wählen Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ den Menüpunkt „Einstellungen“ aus.
- Drücken Sie auf den Button „Online-Konfiguration“.



Weitere Einrichtungen und Konfigurationen an den Online-Komponenten können Sie in der Topologie des Online-Dienstes fertigstellen. Folgen Sie der Anleitung im Kapitel 5.7.2.1 [297]. Beachten Sie die folgenden Informationen zu den Komponenten.

FGT 2 Pro

Das FGT 2 Pro kann der Schließanlage mit der alleinigen Funktion als Freigabeterminal oder als Kombinationsgerät mit der zusätzlichen Funktionalität eines Wandlesers hinzugefügt werden.

Nach der Konfiguration des FGT 2 Pro und EBK 2 Pro können Sie in der Topologie das Kontextmenü des neuen FGT 2 Pro öffnen und eine der folgenden Einstellungen wählen.

- Menüpunkt „nur FGT übernehmen (ohne WL-Funktion)“
  - Das FGT 2 Pro wird nur als Freigabeterminal verwendet und folglich nicht in der Berechtigungsmatrix eingefügt bzw. angezeigt
- Menüpunkt „Zutrittspunkt übernehmen“
  - Das FGT 2 Pro hat zusätzlich die Funktion Wandleser und wird im weiteren Dialog als neuer Zutrittspunkt in der Berechtigungsmatrix angelegt. Der Wandleser überprüft beim Buchen des Transponders zusätzlich die Zutrittsberechtigung und kann mit dieser Information eine Türsteuerung auslösen

Während des Betriebs der Schließanlage kann die Funktion des Wandlesers in der Topologie ein- oder ausgeschaltet werden. Im Kontextmenü des FGT 2 Pro wählen Sie die Eigenschaften aus und aktivieren oder deaktivieren die Checkbox „Wandleser aktiv“

FGT Pro

Das FGT Pro wird nach erfolgreicher Einrichtung der Konfiguration automatisch in die Liste der Topologie übernommen.

Wandleser 2

Nach der Konfiguration des Wandleser 2 online und EBK 2 Pro können Sie in der Topologie das Kontextmenü des neuen Wandleser 2 öffnen und die folgenden Einstellung wählen.

- Menüpunkt „Zutrittspunkt übernehmen“
  - Der Wandleser 2 wird im weiteren Dialog als neuer Zutrittspunkt in der Berechtigungsmatrix angelegt. Der Wandleser überprüft beim Buchen des Transponders die Zutrittsberechtigung und kann mit dieser Information eine Türsteuerung auslösen.

Ixalo Relaismodul

Das Ixalo Relaismodul dient zur Verlagerung der Schaltfunktion des FGT 2 Pro mit aktivem Wandleser-Modul oder des Wandlesers 2 über eine gesicherte Datenübertragung (BUS-Verbindung) in einen gesicherten Bereich zu übertragen und dort auszuführen. Die Ausgänge am Relais-Modul entsprechen den Funktionen der Ausgänge der Zutrittskontrolle. Im BKS KeyManager wird das Ixalo Relaismodul nicht angezeigt.

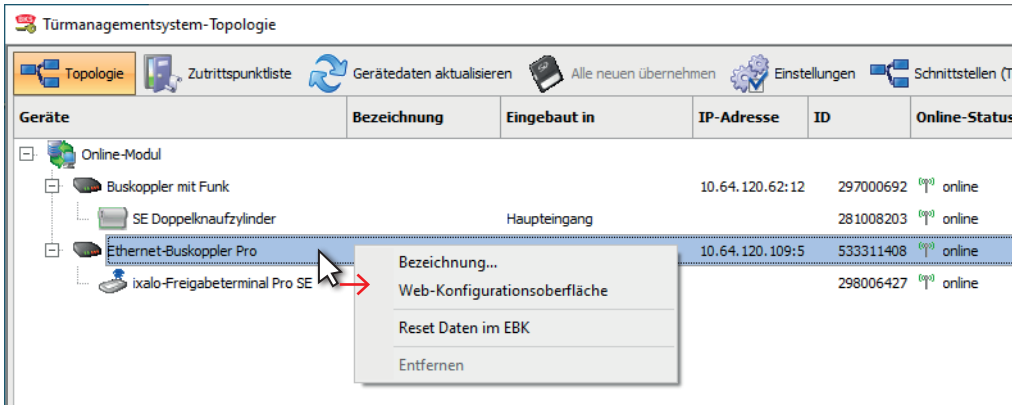
5.7.3.7 Aktualisierung der Topologie

Im BKS KeyManager werden Sie nach Abschluss der Konfiguration aufgefordert, die Topologie zu Aktualisieren.

- Drücken Sie auf den Button „Online-Konfiguration“, um zur Topologie zu gelangen.

Nach erfolgreicher Konfiguration der Komponenten des EBK Pro-Dienstes werden Ihnen diese in der Liste nach dem Öffnen der Topologie mit dem Status „Online“ angezeigt. Wird eine Komponente nicht oder mit einer Fehlermeldung anzeigt, ist die Konfiguration der Komponente und des EBK Pro-Dienstes zu prüfen und zu korrigieren.

- Über die Kontextmenüs der einzelnen Komponenten können Sie noch weitere Änderungen und Einstellungen vornehmen.

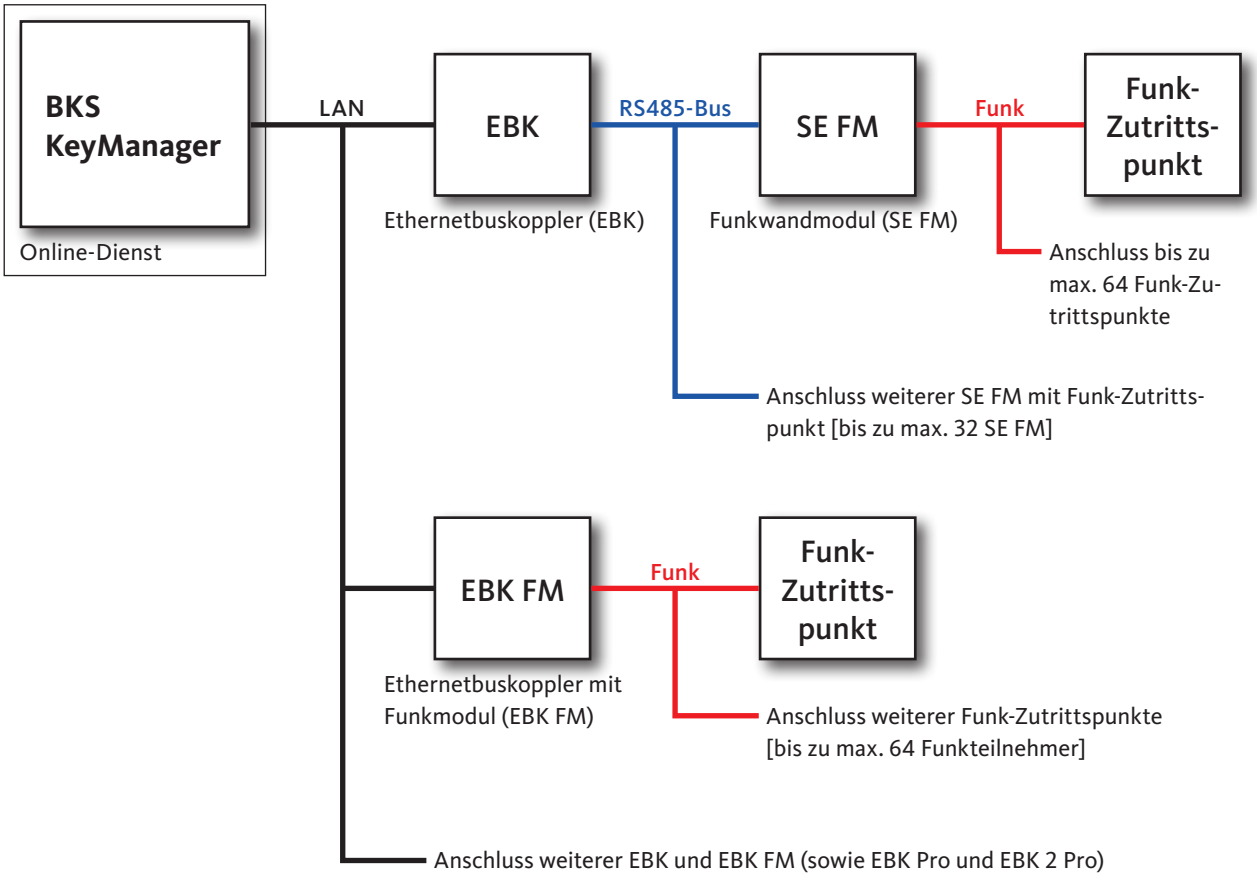


5.7.4 Konfiguration einer Online-Anlage

Voraussetzung der Einbindung der Online-Komponenten in die Schließanlage des BKS KeyManagers ist die Einrichtung in der Online-Konfiguration. Über die Topologie und den weiteren Funktionen wird der Online-Dienst dabei zur Vernetzung der Ethernetbuskoppler und Funk-Zutrittspunkten mit dem BKS KeyManager eingerichtet.

- Der Online-Dienst und der EBK Pro-Dienst können parallel betrieben werden!

5.7.4.1 Systemübersicht Online-Anlage



5.7.4.2 Installation für eine Online-Anlage

Wir empfehlen die Verwendung der folgenden Installationsvariante des BKS KeyManagers, um eine Online-Anlage zu verwalten.

- Einzelplatz- und Serverversion mit Microsoft SQL Server
  – Folgen Sie der Anleitung im Kapitel 2.2 [18]

Alternativ ist beim Client/Server-Betrieb folgende Installationsvariante zu wählen.

- Clients der Netzwerkversion
  – Folgen Sie der Anleitung im Kapitel 2.3 [32]
- Server der Netzwerkversion
  – Folgen Sie der Anleitung im Kapitel 2.5 [47]

Installationsparameter
Während der Installation werden Sie im Dialog durch die Installation geführt. Folgende Parameter sollten bei der Installation gesetzt werden.

- In der Auswahl des Setuptypes aktivieren Sie die Checkbox „SE-Online-Modul installieren“, um den KeyManager Online-Service Manager mit in die Installation einzuschließen und die Checkbox „Aktivieren SQL Server TCP“, um den Microsoft SQL Server während der Installation automatisch zu konfigurieren.

5.7.4.3 Erforderliche Lizenz-Erweiterung der Schließanlage (Online)

Die Schließanlage benötigt folgende Lizenzen, um als Online-Anlage betrieben werden zu können.

- SE-Lizenz Free, Standard oder Professional
- SE-Lizenz Online

Während des Anlegens der Schließanlage werden Sie, wie im Kapitel 5.4 [272] beschrieben, im Dialog aufgefordert die Lizenzen zu laden.
Wurde dieser Schritt bei der Einrichtung übersprungen oder sollen in einer vorhandenen Schließanlage die erforderlichen Lizenzen nachträglich erweitert bzw. geladen werden, folgen Sie der Anweisung im Kapitel 5.3 [269].

- Lesen Sie die erforderlichen Lizenzen nacheinander ein.

5.7.4.4 Systemstatus des Online-Dienstes

Zum Betreiben des Online-Moduls sind der Online-Dienst und/oder der EBK Pro-Dienst notwendig, um die Daten vom BKS KeyManager an die online angebundenen Zutrittspunkte oder Freigabeterminals über Ethernetbuskoppler übermitteln zu können. Den Status des Online-Dienstes können Sie wie im Kapitel 5.7.1 [293] beschrieben prüfen und ggf. Korrekturen durchführen. Zur Einrichtung des Online-Moduls dient das Menü Online-Konfiguration.

HINWEIS

Überprüfen Sie den Systemstatus des Online-Dienstes im Online-Service Managers.
Der Online-Dienst muss „gestartet“ und in allen Instanzen „aktiv“ bzw. „OK“ sein.
Folgen Sie der Anleitung im Kapitel 5.7.1.1 [294].

5.7.4.5 Funk-Zutrittspunkte mit den EBK FM / SE FM verbinden

Damit der BKS KeyManager Daten an die Zutrittspunkte senden kann, müssen die Zutrittspunkte mit einem Ethernetbuskoppler Funk (EBK FM) oder einem Funkwandmodul (SE FM) gepairt sein. Die Installation der RS485-Bus Datenleitungen SE FM sowie die LAN-Infrastruktur für das EBK / EBK FM müssen vorhanden sein.

Bei der Einrichtung der Funkverbindung zwischen den Funk-Zutrittspunkten und dem EBK FM oder EBK mit SE FM wird initial über das Pairing der Geräte ein Sicherheitscode ausgetauscht. Dies ist Grundlage einer sicheren Kommunikation zwischen den Geräten.

Während des Pairing-Vorgangs müssen sich die Komponenten mindestens in Funk-Reichweite oder besser in einer kurzen räumlichen Distanz befinden, um eine gute Verbindung zu gewährleisten.

- Drücken Sie ca. 1 Sekunde auf den Pairingtaster im EBK FM / SE FM zum Starten des Pairingvorgangs.

Nach dem Start der Sequenz sendet das EBK FM / SE FM ca. 5 Minuten lang ein Pairing-Signal in kurzen Abständen aus. Dieser Status wird durch anhaltendes Beepen bzw. rot blinkender Funk-LED angezeigt.

Innerhalb des Pairingzeitraums EBK FM / SE FM muss auch der Funk-Zutrittspunkt in den Pairing-Modus gesetzt werden.

- Bei der Erstinstallation setzen Sie zum Start des Pairings die Batterie in den Funk-Zutrittspunkt ein.
- Ist die Komponente schon einmal gepairt gewesen, folgen Sie der Anleitung des betreffenden Funk-Zutrittspunkts, um den Pairingvorgang zu starten.

Nach dem Start des Pairing-Modus im Funk-Zutrittspunkt wartet dieser ca. 30 s auf den Empfang eines Pairing-Signals vom EBK FM / SE FM.

Befinden sich beide Geräte im Pairing-Modus und in Funk-Reichweite, wird das erfolgreiche Pairing der Komponenten miteinander am EBK FM / SE FM mit 2-maligem Beepen angezeigt. Die Stärke des Funksignals wird über die 3 RSSI-LED signalisiert.

Während des aktivem Pairing-Modus des EBK FM / SE FM können Sie noch weitere Funk-Zutrittspunkt pairen. Starten Sie in den jeweiligen Funk-Zutrittspunkten den Pairing-Modus z. B. durch Einsetzen der Batterie.

Der Pairing-Modus des EBK FM / SE FM wird automatisch nach ca. 5 Minuten oder durch das erneute Drücken der Pairing-Taste im Gerät beendet. Weitere Infos zum Pairing und Pairing-Reset finden sie in der Anleitung der verwendeten Komponenten.

Die Sicherheitscodes von EBK FM / SE FM und Zutrittspunkt sind jeweils in der anderen Komponente gespeichert. Eine leere Batterie beeinflusst das Pairing nicht. Nach einem Batteriewechsel kann der Zutrittspunkt sofort wieder benutzt werden. Ein erneutes Pairing ist nicht notwendig.

5.7.4.6 Konfiguration des Ethernetbuskopplers (EBK / EBK FM)

Vor der Einrichtung im BKS KeyManager müssen die Online-Komponenten ordnungsgemäß in der Schließanlage installiert werden. Für den Einbau und die Verkabelung beachten Sie die jeweils zum Produkt gehörende Anleitung. Schließen Sie die Komponenten erst nach vollendeten Einbau an die Spannungsversorgung an.

Die Online-Komponenten müssen für die elektronische Schließanlage in einem eigenen Netzwerk (z. B. VLAN) zur Verfügung stehen. Hierbei ist zu beachten, das sich alle Komponenten im gleichen Netzwerksegment befinden und eine eigene IP-Adresse haben bzw. diese zugewiesen wurde.

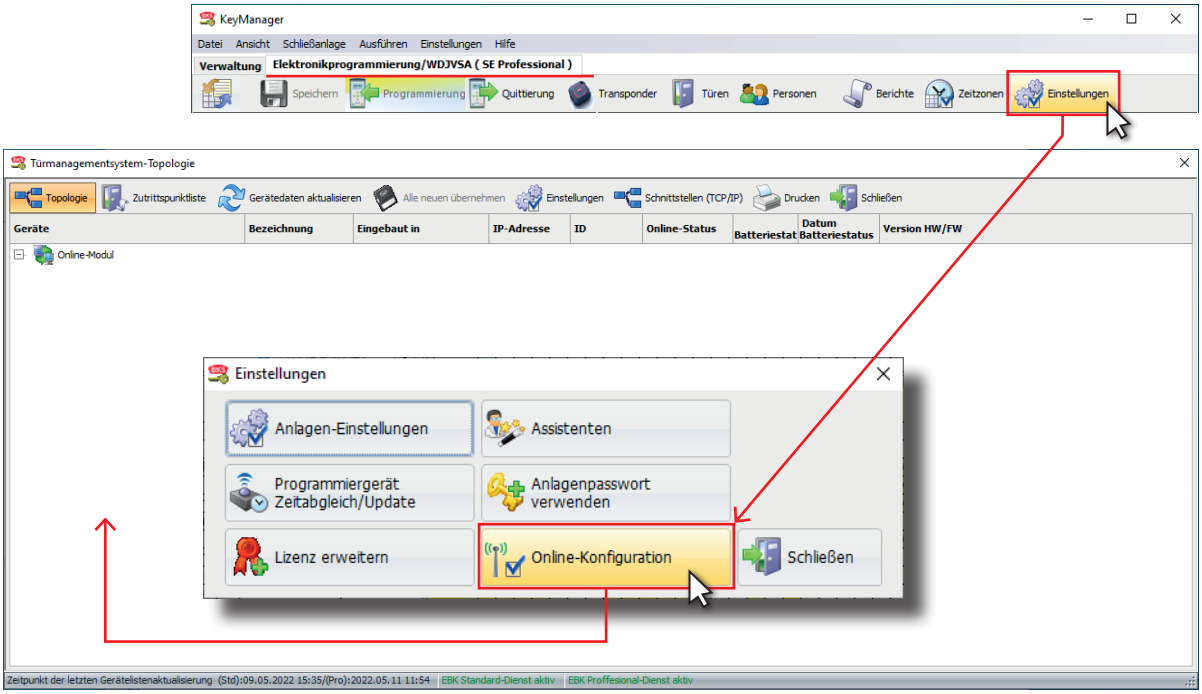
Das Netzwerk inklusive Firewalls, Switches, Virenscanner etc. ist so zu konfigurieren, dass die Kommunikation über die unten angegebenen Ports jederzeit möglich ist. Das Netzwerk sollte zur Sicherheit ausschließlich für das elektronische Schließsystem verwendet werden.

Online-Komponenten	Anleitung | Datenblatt
EBK	C59501138
SE FM	C59501137
EBK FM	C59501138

Die Funkverbindung zwischen EBK FM, SE FM und den Funk-Zutrittspunkten muss über ein Pairing initial hergestellt werden, um eine sichere Verbindung zu gewährleisten.

Die weitere Einrichtung und Konfiguration wird in der Topologie des Online-Dienstes vorgenommen.

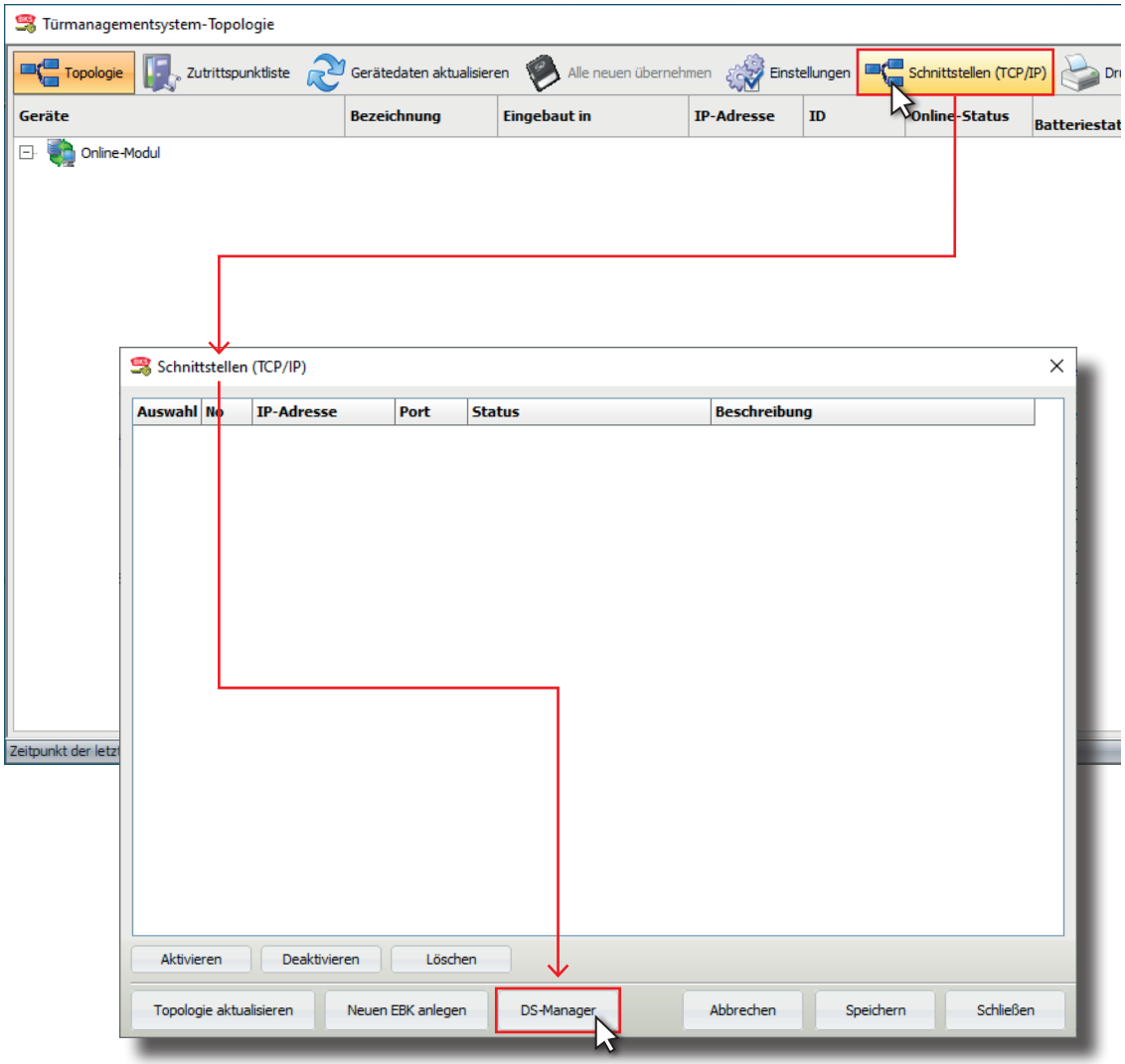
- Wählen Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ den Menüpunkt „Einstellungen“ aus.
- Drücken Sie auf den Button „Online-Konfiguration“.



5.7.4.6.1 Liste der Schnittstellen (TCP/IP)

Bevor Sie die Topologie konfigurieren können, müssen zunächst die Schnittstellen (TCP/IP) des Online-Dienstes eingerichtet werden. Zusätzliche Informationen und/oder die Beschreibung weiterer Funktionen zu den Schnittstellen entnehmen Sie der Anleitung im Kapitel 5.7.2.6 [303].

- Wählen Sie im Fenster „Topologie den Menüpunkt „Schnittstellenverwaltung (TCP/IP)“ zum Einrichten der TCP/IP-Verbindungen aus.
- Drücken Sie auf den Button „DS-Manager“ im Fenster „Schnittstellen (TCP/IP)“.
- Sollte die Firewall Ihres Windows den Zugriff auf den DS-Manager blockieren, drücken Sie bitte in diesem Dialog auf den Button „Zugriff zulassen“.



5.7.4.6.2 Auswahl/Identifizierung der Schnittstelle im DS-Manager

Die Ethernetbuskoppler (EBK und EBK FM) müssen anhand der Schnittstelle im Netzwerk identifiziert und für die jeweilige Netzwerkinfrastruktur eingerichtet werden.

Mit dem sogenannten „DS-Manager“ haben Sie die Möglichkeit, nach EBK und EBK FM-Geräten zu suchen. Im DS-Manager werden Ihnen in einer Liste alle BKS Geräte angezeigt, die über eine Netzwerkschnittstelle verfügen.

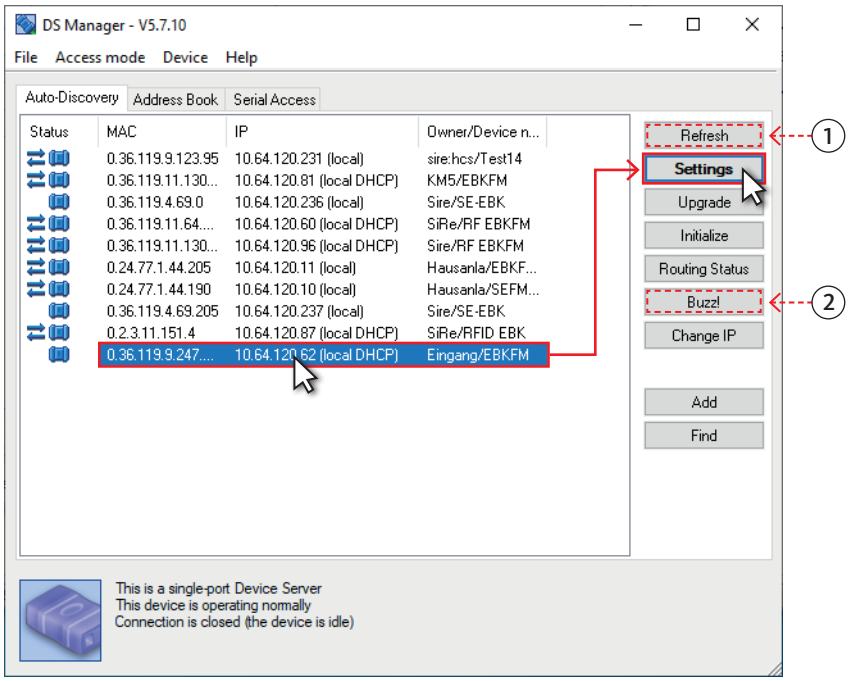
Zusätzlichen Informationen und/oder die Beschreibung weiterer Funktionen entnehmen Sie der Anleitung im Kapitel 5.7.2.6.1 [305].

- Wählen Sie die Schnittstelle des zu identifizierenden EBK/EBK FM aus.

(1) Sollte die gewünschte Schnittstelle nicht angezeigt werden, können Sie mit dem Button „Refresh“ die Liste der Schnittstellen aktualisieren. Überprüfen Sie ggf. die Anschlüsse und die Erreichbarkeit des Geräts, falls es nach dem Refresh nicht angezeigt wird.

(2) Zur Lokalisierung und Prüfung, ob die markierte Schnittstelle bei mehreren Geräten mit dem Gesuchten übereinstimmt, drücken Sie auf den Button „Buzz“. Die LEDs am RJ45-Netzwerkanschluss des EBK/EBK FM leuchten dadurch kurzzeitig auf.

- Drücken Sie auf den Buttons „Settings“. Die gewählte Schnittstelle wird im nächsten Fenster konfiguriert.



5.7.4.6.3 Settings im DS-Manager

Öffnen Sie die Settings der gewählten Schnittstellen im DS-Manager und Überprüfen die Konfiguration. Die Einstellungen der Settings sind voreingestellt. Durch das Bestätigen wird die Schnittstelle in der Liste Schnittstellen (TCP/IP) angezeigt. Zusätzlichen Informationen und/oder die Beschreibung weiterer Funktionen entnehmen Sie der Anleitung im Kapitel 5.7.2.6.2 [306].

- Optional können Sie im Register Network folgende Einstellungen anpassen.

  (1) Angaben zum EBK/EBK FM

  (2) Manuelle Konfiguration der Netzwerkeinstellungen

  – Protokoll: 0 - kein DHCP / 1 - DHCP wird verwendet

  – IP-Adresse: manuelle Eingabe der Adresse

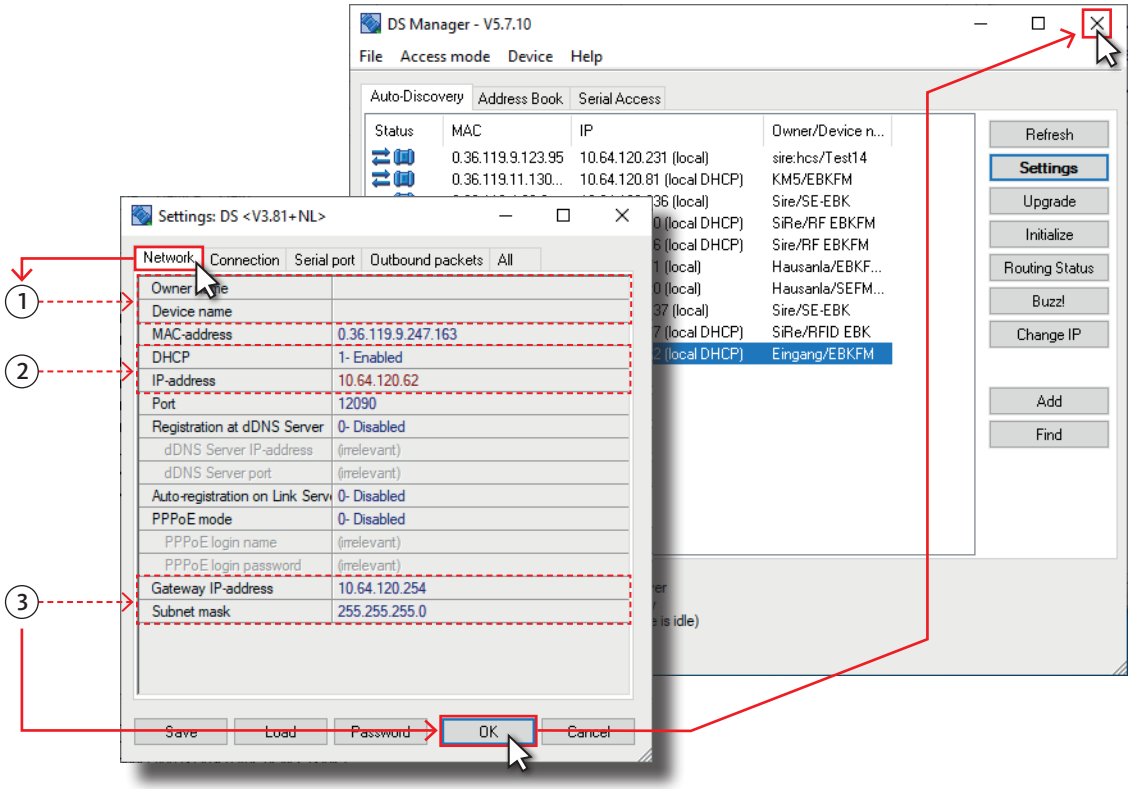
  – Port: 12090 (Der Netzwerkport 12090 sollte verwendet werden)

  (3) Erweiterte Netzwerkeinstellungen

- Drücken Sie zur Übernahme der Änderungen auf „OK“.

Die Einstellungen der anderen Register „Connection | Serial Port | Outbound packets | All“ im Fenster „Settings“ sind vordefiniert und sollten nicht verändert werden.

- Schließen Sie das Fenster „DS-Manager“ über den Button „X“ in der linken Kopfzeile.



5.7.4.6.4 Einrichtung der Schnittstellen (TCP/IP)

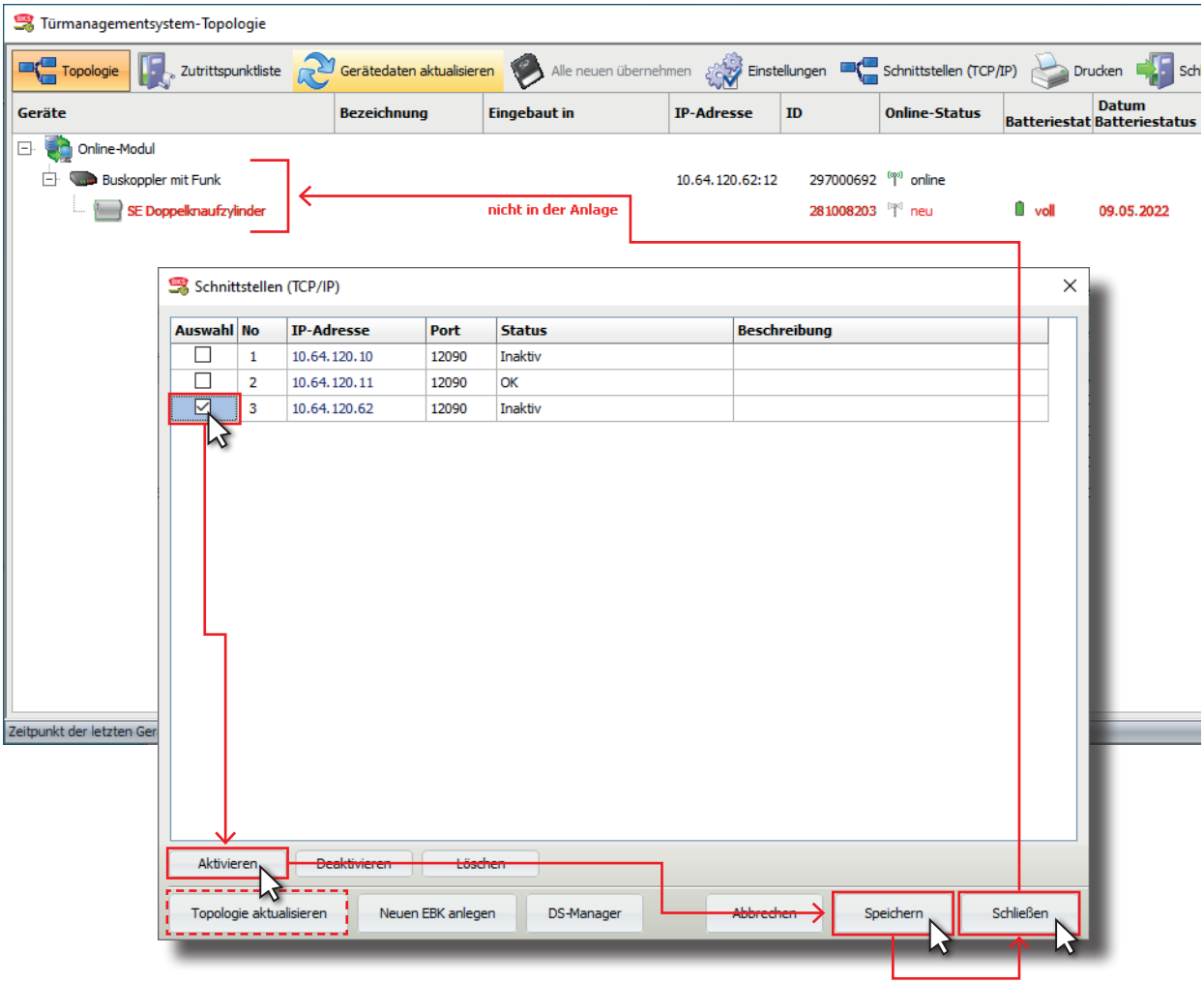
Nach der Identifikation und Einrichtung der gesuchten Schnittstellen im DS-Manager werden die dazugehörenden Geräte in der Liste der Schnittstellen (TCP/IP) angezeigt.

In dieser Liste werden anschließend die IP-Adressen von EBK-Modulen angezeigt. Sollten Adressen dabei sein, die zu einem EBK oder EBK-FM das nicht von Ihnen verwendet wird oder zu einer anderen Schließanlage gehört, kann dieses Gerät deaktiviert werden. Wählen Sie die betreffenden Geräte aus und drücken Sie auf den Button „Deaktivieren“ und „Speichern“.

Sollte eine Schnittstelle, die im DS-Manager eingerichtet wurde, nicht angezeigt werden, drücken Sie auf den Button „Topologie aktualisieren“.

Damit die zur Schnittstelle gehörenden Geräte in der Topologie des Online-Dienstes angezeigt werden, ist der Status der Schnittstelle auf aktiv zusetzen.

- Wählen Sie die inaktive Schnittstelle aus und aktivieren die Checkbox vor der Schnittstelle.
- Drücken Sie auf den Button „Aktivieren“.
- Verlassen Sie das Schnittstellen-Menü und drücken auf den Button „Schließen“.



5.7.4.7 Funk-Komponenten in die Schließanlage übernehmen

Nach dem Schließen des Fensters der Schnittstellen-Einrichtung werden die EBK mit den SE-FM und die EBK-FM Module mit den dazugehörenden Funk-Zutrittspunkten in der Topologie in einer Baumstruktur angezeigt.

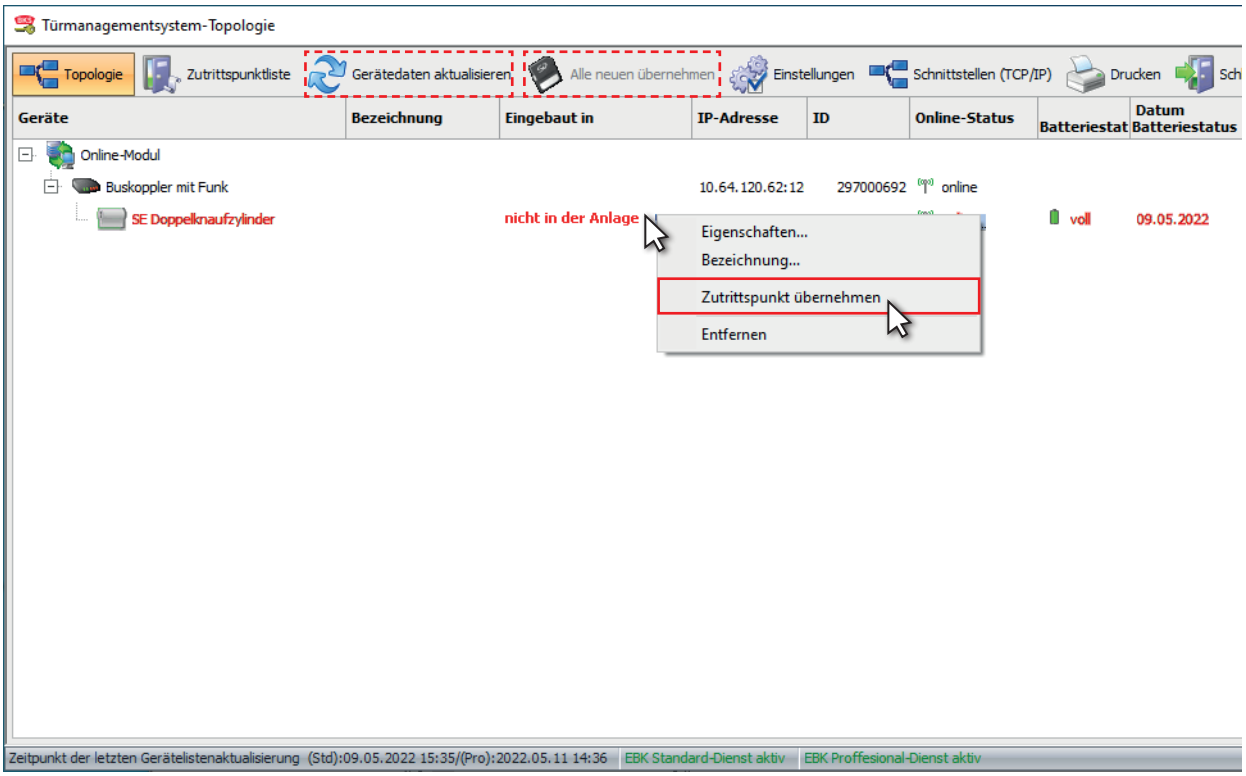
Damit Funk-Zutrittspunkte gefunden bzw. angezeigt werden können, müssen diese mit dem EBK FM / SE FM gepairt sein. Um nach Online-Zutrittspunkten zu suchen, drücken Sie auf den Button „Topologie aktualisieren“.

Die neu gefundenen Funk-Zutrittspunkte werden in Rot dargestellt und müssen der Schließanlage noch hinzugefügt werden.

- Wählen Sie einen neuen Online-Zutrittspunkt aus und öffnen mit der rechten Maustaste das Kontextmenü.
- Drücken Sie im Kontextmenü auf den Menüpunkt „Zutrittspunkt übernehmen“.

Alternativ können alle neuen Online-Zutrittspunkte in die Berechtigungsmatrix zu übernehmen. Drücken Sie hierzu auf den Button „Alle neuen übernehmen“.

- Bestätigen Sie die folgenden Meldungen, um zum Dialog für das Anlegen in der Berechtigungsmatrix zu gelangen.



Wenn Sie mehrere neue Zutrittspunkte übernehmen wollen, welche nicht alle in der Schließanlage verzeichnet sind, werden Sie aufgefordert, die Zutrittspunkte einzeln manuell hinzu zufügen.

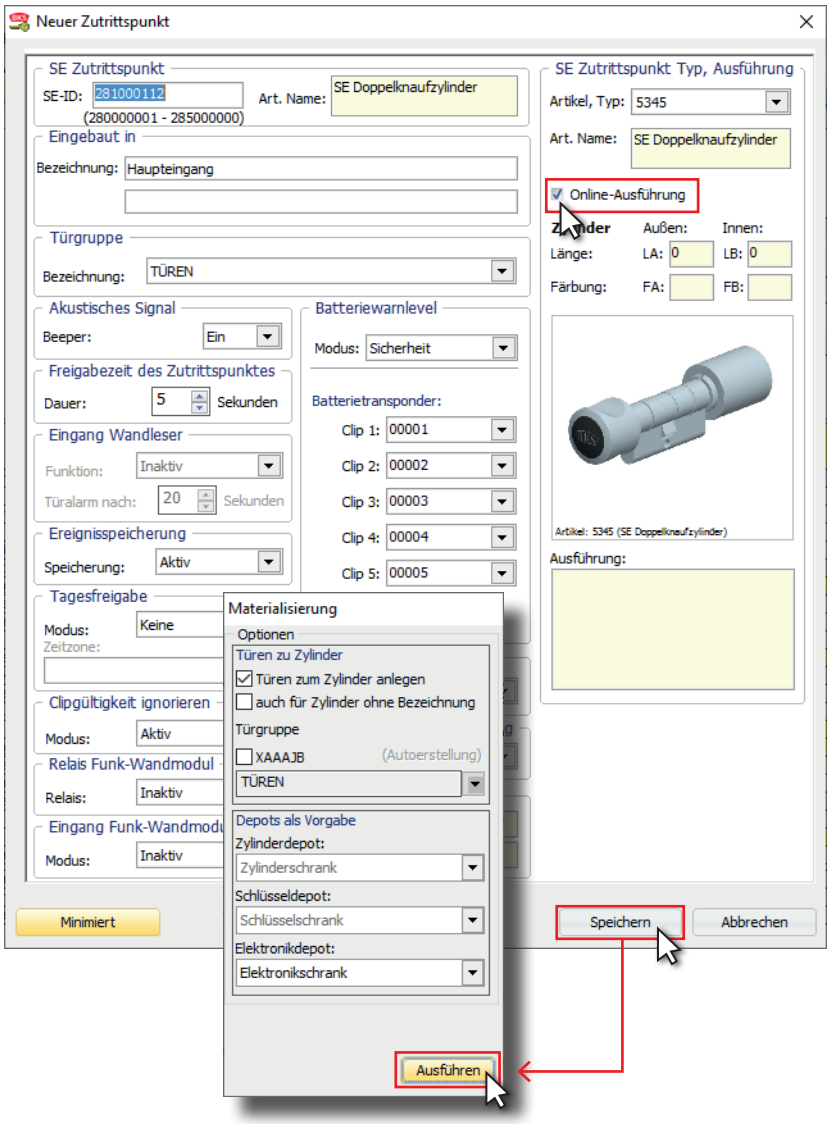
In diesem Fall drücken Sie mit der rechten Maustaste auf die neuen, nicht verzeichneten Zutrittspunkte und wählen Sie „Zutrittspunkt übernehmen“ im Kontextmenü aus.

Es öffnet sich der Dialog aus dem Kapitel zum Anlegen neuer Zutrittspunkte.

- Füllen Sie die Felder im Fenster „Neuer Zutrittspunkt“ aus. Geben Sie die Parameter wie im Kapitel 4.3.1 [202] beschrieben in die einzelnen Felder. Beachten Sie die vorgegebenen Parameter des Zutrittspunkts wie z. B. „ID“ nicht zu verändern.
- Aktivieren Sie die Checkbox „Online Ausführung“.
- Drücken Sie auf den Button „Speichern“ zum Anlegen des Zutrittspunkts.

Nach dem Speichern wird der neu angelegte Zutrittspunkt materialisiert. Das ist die Zuordnung des Zutrittspunkts (z. B. Zylinder) zu einer Tür. Im System werden dadurch Türen zum Zylinder angelegt.

- Übernehmen Sie die Voreinstellung und drücken Sie „Ausführen“, um fortzufahren.



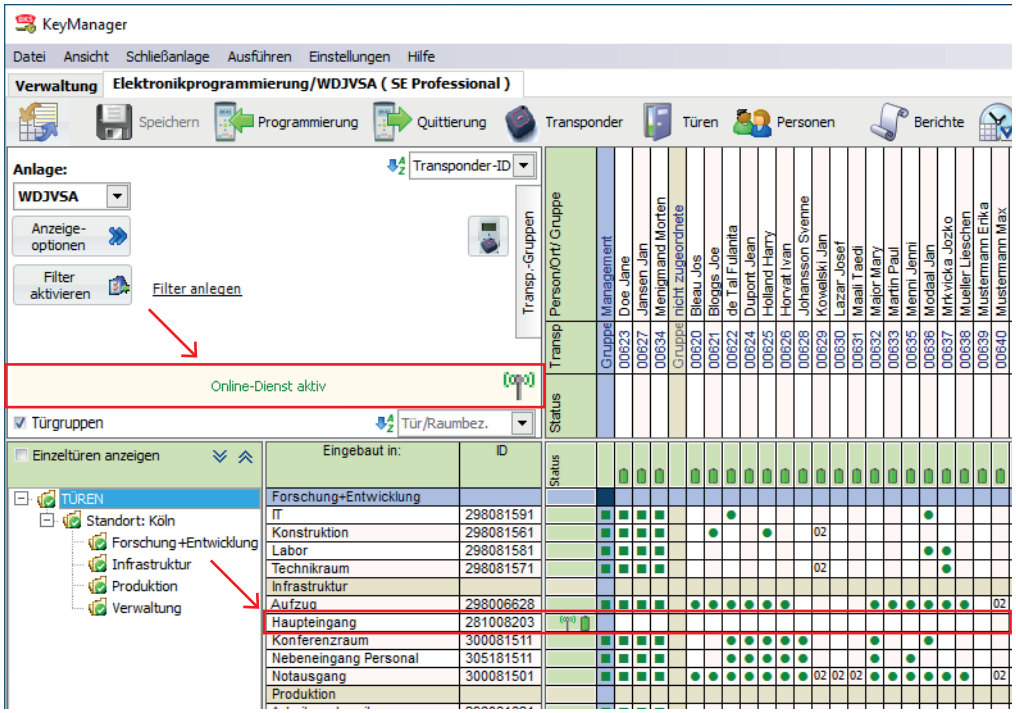
- Drücken Sie auf den Button „Schließen“ in der Topologie, um zur Berechtigungsmatrix zu gelangen.

5.7.4.8 Anzeige der Online-Zutrittspunkte in der Berechtigungsmatrix

Nach erfolgreicher Einstellung der Komponenten, Konfiguration des Online-Dienstes und hinzufügen der Online-Zutrittspunkte werden die Online-Zutrittspunkte in der Berechtigungsmatrix mit dem Status „Online“ angezeigt.

Im Statusfeld wird jeweils ein Icon für den Online-Status und für den Batteriestatus angezeigt.

In der Kopfzeile der Berechtigungsmatrix wird der Status des Online-Dienstes angezeigt. Dieser Dienst muss aktiv sein. Die Kommunikation des BKS KeyManagers mit den Online-Komponenten wird durch diesen Dienst geregelt. Sollte es zu einer Störung im Dienst kommen, wird das durch ein Achtung-Zeichen angezeigt.



Bei der Verwaltung einer Online-Anlage ist die signifikanteste Änderung gegenüber einer Offline-Anlage, das Programmieren der Online-Zutrittspunkte. Diese müssen nicht mehr mit dem Programmiergerät programmiert werden.

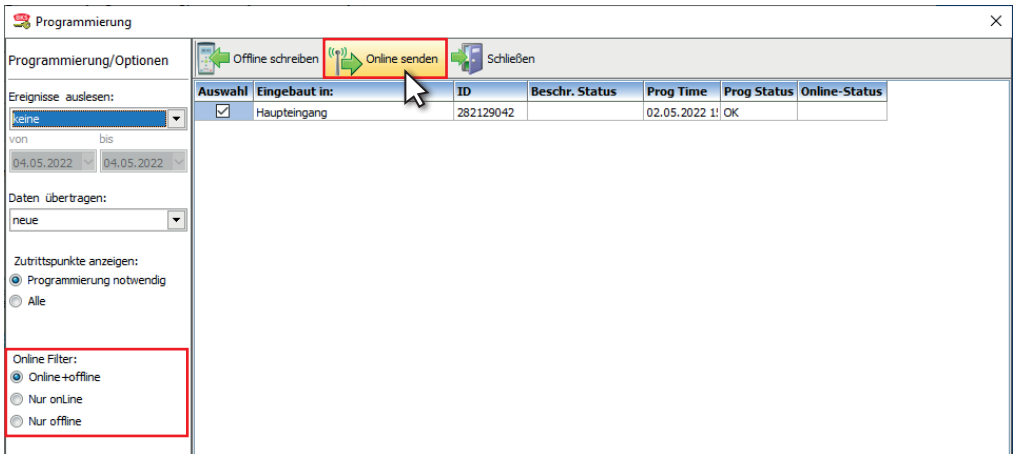
Folgen Sie den Anleitungen der entsprechenden Kapitel.

- Programmieren der Zutrittspunkte über den Button „Programmierung“ siehe Kapitel 3.8.5 [153]
- Programmieren der Zutrittspunkte über den Button „Speichern“ siehe Kapitel 3.7.2 [146]

Das Modul „Programmierung“ ist bei der Online-Anlage zusätzlich mit einem Auswahl-Filter ausgestattet. Dadurch können gezielt nur Online- oder Offline-Zutrittspunkte sowie beide Varianten gleichzeitig anzeigt werden.

Die Funktion „Online senden“ für die direkte Programmierung eines Online-Zutrittspunkts ist ebenfalls hinzugekommen.

Möchten Sie Online-Zutrittspunkte manuell mit einem Programmiergerät programmieren, so nutzen Sie den Button „Offline schreiben“.



Sollte bei einem Zutrittspunkt ein Batteriewarnlevel aufgetreten, werden Sie beim Start des BKS KeyManagers darauf hingewiesen und erhalten eine Warnmeldung.

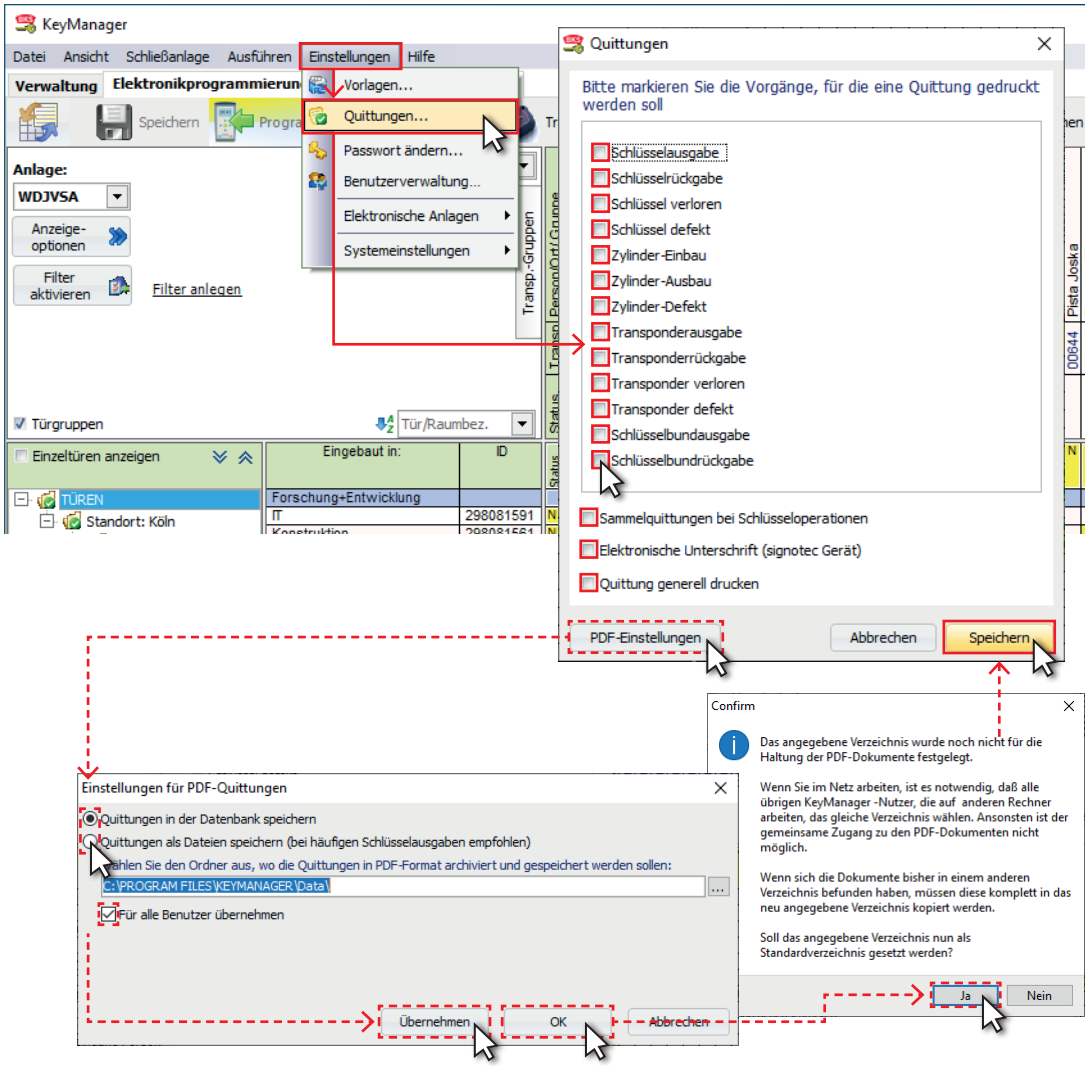
5.8 Quittungen der Vorgänge

Nach dem Ausführen der Vorgänge wie z. B. Ausgabe oder Rückgabe können Quittungen als Beleg für die Tätigkeiten ausgegeben werden. Die Einstellung zur Erstellung der Quittungen kann über diese Funktion zentral verwaltet werden.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Einstellungen“ und wählen den Menüpunkt „Quittungen ...“ aus.
- Aktivieren Sie die Checkboxen zu den jeweiligen Vorgängen, für die nach Ausführung des Vorgangs eine Quittung erstellt werden soll.

Optional können Sie durch Drücken des Buttons „PDF Einstellungen“ den Speicherort der Quittungen festlegen. Folgen Sie bitte hierzu dem Dialog und aktivieren die Checkboxen. Dieses Fenster kann alternativ über das Dropdown-Menü der Menüleiste „Einstellungen“ geöffnet werden.

- Drücken Sie auf den Button „Speichern“ zum Beenden.



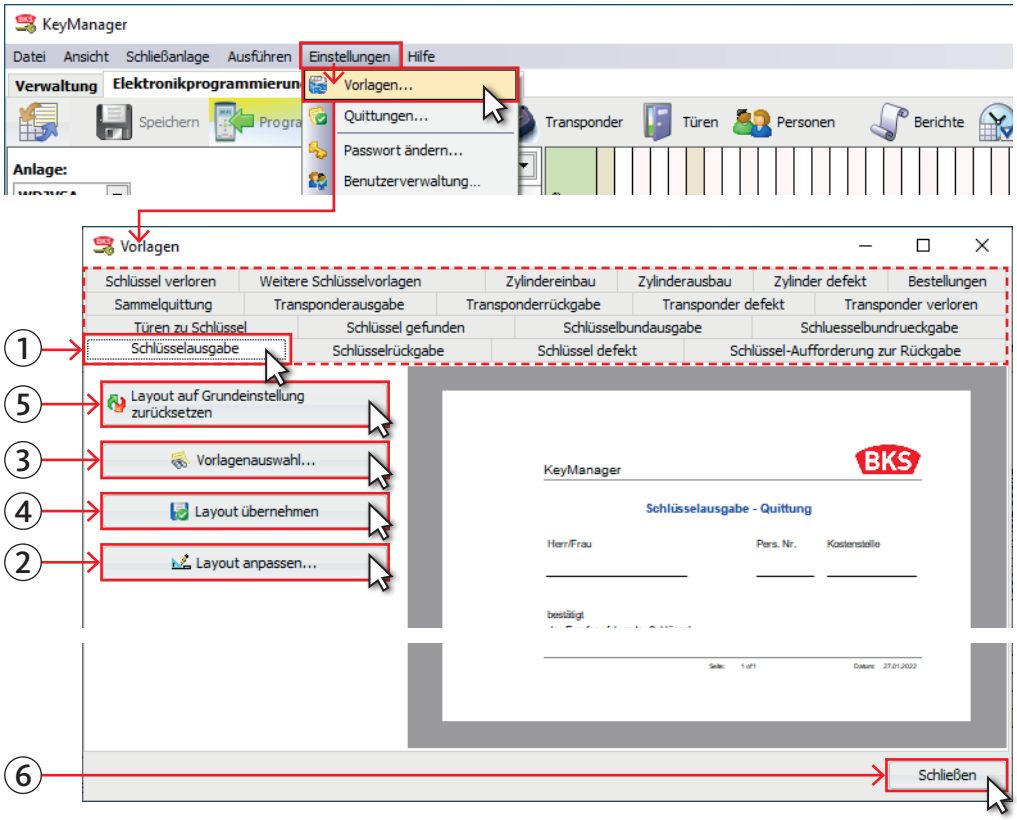
HINWEIS

In den Einzelmenüs der Vorgänge wie z. B. die Transponderausgabe können Sie durch Aktivieren der Checkbox die Funktion zur Ausgabe einer Quittung einschalten bzw. durch Deaktivierung ausschalten. Die Checkbox finden Sie über der Fußzeile des Fensters.

5.9 Layout der Quittungen der Vorgänge

Die Vorlagen zum Druck der Quittungen können mit dieser Funktion nach Ihren Wünschen editiert, als Vorlage abgespeichert oder von einer gespeicherten Vorlage geladen werden.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Einstellungen“ und wählen den Menüpunkt „Vorlagen ...“ aus.

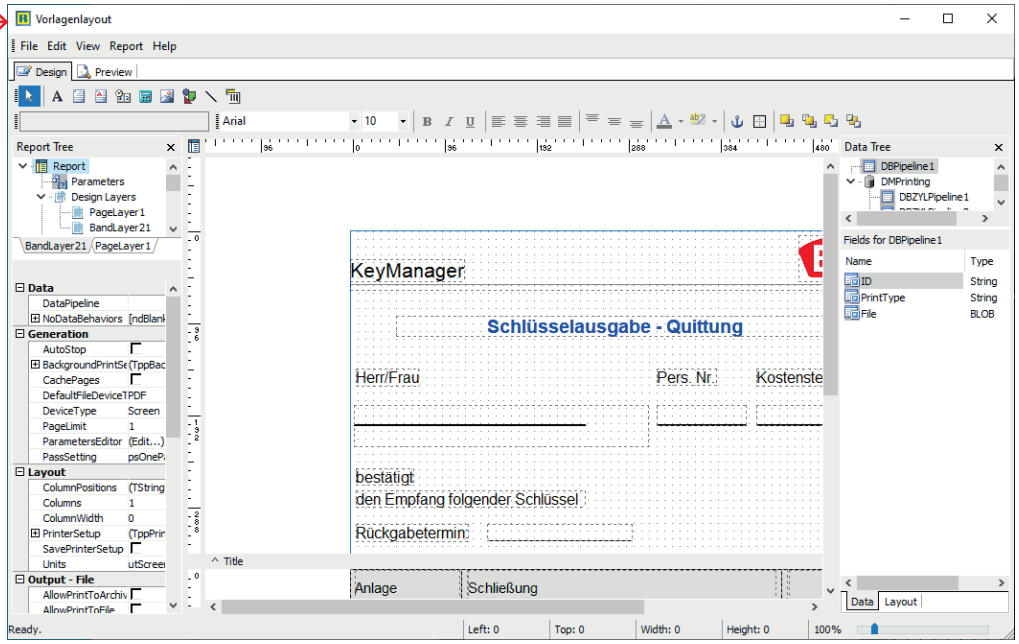


- (1) Wählen Sie ein Register aus, zu dessen Vorgang Sie die Layoutvorlage der Quittung bearbeiten wollen.
- (2) Drücken Sie auf diesen Button, um den Editor „Vorlagenlayout“ für die Erstellung bzw. Überarbeitung des Layouts zu öffnen.
- (2a) Gestalten Sie Ihr Layout im Register „Design“ und nutzen die Bearbeitungsmöglichkeiten des Editors zur Erstellung und Gestaltung. Das Register „Preview“ bietet Ihnen eine Vorschau auf das Ergebnis. Speichern Sie das Layout ab, um es importieren zu können.

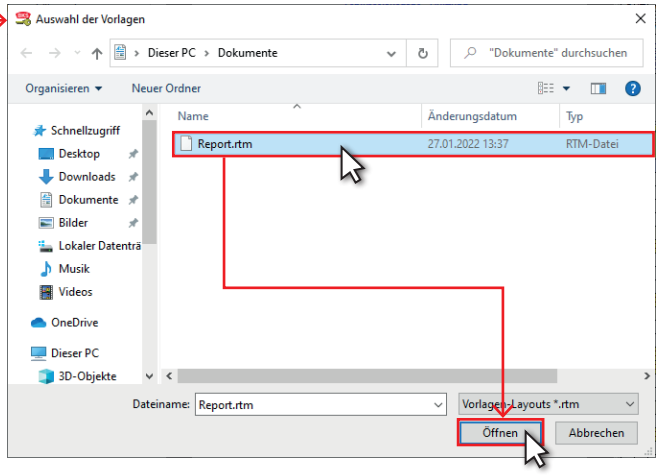
oder

- (3) Importieren Sie eine Layoutvorlage und drücken hierzu auf den Button.
- (3a) Navigieren Sie mit dem Dateibrowser zur Vorlagendatei (*.RTM). Drücken auf den Button „Öffnen“. Das Layout wird geladen.
- (4) Drücken Sie auf diesen Button, um die neu erstellte Layoutvorlage oder die vorher geladene Vorlage im BKS KeyManager zu aktivieren.
- (5) Dieser Button setzt das ausgewählte Register auf die Grundeinstellung zurück.
- (6) Drücken Sie auf den Button „Schließen“ zum Beenden.

2a


Vorlagenlayout
File Edit View Report Help
Design
Preview
Report Tree
Report
Parameters
Design Layers
PageLayer1
BandLayer21
Data
DataPipeline
Generation
AutoStop
CachePages
DefaultFileDeviceTPDF
DeviceType Screen
PageLimit 1
Layout
Output - File
KeyManager
Schlüsselausgabe - Quittung
Herr/Frau
Pers. Nr.
Kostenste
bestätigt
den Empfang folgender Schlüssel
Rückgabetermin:
Title
Anlage
Schließung
Data Tree
DBPipeline1
DMPrinting
DBZYLPipeline1
Fields for DBPipeline1
Name
Type
ID String
PrintType String
File BLOB
Data
Layout
Ready.
Left: 0
Top: 0
Width: 0
Height: 0
100%

3a


Auswahl der Vorlagen
Dieser PC › Dokumente
"Dokumente" durchsuchen
Organisieren
Neuer Ordner
Schnellzugriff
Desktop
Downloads
Dokumente
Bilder
Lokaler Datenträ
Musik
Videos
OneDrive
Dieser PC
3D-Objekte
Name
Änderungsdatum
Typ
Report.rtm
27.01.2022 13:37
RTM-Datei
Dateiname:
Report.rtm
Vorlagen-Layouts *.rtm
Öffnen
Abbrechen

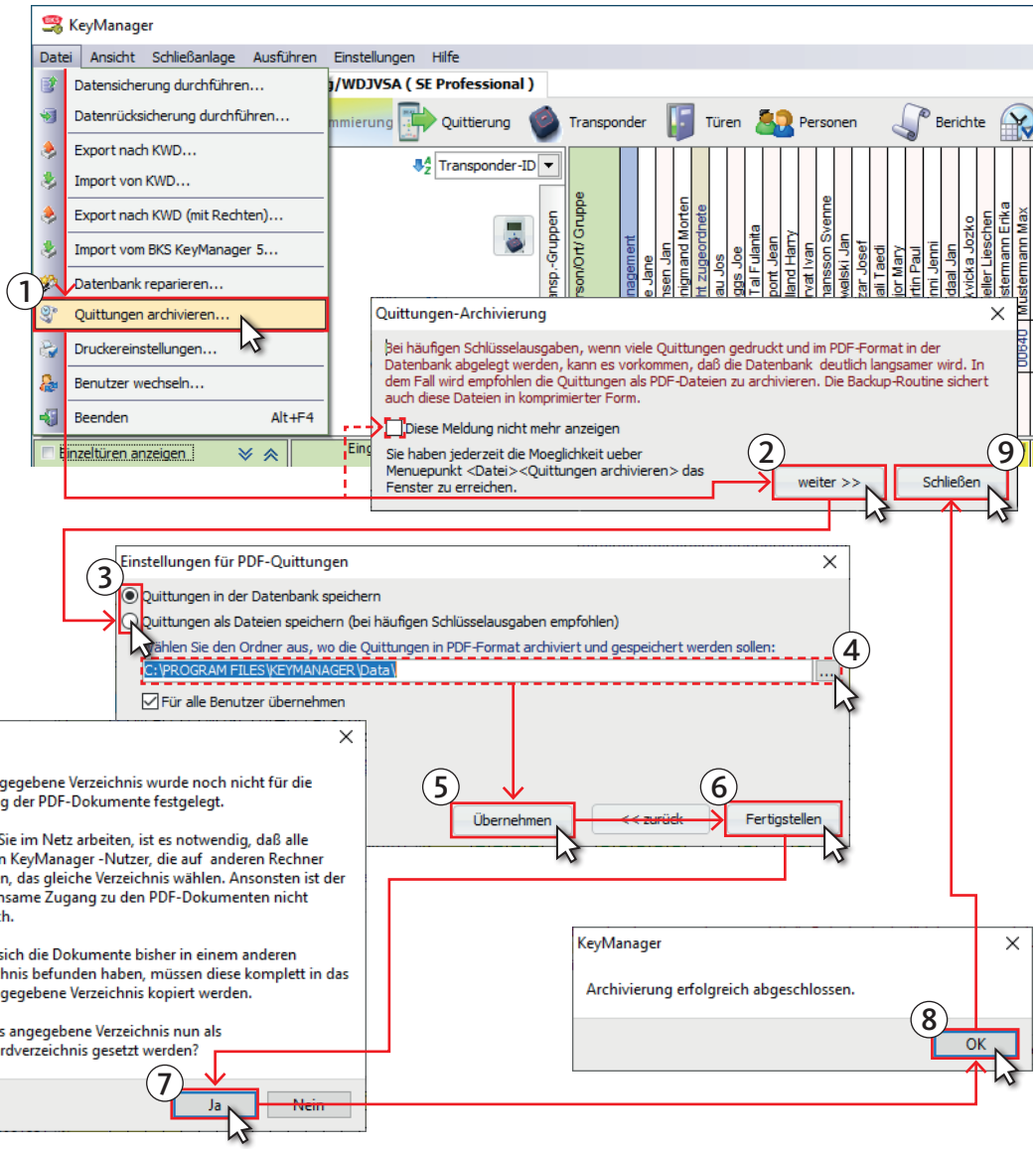
5.9.1 Archivierung der Quittungen

In Abhängigkeit von der Größe Ihrer Schließanlage und wie viele Quittungen von Ihrem System erzeugt werden z. B. durch häufige Transponderausgaben, die mit einem SignoTec-Signatur-Pad unterschrieben werden, kann es zu Einbußen in der Performance der Datenbank kommen.

Einen solchen Leistungsabfall können Sie dadurch verhindern, indem Sie die Quittungen als PDF-Dateien archivieren und außerhalb der Datenbank abspeichern, wodurch diese nicht mehr in der Datenbank abgespeichert werden.

Beim Anlegen des Speicherorts der PDF-Dateien ist sicher zustellen, dass der Ablageordner für jeden Benutzer des BKS KeyManagers verfügbar ist.

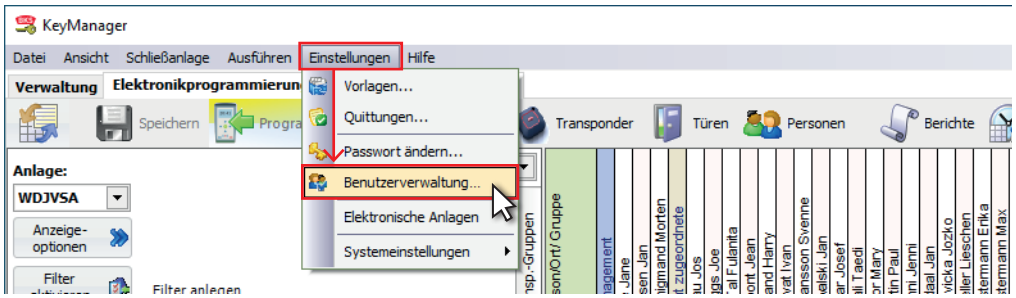
- Folgen Sie den Schritten der Abbildung.



6. Benutzerverwaltung

Die Benutzerverwaltung ermöglicht es Ihnen, den verschiedenen Benutzern des BKS Keymanagers je nach ihrem Aufgabenprofil und Arbeitsgebiet eigene Benutzerprofile mit unterschiedlichen Zugriffsberechtigungen einzurichten.

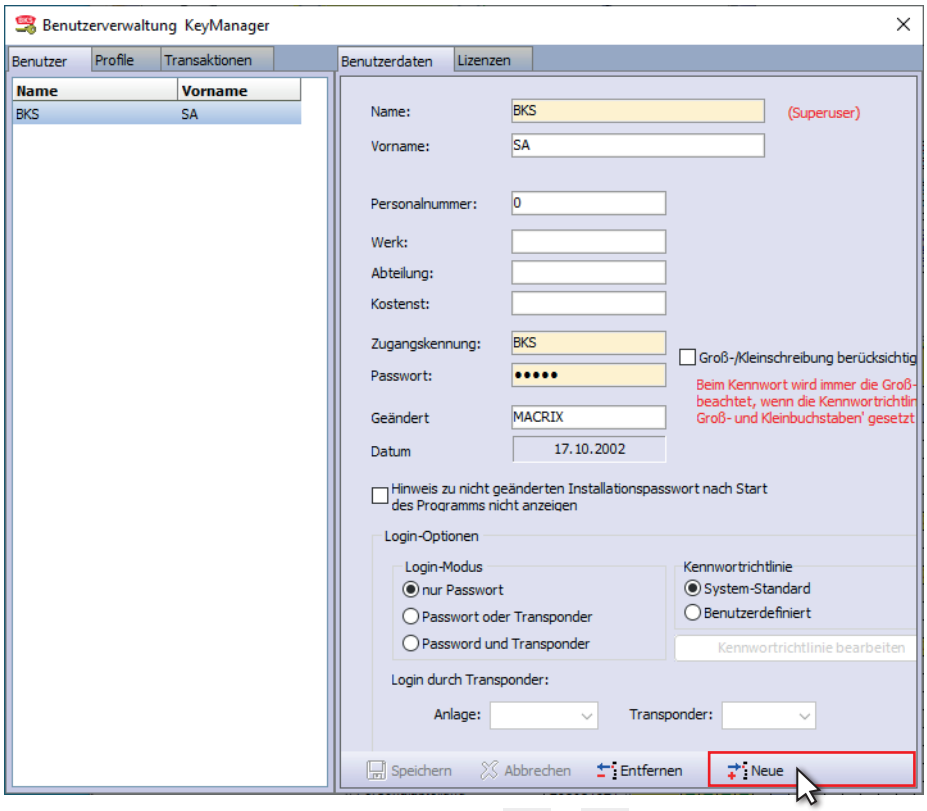
- Öffnen Sie in der Menüleiste das Dropdown-Menü „Einstellungen“ und wählen den Menüpunkt „Benutzerverwaltung ...“ aus.



6.1 Benutzer neu anlegen

Bei der Installation des BKS KeyManagers wird der Benutzer „BKS“ als Superuser mit Administratorrechten angelegt. Dieser Benutzer verfügt über alle Rechte und kann alle Funktionen des BKS KeyManagers ohne Einschränkungen nutzen. Je nach Anlagengröße und Arbeitsumfang wird es im täglichen Gebrauch notwendig sein, dass weitere Benutzer im Schließsystem arbeiten ausführen können. Zur Gewährleistung der Anlagensicherheit dürfen die Benutzer nur die zur Erfüllung benötigten Rechte besitzen. Mit der Benutzerverwaltung können Benutzer mit unterschiedlichen Benutzerprofilen und Zugriffsrechten eingerichtet werden.

- Drücken Sie auf den Button „Neue“, um einen neuen Benutzer anzulegen.

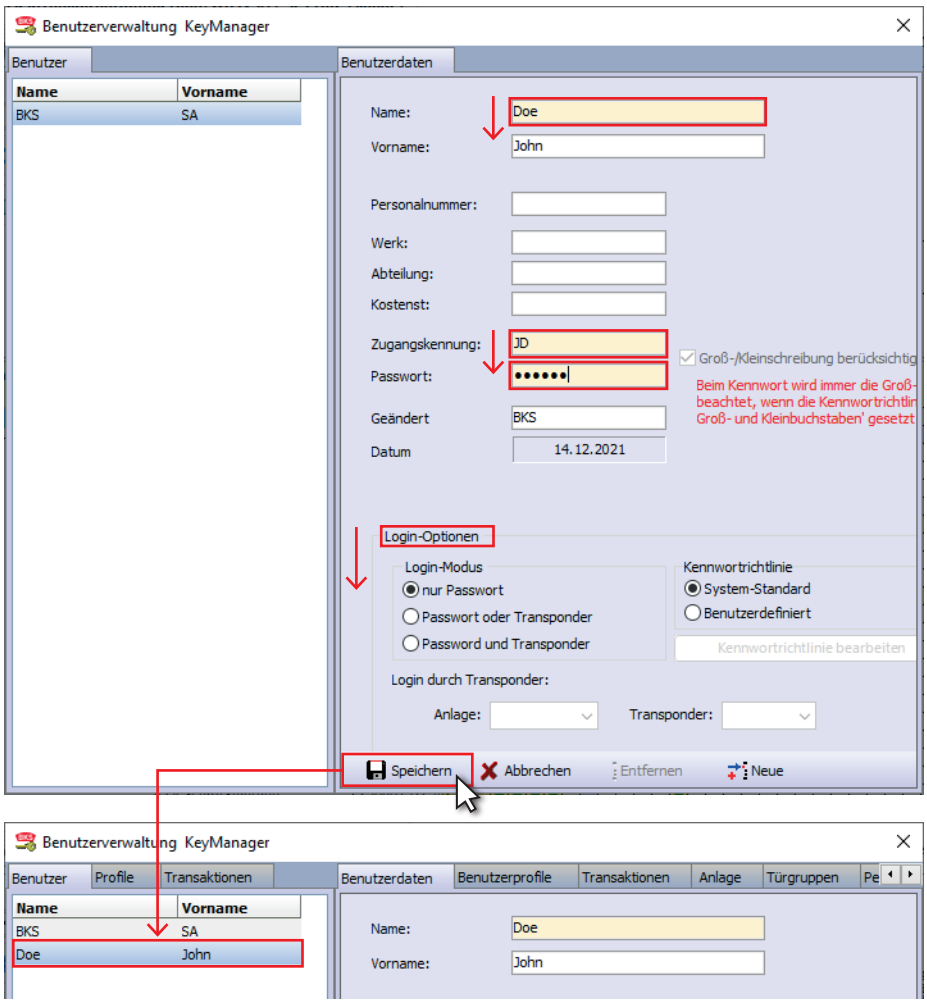


- Zum Anlegen des neuen Benutzers füllen Sie die Felder mit den Benutzerdaten aus.
- Vergeben Sie eine Zugangskennung und ein Passwort für den neuen Benutzer und wählen eine Login-Option aus.

Beachten Sie die Empfehlungen in den beiden folgenden Unterkapitel zur Vergabe des Passworts und den Optionen zum Login. Bei Verwendung eines Modus, der einen Login des Benutzers mit Transponder vorsieht, ist der Transponder mit der zugehörigen Anlage über die beiden Dropdown-Menüs festzulegen.

Die Mindestanforderung an das Passwort kann optional über eine eigene Kennwortrichtlinie individuell angelegt werden. Bei der Vergabe des Passworts wird diese auf Einhaltung geprüft.

- Drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern und ggf. zum Beenden auf das Symbol „X“ zum Schließen des Fensters.



6.1.1 Empfehlungen zur Erstellung des Passwort (DGSVO)

Beim Einsatz und der Verwendung des BKS KeyManagers ist es wichtig, dass Sie auf die Einhaltung der Datenschutz-Grundverordnung (DSGVO) achten. Für alle Programmbenutzer des BKS KeyManagers gelten die folgenden Empfehlungen zur Passwortsicherheit:

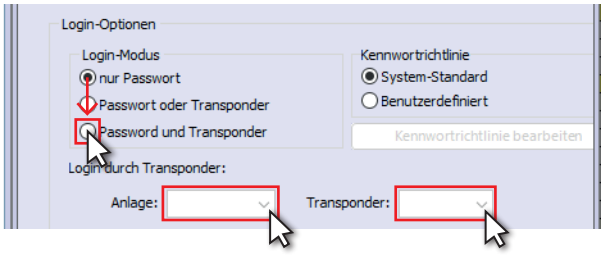
- Definierte Länge des Passworts zwischen 6 und 32 Zeichen
- Je länger das Passwort ist, desto besser
- Ein gutes Passwort sollte mindestens acht Zeichen lang sein
- Für das Passwort können alle verfügbaren Zeichen genutzt werden, beispielsweise Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ? ! % + ...)
- Das Passwort sollte nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern wie „asdfgh“ oder „1234abcd“ bestehen
- Nicht als Passwörter geeignet sind Namen von Familienmitgliedern, des Haustiers, des besten Freundes, des Lieblingsstars, Geburtsdaten und so weiter
- Das vollständige Passwort sollte möglichst nicht in Wörterbüchern vorkommen
- Das Passwort des BKS KeyManagers sollte in regelmäßigen Abständen geändert werden
- Zusätzlich sollte das Passwort nur für den BKS KeyManager verwendet werden und nicht in weiteren Anwendungen

6.1.2 Zwei Faktor Authentifizierung des Benutzers

Ergänzend zur Authentifizierung durch einen Benutzernamen mit dazugehörigen Benutzerpasswort oder Transponder unterstützt der BKS KeyManager auch die Möglichkeit zum Login mit einer Zwei-Faktor-Authentifizierung.

Dabei ist zu beachten, dass bei einem Defekt oder Verlust des Transponders kein Zugriff mehr möglich ist. Bei der Verwendung der zwei Faktor Authentifizierung ist es wichtig, mehrere Benutzer mit Administrator-Rechten zu versehen, damit Redundanzen vorhanden sind.

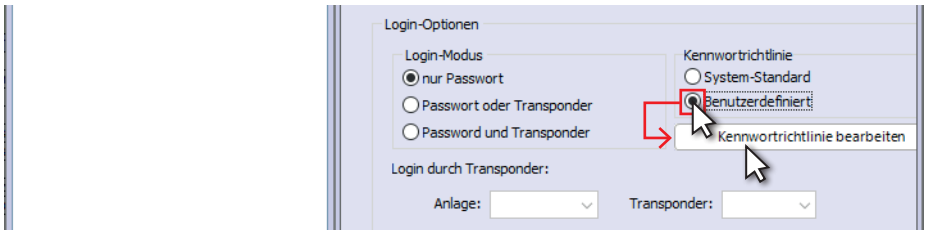
- Zum Ändern des „Login-Modus“ und aktivieren Sie die Checkbox „Passwort und Transponder“ im Feld „Login-Option“.
- Legen Sie den Transponder zum Login in den Dropdown-Menüs fest und wählen über die Auswahlliste die zugeordnete Anlage und den Transponder aus.
- Drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern.



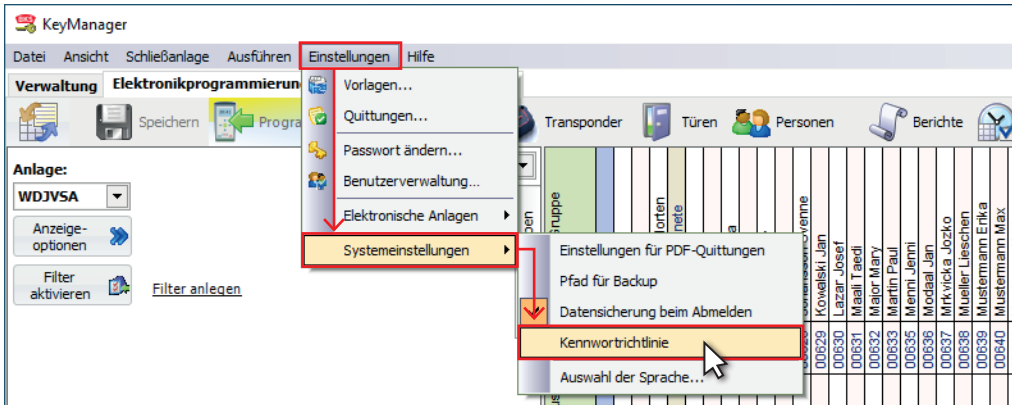
6.1.3 Kennwortrichtlinie

Für die Funktion „Passwort ändern“, mit der ein angemeldeter Benutzer in der Lage ist, sein eigenes Passwort zu ändern, können Sie eine Kennwortrichtlinie festlegen. Hierdurch definieren Sie Mindestanforderungen, welche das neue Passwort erfüllen muss.

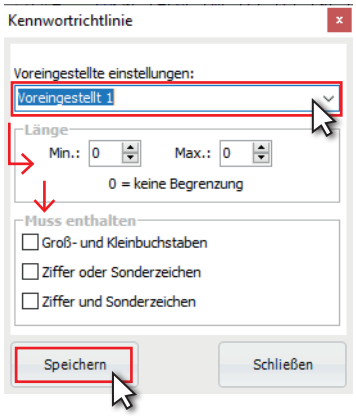
- Aktivieren Sie die Checkbox „Benutzerdefiniert“ in der Benutzerverwaltung.
- Drücken Sie auf den Button „Kennwortrichtlinie bearbeiten“.



- Alternativ können Sie in der Menüleiste das Menü „Einstellungen“ öffnen und im Dropdown-Menü „Systemeinstellungen“ den Menüpunkt „Kennwortrichtlinie“ auswählen.



- Vergeben Sie vorzugsweise einen Namen für die Kennwortrichtlinie oder wählen eine Vorhandene zum Editieren der Einstellungen über das Dropdown-Menü aus.
- Geben die Länge des Passworts sowie die enthaltenen Zeichen vor. Beachten Sie die Empfehlungen zur Erstellung des Passworts bei Erstellung der Richtlinie, siehe Kapitel 6.1.1 [341].
- Drücken Sie auf den Button „Speichern“.

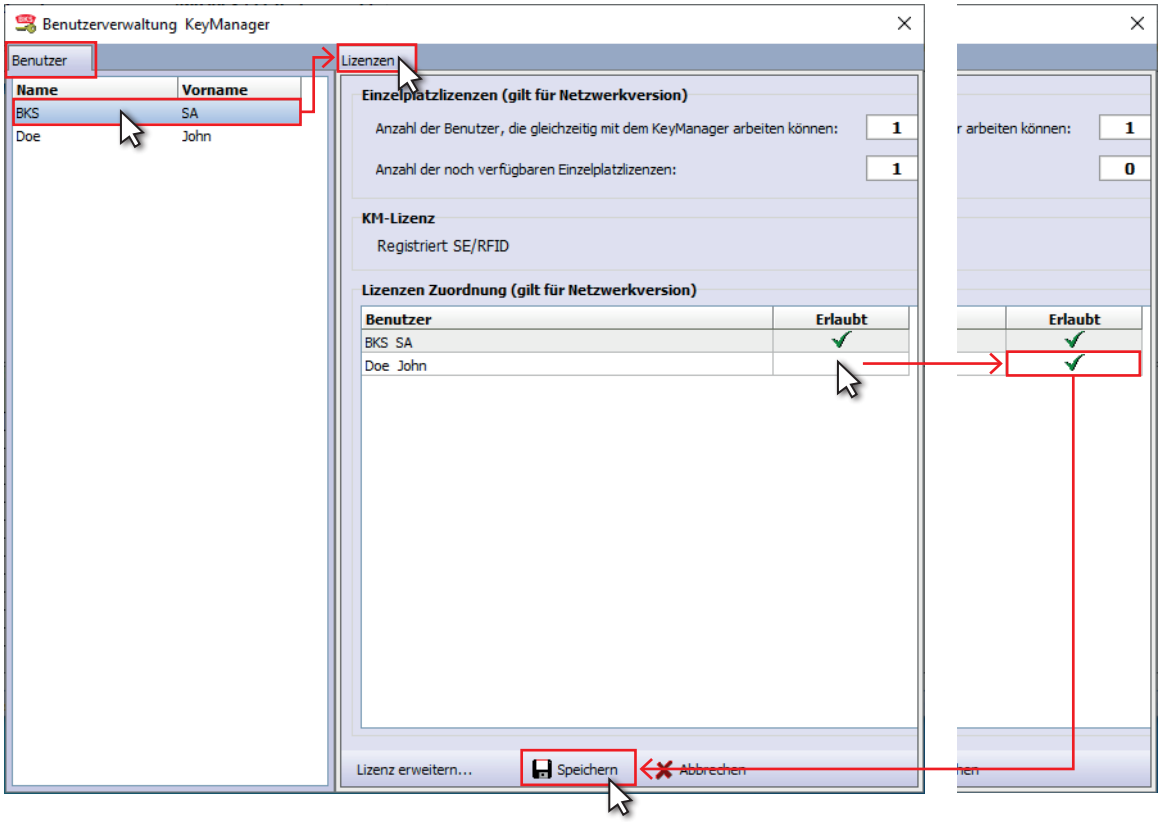


6.2 Zuordnung der Lizenzen zum Benutzer (bei Netzwerkversion)

Bei Verwendung einer Netzwerkversion ist die maximale Anzahl der Benutzer die gleichzeitig arbeiten können sowie Anzahl der Einzelplatzlizenzen über die im BKS KeyManager installierten Lizenzen reglementiert. Damit Benutzer parallel verwendet werden können, müssen dem Profil die Lizenzen zugeordnet werden.

HINWEIS **Die Einstellungen im Register „Lizenzen“ sind nur beim Einsatz des BKS KeyManagers in der Netzwerkversion (Client-/Server-Betrieb) erforderlich.**

- Wählen Sie im Register „Benutzer“ einen Administrator/Superuser, wie in diesem Beispiel den Benutzer „BKS“ aus.
- Drücken Sie auf das Register „Lizenzen“.
- Klicken Sie in das Feld „Erlaubt“, um die Lizenzen dem Benutzer zu zuordnen.
- Drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern.

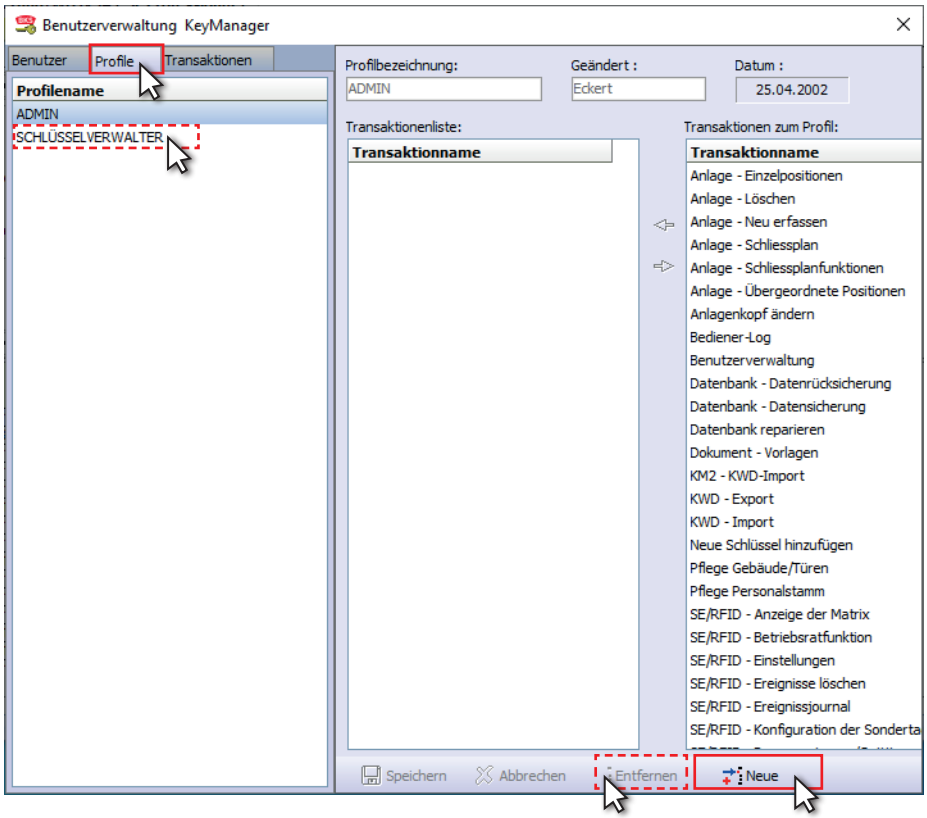


6.3 Benutzerprofile

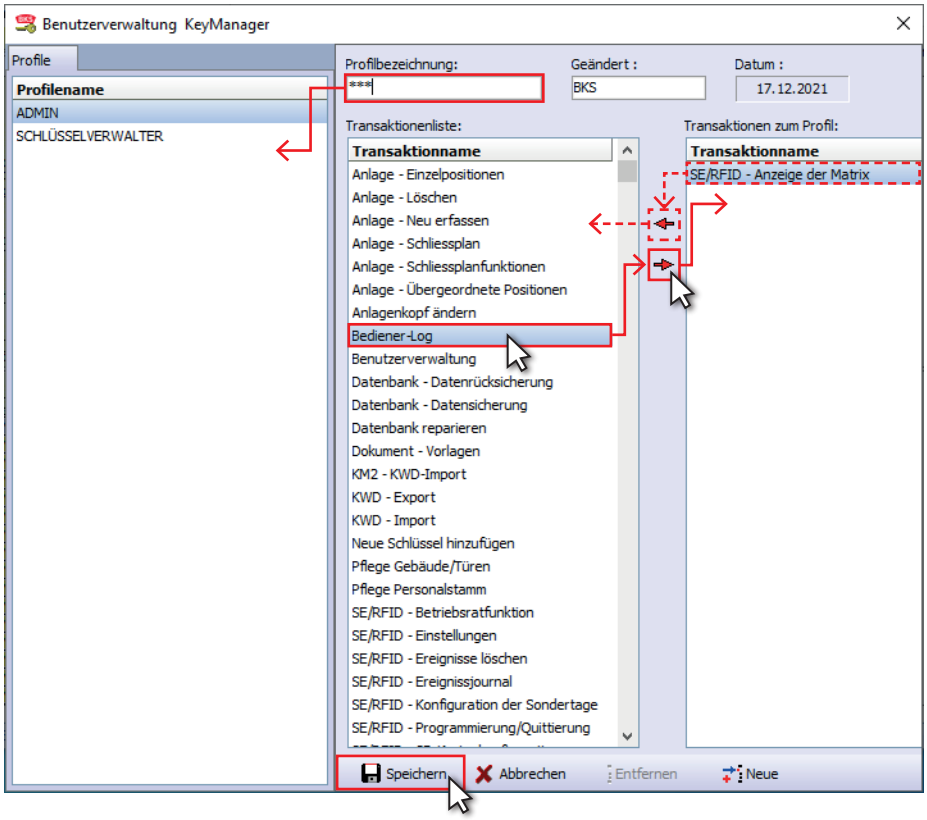
Das Benutzerprofil ist eine Sammlung der Transaktionen, die eine Berechtigung zum Zugriff oder Ausführen der Funktion haben sollen. Nach dem Einrichten des Benutzerprofils wird durch die Zuordnung des Profils zum Benutzer diesem der Zugriff auf diese Transaktionen gewährt.
Grundlage der Zuordnung ist dabei die Rolle des Benutzers während der Bedienung des BKS Key-Managers und welche erforderlichen Legitimationen, Programmzugriffe und Funktionen für diese Tätigkeit über das Benutzerprofil freizuschalten sind.

Das Profil „Admin“ kann nicht verändert werden und enthält die Rechte zu allen Transaktionen. Bei den weiteren Benutzerprofilen sind die Transaktionen individuell zu zuordnen.

- Wählen Sie das Register „Profile“ in der linken Spalte der Benutzerverwaltung aus.
- Zum Bearbeiten eines vorhandenen Benutzerprofils wählen Sie ein schon angelegtes Benutzerprofil aus. Folgen Sie den Schritten zum Hinzufügen und Entfernen der Transaktionen. Zum Löschen dieses Profils drücken Sie auf den Button „Entfernen“.
- Drücken Sie auf den Button „Neue“, um ein neues Benutzerprofil anzulegen.



- Geben Sie für ein neues Profil eine Profilbezeichnung ein oder überarbeiten eine vorhandene Bezeichnung gegebenenfalls.
- Zum Hinzufügen wählen Sie eine Transaktion in der Spalte „Transaktionenliste“ aus. Drücken Sie auf den Button „Pfeil nach rechts“, um die Transaktion in die Spalte „Transaktionen zum Profil“ zu verschieben und zu berechtigen.
- Zum Entfernen wählen Sie eine Transaktion in der Spalte „Transaktionen zum Profil“ aus. Drücken Sie auf den Button „Pfeil nach links“, um die Transaktion in die Spalte „Transaktionenliste“ zurück zu verschieben und die Berechtigung zu dieser Transaktion zu widerrufen.
- Drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern.



6.3.1 Empfehlungen zu den Benutzerrollen (DGSVO)

Die Berechtigung zur Ausführung der einzelnen Funktionen des BKS KeyManager sollten für jeden Benutzer im Sinne der Benutzerrollen in Verbindung mit dem Grundsatz des „Need to Know“-Prinzips erfolgen.

In diesem Sinne sollte das Recht für die Transaktionen abgewogen und nur nach den tatsächlichen Bedürfnissen des Benutzers vergeben werden. Bei der Umsetzung der Benutzerrolle sollten nur die für Benutzer notwendigen Zugriffsfunktionen durch Zuweisung im Benutzerprofil aktiviert werden.

6.3.2 Empfehlungen zur Rechtevergabe (DGSVO)

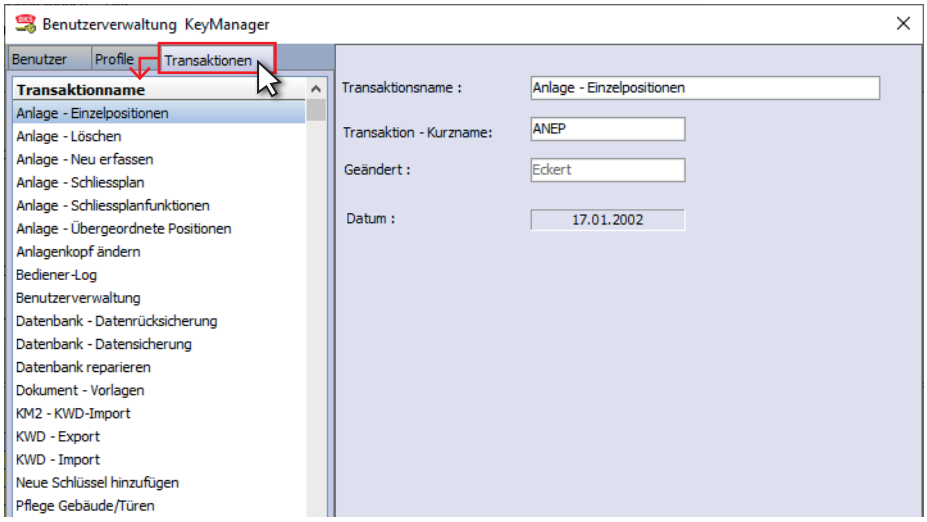
Die folgenden Zugriffsfunktionen erlauben den Zugriff auf personenbezogene Daten und sollten Administratoren vorbehalten bleiben oder durch Aktivierung des „4-Augen-Prinzip“ und der Legitimation durch zwei berechtigte Benutzer geschützt werden:

- Administrator: Vollzugriff auf das System und alle Daten.
- Pflege Personalstamm, Personenliste: Zugriff auf personenbezogenen Daten der Benutzer.
- Bediener-Log: Ausgabe der Aktivitäten (Anlagen, Änderungen) der Benutzer des BKS-KeyManagers (Nur mit der Professional Lizenz möglich).
- Ereignis-Journal: Anzeige welche Tür wann und vom welcher Person geöffnet wurde (elektronische Schließanlagen).

6.3.3 Übersicht der Transaktionen|Funktionen

Mit dieser Funktion können Sie zur Übersicht eine Liste mit den im BKS KeyManager durch einen Benutzer ausführbaren Transaktionen anzeigen lassen. Die Zuordnung der Transaktionen wird im Register „Profile“ durchgeführt.

- Drücken Sie in der linken Spalte der Benutzerverwaltung auf das Register „Transaktionen“, um zur Übersicht der Transaktionen zu gelangen.



6.4 Benutzer

Basis des Zugriffs der Benutzer auf den BKS KeyManagers ist das jeweilige Konto des Benutzers, indem die Zugriffsberechtigungen auf die verschiedenen Komponenten der Schließanlage und die Funktionalitäten der Software geregelt sind.

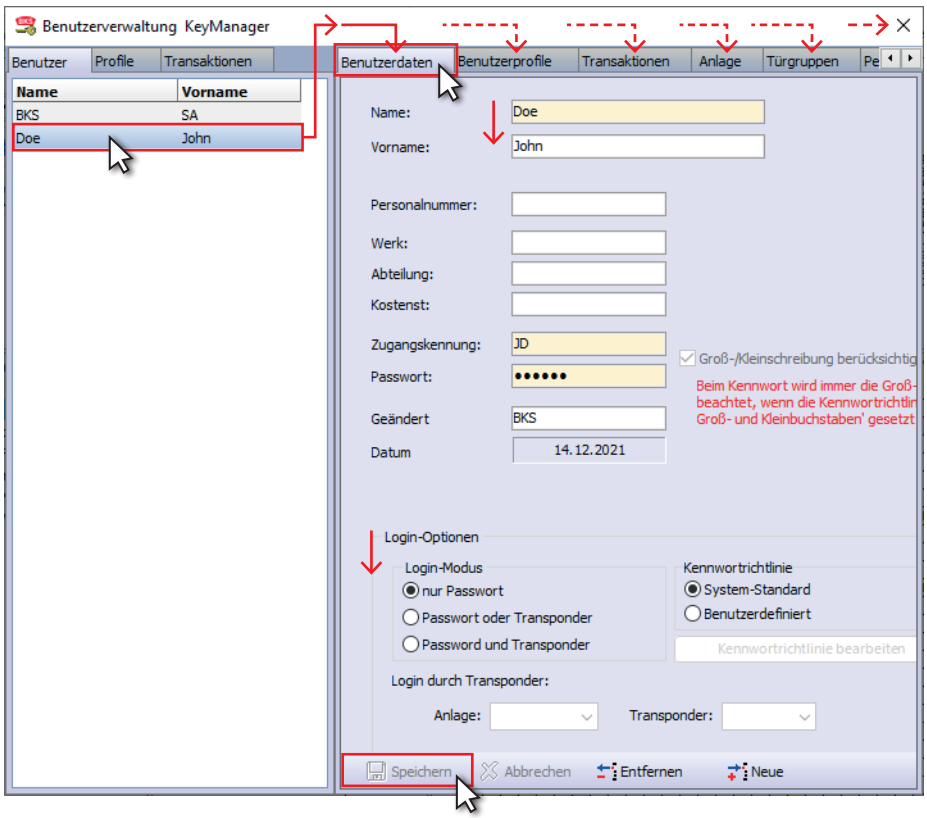
- Drücken Sie auf den Button „Speichern“, um Ihre Eingaben zu sichern.
- Zum Beenden der Benutzerverwaltung drücken Sie auf das Symbol „X“ zum Schließen.

6.4.1 Benutzerdaten

- Wählen Sie zum Bearbeiten in der linken Spalte der Benutzerverwaltung das Register „Benutzer“ ein Benutzerprofil aus.

In der rechten Spalte können Sie zum jeweils ausgewählten Benutzer die verschiedenen Einstellungen unterteilt nach Inhalt in Registern vornehmen.

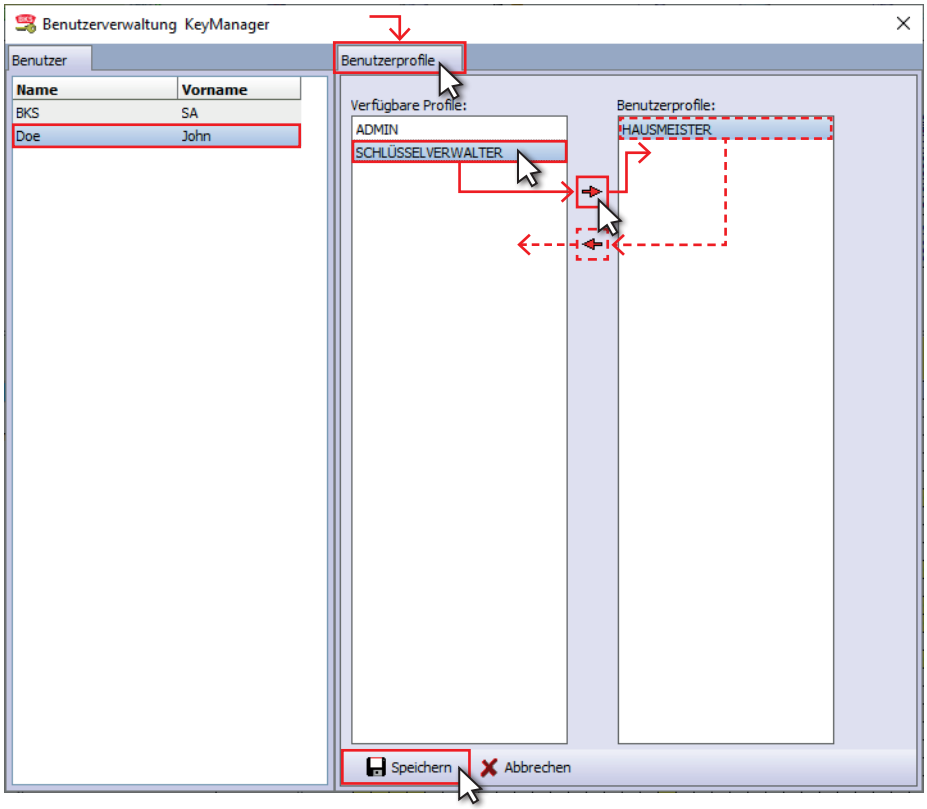
- Wählen Sie das Register „Benutzerdaten“ aus und bearbeiten die Daten zum Benutzer.
- Drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern.



6.4.2 Benutzerprofile zuordnen

Über das Register „Benutzerprofile“ werden dem vorher in der linken Spalte markierten Benutzer durch die Zuordnung eines Benutzerprofils die Rechte zur Nutzung der im Profil enthaltenen Transaktionen gewährt. Bei der Zuordnung mehrere Profile wird die Summe der Rechte gewährt.

- Wählen Sie das Register „Benutzerprofile“ in der rechten Spalte aus.
- Zum Hinzufügen wählen Sie ein Benutzerprofil in der Spalte „Verfügbare Profile“ aus. Drücken Sie auf den Button „Pfeil nach rechts“, um das Profil in die Spalte „Benutzerprofile“ zu verschieben und den Benutzer zu den darin enthaltenen Transaktionen zu berechtigen.
- Zum Entfernen wählen Sie ein Benutzerprofil in der Spalte „Benutzerprofile“ aus. Drücken Sie auf den Button „Pfeil nach links“, um das Profil in die Spalte „Verfügbare Profile“ zurück zu verschieben und die Berechtigung zu den Transaktionen des Profils zu widerrufen.
- Drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern.

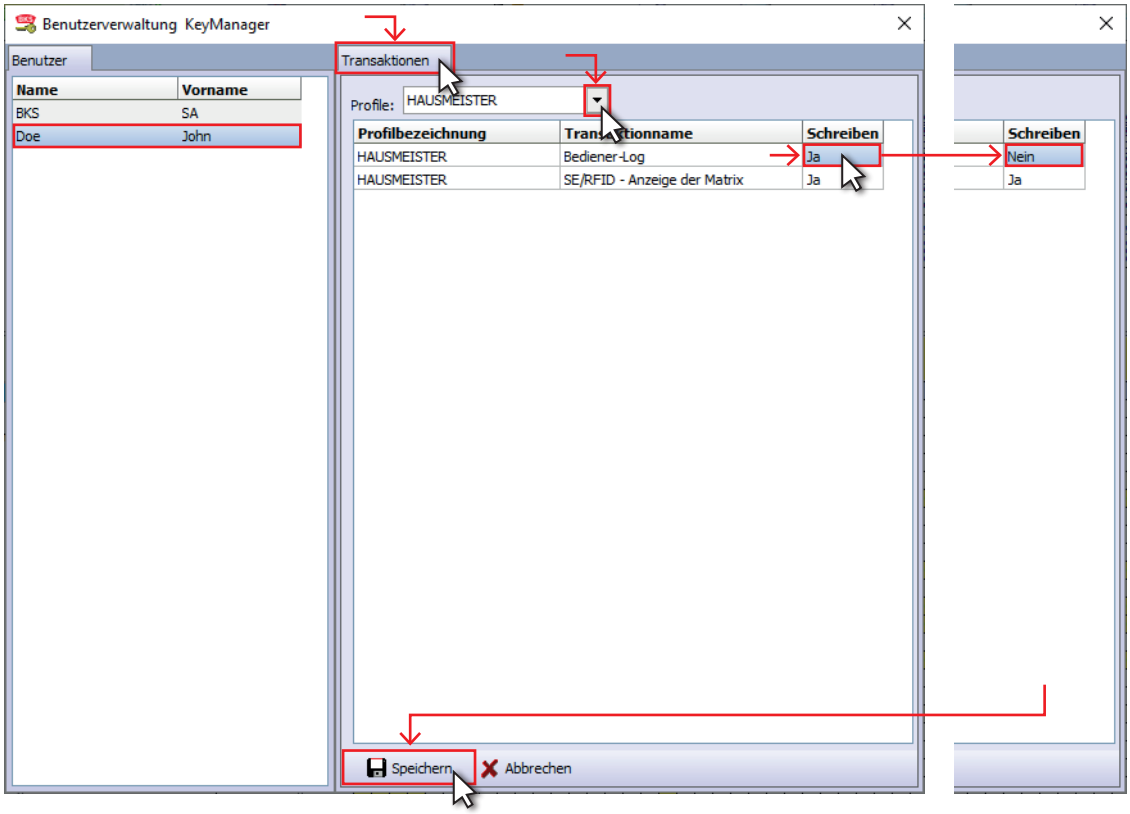


6.4.3 Transaktionen

Mit dem Register „Transaktionen“ wird für den in der linken Spalte markierten Benutzer eine Übersicht der zur Nutzung freigegebenen Transaktionen angezeigt und welche mit der Zuordnung des Benutzerprofils verknüpft worden sind.

Die Rechte zu jeder dieser Transaktionen kann zusätzlich von der voreingestellten Berechtigung zum Schreiben in ein nur Leserecht geändert werden. Ist in der Spalte „Schreiben“ zu einer Transaktion das Attribut „Nein“ gesetzt, hat der Benutzer nur das Recht, sich die Funktionen der Transaktion anzusehen. Bei Transaktionen, welche in der Spalte „Schreiben“ über das Attribut „Ja“ verfügen, kann Benutzer zusätzlich auch Änderungen in der Berechtigungsmatrix im Rahmen der Transaktion ausführen. Aus diesem Grund sollten Benutzer für die Transaktionen, bei denen Sie eine Datenpflege vornehmen, ein Schreibrecht „Ja“ erhalten.

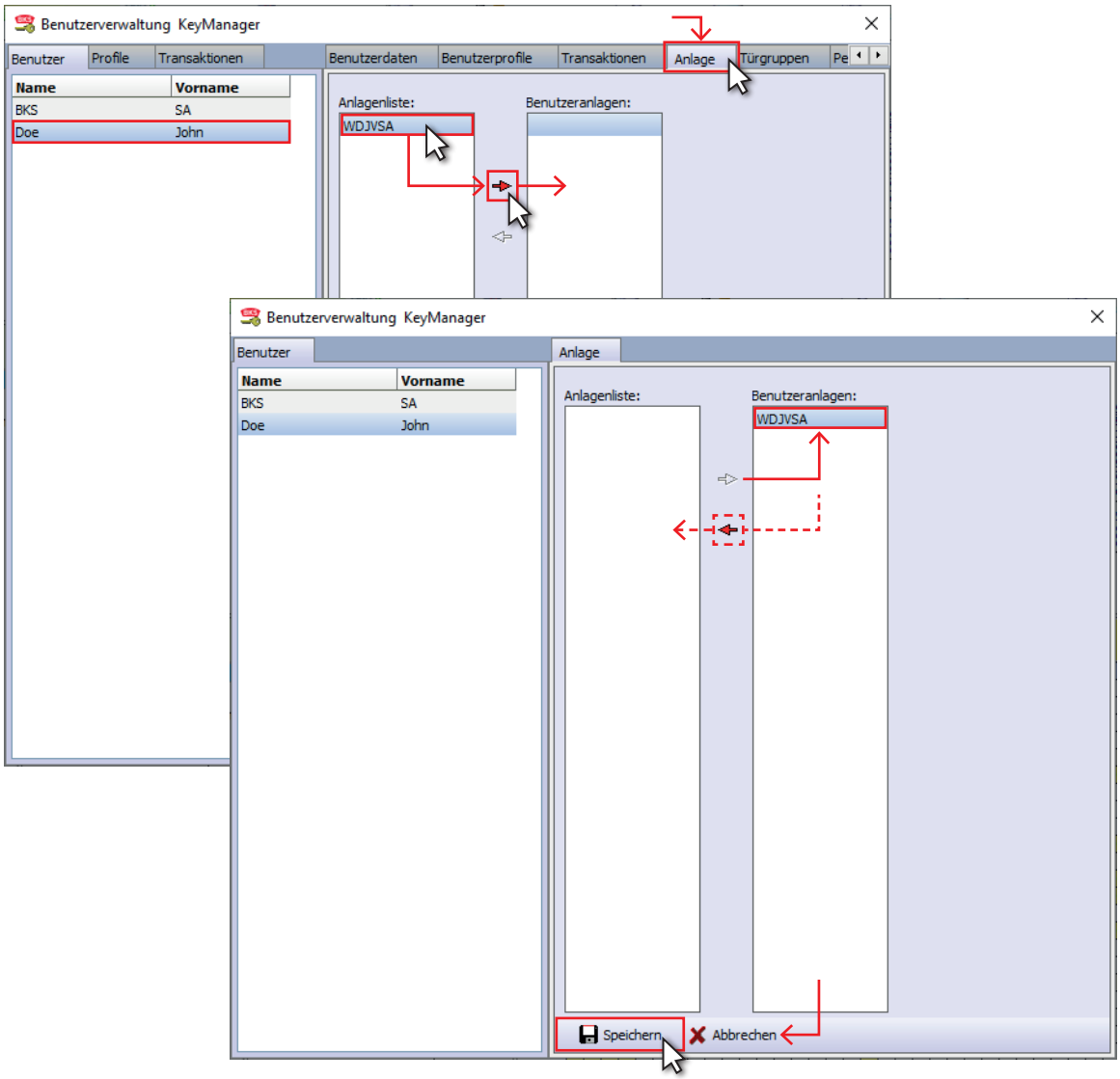
- Wählen Sie das Register „Transaktionen“ in der rechten Spalte aus.
- Über das Dropdown-Menü können Sie die angezeigten Transaktionen durch Auswahl eines Benutzerprofils auf dieses beschränken oder sich alle Transaktionen des Benutzers mit „Alle Rollen“ anzeigen lassen.
- Durch einen Doppelklick auf die Zelle in der Spalte „Schreiben“ kann die Berechtigung zwischen Leserecht „Nein“ und Schreibrecht „Ja“ zu der jeweils in der gleichen Zeile befindlichen Transaktion gewechselt werden.
- Drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern.



6.4.4 Anlagen

Das Register „Anlagen“ zeigt in der Anlagenliste eine Übersicht der im BKS KeyManager verwalteten Schließanlagen an. Durch Zuordnung können Sie festlegen, zu welchen in der Datenbank enthaltenen Schließanlagen der Benutzer Zugriff haben soll. Der in linken Spalte „Benutzer“ markierte Benutzer ist bei den in der Spalte „Benutzeranlagen“ aufgeführten Anlagen zum Zugriff berechtigt.

- Wählen Sie das Register „Anlage“ in der rechten Spalte aus.
- Zum Hinzufügen wählen Sie eine Anlage in der Spalte „Anlagenliste“ aus. Drücken Sie auf den Button „Pfeil nach rechts“, um die Anlage in die Spalte „Benutzeranlagen“ zu verschieben und den Benutzer den Zugriff zu dieser Anlage zu gewähren.
- Zum Entfernen wählen Sie eine Anlage in der Spalte „Benutzeranlagen“ aus. Drücken Sie auf den Button „Pfeil nach links“, um die Anlage in die Spalte „Anlagenliste“ zurück zu verschieben und den Zugriff auf diese Anlage zu widerrufen.
- Drücken Sie auf den Button „Speichern“, um die Eingaben zu sichern.



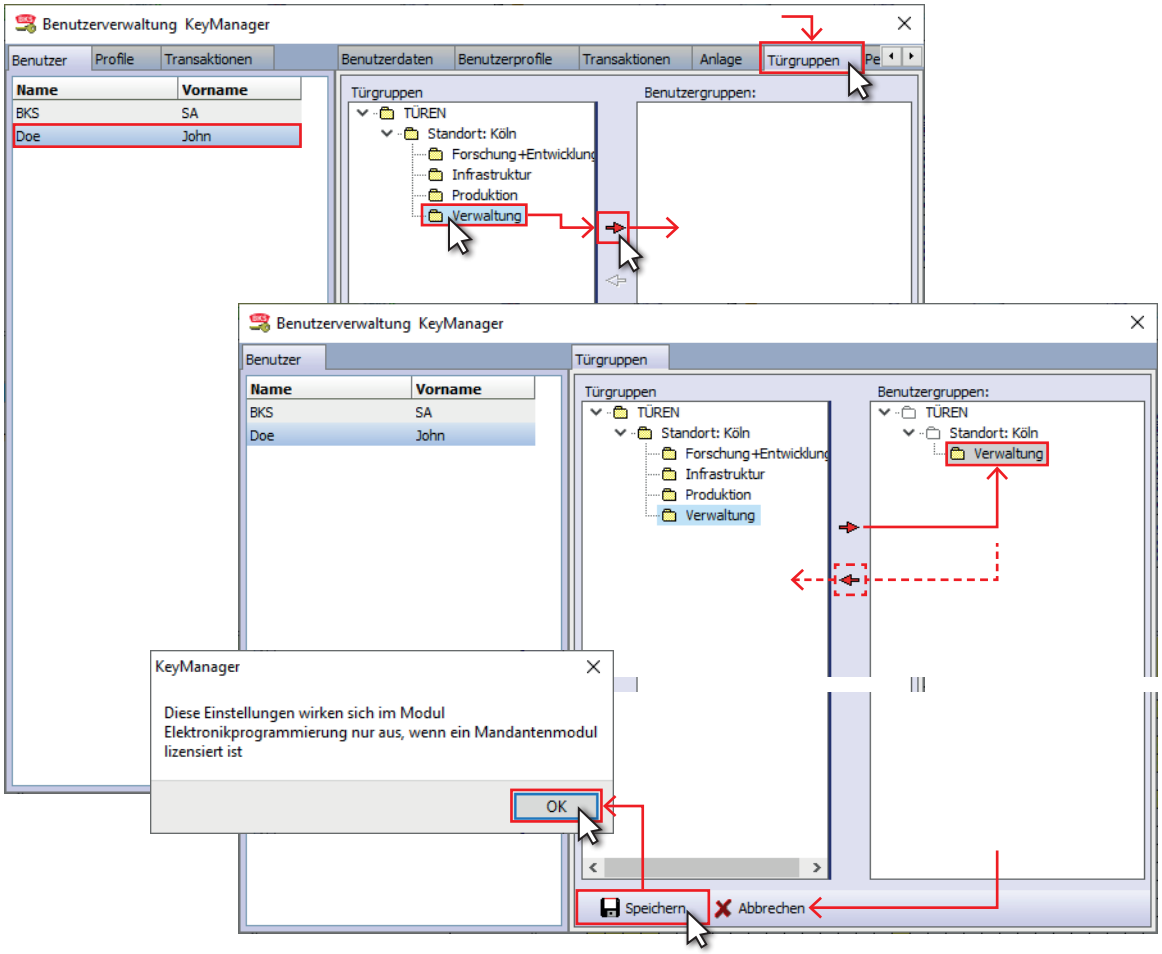
6.4.5 Türgruppen

Im Register „Türgruppen“ können Sie je nach Umfang der verwalteten Schließanlage und Verwendung der Lizenz „Mandanten-Modul“ festlegen, zu welchen Türgruppen der Benutzer Zugriff haben soll. Der in linken Spalte „Benutzer“ markierte Benutzer ist bei den in der Spalte „Benutzergruppen“ aufgeführten Türgruppen zum Zugriff berechtigt.

Dadurch haben Sie die Möglichkeit, über die Struktur der Türengruppen den Zugriff auf bestimmte Türgruppen oder auf alle in der Anlage befindlichen Türengruppen zu gewähren. Falls in Ihrer Schließanlage solche Strukturen innerhalb der Türengruppen noch nicht vorhanden sind, besteht die Möglichkeit, im Nachhinein solche Türengruppen zu erstellen, siehe Kapitel 4.4 [212].

HINWEIS **Die Einstellungen im Register „Türgruppen“ sind nur bei Verwendung des BKS KeyManagers mit dem Mandanten-Modul erforderlich.**

- Wählen Sie das Register „Türgruppen“ in der rechten Spalte aus.
- Zum Hinzufügen wählen Sie eine Türgruppe in der Spalte „Türgruppen“ aus. Drücken Sie auf den Button „Pfeil nach rechts“, um die Gruppe in die Spalte „Benutzergruppen“ zu verschieben und den Benutzer einen Zugriff zu dieser Türgruppe zu gewähren.
- Zum Entfernen wählen Sie eine Türgruppe in der Spalte „Benutzergruppen“ aus. Drücken Sie auf den Button „Pfeil nach links“, um die Gruppe in die Spalte „Türgruppen“ zurück zu verschieben und den Zugriff auf die Türgruppe zu widerrufen.
- Drücken Sie auf den Button „Speichern“ und „OK“, um die Eingaben zu sichern.

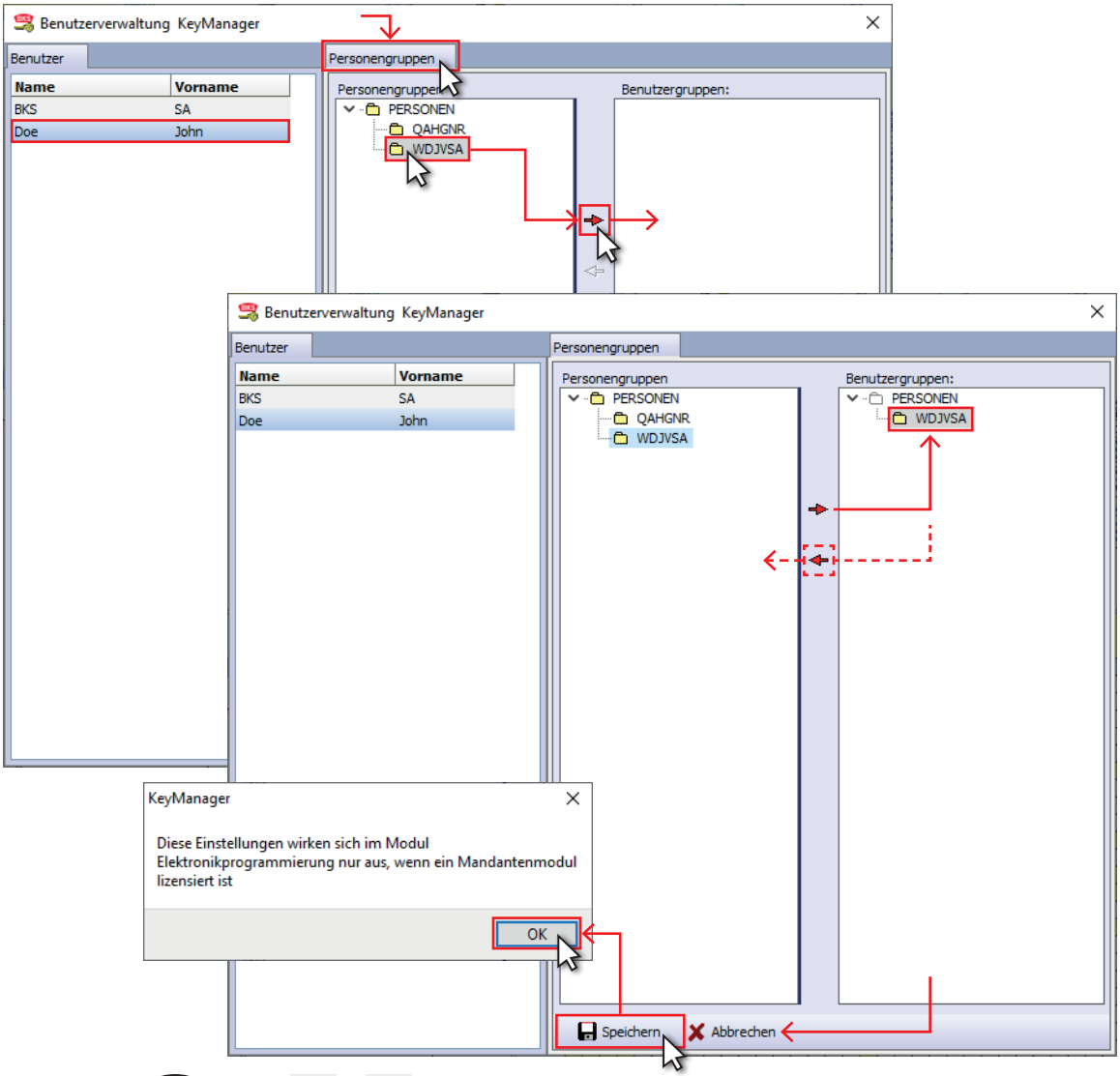


6.4.6 Personengruppen

Im Register „Personengruppen“ können Sie je nach Umfang der verwalteten Schließanlage und Verwendung der Lizenz „Mandanten-Modul“ festlegen, zu welchen Personengruppen der Benutzer Zugriff haben soll. Der in linken Spalte „Benutzer“ markierte Benutzer ist bei den in der Spalte „Benutzergruppen“ aufgeführten Personengruppen zum Zugriff berechtigt.

HINWEIS **Die Einstellungen im Register „Personengruppen“ sind nur bei Verwendung des BKS KeyManagers mit dem Mandanten-Modul erforderlich.**

- Wählen Sie das Register „Personengruppen“ in der rechten Spalte aus.
- Zum Hinzufügen wählen Sie eine Personengruppe in der Spalte „Personengruppen“ aus. Drücken Sie auf den Button „Pfeil nach rechts“, um die Gruppe in die Spalte „Benutzergruppen“ zu verschieben und den Benutzer einen Zugriff zu dieser Personengruppe zu gewähren.
- Zum Entfernen wählen Sie eine Personengruppe in der Spalte „Benutzergruppen“ aus. Drücken Sie auf den Button „Pfeil nach links“, um die Gruppe in die Spalte „Personengruppen“ zurück zu verschieben und den Zugriff auf die Personengruppe zu widerrufen.
- Drücken Sie auf den Button „Speichern“ und „OK“, um die Eingaben zu sichern.

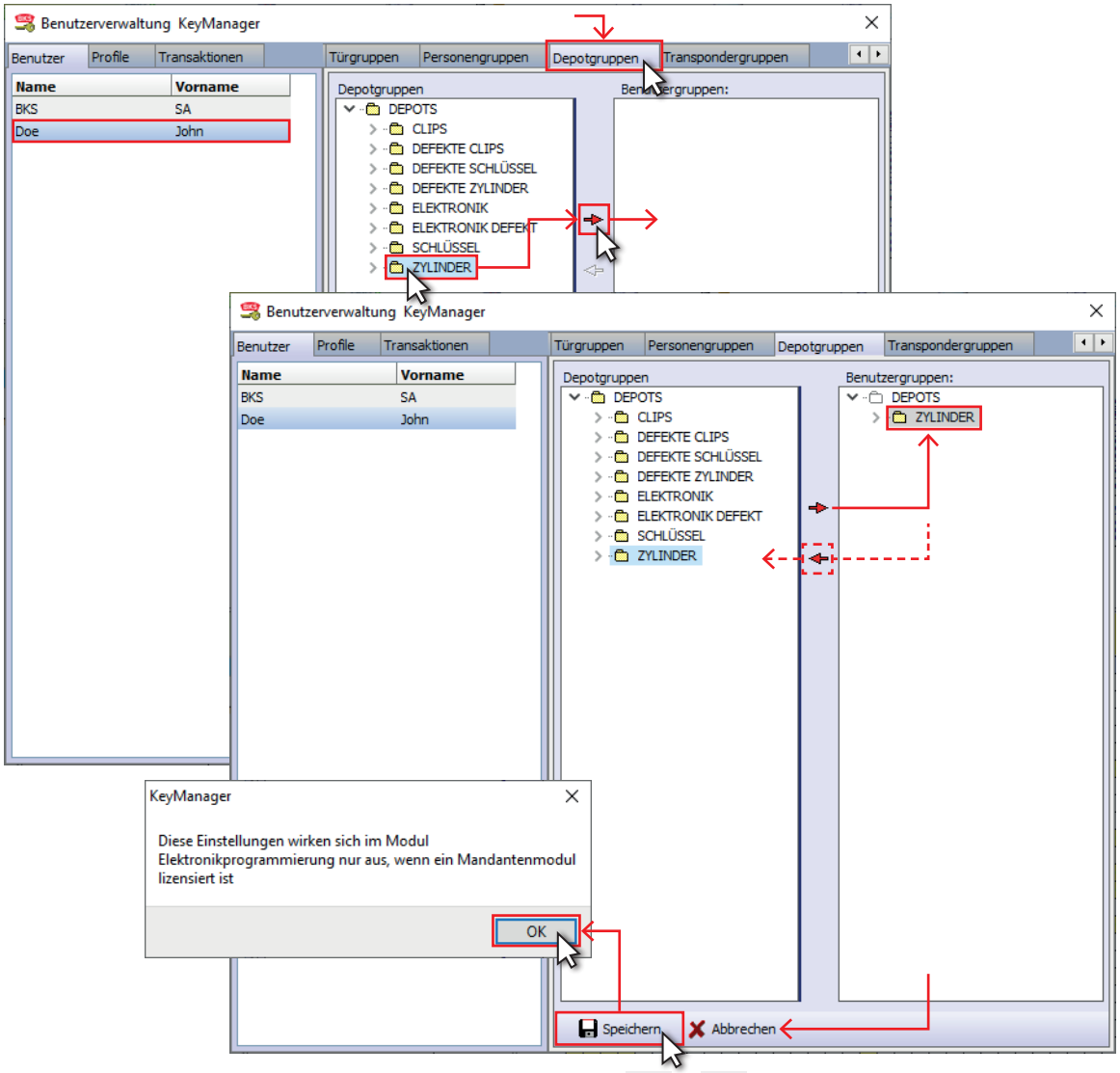


6.4.7 Depotgruppen

Im Register „Depotgruppen“ können Sie je nach Umfang der verwalteten Schließanlage und Verwendung der Lizenz „Mandanten-Modul“ festlegen, zu welchen Depotgruppen der Benutzer Zugriff haben soll. Der in linken Spalte „Benutzer“ markierte Benutzer ist bei den in der Spalte „Benutzeranlagen“ aufgeführten Depotgruppen zum Zugriff berechtigt.

HINWEIS **Die Einstellungen im Register „Depotgruppen“ sind nur bei Verwendung des BKS KeyManagers mit dem Mandanten-Modul erforderlich.**

- Wählen Sie das Register „Depotgruppen“ in der rechten Spalte aus.
- Zum Hinzufügen wählen Sie eine Depotgruppe in der Spalte „Depotgruppen“ aus. Drücken Sie auf den Button „Pfeil nach rechts“, um die Gruppe in die Spalte „Benutzergruppen“ zu verschieben und den Benutzer einen Zugriff zu dieser Depotgruppe zu gewähren.
- Zum Entfernen wählen Sie eine Depotgruppe in der Spalte „Benutzergruppen“ aus. Drücken Sie auf den Button „Pfeil nach links“, um die Gruppe in die Spalte „Depotgruppen“ zurück zu verschieben und den Zugriff auf die Depotgruppe zu widerrufen.
- Drücken Sie auf den Button „Speichern“ und „OK“, um die Eingaben zu sichern.

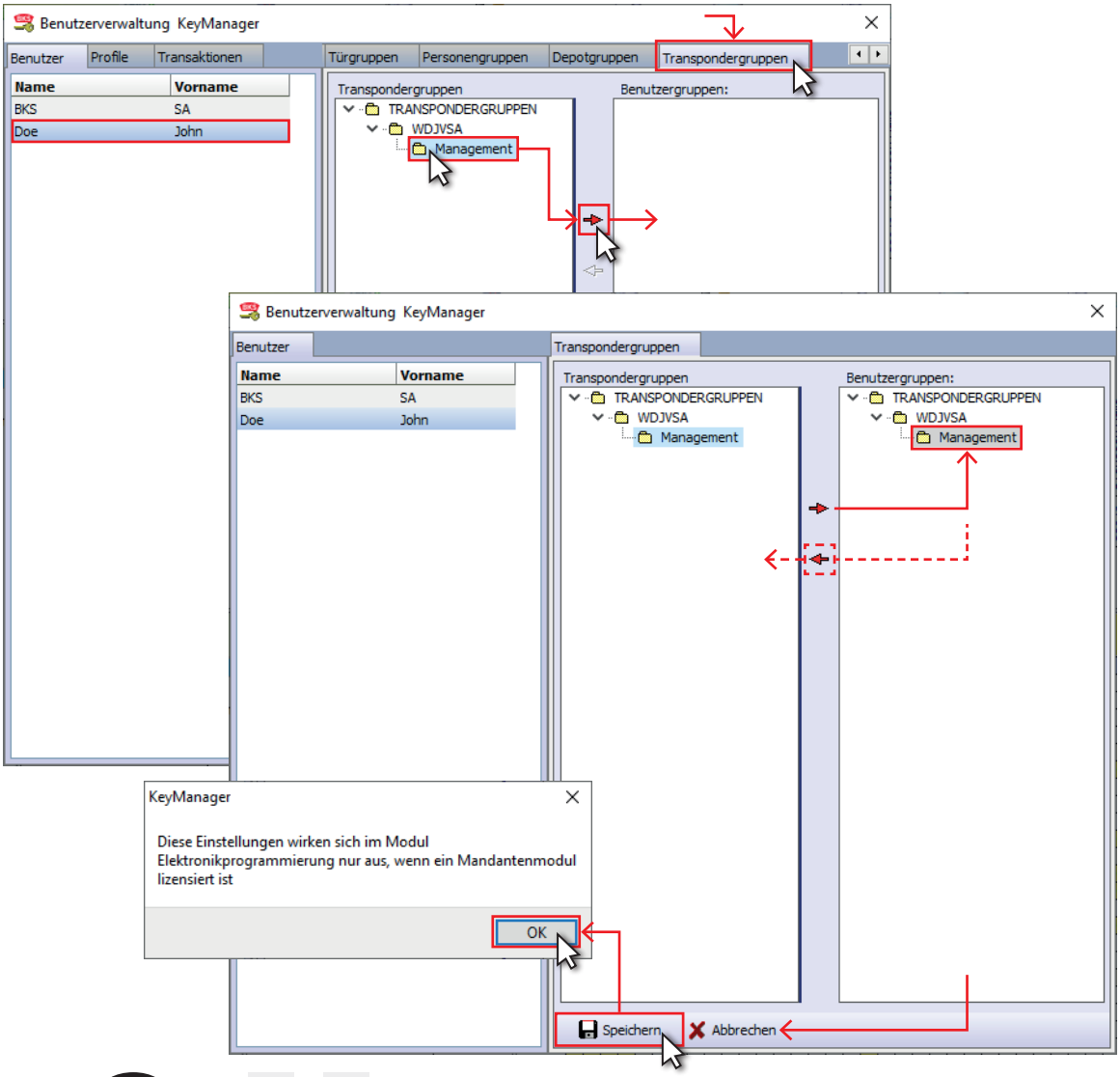


6.4.8 Transpondergruppen

Im Register „Transpondergruppen“ können Sie je nach Umfang der verwalteten Schließanlage und Verwendung der Lizenz „Mandanten-Modul“ festlegen, zu welchen Transpondergruppen der Benutzer Zugriff haben soll. Der in linken Spalte „Benutzer“ markierte Benutzer ist bei den in der Spalte „Benutzergruppen“ aufgeführten Transpondergruppen zum Zugriff berechtigt.

HINWEIS **Die Einstellungen im Register „Transpondergruppen“ sind nur bei Verwendung des BKS KeyManagers mit dem Mandanten-Modul erforderlich.**

- Wählen Sie das Register „Transpondergruppen“ in der rechten Spalte aus.
- Zum Hinzufügen wählen Sie eine Transpondergruppe in der Spalte „Transpondergruppen“ aus. Drücken Sie auf den Button „Pfeil nach rechts“, um die Gruppe in die Spalte „Benutzergruppen“ zu verschieben und den Benutzer einen Zugriff zu dieser Transpondergruppe zu gewähren.
- Zum Entfernen wählen Sie eine Transpondergruppe in der Spalte „Benutzergruppen“ aus. Drücken Sie auf den Button „Pfeil nach links“, um die Gruppe in die Spalte „Transpondergruppen“ zurück zu verschieben und den Zugriff auf die Transpondergruppe zu widerrufen.
- Drücken Sie auf den Button „Speichern“ und „OK“, um die Eingaben zu sichern.

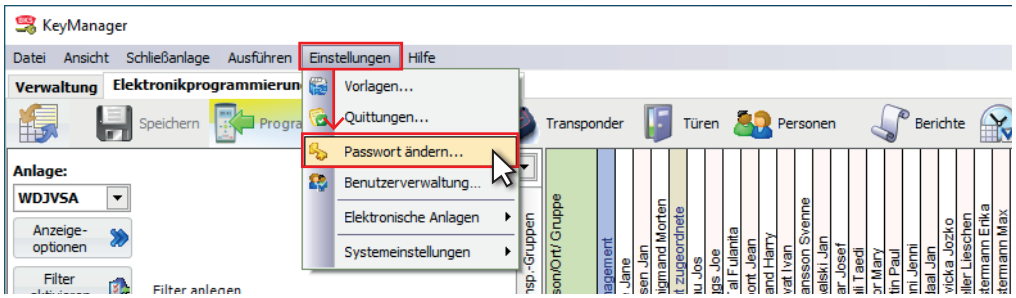


6.5 Passwort des Benutzers ändern

Diese Funktion ermöglicht es, dass der aktuell angemeldete Benutzer sein eigenes Passwort, ohne über spezielle Rechte zu verfügen, ändern kann. Bei der Vergabe des neuen Passworts muss die Kennwortrichtlinie eingehalten werden.

Beachten Sie die Empfehlungen zur Erstellung des Passworts im Kapitel 6.1.1 [341] und Einrichtung der Kennwortrichtlinie im Kapitel 6.1.3 [342]. Der Administrator/Superuser kann die Passwörter auch von nicht angemeldeten Benutzern über die Benutzerverwaltung ändern und so bei Verlust ein neues Passwort für einen Benutzer anlegen.

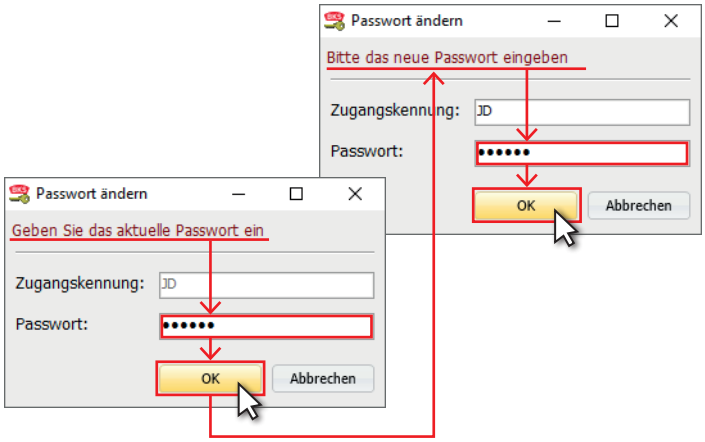
- Öffnen Sie in der Menüleiste das Dropdown-Menü „Einstellungen“ und wählen den Menüpunkt „Passwort ändern ...“ aus.



Im folgenden Dialog müssen Sie das aktuelle und das neue Passwort eingeben.

- Geben Sie das aktuelle Passwort ein und drücken zur Bestätigung auf den Button „OK“.
- Anschließend können Sie das neue Passwort eingeben und das geänderte Passwort durch Drücken des Buttons „OK“ übernehmen.

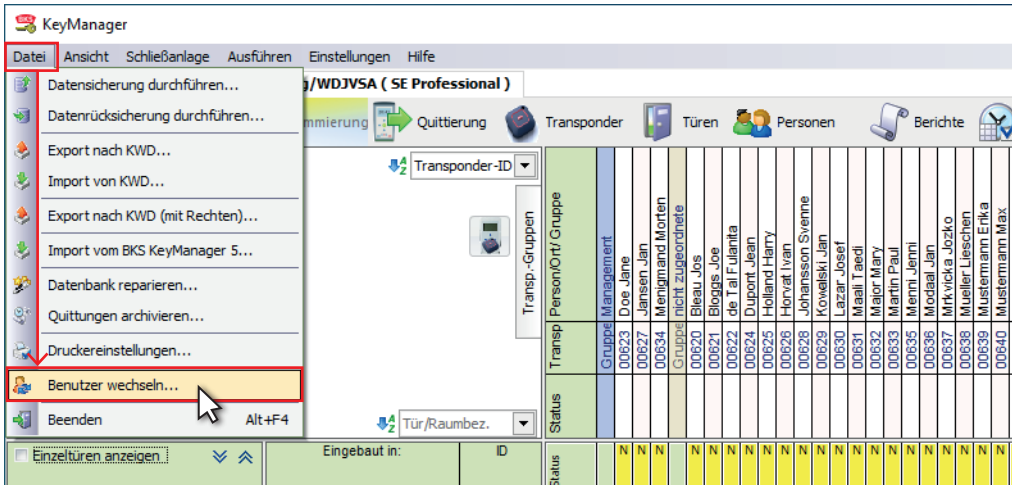
Das Nichteinhalten der Kennwortrichtlinie oder die falsche Eingabe des aktuellen Passworts für zu einer Fehlermeldung und fordert Sie zur Korrektur Ihrer Eingabe auf.



6.6 Wechseln des angemeldeten Benutzers

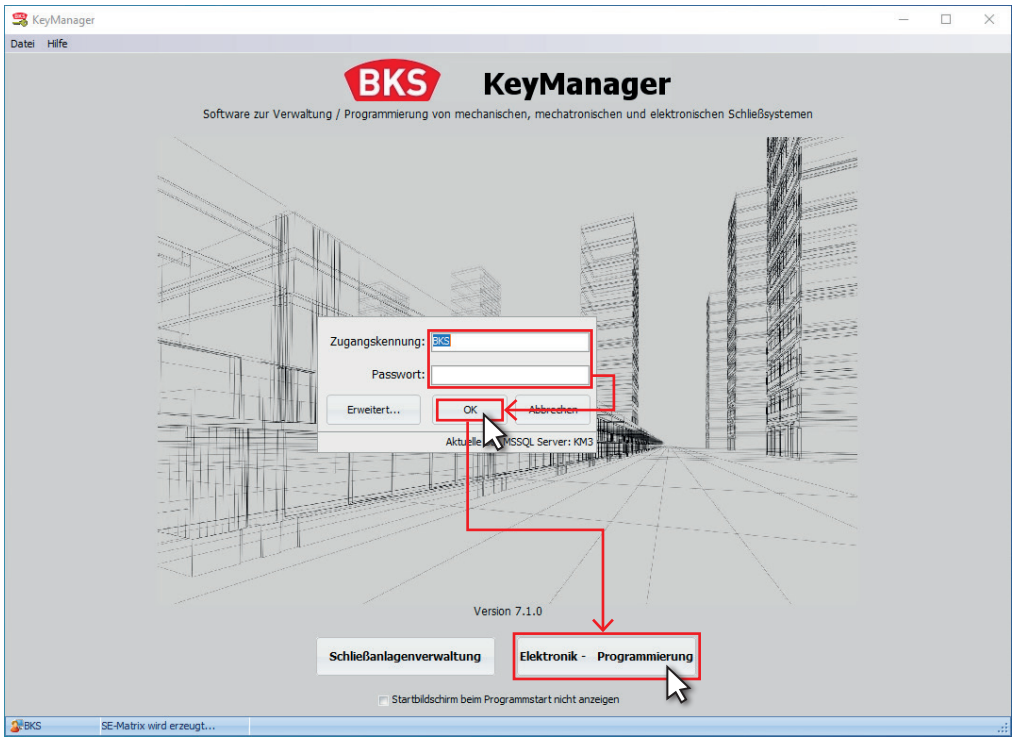
Im laufenden Betrieb des BKS KeyManagers ist es möglich den angemeldeten Benutzer zu wechseln, ohne dass ein Neustart der Software nötig ist.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Datei“ und wählen den Menüpunkt „Benutzer wechseln ...“ aus.



Der aktuelle Benutzer wird abgemeldet und es erscheint der Startbildschirm mit der Aufforderung zur Eingabe der Authentifizierung des neuen Benutzers.

- Geben Sie die „Zugangskennung“ und das „Passwort“ des neuen Benutzers ein.
- Drücken Sie auf den Button „OK“ und auf „Elektronik-Programmierung“ zum Abschluss der Anmeldung.



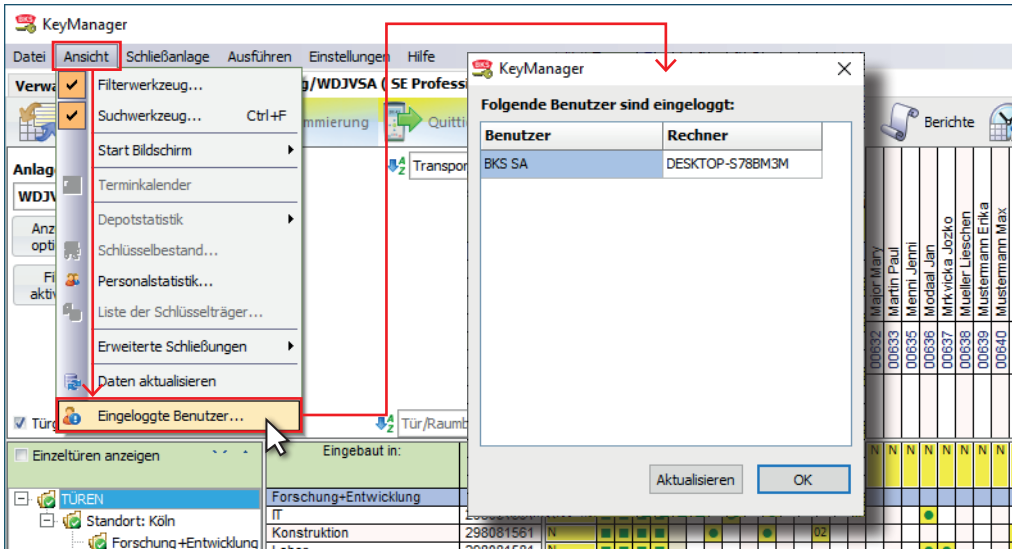
6.7 Anzeige der eingeloggten Benutzer

Mit dieser Funktion können Sie sich alle aktuell in der lokalen Datenbank bzw. im Datenbankserver des BKS KeyManagers angemeldeten Benutzer anzeigen lassen.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Ansicht“ und wählen den Menüpunkt „Eingeloggte Benutzer ...“ aus.

Im Fenster werden alle in der Datenbank aktuell angemeldeten Benutzer angezeigt. Um Benutzer anzuzeigen, die sich nach dem Aufrufen dieses Dialogs in der Datenbank angemeldet haben, drücken Sie auf den Button „Aktualisieren“.

- Drücken Sie auf den Button „OK“, um das Fenster zu schließen.



7. Sonstiges

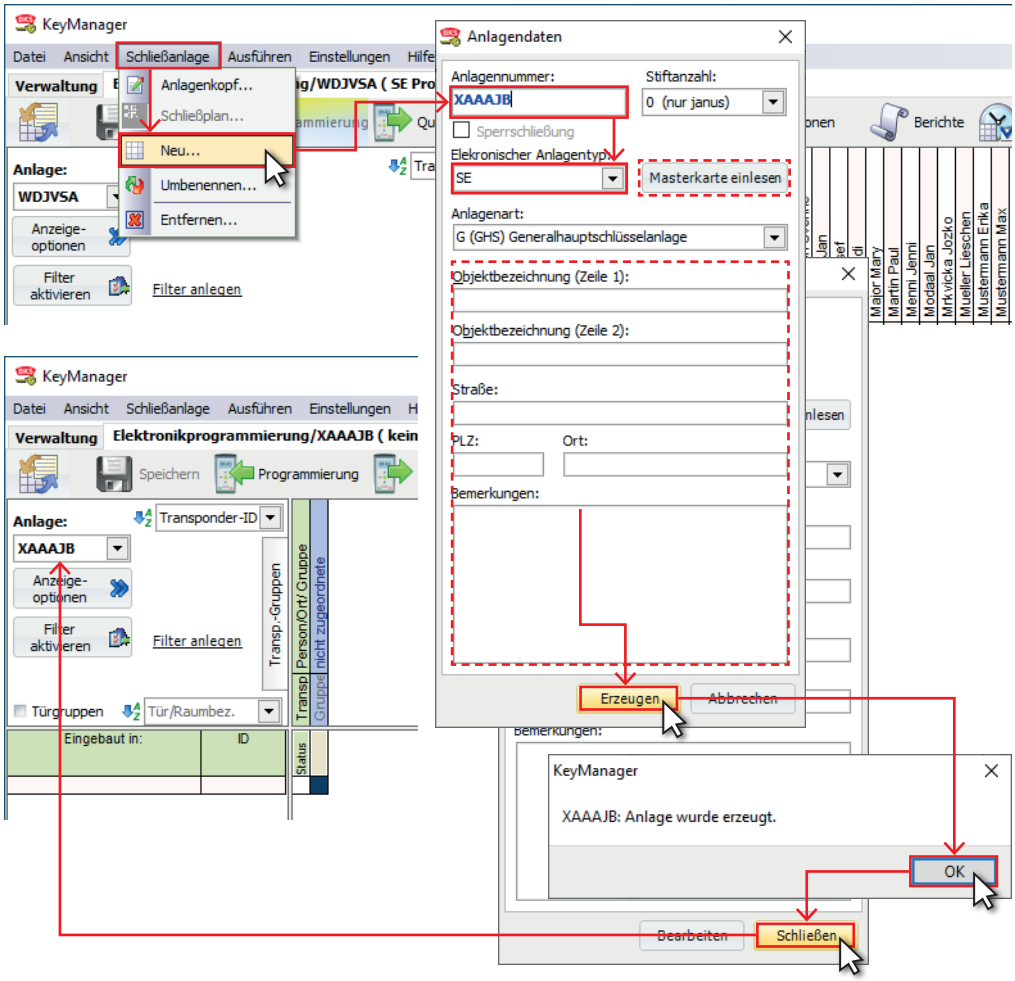
7.1 Schließanlagenverwaltung

Mithilfe der Funktionen der Schließanlagenverwaltung können Sie in der Datenbank mehrere Schließanlagen verwalten.

7.1.1 Anlegen einer neuen Schließanlage

Mit dieser Funktion können Sie eine neue Schließanlage in der Datenbank anlegen. Die neue Anlage wird parallel zu den vorhandenen Anlagen geführt und verwaltet.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Schließanlage“ und wählen den Menüpunkt „Neu ...“ aus.
- Geben Sie die „Anlagennummer:“ und den „Elektronischer Anlagentyp:“ in den Feldern an. Optional können Sie die Masterkarte einlesen und weitere Bezeichnungen zur Anlage eingeben.
- Drücken Sie auf den Button „Erzeugen“.
- Zur Bestätigung drücken Sie auf dem Button „OK“ und „Schließen“zum Beenden.



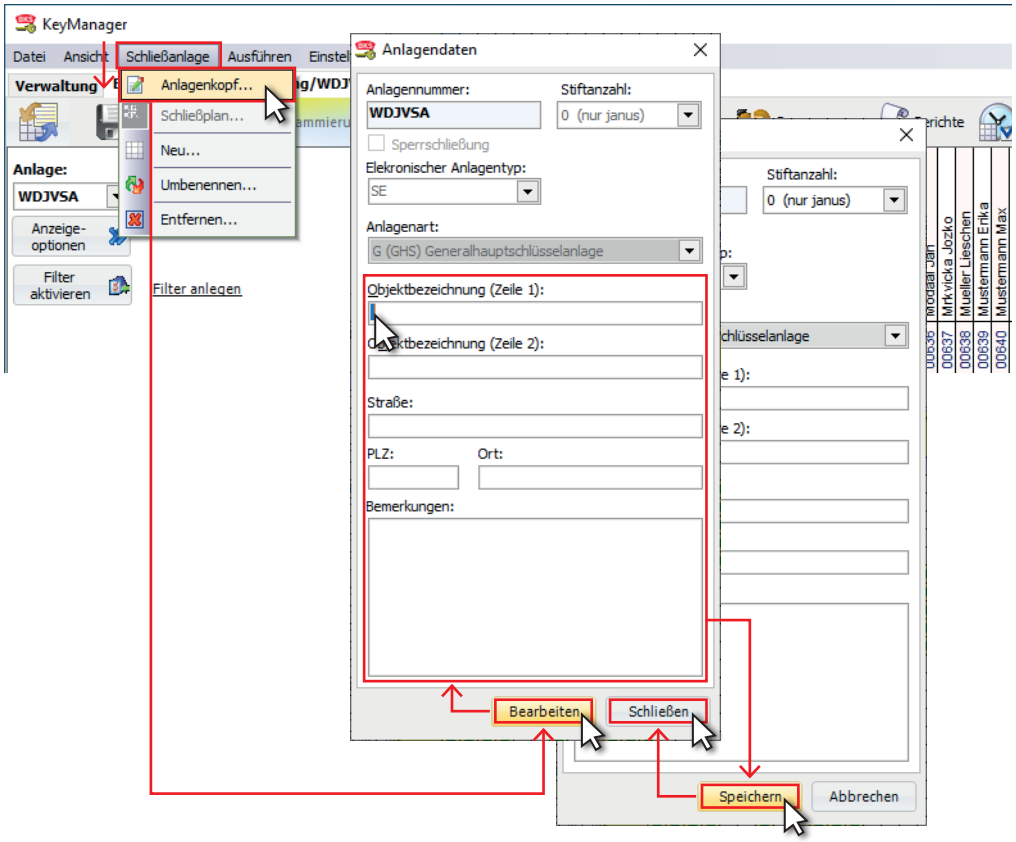
7.1.2 Editieren der Anlagendaten und Bezeichnungen

Die Anlagendaten lassen sich auch nachträglich ändern oder vervollständigen. Nutzen Sie diese Funktion, um die Daten der aktuell aufgerufenen Schließanlage zu bearbeiten.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Schließanlage“ und wählen den Menüpunkt „Anlagenkopf ...“ aus.
- Drücken Sie auf den Button „Bearbeiten“, um die Felder zu editieren.
- Wählen Sie die Felder aus, die verändert werden sollen und bearbeiten den Eintrag.

Änderungen der Anlagendaten im oberen Feld des Fensters dürfen nur bei zwingendem Erfordernis vorgenommen werden, weil Sie die grundlegenden technischen Parameter der Schließanlage betreffen, die von den verwendeten Komponenten vorgegeben werden und bei Falscheingabe die Anlage in ihrer Funktion gestört wird.

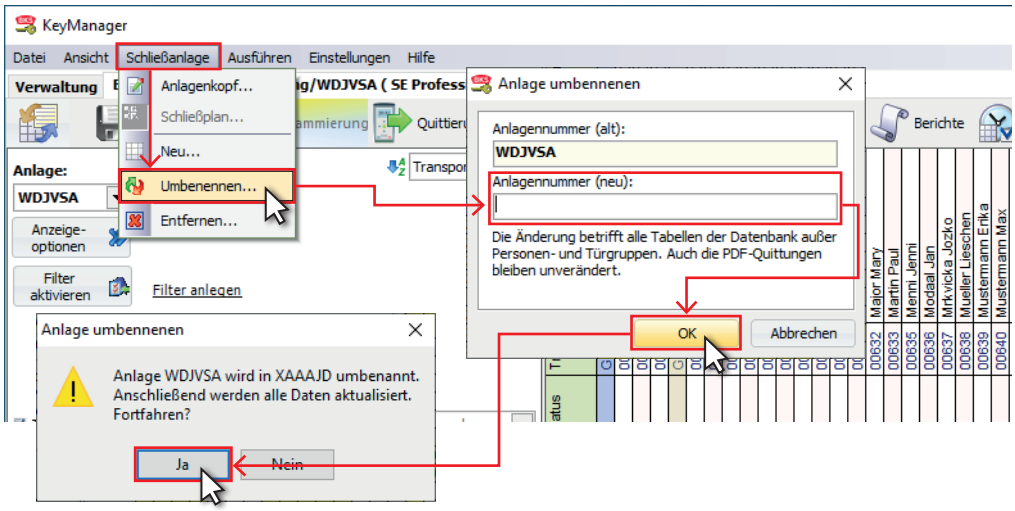
- Drücken Sie auf den Button „Speichern“ und zum Beenden auf den Button „Schließen“.



7.1.3 Umbenennen Schließanlage

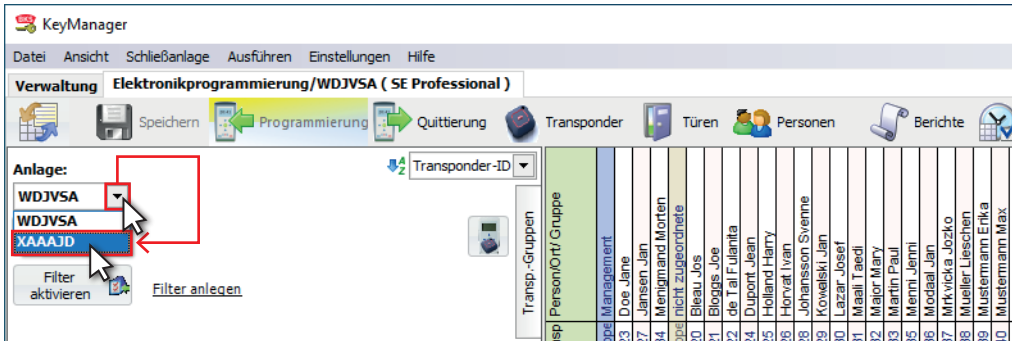
Mit dieser Funktion können Sie die Anlagennummer der Schließanlage umbenennen. Es ist wichtig, dass die Anlagennummer der Schließanlage mit der Anlagennummer der in der Anlage verwendeten Komponenten übereinstimmt.

- Wählen Sie ggf. eine neue Schließanlage zum Umbenennen aus.
- Öffnen Sie in der Menüleiste das Dropdown-Menü „Schließanlage“ und wählen den Menüpunkt „Anlagenkopf ...“ aus.
- Geben Sie im Feld „Anlagennummer (neu):“ eine neue Anlagennummer ein.
- Drücken Sie auf den Button „OK“ und zum Fortfahren auf den Button „Schließen“.



7.1.4 Wechseln der Schließanlage

- Drücken Sie auf das Symbol zum Öffnen des Dropdown-Menüs „Anlage:“.
- Wählen Sie im Dropdown-Menü die Schließanlage aus, zu der Sie wechseln wollen.

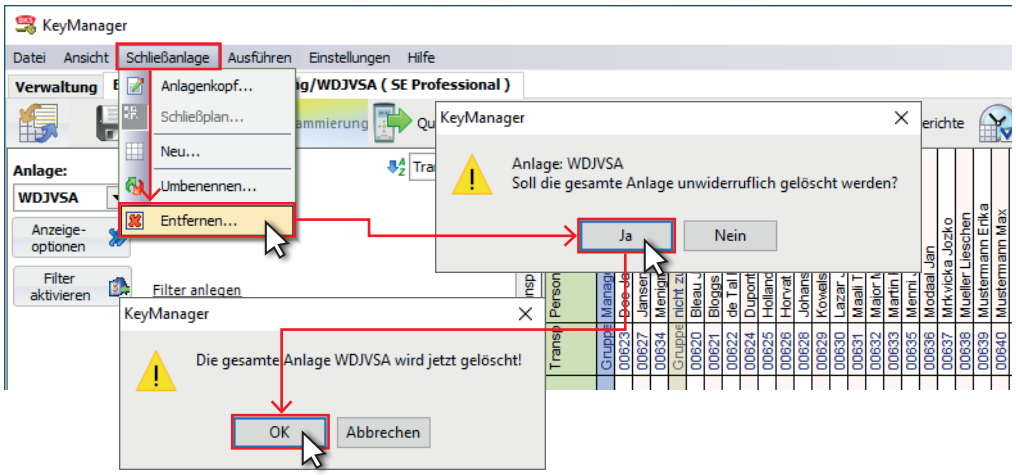


7.1.5 Löschen der Schließanlage

Die aktuell in der Datenbank aktive Schließanlage kann mit dieser Funktion aus der Datenbank gelöscht werden.

- Wählen Sie ggf. eine neue Schließanlage zum Entfernen aus.
- Öffnen Sie in der Menüleiste das Dropdown-Menü „Schließanlage“ und wählen den Menüpunkt „Anlagenkopf ...“ aus.
- Zum Löschen drücken Sie auf den Button „Ja“ und auf „OK“ zur Bestätigung.

Nach dem Entfernen einer von mehreren Schließanlagen aus der Datenbank bleiben verschiedene Anlagendaten wie z. B. Personen, Benutzer etc. in der Datenbank erhalten.

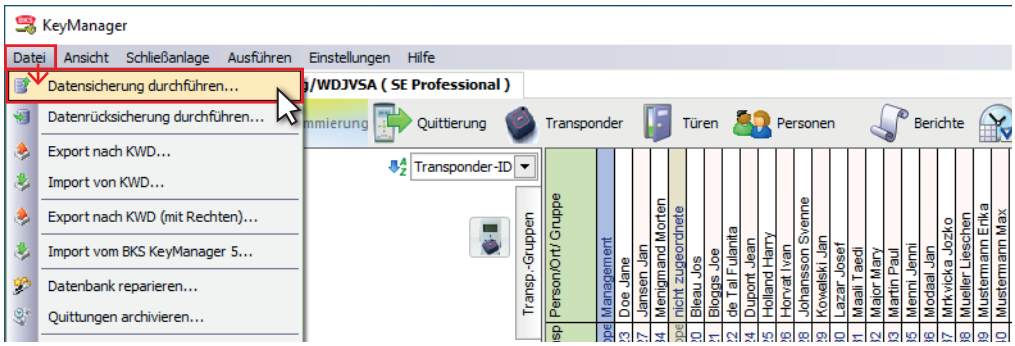


7.2 Datensicherung und Wiederherstellung der Schließanlagen-Datenbank

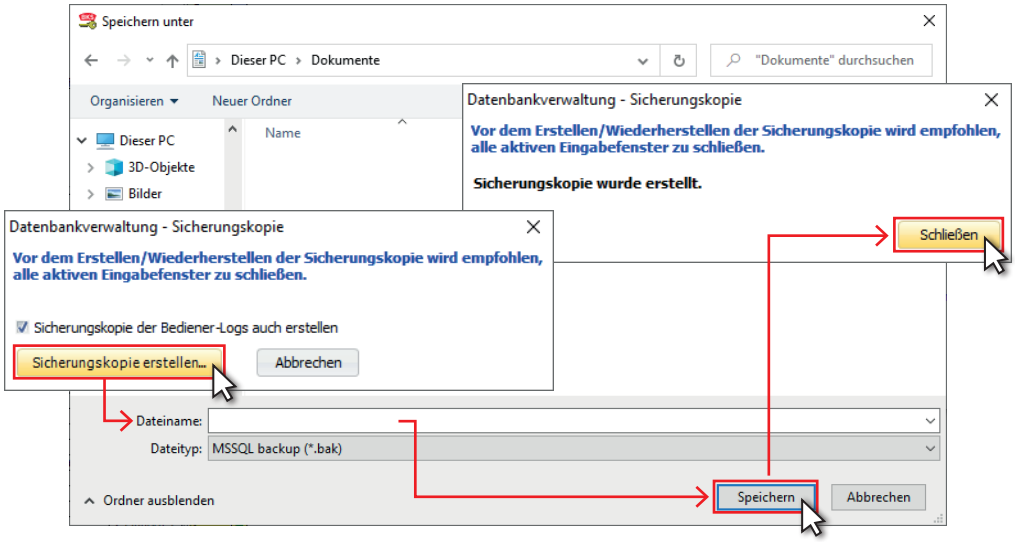
7.2.1 Datensicherung der Schließanlagen-Datenbank erstellen

Zur Vorbeugung von Datenverlusten und zur Steigerung der Datensicherheit wird in regelmäßigen Abständen eine Datensicherung der im BKS KeyManager verwalteten Schließanlagen empfohlen. Dadurch können Sie bei einem Datenverlust die Datenbank und Schließanlagen wiederherstellen und auf den letzten gespeicherten Stand bringen.

- Sollten Sie noch weitere Fenster außer dem Hauptfenster des BKS KeyManagers geöffnet haben, sind diese vor der Datensicherung zu schließen.
- Wählen Sie über das Dropdown-Menü „Datei“ den Menüpunkt „Datensicherung durchführen ...“ aus.



- Drücken Sie auf den Button „Sicherungskopie erstellen ...“.
- Navigieren Sie im Dateibrowser zum Speicherort und geben den Dateinamen ein.
- Drücken Sie auf den Button „Speichern“ und „Schließen“ und Beenden den Dialog.

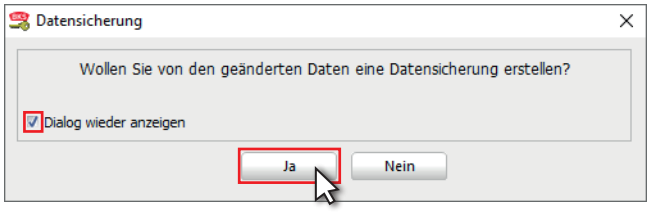


HINWEIS **Der Speicherort der Sicherung sollte den Ansprüchen des Datenschutzes und der Datensicherheit erfüllen, um z. B. Datenverlust durch Defekt oder unberechtigte Zugriffe zu verhindern.**

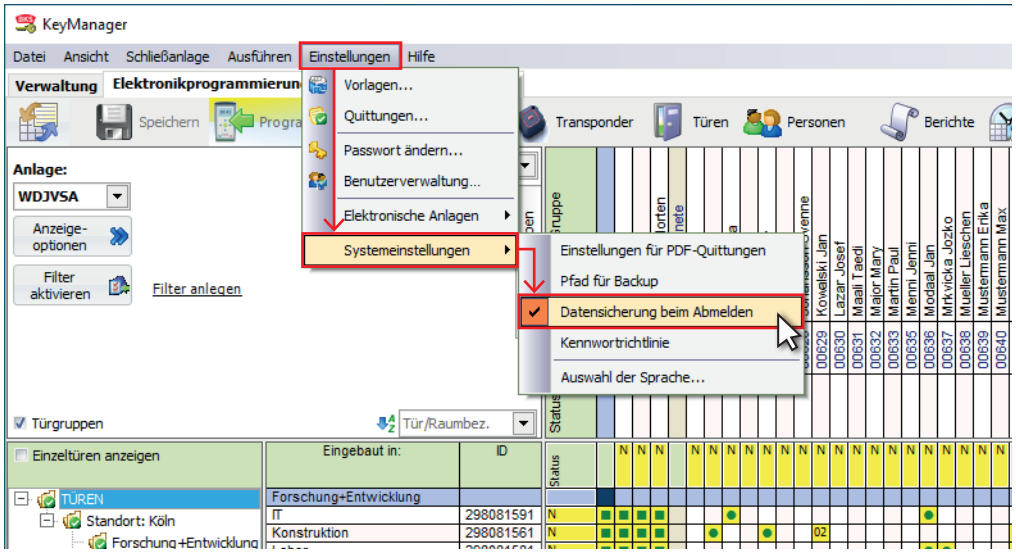
7.2.2 Datensicherung beim Abmelden

Beim Beenden des BKS KeyManagers startet standardmäßig der Dialog „Datensicherung“.

- Drücken Sie auf den Button „Ja“, um eine Datensicherung zu erstellen.
- Der Button „Nein“ beendet den BKS KeyManager ohne eine Sicherung.



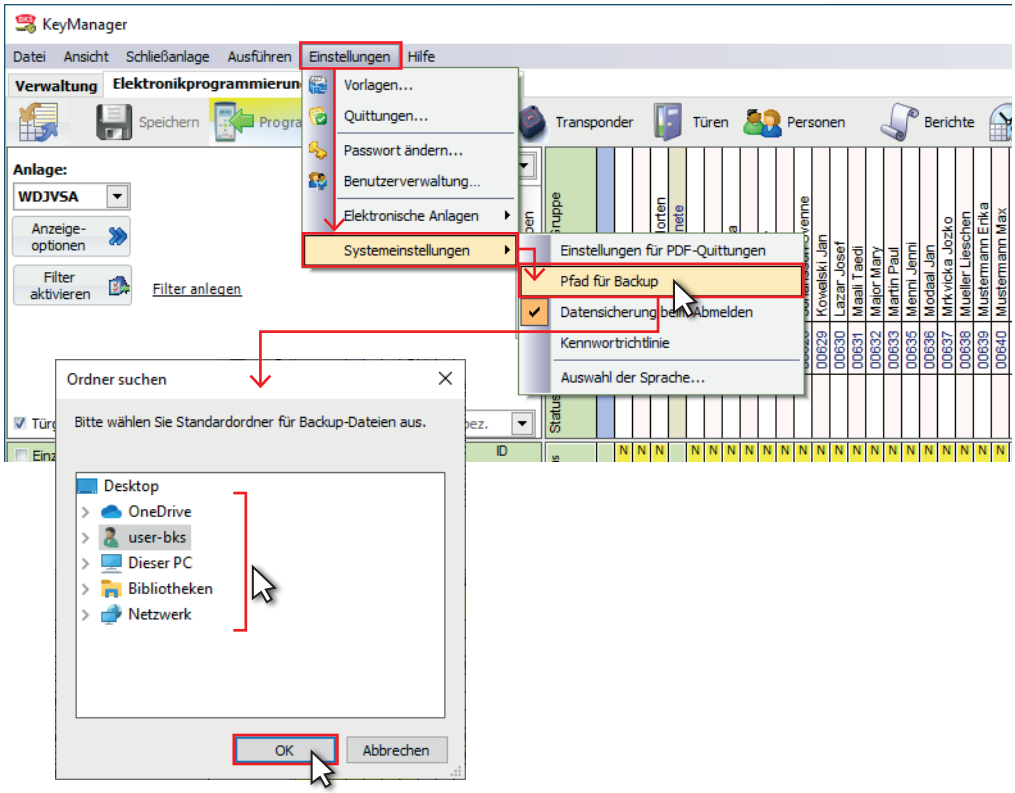
Ist der „Dialog wieder anzeigen“ deaktiviert, z. B. durch Entfernen des Hakens in der Checkbox, wird das Fenster „Datensicherung“ nicht mehr beim Beenden angezeigt. Der Dialog kann durch Auswahl des Menüpunkts „Datensicherung beim Anmelden“ über das unten gezeigte Dropdown-Menü wieder aktiviert werden. Bei Aktivierung steht vor dem Menüpunkt ein Haken. An dieser Stelle ist auch die Deaktivierung möglich.



7.2.3 Pfad für den Speicherort der Datensicherung festlegen

Mit dieser Funktion können Sie einen Ordner als Standard-Speicherort festlegen, an dem die Datensicherung abgelegt werden soll.

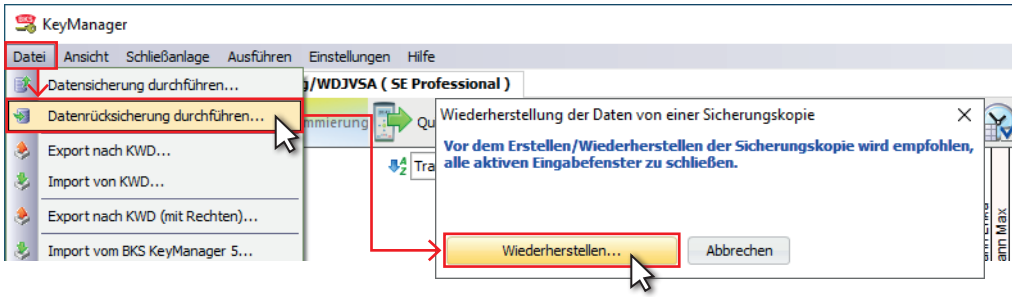
- Öffnen Sie in der Menüleiste das Menü „Einstellungen“ und wählen im Dropdown-Menü „Systemeinstellungen“ den Menüpunkt „Pfad für Backup“ aus.
- Im Fenster „Ordner suchen“ drücken Sie auf das Symbol „>“ und navigieren zu dem Ordner, den Sie als Speicherort festlegen möchten. Wählen Sie diesen Ordner aus.
- Drücken Sie auf den Button „OK“ zum Beenden.



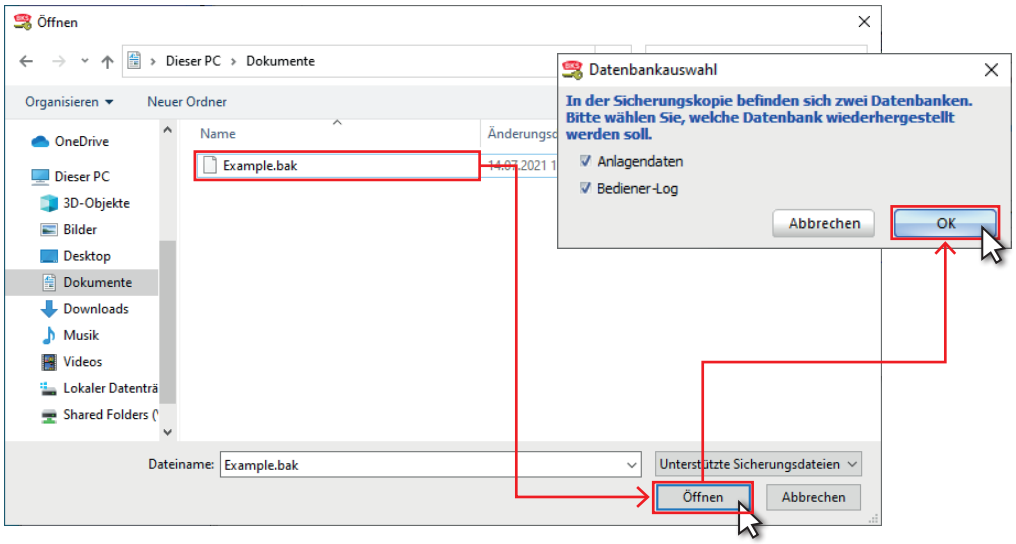
7.2.4 Wiederherstellung der Schließanlagen-Datenbank durch Datenrücksicherung

Diese Funktion ermöglicht es, die Schließanlage mit dem Stand der vorher über die Datensicherung gespeicherten Wiederherstellungsdatei wiederherzustellen. Dabei wird die ggf. aktuell geladene Schließanlage durch die Datenrücksicherung ersetzt.

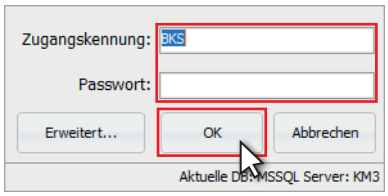
- Wählen Sie über das Dropdown-Menü „Datei“ den Menüpunkt „Datenrücksicherung durchführen ...“ aus.
- Drücken Sie auf den Button „Wiederherstellen ...“.

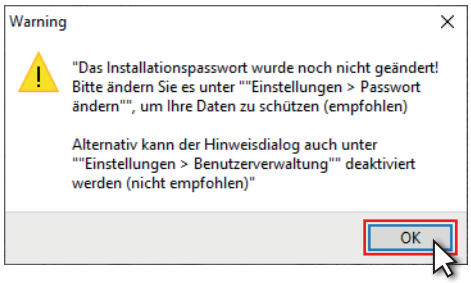


- Navigieren Sie im Dateibrowser zum Speicherort der Wiederherstellungsdatei „*.bak“ oder „*.fbk“. Wählen Sie diese aus und drücken auf den Button „OK“.
- Aktivieren/Deaktivieren Sie ggf. bei Bedarf die Checkboxen und drücken auf den Button „OK“.

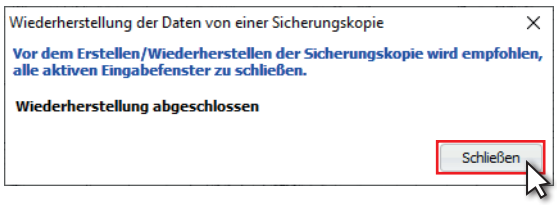


- Melden Sie sich in der Datenbank mit Ihrer „Zugangskennung“ und „Kennwort“ an und drücken auf den Button „OK“. Falls das Passwort noch nicht geändert wurde, ist der Hinweis mit „OK“ zu bestätigen.





- Drücken Sie auf den Button „Schließen“ und beenden den Dialog.



7.3 Schließanlagendatei (KWD-Datei)

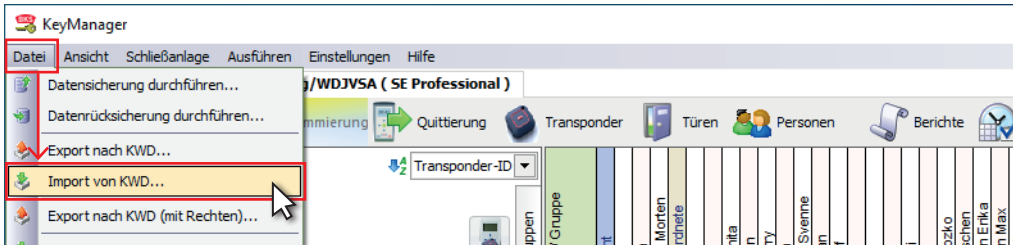
Die KWD-Datei ist ein spezielles Austauschformat, das die Daten der Komponenten enthält, die Bestandteil einer von BKS verwalteten mechanischen oder elektronischen Schließanlage sind bzw. werden sollen. Eine KWD-Datei kann vom BKS KeyManager exportiert oder beim Erwerb von BKS bezogen und über die Importfunktion des BKS KeyManager eingelesen werden.

7.3.1 Import einer KWD-Datei in eine Schließanlage

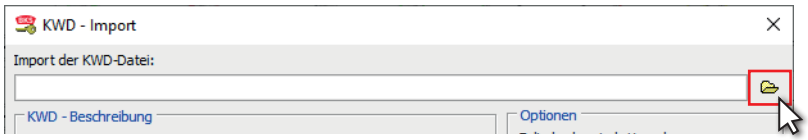
Die Importfunktion kann zum Aufbau oder Erweiterung der Schließanlage, aber auch zum Hinzufügen von einzelnen Transpondern und Zutrittspunkten zur Schließanlage verwendet werden. Beim importieren der KWD-Datei werden die in der Datei enthaltenen Daten der Komponenten automatisch der aktiven Schließanlage hinzugefügt. Die Berechtigungsmatrix und deren Einstellungen sowie die Ereignisse sind über diese Funktion nicht importierbar.

Nach dem Erwerb weiterer Zutrittspunkte können Sie diese mit der Funktion Import KWD-Datei der Schließanlage hinzufügen. Dadurch entfällt ein manuelles Hinzufügen. Eine passende KWD-Datei kann über Ihren Vertriebspartner bezogen werden.

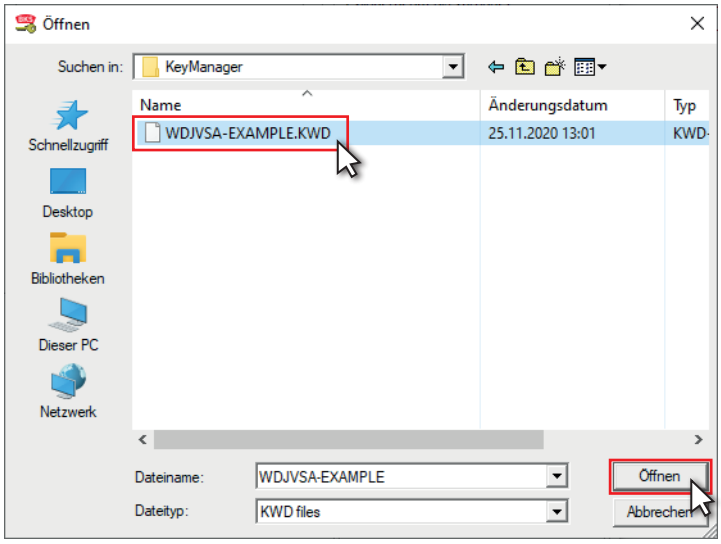
- Öffnen Sie in der Menüleiste das Dropdown-Menü „Datei“ und wählen den Menüpunkt „Import von KWD ...“ aus.



- Drücken Sie auf das Verzeichnissymbol für „KWD-Datei öffnen“.

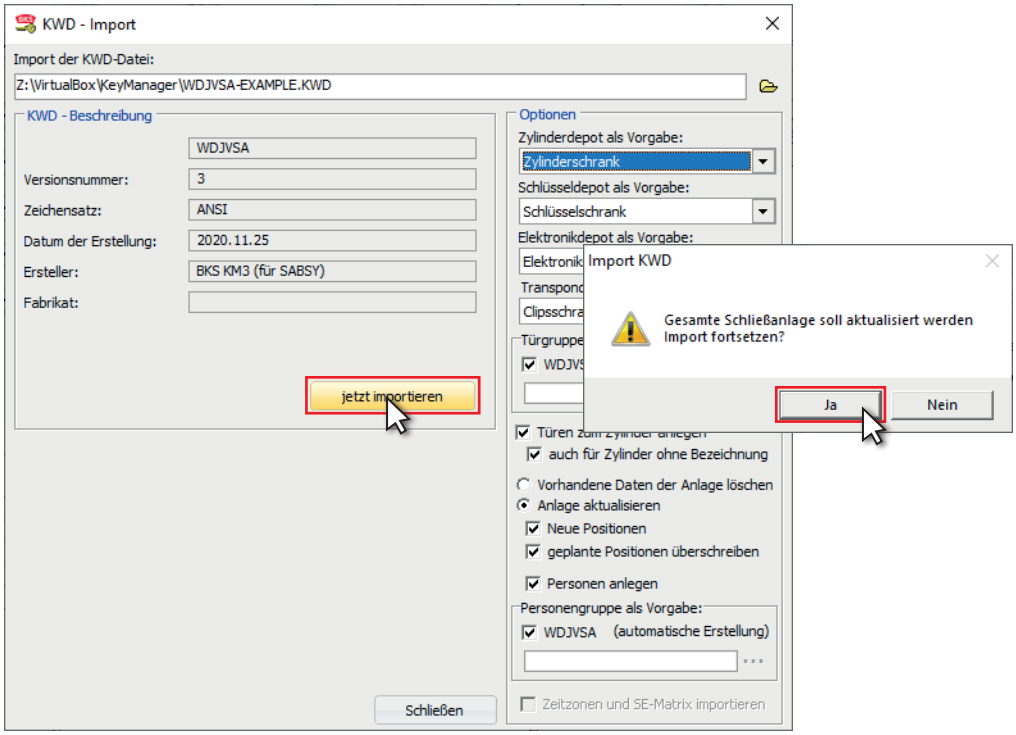


- Navigieren Sie zur KWD-Datei, wählen diese aus und drücken auf den Button „Öffnen“.

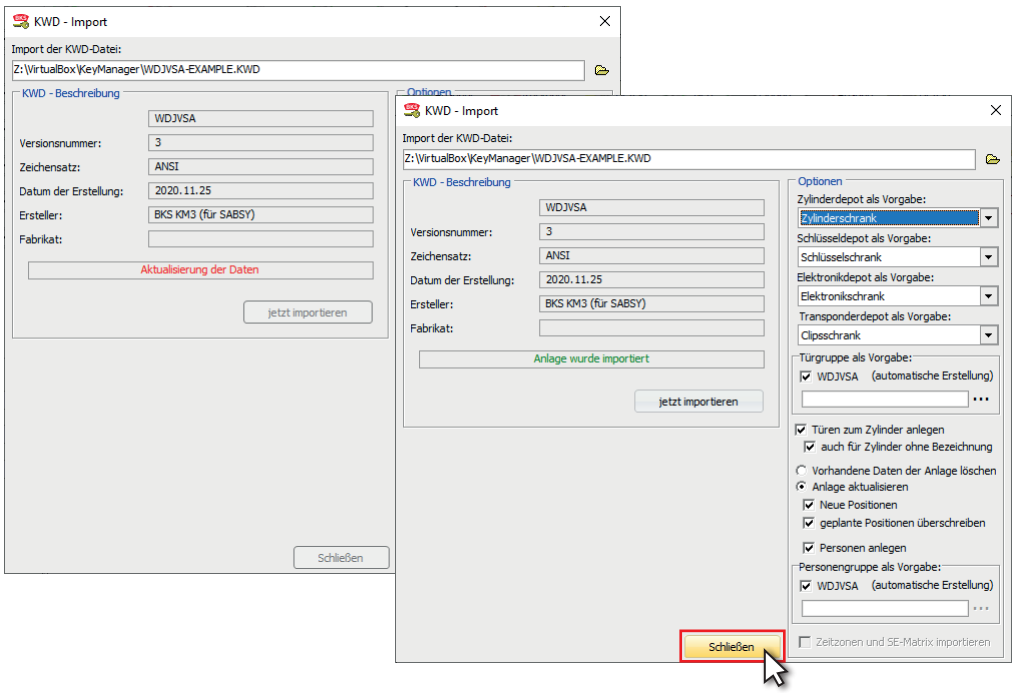


Überprüfen Sie die Importoptionen und passen diese ggf. an.

- Starten Sie die Aktualisierung mit „jetzt importieren“ und bestätigen den Dialog mit „Ja“.



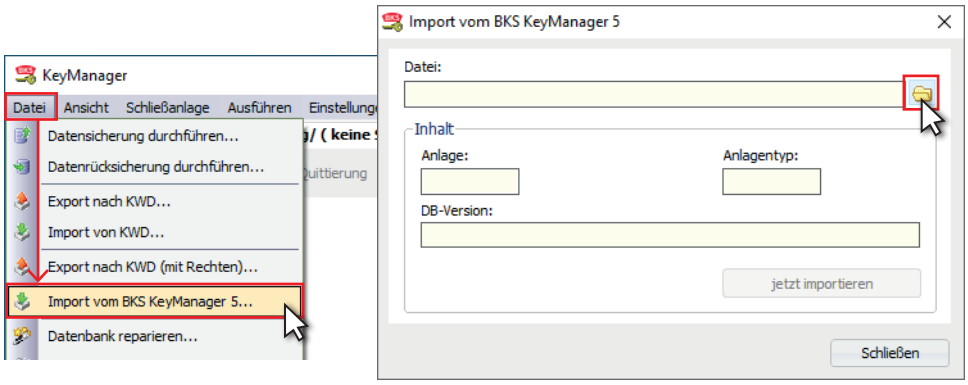
- Nach erfolgreichem Import drücken Sie auf den Button „Schließen“.



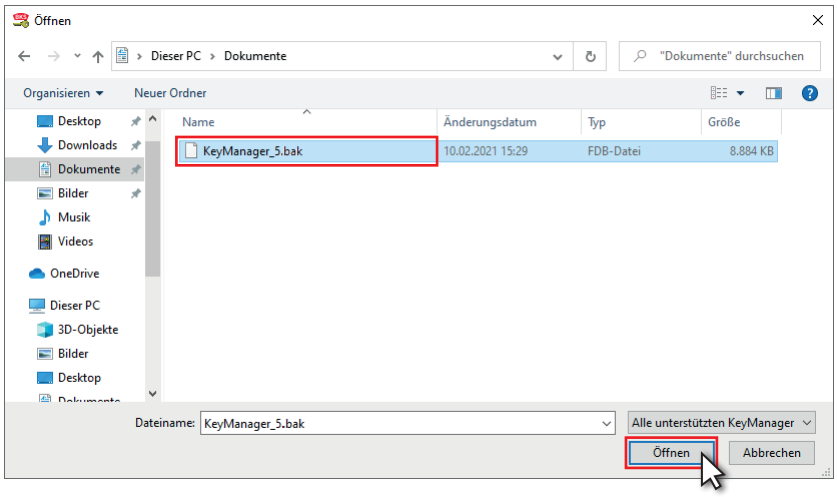
7.3.2 Import einer Schließanlage von Version 5 des BKS KeyManagers

Eine bestehende Schließanlage des BKS KeyManagers 5 ist mit der folgenden Funktion in den BKS KeyManager 7 zu importieren. Grundvoraussetzung ist, dass der BKS KeyManager mit einer MS SQL-Datenbank installiert wurde. Die Version mit interner Datenbank kann hierfür nicht verwendet werden. Weiterhin ist eine in der Programmversion 5 erstellte Datenbank-Datei (*.bak) erforderlich.

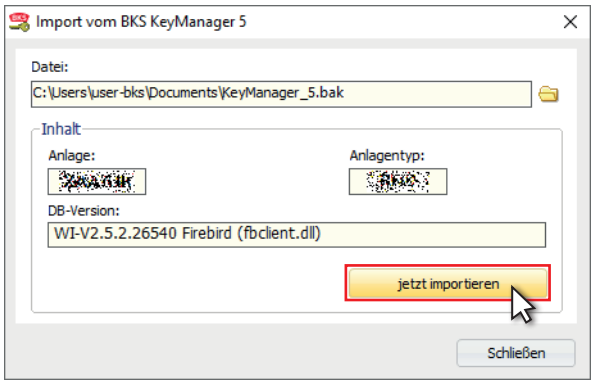
- Wählen Sie über das Dropdown-Menü „Datei“ den Menüpunkt „Import vom KeyManager 5 ...“ aus.
- Drücken Sie auf das Verzeichnissymbol.



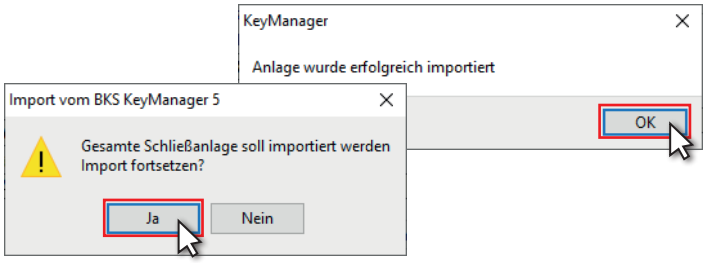
- Navigieren Sie mit dem Dateibrowser zur entsprechenden Sicherungsdatei „*.bak“ und wählen diese aus. Drücken Sie auf den Button „Öffnen“.



- Starten Sie den Import und drücken den Button „jetzt importieren“.



- Beenden Sie den Import der Schließanlage und drücken in den beiden Fenstern jeweils auf den Button „Ja“ und „OK“.



HINWEIS

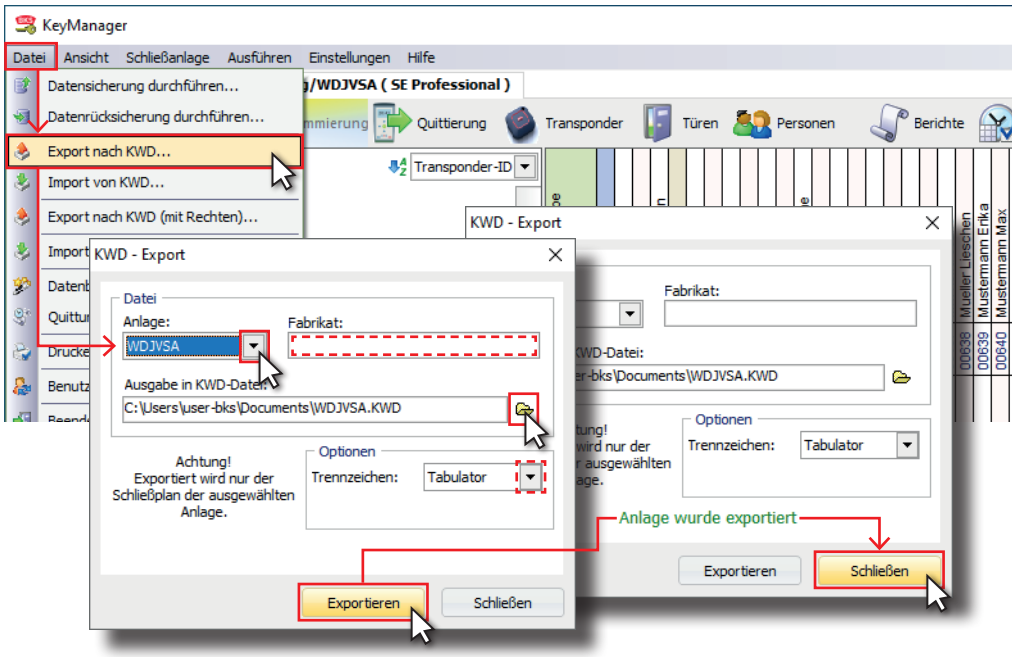
Beim Import der Daten einer Schließanlage der Version 5 des BKS KeyManagers, können versionsbedingt nicht alle Inhalte der alten Version geladen werden.

- **Bitte richten Sie die Benutzer des BKS KeyManagers, inklusive der Berechtigungen zu den Transaktionen in der Berechtigungsmatrix, in der Benutzerverwaltung neu ein.**
- **Die in der Schließanlage verwendeten Ethernet-Buskoppler (EBK, EBK Pro und EBK 2 Pro) müssen auf die Version 7 des BKS KeyManagers umgestellt werden. Verwender Sie bitte die Konfigurationsoberfläche der jeweils verwendeten EBK-Modelle und schalten diese um**
- **Mechanische Schließanlagen werden nicht importiert.**

7.3.3 Export der Komponenten einer Schließanlage in eine KWD-Datei

Diese Funktion exportiert alle Transponder und Zutrittspunkte der gewählten Schließanlage in eine KWD-Datei. Allerdings werden beim Exportieren die Daten der Berechtigungsmatrix und deren Einstellungen und Ereignisse nicht in der KWD-Datei gespeichert.

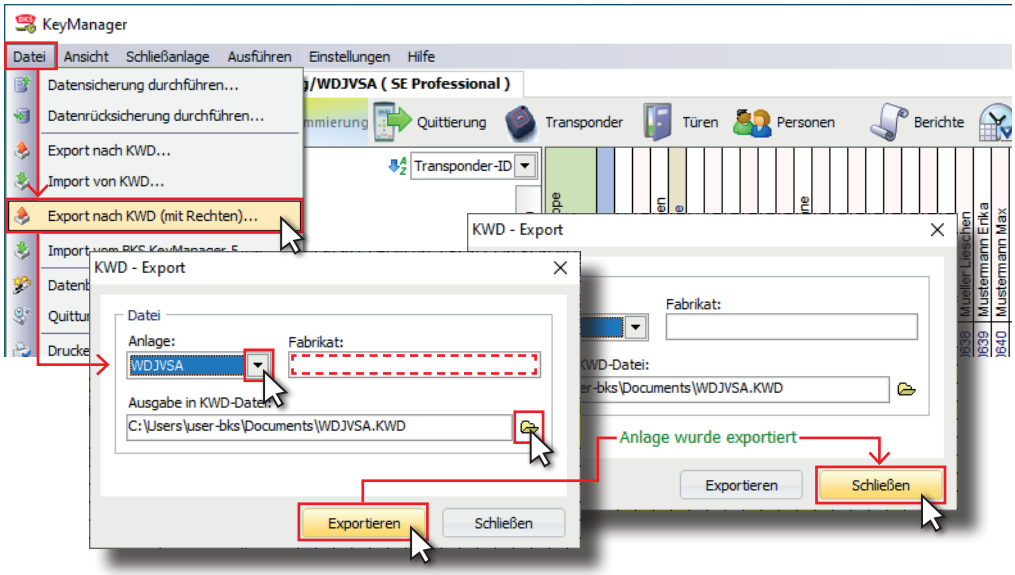
- Öffnen Sie in der Menüleiste das Dropdown-Menü „Datei“ und wählen den Menüpunkt „Export nach KWD ...“ aus.
- Wählen Sie im Dropdown-Menü die Schließanlage aus, die exportiert werden soll.
  - Geben Sie falls gewünscht einen Namen für die Schließanlage im Feld „Fabrikat“ ein.
  - Als Trennzeichen sollte der Tabulator verwendet werden. Optional besteht die Möglichkeit zur Wahl eines anderen Trennzeichens.
- Legen Sie ggf. über das Verzeichnissymbol einen neuen Speicherort fest.
- Drücken Sie auf den Button „Exportieren“ und nach dem Abschluss des Exportvorgangs auf den Button „Schließen“.



7.3.4 Export der Komponenten einer Schließanlage mit Rechten in eine KWD-Datei

Diese Funktion exportiert alle Transponder und Zutrittspunkte auch mit den Zutrittsberechtigungen der gewählten Schließanlage in eine KWD-Datei.
Dieses Exportformat kann nicht in den BKS KeyManager importiert werden.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Datei“ und wählen den Menüpunkt „Export nach KWD (mit Rechten) ...“ aus.
- Wählen Sie im Dropdown-Menü die Schließanlage aus, die exportiert werden soll.
  – Geben Sie falls gewünscht einen Namen für die Schließanlage im Feld „Fabrikat“ ein.
- Legen Sie ggf. über das Verzeichnissymbol einen neuen Speicherort fest.
- Drücken Sie auf den Button „Exportieren“ und nach dem Abschluss des Exportvorgangs auf den Button „Schließen“.

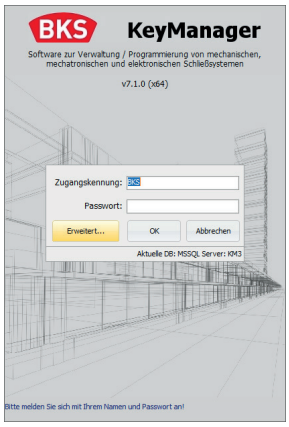


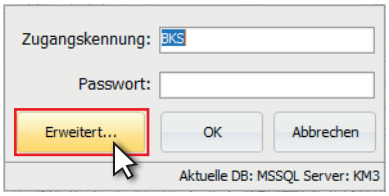
7.4 Datenbank

Die Grundlage der Datenverwaltung des BKS KeyManagers ist die Datenbank. Je nach Systemarchitektur arbeitet der BKS KeyManager mit einer Microsoft SQL Server Datenbank als interne Installation auf ihren Computer oder auf einem externen Server bzw. mit einer internen Firebird-Datenbank zusammen.

Während des Programmstarts können Sie die Einstellungen zu Ihrer Datenbank bearbeiten.

- Drücken Sie auf den Button „Erweitert“ und starten den Dialog.

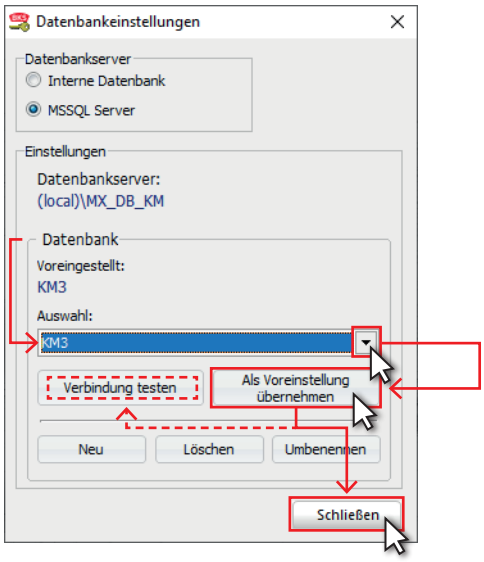




7.4.1 Auswahl | Wechseln der Datenbank

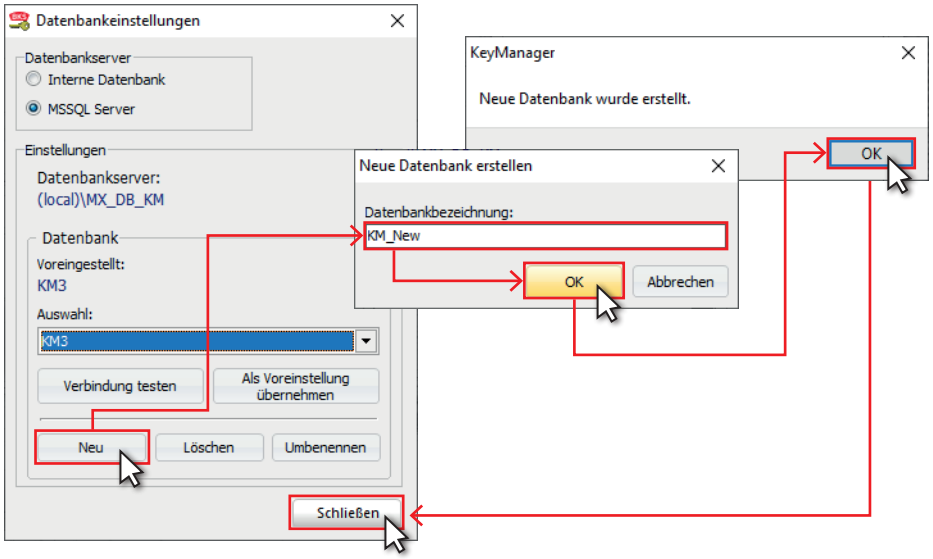
Diese Funktion ermöglicht es Ihnen, die vom BKS KeyManager verwendete Datenbank zu wechseln. Die einzelnen Datenbanken werden voneinander getrennt verwendet. Aus diesem Grund können Sie unterschiedliche Projekte isoliert und ohne Gemeinsamkeiten in einzelnen Datenbanken verwalten.

- Öffnen Sie das Dropdown-Menü und wählen in der Liste die Datenbank aus, auf welche der BKS KeyManager nach der Anmeldung zugreift.
- Drücken Sie auf den Button „Als Voreinstellung übernehmen“.
- Optional können Sie die Verbindung über den entsprechenden Button testen. Drücken Sie auf den Button „Schließen“ zum Beenden.



7.4.2 Anlage einer neuen Datenbank

- Drücken Sie auf den Button „Neu“, um eine neue leere Datenbank anzulegen.
- Geben Sie eine Datenbankbezeichnung im Eingabefeld ein. Entsprechend üblicher Namenskonventionen sind bestimmte Zeichen nicht zulässig.
- Drücken Sie auf den Button „OK“ und anschließend auf „Schließen“ zum Beenden.

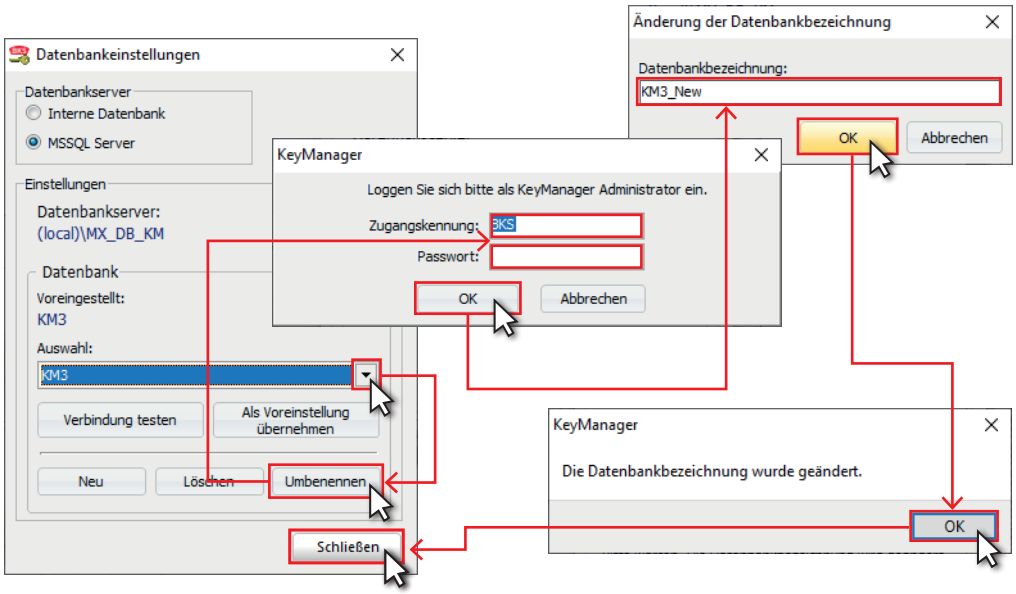


7.4.3 Umbenennen einer Datenbank

- Öffnen Sie das Dropdown-Menü und wählen in der Liste die gewünschte Datenbank aus.
- Drücken Sie auf den Button „Umbenennen“, um einen Namen zu vergeben.

Zum Umbenennen müssen Sie sich als Administrator in der Datenbank einloggen.

- Geben Sie Ihre Zugangskennung und Passwort ein und bestätigen die Eingabe mit „OK“.



- Geben Sie eine neue Datenbankbezeichnung im Eingabefeld ein. Entsprechend üblicher Namenskonventionen sind bestimmte Zeichen nicht zulässig.
- Drücken Sie auf den Button „OK“ und „Schließen“ zum Beenden.

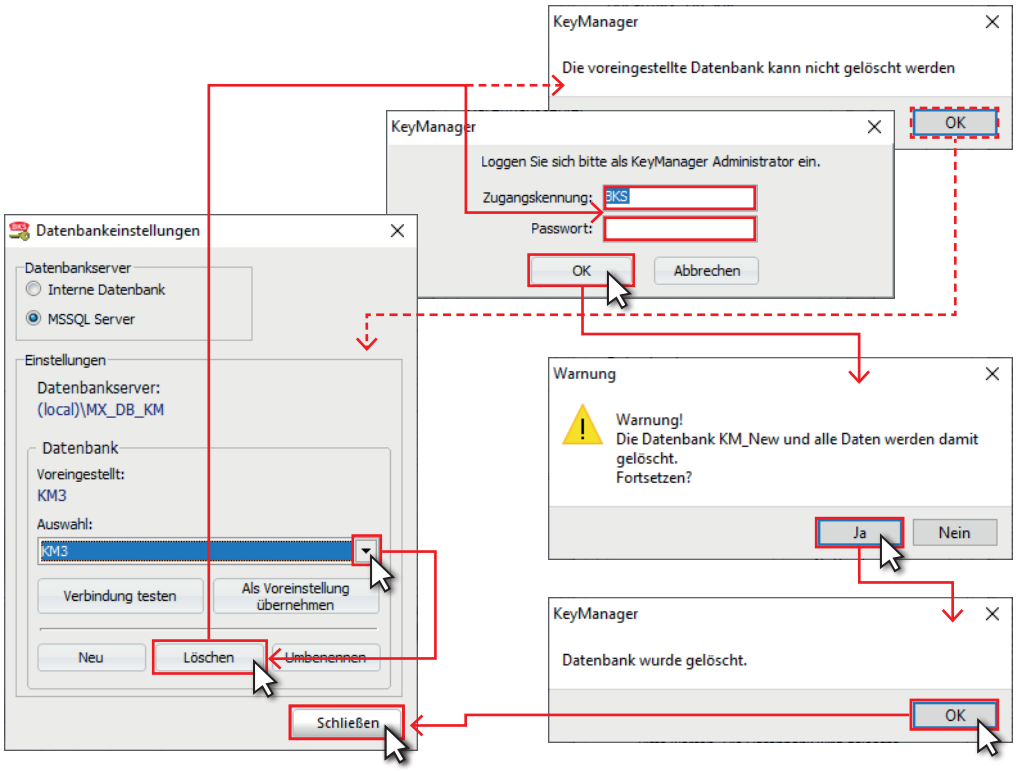
7.4.4 Löschen einer Datenbank

- Öffnen Sie das Dropdown-Menü und wählen in der Liste die gewünschte Datenbank aus.
- Drücken Sie auf den Button „Löschen“, um die Datenbank zu entfernen.

Die voreingestellte Datenbank kann nicht gelöscht werden und wird im Fenster quittiert.
- Drücken Sie auf den Button „OK“.
- Ändern Sie die voreingestellte Datenbank durch Auswahl einer anderen Datenbank im Dropdown-Menü.
- Drücken auf den Button „Als Voreinstellung übernehmen“, siehe auch Kapitel 7.4.1 [373].
- Beginnen Sie mit dem Ablauf zum Löschen von vorne.

Zum Löschen müssen Sie sich als Administrator in der Datenbank einloggen.

- Geben Sie Ihre Zugangskennung und Passwort ein und bestätigen die Eingabe mit „OK“.
- Drücken Sie auf den Button „Ja“ zum Löschen und „OK“ zum Beenden.



7.4.5 Wechsel von interner Datenbank auf Microsoft SQL-Datenbank

Sie haben nachträglich die Möglichkeit, von einer Installation des BKS KeyManagers mit interner Datenbank auf eine Microsoft SQL Server Installation zu wechseln.

HINWEIS **Ein umgekehrter Wechsel der Datenbank von Microsoft SQL-Datenbank zu der internen Datenbank des BKS KeyManagers ist nicht möglich.**

Die Wechsel der Datenbank erfolgt in 4 Schritten.

Schritt 1: Sicherung der internen Datenbank
Vor der Installation ist eine Datensicherung der internen Datenbank durchzuführen.

Folgen Sie der Anleitung im Kapitel 7.2.1 [362] bzw. in Kurzform den folgenden Schritten.

- Wählen Sie über das Dropdown-Menü „Datei“ den Menüpunkt „Datensicherung durchführen ...“ aus. Drücken Sie auf den Button „Sicherungskopie erstellen ...“.
- Navigieren Sie im Dateibrowser zum gewünschten Speicherort und geben den Dateinamen für die Datensicherung der Datenbank in eine „*.bak-Datei“ im Feld Dateiname ein.
- Zum Starten der Datenrücksicherung drücken Sie auf „Speichern“.
- Drücken Sie auf den Button „Speichern“ und „Schließen“ und Beenden den Dialog.

Schritt 2: Installation des Microsoft SQL Servers
Vor der Installation des Microsoft SQL Servers muss der BKS KeyManager geschlossen werden.

- Wählen Sie über das Dropdown-Menü „Datei“ den Menüpunkt „Beenden“ aus.

Die Installation des Microsoft SQL Servers mithilfe des USB-Sticks oder einer Download-Datei sind in den folgenden Kapiteln beschrieben. Folgen Sie den dort beschriebenen Anweisungen und Vorgaben.

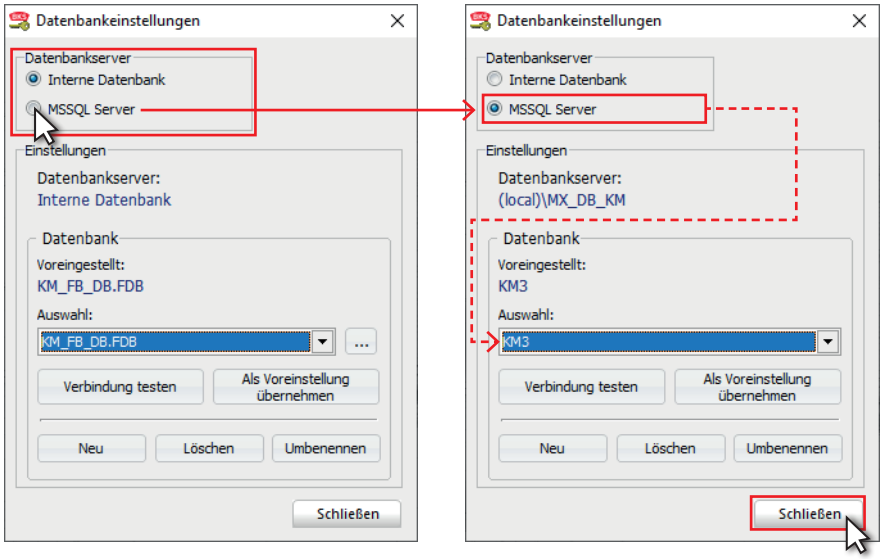
- Beachten Sie die Voraussetzung zur Installation im Kapitel 2 [17].
- Starten Sie die Installation wie im Kapitel 2.2 [18] beschrieben.
- Folgen Sie dem Dialog der Installation im Kapitel 2.2.1 [19].
- Optionale Konfiguration der Servereinstellungen im Kapitel 2.2.2 [24].

Schritt 3: Einstellung des Datenbankservers

- Starten Sie den BKS KeyManager neu und warten, bis das Login-Fenster angezeigt wird.
- Drücken Sie auf den Button „Erweitert“, um zu den Datenbankeinstellungen zu gelangen.
- Wählen Sie die Checkbox „MSSQL Server“ für die Verwendung des Microsoft SQL Servers aus und übernehmen diesen als Voreinstellung.

Die neue Datenbank „KM3“ wird erstellt und als voreingestellte Datenbank gesetzt.

- Drücken Sie auf den Button „Schließen“ zum Beenden und kehren zum Login-Fenster zurück.



Schritt 4: Datenrücksicherung der gespeicherten Datenbank aus der internen Datenbank

- Melden Sie sich im Login-Fenster mit der Zugangskennung: „BKS“ und dem Kennwort „Admin“ an.

Beim Programmstart werden Sie aufgefordert, die Datenbank zu aktualisieren. Folgen Sie dem Dialog und drücken auf den Button „OK“ und melden sich erneut an.
Nach dem Programmstart wird Ihnen das Fenster „Assistenten“ angezeigt.

- Drücken auf den Button „Schließen“.

Folgen Sie der Anleitung von Kapitel 3.4.2 [73] bzw. in Kurzform den folgenden Schritten.

- Wählen Sie über das Dropdown-Menü „Datei“ den Menüpunkt „Datenrücksicherung durchführen ...“ aus. Drücken Sie auf den Button „Wiederherstellen ...“.

Um die Datensicherung von Schritt 1 in die Microsoft SQL Serverversion einzuspielen, wählen Sie die von Ihnen gespeicherte „*.bak-Datei“ im Datei-Browser aus.

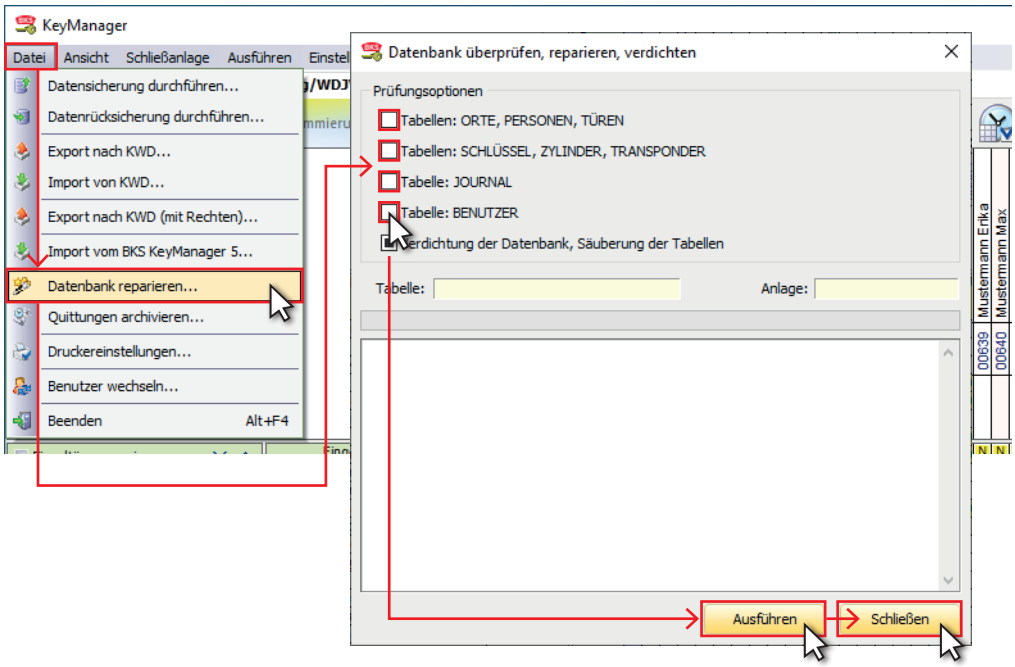
- Zum Starten der Datenrücksicherung drücken Sie auf „Öffnen“ und im Weiteren auf „OK“.
- Melden Sie sich in der Datenbank mit Ihrer „Zugangskennung“ und „Kennwort“ an und drücken zum Beenden der Datenrücksicherung auf den Button „Schließen“.

Die Übernahme der Daten aus der Internen in die Microsoft SQL Datenbank ist abgeschlossen.

7.4.6 Wartung der Datenbank

Bei der Verwendung des BKS KeyManagers kann es im alltäglichen Gebrauch zu leichten, aber auch zu spürbaren Performance-Verlusten kommen. Speziell bei größeren Datenbanken kann dies auftreten. Durch eine Verdichtung der Datenbank, die Entfernung der sogenannten Kartei-Leichen und die Erstellung eines neuen Index können Sie Ihre Datenbank reparieren und diesem Phänomen vorbeugen. Wir empfehlen aus diesem Grund eine Wartung in einem jährlichen Intervall mit dieser Funktion durchzuführen.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Datei“ und wählen den Menüpunkt „Datenbank reparieren ...“ aus.
- Aktivieren Sie die Checkboxen der Prüfoptionen, für die Sie eine Überprüfung wünschen und in welchen Tabellen überprüft werden sollen.
- Drücken Sie auf den Button „Ausführen“, um die Wartung zu starten und nach Beendigung des Vorgangs auf „Schließen“.



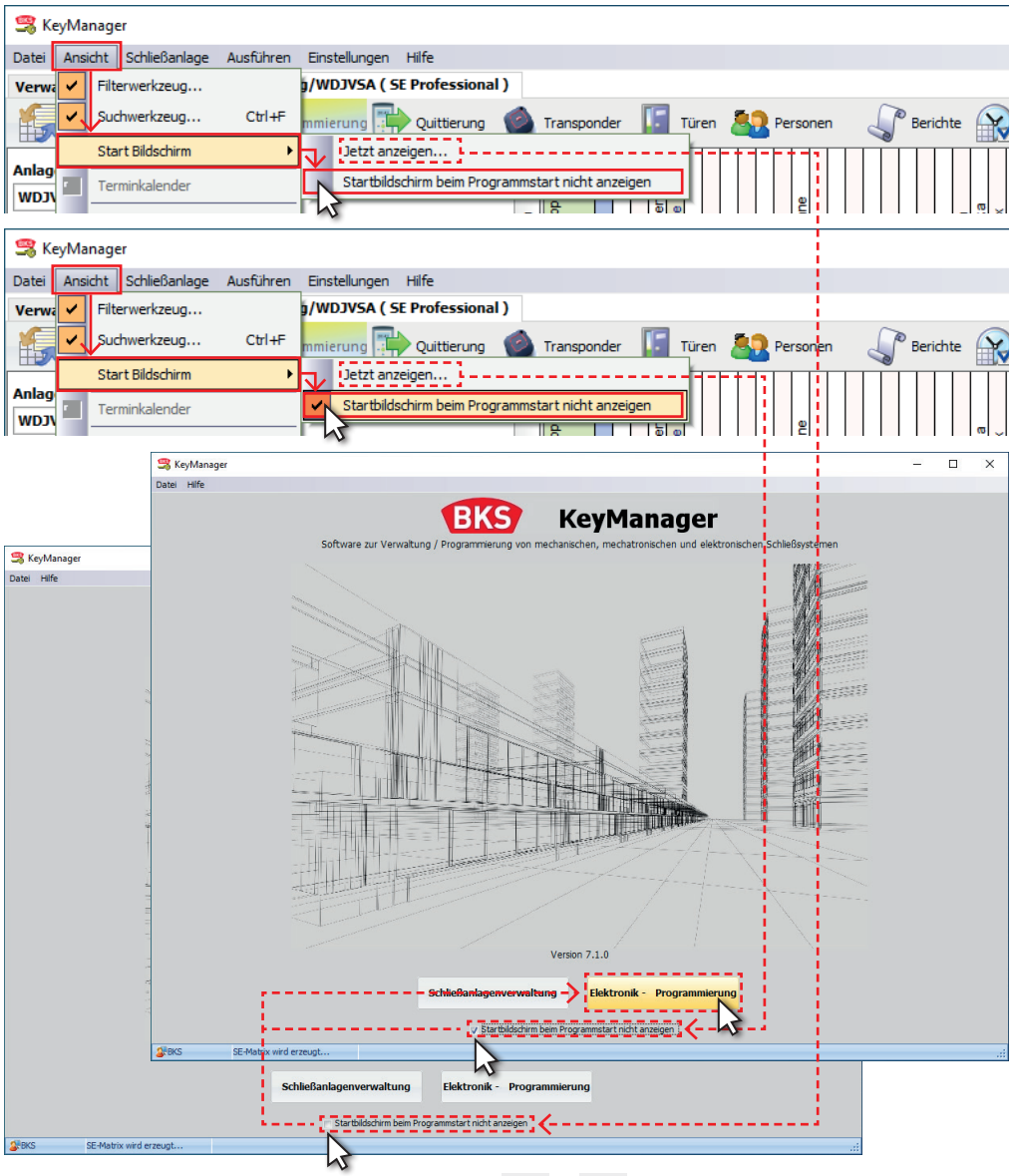
7.5 Startbildschirm aktivieren/deaktivieren

Während des Programmstarts wird nach Anmeldung in der Datenbank der Startbildschirm angezeigt. Wenn dieses Fenster beim Start übersprungen werden soll, können Sie die Anzeige deaktivieren.

- Zur Deaktivierung des Startbildschirms öffnen Sie in der Menüleiste das Menü „Ansicht“ und wählen im Dropdown-Menü „Startbildschirm“ den Menüpunkt „Startbildschirm beim Programmstart nicht anzeigen“ aus. Der Startbildschirm wird dadurch nicht mehr während des Starts angezeigt.

Alternativ kann über den Menüpunkt „Jetzt anzeigen“ die Anzeige des Startbildschirms, über das setzen des Hakens in der Checkbox „Startbildschirm beim Programmstart nicht anzeigen“ deaktiviert und durch das Entfernen des Hakens wieder aktiviert werden. Während des Programmstarts kann die Anzeige des Startbildschirms auch direkt deaktiviert werden.

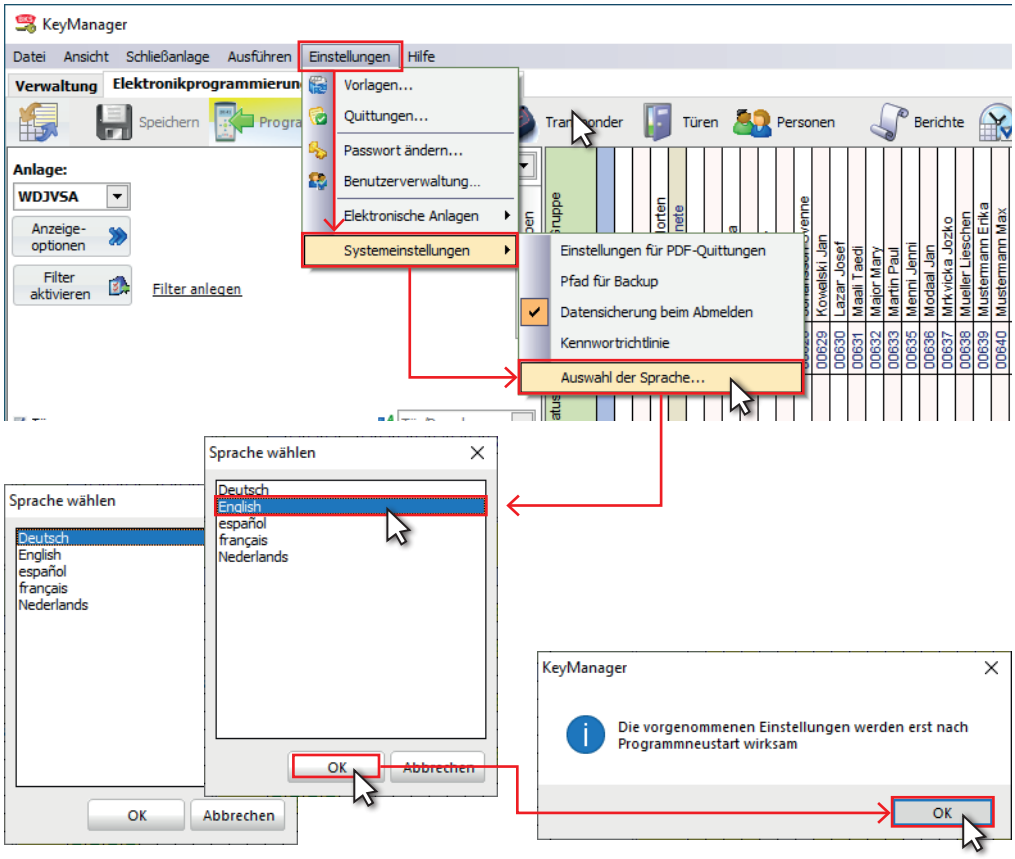
- Um beim Programmstart den Startbildschirm wieder anzeigen zu lassen, wählen Sie über das Dropdown-Menü „Startbildschirm“ den Menüpunkt „Startbildschirm beim Programmstart nicht anzeigen“ aus und entfernen dadurch den Haken. Dadurch ist die Funktion wieder aktiv.



7.6 Sprache der Benutzeroberfläche wechseln

Die Sprache der Benutzeroberfläche kann wie folgt geändert werden.

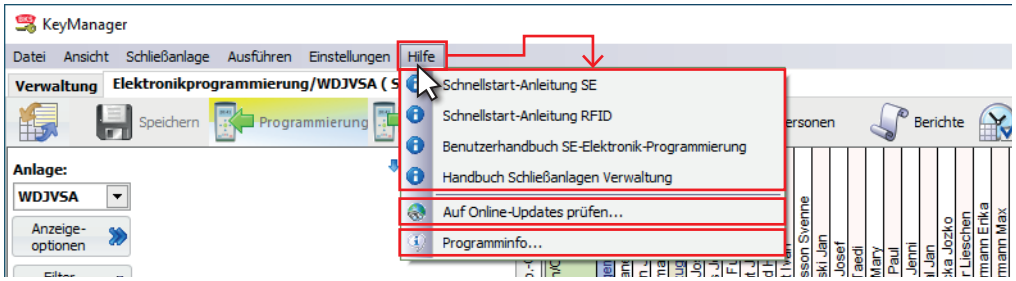
- Öffnen Sie in der Menüleiste das Menü „Einstellungen“ und wählen im Dropdown-Menü „Systemeinstellungen“ den Menüpunkt „Auswahl der Sprache ...“ aus.
- Wählen Sie im Fenster „Sprache wählen“ die gewünschte Sprache aus. Zur Bestätigung drücken Sie in diesem und dem folgendem Fenster auf „OK“.
- Beenden Sie den BKS KeyManager und starten die App neu. Erst nach dem Neustart wird der BKS KeyManager in die gewünschte Sprache umgestellt.



7.7 Hilfe-Menü

Im Menü Hilfe finden Sie die Benutzerhandbücher und Schnellstart-Anleitungen zum BKS KeyManager und können diese über das Dropdown-Menü einsehen. Über den Menüpunkt „Auf Online-Updates prüfen ...“ können Sie nach Updates für den BKS KeyManager suchen. Näheres finden Sie auch im Kapitel Installation oder Kapitel 7.7.2 [382].
Der Menüpunkt „Programminfo ...“ liefert Ihnen die aktuellen Informationen zu der von Ihnen verwendeten Version des BKS KeyManagers.

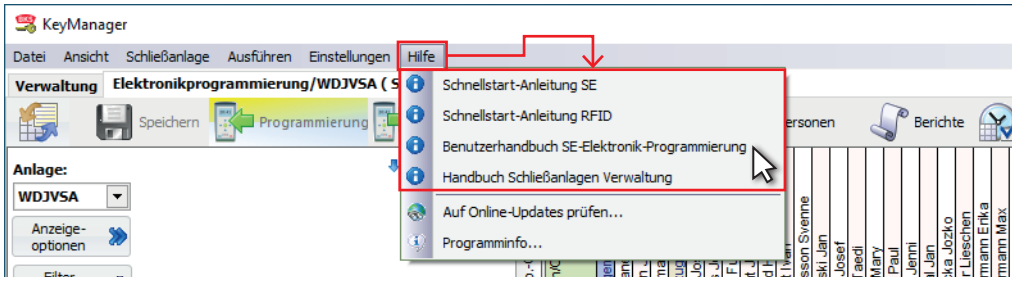
- Öffnen Sie in der Menüleiste das Menü „Hilfe“ und wählen im Dropdown-Menü den gewünschten Menüpunkt zu den Themen Anleitung, Update oder Info aus.



7.7.1 Anleitungen zum BKS KeyManager

Das Benutzerhandbuch und die Schnellstart-Anleitung zum BKS KeyManager können Sie über das Hilfe-Menü öffnen.

- Öffnen Sie in der Menüleiste das Menü „Hilfe“ und wählen im Dropdown-Menü den Menüpunkt zur gewünschten Anleitung aus. Die Anleitung wird Ihnen im PDF-Format angezeigt.



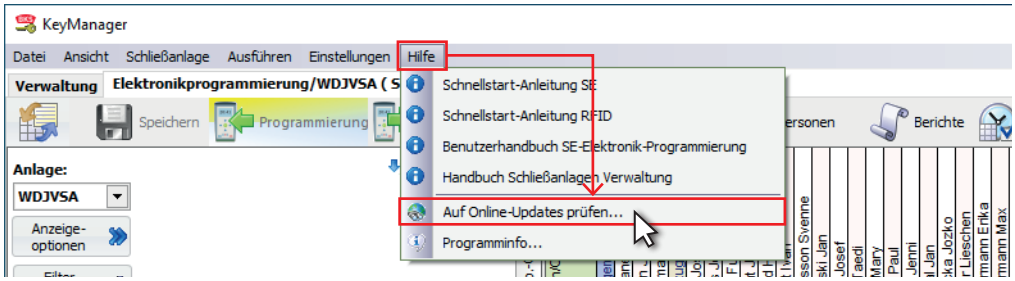
7.7.2 Update

Über die Update-Funktion können Sie eine direkte Aktualisierung der installierten Version des BKS KeyManager ausführen. Zum Updaten muss an Ihrem Computer eine Verbindung zum Internet zur Verfügung stehen. Nach dem Start der Funktion findet ein Versionsvergleich statt und bei Gleichheit wird der Vorgang beendet.

HINWEIS **Vor jedem Update ist zur Vorbeugung von Datenverlusten und zur Steigerung der Datensicherheit eine Datensicherung zu erstellen, siehe Kapitel 7.2.1 [362].**

Wurde bei der Installation die Option „Automatische Suche nach Updates“ aktiviert, sucht der BKS KeyManager beim Start automatisch nach vorhandenen Updates. Der folgende Dialog wird beim Programmstart angezeigt, wenn ein neues Update verfügbar ist.

- Öffnen Sie in der Menüleiste das Menü „Hilfe“ und wählen im Dropdown-Menü den Menüpunkt „Auf Online-Updates prüfen“ aus.

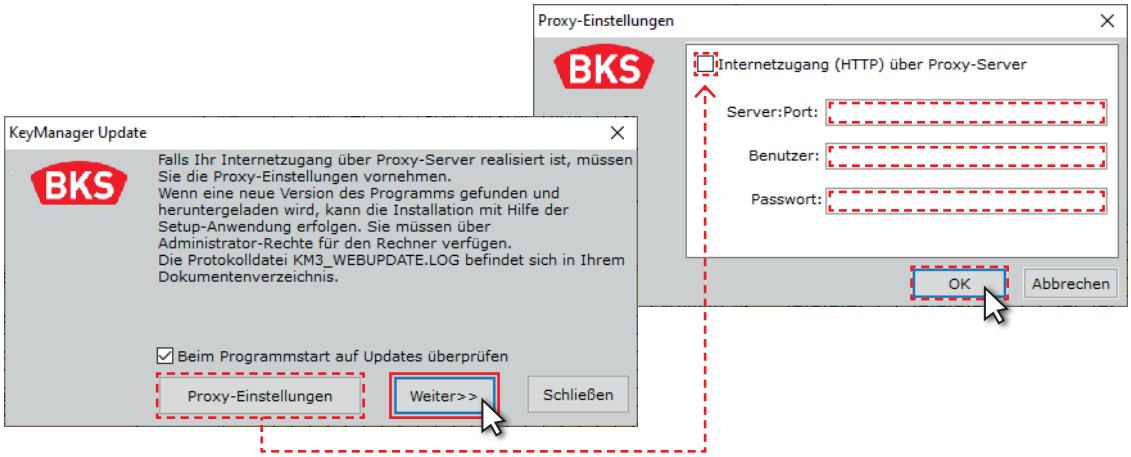


Optional können Sie vor dem Start des Updates, falls Ihr Computer über einen Proxy-Server mit dem Internet verbunden soll, den Dialog zur Anmeldung an Ihren Proxy-Server starten.

- Drücken Sie auf den Button „Proxy-Einstellungen“.
- Aktivieren Sie die Checkbox „Internetzugang (HTTP) über Proxy-Server.
- Füllen Sie die Felder zur Anmeldung am Proxy-Server aus.

Die Anmeldeinformationen werden abgespeichert und bei kommenden Updates zur Anmeldung verwendet. Sollten Ihnen diese Informationen nicht zur Verfügung stehen, wenden Sie sich an Ihren Netzwerk-Administrator.

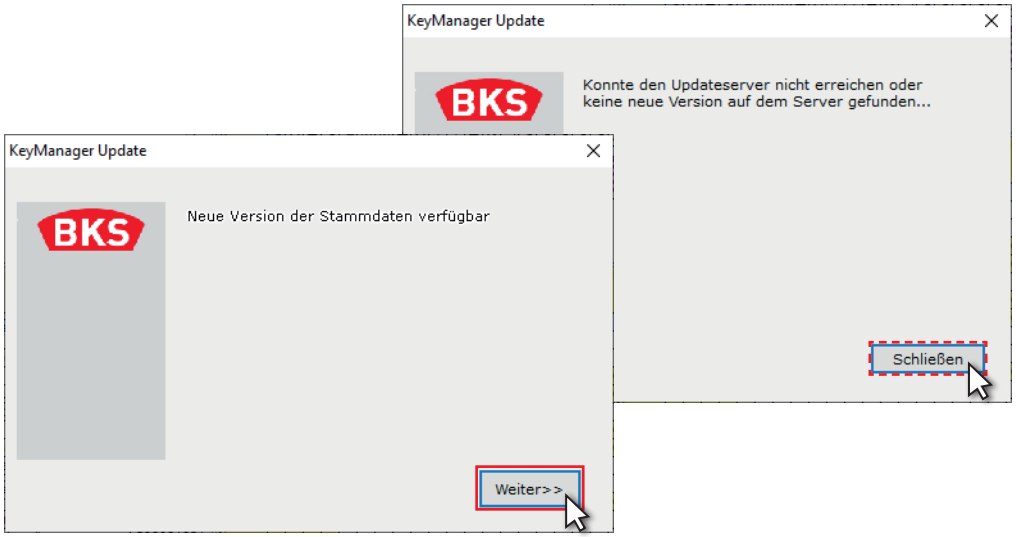
- Drücken Sie auf den Button „Weiter“, um die Installation zu starten.



■ Drücken Sie auf den Button „Weiter“, um mit dem Update fortzufahren.

Sollte sich beim Versionsvergleich herausstellen, dass die auf Ihren Computer installierte Version des BKS KeyManagers auf dem neuesten Stand befindet, werden Sie zum Beenden des Updates aufgefordert.

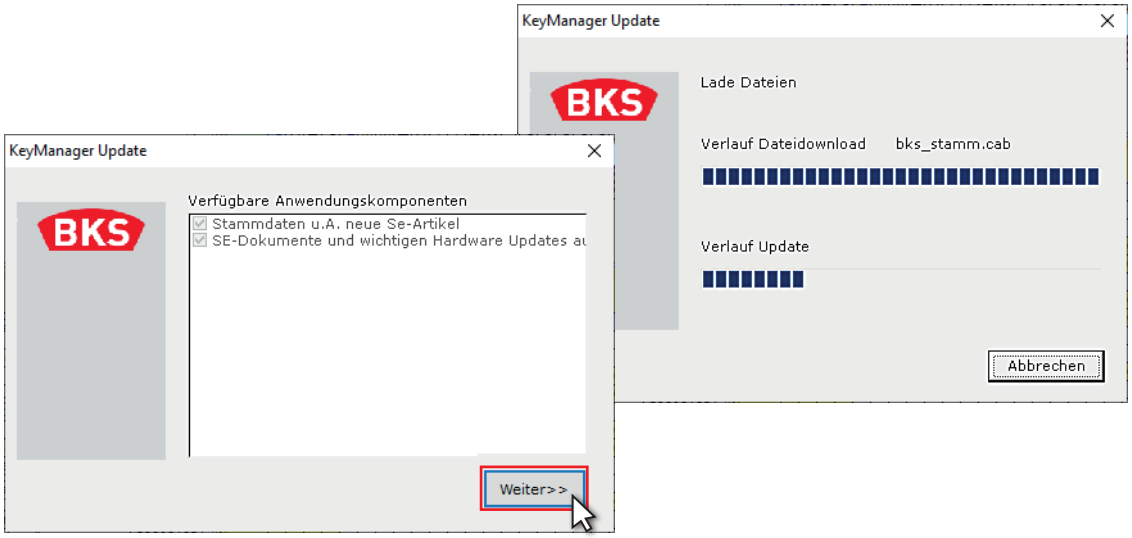
■ Drücken Sie auf den Button „Schließen“ und Beenden den Dialog.



Im nächsten Fenster können Sie optional in den Checkboxen durch Aktivierung oder Deaktivierung dieser die verfügbaren Komponenten, die installiert werden sollen, auswählen bzw. abwählen.

■ Drücken Sie auf den Button „Weiter“ und starten den Downloadvorgang.

Unterbrechen Sie den Downloadvorgang nicht und warten, bis der Vorgang beendet ist.



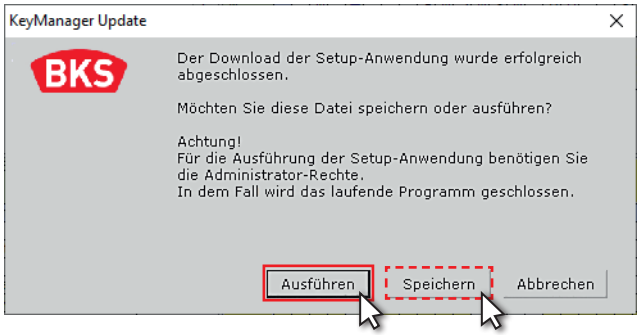
Nach erfolgreichem Abschluss des Downloadvorganges haben Sie die Option, ob die Installation sofort ausgeführt werden soll oder eine Installationsdatei gespeichert wird.

Beachten Sie, dass bei der Installation des BKS KeyManagers der Benutzer des Computers über die notwendigen Administratorenrechte verfügen müssen. Die Software BKS KeyManager wird zur Installation automatisch geschlossen und die Installation gestartet. Folgen Sie im weiteren Dialog der Installation dem Installationsassistenten.

- Drücken Sie auf den Button „Ausführen“ und starten die Installation des Updates.

Alternativ können Sie die Installationsdatei für einen späteren Zeitpunkt abspeichern, z. B. falls Sie nicht über die zur Installation benötigten Administrationsrechte für den Computer verfügen. Mit der gespeicherten Datei kann die Installation von einem Administrator durchgeführt werden.

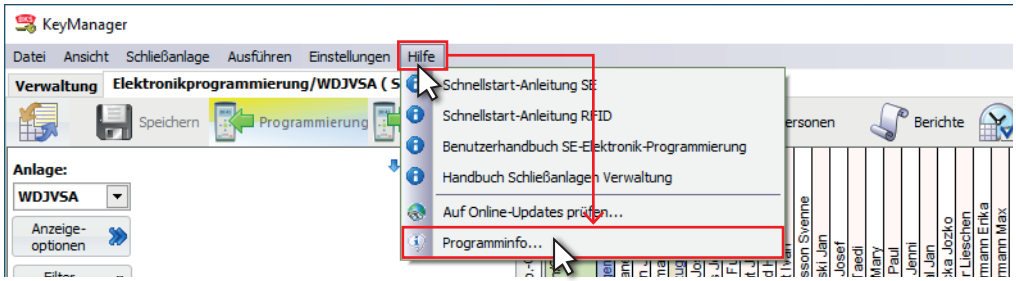
- Drücken Sie auf den Button „Speichern“, um die Installation zu einem späteren Zeitpunkt auszuführen.



7.7.3 Programminfo

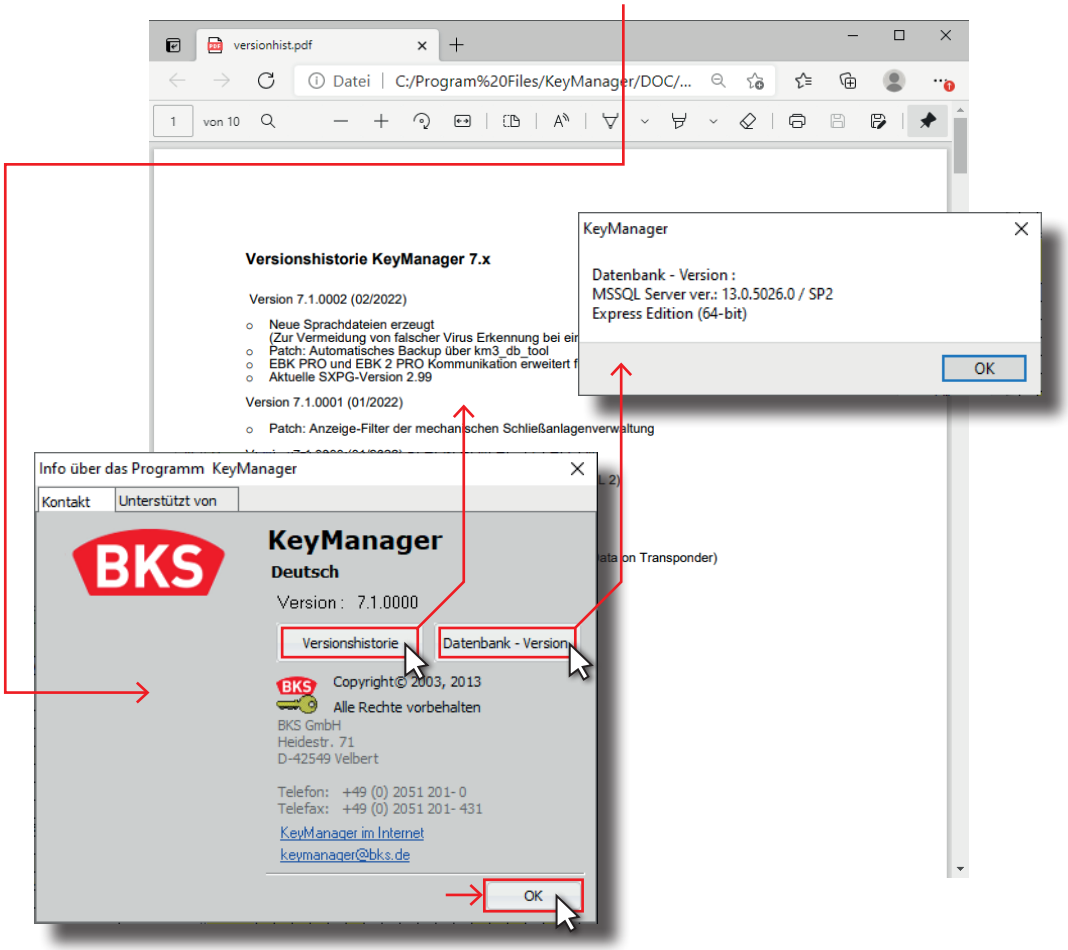
Die Funktion „Programminfo ...“ zeigt Ihnen ein Fenster mit den aktuellen Versionshinweisen zu der aktuell verwendeten Version des BKS KeyManagers an.

- Öffnen Sie in der Menüleiste das Menü „Hilfe“ und wählen im Dropdown-Menü den Menüpunkt „Programminfo ...“ aus.



Im folgenden Informationsfenster die Versionsnummer des BKS KeyManagers und eine Übersicht der Kontaktdaten angezeigt.

- Drücken Sie auf den Button „Versionshistorie“, um Informationen zur Software und eine Änderungshistorie in einem PDF-Dokument angezeigt zu bekommen.
- Drücken Sie auf den Button „Datenbank-Version“ zum Öffnen des Informationsfensters und auf „OK“, um dieses zu schließen.

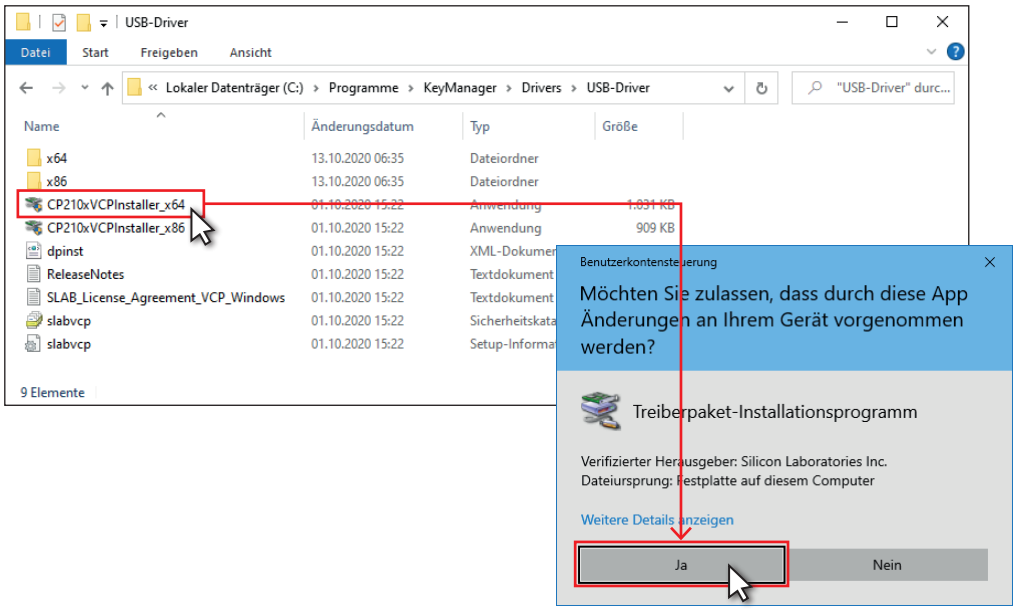


7.8 Installation Programmiergerät

Nach der Installation kann das Programmiergerät durch ein USB-Kabel mit dem Computer verbunden werden. Der USB-Treiber des Programmiergerätes wird dabei automatisch installiert. Sollte das Programmiergerät nicht im BKS KeyManager zur Verfügung stehen, können Sie den USB-Treiber manuell installieren.

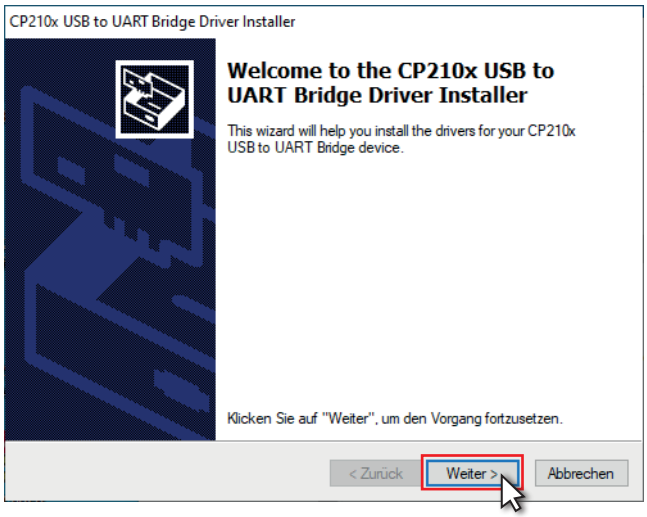
Navigieren Sie auf Ihrer Festplatte zum Installationsverzeichnis des BKS KeyManagers z. B. „C:\ ... \KeyManager“.

- Öffnen Sie im Verzeichnis „Drivers“ den Ordner „USB-Drivers“.
- Führen Sie die Datei „CP210xVCPInstaller_x64.exe“ bei Verwendung eines 64 Bit Systems aus.
- Bestätigen Sie die Warnmeldung mit „Ja“.



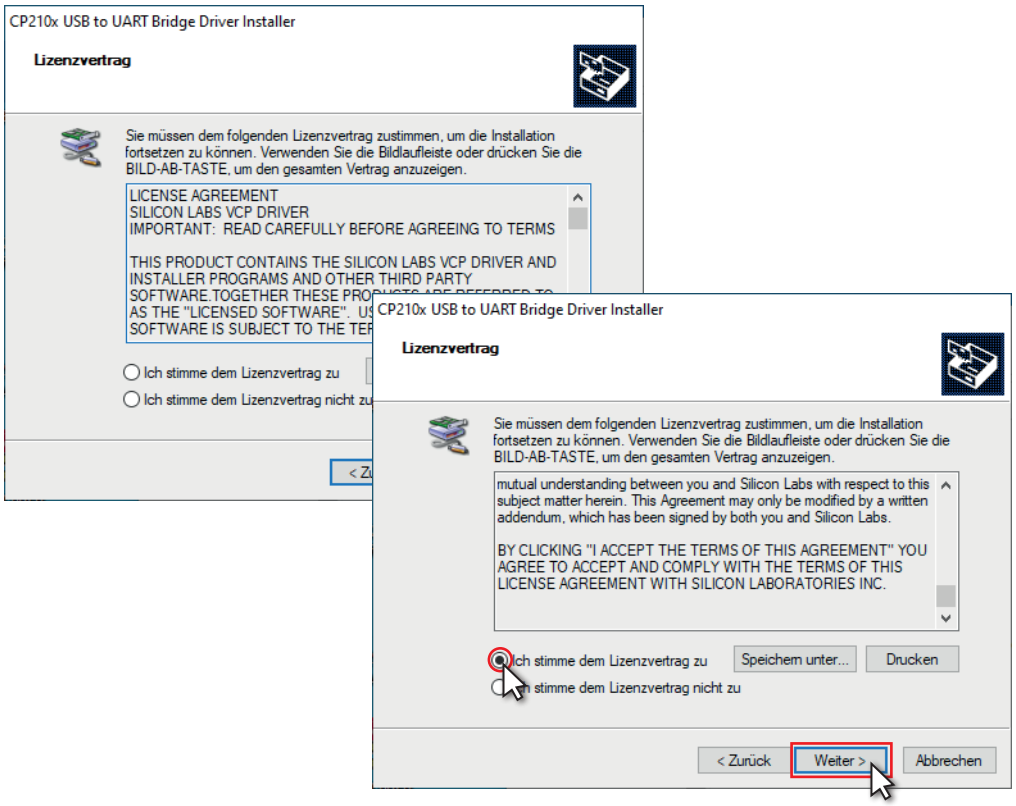
Es öffnet sich der Installationsassistent für den USB-Treiber des SE-Programmiergerätes.

Drücken Sie auf den Button „Weiter >“.

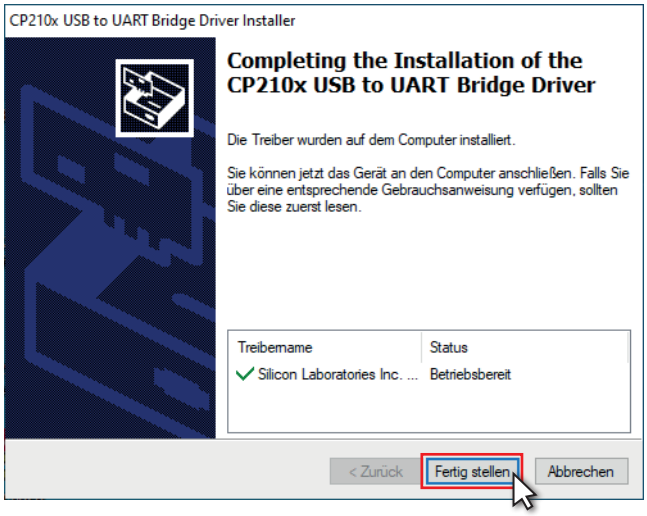


Lesen Sie sich den Lizenzvertrag sorgfältig durch.

- Akzeptieren Sie die gelesenen Bedingungen und Lizenzvereinbarung und drücken auf den Button „Weiter >“.



- Zur Beendigung der Installation drücken Sie den Button „Fertigstellen“.



8. Data on Transponder-Schließanlage (DoT)

Die Data on Transponder-Schließanlagen (DoT) zeichnen sich in erster Linie dadurch aus, dass der Speicherort der Zutrittsberechtigungen auf den Transpondern liegt und in den Türen/Zutrittspunkte die Berechtigung nur eine initiale Programmierung erforderlich ist. Die auf dem Transponder programmierte Zutrittsberechtigung ermöglicht dem Träger des Transponders nach dem Buchen am Zutrittspunkt den freien Zugang. Liegt keine Berechtigung im Transponder vor oder ist der Transponder im Zutrittspunkt gesperrt, wird der Zugang verwehrt.

Der Schließanlagentyp DoT bietet dadurch einen Mix der Vorteile von Online- und Offline-Anlagen. Die Verwaltung der Schließanlage kann von einer zentralen Stelle mit überschaubaren Wegen für die Programmierung ausgeübt werden. Durch eine Installation, die nahezu ohne Verkabelung der Komponenten auskommt, wird der Aufwand gegenüber einer direkten Anbindung reduziert.

Eine DoT-Anlage kann auch ohne Freigabeterminal Professional (FGT) betrieben werden. In diesem Fall werden die Transponder über das Programmiergerät programmiert. Es wird jedoch empfohlen, eine DoT-Anlage mit FGT zu betreiben.

Wird in der DoT-Anlage das FGT mit dem Rechtesystem der relativen Gültigkeit der Transponder als zentrales Element eingesetzt, ermöglicht dies eine indirekte Vernetzung der Zutrittspunkte mit dem BKS KeyManager über eine regelmäßige Datenübertragung. Gegenüber Onlinesystemen mit direkter Vernetzung durch Verkabelung und Funkverbindung werden die Daten z. B. Änderungen der Berechtigungen automatisch an das FGT übertragen und der Transponder wird zum Bindeglied beim Zusammenspiel der Komponenten der Schließanlage.

Damit eine regelmäßige Datenübertragung ohne eine direkte Vernetzung gewährleistet ist, verlieren die Transponder nach Ablauf der Gültigkeit ihre Berechtigungen, wodurch sie gezwungen sind, kontinuierlich über das Aufsuchen eines FGT die Gültigkeit zu verlängern. Mit jeder Gültigkeitsverlängerung am FGT werden die aktuellen Programmierdaten an die Transponder übertragen. Während der Begehung der Schließanlage werden die Einzelrechte und/oder die Transpondergruppenzuordnung der Transponder über das FGT aktualisiert und die Daten aus den Türen werden beim Buchen zurück zur Quittierung übertragen.

Technische Voraussetzung für den Einsatz eines FGT (FGT Pro / FGT 2 Pro) ist die Installation der Ethernetbuskoppler Professional (EBK Pro / EBK 2 Pro). Das EBK wandelt die Signale des FGT vom RS485-Bus auf Ethernet/LAN zum BKS KeyManager um.

Bitte beachten Sie, dass an jedem EBK nur **ein** FGT angeschlossen werden kann.
Alternativ hierzu ist es möglich, an jedem EBK **acht** reine Wandleser anzuschließen.
An das EBK 2 Pro kann ebenfalls nur **ein** FGT 2 Pro mit aktivierter Funktion Wandleser angeschlossen werden, weil es kein reiner Wandleser ist.

8.1 Data on Transponder-Schließanlage (DoT) mit Freigabeterminal (FGT) und Offline-Zutrittspunkte

8.1.1 Systemübersicht DoT-Anlage mit FGT und Offline-Zutrittspunkte

Beim Offline-Betrieb einer Data on Transponder-Anlage und in Verbindung mit der Verwendung von Freigabeterminals werden folgende Elemente benötigt.

Schließanlage mit SE-Technologie

- Transponder (Data on Transponder kompatibel)
- Türen|Zutrittspunkte wie z. B. Zylinder, Schlösser, Beschläge, Wandleser, Relaismodule etc.
- Ethernetbuskoppler Professional (EBK Pro)
  – Varianten EBK Pro / EBK 2 Pro
- Freigabeterminal Professional (FGT Pro)
  – Varianten: FGT Pro / FGT 2 Pro zum Anschuss am EBK Pro / EBK 2 Pro
- Programmiergerät (SXPG)
- Vernetzung des KeyManagers
  – Anschluss EBK über LAN
  – Anbindung FGT über den RS485-Bus an das EBK

BKS KeyManager

- SE-Lizenz Free, Standard oder Professional
- SE-Lizenz Data on Transponder

8.1.2 Installationsarten DoT-Anlage mit FGT und Offline-Zutrittspunkte

Empfohlene Installation des BKS KeyManagers

- Einzelplatz- und Serverversion mit Microsoft SQL Server
  – Für einen einzelnen Arbeitsplatz (Single User)
  – Folgen Sie der Anleitung im Kapitel 2.2 [18]
- Ethernetbuskoppler Professional-Dienst (EBK Pro-Dienst)
  – Bei Verwendung von Ethernetbuskopplern erforderlich
  – Folgen Sie der Anleitung im Kapitel 2.8 [57]

Alternative Installationsvarianten

- Clients der Netzwerkversion
  – Zur Einrichtung weiterer Arbeitsplätze mit dem Datenbankserver „Einzelplatz- und Serverversion mit Microsoft SQL Server“, um von weiteren Arbeitsplätzen das Arbeiten zu ermöglichen
  – Folgen Sie der Anleitung im Kapitel 2.3 [32]
- Server der Netzwerkversion
  – Als Datenbankserver ohne Arbeitsplatz für die Clients der Netzwerkversion
  – Folgen Sie der Anleitung im Kapitel 2.5 [47]
  – Ethernetbuskoppler Professional-Dienst (EBK Pro-Dienst), siehe Kapitel 2.8 [57]

8.2 Data on Transponder-Schließanlage (DoT) mit Freigabeterminal (FGT) und Online-Zutrittspunkte

8.2.1 Systemübersicht DoT-Anlage mit FGT und Online-Zutrittspunkte

Beim Online-Betrieb einer Data on Transponder-Anlage und in Verbindung mit der Verwendung von Freigabeterminals werden folgende Elemente benötigt.

SE-Schließanlage mit SE-Technologie

- Transponder (Data on Transponder kompatibel)
- Online-Türen|Zutrittspunkte wie z. B. Funk-Zylinder, Funk-Schlösser, Funk-Beschläge, Funkwandmodul (SE FM) etc.
- Ethernetbuskoppler-Funkmodul (EBK FM) oder dem Online Wandleser B 5368
- Ethernetbuskoppler (EBK) für Funkwandmodul (SE FM)
- Vernetzung des KeyManagers über LAN zum EBK FM und EBK; Anschluss SE FM am EBK über Bus; Verbindung von EBK FM und SE FM zu den Zutrittspunkten über Funk
- Offline-Türen|Zutrittspunkte wie z. B. Zylinder, Schlösser, Beschläge, Wandleser, Relaismodule etc.
- Ethernetbuskoppler Professional (EBK Pro)
  – Varianten EBK Pro / EBK 2 Pro
- Freigabeterminal Professional (FGT Pro)
  – Varianten: FGT Pro / FGT 2 Pro zum Anschuss am EBK Pro / EBK 2 Pro
- Programmiergerät (SXPG)
- Vernetzung des KeyManagers
  – Anschluss EBK über LAN und EBK Pro (2)
  – Anbindung SE FM über den RS485-Bus an das EBK
  – Verbindung EBK FM / SE FM zu den Zutrittspunkten über Funk

BKS KeyManager

- SE-Lizenz Free, Standard oder Professional
- SE-Lizenz Data on Transponder
- SE-Lizenz Online

8.2.2 Installationsarten DoT-Anlage mit FGT und Online-Zutrittspunkte

Empfohlene Installation des BKS KeyManagers

- Einzelplatz- und Serverversion mit Microsoft SQL Server
  - Für einen einzelnen Arbeitsplatz (Single User)
  - Aktivieren Sie „SE-Online-Modul installieren“.
  - Folgen Sie der Anleitung im Kapitel 2.2 [18]
- Ethernetbuskoppler Professional-Dienst (EBK Pro-Dienst)
  - Bei Verwendung von Ethernetbuskopplern erforderlich
  - Folgen Sie der Anleitung im Kapitel 2.8 [57]

Alternative Installationsvarianten

- Clients der Netzwerkversion
  - Zur Einrichtung weiterer Arbeitsplätze mit dem Datenbankserver „Einzelplatz- und Serverversion mit Microsoft SQL Server“, um von weiteren Arbeitsplätzen das Arbeiten zu ermöglichen
  - Folgen Sie der Anleitung im Kapitel 2.3 [32]
- Server der Netzwerkversion
  - Als Datenbankserver ohne Arbeitsplatz für die Clients der Netzwerkversion
  - Aktivieren Sie „SE-Online-Modul installieren“.
  - Folgen Sie der Anleitung im Kapitel 2.5 [47]
  - Ethernetbuskoppler Professional-Dienst (EBK Pro-Dienst), siehe Kapitel 2.8 [57]

8.3 Data on Transponder-Schließanlage (DoT) ohne Freigabeterminal (FGT) und Offline-Zutrittspunkte

8.3.1 Systemübersicht DoT-Anlage ohne FGT und Offline-Zutrittspunkte

Beim Offline-Betrieb einer Data on Transponder-Anlage werden folgende Elemente benötigt.

SE-Schließanlage mit SE-Technologie

- Transponder (Data on Transponder kompatibel)
- Türen|Zutrittspunkte wie z. B. Zylinder, Schlösser, Beschläge, Wandleser etc.
- Programmiergerät (SXPG)

BKS KeyManager

- SE-Lizenz Free, Standard oder Professional
- SE-Lizenz Data on Transponder

8.3.2 Installationsarten DoT-Anlage ohne FGT und Offline-Zutrittspunkte

Empfohlene Installation des BKS KeyManagers

- Einzelplatz- und Serverversion mit Microsoft SQL Server
  - Für einen einzelnen Arbeitsplatz (Single User)
  - Folgen Sie der Anleitung im Kapitel 2.2 [18]

Alternative Installationsvarianten:

- Clients der Netzwerkversion
  - Zur Einrichtung weiterer Arbeitsplätze mit dem Datenbankserver „Einzelplatz- und Serverversion mit Microsoft SQL Server“, um von weiteren Arbeitsplätzen das Arbeiten zu ermöglichen
  - Folgen Sie der Anleitung im Kapitel 2.3 [32]
- Server der Netzwerkversion
  - Als Datenbankserver ohne Arbeitsplatz für die Clients der Netzwerkversion
  - Folgen Sie der Anleitung im Kapitel 2.5 [47]

9. Online- und Offline-Schließanlagen (nonDoT)

Die Online- und Offline-Schließanlagen (nonDoT) zeichnen sich in erster Linie dadurch aus, dass der Speicherort der Zutrittsberechtigungen in den Türen/Zutrittspunkten liegt. Eine Programmierung der Transponder ist dadurch nicht möglich. Die im Zutrittspunkt programmierte Zutrittsberechtigung ermöglicht dem Träger des Transponders nach dem Buchen am Zutrittspunkt den freien Zugang. Liegt keine Berechtigung für diesen Transponder vor, wird der Zugang verwehrt.

Der Schließanlagentyp nonDoT ist die klassische Ausführung bei der die Daten zwischen dem BKS KeyManager direkt an die verkabelten Zutrittspunkte oder indirekt durch eine Programmierung mit einem Programmiergerät vor Ort an die (Offline-) Zutrittspunkte übermittelt werden.

In Online-Schließanlagen werden durch den Online-Dienst die Zutrittsberechtigungen bequem per Funk an die Zutrittspunkte übertragen. Ein Ablaufen der Zutrittspunkte mit einem Programmiergerät ist nicht mehr notwendig.

Voraussetzung für die Funktion ist die Installation von Netzwerkkomponenten und Funk-Zutrittspunkten. Verwenden Sie als Netzwerkkomponente Ethernetbuskoppler (EBK) und Funkwandmodule (SE FM). Der Buskoppler wandelt die Signale von RS485-Bus auf Ethernet/LAN um. Sollte als Netzwerkkomponente ein Ethernetbuskoppler Funk (EBK FM) verwendet werden, ist ein Funkbaustein im EBK integriert, sodass die Funk-Zutrittspunkte direkt angesteuert werden.

Dagegen werden in Offline-Schließanlagen die Zutrittsberechtigungen indirekt mit einem Programmiergerät in die Zutrittspunkte übertragen. In Reihenfolge wird zur Übermittlung das Programmiergerät mit dem BKS KeyManager verbunden und die Daten eingespielt. Die Programmierung des Zutrittspunkts wird dann vor Ort am Zutrittspunkt ausgeführt. Zur Quittierung ist das Programmiergeräts mit dem BKS KeyManager zu verbinden. Vorteile sind eine einfache Installation und Einrichtung wie z. B. eine Verkabelung ist bei diesen Anlagen nicht notwendig.

9.1 Online-Schließanlage (nonDoT)

9.1.1 Systemübersicht nonDoT-Anlage online

Beim Betrieb einer Online-Anlage werden folgende Elemente benötigt.

SE-Schließanlage mit SE-Technologie

- Transponder
- Online-Türen|Zutrittspunkte wie z. B. Funk-Zylinder, Funk-Schlösser, Funk-Beschläge, Funkwandmodul (SE FM) etc.
- Ethernetbuskoppler-Funkmodul (EBK FM)
- Ethernetbuskoppler (EBK) für Funkwandmodul (SE FM)
- Offline-Türen|Zutrittspunkte wie z. B. Zylinder, Schlösser, Beschläge, Wandleser etc.
- Programmiergerät (SXPG)
- Vernetzung des KeyManagers
  - Anschluss EBK über LAN
  - Anbindung SE FM über den RS485-Bus an das EBK
  - Verbindung EBK FM / SE FM zu den Zutrittspunkten über Funk

BKS KeyManager

- SE-Lizenz Free, Standard oder Professional
- SE-Lizenz Online

9.1.2 Installationsarten nonDoT-Anlage online

Empfohlene Installation des BKS KeyManagers

- Einzelplatz- und Serverversion mit Microsoft SQL Server
  - Für einen einzelnen Arbeitsplatz (Single User)
  - Aktivieren Sie „SE-Online-Modul installieren“.
  - Folgen Sie der Anleitung im Kapitel 2.2 [18]
- Optional ist bei Verwendung von Wandlesern der EBK Pro-Dienst zu installieren
  - Folgen Sie der Anleitung im Kapitel 2.8 [57]

Alternative Installationsvarianten

- Clients der Netzwerkversion
  - Zur Einrichtung weiterer Arbeitsplätze mit dem Datenbankserver „Einzelplatz- und Serverversion mit Microsoft SQL Server“, um von weiteren Arbeitsplätzen das Arbeiten zu ermöglichen
  - Folgen Sie der Anleitung im Kapitel 2.3 [32]
- Server der Netzwerkversion
  - Als Datenbankserver ohne Arbeitsplatz für die Clients der Netzwerkversion
  - Aktivieren Sie „SE-Online-Modul installieren“.
  - Folgen Sie der Anleitung im Kapitel 2.5 [47]

9.2 Offline-Schließanlagen (nonDoT)

9.2.1 Systemübersicht nonDoT-Anlage offline

Beim Betrieb einer Offline-Anlage werden folgende Elemente benötigt.

SE-Schließanlage mit SE-Technologie

- Transponder
- Türen|Zutrittspunkte wie z. B. Zylinder, Schlösser, Beschläge, Wandleser etc.
- Programmiergerät (SXPG)

BKS KeyManager

- SE-Lizenz Free, Standard oder Professional

9.2.2 Installationsarten nonDoT-Anlage offline

Empfohlene Installation des BKS KeyManagers

- Einzelplatz- und Serverversion mit Microsoft SQL Server
  - Für einen einzelnen Arbeitsplatz (Single User)
  - Folgen Sie der Anleitung im Kapitel 2.2 [18]

Alternative Installationsvarianten:

- Einzelplatzversion mit interner Datenbank
  - Für Kleinstanlagen mit einem Arbeitsplatz (Single User) und interner Firebird-Datenbank
  - Folgen Sie der Anleitung im Kapitel 2.4 [40]
- Clients der Netzwerkversion
  - Zur Einrichtung weiterer Arbeitsplätze mit dem Datenbankserver „Einzelplatz- und Serverversion mit Microsoft SQL Server“, um von weiteren Arbeitsplätze das Arbeiten zu ermöglichen
  - Folgen Sie der Anleitung im Kapitel 2.3 [32]
- Server der Netzwerkversion
  - Als Datenbankserver ohne Arbeitsplatz für die Clients der Netzwerkversion
  - Folgen Sie der Anleitung im Kapitel 2.5 [47]

10. Mandanten-Modul

Das Mandanten-Modul ist eine Funktion des BKS KeyManagers, mit der Sie in der Lage sind, in Ihrer Schließanlage mehrere Mandanten zu verwalten, ohne das diese einen gegenseitigen Einblick in die Daten, Benutzerverwaltung etc. der Schließanlagen der anderen Mandanten zu haben.

Die Schließanlage kann als eine Einheit bestehen bleiben und wird nicht physisch in Instanzen bzw. verschiedene Datenbanken geteilt. Die Unterteilung wird über das Strukturieren der Anlage in einzelne Mandantenbereiche in Unteranlagen ermöglicht.

Jeder Mandant, sprich Kunde oder Auftraggeber, verwaltet seinen Bereich selbstständig, ohne Einsicht oder Zugriff auf die anderen Mandanten zu haben. Ein Mandant kann z. B. ein Unternehmen sein, dass eine Etage in einem Bürogebäude gemietet hat. Der BKS KeyManager ermöglicht es diesen Mieter, den gemieteten Bereich als Teil der Schließanlage zu verwalten. Über die gemietete Etage hinaus besteht aber kein Zugriff auf die Verwaltung der anderen Etagen.

Um in Ihrer Schließanlage Mandanten verwalten zu können, bietet Ihnen der BKS KeyManager zwei Möglichkeiten die Strukturierung bzw. Aufteilung vorzunehmen.

- Unterteilung der Anlage in Mandanten basierend auf Benutzerrechten.
  Die Benutzer jedes Mandanten erhalten jeweils nur auf den zum Mandanten gehörenden Teil der Schließanlage einen Zugriff. Die anderen Teile der Schließanlage sind für den Benutzer nicht sichtbar und können nicht bearbeitet werden.
- Unterteilung der Anlage in Mandanten über Unteranlagen und Benutzerrechte
  Zusätzlich zur Unterteilung durch Benutzerrechte (siehe oben) werden die Transponder, Türen und Freigabeterminals vom Schließanlagenteil des jeweiligen Mandanten in Unteranlagen strukturiert. Dadurch wird eine klarere Unterteilung der Anlage erreicht. Die Transponder und Türen der Unteranlagen können auch nur in ihrer Unteranlage, der sie zugewiesen wurden, verwaltet und programmiert werden. Transponder und Türen können für die Verwendung in anderen Unteranlage freigegeben werden.

HINWEIS **Vor der Installation und Einrichtung des Mandanten-Moduls empfehlen wir, ein Back-up Ihrer Schließanlage durchzuführen, siehe Kapitel 7.2.1 [362]!**

HINWEIS **Durch das Erstellen von Unterlagen gehen die vorhandenen Berechtigungen der Transponder und Türen, die Unteranlagen zugeordnet wurden, verloren und müssen neu vergeben werden.**

10.1 Installation des Mandanten-Moduls

Zum Freischalten des Mandanten-Moduls und zur Nutzung der Funktionen ist es erforderlich, die Lizenz „Mandanten-Modul“ einzulesen. Diese Lizenzerweiterung können Sie nachträglich in Ihrer Bestandsanlage, aber auch bei der Einrichtung einer neuen Anlage installieren.

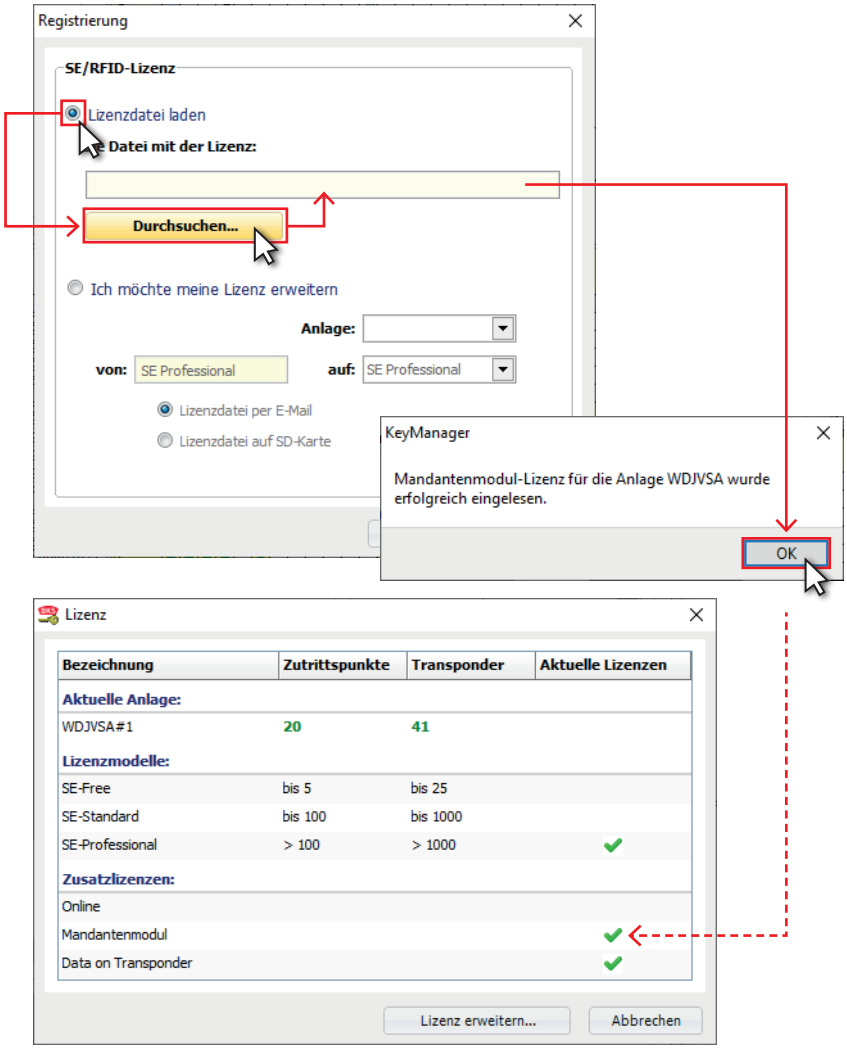
Bei einer vorhandenen Anlage die Lizenz Mandanten-Modul hinzufügen.

- Die Schritte der Installation mit Erklärung finden Sie im Kapitel 5.3 [269].

Bei der Erstellung einer neuen Anlage die Lizenz Mandanten-Modul einlesen.

- Die Beschreibung des Ablaufs der Erstellung einer neuen Anlage mit den Assistenten finden Sie im Kapitel 5.4 [272]. Die Schritte zum Einlesen der Lizenz sind explizit je nach Art der Einrichtung in den Unterkapiteln 5.4.1.1 [275] oder 5.4.2.1 [282] erläutert.

Im Fenster „Lizenz“ können Sie sich die Übersicht der aktuell in Ihrer Anlage verwendeten Lizenzen anzeigen lassen. Folgen Sie hierzu der Beschreibung von Kapitel 5.1.2.1 [264].



10.2 Voraussetzung für die Einführung des Mandanten-Moduls

Das Mandanten-Modul ist eine Erweiterung des BKS KeyManagers, die mit den im Kapitel 8 [388] und Kapitel 9 [393] beschrieben Schließanlagen kompatibel ist.

Die Grundlage eines erfolgreichen Betriebs Ihrer Schließanlage mit dem Mandanten-Modul ist eine gründliche Vorbereitung auf die Umstellung. Erstellen Sie ein Layout Ihrer Anlage, mit dem Sie die Strukturierung in die einzelnen Mandanten und deren Teile der Anlage über die Gruppenberechtigungen umsetzen können.

Layout
Erstellen Sie ein Layout Ihrer Schließanlage mit Mandanten, inventarisieren Sie die Komponenten, indem Sie den einzelnen Mandanten die Komponenten zuordnen und in folgenden Punkten definieren.

- Aufteilung der Türen, Transponder und Freigabeterminals (FGT) und Festlegung, zu welchen Mandaten diese gehören.
- Festlegung, welche Türen, Transponder und FGTs zu übergeordneten oder allgemeinen Bereichen zugehören und so Bestandteil der Hauptanlage bleiben.
- Türen und Transponder, die von mehreren Unteranlagen verwendet werden, auflisten.
- Temporäre mehrfache Verwendungen von Türen und Transponder, die von mehreren Unteranlagen verwendet werden, auflisten.
- Optionale Festlegung von globalen Zeitzonen in der Hauptanlage als Rahmen für die Zeitzonen der Unteranlagen.

Gruppen
Clustern Sie nach Ihrem Layout die Transponder und Türen in Gruppen nach der Struktur der Mandanten mit den unten aufgeführten Funktionsmenüs.

- Fassen Sie die Transponder nach Zugehörigkeit zu Transpondergruppen zusammen
  siehe Kapitel 4.2.7 [186].
- Fassen Sie die Türen nach Zugehörigkeit zu Türgruppen zusammen,
  siehe Kapitel 4.4 [212].

Die eigentliche Umsetzung und Strukturierung Ihrer Schließanlage in Mandanten wird mithilfe dieser Gruppen in den nächsten Kapiteln beschrieben.

10.3 Mandantenanlage auf Grundlage der Benutzerrechte

Eine Möglichkeit, eine Mandantenanlage im BKS KeyManager einzurichten, ist über die Benutzerrechte für die Mandaten nur partielle Bereiche der Schließanlage freizuschalten. Die Unterteilung in Mandanten wird nur über die Zugriffsrechte der Benutzer der Mandanten und die Einschränkung auf die mandantenbezogenen Anlagenteile erreicht.

Mit Hilfe der im vorherigen Kapitel erstellten Gruppen können Sie den Benutzern der Mandanten die Zugriffsrechte auf den Bereich des Mandanten der Schließanlage gewähren. Voraussetzung ist, dass die Gruppen den Mandantenbereich abdecken. Die Zugriffsrechte werden über die von Ihnen bestimmten Tür-, Personen-, Depot- und Transpondergruppen gesteuert und geben nur den Teil der Schließanlage frei, den die Gruppen abdecken. Die Gruppenrechte sind so zu vergeben, dass der Benutzer des Mandanten seinen Teil der Schließanlage selbstständig verwalten kann.

Andere Bereiche der Anlage sind nicht sichtbar bzw. freigeschaltet. Folglich kann der Benutzer diese auch nicht bearbeiten. Die Tiefe der Bearbeitungsmöglichkeiten ist abhängig von den Rechten des Benutzerprofils und den nach ihrem Aufgabenprofil und Arbeitsgebiet mit unterschiedlichen Möglichkeiten der Zugriffsberechtigungen.

In der Benutzerverwaltung können vom Administrator die Benutzer der Mandanten angelegt werden.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Einstellungen“ und wählen den Menüpunkt „Benutzerverwaltung ...“ aus.
- Folgen Sie der Anleitung im Kapitel 6.4 [347] zur grundsätzlichen Einrichtung des Benutzers und im Folgenden der Beschreibung zum Mandanten-Modul.

In den vier letzten Registern der Benutzerverwaltung werden die Rechte, die den Mandanten betreffen, im Benutzerprofil verwaltet.

(1) Türgruppen, siehe auch Kapitel 6.4.5 [351].
Wählen Sie eine oder mehrere Türgruppen aus, welche für den gewählten Benutzer freigeschaltet sein sollen. Drücken Sie zur Bestätigung auf Speichern.

(2) Personengruppen (der Anlage), siehe auch Kapitel 6.4.6 [352]
Wählen Sie eine oder mehrere Personengruppen aus, welche für den gewählten Benutzer freigeschaltet sein sollen. Drücken Sie zur Bestätigung auf Speichern.

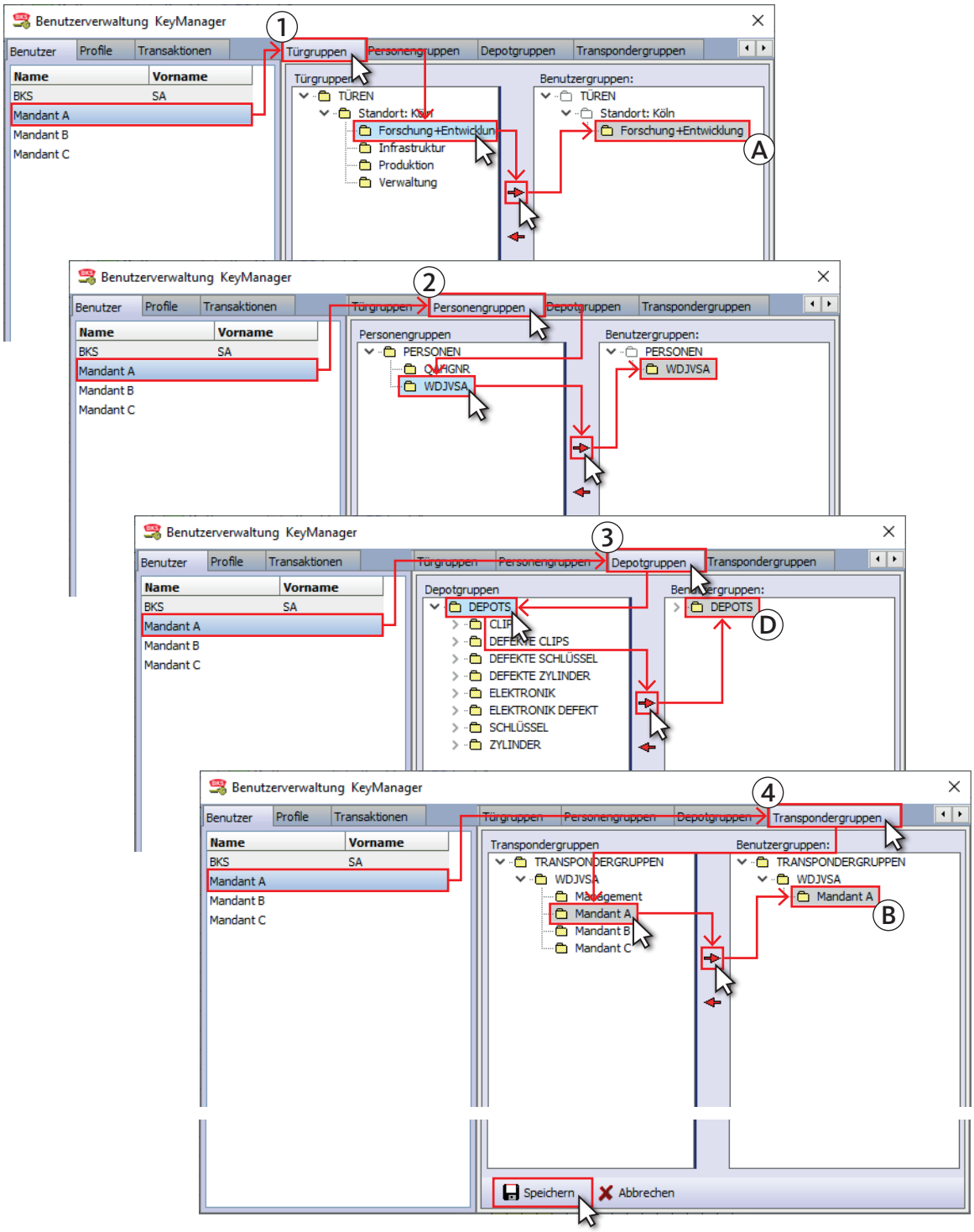
HINWEIS **Transponder, welche an Personen ausgegeben worden sind, werden nur in der Matrix (B) angezeigt, wenn die Personengruppe und die Transpondergruppe freigeschaltet ist.**

(3) Depotgruppen, siehe auch Kapitel 6.4.7 [353]
Wählen Sie eine oder mehrere Depots aus, welche für den gewählten Benutzer freigeschaltet sein sollen. Drücken Sie zur Bestätigung auf Speichern.

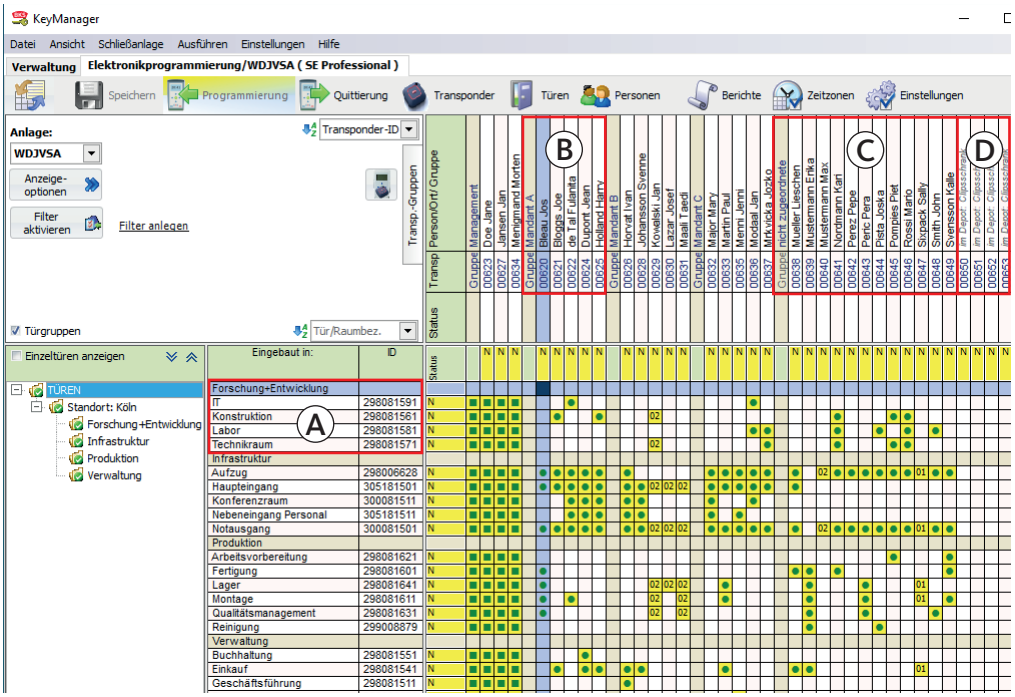
(4) Transpondergruppen, siehe auch Kapitel 6.4.8 [354]
Wählen Sie eine oder mehrere Transpondergruppen aus, welche für den gewählten Benutzer freigeschaltet sein sollen. Drücken Sie zur Bestätigung auf Speichern.

Ist der Mandant über die Benutzerrechte richtig abgebildet, wird nach der Anmeldung des Benutzers nur noch der den Mandanten betreffenden Teil der Schließanlage angezeigt.

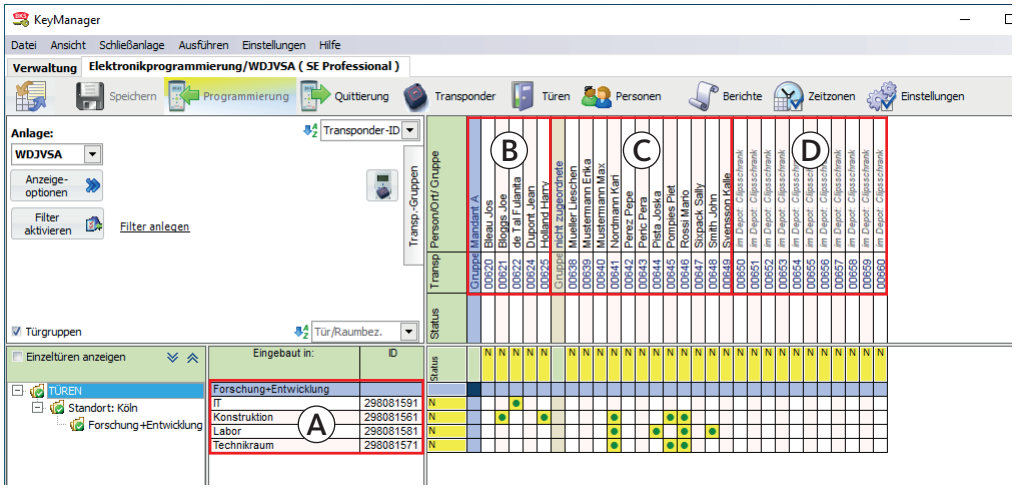
Berechtigungen des Benutzers für das Mandanten-Modul



10.3.1 Ansicht der Berechtigungsmatrix als angemeldeter Benutzer „Administrator“.



10.3.2 Ansicht der Berechtigungsmatrix als angemeldeter Benutzer „Mandant A“.



(A) Anzeige der für den Benutzer freigegebenen Türgruppen.
(B) Anzeige der für den Benutzer freigegebenen Transpondergruppen.
(C) Anzeige der Transponder die keiner Tranpondergruppe zugeordnet sind aber über die Personengruppe freigeben sind.
(D) Anzeige der Transponder die über das Depot sind freigegeben sind.

Angezeigte Elemente sind im Rahmen des Benutzerprofils zu bearbeiten. Zutrittsberechtigungen der Transponder und Türen bleiben bestehen.
Keine Berechtigung und Anzeige zu Türen und Transponder, die zu einer Gruppe gehören und für die der Benutzer nicht berechtigt wurde.

10.4 Mandantenanlage auf Grundlage von Unteranlagen und Benutzerrechten

Eine weitere Möglichkeit Ihre Schließanlage in Mandaten zu strukturieren, ist die Aufteilung in Unteranlagen mithilfe der Funktionen Unteranlagen und Benutzerrechte. Bei der Umstellung in eine Mandantenanlage werden die Hauptanlage und die Unteranlagen im BKS KeyManager einzelne Anlagen strukturiert. In der Berechtigungsmatrix werden die Hauptanlage und die Unteranlage getrennt dargestellt und verwaltet, wobei die Anlage weiterhin eine zusammenhängende Einheit bildet.

Für jeden Mandanten wird eine eigene Unteranlage erstellt, für die im weiteren Benutzer definiert werden. Mit den Funktionen Unteranlagen und Benutzerrechte ist eine genauere Abgrenzung der Anlagenteile und eine feinere Auflösung der Struktur ermöglicht.

Im Menü Unteranlagen und der Benutzerverwaltung können die Unteranlagen und Benutzer der Mandanten vom Administrator angelegt werden.

- Zur Einrichtung der Unteranlagen öffnen Sie das Menü „Unteranlagen“. Folgen Sie den Anleitungen von Kapitel 10.4.1 [404] und der weiteren Kapitel in diesem Abschnitt.
- Für die Einrichtung der Benutzer folgen Sie den Anleitungen von Kapitel 10.3 [399] sowie Kapitel 10.4.8 [415].

Grundsätzlich sind bei der Einrichtung der Hauptanlage und der Unteranlagen sowie der damit zusammenhängen Umstellung der Berechtigungsmatrix die Transponder und Türen in Abhängigkeit der Verwendung und örtlichen Einrichtung in den folgenden Punkten den Mandanten anzupassen bzw. in dessen Strukturen aufzuteilen.

Zuordnung
Türen, Türgruppen, Transponder und Transpondergruppen werden Bestandteil des Mandanten und durch die Benutzer der Unteranlage verwaltet. Eine Zuordnung ist jeweils nur einmal möglich. Wird keine Zuordnung getroffen, sind die Komponenten Teil der Hauptanlage, siehe 10.4.3 [406]. Buskoppler mit Freigabeterminals können mehrere Mandanten zugeordnet werden, 10.4.5 [410].

Freigabe
Transpondergruppen, die in der Hauptanlage verwaltet werden, können für die Türen der Mandanten freigegeben werden. Eine Freigabe kann für mehrere Untergruppen vergeben werden. Die Benutzer der Mandanten sind in der Regel nicht zur Verwaltung berechtigt, siehe 10.4.4 [408].

Sichtbare Transponder in Unteranlagen
Transponder, die einem Mandanten zugeordnet wurden, können für andere Mandanten zu einer gemeinsamen Nutzung freigeben werden. Die Benutzer der Untergruppen können die Berechtigung, die ihre Türen Betreffen selbst verwalten. Eine Freigabe kann für mehrere Mandanten vergeben werden, aber nicht für die Hauptgruppe 10.4.4 [408].

Vergabe der Berechtigungen der Benutzer
Die Benutzer können nur die Verwaltung innerhalb der Grenzen, der sie für Transaktionen in ihrem Benutzerprofil berechtigt wurden, ausführen. Der Benutzer „Administrator“ kann alle Mandanten verwalten, 10.4.8 [415].

Verwaltung
Es kann immer nur der in der Berechtigungsmatrix ausgewählte Mandant verwaltet. Für die Verwaltung eines anderen Mandanten muss dieser vorher ausgewählt werden. Freischaltung der Benutzer der Mandanten für die erforderlichen Transaktionen.

Programmierung
Die Benutzer der Mandanten können nur die für sie sichtbaren Teile der Schließanlage bzw. die Komponenten ihrer eigenen Unteranlage programmieren.

Spezielle Anforderungen

Den Mandanten zugeordnete Transponder können nicht zu Türen der Hauptschließanlage wie z. B. Eingangstür, Schranke oder Aufzugstür berechtigt werden. Mithilfe einer geeigneten Strukturierung der Mandantenanlage sind hier beispielhaft zwei Wege zur Umsetzung aufgezeigt.

– Erstellen Sie eine neue Unteranlage neben den Mandantenanlagen und ordnen dieser Unteranlage die von den Mandanten zu begehenden Türen der Hauptanlage zu. Die Transponder der Mandanten können dadurch über die Funktion „Sichtbare Transponder in Unteranlage“ für diese Tür freigeschaltet werden. Transpondergruppen der Hauptanlage sind über die Funktion „Freigabe“ freizuschalten. Einzelne Transponder der Hauptanlage sind Transpondergruppen hinzuzufügen.

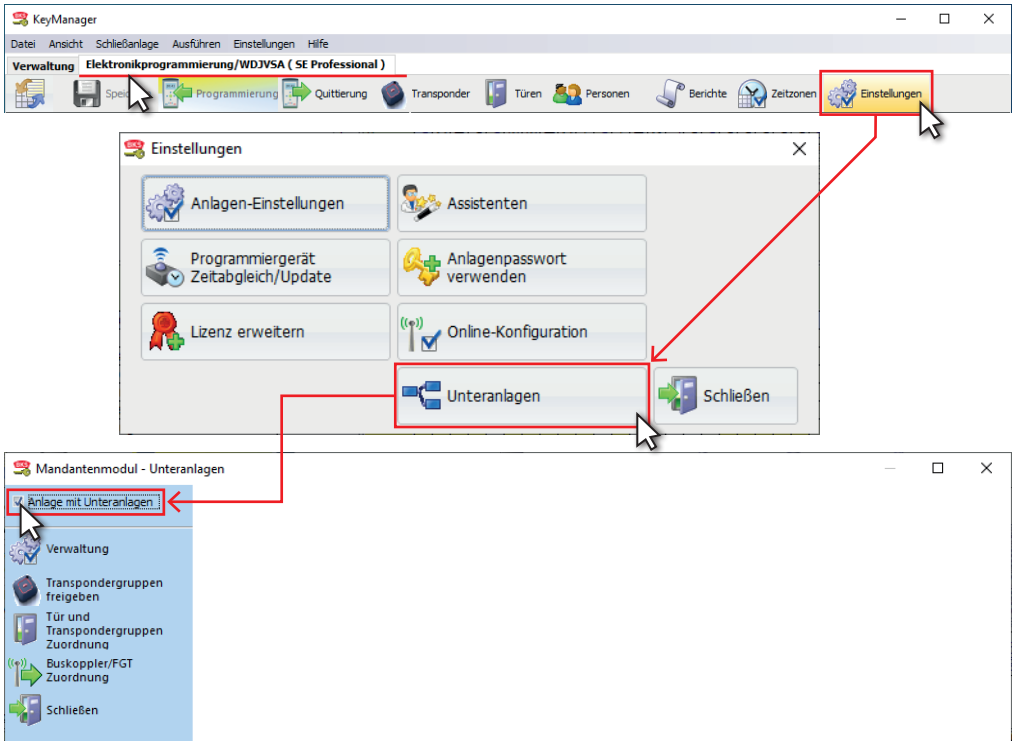
– Erstellen Sie vor der Aufteilung der Schließanlage in Unteranlagen Transpondergruppen mit den Transpondern, die eine Berechtigung zu Türen der späteren Hauptanlage erhalten sollen. Berechtigen Sie die Transpondergruppen zu den gewünschten Türen der späteren Hauptanlage über eine Gruppenberechtigung. Die Berechtigungen können nach der Umwandlung in eine Mandantenanlage nur durch die Benutzer der Hauptanlage erfolgen.

10.4.1 Einrichtung der Unteranlagen

Im Menü „Unteranlagen“ können Sie die Schließanlage in Unteranlagen unterteilen. Die Anlagenteile, die nicht einer Unteranlage zugeordnet worden sind, werden zur Hauptanlage. Die Unteranlagen sind immer der Hauptanlage untergeordnet.

Durch die Aktivierung der Checkbox werden die weiteren Menüpunkte freigeschaltet und Sie können mit der Strukturierung beginnen. Die weiteren Erstellungen und Konfigurationsmöglichkeiten entnehmen Sie bitte den folgenden Kapiteln dieses Abschnitts.

- Wählen Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ den Menüpunkt „Einstellungen“ aus.
- Drücken Sie auf den Button „Unteranlagen“.
- Aktivieren Sie die Checkbox „Anlage mit Unteranlagen“.



Die Beschreibung der weiteren Menüpunkte und wie Sie mit deren Hilfe die Schließanlage in eine Hauptanlage und in Unteranlagen aufteilen können, entnehmen Sie bitte den nächsten Kapiteln.

- Nach Strukturierung Ihrer Schließanlage drücken Sie auf den Button „Schließen“, um den Dialog „Mandantenmodul“ zu beenden.

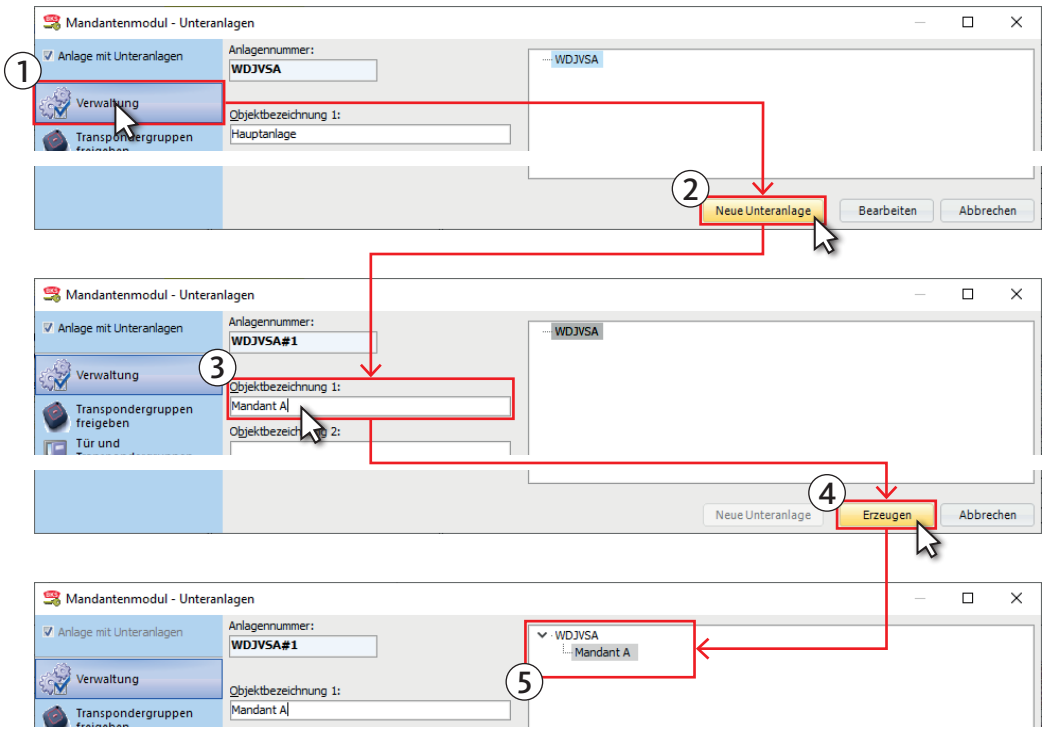
10.4.2 Verwaltung der Unteranlagen

Im Menü „Verwaltung“ können Sie neue Unteranlagen erzeugen und die Angaben und Bezeichnungen schon vorhandener Unteranlagen bearbeiten. Die Unteranlagen sind so anzulegen, dass sie die Struktur der Mandanten abbilden und die Schließanlage unterteilen. Die Unteranlagen werden in der Baumansicht unter der Hauptanlage dargestellt.

Ziel ist es, durch die Unteranlagen die Struktur der Mandanten abzubilden. Legen Sie die Struktur vor der Umsetzung fest und fügen keine nicht benötigten Unteranlagen hinzu, weil einmal angelegte Unteranlagen nicht aus der Baumansicht gelöscht werden können.

- Wählen Sie den Menüpunkt (1) „Verwaltung“ aus.
- Drücken Sie auf den Button (2) „Neue Unteranlage“.
- Geben Sie in Feld (3) „Objektbezeichnung 1:“ einen Namen bzw. eine Bezeichnung für die neue Unteranlage ein. Optional können Sie in den unter diesem Feld stehenden Feldern weitere Angaben zur Unteranlage machen.
- Drücken Sie auf den Button (4) „Erzeugen“.
- Die neue Unteranlage wird im Verzeichnisbaum (5) der Schließanlage angezeigt.

Wiederholen Sie diesen Vorgang um weitere Unteranlagen hinzuzufügen. Einmal erzeugte Unteranlagen können nur bearbeitet aber nicht gelöscht werden.

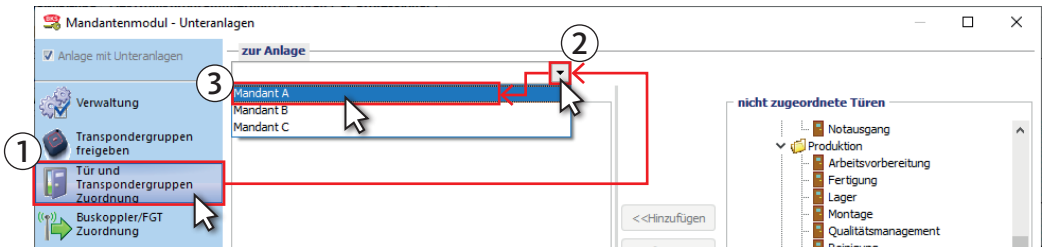


10.4.3 Zuordnung von Türen und Transpondern sowie Gruppen von diesen zu einer Unteranlage

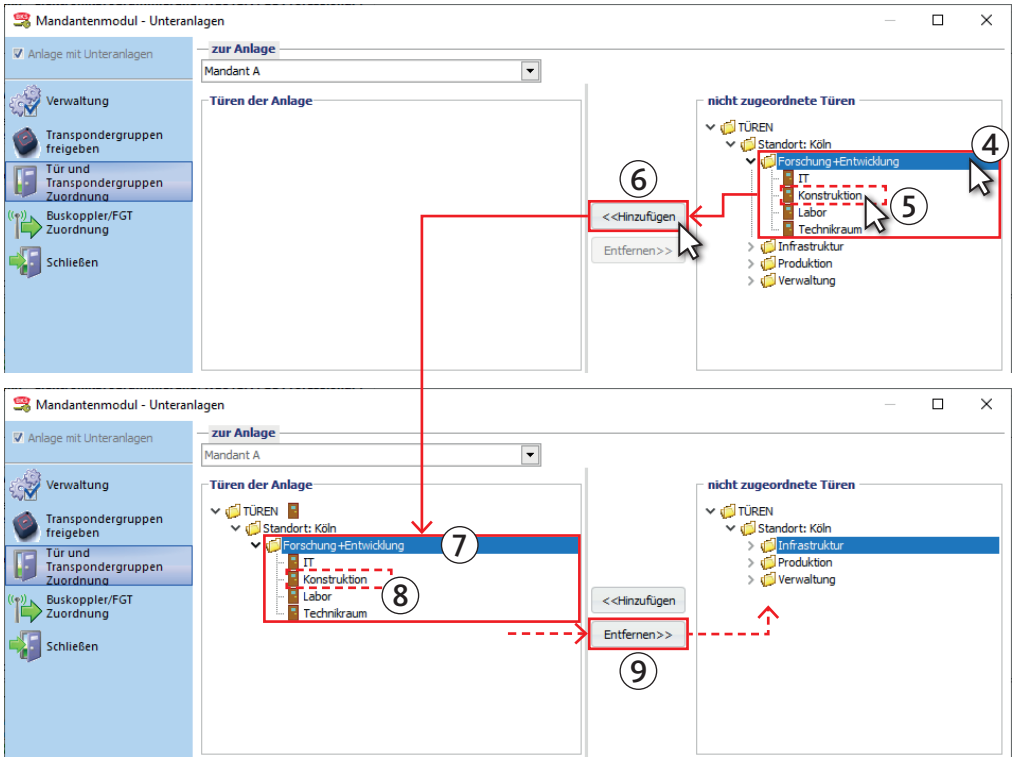
Im Menü „Tür und Transpondergruppen Zuordnung“ werden Türen, Türgruppen, Transponder und Transpondergruppen der ausgewählten Unteranlage zugeordnet. Eine Mehrfachverwendung ist nicht möglich und einmal zugeordneten Komponenten lassen sich nicht anderen Unterlagen zuordnen oder für diese Freigeben, siehe Kapitel 10.4.4 [408]. Nur eine gemeinsame Nutzung einzelner Transponder in anderen Unteranlagen, wie im Kapitel 10.4.4 [408] beschrieben, ist möglich.

Erstellen Sie ggf. vor der Zuordnung im Rahmen der Planung der Unteranlagen die benötigten Türgruppen, siehe Kapitel 4.4 [212] und Transpondergruppen, siehe Kapitel 4.2.7 [186].

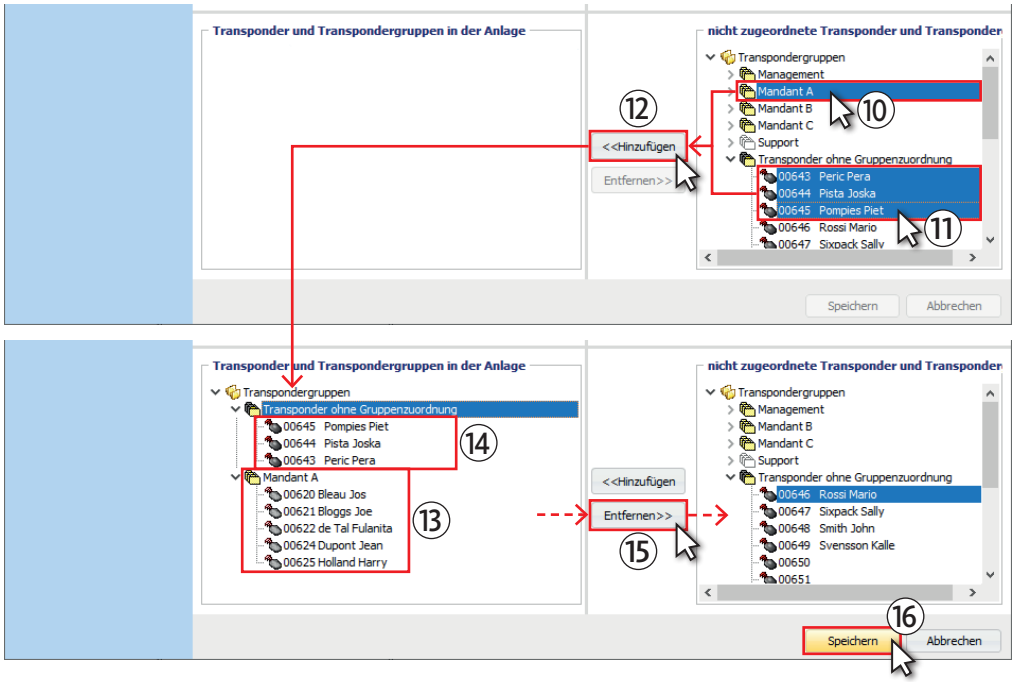
- Wählen Sie den Menüpunkt (1) „Tür und Transpondergruppen Zuordnung“ aus.
- Öffnen Sie das Dropdown-Menü (2) und wählen die zu editierende Unteranlage (3) aus.



- Wählen Sie die Türgruppen (4) und/oder einzelnen Türen (5) aus, welche zur Unteranlage (3) zugeordnet bzw. hinzugefügt werden sollen.
- Drücken Sie auf den Button (6)„<< Hinzufügen“.



- Die ausgewählten Türgruppen (4) und/oder Türen (5) werden in die Spalte „Türen der Anlage“ zu den Komponenten der Unteranlage (7), (8) verschoben und so zum Bestandteil der ausgewählten Unteranlage (3) bzw. dieser zugeordnet.
- Zum Entfernen der Türgruppen (7) und/oder Türen (8) aus der Unteranlage, wählen Sie die gewünschten Türgruppen und Türen aus und drücken auf den Button „Entfernen>>“.
- Wählen Sie die Tranpondergruppen (10) und/oder einzelnen Transponder 11) aus, welche zur Unteranlage (3) zugeordnet bzw. hinzugefügt werden sollen.
- Drücken Sie auf den Button (12) „<< Hinzufügen“.



- Die ausgewählten Transpondergruppen (10) und/oder Transponder (11) werden in die Spalte „Transponder und Transpondergruppen der Anlage zu den Komponenten der Unteranlage (13), (14) verschoben und so zum Bestandteil der ausgewählten Unteranlage (3) bzw. dieser zugeordnet.
- Zum Entfernen der Transpondergruppen (13) und/oder Transponder (14) aus der Unteranlage wählen Sie die gewünschten Transpondergruppen und Transponder aus und drücken auf den Button „Entfernen>>“ (15).
- Drücken Sie auf den Button (16) „Speichern“, um die Eingaben zu sichern.

Typische Anwendungsfälle für die Zuordnung sind Komponenten der Anlage, welche fest einem einzelnen Mandanten bzw. dessen Anlagenteil zugeordnet werden können und keine Überschreitung mit der Hauptanlage haben wie z. B. die Türen eines vermieteten Bereichs oder Transponder der dort beschäftigten Personen.

10.4.4 Freigabe von Transpondergruppen für Unteranlagen

Im Menü „Transpondergruppen freigeben“, werden Transpondergruppen für die ausgewählte Unteranlagen freigegeben. Die Transponder der Gruppe können zu den Türen der freigegebenen Unteranlage eine Berechtigung zum Zutritt erhalten. Die Transpondergruppe mit den dazugehörigen Transpondern bleibt Bestandteil der Hauptanlage. Aus diesem Grund kann die Transpondergruppe nur von einem Benutzer mit Rechten für die Hauptanlage und die Unteranlage, in der die Transpon-spondergruppe freigegeben ist, verwaltet werden.

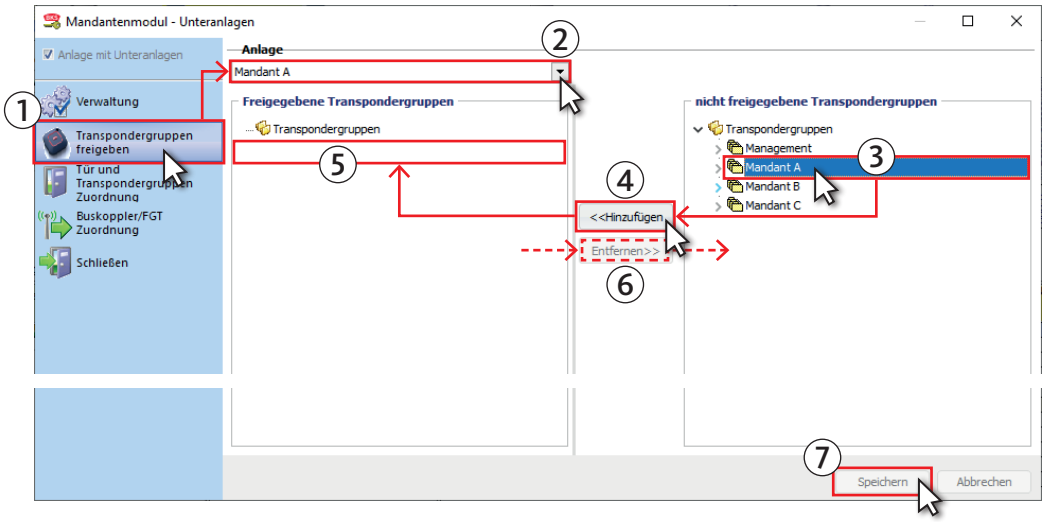
Eine Transpondergruppe kann für mehrere Unteranlagen freigegeben werden. Eine Kombination der Freigabe und Zuordnung zu Unteranlagen, siehe Kapitel 10.4.3 [406], ist nicht möglich. Freigegebene Transpondergruppen können keiner Unteranlage zugeordnet werden bzw. einmal zugeordnete Transpondergruppen können nicht freigegeben werden.

Die Freigabe von Transpondergruppen ist dann sinnvoll, wenn Transponder in verschiedenen Teilen der Anlage wie z. B. in der Haupt- und einer Unteranlage einen Zutritt erhalten sollen, ohne das die Benutzer der Unteranlage die Transpondergruppen verwalten können. Die Benutzer der Unteranlage haben trotz der Freigabe keinen Zugriff auf die Verwaltung und können folglich für die freigegebene Transpondergruppe keine Rechte in ihre Unteranlage vergeben.

Transpondergruppen mit der Berechtigung Generalhauptschließanlage (GHS) sind in allen Unteranlagen berechtigt, aber nur nach Freigabe für die Benutzer der Untergruppen sichtbar. Für die Verwaltung ist das Benutzerprofil „Administrator“ notwendig.

Erstellen Sie ggf. vor der Zuordnung im Rahmen der Planung der Unteranlagen die benötigten Transpondergruppen, siehe Kapitel 4.2.7 [186].

- Wählen Sie den Menüpunkt (1) „Transpondergruppen freigeben“ aus.
- Öffnen Sie das Dropdown-Menü (2) und wählen eine Unteranlage aus, für die Transpondergruppen freigegeben werden sollen.
- Wählen Sie eine Transpondergruppe (3) in der Spalte „Nicht freigegebene Transpondergruppen“ aus, die in den nächsten Schritten freigegeben werden soll.



- Zur Freigabe dieser Transpondergruppe in der gewählten Unterlage und zum Verschieben in die Spalte „Freigegebene Transpondergruppen“ drücken Sie auf den Button (4) „<<Hinzufügen“.
- Zum Entfernen einer Transpondergruppe aus der Unterlage bzw. aus der Spalte „Freigegebene Transpondergruppen“ wählen Sie die gewünschte Transpondergruppe (5) aus und drücken auf den Button (6) „Entfernen>>“.
- Drücken Sie auf den Button (7) „Speichern“, um die Eingaben zu sichern.

Typische Anwendungsfälle für die Freigabe von Transpondergruppen sind Dienste, welche die Zuordnung der einzelnen Mandanten bzw. Anlagenteile überschreiten können wie z. B. Hausmeister, Reinigung, Service oder die Geschäftsleitung die in der gesamten Schließanlage berechtigt werden können.

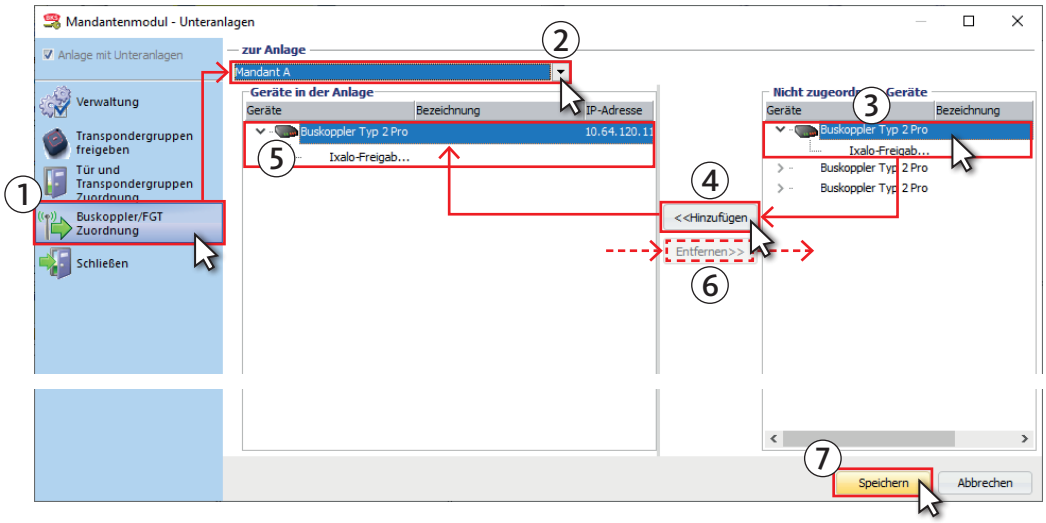
10.4.5 Zuordnung der Buskoppler und Freigabeterminals zur Unteranlage

Im Menü „Buskoppler/FGT Zuordnung“ können die mit dem BKS KeyManager verbundenen Buskoppler [Ethernet-Buskoppler (EBK)] und die an diese angeschlossenen Freigabeterminals (FGT) zu einer Unteranlage zugeordnet werden.

Eine mehrfache Verwendung der Buskoppler ist möglich. Ein Buskoppler kann zu mehreren Unteranlagen zugeordnet werden. Alle an den Buskoppler angeschlossenen FGTs werden dabei mit zugeordnet. Nicht zugeordnete Buskoppler sind nur der Hauptanlage zugeordnet und stehen in den Unterlagen nicht zur Verfügung und können von diesen nicht genutzt werden.

Der Betrieb von Buskoppler und Freigabeterminals ist nur in einer Data on Transponder-Anlage (DoT-Anlage) möglich.

- Wählen Sie den Menüpunkt (1) „Buskoppler/FGT Zuordnung“ aus.
- Öffnen Sie das Dropdown-Menü (2) und wählen die Unteranlage aus, zu welcher der Buskoppler zugeordnet werden soll.
- Zur Auswahl drücken Sie in der Spalte „Nicht zugeordnete Geräte“ auf einen Buskoppler (3).
- Zum Hinzufügen dieses Buskopplers zur gewählten Unterlage und zum Verschieben in die Spalte „Geräte der Anlage“ drücken Sie auf den Button (4) „<<Hinzufügen“.
- Zum Entfernen des Buskopplers aus der Unterlage bzw. aus der Spalte „Geräte der Anlage“ wählen Sie den gewünschten Buskoppler (5) aus und drücken auf den Button (6) „Entfernen>>“.
- Drücken Sie auf den Button (7) „Speichern“, um die Eingaben zu sichern.



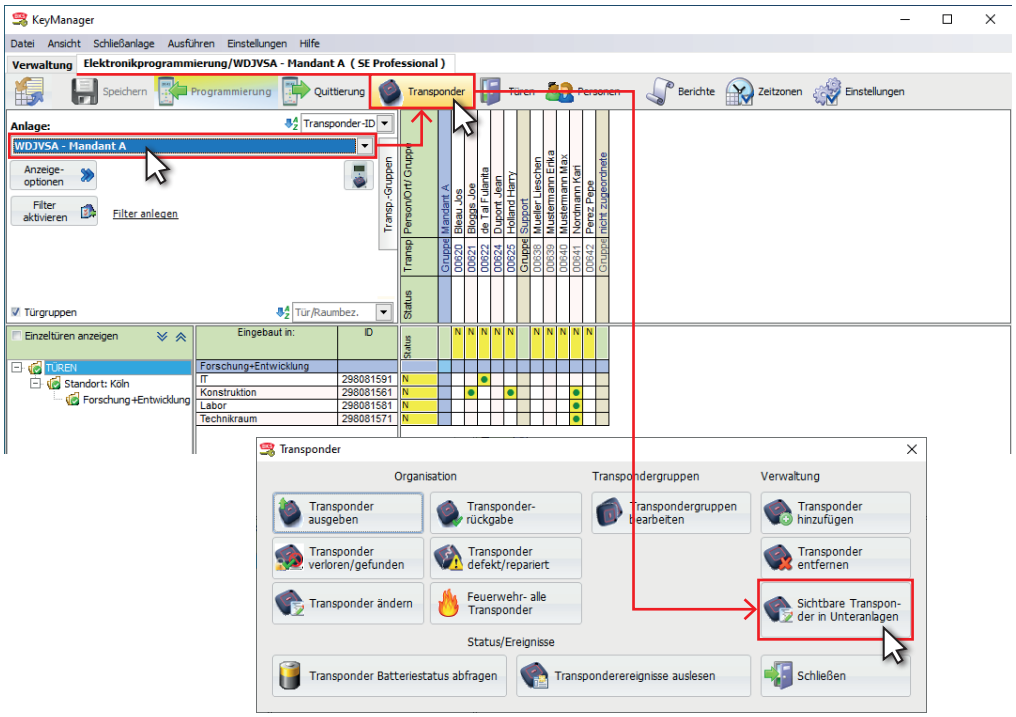
10.4.6 Freigabe von Transponder für andere Unteranlagen

Im Menü „Sichtbare Transponder in Unteranlagen“ können Sie Transponder, welche einer Unteranlage zugeordnet worden sind, für eine gemeinsame Nutzung mit anderen Unteranlagen freigeben.

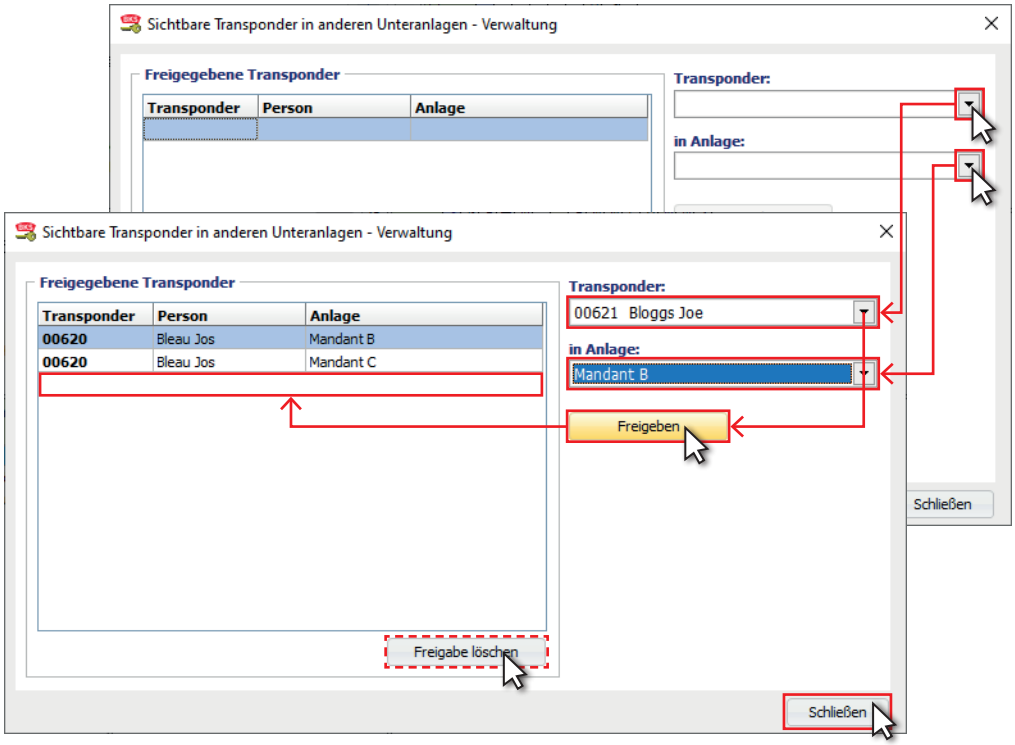
Diese Transponder können durch eine Freigabe für den Zutritt zu Türen anderer Unteranlagen berechtigt werden. Die Benutzer der Unteranlage, für welche die Transponder freigeben worden sind, können innerhalb ihrer Benutzerrolle die gemeinsam genutzten Transponder in ihrer Unteranlage verwalten.

Gemeinsam genutzte Transponder, welche eine Zugehörigkeit zu einer Transpondergruppe in der zugeordneten Unteranlage haben, werden ohne Anpassung der Benutzerrechte nicht angezeigt. Damit die Transponder von den Benutzern der freigegebenen Untergruppe verwaltet werden können, benötigen diese die Berechtigung zu der Transpondergruppe in der eigentlich zugeordneten Unteranlage.

- Wählen Sie im Dropdown-Menü „Anlage:“ die Unteranlage aus, von der Sie zugeordnete Transponder für eine gemeinsame Nutzung freigeben wollen.
- Drücken Sie in der Berechtigungsmatrix des Registers „Elektronikprogrammierung/...“ auf den Menüpunkt „Transponder“.
- Drücken Sie auf den Button „Sichtbare Transponder in Unteranlagen“.



- Wählen Sie im Dropdown-Menü „Transponder“ einen Transponder aus, der auch in einer anderen Unteranlage genutzt werden soll.
- Im Dropdown-Menü „in Anlage:“ wählen Sie die Unteranlage aus, für die der Transponder für die gemeinsame Nutzung freigeschaltet werden soll.
- Drücken Sie auf den Button „Freigeben“ zur Freischaltung.
- Die für die gemeinsame Nutzung freigegebenen Transponder werden in der Spalte „Freigegebene Transponder“ mit der Unteranlage, für die sie freigeschaltet sind, angezeigt.
- Zum Entfernen eines Transponders aus der Spalte „Freigegebene Transponder“ und Entziehen der erteilten Freigabe für eine andere Unteranlage, wählen Sie den gewünschten Transponder aus und drücken auf den Button „Freigabe löschen“.
- Drücken Sie auf den Button „Schließen“, um den Dialog zu beenden.



In der Berechtigungsmatrix der Unteranlagen, zu denen die Transponder nicht zugeordnet wurden, werden die zur gemeinsamen Nutzung freigegebenen Transponder in Spalte „Gruppe“ unter der Bezeichnung „nicht zugeordnet“ einsortiert und angezeigt.

10.4.7 Zeitzonen im Mandanten-Modul

Im Menü „Zeitzonen“ können auch bei aktiviertem Mandanten-Modul Zeitzonen angelegt und bearbeitet werden. Zum Anlegen oder Bearbeiten der Zeitzonen beachten Sie die Beschreibung im Kapitel 4.7 [243].Bei der Verwendung der Zeitzonen im Mandanten-Modul ist es wichtig, das vor dem Editieren die Anlage ausgewählt wurde, für welche eine Zeitzone erstellt werden soll.

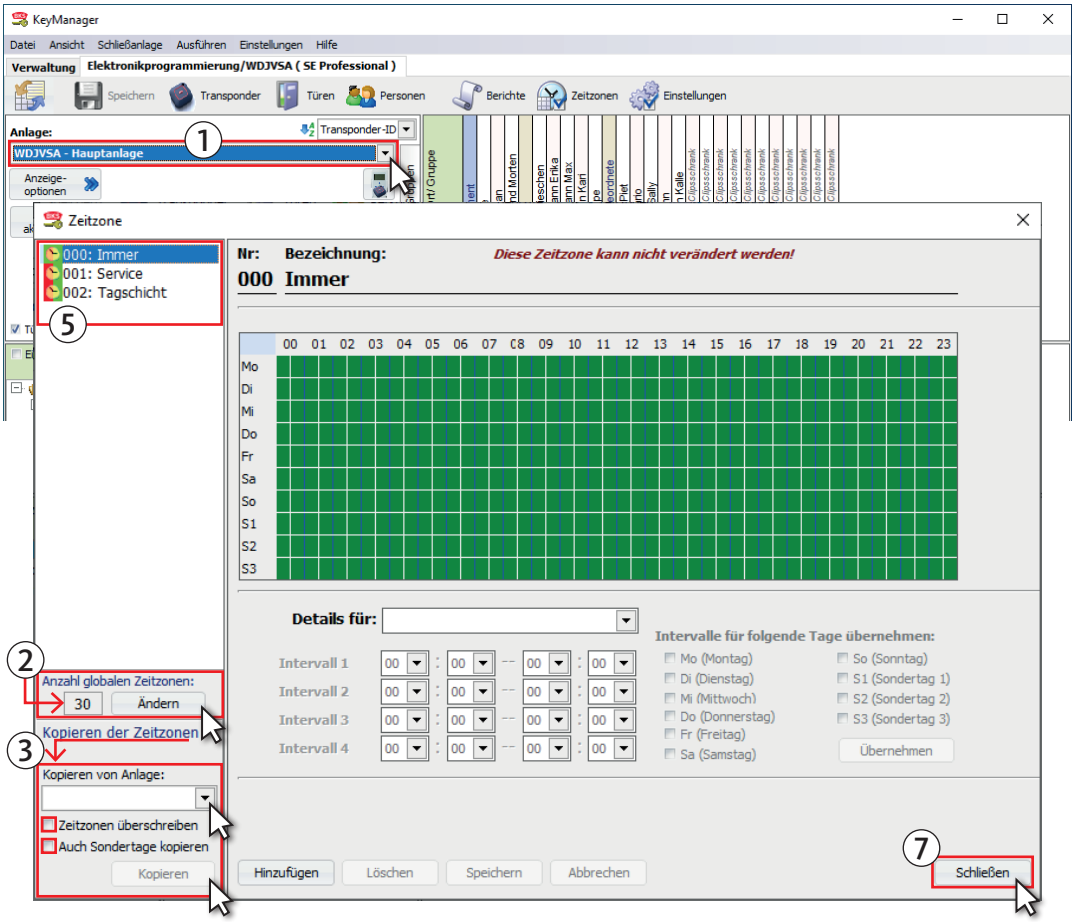
- Wählen im Dropdown-Menü (1) den Teil der Anlage aus welchen Sie bearbeiten wollen. Wird die Hauptanlage ausgewählt, können Sie globale Zeitzonen (5) anlegen, die auch für die Unteranlagen gültig sind bzw. bearbeiten die globalen Zeitzonen.

Die Anzahl der Zeitzonen in Ihrer Schließanlage ist auf 128 Zonen begrenzt. Nach Festlegung der Anzahl der globalen Zeitzonen können die restlichen freien Plätze in den Unteranlagen als Zeitzonen (6) festgelegt werden.

- Im Feld (2) „Anzahl der globalen Zeitzonen“ können Sie die maximale Anzahl der globalen Zeitzonen vorgeben. Drücken Sie auf den Button „Ändern“.

Verwalten Sie im KeyManager mehrere Schließanlagen, können Sie die Zeitzonen aus einer anderen Hauptanlage in die aktuell gewählte Hauptanlage kopieren.

- Im Feld (3) „Kopieren der Zeitzonen“ können Sie im Dropdown-Menü die gewünschte Hauptanlage auswählen. Drücken auf den Button „Kopieren“.
- Drücken Sie auf den Button (7) „Schließen“ und beenden den Dialog.



Die Zeitzonen (6) für Unteranlagen können Sie nach Auswahl der Unteranlage erstellen bzw. bearbeiten. Diese Zeitzonen sind nur für die gewählte Untergruppe gültig. Die Benutzer der Unteranlagen müssen zur Erstellung von Zeitzonen in ihren Benutzerprofilen berechtigt worden sein.

In Abhängigkeit der Anzahl der globalen Zeitzonen (2) beginnt die Zählung der Zeitzonen (6) in den Unteranlagen einen Zähler nach der maximalen Anzahl der globalen Zeitzonen. Die Anzahl aller Zeitzonen ist auf 128 Zonen begrenzt.

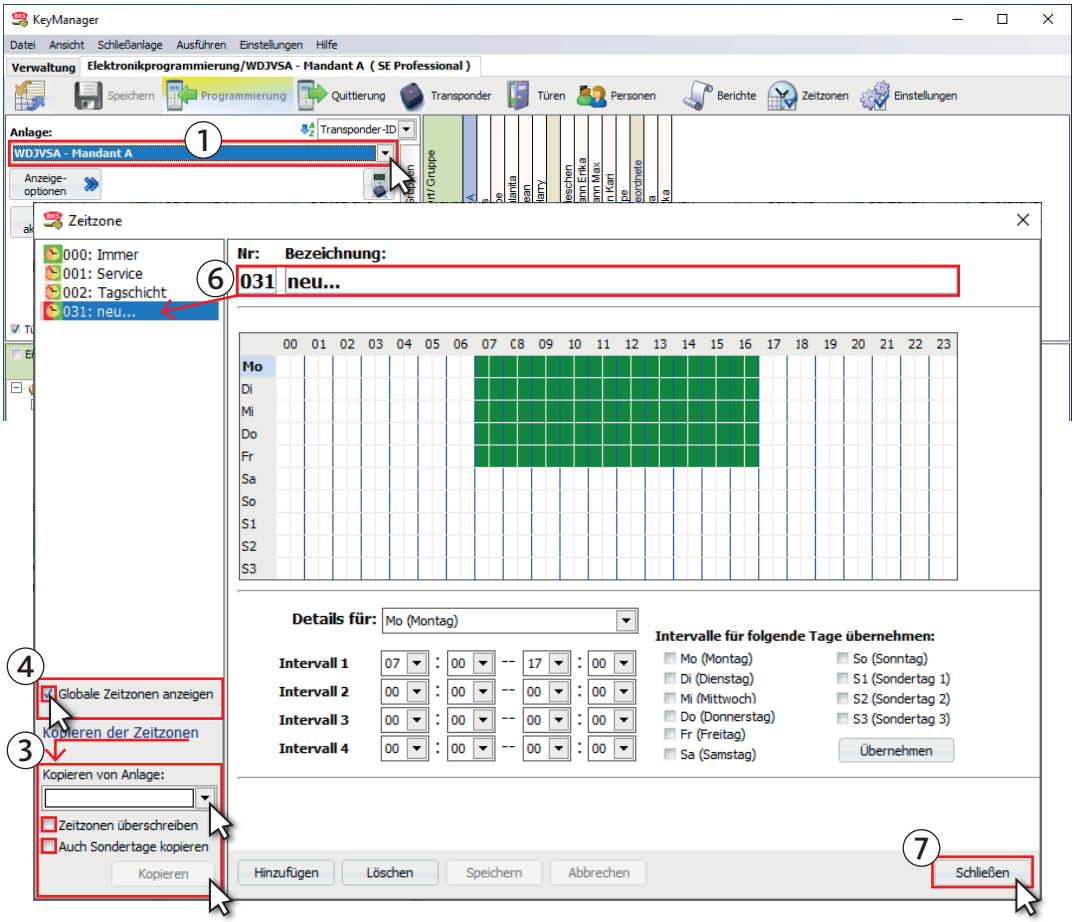
- Wählen im Dropdown-Menü (1) eine Unteranlage aus.

Die globalen Zeitzonen können in den Unteranlagen ein- oder ausgeblendet werden.

- Aktivieren Sie die Checkbox (4) „Globale Zeitzonen anzeigen“ zum Einblenden.

Verwalten Sie in Ihrer Schließanlage mehrere Unteranlagen, können Sie die Zeitzonen aus einer anderen Unteranlage in die aktuell gewählte Unteranlage kopieren.

- Im Feld (3) „Kopieren der Zeitzonen“ können Sie im Dropdown-Menü die gewünschte Unteranlage auswählen. Drücken auf den Button „Kopieren“.
- Drücken Sie auf den Button (7) „Schließen“ und beenden den Dialog.



10.4.8 Einrichtung der Benutzerrechte

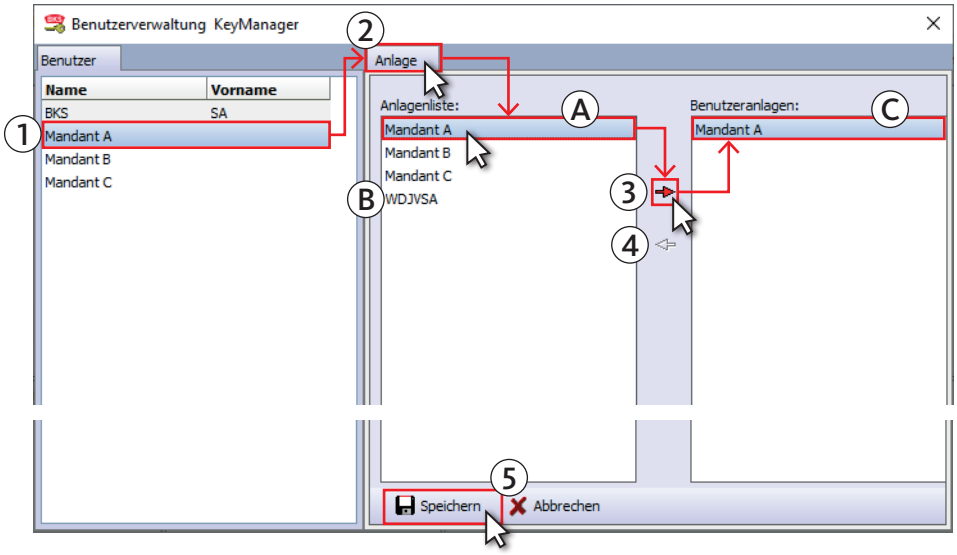
Nach der Strukturierung der Anlage in eine Hauptanlage und Unteranlagen müssen für die Unteranlagen eigene Benutzer angelegt werden, damit von diesen Benutzern die Unteranlagen verwaltet werden können. Die Zugriffsrechte der Benutzer der Mandanten sind so zu gewähren, dass der Benutzer zum Ausführen der Tätigkeiten berechtigt ist und gleichzeitig den Zugriff zum Bereich der Unteranlage erhält.

Die Zugriffsrechte der Benutzer werden in der Benutzerverwaltung vom Administrator verwaltet. In diesem Menü können auch die Benutzer der Mandanten angelegt werden.

- Öffnen Sie in der Menüleiste das Dropdown-Menü „Einstellungen“ und wählen den Menüpunkt „Benutzerverwaltung ...“ aus.
- Folgen Sie der Anleitung im Kapitel 6.4 [347] zur grundsätzlichen Einrichtung des Benutzers und im Folgenden der Beschreibung zum Mandanten-Modul.

Im Register „Anlage“ der Benutzerverwaltung wird die Berechtigung des Benutzers zu den Unteranlagen (A) und zur Hauptanlage (B) verwaltet.

- Wählen Sie den Benutzer (1) und das Register (2) „Anlage“ aus.
- Zur Auswahl drücken Sie in der Anlagenliste auf die Bezeichnung (A) für eine Unterlage bzw. die Bezeichnung (B) zur Auswahl der Hauptanlage.
- Drücken Sie auf den Button (3) zum Hinzufügen und die ausgewählte Anlage (A) wird in die Spalte Benutzeranlagen als Anlage (C) verschoben.
- Zum Entfernen von Anlagen aus den Benutzeranalgen wählen Sie die gewünschte Bezeichnung (C) aus und drücken auf den Button (4) zum Entfernen.
- Drücken Sie auf den Button (5) „Speichern“, um die Eingaben zu sichern.



Vervollständige Sie das Benutzerprofil in den vier letzten Registern der Benutzerverwaltung und definieren die Rechte die den Mandanten betreffen. Folgen Sie der Anleitung im Kapitel 10.3 [399].

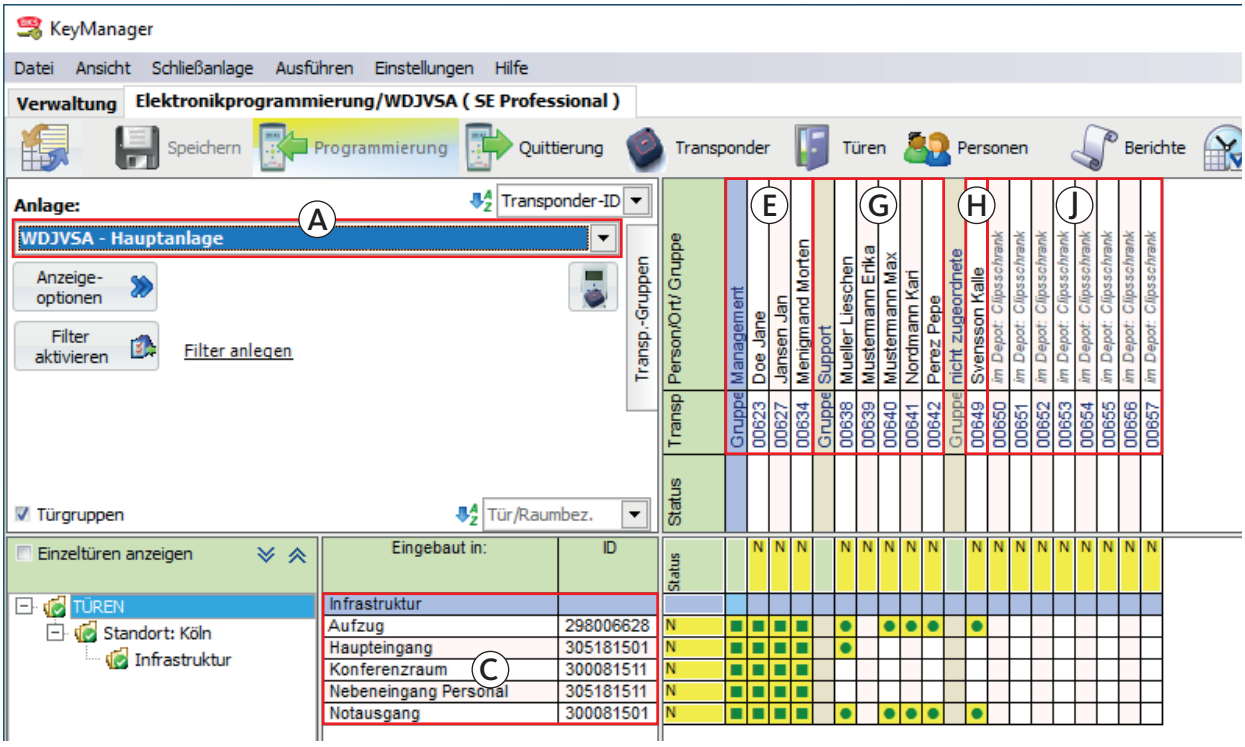
- Komplettieren Sie das Benutzerprofil in den Registern „Türgruppen“, „Personengruppen“ (der Anlage), „Depotgruppen“ und „Transpondergruppen“.

10.4.9 Berechtigungsmatrix mit Unteranlagen

Durch Aktivierung der Unteranlagen wird die Berechtigungsmatrix in eine Hauptanlage und Unteranlagen strukturiert. Eine gleichzeitige Ansicht von allen Teilanlagen in einer kompletten Matrix ist nach der Aktivierung nicht mehr möglich.

10.4.9.1 Ansicht der Hauptanlage in der Berechtigungsmatrix

- Wählen Sie im Dropdown-Menü (A) „Anlage:“ die Hauptanlage aus, damit diese in der Berechtigungsmatrix angezeigt wird. Die Bezeichnung der Hauptanlage ist nach der Anlagennummer benannt.



(A) Anzeige der aktuell angezeigten Anlage: Hauptanlage in der Berechtigungsmatrix.

(C) Türgruppen und/oder Türen, die über die Zuordnung keiner Unteranlage zugeordnet wurden, werden der Hauptanlage zugeordnet und können nur in der Hauptanlage verwaltet werden.

(E) – Transpondergruppen, die über die Zuordnung keiner Unteranlage zugeordnet wurden, werden der Hauptanlage zugeordnet und können nur in der Hauptanlage verwaltet werden.
– Transpondergruppen mit der Berechtigung Generalhauptschließanlage (GHS) werden der Hauptanlage zugeordnet und können nur in der Hauptanlage verwaltet werden. Durch eine Freigabe wird die GHS-Transpondergruppe in der Unteranlage angezeigt.

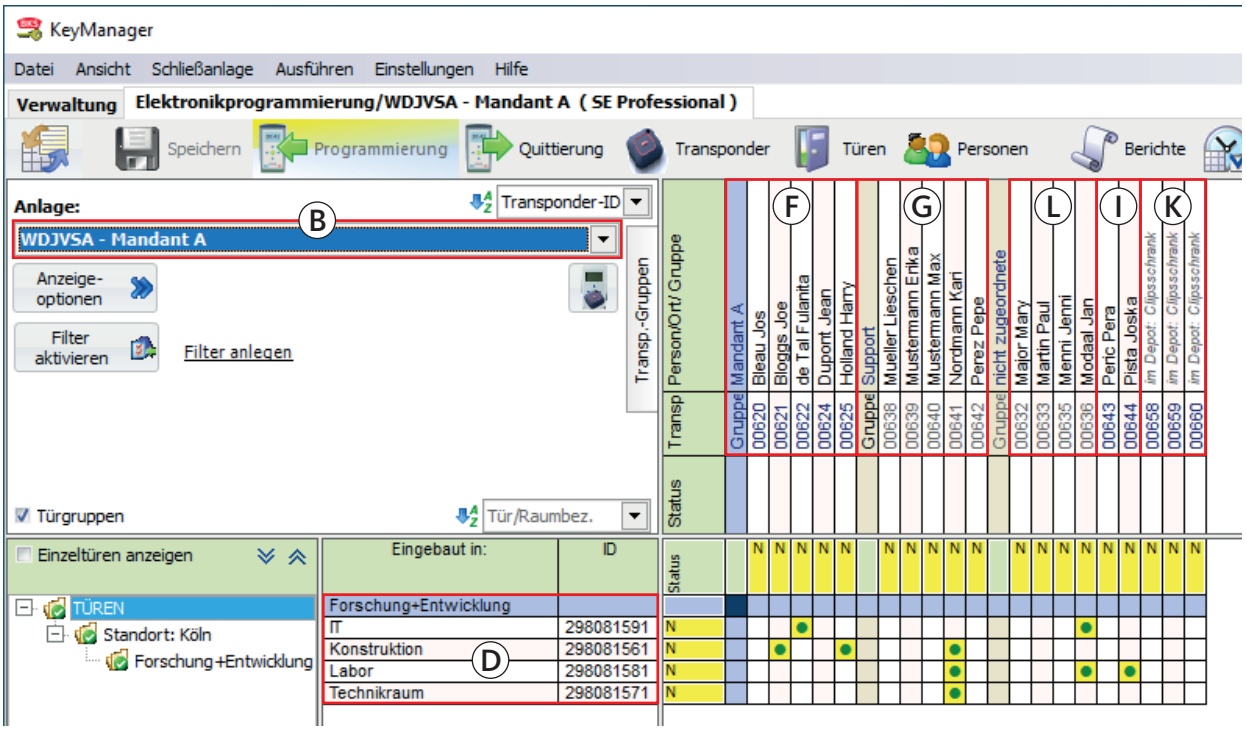
(G) Transpondergruppen, die über die Freigabe für Unterablagen freigegeben sind, können nur in der Hauptgruppe verwaltet werden. In der Unteranlage werden diese Gruppen nur angezeigt.

(H) Transponder, die über die Zuordnung keiner Unteranlage zugeordnet und an keine Person ausgeben wurden, werden der Hauptanlage zugeordnet und können nur in der Hauptanlage verwaltet werden.

(J) Transponder die über die Zuordnung keiner Unteranlage zugeordnet und an keine Person ausgeben wurden, werden der Hauptanlage zugeordnet und können nur in der Hauptanlage verwaltet werden.

10.4.9.2 Ansicht der Unteranlage „Mandant A“ in der Berechtigungsmatrix

- Wählen Sie im Dropdown-Menü (B) „Anlage:“ die gewünschte Unteranlage aus, damit diese in der Berechtigungsmatrix angezeigt wird. Die Bezeichnung der Unteranlagen wird in der Verwaltung, siehe Kapitel 10.4.2 [405] vergeben.



(B) Anzeige der aktuell angezeigten Anlage: Unteranlage in der Berechtigungsmatrix.

(D) Türgruppen und/oder Türen, die über die Zuordnung ausschließlich der Unteranlage (B) zugeordnet sind und in der Unteranlage verwaltet werden.

(F) Transpondergruppen und/oder Transponder, die über die Zuordnung ausschließlich der Unteranlage (B) zugeordnet sind, können in dieser Unteranlage verwaltet werden.

(G) Transpondergruppen, die über die Freigabe für Unteranlagen freigegeben sind, können nur in der Hauptgruppe verwaltet werden. In der Unteranlage werden diese Gruppen nur angezeigt.

(I) Transponder, die zu keiner Transpondergruppe gehören und einer Unteranlage zugeordnet sind, werden in der Unteranlage angezeigt und können in Unteranlagen verwaltet werden.

(K) Transponder, die noch an keine Person ausgeben sind und einer Unteranlage zugeordnet oder über das Transpondermenü für diese freigeben wurden, werden in der Unteranlage angezeigt und können in Unteranlage verwaltet werden.

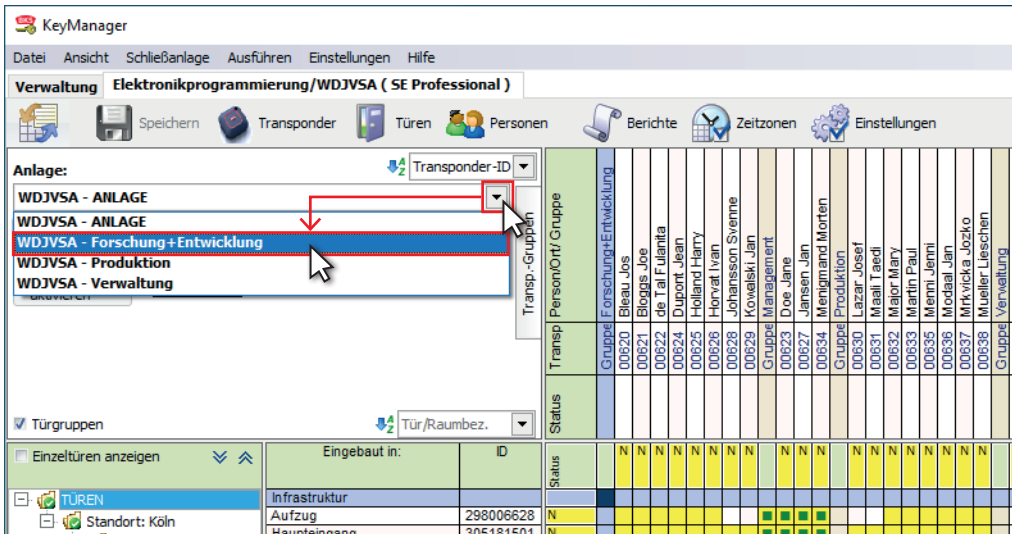
(L) Transponder, die über das Transpondermenü für eine Unteranlage freigeben wurden, werden in der Unteranlage angezeigt und können in Unteranlage verwaltet werden.

10.4.10 Ansichtswechsel zwischen der Hauptanlage und den Unteranlagen

Nach Fertigstellung der Mandantenanlage können Sie als Benutzer mit dem Profil „Admin“ zwischen den verschiedenen Unteranlagen in der Berechtigungsmatrix wechseln und diese ohne Einschränkung bearbeiten.

Ein angemeldeter „normaler“ Benutzer dagegen kann nur im Rahmen des für ihm in der Benutzerverwaltung erstellten und zugewiesenen Benutzerprofils sich die für ihn freigegebenen Unteranlagen anzeigen lassen und zwischen ihnen wechseln. Eine Bearbeitung ist nur im Rahmen dieser Rechte möglich.

- Wählen Sie im Dropdown-Menü „Anlage:“ die gewünschte Unteranlage oder Hauptanlage aus, um die Berechtigungsmatrix angezeigt zu bekommen.



Notizen | Notes | Notes | Notas

Herausgeber:
BKS GmbH
Heidestr. 71
42549 Velbert
Deutschland
Tel. + 49 (0) 2051 201-0
Fax + 49 (0) 2051 201-97 33

www.g-u.com

Fehler, Irrtümer und technische Änderungen vorbehalten.

Vorsprung mit System