Handbuch MobileKey

03.2018

ALLEGION

SimonsVoss technologies

Handbuch MobileKey

Inhaltsverzeichnis

1 Einleitung ... 5
1.1 Sicherheitshinweise ... 5
1.2 Systemvoraussetzungen ... 5
1.2.1 Verwaltung der Schließanlage ... 5
1.2.2 Programmierung ... 6
2 Die Matrix ... 8
3 Grundfunktionen ... 10
3.1 Schloss anlegen ... 10
3.2 Schlüssel anlegen ... 11
3.3 PinCode-Tastatur anlegen ... 11
3.4 Berechtigung vergeben und abspeichern ... 12
3.5 Zeitplan vergeben ... 12
3.6 Programmieren von Komponenten ... 13
3.6.1 HINWEIS: Programmieren über ein Windows-Gerät ... 14
3.6.2 HINWEIS: Programmieren über ein Android-Gerät ... 14
3.6.3 HINWEIS: Programmieren über ein macOS-Gerät ... 14
3.7 Zurücksetzen von Komponenten ... 15
3.8 Erzwungenes Löschen von Komponenten ... 15
3.9 Zutrittsprotokoll auslesen ... 16
4 MobileKey ONLINE-Erweiterung ... 17
4.1 SmartBridges ... 17
4.1.1 SmartBridges aufstellen ... 17
4.1.2 SmartBridges einrichten ... 18
4.1.3 SmartBridges löschen ... 19
4.2 Schloss mit Netzwerkknoten (LockNode) einrichten ... 20
4.3 Schloss mit Netzwerkknoten (LockNode) löschen ... 21
4.4 Online-Komponenten konfigurieren ... 21
4.5 Programmieren von Komponenten ... 22
4.6 Verbindung zu Online-Komponenten trennen ... 22
4.7 Fernöffnung durchführen ... 23
4.8 Key4Friends ... 23
4.8.1 Schlüssel teilen ... 23
4.8.2 Schlüssel verwalten ... 24
4.9 DoorMonitoring Schloss - Angezeigte Schlosszustände ... 24
5 Eventmanagement ... 27
5.1 Benachrichtigungen in der Web-App ansehen ... 27

Handbuch MobileKey

5.2 Regeln erstellen ... 27
5.2.1 Regel vom Typ "Zutritt" erstellen ... 27
5.2.2 Regel vom Typ "DoorMonitoring" erstellen ... 28
5.2.3 Regel vom Typ "Alarme" erstellen ... 29
5.3 Wichtige Hinweise ... 29

6 Hilfestellungen ... 31
6.1 Hilfe mit Schlüsseln (Transpondern) ... 31
6.2 Hilfe mit Schlössern (z.B. Schließzylinder) ... 32
6.3 Gelöschte Komponenten zurücksetzen oder wiederverwenden ... 33
6.4 Komponenten auslesen ... 34
6.5 Hilfe zur SmartBridge ... 34
6.6 Hilfe zu Online-Schlössern ... 35
6.7 Netzwerkfehler ... 35
6.8 Manuelles Zurücksetzen der LockNodes ... 35

7 Wartung, Reinigung und Desinfektion ... 37

8 MobileKey Apps ... 38

9 Konformitätserklärung ... 39

10 Hilfe & Kontakt ... 40

11 Tipps & Tricks ... 41
11.1 Verknüpfung zur Web-App ... 41
11.2 Verwendung von Schlüsseln ohne USB-Programmierstick ... 41
11.3 Sprache einstellen ... 42

12 Anhang: Handbücher der einzelnen Komponenten ... 43
12.1 Handbuch Schließzylinder ... 43
12.1.1 Bestimmungsgemäßer Gebrauch ... 43
12.1.2 Sicherheitshinweise ... 43
12.1.3 Allgemein ... 45
12.1.4 Ausführungen ... 48
12.1.5 Einbauanleitung ... 61
12.1.6 Signaltöne ... 67
12.1.7 Batteriewechsel ... 68
12.1.8 Wartung, Reinigung und Desinfektion ... 70
12.1.9 Einsatzmöglichkeiten ... 71
12.1.10 Zubehör ... 72
12.1.11 Datenblätter ... 72
12.2 Handbuch PinCode-Tastatur ... 74
12.2.1 Bestimmungsgemäßer Gebrauch ... 74
12.2.2 Sicherheitshinweise ... 74
12.2.3 Konfiguration ... 75

Handbuch MobileKey

12.2.4 Programmierung ... 76
12.2.5 Montage & Batteriewechsel ... 76
12.2.6 Bedienung ... 77
12.2.7 Technische Daten ... 77
12.2.8 Konformitätserklärung ... 77

12.3 Handbuch SmartBridge ... 77
12.3.1 Allgemein ... 77
12.3.2 Sicherheitshinweise ... 78
12.3.3 Gehäuse ... 79
12.3.4 Aufputz Leitungszuführung ... 80
12.3.5 Konfiguration der IP-Settings ... 81
12.3.6 Technische Anschlüsse ... 81
12.3.7 Beschaltung IO-Connector ... 81
12.3.8 RouterNode zurücksetzen ... 84
12.3.9 Technische Daten ... 85
12.3.10 Antenne ... 87
12.3.11 Spannungsversorgung ... 88
12.3.12 Konformitätserklärung ... 88
12.3.13 Hilfe & Kontakt ... 88

12.4 Handbuch SmartRelais ... 89
12.4.1 Bestimmungsgemäßer Gebrauch ... 89
12.4.2 Sicherheitshinweise ... 89
12.4.3 Allgemein ... 91
12.4.4 Inbetriebnahme ... 96
12.4.5 Anschlüsse ... 98
12.4.6 Konfigurationen in der Software ... 100
12.4.7 Signalisation ... 105
12.4.8 Wartung ... 105
12.4.9 Technische Daten ... 106

12.5 Handbuch Programmierstick ... 108
12.5.1 Bestimmungsgemäßer Gebrauch ... 108
12.5.2 Sicherheitshinweise ... 108
12.5.3 Lieferumfang ... 109
12.5.4 Inbetriebnahme ... 109
12.5.5 Programmierung ... 109
12.5.6 Technische Daten ... 110

Handbuch MobileKey

1 Einleitung

MobileKey ist eine unabhängige Produktkategorie für kleine Schließanlagen. Es werden bis zu 100 Schlüssel *(Transponder)* und 20 Schlösser *(Schließzylinder und SmartRelais)* unterstützt.

HINWEIS Die Verwaltung des Schließplans erfolgt ausschließlich über die MobileKey-Web-App. Diese ist über www.my-mobilekey.com erreichbar. Über einen Klick auf "Login Web-App" gelangen Sie direkt zur Anwendung. Erstellen Sie sich hier ein kostenfreies Benutzerkonto, um mit MobileKey zu arbeiten.

1.1 Sicherheitshinweise

⚠ VORSICHT Durch fehlerhaft installierte oder programmierte SimonsVoss-Komponenten kann der Zugang durch eine Tür versperrt werden. Für die Folgen fehlerhafter Installationen, wie nicht möglicher Zugang zu verletzten Personen, Sachschäden oder andere Schäden, haftet die SimonsVoss Technologies GmbH nicht.

HINWEIS Für Beschädigungen der Türen oder der Komponenten durch fehlerhafte Montage übernimmt die SimonsVoss Technologies GmbH keine Haftung.

HINWEIS Die SimonsVoss-Komponenten dürfen nur für den vorgesehenen Zweck, das Öffnen und Schließen von Türen genutzt werden. Ein anderer Gebrauch ist nicht zulässig.

HINWEIS Änderungen bzw. technische Weiterentwicklungen können nicht ausgeschlossen sowie ohne Vorankündigung umgesetzt werden.

HINWEIS Alle Möglichkeiten der Online-Erweiterung setzen ein ordnungsgemäß konfiguriertes MobileKey-Funknetzwerk voraus. Alle Online-Funktionen können nur ausgeführt werden, solange eine stabile Internetverbindung und Stromversorgung gewährleistet ist.

1.2 Systemvoraussetzungen

1.2.1 Verwaltung der Schließanlage

Der Schließplan kann mit jedem üblichen Standardbrowser plattformunabhängig **angezeigt und bearbeitet** werden. Grundsätzlich ist keine spezielle Hardware nötig, jedoch sollte das Endgerät einen der folgenden Web-Browser in einer aktuellen Version unterstützen:

– Microsoft Internet Explorer

- Mozilla Firefox
- Google Chrome
- Apple Safari
- Opera

Außerdem muss jederzeit eine Internetverbindung bestehen. Für flüssiges Arbeiten wird ein HighSpeed-Internetzugang vorausgesetzt.

1.2.2 Programmierung

Die MobileKey-Schließkomponenten können mit Hilfe des USB-Programmiersticks über folgende Geräte programmiert werden:

- **Windows-Gerät**
  - Betriebssystem: Windows 7, 8 oder 10.
  - Hardware: USB-Schnittstelle zum Anschluss des USB-Programmiersticks.

    Für die Programmierung werden keine besonderen Hardwarekonfigurationen vorausgesetzt. Das Betriebssystem muss stabil und fehlerfrei laufen.
  - Auf dem Computer muss das aktuelle .NET Framework (mindestens Version 3.5) von Microsoft installiert sein.

  Folgen Sie den Anweisungen zur Installation der Programmier-App, um die MobileKey-Schließkomponenten zu programmieren.

- **Android-Gerät**
  - Für die Verwendung muss die MobileKey-App aus dem Google-Play-Store installiert werden.

    Änderungen am Schließplan werden weiterhin über den Browser in der MobileKey Web-App durchgeführt.
  - Der USB-Programmierstick kann je nach Anschlussmöglichkeit direkt oder ggf. über ein separat erhältliches OTG-Kabel am Android-Gerät angeschlossen werden.

    Das Android-Gerät muss in diesem Fall die OTG-Funktion unterstützen. Falls Sie sich über die OTG-Unterstützung ihres Android-Geräts nicht sicher sind, können Sie diese Funktion durch entsprechende Apps in Google Play prüfen lassen. Suchen Sie beispielsweise nach "OTG check".

    Achtung: Diese Apps haben nichts mit der SimonsVoss Technologies GmbH zu tun. Für eventuelle Schäden oder auftretende Problemen wird somit keine Haftung übernommen!

  Starten Sie die MobileKey-App über die MobileKey Web-App, um die MobileKey-Schließkomponenten zu programmieren.

- **macOS-Gerät**

Handbuch MobileKey

- Betriebssystem: OS X ab 10.11 "El Capitan"
- Hardware: USB-Schnittstelle zum Anschluss des USB-Programmiersticks.

  Für die Programmierung werden keine besonderen Hardwarekonfigurationen vorausgesetzt. Das Betriebssystem muss stabil und fehlerfrei laufen.

- **Optional: Online über SmartBridge**

  Schlösser können auch online ohne USB-Programmierstick programmiert werden. Siehe Programmieren von Komponenten [▸ 22]. *In diesem Fall müssen nur noch die Transponder mit Hilfe des USB-Programmiersticks programmiert werden.*

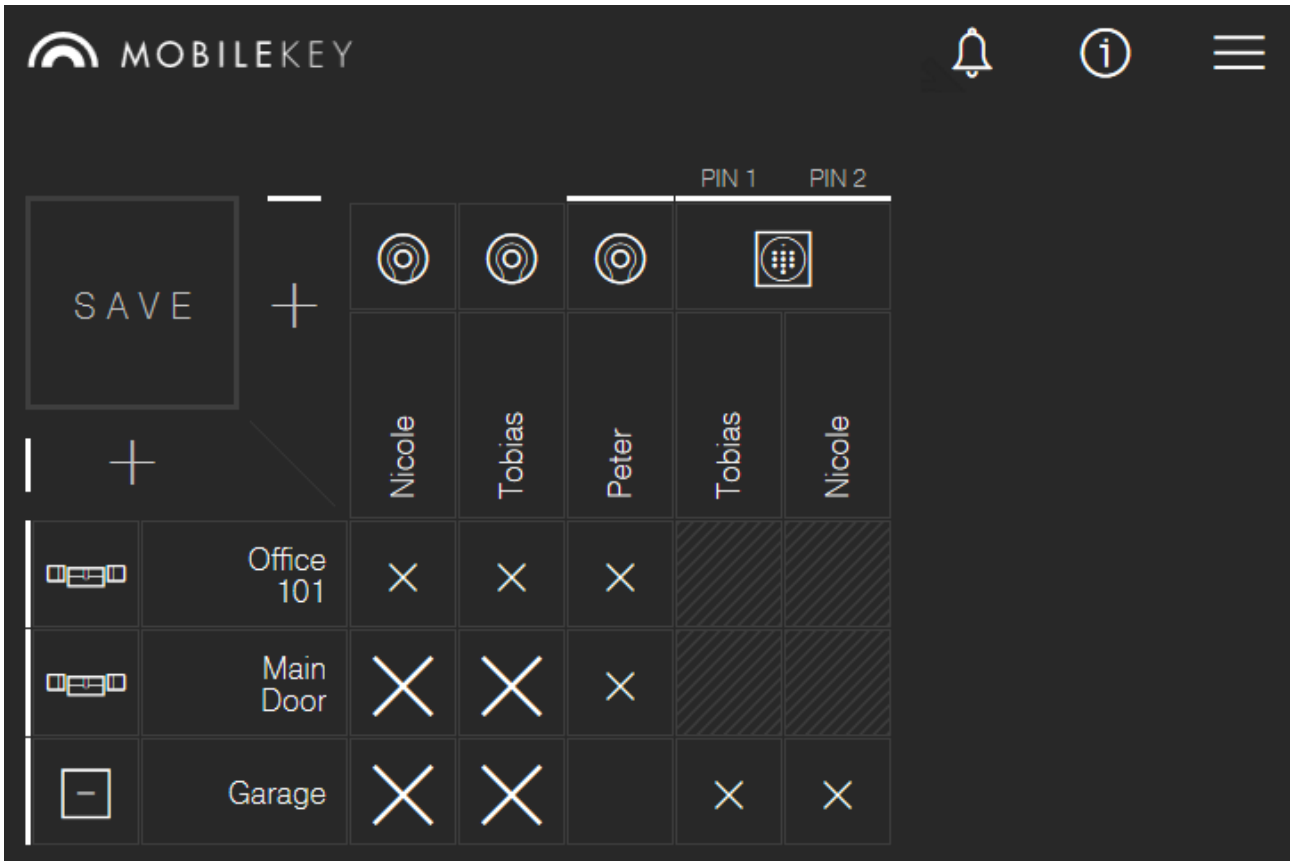
  Tipp:

  Sollte während des Betriebs kein Windows- oder Android-Gerät für die Programmierung neuer Schlüssel zur Verfügung stehen empfiehlt es sich, vorab weitere Transponder als Reserve zu programmieren. Diese können dann zu einem späteren Zeitpunkt den vernetzten Online-Schlössern zugewiesen werden. Siehe hierfür Verwendung von Schlüsseln ohne USB-Programmierstick [▸ 41].

Handbuch MobileKey

2 Die Matrix

Die Matrix stellt die gesamte Schließanlage übersichtlich dar. Somit ist diese Ansicht der Mittelpunkt aller Funktionen. Horizontal werden alle Schlüssel (z.B. Transponder) und vertikal alle Schlösser (z.B. Schließzylinder) dargestellt. Wichtige Menüs sind über die Symbole "Nachrichten-Center", "Hilfe" und "Menü" aufrufbar.



Um die Matrix so übersichtlich wie möglich zu halten, werden verschiedene Symbole eingesetzt.

Berechtigungen

SYMBOL	BESCHREIBUNG
×	**Berechtigungskreuz: Neu** Die Berechtigung wurde gesetzt; allerdings noch nicht programmiert.
×	**Berechtigungskreuz: Gesetzt** Die Berechtigung wurde gesetzt und ist aktiv.

Handbuch MobileKey

	Berechtigungskreuz: Entfernen Die Berechtigung wurde entfernt; allerdings noch nicht ausprogrammiert.
	Berechtigungskreuz: Keine Berechtigung Wenn im Feld keines der drei vorherigen Kreuze angezeigt wird, gibt es an dieser Stelle (noch) keine Berechtigung.

Schlösser & Schlüssel

SYMBOL	BESCHREIBUNG
	Schloss: Schloss Bei dieser Komponente handelt es sich um ein Schloss bzw. einen Schließzylinder. *Ein zusätzliches Funksymbol in der linken, unteren Ecke zeigt an , ob das Schloss über einen LockNode für MobileKey ONLINE verfügt.*
	Schloss: SmartRelais Bei dieser Komponente handelt es sich um ein SmartRelais. *Ein zusätzliches Funksymbol in der linken, unteren Ecke zeigt an , ob das Schloss über einen LockNode für MobileKey ONLINE verfügt.*
	Schlüssel: Transponder Bei dieser Komponente handelt es sich um einen Transponder.
	Schlüssel: PinCode-Tastatur Bei dieser Komponente handelt es sich um eine PinCode-Tastatur.

Sehen Sie dazu auch

- Hilfe zu Online-Schlössern [▸ 35]
- Hilfe zur SmartBridge [▸ 34]

Handbuch MobileKey

3 Grundfunktionen

Bei erstmaliger Anmeldung im MobileKey-Konto erscheint ein Assistent zur einfachen Einrichtung. Dieser Assistent hilft Ihnen dabei, schnell und komfortabel Schlösser und Schlüssel anzulegen.

3.1 Schloss anlegen

✓ Matrixansicht geöffnet

1. Klicken Sie auf das Schloss-hinzufügen-Symbol (Plus unterhalb der "SAVE"-Schaltfläche).
2. Wählen Sie den Schloss-Typ aus, z.B. "ZYLINDER" für einen normalen Schließzylinder.
3. Vergeben Sie einen Namen, z.B. Haustür.
4. Klicken Sie auf die Schaltfläche "Öffnungsdauer in Sekunden" oder "Daueröffnung".
   ⇨ Wenn Sie "Daueröffnung" aktiviert haben, dann bleibt das Schloss solange eingekuppelt, bis es erneut mit einem Schlüssel oder per Fernöffnung betätigt wird.

⚠ VORSICHT

Sicherheitsrisiko durch Daueröffnung

Eine dauerhaft geöffnete Tür kann ein Sicherheitsrisiko darstellen. Die SimonsVoss Technologies GmbH empfiehlt deshalb, die Öffnungsdauer zeitlich zu begrenzen.

5. Klicken Sie auf die Schaltfläche "SPEICHERN" oder "SPEICHERN + KOPIEREN".
   ⇨ "SPEICHERN" speichert das Schloss und navigiert zurück zur Matrixansicht.
   ⇨ "SPEICHERN + KOPIEREN" speichert das Schloss und bereitet gleich ein weiteres Schloss mit den selben Eigenschaften vor.

HINWEIS

Erweiterte Netzwerkeinstellungen werden erst angezeigt, sobald mindestens eine SmartBridge angelegt und konfiguriert wurde. Nach der Erstprogrammierung von DM-Schlössern werden weitere Online-Optionen, z.B. der Wert für "Tür zu lange offen", sichtbar.

HINWEIS

Beim **SmartRelais 2** ist es möglich, den **Ausgang (Relaiskontakt) zu invertieren**. Hierfür muss erst ein SmartRelais angelegt und programmiert werden. Anschließend wird die Einstellung "RELAISKONTAKT KONFIGURIEREN" mit der Option "Ausgang invertieren" in den Eigenschaften des SmartRelais sichtbar. Wenn Sie diese Option aktivieren, muss das SmartRelais 2 nachprogrammiert werden.

3.2 Schlüssel anlegen

✓ Matrixansicht geöffnet

1. Klicken Sie auf das Schlüssel-hinzufügen-Symbol (PLUS neben der "SAVE"-Schaltfläche).
2. Wählen Sie den Schlüssel-Typ aus, z.B. "TRANSPONDER".
3. Vergeben Sie einen Namen, z.B. "Hans Müller".
4. Bestimmten Sie gegebenenfalls die Gültigkeit.
   ⇨ "Gültig von": Ein Datum festlegen, ab dem der Schlüssel in der Schließanlage berechtigt sein soll.
   ⇨ "Gültig bis": Ein Datum festlegen, bis zu dem der Schlüssel in der Schließanlage berechtigt sein soll.
5. Klicken Sie auf die Schaltfläche "SPEICHERN" oder "SPEICHERN + KOPIEREN".
   ⇨ "SPEICHERN" speichert den Schlüssel und navigiert zurück zur Matrixansicht.
   ⇨ "SPEICHERN + KOPIEREN" speichert den Schlüssel und bereitet gleich einen weiteren Schlüssel mit den selben Eigenschaften vor.

⇨ Neuer Schlüssel ist angelegt.

3.3 PinCode-Tastatur anlegen

✓ PinCode-Tastatur bereits konfiguriert; siehe Konfiguration [▸ 75]
(Master-Pin und mindestens eine User-Pin müssen eingerichtet sein!)

✓ Schloss für PinCode-Tastatur angelegt

✓ Matrixansicht geöffnet

1. Klicken Sie auf das Schlüssel-hinzufügen-Symbol (PLUS neben der "SAVE"-Schaltfläche).
2. Typ "PINCOEDE-TASTATUR" auswählen.
3. Schloss festlegen, an welchem die PinCode-Tastatur betrieben wird.
4. Namen für PIN 1 *(entspricht User-Pin 1)* vergeben, z.B. "Hans Müller". Die weiße Checkbox für PIN 1 ist bereits aktiviert.
5. Optional auch noch Namen für PIN 2 & 3 vergeben. Hierfür zuerst die weißen Checkboxen aktivieren, um die PINs zu aktivieren.
6. Klicken Sie auf die Schaltfläche "SPEICHERN" oder "SPEICHERN + KOPIEREN".
   ⇨ "SPEICHERN" speichert den Schlüssel und navigiert zurück zur Matrixansicht.
   ⇨ "SPEICHERN + KOPIEREN" speichert den Schlüssel und bereitet gleich einen weiteren Schlüssel mit den selben Eigenschaften vor.

HINWEIS Bis zu 3 User-Pins können direkt über die PinCode-Tastatur eingerichtet werden. Diese User-Pins müssen in der Web-App bei der Zuweisung der PinCode-Tastatur zu einem Schloss aktiviert werden.

HINWEIS Das Ändern von einzelnen User-Pins einer bereits angelegter Pin-Code Tastatur erfolgt durch Klicken auf die entsprechende Tastatur (in der Matrix) und der Auswahl von "BEARBEITEN".

3.4 Berechtigung vergeben und abspeichern

In der Matrixansicht können Berechtigungen vergeben oder zurückgezogen werden.

- Schlüssel an Schloss berechtigen: Auf das leere Feld im Schnittpunkt von Schlüssel und Schloss klicken, um ein Kreuzchen zu setzen.

  Bis die neue Berechtigung programmiert wurde, ist das Kreuzchen verkleinert dargestellt. Nach dem erfolgreichen Programmieren füllt das Kreuz das komplette Matrix-Quadrat aus.
- Berechtigung eines Schlüssels am Schloss widerrufen: Auf das entsprechende Kreuzchen im Schnittpunkt von Schlüssel und Schloss klicken, um dieses Berechtigungskreuz zu entfernen.

  Bis die neue Änderung programmiert wurde, ist das Kreuz unvollständig dargestellt. Erst nach dem erfolgreichen Programmieren ist das Berechtigungskreuz komplett verschwunden.

HINWEIS Änderungen werden mit gelben Umrandungen angezeigt. Diese müssen vor dem Programmieren unbedingt über die Schaltfläche "SAVE" gespeichert (bzw. übernommen) werden!

HINWEIS Alle Änderungen und Berechtigungen der Komponenten müssen programmiert werden, bevor sie tatsächlich in Kraft treten.

3.5 Zeitplan vergeben

Diese Zusatzfunktion ist optional. Sie müssen diese also nicht zwingend nutzen.

Es gibt grundsätzlich zwei Typen von Zeitplänen:

- Wochenplan: Für jeden Wochentag können individuelle Zeitintervalle vergeben werden. BEISPIEL: Der Haushälterin wird nur an bestimmten Tagen zu gewissen Zeiten Zugang gewährt – z.B. Montag 08:00 bis 12:00 Uhr und Donnerstag 13:00 bis 15:30 Uhr.
- Tagesplan: Ein Zeitzonenplan kann pauschal für eine komplette Woche angelegt werden. BEISPIEL: Mitarbeiter John Dorian ist von Mo. bis Fr. von 07:00 bis 19:00 Uhr an den Schlössern berechtigt.

Gehen Sie wie folgt vor, um einem Schlüssel einen Zeitplan zuzuweisen:

✓ Matrixansicht geöffnet

1. Klicken Sie auf den gewünschten Schlüssel in der Matrixansicht.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "ZEITPLAN".
3. Wählen Sie den Typ des Zeitplans aus.
   ⇨ Wochenplan: Tag auswählen und "Zeitintervall anlegen". Es können mehrere Zeitintervalle an verschiedenen Tagen angelegt werden.
   ⇨ Tagesplan: "Wochenende ausnehmen" anklicken, falls der Plan nur von Montag bis Freitag gelten soll. Anschließend ein "Zeitintervall anlegen". Es können mehrere Zeitintervalle angelegt werden.
4. Klicken Sie auf die Schaltfläche "SPEICHERN".
   ⇨ Schlüssel wird gespeichert.
   ⇨ Matrixansicht wird angezeigt.

⇨ Schlüssel ist Zeitplan zugeordnet.

HINWEIS Überschreitet ein Zeitintervall Mitternacht, müssen zwei Zeitintervalle angelegt werden: Ein Zeitintervall von "Zeit vor Mitternacht bis Mitternacht" und "Mitternacht bis Zeit nach Mitternacht".

3.6 Programmieren von Komponenten

HINWEIS Es wird dringend empfohlen, jedes Schloss vor dem Einbau in die Tür zu programmieren!

Gehen Sie folgendermaßen vor, um die Programmier-App aus der MobileKey-Web-App zu starten und somit die einzelnen Programmieraufgaben durchzuführen:

✓ Programmieraufgaben vorhanden (in Matrix an entsprechenden Komponenten gezeigt)

1. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
   ⇨ Programmier-App startet.
3. Melden Sie sich gegebenenfalls an.
   ⇨ Aufgabenliste zeigt Komponenten mit Programmierbedarf.
4. Führen Sie alle anstehenden Aufgaben durch.
5. Klicken Sie auf die erste Komponente, um deren Programmierung zu starten.
6. Folgen Sie anschließend den Anweisungen der Programmier-App.

Handbuch MobileKey

3.6.1 HINWEIS: Programmieren über ein Windows-Gerät

Die Programmier-App muss einmalig heruntergeladen und installiert werden. Außerdem müssen Benutzername und Passwort eingegeben werden. Für die Programmierung muss der USB-Programmierstick mit dem USB-Anschluss des Computers verbunden sein.

Auf diese Installation wird hingewiesen, sobald Sie auf Menü/ Programmieren klicken. Die dann erscheinende Meldung zeigt Ihnen den direkten Download-Link an. Installieren Sie die Programmier-App. Sie benötigen Administratorrechte, um die Programmier-App zu installieren.

Beachten Sie die Hardwareanforderungen: Programmierung [▸ 6]

Sehen Sie dazu auch

🗎 Programmierung [▸ 6]

3.6.2 HINWEIS: Programmieren über ein Android-Gerät

Laden Sie sich die kostenlose MobileKey-App im Google Play Store herunter und verbinden Sie den Programmierstick mit dem Android-Gerät (ggf. über ein separat erhältliches OTG-Kabel).

Starten Sie die App einmalig, um Ihren Benutzername und das Passwort eingeben zu können.

Beachten Sie die Hardwareanforderungen: Programmierung [▸ 6]

Sehen Sie dazu auch

🗎 Programmierung [▸ 6]

3.6.3 HINWEIS: Programmieren über ein macOS-Gerät

Die Programmierung unter macOS erfordert die einmalige Installation eines Services. Wenn der Service noch nicht installiert oder nicht gestartet ist, dann werden Sie darauf hingewiesen. Sobald der Service läuft, müssen Sie den Browser nicht mehr verlassen. Geräte mit aktivierter Online-Erweiterung müssen nicht programmiert werden. Für die Programmierung der Schlüssel und der Schlösser ohne Online-Erweiterung gibt es unter macOS zwei Möglichkeiten.

Beachten Sie die Hardwareanforderungen: Programmierung [▸ 6]

Programmierung im Menü

Die erste Möglichkeit ist die Programmierung über das Kontextmenü. Diese Methode ist geeignet, wenn wenige Schlüssel oder Schlösser geändert wurden.

1. Klicken Sie auf die Komponente, die programmiert werden soll.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
   ⇨ Programmierfenster öffnet sich.
3. Folgen Sie den Bildschirmanweisungen.

⇨ Programmierung ist abgeschlossen.

Programmierung mit Programmierliste

Die zweite Möglichkeit ist die Programmierung über die Programmierliste. Diese Methode ist geeignet, wenn viele Schlüssel oder Schlösser in der Matrix geändert wurden.

✓ Matrixansicht geöffnet

1. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
   ⇨ Programmierliste öffnet sich.
3. Klicken Sie auf eine Komponente in der Liste, die programmiert werden soll.
4. Folgen Sie den Bildschirmanweisungen.
   ⇨ Komponente wird programmiert.
5. Klicken Sie ggfs. auf die nächste Komponente in der Liste, um sie zu programmieren.

⇨ Programmierung ist abgeschlossen.

3.7 Zurücksetzen von Komponenten

Komponenten können leicht zurückgesetzt werden. Anschließend befinden sich diese im unprogrammierten Auslieferungszustand und können in einem anderen Schließsystem verwendet werden.

1. Klicken Sie die entsprechende Komponente an .
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "LÖSCHEN".
3. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
   ⇨ Programmier-App startet.
4. Führen Sie alle Aufgaben aus.
   ⇨ Komponente ist nach erfolgreicher Programmierung auch aus Schließplan gelöscht.

3.8 Erzwungenes Löschen von Komponenten

Kann eine defekte Komponente nicht problemlos zurückgesetzt werden (siehe Zurücksetzen von Komponenten [▶ 15]) ist es dennoch möglich, diese aus dem Schließplan zu löschen. Ein erneutes Löschen der Komponente führt zu einer erzwungenen Löschung der Komponente.

✓ Komponente bereits gelöscht.

✓ Komponente zuvor programmiert.

1. Klicken Sie die Komponente erneut an.

2. Klicken Sie auf "LÖSCHEN ERZWINGEN" und bestätigen Sie die Eingabe.

HINWEIS Das erzwungene Löschen macht eine (noch) programmierte Komponente für den weiteren Einsatz unbrauchbar. Dieses Vorgehen darf nur bei defekten Komponenten durchgeführt werden!

3.9 Zutrittsprotokoll auslesen

Jeder Zutritt mit einen Schlüssel wird im Schloss protokolliert. Gehen Sie wie folgt vor, um das Zutrittsprotokoll anzuzeigen:

✓ Matrixansicht geöffnet

1. Klicken Sie auf das gewünschte, bereits programmierte Schloss, dessen Protokoll sie auslesen wollen.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "ZUTRITTSPROTOKOLL".
3. Ändern Sie bei Bedarf den Zeitraum des Zutrittsprotokolls.
4. Klicken Sie auf die Schaltfläche "PROTOKOLL AUSLESEN".
   ⇨ Der Befehl "Zutrittsprotokoll auslesen" wird als Aufgabe an die Programmier-App gesendet.
5. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
6. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
   ⇨ Programmier-App startet.
7. Führen Sie die Programmieraufgabe durch.
8. Schließen Sie die Programmier-App.
9. Öffnen Sie die Matrix.
10. Klicken Sie auf das Schloss, dessen Protokoll Sie auslesen wollen.
    ⇨ Menü öffnet sich.
11. Klicken Sie auf die Schaltfläche ZUTRITTSPROTOKOLL.

⇨ Zutrittsprotokoll wird angezeigt.

4 MobileKey ONLINE-Erweiterung

Über eine SmartBridge (welche als Accesspoint dient) können Schlösser vernetzt werden, um direkt mit der Web-App zu kommunizieren. Damit ergeben sich unter anderem einige neue Funktionen:

- Das Programmieren von Schlössern kann plattformunabhängig durchgeführt werden.
- Die Zustände der Tür (offen, geschlossen, verriegelt) können in Echtzeit verfolgt werden.
- Die Zutrittslisten der Schlösser können prinzipiell von überall auf der Welt ausgelesen werden.
- Schlüssel können über Key4Friends mit Freunden geteilt werden.
- Über die Web-App können Fernöffnungen durchgeführt werden.

Für die Nutzung dieser Funktionen sind spezielle Komponenten erforderlich:

- SmartBridge: Als Accesspoint ist sie dauerhaft mit dem Internet verbunden.
- Onlinefähiges Schloss: Alle MobileKey-Schlösser können mit einem speziellen Netzwerkknoten *(SmartRelais mit entsprechender Platine*) ausgerüstet werden, um die Onlinefunktionalität nachzurüsten. Hier spricht man von so genannten LockNodes. Schlösser mit "DoorMonitoring-Konfiguration" verfügen darüber hinaus über eine ausgeklügelte Sensorik. Diese Schlösser können die Türzustände (offen, geschlossen, verriegelt) feststellen und der Web-App mitteilen.

4.1 SmartBridges

Mindestens eine SmartBridge muss als Accesspoint betrieben werden. Diese ist an das Internet angeschlossen und garantiert somit die Verbindung zu Server und Web-App.

HINWEIS Erweiterte Netzwerkeinstellungen *(z.B. beim Anlegen eines Schlosses)* werden erst angezeigt, sobald mindestens eine SmartBridge angelegt wurde.

HINWEIS Beachten Sie, dass mit MobileKey maximal 10 SmartBridges eingesetzt werden können.

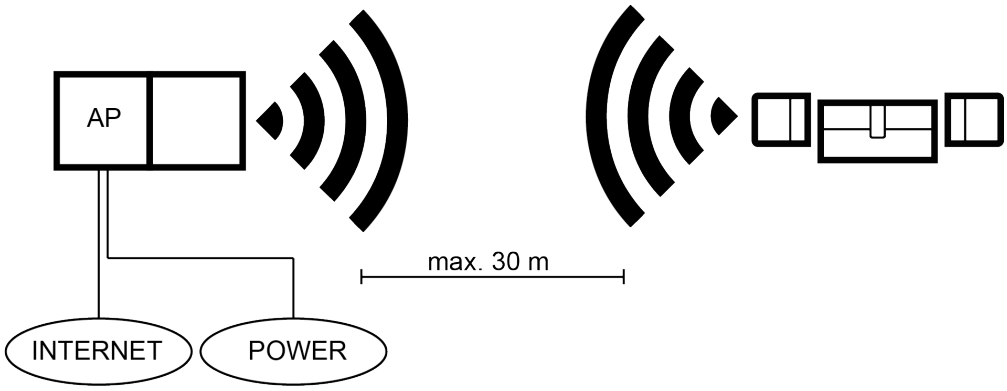
4.1.1 SmartBridges aufstellen

SmartBridges können je nach Einsatz und Konfiguration auf unterschiedliche Weise betrieben werden. Im Folgenden werden die wichtigsten Szenarien gezeigt.

Handbuch MobileKey

4.1.1.1 Eine SmartBridge

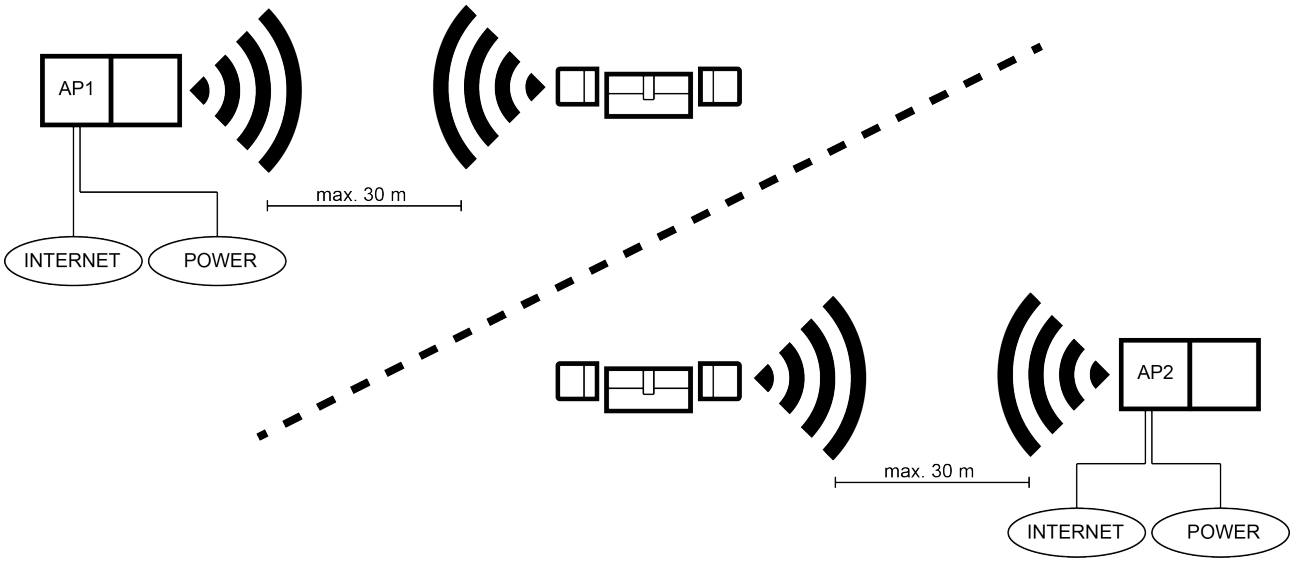
Der Einsatz einer als Accesspoint konfigurierten SmartBridge ist der einfachste Anwendungsfall für MobileKey ONLINE.



4.1.1.2 Zwei oder mehrere SmartBridges

MobileKey ONLINE kann mehrere Accesspoints verwalten. Auf diese Weise können mehrere Standorte oder sehr weit entfernte Schlösser mit dem MobileKey ONLINE Netzwerk abgedeckt werden.

Welches Schloss von welchem Accesspoint angesprochen wird, wird von MobileKey ONLINE automatisch durch Berücksichtigung der Signalstärke bestimmt. Den Weg der Kommunikation können Sie im Menü "NETZWERK" nachverfolgen, indem Sie die Option "Zeige zugewiesene SmartBridge" aktivieren.



4.1.2 SmartBridges einrichten

So fügen Sie in der Web-App eine neue SmartBridge hinzu:

1. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "NETZWERK".
3. Fügen Sie eine neue SmartBridge über das PLUS-Symbol bei SmartBridges hinzu.
   ⇨ Dialog zum Hinzufügen einer neuen SmartBridge startet
4. Wählen Sie einen Typ aus.
   ⇨ Wählen Sie "STANDARD", um eine SmartBridge als Accesspoint zu konfigurieren.
5. Vergeben Sie einen Namen.
   ⇨ Geben Sie einen eindeutigen Namen ein, z.B. "SmartBridge Büro 2"
6. Geben Sie die MobileKey-ID ein.
   ⇨ Die MobileKey-ID finden Sie auf der Verpackung oder auf der Rückseite der SmartBridge.
7. Klicken Sie auf die Schaltfläche "SPEICHERN".
   ⇨ Konfiguration wird gespeichert. Sie gelangen automatisch ins Menü "NETZWERK" zurück.

4.1.3 SmartBridges löschen

HINWEIS

Die LockNodes der Schlösser können nur über die verbundene SmartBridge zurückgesetzt werden. Wenn Sie die SmartBridge löschen, werden alle verbundenen LockNodes automatisch zurückgesetzt. Sofern die Schlösser nicht zum Löschen vorgemerkt sind, behalten diese die jeweilige Konfiguration. Allerdings sind die Schlösser danach nur über eine neue SmartBridge oder über das Programmiergerät erreichbar.

So löschen Sie Ihre SmartBridge in der Web-App:

✓ Verbundene Schlösser weisen Status "ONLINE" auf

1. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "NETZWERK".
3. Klicken Sie auf die zu löschende SmartBridge.
4. Klicken Sie auf die Schaltfläche "LÖSCHEN".
   ⇨ Die SmartBridge wird zum Löschen vorgemerkt.
5. Starten Sie die Netzwerkkonfiguration über die Schaltfläche "KONFIGURATION STARTEN".
6. Der Programmiervorgang (in diesem Fall das Zurücksetzen der SmartBridge und aller verbundenen LockNodes) wird ausgeführt. SmartBridge und LockNodes können anschließend in jeder MobileKey-Schließanlage neu eingebunden werden.

4.2 Schloss mit Netzwerkknoten (LockNode) einrichten

HINWEIS

Bereits eingebaute und programmierte Schlösser ohne Online-Funktion können auch nachträglich in MobileKey ONLINE eingebunden werden. Hierfür muss lediglich die Knaufkappe *(Innenknaufknappe bei FD-, Außenknaufkappe bei CO-Schlössern oder Zusatzplatine bei SmartRelais)* durch eine Online-Knaufkappe mit LockNode ausgetauscht werden. Anschließend kann dem Schloss in der Web-App die Chip-ID des neuen LockNodes hinzugefügt werden.

So fügen Sie ein neues Online-Schloss hinzu:

✓ SmartBridge angelegt *(Siehe* SmartBridges einrichten [▸ 18]*)*

✓ Matrixansicht geöffnet

1. Klicken Sie auf das Schloss-hinzufügen-Symbol (Plus unterhalb der "SAVE"-Schaltfläche).
2. Wählen Sie den Schloss-Typ aus, z.B. "ZYLINDER" für einen normalen Schließzylinder.
3. Vergeben Sie einen Namen, z.B. Haustür.

⚠ VORSICHT

Sicherheitsrisiko durch Daueröffnung

Eine dauerhaft geöffnete Tür kann ein Sicherheitsrisiko darstellen. Die SimonsVoss Technologies GmbH empfiehlt deshalb, die Öffnungsdauer zeitlich zu begrenzen.

4. Klicken Sie auf die Schaltfläche "Öffnungsdauer in Sekunden" oder "Daueröffnung".
   ⇨ Wenn Sie "Daueröffnung" aktiviert haben, dann bleibt das Schloss solange eingekuppelt, bis es erneut mit einem Schlüssel oder per Fernöffnung betätigt wird.
5. Tragen Sie Chip-ID ein (auf der Verpackung und auf der Innenseite der Knaufkappe abgedruckt).

HINWEIS

Geringere Batterielaufzeit

Mit Aktivieren von Schnellere Kommunikation/Fast Wake-Up prüft die Schließung häufiger, ob eine Aktion durchgeführt werden soll. Das verkürzt die Reaktionszeit, führt aber auch zu einer bis zu 30% kürzeren Batterielaufzeit.

6. Aktivieren Sie optional Schnellere Kommunikation/Fast Wake-Up.
7. Klicken Sie auf die Schaltfläche "SPEICHERN" oder "SPEICHERN + KOPIEREN".
   ⇨ "SPEICHERN" speichert das Schloss und navigiert zurück zur Matrixansicht.

⇨ "SPEICHERN + KOPIEREN" speichert das Schloss und bereitet gleich ein weiteres Schloss mit den selben Eigenschaften vor.

⇨ Schloss mit Online-Funktion (LockNode) erstellt.

4.3 Schloss mit Netzwerkknoten (LockNode) löschen

So löschen Sie ein bestehendes Online-Schloss über die SmartBridge:

✓ SmartBridge angelegt *(Siehe* SmartBridges einrichten [▶ 18]*)*

✓ Netzwerk eingerichtet und funktionsfähig

✓ Online-Status des zu löschenden Schlosses "ONLINE"

1. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "NETZWERK".
3. Klicken Sie im Menü "NETZWERK" auf das zu löschende Schloss.
4. Klicken Sie auf die Schaltfläche "LÖSCHEN".
   ⇨ Das Schloss wird zum Löschen vorgemerkt.
5. Starten Sie die Netzwerkkonfiguration über die Schaltfläche "KONFIGURATION STARTEN".
   ⇨ Programmiervorgang *(in diesem Fall das Zurücksetzen)* wird ausgeführt.
   ⇨ Schloss kann anschließend in jeder MobileKey-Schließanlage neu eingebunden werden.

⇨ Schloss ist gelöscht.

4.4 Online-Komponenten konfigurieren

✓ Mindestens eine angelegte SmartBridge

✓ SmartBridge mit Internet verbunden und betriebsbereit

✓ Mindestens ein Schloss mit Online-Chip-ID angelegt

✓ Distanz zwischen SmartBridge und Schlössern weniger als 30 m. *Alle Komponenten sollten sich zu jeder Zeit innerhalb des Funkbereiches der SmartBridge befinden!*

1. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "NETZWERK".
3. Klicken Sie auf die Schaltfläche "KONFIGURATION STARTEN".
   ⇨ Die Konfiguration des MobileKey-Netzwerks läuft komplett automatisch ab.

⇨ Am Ende der Konfiguration müssen die Status von SmartBridges und Schlössern auf "ONLINE" stehen.

Führen Sie folgende Checkliste durch, falls die automatische Konfiguration nicht erfolgreich war: Hilfe zu Online-Schlössern [▸ 35].

4.5 Programmieren von Komponenten

Das Programmieren von Online-Schlössern ist auch über die SmartBridge möglich. Schlüssel bzw. Transponder müssen über den USB-Programmierstick programmiert werden, da diese keinen Netzwerkknoten (LockNode) besitzen.

HINWEIS Es wird dringend empfohlen, jedes Schloss vor dem Einbau in die Tür zu programmieren!

HINWEIS Bei jeder Neuprogrammierung wird die im Schloss gespeicherte Zutrittsliste zurückgesetzt. Nur die bereits ausgelesenen Zutritte in der Web-App bleiben erhalten.

So führen Sie eine Programmierung über die SmartBridge durch:

✓ Chip-ID des Schlosses beim Anlegen des Schlosses angegeben

✓ Netzwerk erfolgreich konfiguriert

✓ Matrixansicht geöffnet

1. Legen Sie eine Komponente an.
2. Vergeben Sie gegebenenfalls Berechtigungen.
3. Klicken Sie auf "SAVE".
   - ⇨ Programmiervorgang startet automatisch über die SmartBridge.
   - ⇨ Während Programmiervorgang wird Wartungssymbol in Matrix gezeigt.

Die vollständige Programmierung des Schlosses wird über einen schnellen, sich 3-mal wiederholenden Ton signalisiert. *(Piep-Piep-Piep)*

4.6 Verbindung zu Online-Komponenten trennen

Online-Komponenten können bei Bedarf wieder aus dem System entfernet werden. Ein mechanisches Entfernen der Komponenten (z.B. durch Entfernen aus dem Funkbereich von MobileKey) hat entsprechende Warnmeldungen zur Folge. Melden Sie deswegen die entsprechenden Komponenten immer ordnungsgemäß aus dem System ab. Durch den Abmeldevorgang wird der LockNode zurückgesetzt. Das Schloss behält seine Konfiguration und ist anschließend bis zu einer neuen Online-Einrichtung nur noch über den USB-Programmierstick erreichbar.

✓ Mindestens ein Online-Schloss/SmartBridge angelegt

1. Klicken Sie auf die Menü-Schaltfläche.
   - ⇨ Menü öffnet sich.

2. Klicken Sie auf die Schaltfläche "NETZWERK".
3. Klicken Sie auf das zu trennende Schloss.
   ⇨ Menü öffnet sich.
4. Klicken Sie im Menü auf die Schaltfläche "VERBINDUNG TRENNEN".
5. Starten Sie die Onlinekonfiguration über die Schaltfläche "KONFIGURATION STARTEN".

Sehen Sie dazu auch

🗎 Hilfe zu Online-Schlössern [▸ 35]

4.7 Fernöffnung durchführen

✓ Schließanlage ordnungsgemäß konfiguriert
✓ Accesspoint mit Internet verbunden
✓ Schloss besitzt LockNode
✓ Schloss ordnungsgemäß konfiguriert
✓ Matrixansicht geöffnet

1. Klicken Sie auf die Schließung, die sie aus der Ferne öffnen wollen.
2. Klicken Sie auf "ÖFFNEN".
   ⇨ Der Befehl wird direkt über die SmartBridge zum Schloss geschickt. Natürlich kann auf diese Weise auch eine Tür verriegelt werden.

⇨ Schloss wird geöffnet/geschlossen.

4.8 Key4Friends

Key4Friends ermöglicht das Teilen von Schlüsseln über Smartphones. Schlüssel können so einfach mit Freunden geteilt werden.

Ihr Freund bekommt eine E-Mail, die ihn über Ihren geteilten Schlüssel informiert. In der E-Mail ist genau beschrieben, wie dieser geteilte Schlüssel mit Hilfe der kostenlosen Key4Friends-App verwendet werden kann.

Ihr Freund installiert die Key4Friends-App und registriert sich schnell und kostenlos mit E-Mail-Adresse und Telefonnummer. Nur durch diese eindeutige Kombination kann sichergestellt werden, dass Ihr Schlüssel auch ausschließlich vom Telefon Ihres Freundes verwendet werden kann.

4.8.1 Schlüssel teilen

✓ Schließanlage ordnungsgemäß konfiguriert
✓ Accesspoint mit Internet verbunden und online
✓ Matrixansicht geöffnet

1. Klicken Sie auf das Schloss, dessen Schlüssel Sie teilen wollen.

⇨ Menü öffnet sich.

2. Klicken Sie auf die Schaltfläche "KEY4FRIENDS ANLEGEN".
3. Füllen Sie die Werte nach Belieben aus.
4. Ergänzen Sie die Angaben zum Empfänger.
5. Schränken Sie die Gültigkeit des Schlüssels ein.
6. Klicken Sie auf die Schaltfläche "SENDEN".

⇨ Ihr Freund erhält umgehend eine E-Mail. In der E-Mail ist genau beschrieben, wie er den Schlüssel verwenden kann.

Alle Einstellungen und Angaben der geteilten Schlüssel können jederzeit geändert oder widerufen werden, siehe Schlüssel verwalten [▸ 24].

HINWEIS Beachten Sie, dass das Zeitfenster von geteilten Schlüsseln auf 3 Wochen limitiert ist! *Benutzen Sie Transponder oder eine PinCode-Tastatur, um Freunden dauerhaften Zutritt zu gewähren.*

4.8.2 Schlüssel verwalten

1. Klicken Sie auf die Menü-Schaltfläche.

   ⇨ Menü öffnet sich.

2. Klicken Sie auf die Schaltfläche "KEY4FRIENDS VERWALTEN".

   ⇨ Im Typ "Aktiv" sehen Sie alle aktuell geteilten Schlüssel.

   ⇨ Im Typ "Alle" sehen Sie auch alle zur Zeit nicht geteilten Schlüssel.

Jeder geteilte Schlüssel kann durch Anklicken bearbeitet bzw. widerrufen werden.

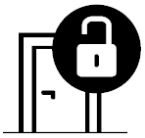
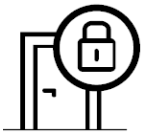
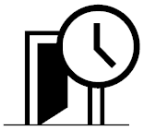
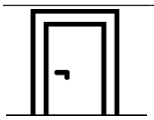
4.9 DoorMonitoring Schloss - Angezeigte Schlosszustände

Schlösser mit DoorMonitoring-Option teilen mithilfe einer speziellen Stulpschraube die Zustände der Tür mit. Diese Schlösser sind von Haus aus für MobileKey ONLINE ausgelegt - verfügen also bereits serienmäßig über einen sogenannten LockNode.

Folgende Türzustände des DoorMonitoring-Schlosses werden (teilweise kombiniert) über ein entsprechendes Icon in der Matrix der Web-App angezeigt:

SYMBOL	BESCHREIBUNG
	Tür offen.

Handbuch MobileKey

	Tür geschlossen, aber nicht verriegelt.
	Tür sicher geschlossen und Schloss verriegelt.
	Tür zu lange geöffnet. *Die Zeit kann nach der Erstprogrammierung des DM-Schlosses in den Schlosseinstellungen vorgenommen werden.*
	Tür geschlossen. Verriegelungszustand nicht überwacht.

Zusätzlich zu den herkömmlichen Warnungen *(siehe* Die Matrix [▸ 8]*)* können beim DoorMonitoring-Schloss weitere Warnungen angezeigt werden:

SYMBOL	BESCHREIBUNG
	Einbruch An der Tür wurde ein Einbruchsversuch gemeldet. Möglicherweise wurde der Versuch unternommen, die Tür gewaltsam aufzubrechen.
	Magnetmanipulation Jemand hat sich an der Tür, bzw. am Magnetplättchen zu schaffen gemacht.
	Schraubenmanipulation Jemand hat sich an der Tür, bzw. der Stulpschraube zu schaffen gemacht.
	Hardwarefehler In selten Fällen kann es zu Problemen an der Sensorik kommen. Wenden Sie sich an Ihren Fachhändler oder direkt an die SimonsVoss Technologies GmbH (siehe Hilfe & Kontakt [▸ 40]), um weitere Hilfe zu erhalten. Wahrscheinlich muss Ihre Hardware ausgetauscht werden.

Handbuch MobileKey

HINWEIS

Wenn ein Einbruch oder eine bewusste Manipulation des DoorMonitoring-Schlosses erkannt wird, muss die entsprechende Tür sofort gründlich geprüft werden. Achten Sie auf Schäden an der Tür und dem Schloss. Anschließend muss das Schloss zurückgesetzt werden! *Siehe* Programmieren von Komponenten [▸ 22]

⚠ VORSICHT

Riegel nicht überwacht

Wenn der FlipFlop-Modus eingestellt ist, dann wird der Zustand des Riegels nicht überwacht!

a) Verzichten Sie auf den FlipFlop-Modus, wenn Sie den Riegel ebenfalls überwachen wollen.

HINWEIS

Bei jeder Neuprogrammierung wird die im Schloss gespeicherte Zutrittsliste zurückgesetzt. Nur die bereits ausgelesenen Zutritte in der Web-App bleiben erhalten.

HINWEIS

Bitte beachten Sie, dass Ihr MobileKey-Netzwerk erfolgreich konfiguriert sein muss! Die Status von Smartbridge und DoorMonitoring-Schloss müssen beide stets "ONLINE" sein. *Siehe* Hilfe zu Online-Schlössern [▸ 35] *für weitere Hilfe.*

Sehen Sie dazu auch

- Hilfe zu Online-Schlössern [▸ 35]
- Programmieren von Komponenten [▸ 22]

5 Eventmanagement

Mit Hilfe von individuellen Regeln (Events) können gezielte Benachrichtigungen erzeugt werden. Diese Benachrichtigungen können sowohl an verschiedene E-Mail-Adressen verschickt sowie über Push-Benachrichtigungen direkt auf das Smartphone gesendet werden. Außerdem werden alle Benachrichtigungen unter "MELDUNGEN" der MobileKey-Web-App angezeigt.

5.1 Benachrichtigungen in der Web-App ansehen

Im Menü "MELDUNGEN" in der Matrix (über das -Symbol aufrufbar) werden alle über das Eventmanagement ausgelösten Benachrichtigungen sowie wichtige Hinweise und Warnungen angezeigt.

Das Meldungen-Symbol in der Matrix-Hauptansicht informiert ständig über die neusten Events. Alle Events können gefiltert oder quittiert werden.

5.2 Regeln erstellen

Individuelle Events können in den Einstellungen der Schließanlage erstellt werden.

1. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "EINSTELLUNGEN".
3. Klicken Sie auf die Plus-Schaltfläche unter "EVENTMANAGEMENT".

⇨ Assistent zur Erstellung neuer Regeln öffnet sich.

5.2.1 Regel vom Typ "Zutritt" erstellen

TYP ZUTRITT

AUSLÖSER	BESCHREIBUNG
Fernöffnung	Bei allen Fernöffnungen wird eine Benachrichtigung verschickt.
Key4Friends	Bei einer bzw. allen über Key4Friends ausgelösten Öffnungen wird eine Benachrichtigung verschickt.
Transponder/PINs	Bei einer bzw. allen durch einen Schlüssel (Transponder) oder PIN-Code ausgelösten Öffnung wird eine Benachrichtigung verschickt.

Klicken Sie nach jedem Schritt auf die Schaltfläche "WEITER". Nachdem alle Einstellungen angepasst wurden, können Sie das Event über die Schaltfläche "SPEICHERN" aktivieren.

1. Wählen Sie den Event-Typ "ZUTRITT".
2. Bestimmen Sie die Schlüssel, welche das Event auslösen sollen.

⇨ Deaktivieren Sie den Schieberegler, um die Auswahl der Schlüssel und Key4Friends individuell einzuschränken.

3. Bestimmen Sie, bei welchen Schlössern das Event ausgelöst werden soll.
   ⇨ Deaktivieren Sie den Schieberegler, um die Auswahl der Schlösser individuell einzuschränken.
4. Bestimmen Sie einen Zeitraum, an dem Events ausgelöst werden sollen.
   ⇨ Standardmäßig sind alle Zeiten ausgewählt, damit Events zu jeder Zeit ausgelöst werden können. Sie können die Auswahl nach Belieben einschränken.
5. Geben Sie einen passenden Namen für das Event an.
6. Geben Sie an, wie Sie über die Events benachrichtigt werden wollen.
7. Klicken Sie auf die Schaltfläche "SPEICHERN".

⇨ Event ist aktiviert.

5.2.2 Regel vom Typ "DoorMonitoring" erstellen

TYP DOOR MONITORING

AUSLÖSER	BESCHREIBUNG
Tür auf	Eine Benachrichtigung wird verschickt, sobald die Tür physisch geöffnet wird.
Tür zu	Eine Benachrichtigung wird verschickt, sobald die Tür physisch geschlossen wird.
Tür zu lange offen	Eine Benachrichtigung wird verschickt, sobald die Tür zu lange physisch geöffnet ist.
Tür geschlossen nach zu lange offen	Eine Benachrichtigung wird verschickt, sobald die Tür nach einem zu langen physischen Öffnen wieder geschlossen wird.
Tür entriegelt	Eine Benachrichtigung wird verschickt, sobald die Tür entriegelt wird.
Tür verriegelt	Eine Benachrichtigung wird verschickt, sobald die Tür ordnungsgemäß verriegelt wird.

Klicken Sie nach jedem Schritt auf die Schaltfläche "WEITER". Nachdem alle Einstellungen angepasst wurden, können Sie das Event über die Schaltfläche "SPEICHERN" aktivieren.

1. Wählen Sie den Event-Typ "DOOR MONITORING".
2. Bestimmen Sie die Ereignisse, welche das Event auslösen sollen.
3. Bestimmen Sie, bei welchen DoorMonitoring-Schlössern das Event ausgelöst werden soll.
   ⇨ Deaktivieren Sie den Schieberegler, um die Auswahl der Schlösser individuell einzuschränken.

4. Bestimmen Sie einen Zeitraum, an dem Events ausgelöst werden sollen.
   ⇨ Standardmäßig sind alle Zeiten ausgewählt, damit Events zu jeder Zeit ausgelöst werden können. Sie können die Auswahl nach Belieben einschränken.
5. Geben Sie einen passenden Namen für das Event an.
6. Geben Sie an, wie Sie über die Events benachrichtigt werden wollen.
7. Klicken Sie auf die Schaltfläche "SPEICHERN".

⇨ Event ist aktiviert.

5.2.3 Regel vom Typ "Alarme" erstellen

TYP ALARM

AUSLÖSER	BESCHREIBUNG
Batterie schwach	Eine Benachrichtigung wird verschickt, sobald der Batteriestand in einem Schloss niedrig ist.
Netzwerkfehler	Eine Benachrichtigung wird verschickt, sobald ein Netzwerkfehler auftritt.
Einbruch	Eine Benachrichtigung wird verschickt, sobald ein DoorMonitoring-Schloss einen Einbruchsversuch detektiert.
Hardwarefehler	Eine Benachrichtigung wird verschickt, sobald ein Hardwarefehler erkannt wird.

Klicken Sie nach jedem Schritt auf die Schaltfläche "WEITER". Nachdem alle Einstellungen angepasst wurden, können Sie das Event über die Schaltfläche "SPEICHERN" aktivieren.

1. Wählen Sie den Event-Typ "ALARM".
2. Bestimmen Sie, welche Alarme das Event auslösen sollen.
3. Geben Sie einen passenden Namen für das Event an.
4. Geben Sie an, wie Sie über die Events benachrichtigt werden wollen.
5. Klicken Sie auf die Schaltfläche "SPEICHERN".

⇨ Event ist aktiviert.

5.3 Wichtige Hinweise

HINWEIS

Alle Events werden über die SmartBridge übertragen. Sie erhalten keine Benachrichtigungen über Events, wenn die Internetverbindung gestört oder die Spannungsversorgung unterbrochen wurde. Über den Zeitraum, in dem die SmartBridge nicht ordnungsgemäß online ist, gehen alle auftretenden Events verloren.

Handbuch MobileKey

HINWEIS

Eine Benachrichtigung vom Typ "ALARM" wird in jedem Fall empfohlen. So können Sie dieses Event einrichten: Regel vom Typ "Alarme" erstellen [▸ 29]

HINWEIS

Benachrichtigungen über Events werden nur in Echtzeit gemeldet, wenn die Schlösser mit der SmartBridge vernetzt wurden. Alarme werden allerdings auch bei nicht vernetzten Schlössern erfasst, sobald eine Programmieraufgabe am entsprechenden Schloss durchgeführt wurde. Unter "MELDUNGEN" können alle Events und Alarme angezeigt, gefiltert und quittiert werden.

Sehen Sie dazu auch

🗎 Regel vom Typ "Alarme" erstellen [▸ 29]

6 Hilfestellungen

Im Folgenden werden Hilfestellungen zu möglichen Alltagsproblemen gezeigt.

6.1 Hilfe mit Schlüsseln (Transpondern)

Schlüssel bzw. Transponder können unter Umständen verloren gehen, beschädigt oder gestohlen werden. Alle Szenarien führen dazu, dass der alte Schlüssel im Schließplan gelöscht und ein Ersatzschlüssel angelegt werden muss. Aus Sicherheitsgründen müssen in allen Schlössern die Berechtigungen des gelöschten Schlüssels entfernt werden. Dies erfolgt über eine Neuprogrammierung aller Schlösser.

Über die folgende Vorgehensweise wird ein "nicht mehr vorhandener" bzw. defekter Schlüssel optional durch einen neuen Schlüssel ersetzt.

✓ Matrixansicht geöffnet

1. Suchen Sie den betroffenen Schlüssel im Schließplan.
2. Heben Sie alle Berechtigungen auf.
3. Klicken Sie auf die Schaltfläche "SAVE".
   ⇨ Änderungen sind gespeichert.
4. Klicken Sie den Schlüssel im Schließplan an.
   ⇨ Menü öffnet sich.
5. Klicken Sie auf die Schaltfläche "LÖSCHEN".
   ⇨ Schlüssel wird zum Zurücksetzen vorgemerkt.
   ⇨ Aufgabe wird später in der Programmier-App abgearbeitet.
6. Bei verlorenem, gestohlenem oder defektem Schlüssel: Klicken Sie auf den betroffenen Schlüssel im Schließplan.
   ⇨ Menü öffnet sich.
7. Klicken Sie auf die Schaltfläche "LÖSCHEN ERZWINGEN".
   ⇨ Schlüssel ist im Schließplan gelöscht.
   ⇨ Schlüssel ist noch nicht im Schloss gesperrt.
8. Legen Sie gegebenenfalls einen neuen Schlüssel an.
9. Vergeben Sie gegebenenfalls nötige Berechtigungen.
10. Klicken Sie gegebenenfalls auf die Schaltfläche "SPEICHERN" oder "SPEICHERN + KOPIEREN".
    ⇨ "SPEICHERN" speichert den Schlüssel und navigiert zurück zur Matrixansicht.
    ⇨ "SPEICHERN + KOPIEREN" speichert den Schlüssel und bereitet gleich einen weiteren Schlüssel mit den selben Eigenschaften vor.
11. Klicken Sie auf die Menü-Schaltfläche.
    ⇨ Menü öffnet sich.

12. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
    ⇨ Programmier-App startet.
13. Führen Sie alle Aufgaben durch.
    ⇨ Folgende Programmieraufgaben sind zu erwarten: Berechtigungen des gelöschten Schlüssels in allen Schlössern entfernen und optional einen neuen Schlüssel an den Schlössern berechtigen.

⇨ Programmierung wird durchgeführt.

⚠ VORSICHT

Unberechtigter Zutritt nach Diebstahl

Ein gestohlener Schlüssel ist solange an der Schließanlage berechtigt, bis alle Berechtigungen entfernt und die Schlösser neu programmiert wurden.

a) Programmieren Sie bei Schlüsselverlust sofort alle berechtigten Schlösser neu.

6.2 Hilfe mit Schlössern (z.B. Schließzylinder)

Schlösser bzw. Schließzylinder können unter Umständen einen Defekt erleiden. Wechseln Sie zunächst die Batterien des Schlosses und versuchen Sie, dieses neu zu programmieren. Funktioniert das Schloss immer noch nicht korrekt, muss dieses ausgetauscht werden.

Wird ein Schloss mit anderen Eigenschaften benötigt, kann dieses einfach ausgetauscht werden.

Gehen Sie folgendermaßen vor, um ein Schloss auszutauschen:

✓ Matrixansicht geöffnet

1. Entfernen Sie das betroffene Schloss aus der Tür.
   ⇨ *Es kann unter Umständen schwierig sein, ein Schloss aus einer verschlossenen Tür zu entfernen. Fragen Sie ggf. den Fachhändler, der Ihnen die SimonsVoss-Produkte installiert hat, um Rat.*
2. Klicken Sie im Schließplan auf das betroffene Schloss.
   ⇨ Menü öffnet sich.
3. Klicken Sie auf die Schaltfläche "LÖSCHEN".
   ⇨ Schloss wird zum Zurücksetzen vorgemerkt.
   ⇨ Aufgabe wird später in der Programmier-App abgearbeitet.
4. Bei defektem Schloss: Klicken Sie auf das Schloss.
   ⇨ Menü öffnet sich.
5. Klicken Sie auf die Schaltfläche "LÖSCHEN ERZWINGEN".
   ⇨ Schloss wird im Schließplan unwiderruflich gelöscht.
6. Legen Sie einen neuen Schlüssel an.
7. Vergeben Sie nötige Berechtigungen.

8. Klicken Sie auf die Schaltfläche "SPEICHERN" oder "SPEICHERN + KOPIEREN".
   ⇨ "SPEICHERN" speichert den Schlüssel und navigiert zurück zur Matrixansicht.
   ⇨ "SPEICHERN + KOPIEREN" speichert den Schlüssel und bereitet gleich einen weiteren Schlüssel mit den selben Eigenschaften vor.
9. Legen Sie ein neues Schloss an.
10. Vergeben Sie nötige Berechtigungen.
11. Klicken Sie auf die Schaltfläche "SPEICHERN" oder "SPEICHERN + KOPIEREN".
    ⇨ "SPEICHERN" speichert den Schlüssel und navigiert zurück zur Matrixansicht.
    ⇨ "SPEICHERN + KOPIEREN" speichert den Schlüssel und bereitet gleich einen weiteren Schlüssel mit den selben Eigenschaften vor.
12. Klicken Sie auf die Menü-Schaltfläche.
    ⇨ Menü öffnet sich.
13. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
    ⇨ Programmier-App startet.
14. Führen Sie alle Aufgaben durch.

⇨ Programmierung wird durchgeführt.

6.3 Gelöschte Komponenten zurücksetzen oder wiederverwenden

Sollte eine SimonsVoss-Komponente (z.B. Schlüssel oder Schloss) aus der Schließanlage gelöscht worden sein, ohne diese vorher korrekt zurückzusetzen, kann sie trotzdem weiter genutzt werden:

✓ Matrixansicht geöffnet

1. Legen Sie die entsprechende Komponente (z.B. Schlüssel bzw. Transponder) im Schließplan neu an.
2. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
3. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
   ⇨ Programmier-App startet.
4. Führen Sie alle Aufgaben aus.
   ⇨ Der erste Versuch, die Komponente neu zu programmieren, wird mit einer Fehlermeldung quittiert.
5. Führen Sie die Aufgabe erneut aus.

⇨ Komponente ist jetzt neu programmiert.

Setzten Sie die Komponenten immer korrekt zurück, um dieses Problem zu vermeiden!

6.4 Komponenten auslesen

Sie können alle MobileKey-Komponenten auslesen um nachträglich zu erfahren, wo deren Einsatzzweck ist. Dies kann beispielsweise dann wichtig sein, wenn Sie einen Schlüssel (z.B. Transponder) finden, den Sie keinem Benutzer zuordnen können.

MobileKey-Komponenten können schnell ausgelesen werden:

1. Klicken Sie auf die Menü-Schaltfläche.
   ⇨ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
   ⇨ Programmier-App startet.
3. Klicken Sie auf die Schaltfläche "AUSLESEN".

HINWEIS

Auslesen unter macOS/Android

Anstelle einer Programmier-App öffnet sich die Programmieroberfläche direkt in derselben Anwendung. Die Schaltfläche "AUSLESEN" gibt es nicht. Klicken Sie stattdessen auf die Funksymbol-Schaltfläche.

4. Wählen Sie die Komponente, die Sie auslesen wollen.

⇨ Rückmeldung zeigt z.B. an, welchen Namen der Schlüssel hat (Hans Müller) oder ob es eine unprogrammierte MobileKey-Komponente im Auslieferungszustand ist.

6.5 Hilfe zur SmartBridge

Führen Sie bei einem Problem mit der SmartBridge folgende Checkliste durch, falls die automatische Netzwerk-Konfiguration nicht erfolgreich war:

- **Stromversorgung** überprüfen.
  - Blinkt die LED der SmartBridge?
- Beträgt die **Distanz** zwischen SmartBridge und Schloss mehr als 1,5 m und weniger als ca. 30m?
  - Testen Sie das Setup ggf. bei einer Entfernung von Luftlinie 3 m ohne Hindernisse.
  - Umwelteinflüsse, Mauern/Wände, Gegenstände und viele weitere Faktoren haben erheblichen Einfluss auf die Signalqualität. Die Angabe von bis zu ca. 30 m Netzabdeckung kann nicht garantiert werden.
- **Internetzugang** überprüfen.
  - Ist der Port 8883 der Firewall geöffnet? Fügen Sie ggf. entsprechende Ausnahmen hinzu, um die SmartBridge über die Ports 1883 und 8883 nach außen kommunizieren zu lassen.
  - Ist der DHCP-Server so konfiguriert, dass sich ein Gerät im Netzwerk anmelden kann?

Über einen Windows-PC kann die SmartBridge auch optional mit dem **SimonsVoss OAM-Tool** erreicht werden. Mit Hilfe des OAM-Tools lassen sich erweiterte Einstellungen der SmartBridge, wie beispielsweise die Zuweisung einer festen IP-Adresse oder Einstellungen des integrierten DHCP-Servers einstellen. Das OAM-Tool finden Sie auf der SimonsVoss-Homepage (www.simons-voss.com) im Supportbereich unter Software-Downloads.

HINWEIS

Verwendung fester IP-Adressen

Bei Verwendung einer festen IP-Adresse muss auch ein DNS (Domain Name Service) über das OAM-Tool eingetragen werden.

– Prüfen Sie, ob **Chip-IDs und MobileKey-IDs** korrekt eingegeben wurden.

6.6 Hilfe zu Online-Schlössern

Führen Sie bei **Problemen mit Online-Schlössern** folgende Checkliste durch, falls die automatische Netzwerk-Konfiguration nicht erfolgreich war:

– Prüfen Sie, ob die **Chip-IDs** der Schlösser alle korrekt eingegeben wurden.

– Prüfen Sie den **korrekten Einbau des LockNodes**.

  Nach der korrekten Kontaktierung zwischen LockNode und Schloss müssen 4 kurze Töne zu hören sein!

– Prüfen Sie bei der Nachrüstung oder dem Austausch von LocksNodes die richtige Zuweisung der Schlösser!

6.7 Netzwerkfehler

Netzwerkfehler müssen nicht immer schwerwiegende Probleme bedeuten. Prüfen Sie die Stabilität Ihrer Internetverbindung, wenn innerhalb von 24 Stunden mehrere Netzwerkfehler auftreten.

HINWEIS

Viele handelsübliche Internet-Router beziehen in bestimmten Abständen eine neue IP-Adresse, was eine kurzzeitige Unterbrechung der Internetverbindung zur Folge haben kann. Es wird zu einer Fehlermeldung kommen *(vorwiegend nachts)*, wenn dieser Vorgang länger als 30 Sekunden dauert.

6.8 Manuelles Zurücksetzen der LockNodes

Ein programmiertes Online-Schloss besteht aus zwei getrennt voneinander programmierten Komponenten: Dem Schloss und dem LockNode. Beide Komponenten sind passend aufeinander abgestimmt und können im programmierten Zustand in keiner anderen Schließanlage eingesetzt werden. Setzen Sie den LockNode immer über die WebApp zurück; siehe Verbindung zu Online-Komponenten trennen [▸ 22].

Sollte dieser Schritt nicht möglich sein, kann die Konfiguration des LockNodes nur mit Hilfe eines nicht zur Schließanlage gehörenden Schlosses zurückgesetzt werden. Montieren Sie hierfür temporär den LockNode auf eine unbekannte Schließung. Nach wenigen Sekunden wird das Zurücksetzen des LockNode signalisiert:

– Schließzylinder: Akustisches Signal (4x Beep)
– SmartRelais: Optische Signalisierung durch LED. (Achten Sie auf die korrekte Spannungsversorgung!)

Nach dem Zurücksetzen kann der LockNode wieder mit jeder SmartBridge verbunden werden.

7 Wartung, Reinigung und Desinfektion

⚠

Beschädigung der Oberflächen

Durch Verwendung nicht geeigneter bzw. aggressiver Reinigungs- oder Desinfektionsmittel können MobileKey-Komponenten beschädigt werden.

MobileKey-Komponenten dürfen nicht mit ÖL, Farbe, Fett oder Säure in Verbindung gebracht werden!

Zur Desinfektion dürfen nur Mittel verwendet werden, welche ausdrücklich zur Desinfektion empfindlicher metallischer Oberflächen bzw. Kunststoffe vorgesehen sind.

a) Reinigen Sie MobileKey-Komponenten bei Bedarf mit einem weichen, ggfs. feuchten Tuch.

⚠ **VORSICHT**

Batteriewechsel

Leere Batterien müssen stets durch neue, von SimonsVoss freigegebene, Batterien ersetzt werden. Alte Batterien sind stets fachgerecht zu entsorgen!

Handbuch MobileKey

8 MobileKey Apps

In den App-Stores von iOS und Android ist die MobileKey-App verfügbar, welche folgende Funktionen unterstützt:

- Überblick über Türzustände (bei Verwendung DM-Zylinder).
- Fernöffnungen.
- Versenden von Key4Friends-Berechtigungen.
- Auslesen und Anzeige der Zutrittsliste.
- Empfang von Push-Nachrichten aus dem Eventmanagement.
- Verwendung von Touch-ID für sicherheitsrelevante Aktionen (Fernöffnung, Key4Friends, Push-Nachrichten deaktivieren).
- Programmierung von Schlüsseln und Schlössern über den USB-Programmierstick. *Nur bei Android-Geräten mit OTG-Funktion und zusätzlichem OTG-Kabel verfügbar.*

9 Konformitätserklärung

Dokumente wie Konformitätserklärungen und sonstige Zertifikate sind online unter www.my-mobilekey.com abrufbar.

Handbuch MobileKey

10 Hilfe & Kontakt

Anleitungen

Detaillierte Informationen zum Betrieb und zur Konfiguration von MobileKey-Komponenten finden Sie online unter www.my-mobilekey.com.

Hotline

Bei technischen Fragen hilft Ihnen die SimonsVoss Service-Hotline unter +49 (0) 89 99 228 333.

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

hotline@simons-voss.com

FAQ

Weitere Informationen und Hilfestellungen zu MobileKey-Produkten finden Sie auf der MobileKey-Homepage (www.my-mobilekey.com) im Infocenter unter Downloads.

SimonsVoss Technologies GmbH

Feringastraße 4

85774 Unterföhring

Deutschland

11 Tipps & Tricks

11.1 Verknüpfung zur Web-App

Auf jedem Gerät kann eine direkte Verknüpfung zur MobileKey Web-App erstellt werden. Besonders auf dem Desktop bzw. Homescreen lässt sich die Web-App so schnell und komfortabel starten - auch bei Smartphones und Tablets. Probieren Sie es einfach aus!

11.2 Verwendung von Schlüsseln ohne USB-Programmierstick

Momentan müssen alle Schlüssel (Transponder) über den USB-Programmierstick programmiert werden. Besonders ohne Zugriff auf ein Windows- oder Android-Gerät wird es hier schwierig. Im Folgenden wird eine Möglichkeit gezeigt, wie Sie vorprogrammierte Schlüssel mit jedem unterstützen Endgerät ohne USB-Programmierstick zuweisen können:

- ✓ Schlösser mit ONLINE-Erweiterung
- ✓ Schlösser mit Status "ONLINE"
- ✓ Matrixansicht geöffnet

1. Legen Sie zu Beginn einige Schlüssel an, z.B. Schlüssel "Extra1, Extra2, Extra3, usw".
   - ⇨ Diese Schlüssel bekommen zunächst keine Berechtigungen.
2. Programmieren Sie alle Schlüssel einmalig mit dem USB-Programmierstick und markieren Sie diese optional mit den jeweiligen Namen.
   - ⇨ Ein Auslesen des Schlüssels ist selbstverständlich auch später möglich.
3. Anstatt irgendwann einen neuen Schlüssel anzulegen und über den USB-Programmierstick zu programmieren, ändern Sie einfach die Eigenschaften eines zuvor angelegten Schlüssels, z.B. "Extra1".
4. Klicken Sie auf den bereits angelegten Schlüssel, z.B. "Extra1" und wählen Sie "BEARBEITEN".
5. Ändern Sie den Namen.
6. Geben Sie optional Daten für "Gültig von" und "Gültig bis" an.
7. Klicken Sie auf die Schaltfläche "SPEICHERN" und kehren Sie zur Matrix zurück.
   - ⇨ Schlüssel ist gespeichert.
8. Berechtigen Sie den Schlüssel an allen gewünschten Schlössern.
9. Klicken Sie auf die Schaltfläche "SAVE".
   - ⇨ Matrixansicht wird geöffnet.
10. Klicken Sie auf das Schloss, an dem der Schlüssel berechtigt sein soll.
    - ⇨ Menü öffnet sich.

11. Klicken Sie auf die Schaltfläche
12. Klicken Sie auf die Schaltfläche "PROGRAMMIEREN".
    ⇨ Die Programmierung erfolgt online über die SmartBridge.
13. Wiederholen Sie diese Schritte, bis Sie alle Schlösser programmiert haben.

⇨ Schlüssel sind an gewählten Schlössern berechtigt.

11.3 Sprache einstellen

Sie können die Sprache der Web-App ganz einfach einstellen. Zur Verfügung stehen:

- Englisch
- Dänisch
- Deutsch
- Französisch
- Italienisch
- Niederländisch
- Schwedisch

Vorgehen:

✓ Matrixansicht geöffnet

1. Klicken Sie auf das Menü-Symbol.
   ⇨ Menü auf der rechten Seite öffnet sich.
2. Klicken Sie auf den Eintrag mit Ihrem Namen.
   ⇨ Menü ändert sich.
3. Klicken Sie auf die Schaltfläche "KONTO VERWALTEN".
   ⇨ Menü Kontodaten wird angezeigt.
4. Klicken Sie auf die Schaltfläche "SPRACHEN".
   ⇨ Auswahlmenü für Sprachen wird geöffnet.
5. Wählen Sie Ihre gewünschte Sprache aus.

⇨ Sprache ist eingestellt.

Handbuch MobileKey

12 Anhang: Handbücher der einzelnen Komponenten

Die folgenden Produkthandbücher sind teilweise für den Betrieb mit der LSM-Software ausgelegt. In MobileKey wird sowohl für die Verwaltung als auch die Programmierung die MobileKey Web-App benutzt. Die MobileKey Web-App bietet ein einfaches Handling, wobei spezielle Funktionen wie beispielsweise Zutrittsprotokolle, Zeitpläne oder DoorMonitoring-Funktionen unterstützt werden.

12.1 Handbuch Schließzylinder

12.1.1 Bestimmungsgemäßer Gebrauch

Digitale SimonsVoss-MobileKey-Schließzylinder werden in dafür vorgesehene Türschlösser (z.B. DIN-Einsteckschlösser) eingebaut, um diese in ein digitales Schließsystem einzubinden. Digitale Halbzylinder können zusätzlich in optional erhältlichen SimonsVoss-Vorhangschlössern betrieben werden.

Der digitale MobileKey-Schließzylinder darf nur für diesen bestimmten Zweck in einem vorgesehenen Türschloss betrieben werden. Ein anderweitiger Gebrauch ist nicht zulässig!

Digitale MobileKey-Schließzylinder sind in verschiedenen Längen verfügbar. Die Auswahl der richtigen Größe ist von entscheidender Bedeutung. Die Länge des Schließzylinders ist auf der Verpackung abgedruckt und kann jederzeit nachgemessen werden. Ist der Zylinder zu kurz, können die Knäufe nicht montiert werden. Ist der Zylinder zu lang, kann er aus dem Schloss gerissen werden. Der Zylinder muss weniger als 3 mm auf jeder Seite der Tür vorstehen, um einen ordnungsgemäßen Betrieb zu gewährleisten.

Das Produkt darf in keiner Weise verändert werden, außer in Übereinstimmung mit den in den Anweisungen beschriebenen Änderungen.

12.1.2 Sicherheitshinweise

Vorsicht:

- Durch fehlerhaft installierte oder programmierte MobileKey-Schließzylinder kann der Zugang durch eine Tür versperrt werden. Für die Folgen fehlerhafter Installationen, wie nicht möglicher Zugang zu verletzten Personen, Sachschäden oder andere Schäden haftet die SimonsVoss Technologies GmbH nicht.
- Die im digitalen MobileKey-Schließzylinder eingesetzten Batterien können bei Fehlbehandlung eine Feuer- oder Verbrennungsgefahr darstellen. Die Batterien nicht aufladen, öffnen, erhitzen oder verbrennen! Batterien nicht kurzschließen!

Handbuch MobileKey

- Bei Verwendung in Kombination mit Panikschlössern, ist nach dem Einbau unbedingt sicherzustellen, dass sich alle Teile des Verschlusses in einem betriebsbereiten Zustand befinden und die Panikfunktion des Einsteckschlosses gewährleistet ist.
- Der Antipanikzylinder darf nur in die Schlösser eingebaut werden, für die dieser auch ausdrücklich zugelassen ist! Bitte beachten Sie hierzu auch die Unterlagen/Dokumentationen der Schlosshersteller.
- Beim Einsatz des Antipanikzylinders in nicht zugelassene Schlösser kann die Fluchttürfunktion gestört sein und nicht wieder freigegeben werden. Kontaktieren Sie die SimonsVoss Technologies GmbH für nähere Informationen zu diesem Thema.
- Im nicht eingebauten Zustand besteht beim Betätigen des Antipanikzylinders Verletzungsgefahr durch den zurückschnellenden Mitnehmer.
- Nach der Europäischen Norm EN 179 Anhang C ist im Rahmen der Wartung von Notausgangsverschlüssen in Abständen von nicht mehr als einem Monat sicherzustellen, dass sämtliche Teile des Verschlusses vom Antipanikzylinder in einem zufriedenstellenden betriebsfähigen Zustand sind.

Hinweise:

- Für Beschädigungen der Türen oder der Komponenten durch fehlerhafte Montage übernimmt die SimonsVoss Technologies GmbH keine Haftung.
- Der SimonsVoss MobileKey-Schließzylinder darf nur für den vorgesehenen Zweck, das Öffnen und Schließen von Türen genutzt werden. Ein anderer Gebrauch ist nicht zulässig.
- Der Einbau darf nur durch geschultes Fachpersonal durchgeführt werden!
- Zylinder nicht mit Öl, Farbe oder Säuren in Verbindung bringen!
- Im Außeneinsatz ist die Variante .WP einzusetzen.
- Der Innenknauf des MobileKey-Schließzylinder weist die Schutzklasse IP40 auf. Deshalb muss sichergestellt werden, dass der Innenknauf keinem Kontakt mit Wasser ausgesetzt wird.
- Beim freidrehenden Antipanikzylinder sind beide Knäufe freidrehend, und können nur mit einem berechtigten Identmedium eingekuppelt werden.
- Im Außeneinsatz ist die Funktion des Antipanikzylinders bei Temperaturen unter - 20°C und über + 50°C nicht mehr gewährleistet.
- Nach dem Einbau und oder dem Batteriewechsel des Antipanikzylinders ist unbedingt ein Funktionstest durchzuführen!
- Für den Außeneinsatz muss beim Antipanikzylinder die Variante „WP“ verwendet werden.

Handbuch MobileKey

– Änderungen bzw. technische Weiterentwicklungen vorbehalten.
– Die Dokumentation wurde nach bestem Wissen erstellt, evtl. Fehler können aber nicht ausgeschlossen werden. Hierfür kann keine Haftung übernommen werden.
– Sollten Abweichungen von Inhalten in Fremdsprachenversionen der Dokumentation bestehen, gilt im Zweifelsfalle das deutsche Original.
– Alle Anweisungen müssen beim Einbau genau befolgt werden. Diese Anweisungen und jegliche Anweisungen bezüglich der Wartung sollten von der den Einbau vornehmenden Person an den Benutzer weitergegeben werden.
– Aus Sicherheitsgründen muss sich das Schließanlagenpasswort aus mindestens 8 Zeichen zusammensetzen. Die Codelänge bei digitalen Schließzylindern *(sowohl bei System 3060/3061 und MobileKey)* entspricht 2^{168} Bit.

Hinweise zum Batteriewechsel

– Der Batteriewechsel darf nur durch geschultes Fachpersonal durchgeführt werden!
– Ein Vertauschen der Polarität kann zu Beschädigungen des MobileKey-Schließzylinder führen!
– Es sind nur Batterien zu verwenden, welche von SimonsVoss freigegeben sind!
– Der Zylinder muss mit zwei Batterien betrieben werden!
– Alte bzw. verbrauchte Batterien fachgerecht entsorgen, und nicht in Reichweite von Kindern aufbewahren!
– Bei einem Batteriewechsel immer beide Batterien erneuern!
– Bei einem Batteriewechsel die Kontakte der neuen Batterien nicht mit den Händen berühren. Verwenden Sie hierzu saubere und fettfreie Handschuhe.
– Beim Batteriewechsel darauf achten, dass die Elektronik nicht z.B. mechanisch belastet wird bzw. anderweitig zu Schaden kommt.
– Zum Batteriewechsel ausschließlich den Montage-/ Batterieschlüssel (Z4.SCHLÜSSEL) von SimonsVoss verwenden.

12.1.3 Allgemein

12.1.3.1 Produktbeschreibung

Das digitale Schließ- und Zutrittskontrollsystem von SimonsVoss ist eine elektronische Variante einer mechanischen Schließanlage mit der Funktionalität einer klassischen Zutrittskontrolle.

Der digitale Schließzylinder und der digitale Halbzylinder sind eine zentrale Komponente des Schließ- und Zutrittskontrollsystems. Funkkommunikation ersetzt die mechanische Authentifizierung eines Schlüssels.

Handbuch MobileKey

In dieser Produktbeschreibung werden sowohl der Schließzylinder als auch der Halbzylinder beschrieben. Der Aufbau und die Funktionsweise der beiden Produkte sind in vielen Hinsichten vergleichbar. Auf Unterschiede zwischen den beiden Produkten als auch auf unterschiedliche Varianten wird in den entsprechenden Kapiteln hingewiesen.

Falls nicht explizit erwähnt oder aus dem Kontext zu entnehmen, wird in diesem Dokument unter „Schließzylinder“ sowohl der Schließzylinder als auch der Halbzylinder verstanden.

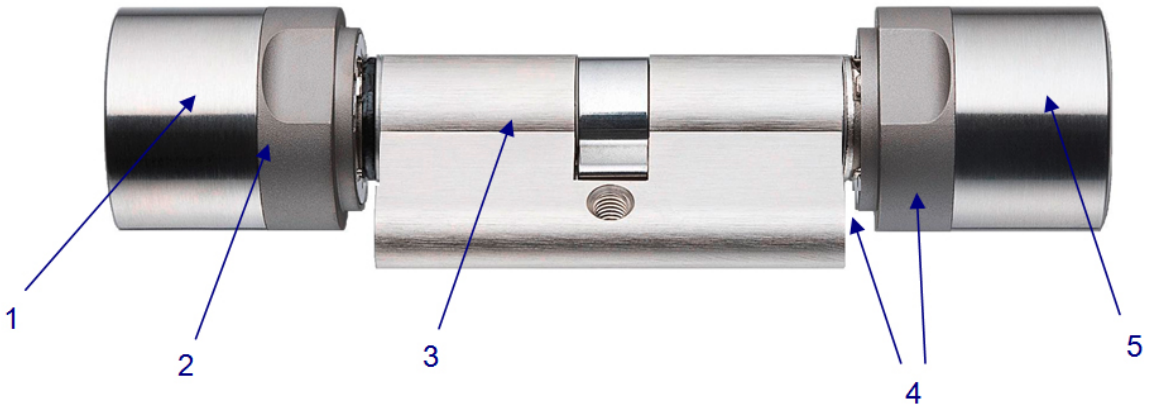
Die Datenübertragung zur Authentifizierung erfolgt mit einem Transponder (25kHz induktiv).

Die digitalen Schließzylinder werden durch zwei redundant ausgelegte Batterien mit Strom versorgt. Durch diese integrierte Spannungsversorgung sind die Zylinder autark. Dadurch entfällt ein Verkabelungsaufwand an der Tür. Die Ausfallsicherheit wird zusätzlich durch ein intelligentes Batteriewarnsystem erhöht.

Die Systemelemente von SimonsVoss werden ab Werk in einem unkonfigurierten Zustand ausgeliefert. Erst bei der Erstprogrammierung wird dieser der Schließanlage zugewiesen. Dieses erleichtert die Lagerhaltung und vereinfacht die Produktverwaltung.

Alle Schließzylinder integrieren sich aufgrund der Modularität nahtlos in SimonsVoss Systeme und können wie alle SimonsVoss Komponenten mit der jeweiligen Schließplansoftware *(z.B. LSM oder MobileKey Web-App)* programmiert werden. Verschiedene andere Authentifizierungsmedien *(z.B. eine PinCode-Tastatur)* können verkabelungsfrei angeschlossen werden. Im späteren Ausbau lassen sich die Zylinder auch ohne Verkabelung vernetzen *(z.B. für WaveNet bzw. MobileKey ONLINE)* und in einem Onlineverbund verwalten.

12.1.3.2 Aufbau des Schließzylinders

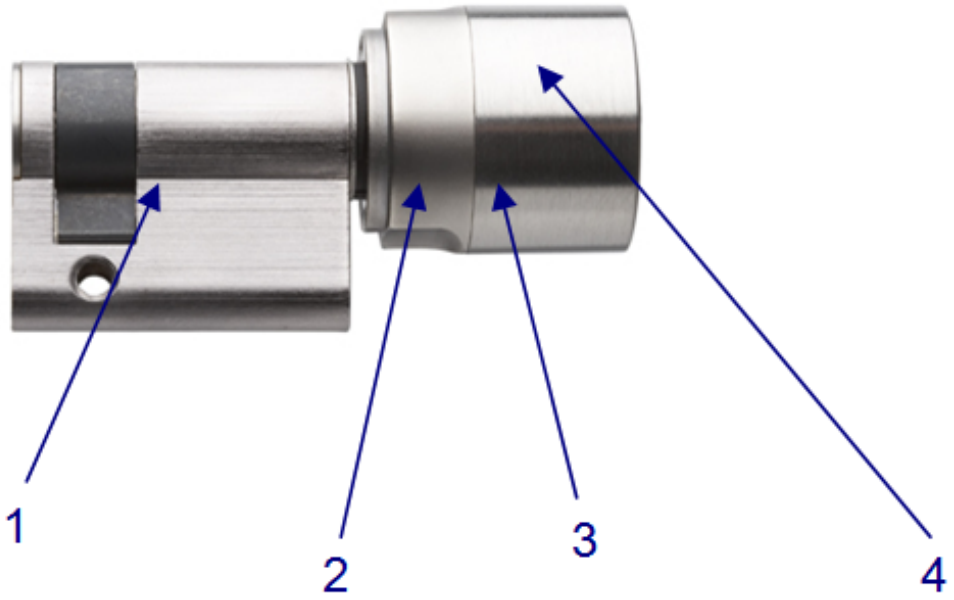


1. Innenknauf

Handbuch MobileKey

2. Batterien / Elektronik
3. Aktor
4. Bohrschutz
5. Außenknauf

12.1.3.3 Aufbau Halbzylinder



1. Aktor
2. Elektronik
3. Batterien
4. Knauf

12.1.3.4 Öffnen und Schließen von Außen

Bei Freidrehenden Schließzylindern (FD)

Beim freidrehenden MobileKey-Schließzylinder drehen im nicht aktivierten Zustand der Außen- und Innenknauf frei durch. Ein Öffnen oder Schließen der Tür ist ohne gültiges Identmedium nicht möglich. Identifizieren Sie sich zum Betätigen des Zylinders mit Ihrem gültigen Identmedium am Außenknauf. Sofern es sich um ein berechtigtes Identmedium handelt, ertönt ein doppelter Signalton sowie ein zweimaliges Aufblinken der blauen LED und der Schließzylinder kuppelt ein. Drehen Sie den Außenknauf in Sperr- bzw. Öffnungsrichtung. Für diesen Vorgang haben Sie ca. fünf Sekunden Zeit. Die Kupplungszeit kann konfiguriert werden. Danach ertönt ein einzelner Signalton und der Außen- bzw. Innenknauf dreht wieder frei durch. Vergewissern Sie sich, dass der Außen- bzw. Innenknauf des Schließzylinders nach dem Kupplungsvorgang wieder frei dreht.

Handbuch MobileKey

HINWEIS

Falls es sich um ein Identmedium handelt, der aufgrund des Zeitzonenplans momentan nicht zugelassen ist, ertönt ein einzelner Signalton. Der Zylinder kuppelt jedoch nicht ein, so dass der Außen- bzw. Innenknauf weiterhin frei dreht und sich die Tür nicht öffnen lässt. Dieses Verhalten ist im Fremdsystem gesondert einzustellen.

12.1.3.5 Öffnen und Schließen von Innen

Bei freidrehenden Schließzylindern (FD)

Beim freidrehenden MobileKey-Schließzylinder drehen im nicht aktivierten Zustand der Außen- und Innenknauf frei durch. Ein Öffnen oder Schließen der Tür von außen ist nur durch Betätigen des Identmediums am Innenknauf möglich.

Bei nicht freidrehenden Schließzylindern (CO)

Auf der Innenseite fest eingekuppelte MobileKey-Schließzylinder sind von Innen ohne Identmedium bedienbar. In diesem Fall kann die Tür am Innenknauf auch ohne ein berechtigtes Identmedium auf- und zugeschlossen werden.

12.1.4 Ausführungen

12.1.4.1 FD-Version (Standard)

Beidseitig freidrehender MobileKey-Schließzylinder.

Der Doppelknaufzylinder .FD steht ab einer Länge von 30-30 mm zur Verfügung.

12.1.4.2 HZ-Version (Standard)

Die Standardversion des Halbzylinders.

12.1.4.3 TS-Version

Ausführung wie Standardversion; jedoch mit der zusätzlichen Möglichkeit, den Zylinder ohne Identmedium von Innen einkuppeln zu lassen. Diese Zylindervariante kann mit Hilfe zweier am Innenknauf angebrachter Knöpfe mechanisch zum Einkuppeln gebracht werden. D.h. von der Innenseite der Tür wird kein Transponder benötigt. Der Zylinder kuppelt dann für 5 Sekunden ein (konfigurierbar), und die Tür kann geöffnet oder verschlossen werden. Nach dieser Zeit dreht der Zylinder wieder beidseitig frei durch.

Die Version .TS ist nicht nachrüstbar.

12.1.4.4 AP2-Version

Bei allen Türen, bei denen die Panikfunktion des Schlosses durch die Stellung des Mitnehmers negativ beeinflusst werden kann, muss ein Zylinder mit Antipanikfunktion eingebaut werden. Diese Version besitzt

einen integrierten Federmechanismus welcher den Schließbart in eine unkritische Position zieht, weshalb die Panikfunktion eines Panikschlosses nicht blockiert werden kann.

Die Montage erfolgt wie beim regulären MobileKey-Schließzylinder.

Bei Türen im Verlauf von Rettungswegen, die nach dem 01. April 2003 eingebaut wurden (Verschlüsse nach DIN EN 179 bzw. DIN EN 1125), sind folgende Punkte zu beachten: Bei allen Verschlüssen, in deren Zulassung steht, dass der MobileKey-Schließzylinder keine Auswirkung auf die Funktion des Schlosses hat, dürfen alle MobileKey-Schließzylinder eingesetzt werden. Bei allen Verschlüssen, bei denen die Mitnehmerstellung der MobileKey-Schließzylinder Auswirkungen auf die Funktion des Schlosses hat, muss gegebenenfalls der MobileKey-Schließzylinder Typ .AP2 (Antipanikzylinder) verwendet werden; dieser muss in der Zulassung des Schlossherstellers aufgeführt sein.

⚠ GEFAHR

Aufgrund der konstruktiven Beschaffenheit von Panikschlössern ist es nicht zulässig, bei geschlossener Tür den Knauf des MobileKey-Schließzylinder auf Anschlag zu drehen, da hierdurch die Panikfunktion des Schlosses beeinflusst werden kann.

12.1.4.5 WP-Version (FD)

Bei der WP-Version (Weather Proof) des MobileKey-Schließzylinder erhöht sich die Schutzklasse von IP 54 auf IP 66. Daher eignet sich diese Version für den Einsatz im Außenbereich oder Außentüren auch wenn der Zylinder nicht direktem Spritzwasser ausgesetzt ist.

Antipanikzylinder: Die WP-Version ist speziell für den Außenbereich bestimmt und sollte verbaut werden, wenn der Außenknauf mit Wasser (z.B. Regenwasser) in Verbindung kommen kann. Die WP-Version weist eine höhere Widerstandskraft gegenüber Wasser auf, wobei der Mitnehmer nicht mit Wasser in Berührung kommen darf.

Diese Version steht ab der Länge 30-35 mm und in den Varianten .FD, .ZK, .MS und .FH zur Verfügung.

12.1.4.6 WP-Version (HZ/CO/AP)

Bei der WP-Version (Weather Proof) des Halb-, Comfort- oder Antipanikzylinders ist der Elektronikknauf abgedichtet, womit dieser eine erhöhte Schutzklasse von IP 66 aufweist. Daher eignet sich diese Version, wenn sich die Elektronikseite im Außenbereich befindet, d.h. der Elektronikknauf bspw. Regen ausgesetzt ist. Es ist nicht zulässig das Wasser durch die Tür eintritt.

Handbuch MobileKey

12.1.4.7 DM-Version (Schließzylinder DoorMonitoring)

Allgemein

Dieses Handbuch ist ein ergänzendes Dokument zu dem Handbuch „Digitaler Schließzylinder und digitaler Halbzylinder (TN4)“. In dem vorgenannten Dokument wird auf die Installation, die Bedienung und den Batteriewechsel der Zylindergeneration TN4 eingegangen, die ebenfalls für den Door Monitoring (DM) Zylinder Anwendung finden. Auch werden in dem Dokument Sicherheitshinweise aufgelistet, die ebenfalls für den DM Zylinder gültig sind.

Dieses Dokument beschreibt die Funktionen des DM-Zylinders. In den Grundfunktionen verhält sich der DM-Zylinder genauso wie ein Digitaler Schließzylinder von SimonsVoss. Daher wird in dieser Produktbeschreibung nur auf die Besonderheiten des DM-Zylinders eingegangen. Es wird auf das Produkthandbuch „Digitaler Schließzylinder und digitaler Halbzylinder (TN4)“ verwiesen, dass die Zylinder, deren Installation und Handhabung beschreibt.

Beschreibung

Beim Door Monitoring Zylinder (DM-Zylinder) handelt es sich um einen elektronischen Schließzylinder mit integrierter Türüberwachung. Die integrierte Türüberwachung des DM-Zylinders lässt sich ohne Verkabelung der Türe realisieren.

Sensoren innerhalb des DM-Zylinders überwachen die Drehbewegung des Schließbarts. Sensoren in der intelligenten Stulpschraube überwachen den Öffnungszustand der Tür.

Der Door Monitoring Zylinder zeichnet die Zutritte auf (Zutrittslisten) und überwacht den Zustand und die Zustandsänderungen der Tür (offen, geschlossen, verriegelt, sicher verriegelt, Manipulationsversuch und gewaltsames Öffnen).

Folgende Türzustände werden aufgezeichnet:

- Tür - offen / geschlossen
- Schließbart einmal / zweimal (maximal viermal) gedreht - Tür - unverschlossen / verriegelt / sicher verriegelt
- Alarm

Diese Türzustände können durch das Netzwerk an die Software bzw. Web-App übertragen und dort dargestellt werden, so dass der Nutzer auf einen Blick den übertragenen Zustand erkennen kann.

Handbuch MobileKey

Spezifikationen

HINWEIS

DM-Zylinder dürfen nicht in Mehrfachverriegelungen mit Getriebe (Getriebeschlösser) betrieben werden!

Zylinder vom Typ DM.AP2 (ohne Riegelüberwachung) sind davon ausgenommen und können auch in Mehrfachverriegelungen mit Getriebe betrieben werden.

Standardausführung

Der DM-Zylinder wird in folgender Standardkonfiguration ausgeliefert:

- .DM Türüberwachung
- .ZK Zutrittskontrolle, Zeitzonensteuerung und Protokollierung

Zu der Standardkonfiguration muss folgendes Zubehör bestellt werden:

- Z4.DM.dd.SCREW.n Stulpschraube

HINWEIS

Bei der Bestellung der Stulpschraube muss das Dornmaß angegeben werden

Die Stulpschraube wird nach dem Dornmaß gefertigt und ist entsprechend einige Millimeter länger

Nur wenn die Stulpschraube die richtige Länge hat, werden die Informationen korrekt an den Zylinder übertragen.

dd steht für das Dornmaß des Schlosses. Die Stulpschraube wird standardmäßig für die Dornmaße von 25 bis 110mm in Schritten von 5mm angeboten. Größere Längen in Schritten von 5mm sind möglich.

Baulängen

Der DM-Zylinder wird ab 30-35mm (Außen – Innen) angeboten.

Bestellcodes

Für die entsprechenden Bestellcodes wird auf die jeweils gültige Preisliste, bzw. den aktuellen Produktkatalog verwiesen.

Inbetriebnahme

Überblick

Je nach Konfiguration stehen Ihnen unterschiedliche Funktionen zur Verfügung:

	Offline	Online
Nachverfolgung wer Tür zuletzt entriegelt/ verriegelt hat	Zutrittsliste auslesen über Programmierstick	Zutrittsliste auslesen über Programmierstick oder das Funknetzwerk
Überwachung des Zustands der Tür	Nein	Ja

Handbuch MobileKey

	Offline	Online
Übermittlung von Alarmen an die Matrix	Nein	Ja. Anzeige in Matrix
Ereignisse generieren, z.B Pop-up Fenster	Nein	Nein
Schloss mit PZ-Profil einbinden	Ja	Ja
Überwachen eines SVP* Schlosses	Nein	Nein

Montagehinweise

Installation und Montage

Der Einbau des DM Zylinders erfolgt analog zu dem Einbau eines anderen digitalen Zylinders von SimonsVoss.

Batterien sind bei Lieferung bereits eingebaut. Der Zylinder ist sofort einsatzbereit.

Bei der Installation des digitalen Schließzylinders ist darauf zu achten, dass sich keine niederfrequenten Störquellen im Umkreis befinden. Typische Quellen sind:

- Schaltnetzteile
- Starke Stromleitungen
- Generatoren
- Frequenzwechsler

Schließzylinder sollten mindestens im Abstand von 0,5 m voneinander entfernt montiert werden, Smart Relais bzw. Scharfschalteinheiten im Abstand von 1,5m

Das PZ-Gehäuse des Schließzylinders darf im Außenbereich maximal 3 mm aus der Tür bzw. aus dem Beschlag herausstehen, gegebenenfalls ist eine Profilzylinder-Rosette bzw. –Beschlag zu verwenden

Bei der Montage nicht gegen die Knäufe schlagen

HINWEIS

Der Door Monitoring Zylinder darf nicht mit herkömmlichen Stulpschrauben montiert werden

Herkömmliche Stulpschrauben können den Zylinder zerstören

a) Der DM Zylinder muss zusammen mit einer speziell für den Zylinder hergestellten Stulpschraube montiert werden

b) Die Stulpschraube ist nicht im Lieferumfang enthalten und muss separat bestellt werden

Die Stulpschraube wird standardmäßig für ein Dornmaß von 25mm bis 110mm in 5mm Schritten angeboten. Bei Bestellung muss das Dornmaß des Schlosses angegeben werden. Bei der Verwendung einer zu kurzen

Handbuch MobileKey

Stulpschraube kann die Schraube nicht fassen, bei einer zu langen Schraube kann die Schraube nicht vollständig in das Türblatt geschraubt werden

In dem Kopf der Stulpschraube befindet sich ein Sensor. Die Schraube ist mit einem speziellen Schraubenzieher bzw. Adapter einzudrehen. Wird ein herkömmlicher Schlitzschraubenzieher verwendet, könnte er die Schraube und somit den Sensor zerstören

Die Norm für Schlösser sieht vor, dass der Lochdurchmesser für die Stulpschraube mindestens 5,4mm betragen muss. Manche Schlösser werden mit einem kleineren Bohrloch ausgeliefert. Ist das der Fall, kann das Loch mit einem 5,5mm Stahlbohrer vergrößert werden

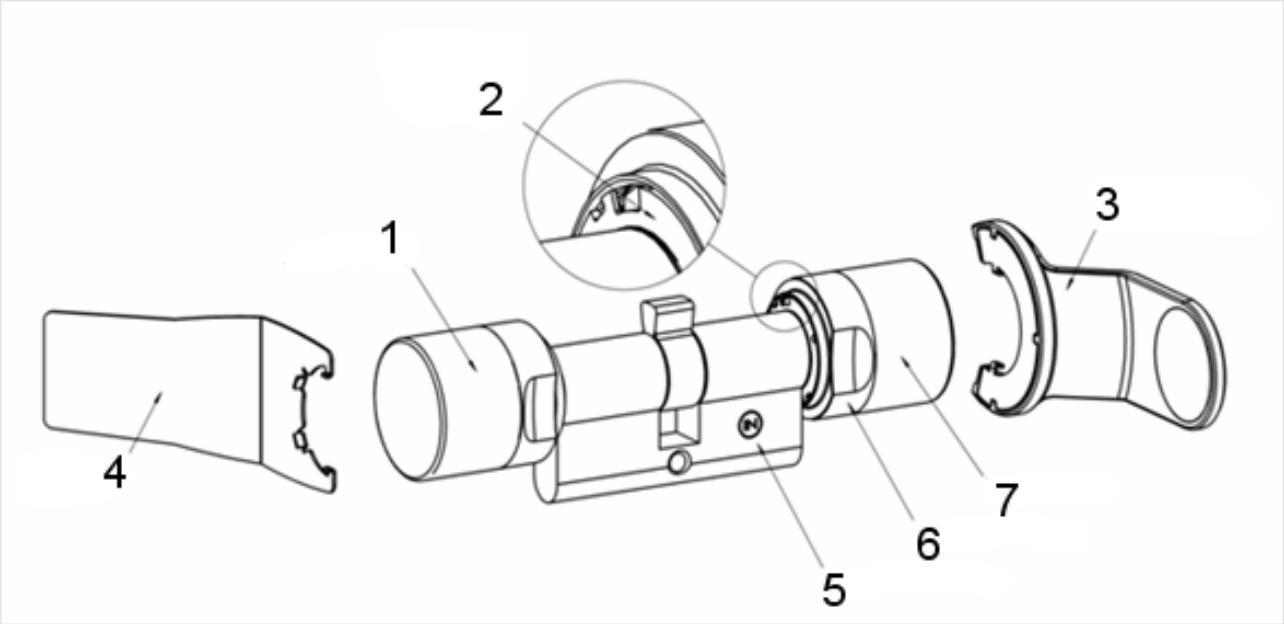
Montage

Beim digitalen Schließzylinder gibt es einen Knauf mit Elektronik und einen Knauf ohne Elektronik. Für die Montage muß der Knauf Elektronik entfernt werden. Bei fast allen Zylindervarianten ist der Elektronikknauf innen. Die einigen Ausnahmen sind:

- Comfort Zylinder: .CO
- Schweizer Rundzylinder: .SR

Die Innenseite des Zylinders ist die Gravur "IN" auf den Zylinderkörper gekennzeichnet

Bei Auslieferung ist der Knauf ohne Elektronik nur aufgesteckt und kann einfach abgezogen werden

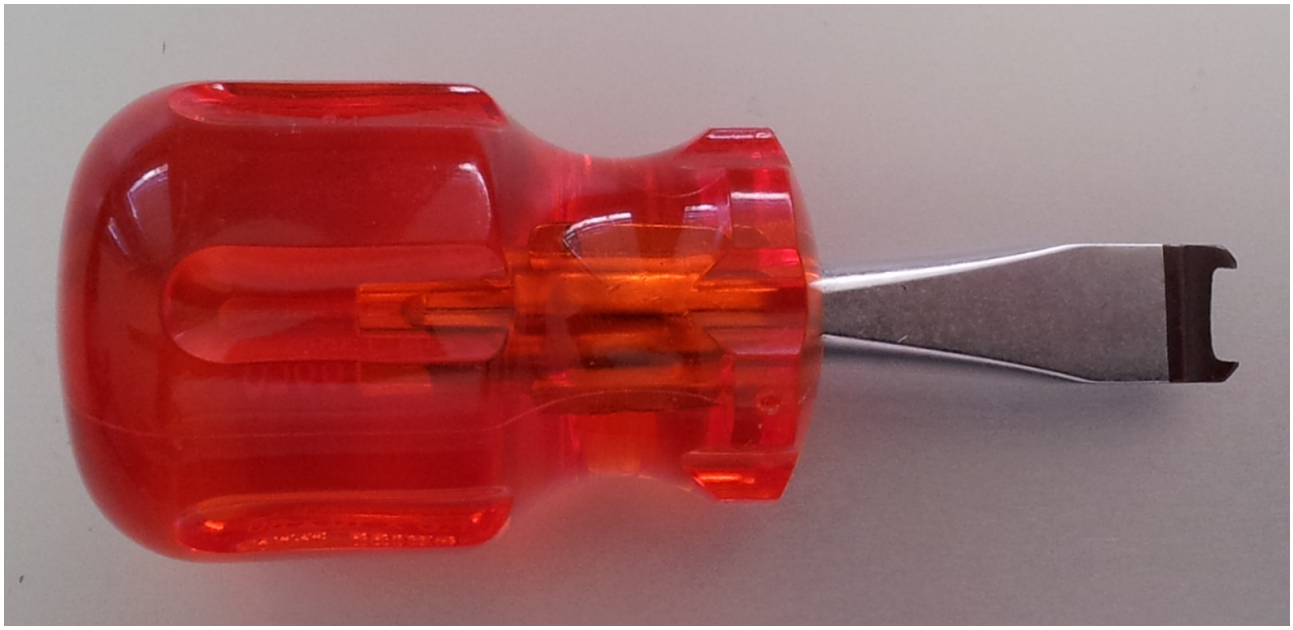


1. Außenknauf (Ohne Elektronik)
2. Rastscheibe mit Öffnung
3. Montage- und Batterieschlüssel

Handbuch MobileKey

4. Montageschlüssel (nicht für Batteriewechsel)
5. Seitenmarkierung
6. Griffmuldenring
7. Innenknauf (Mit Elektronik)

1. Ziehen Sie den Knauf ohne Elektronik ab
2. Den Zylinder durch das Schloss stecken



3. Mit der passenden Stulpschraube den Zylinder befestigen. Schraube nicht zu fest anziehen. Nur den passenden Schraubendreher verwenden

HINWEIS

Eine zu fest angezogene Stulpschraube kann zu Fehlfunktionen (z.B. Blockade) des Schließzylinders im Schloss führen.

Die Stulpschraube handfest (max. 3,5 Nm) anziehen

Keinen Akkuschrauber verwenden

HINWEIS

Ein herkömmlicher Schraubendreher kann den Sensor in der Stulpschraube beschädigen

Die Stulpschraube nur mit dem passenden Schraubendreher anziehen

4. Knauf wieder aufstecken und soweit drehen, dass der Knauf in die Mulden des Flanschs eingreift

Handbuch MobileKey

5. Montageschlüssel so ansetzen, dass die beiden Nasen des Montagewerkzeugs in den Außenknauf eingreifen (bei Bedarf Knauf drehen, bis beide Nasen des Schlüssels in den Knauf einhaken)
6. Den Knauf durch eine 30° Drehung im Uhrzeigersinn wieder verschließen

Magnetmontage

Für die Türüberwachung müssen die Magnetplättchen, die der Stulpschraube beigefügt sind, in die Türzarge geklebt werden. Die Magnete dienen als Signalgeber für den Sensor in der Stulpschraube. Danach sollte ein Funktionstest durchgeführt werden

In Abhängigkeit von dem Material der Türe / der Zarge und der Spaltgröße müssen ein oder mehrere Magnetplättchen aufgebracht werden

1. Magnetplättchen lose in die Türzarge kleben, so dass die Plättchen gegenüber dem Kopf der Stulpschraube liegen
2. Tür vorsichtig schließen, so dass die Falle fast einrastet
3. Wenn beim Fast-Schließen der Tür die Anzeige in der LSM von „offen“ auf „geschlossen“ springt:
   - die Anzahl der Magnetplättchen verringern
   - das Plättchen weiter in Richtung Zargenmitte verschieben
   - das Plättchen verkleinern
4. Tür schließen. Die Anzeige in der LSM muss von „offen“ auf geschlossen springen. Erfolgt diese nicht, ist das Magnetfeld zu schwach für den Sensor. Zusätzliches Plättchen auf die Zarge kleben und den Test wiederholen

Ein zu großes Magnetfeld (zu viele Plättchen) führt zu einer Übersteuerung des Sensors, so dass dieser nicht mehr anspricht

Einsatz in Fluchttüren

Einsatz im Fluchttürschloss

Panikschlösser haben die Eigenschaft sich von der Innenseite der Tür durch drücken des Türgriffs zu entriegeln und zu öffnen. Das Schloss entriegelt ohne, dass der Mitnehmer gedreht wird. Manche Schlösser benötigen einen Antipanikzylinder, da der Mitnehmer bei gewissen Positionen zu einem Blockieren des Schlosses führen kann. Mit dem Schlosshersteller ist zu klären, ob ein AP Zylinder eingesetzt werden muss. Bei dem Einsatz des DM Zylinders in Fluchttürschlösser sind im Vorfeld verschiedene Themen zu klären:

- SVP Schloss oder Nicht SVP Schloss
- Einsatz eines AP Zylinders notwendig, damit ein Blockieren des Schlosses verhindert wird
- Typisches Begehungsverhalten der Tür.

Handbuch MobileKey

Wird die Tür normalerweise mit einem berechtigten Transponder geöffnet oder durch Drücken des Innendrückers? Der DM Zylinder registriert die Bewegungen des Mitnehmers und schließt über die Drehungen und die Drehrichtung auf den Zustand des Schlosses. Das Zurückfahren des Riegels und somit das Entriegeln der Tür wird nicht registriert. Beim DM.AP2 Zylinder ist die Überwachung des Mitnehmers deaktiviert. Ein manuelles Verriegeln wird nicht überwacht.

HINWEIS **Bei einem Einbau in ein Fluchttürschloss sind immer die Anforderungen aus DIN EN 179 bzw. EN 1125 zu beachten.**

Einsatz im SVP Schloss

Ein SVP (Selbst verriegelndes Panik) Schloss lässt sich von Innen durch Drücken der Klinke öffnen und beim Schließen der Tür verriegeln. Somit zeigt der DM Zylinder nicht zuverlässig (gar nicht) die Riegelposition an. Der DM.AP2 überwacht die Riegelposition nicht. Somit lässt sich nur der Öffnungszustand der Tür überwachen.

Tagesbetrieb

Lassen Sie sich die wichtigsten Informationen Ihrer Schließanlage direkt im Schließplan anzeigen. Die Türzustände des DM Zylinders lassen sich direkt im Schließplan darstellen

Die Türzustände werden über verschiedene Symbole in der Matrix dargestellt

Symbol	Zustand	Information
	sicher verriegelt	Tür ist geschlossen und Mitnehmer wurde rotiert bis zur Einstellung [sicher verriegelt]
	geschlossen	Tür ist geschlossen und Riegel zurückgefahren
	offen	Tür geöffnet
	Fehlermeldung – Undefinierter Zustand / Warnung / Alarm	Dieses Symbol hat unterschiedliche Bedeutungen: Tür zu lange offen Stulpschraube wurde manipuliert (spricht nicht mehr an, wurde entfernt) Magnetfeld-Manipulation (Magnetfeld an der Stulpschraube ist zu groß) Tür wurde gewaltsam geöffnet (trotz Verriegelung wird die Tür geöffnet)

Handbuch MobileKey

Symbol	Zustand	Information
?	Zustand unbekannt	Undefinierter Zustand – Aufgrund einer Störung, bzw. einer dem System unlogischen Veränderung ist der Zustand unbekannt

Tab. 1: Door Monitoring Symbole in der Matrix

Unbekannter Zustand

Das Symbol „unbekannter Zustand“ und das Alarmsymbol verändert sich nicht selbstständig, wenn der Grund für die Störung verschwindet (Ausnahme ist der „Tür zu lange offen Alarm“, der bei Schließen der Tür nicht verschwindet).

Fehlermeldung	Aktion
Undefinierter Zustand der Tür	Tür muss geöffnet und wieder geschlossen werden. Der Zylinder erkennt den Zustand und schickt diesen an die Software bzw. WebApp.
Tür zu lange offen	Tür schließen
Stulpschraube wurde manipuliert (wurde entfernt)	Stulpschraube prüfen. Nach Fehlerbehebung den Fehler wieder zurücksetzen, siehe Kapitel Zylinder
Magnetfeld-Manipulation (Magnetfeld an der Stulpschraube ist zu groß)	Tür prüfen. Fehler zurücksetzen, siehe Kapitel Zylinder
Tür ist gewaltsam geöffnet worden (trotz Verriegelung wird die Tür geöffnet)	Tür prüfen. Fehler zurücksetzen

HINWEIS

Rücksetzen der Alarmmeldungen

Beim Offline-Betrieb müssen wichtige Alarmmeldungen (Einbruch) manuell über eine Neuprogrammierung zurückgesetzt werden! Daher wird stets eine Vernetzung über WaveNet oder MobileKey ONLINE empfohlen!

Batterien

Batterielebensdauer

Die Batterielebensdauer ist abhängig von den Konfigurationseinstellungen des DM Zylinders und dem Nutzungsverhalten. Einfluss auf die auf die Batterielebensdauer haben:

- Abtastrate der Stulpschraube
- Anzahl der Betätigungen
- Auslesen der Zutrittsliste
- Umprogrammierungen

Handbuch MobileKey

– Anzahl der Tasks

Die Zahl der Betätigungen beträgt bis zu 50.000.
Die Batterielebensdauer in Abhängigkeit der Stulpschraubeneinstellung:

Abtastrate	Batteriestandzeit
fest eingestellt	bis zu 4 Jahre

Tab. 2: Abtastrate und Batteriestandzeit

Die angegebenen Batteriestandzeiten sind Richtwerte. Eine Batteriewarnung erfolgt nicht nach Ablauf der o.a. Standzeit, sondern aufgrund der gemessenen Kapazität der Batterie.

Batteriewarnstufen

Warnstufe 1	Warnstufe 2
8 kurze Töne vor dem Einkuppeln	30 Sekunden lang acht kurze Töne mit jeweils einer Sekunde Pause vor dem Einkuppeln
Bis zu 15.000 Öffnungen oder bis zu 9 Monaten	Bis zu 50 Öffnungen oder bis zu 30 Tagen

Tab. 3: Batteriewarnstufen DM Zylinder

HINWEIS

Ab Batterie-Warnstufe 2 ist die Überwachungsfunktionalität des Zylinders deaktiviert! Es werden weder Zustandsänderungen aufgezeichnet noch übertragen.

Nach erstmaligem Auftreten der Warnstufe 2 können noch zirka 50 Öffnungen mit einem Transponder durchgeführt werden.

Fehlerdiagnose

Symptom	Ursache	Lösung
Stulpschraube lässt sich nicht ganz eindrehen	Stulpschraube zu lang	Dornmaß nachmessen. Stulpschraube gemäß dem Dornmaß bestellen Die Stulpschraube darf auf keinen Fall gekürzt werden. Dadurch würde der Sensor zerstört werden
Stulpschraube greift beim Eindrehen nicht	Stulpschraube zu kurz	Dornmaß nachmessen Stulpschraube gemäß dem Dornmaß bestellen

Handbuch MobileKey

Symptom	Ursache	Lösung
Türzustand wird nicht in der WebApp gezeigt	Verbindung zwischen Zylinder und WebApp gestört	Prüfen ob dieser Fehler auch beim Drehen des Mitnehmerbartes auftritt. Wenn ja, ist die Verbindung gestört. Netzwerk Überprüfen Ist der Zylinder (die Netzwerkkappe) im Netzwerk eingebunden?
	Magnetfeld am Stulpschrauben-Sensor zu schwach Bei einem zu schwachen Magnetfeld registriert der Sensor dieses nicht	Zusätzliches Magnetfeldplättchen anbringen Spalt zwischen Tür und Rahmen verringern
	Magnetfeld am Stulpschrauben-Sensor zu hoch Bei einem zu starken Magnetfeld, übersteuert der Sensor	Magnetfeldplättchen entfernen Spalt zwischen Tür und Rahmen vergrößern
	Stulpschraube zu kurz. Kein Kontakt zwischen dem Sensor in der Stulpschraube und Zylinder	Dornmaß nachmessen Stulpschraube gemäß dem Dornmaß bestellen
	DM Zylinder falsch konfiguriert	DM Zylinder Konfiguration prüfen. Haken bei Tür offen Ereignis in der Zutrittsliste gesetzt? Übertragung über Netzwerk gesetzt? Abtastintervall der Stulpschraube gesetzt?
		Flip-Flop-Modus, oder Zeitumschaltung eingestellt? > Der Riegelzustand kann nicht überprüft werden

Handbuch MobileKey

Symptom	Ursache	Lösung
	Zylinder defekt	Zylinder tauschen
	DM Zylinder im Flip-Flop Modus oder Zeitumschaltung aktiviert	DM Zylinder kann nicht im Flip-Flop Modus oder mit Zeitumschaltung betrieben werden. Modus ändern und Tür öffnen und schließen damit Zylinder in einen definierten Zustand zurückkehrt
	Zylinder defekt	Zylinder tauschen
	Netzwerkverbindung instabil	Umgebung auf Störquellen untersuchen. z.B. Leuchtstoffröhren, Dimmschalter, Generatoren, Netzteile

Ereignisse weiterleiten

Überprüfen Sie die Netzwerkeinstellungen, wenn die Türzustände nicht korrekt angezeigt werden.

Zubehör

Batterie-Set

Es steht ein Batterie-Set mit Ersatzbatterien für den Zylinder zur Verfügung. Das Set besteht aus 10 Stück CR2450 Batterien.

Bestellnummer: Z4.BAT.SET

Stulpschraube

Der DM Zylinder benötigt eine spezielle Stulpschraube mit dem integrierten Türöffnungssensor.

Bestellnummer: Z4.DM.xx.SCREW.n

Stulpschraube xx steht für das Dornmaß des Schlosses und ist nicht mit der Länge der Stulpschraube zu verwechseln. Die Stulpschrauben werden standardmäßig für die Dornmaße von 25 bis 70mm in Schritten von 5mm angeboten. Sonderlängen sind auf Anfrage erhältlich.

Schraubendreher

Der Schraubkopf der Stulpschraube hat in der Mitte eine Erhebung, so dass die Stulpschraube nicht mit einem regulären Schlitzschraubendreher eingeschraubt werden kann. Als Werkzeug steht ein Schraubendreher zur Verfügung.

Bestellnummer: Z4.DM.SCREWDRIVER

Wavenet Netzwerkkappe LN.I

Die Wavenet Netzwerkkappe ist eine Tauschkappe und beinhaltet die Elektronik für die Netzwerkanbindung des DM Zylinders.

Handbuch MobileKey

Technische Daten

Zylindertyp	Europrofil Door Monitoring Zylinder gemäß DIN 18252/ EN1303, Edelstahl, beidseitig freidrehend
Protokollgenerationen	G2 oder MobileKey
Knaufdurchmesser	30 mm
Basis-Baulänge	30 – 35 mm (Außen-/Innenmaß)
Schutzart	IP 54 (im eingebauten Zustand)
Luftfeuchtigkeit:	<95%; nicht kondensierend
Batterietyp	2 x Lithium CR2450 3V
Batterielebensdauer	Bis zu 50.000 Betätigungen oder 4 Jahre Standby bei Abtastintervall Stulpschraube von 2 Sekunden
Temperaturbereich	Betrieb –25 °C bis +65 °C Lagerung –35 °C bis +70 °C
Zutrittsspeicher	Ca. 1000 Türzustände speicherbar
Zeitzonengruppen	100+1 *(Zeitzonengruppen werden in MobileKey nicht unterstützt)*
Anzahl Transponder pro Schließzylinder	Bis zu 64.000 bzw. 100 bei MobileKey
Vernetzung	Direkt vernetzt mit integriertem LockNode (Netzwerk-Knaufkappe WNM.LN.I)

Tab. 4: Technische Daten - Door Monitoring Zylinder

12.1.5 Einbauanleitung

12.1.5.1 Allgemeine Hinweise

Bei der Installation des digitalen MobileKey-Schließzylinder ist darauf zu achten, dass sich keine niederfrequenten Funkstörquellen im Umkreis befinden.

Das Gehäuse des Profilzylinders sollte im Außenbereich bündig abschließen, maximal jedoch 3 mm herausstehen; gegebenenfalls ist eine Profilzylinder-Rosette bzw. ein Sicherheitsbeschlag anzubringen. Darüber hinaus muss sichergestellt sein, dass über den Mitnehmerbereich kein Wasser in den Zylinder eindringen kann.

Bei der Montage auf keinen Fall gegen die Knäufe schlagen.

Alle Knäufe sind durch Bajonettverschlüsse verschlossen.

Handbuch MobileKey

Die Innenseite des MobileKey-Schließzylinder ist zum einen durch eine Laserung (IL für Innenlänge) auf dem PZ-Gehäuse gekennzeichnet, zum anderen erkennt man die Elektronikseite am schwarzen Kunststoffring zwischen dem Knauf und dem Profilzylinder-Gehäuse.

Die Batterien sind bei Lieferung bereits eingebaut!

Alle aufgeführten Arbeiten in diesem Kapitel können alternativ auch mit dem Montage-/Batterieschlüssel durchgeführt werden.

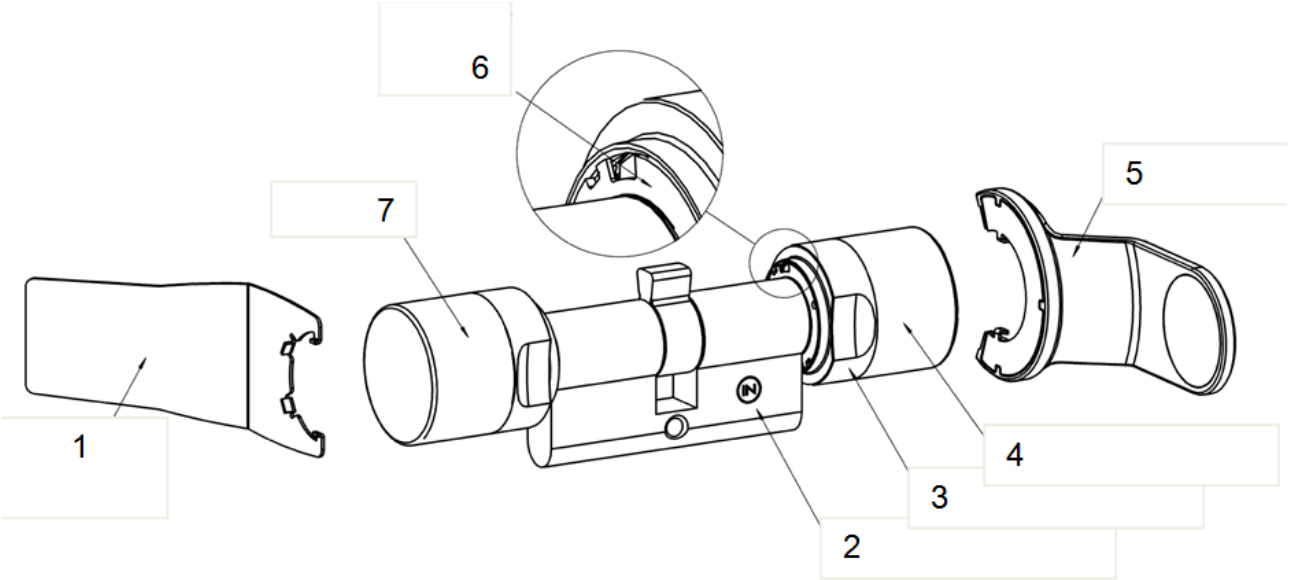
12.1.5.2 Programmierung

Vor der Installation müssen der digitale MobileKey-Schließzylinder und die dazugehörigen Identifikationsmedien programmiert werden.

Programmeiren von MobileKey-Schließzylinder in MobileKey: Siehe Programmieren von Komponenten [▸ 13]

12.1.5.3 Montagevarianten

Montage Doppelknaufzylinder (außer Typ .AP/.SKG/.VDS)



1. Montageschlüssel
2. Seitenmarkierung
3. Griffmuldenring
4. Innenknauf
5. Batteriewechselschlüssel
6. Rastscheibe mit Öffnung (Außenseite identisch)
7. Außenknauf

Handbuch MobileKey

Außenknauf abnehmen

Den Montageschlüssel am Außenknauf so ansetzen, dass die beiden Nasen des Montagewerkzeuges in den Außenknauf eingreifen, bei Bedarf Knauf drehen bis beide Nasen des Schlüssels in die Rastscheibe einhaken.

HINWEIS Damit das Montagewerkzeug in die Rastscheibe eingreifen kann, muss das Werkzeug plan an der Innenstirnfläche des Knaufes anliegen.

Außenknauf festhalten und Montagewerkzeug vorsichtig ca. um 30° im Uhrzeigersinn drehen (bis ein Knacken zu vernehmen ist). Knauf abziehen.

Digitalen Zylinder im Schloss befestigen

Den Mitnehmer soweit drehen, bis dieser senkrecht nach unten steht. Den digitalen Schließzylinder so durch das Schloss stecken, dass der Innenknauf (siehe Bild oben) Richtung Innenseite der Tür zeigt. Den Zylinder mit der Stulpschraube im Einsteckschloss befestigen.

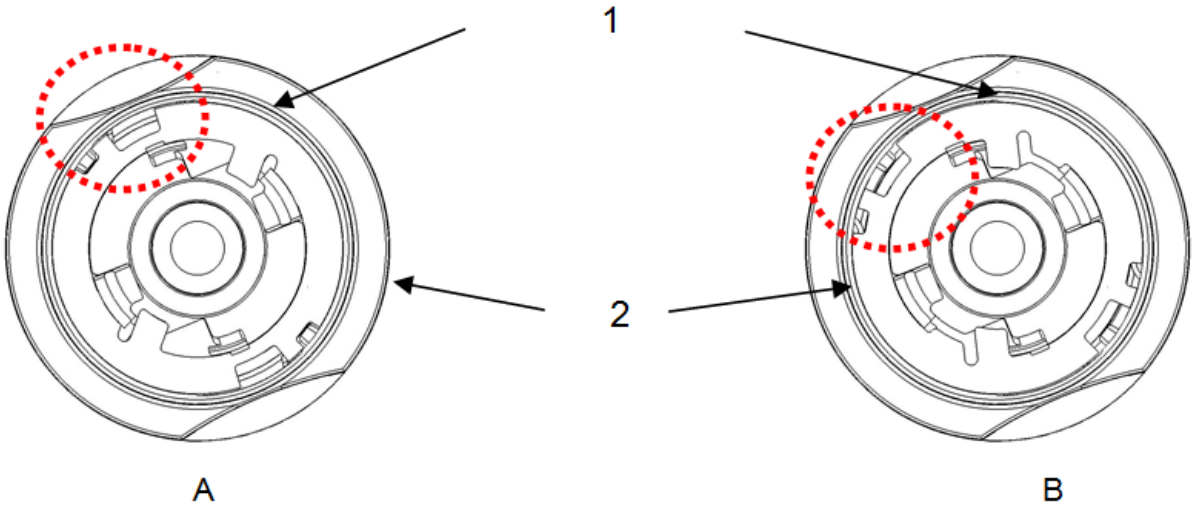
HINWEIS Bei der Montage auf keinen Fall gegen die Knäufe schlagen. Zylinder nicht mit Öl, Fett, Farbe oder Säure in Verbindung bringen.

Außenknauf befestigen

Knauf wieder aufstecken und unter leichtem Druck soweit gegen den Uhrzeigersinn drehen, dass der Außenknauf in die Mulden des Flansches eingreift. Evtl. den Knauf in dieser Position in Richtung des Profilzylindergehäuses drücken.

HINWEIS Das Verdrehen der Bajonettscheibe im nicht montiertem Zustand kann die Befestigung des Knaufes verhindern. In diesem Fall die Scheibe mittels des Montagewerkzeuges in die Ursprungsposition "Bajonettscheibe offen" zurückschieben. (Siehe Bilder)

Handbuch MobileKey



1. Bajonettscheibe
2. Knauf
3. Bajonettscheibe geschlossen
4. Bajonettscheibe offen

Montageschlüssel so ansetzen, dass die beiden Nasen des Montagewerkzeuges in den Außenknauf eingreifen (bei Bedarf Knauf drehen, bis beide Nasen des Schlüssels in den Knauf einhaken). Den Knauf durch eine 30° Drehung im Uhrzeigersinn wieder verschließen.

Funktionstest durchführen

1. Zylinder mittels gültigem Identmedium einkuppeln lassen und bei geöffneter Tür den Knauf in Sperr- und Öffnungsrichtung drehen. Der Knauf muss sich hierbei leichtgängig drehen lassen.
2. Tür schließen und den Vorgang wiederholen. Sollte der Schließzylinder schwergängig sein, so ist ein Ausrichten der Tür bzw. eine Nachbearbeitung des Schließbleches erforderlich.

Montage Antipanikzylinder

Innenknauf abnehmen

Den Gewindestift des Innenknaufes (siehe Bild oben) mit einem Innensechskantschlüssel lösen (nicht vollständig herausschrauben). Den Mitnehmer festhalten und danach den Innenknauf gegen den Uhrzeigersinn abdrehen, bzw. beim freidrehenden .AP-Zylinder den Knauf nach dem Lösen des Gewindestiftes abziehen.

Handbuch MobileKey

Digitalen Zylinder im Schloss befestigen

Zuerst den Mitnehmer drehen, bis dieser senkrecht nach unten steht. Den digitalen Schließzylinder von der Außenseite so durch das Schloss stecken, dass der Außenknauf in Richtung Außenseite der Tür zeigt. Den Zylinder mit der Stulpschraube im Einsteckschloss befestigen.

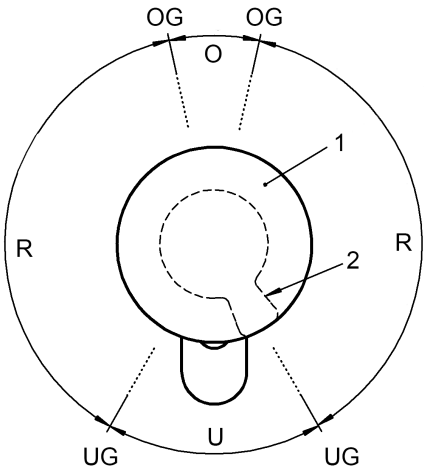
HINWEIS Bei der Montage auf keinen Fall gegen die Knäufe schlagen. Zylinder nicht mit Öl, Farbe oder Säure in Verbindung bringen.

Innenknauf befestigen

Den Innenknauf auf das Gewinde drehen, die Gegenkraft bildet dabei der Anschlag des Mitnehmers im Schloss. Ziehen Sie den Innenknauf an, bzw. schieben Sie beim freidrehenden AP-Zylinder den Innenknauf bis zum Anschlag auf. Drehen Sie den Gewindestift mit dem Innensechskantschlüssel fest.

Funktionstest

- Um die Funktion des AP2-Zylinders in einem Antipanikschloss zu überprüfen, ist die Leichtgängigkeit des Mitnehmers und das Öffnen der Tür gemäß dem unten beschriebenen Vorgehen zwingend zu kontrollieren.
- Der Funktionstest ist in Richtung des Fluchtwegs durchzuführen.
- Wenn der Zylinder neu ausgerichtet oder der Sitz der Stulpschraube verändert wurde, ist ein Funktionstest zwingend durchzuführen!
- Zur Durchführung des Funktionstests ist ein berechtigtes Identmedium notwendig.
- Vor dem Funktionstest ist der Riegel einzufahren.



Handbuch MobileKey

Bereich U:	Keine Rückstellkraft auf den Mitnehmer
Bereich R:	Rückstellbereich Richtung Bereich U
Bereich O:	Oberer Totpunkt des Riegelvorschubs (Keine Rückstellkraft auf Mitnehmer)
OG:	Oberer Grenzbereich
UG:	Unterer Grenzbereich
1:	Knauf
2:	Lage des Mitnehmers (verdeckt)

1. Drehen Sie den Knauf zunächst bei gekuppeltem Zylinder in Sperrrichtung des Schlosses bis zum Riegelvorschub in den Bereich „R“.
   ⇨ Sie spüren ein Rückstellmoment. Wenn Sie den Knauf in diesem Bereich loslassen, muss er selbsttätig in den Bereich „U“ zurückdrehen.
2. Verschließen Sie das Schloss und prüfen Sie die Rückstellkraft . Dazu den gekuppelten Knauf in Sperrrichtung des Schlosses durch den Bereich „R“ in den Bereich „O“ drehen.
   ⇨ Der Riegel schiebt sich vor. In dem Bereich „O“ wirkt keine Rückstellkraft.
3. Bewegen Sie den Knauf geringfügig über die Grenze zwischen den Bereichen „O“ und „R“ in gleicher Drehrichtung weiter.
   ⇨ Der Riegel fährt vollständig aus. Von diesem Punkt aus muss die Rückstellkraft den Knauf selbstständig bis zum Bereich „U“ weiterdrehen, wenn er losgelassen wird.
   ⇨ Sollte sich der Knauf nicht selbstständig in den Bereich U drehen, ist entweder die Stulpschraube zu fest angezogen oder das Schloss falsch ausgerichtet worden. Nach der Fehlerbehebung ist der Test erneut durchzuführen. Eine zu fest angezogene Stulpschraube wirkt sich bremsend auf den Rückstellmechanismus aus.
4. Verschließen Sie die Tür und prüfen Sie die Funktion des Schlosses durch Drücken der Klinke/Panikstange in Richtung des Fluchtwegs.
   ⇨ Der Riegel muss zurückschnappen und die Tür muss sich leicht öffnen lassen.
   ⇨ Sollte der Riegel beim Betätigen der Klinke nicht zurückfahren oder hakt die Klinke, ist entweder der Schließzylinder oder das Schloss falsch ausgerichtet oder defekt. Nach der vorgenannten Fehlerbehebung sind die vorherigen Tests erneut durchzuführen.

Kann die korrekte Funktion des Schlosses nach dem Funktionstest nicht sichergestellt werden, nehmen Sie bitte Kontakt mit dem Schlosshersteller auf.

Handbuch MobileKey

12.1.6 Signaltöne

Der MobileKey-Schließzylinder gibt den Zustand und eine Autorisierung akustisch wieder. Die Tabelle unten beschreibt die Bedeutung der Signaltöne.

2 kurze Töne vor dem Einkuppeln und ein kurzer Ton nach dem Auskuppeln.	Normale Betätigung	Keine
1 kurzer Signalton; Zylinder kuppelt nicht ein.	Zutrittsversuch eines in der Schließanlage gelisteten Transponders, aber: – Außerhalb der Zeitzone gebucht .	Keine
Batteriewarnstufe 1: 8 kurze Töne vor dem Einkuppeln.	Ladezustand der Batterien ist niedrig.	Batterien im Zylinder wechseln.
Batteriewarnstufe 2: 30 Sekunden lang 8 kurze Töne mit jeweils einer Sekunde Pause vor dem Einkuppeln.	Batterien sind fast vollständig entladen.	Sofort die Batterien im Zylinder wechseln!
8 kurze Töne nach dem Auskuppeln.	Ladezustand der Transponderbatterie ist niedrig.	Transponderbatterie wechseln lassen.

12.1.6.1 Batteriewarnungen

In den Schließzylindern und Transpondern wurde ein Batteriemanagement implementiert, welches frühzeitig auf nachlassende Batteriekapazität hinweist. Somit wird verhindert, dass es zu einer vollständigen Entladung der Batterien kommen kann. Im nachfolgenden werden die einzelnen Batteriewarnstufen beschrieben.

Die Batterien der Schließzylinder arbeiten redundant. Fällt eine der Batterien aus, oder beträgt die Ladekapazität einen Schwellwert schaltet das System eine Batteriewarnstufe.

– Warnstufe 1: Schwache Batterien

  Unterschreitet die Ladekapazität eine der Batterien 25% aktiviert sich die Batteriewarnstufe 1. Nach Betätigung des Transponders sind vor dem Einkuppeln des Zylinders acht kurze, schnell aufeinanderfolgende Signaltöne zu hören. Die Batterien müssen ausgetauscht werden.

– Warnstufe 2: Extrem schwache Batterien

Handbuch MobileKey

Entladen sich die Batterien des Schließzylinders noch weiter, erfolgen nach Betätigung des Transponders vor dem Einkuppeln des Zylinders für ca. 30 Sekunden kurze, schnell aufeinanderfolgende Signaltöne. Erst danach kuppelt der Zylinder ein. Die Batterien sollten so schnell wie möglich ausgetauscht werden.

	WARNSTUFE 1	WARNSTUFE 2
Zylinder aktiv:	8 kurze Töne vor dem Einkuppeln	30 Sekunden lang acht kurze Töne mit jeweils einer Sekunde Pause vor dem Einkuppeln
	Bis zu 15.000 Öffnungen oder bis zu 9 Monaten	Bis zu 50 Öffnungen oder bis zu 30 Tagen

12.1.6.2 Batteriewarnung Transponder

Bei einem niedrigen Ladezustand der Transponderbatterie, ertönen nach jeder Transponderbetätigung am Schließzylinder (nicht Transponder) nach dem Auskuppeln acht kurze, schnell aufeinanderfolgende Signaltöne.

12.1.7 Batteriewechsel

12.1.7.1 Allgemeine Hinweise

Das Auswechseln der Batterien darf nur von Fachpersonal durchgeführt werden.

Beim Wechseln der Batterien sind fettfreie, saubere Stoffhandschuhe zu tragen, um ein Verdrecken der Batterien durch Fingerabdrücke zu verhindern. Fingerabdrücke auf den Batterien können die Lebensdauer der Batterien erheblich reduzieren.

Es sollten ausschließlich Batterien eingesetzt werden, die von SimonsVoss freigegeben sind.

HINWEIS

Ein Vertauschen der Polarität kann zu Beschädigungen des MobileKey-Schließzylinder führen. Die in diesem Gerät verwendeten Batterien können bei Fehlbehandlung eine Feuer- oder Verbrennungsgefahr darstellen. Batterien nicht aufladen, öffnen, über 100° C erhitzen, kurzschließen oder verbrennen!

HINWEIS

Lithium-Batterien bitte im entladenen Zustand sofort fachgerecht zu entsorgen. Nicht in Reichweite von Kindern aufbewahren, nicht öffnen und nicht ins Feuer werfen. Bei einem Batteriewechsel müssen immer beide Batterien erneuert werden! Sicherheitshinweise beachten!

Handbuch MobileKey

Auch ohne Spannungsversorgung durch Batterien behält der Schließzylinder dauerhaft seinen Zustand, die Programmierung sowie die gespeicherten Protokolle.

12.1.7.2 Batterielebensdauer

Die Batterielebensdauer ist für verschiedene Versionen von Schließzylindern unterschiedlich, da unterschiedlich viel Strom bei einer Aktivierung/Datenverbindung gezogen wird.

VERSION	STANDZEIT	ANZAHL BETÄTIGUNGEN	ANZAHL BATTERIEN
Standardzylinder und Varianten	bis zu 10 Jahre	bis zu 300.000	2
WN (LNI / LockNode)	bis zu 5 Jahre	bis zu 150.000	2

Die angegebene Batterielebensdauer ist nur ein Richtwert. Eine Batteriewarnung erfolgt nicht nach Ablauf der o.a. Lebensdauer, sondern aufgrund des gemessenen Zustandes der Batterie.

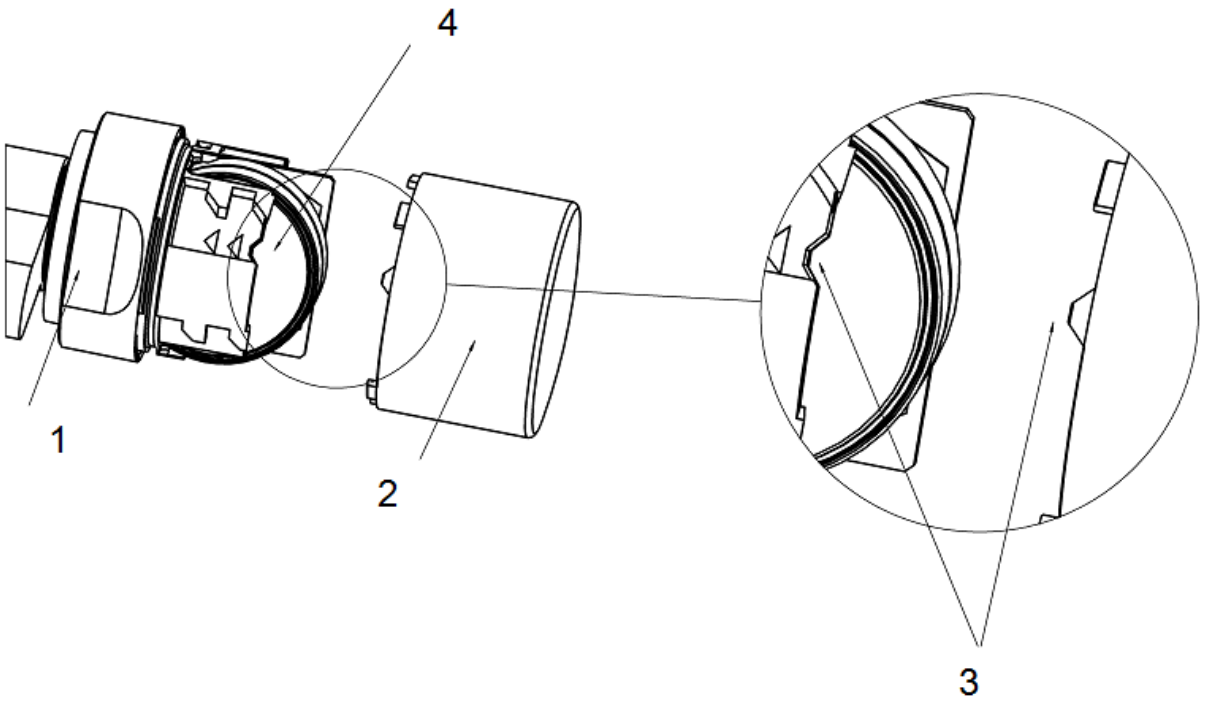
12.1.7.3 Vorgehensweise

1. Den Montage-/Batterieschlüssel am Innenknauf so ansetzen, dass die beiden Nasen in die Öffnungen der Rastscheibe eingreifen (bei Bedarf Knauf drehen bis beide Nasen des Schlüssels in den Knauf einhaken).

HINWEIS Damit der Montage-/Batterieschlüssel in die Rastscheibe eingreifen kann, muss dieser plan an der Innenstirnfläche des Griffmuldenringes aufliegen.

2. Innenknauf festhalten und Montage-/Batterieschlüssel vorsichtig ca. um 30° im Uhrzeigersinn drehen (bis Sie ein Knacken vernehmen).
3. Montage-/Batterieschlüssel vom Knauf entfernen.
4. Griffmuldenring nach hinten Richtung Tür schieben, so dass er sich vom Knauf löst.
5. Griffmuldenring festhalten, und Knauf ca. 10° gegen den Uhrzeigersinn drehen und abziehen.
6. Nur bei MH-Zylindern: Antenne vorsichtig nach oben abklappen.
7. Beide Batterien vorsichtig aus der Halterung ziehen.
8. Die neuen Batterien, mit den Pluspolen zueinander, gleichzeitig in die Halterung schieben (Batterien schnellstmöglich wechseln!). Die neuen Batterien nur mit sauberen und fettfreien Handschuhen berühren.

Handbuch MobileKey



9. Nur bei MH-Zylindern: Antenne durch Einrasten wieder arretieren.
10. Knauf wieder aufstecken (entsprechend der dreieckigen Markierungen, siehe Skizze), Griffmuldenring festhalten und den Innenknauf im Uhrzeigersinn drehend (ca. 10°) befestigen. (Abbildung kann leicht vom Produkt abweichen!)
11. Griffmuldenring wieder auf den Knauf schieben, so dass Knauf und Ring bündig abschließen.
12. Den Montage-/Batterieschlüssel am Innenknauf so ansetzen, dass die beiden Nasen in die Öffnungen der Rastscheibe eingreifen (bei Bedarf Knauf drehen, bis beide Nasen des Schlüssels in den Knauf einhaken).
13. Knauf durch eine Drehung um ca. 30° im Uhrzeigersinn wieder verschließen (bis Sie ein Knacken vernehmen).

Betätigen Sie nun einen berechtigtes Identmedium und testen Sie die Funktion.

12.1.8 Wartung, Reinigung und Desinfektion

HINWEIS Digitale Schließzylinder dürfen nicht mit Öl, Farbe, Fett oder Säure in Verbindung gebracht werden!

Handbuch MobileKey

HINWEIS

Durch Verwendung nicht geeigneter bzw. aggressiver Reinigungs- oder Desinfektionsmittel kann der Schließzylinder beschädigt werden.

Reinigen Sie den Schließzylinder bei Bedarf mit einem weichen, ggf. feuchten Tuch.

Zur Desinfektion dürfen nur Mittel verwendet werden, welche ausdrücklich zur Desinfektion empfindlicher metallischer Oberflächen und Kunststoffen vorgesehen sind.

HINWEIS

HZ.SL:*Bei häufiger Verwendung der Selbstverriegelung empfiehlt es sich, die Einrastkante am Schaltschrankhebelgriff etwas zu fetten.*

Leere Batterien müssen stets durch neue, von SimonsVoss freigegebene, Batterien ersetzt werden. Alte Batterien sind fachgerecht zu entsorgen.

Beim Wechsel der Batterien vom Antipanikzylinder ist ein erneuter Funktionstest durchzuführen.

12.1.9 Einsatzmöglichkeiten

12.1.9.1 Allgemein

Der digitale Schließzylinder passt in Schlösser für Europrofilzylinder nach DIN 18252 und EN1303.

12.1.9.2 Brandschutztüren

Ein Einbau in Brandschutztüren ist grundsätzlich möglich. Jedoch muss geprüft werden, ob der Einsatz auch zulässig ist.

12.1.9.3 Türen im Verlauf von Rettungswegen

Für den Einsatz in Türen mit Antipanikfunktion, in denen die Stellung des Mitnehmers einen Einfluss auf die Funktion des Schlosses haben kann, ist der Typ .AP zu installieren. Dieser muss in der Zulassung des Schlossherstellers aufgeführt sein. Siehe hierzu auch die Normen DIN EN 179 und DIN EN 1125 sowie die Produktdatenblätter der einzelnen Schlosshersteller.

12.1.9.4 Einbausituationen im Außenbereich

Falls nicht sichergestellt werden kann, dass durch die Tür kein Wasser eindringen kann, wird empfohlen, die jeweiligen .WP Versionen zu verwenden. Bei der Variante Antipanikzylinder ist der Außenknauf, und bei der Variante Doppelknaufzylinder der komplette Zylinder abgedichtet.

Handbuch MobileKey

12.1.10 Zubehör

12.1.10.1 Knäufe

Als Zubehör sind folgende Sonderknäufe erhältlich:

- Außenknauf im TN4 Design
- Außenknauf 42 mm Durchmesser mit Griffmulden
- Innenknauf 36 mm Durchmesser für .TS-Zylinder
- Außenknauf verkürzt
- Messingknauf Matt (Innen- und Außenknauf)

Diese Knäufe können jederzeit gegen die Originalknäufe der Schließzylinder ersetzt werden. Montage der Knäufe siehe Einbauanleitung [▸ 61] bzw. Batteriewechsel [▸ 68].

12.1.10.2 Kernziehschutzadapter (Z4.KA.SET)

Dieser Adapter ist kompatibel zu den SKG/VDS-Zylindern bis Baujahr 2010 und den .FD-Zylindern.

Für Kernziehschutzbeschläge gibt es eine mechanische Verlängerung, da bei diesen Beschlägen das PZ-Profil nicht ausgefräst ist. Die Länge der Verlängerung beträgt 8 mm und kann jederzeit nachgerüstet werden.

12.1.10.3 Werkzeug

Neben dem Montagewerkzeug, welches bei der Bestellung mitgeliefert wird, gibt es einen Batteriewechselschlüssel. Mit diesem Werkzeug können sowohl die Außenknäufe montiert bzw. demontiert werden als auch der Batteriewechsel durchgeführt werden.

12.1.10.4 Batterieset

Es steht ein Batteriepack zur Nachbestellung zur Verfügung. Dieses Set enthält 10 Batterien des Typs CR2450. E sind nur freigegebene Batterien von SimonsVoss zu verwenden!

12.1.11 Datenblätter

12.1.11.1 Schließzylinder

Profilzylinder

Grundlänge:	Außen 30 mm, innen 30 mm (AP/ WP 35mm)

Baulängen in 5 mm Abstufungen bis 140 mm Gesamtlänge (max. 90 mm auf einer Seite), Sonderlängen auf Anfrage.

Batterien

Typ:	CR 2450 3V
Hersteller:	Sony, Panasonic, Varta

Handbuch MobileKey

	Anzahl:	2 Stück
	Lebensdauer:	bis zu 300.000 Betätigungen oder bis zu 10 Jahren Standby
Umgebungsbedingungen	Betriebstemperatur:	-25°C bis +65°C
	Lagertemperatur:	-35°C bis +65°C
	Schutzklasse:	IP 54 (im eingebauten Zustand) Variante .WP: IP 65

Merkmale

- 3.000 Zutritte speicherbar (ZK)
- Direkt vernetzbar mit integriertem LockNode (WN)
- LockNode nachrüstbar
- Max. Anzahl Transponder pro Zylinder: 100
- Verschiedene Dauer/Offen-Modi

Knäufe	Material:	Edelstahl
	Farben:	Edelstahl gebürstet
	Durchmesser:	30 mm
	Länge:	37 mm (ab Profilstirnfläche)

12.1.11.2 Halbzylinder

Knäufe	Material:	Edelstahl
	Farben:	Edelstahl gebürstet
	Durchmesser:	30 mm
	Länge:	37 mm (ab Profilstirnfläche)
Profilzylinder	Grundlänge:	Außen 30 mm, Innen 10 mm
	Baulängen in 5 mm - Abstufungen (kein Bausatz) bis 100 mm Gesamtlänge, wobei die Außenseite des Zylinders eine max. Länge von 90 mm haben kann. Größere Längen auf Anfrage.	
Batterien	Typ:	CR 2450 3V
	Hersteller:	Sony, Panasonic, Varta
	Anzahl:	2 Stück
	Lebensdauer:	bis zu 300.000 Betätigungen oder bis zu 10 Jahren Standby

Merkmale

- 3.000 Zutritte speicherbar (ZK)
- Direkt vernetzbar mit integriertem LockNode (WN)
- LockNode nachrüstbar
- Verschiedene Dauer/Offen-Modi

Umgebungsbedingungen	Betriebstemperatur:	-25°C bis +65°C
	Lagertemperatur:	-35°C bis +65°C

Handbuch MobileKey

Schutzklasse:	IP 54 (im eingebauten Zustand) Variante .WP: IP 65 (Knauf)

12.2 Handbuch PinCode-Tastatur

12.2.1 Bestimmungsgemäßer Gebrauch

Die PinCode-Tastatur kann eingesetzt werden, um entsprechende SimonsVoss-Schließungen *(wie z.B. Schließzylinder, SmartHandle oder SmartRelais)* über die Eingabe eines Zahlencodes zu betätigen.

Die Einbindung der PinCode-Tastatur in die Schließanlage erfolgt über die entsprechende Schließanlagensoftware.

- Die PinCode-Tastatur kann bis zu 3 User-PINs speichern, welche jeweils als 3 separate Transponder angesehen werden können.
- User-PINs können wahlweise zwischen 4 und 8 Zeichen lang sein.
- Die Konfiguration der User-PINs kann direkt an der PinCode-Tastatur über die Eingabe der Master-PIN erfolgen.

12.2.2 Sicherheitshinweise

⚠ WARNUNG

Durch fehlerhaft montierte und/oder programmierte Komponenten kann der Zugang durch eine Tür versperrt werden. Für Folgen fehlerhafter Installation, wie versperrter Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss Technologies GmbH nicht!

⚠ VORSICHT

Die in diesem Produkt verwendeten Batterien können bei Fehlbehandlung eine Feuer- oder Verbrennungsgefahr darstellen. Diese Batterien nicht aufladen, öffnen, über 100°C erhitzen oder verbrennen.

⚠ VORSICHT

Die in diesem Handbuch beschriebenen Produkte/Systeme dürfen nur von Personen betrieben werden, welche für die jeweiligen Aufgabenstellungen qualifiziert sind. Qualifiziertes Personal ist aufgrund seines Wissens befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

HINWEIS

Der Master-PIN ist zentraler Bestandteil des Sicherheitskonzepts der PinCode-Tastatur. Es ist sorgsam darauf zu achten, dass der Master-PIN sicher aufbewahrt und jederzeit eingesehen werden kann! Ein Verlust der Master-PIN führt zu erheblichen Einbußen im Betrieb der Schließanlage.

Handbuch MobileKey

HINWEIS

Achten Sie darauf, dass diePinCode-Tastatur nicht verschmutzt oder verkratzt wird. Die PinCode-Tastatur darf nicht zu Boden fallen oder sonstigen starken Stößen ausgesetzt werden.

HINWEIS

Die SimonsVoss Technologies GmbH behält sich das Recht vor, Produktänderungen ohne Vorankündigung durchzuführen. Aufgrund dessen können Beschreibungen und Darstellungen dieser Dokumentationen von den jeweils aktuellsten Produkt- und Softwareversionen abweichen. Generell ist in Zweifelsfällen die deutsche Originalausgabe inhaltliche Referenz. Irrtümer und Rechtschreibfehler vorbehalten. Weitere Informationen über die Produkte von SimonsVoss erhalten Sie im Internet unter: www.simons-voss.com

HINWEIS

Die Batterieentsorgung hat in Übereinstimmung mit den lokalen und landesspezifischen Vorschriften zu erfolgen!

12.2.3 Konfiguration

12.2.3.1 Master-PIN ändern

Dieser Schritt muss nur ausgeführt werden, wenn noch kein neuer Master-PIN einprogrammiert wurde.

1. Eingabe 0 0 0 0
2. Eingabe alte Master-PIN: 1 2 3 4 5 6 7 8
3. Eingabe neue Master-PIN
   ⇨ Die neue Master-PIN muss aus 8 Zeichen bestehen, welche weder fortlaufend noch identisch sind und darf nicht mit 0 beginnen!
4. Eingabe des neuen Master-PIN zur Wiederholung

HINWEIS

Der Master-PIN ist für die Nutzung der PinCode-Tastatur essentiell und kann nicht ausgelesen oder wiederhergestellt werden. Notieren Sie den Master-PIN und bewahren Sie ihn an einem sicheren und geheimen Ort auf.

Es ist jederzeit möglich, den Master-PIN wieder zu ändern. Dies zieht keinen Programmierbedarf mit sich.

12.2.3.2 User-PIN programmieren

In der PinCode-Tastatur können bis zu drei User-PINs vergeben werden. Die Länge des User-PIN kann zwischen 4 und 8 stellen betragen, welche nicht fortlaufend oder identisch sind.

Handbuch MobileKey

Zum besseren Verständnis: Jeder User-PIN *verhält sich wie ein eigener Transponder. Deshalb müssen diese einzelnen* User-PINs *in den jeweiligen (internen) Transpondern (1, 2 & 3) programmiert werden.*

1. Eingabe 0
2. Eingabe Master-PIN
3. Eingabe User-PIN - z.B 1 für User-Pin 1
4. Eingabe der Länge desUser-PIN - z.B. 4 für einen 4-stelligen User-PIN
5. Eingabe User-PIN

Wiederholen Sie den Vorgang, um weitere User-PINs in der PinCode-Tastatur zu programmieren.

12.2.3.3 User-PIN löschen

User-PINs können gelöscht werden, indem die Länge des PIN auf 0 Zeichen gesetzt wird:

1. Drücken Sie die „0“ um in den Programmiermodus zu wechseln.
2. Geben Sie die „Master-PIN “ ein.
3. Drücken Sie z.B. die Taste „1“ der PinCode-Tastatur, um den User-Pin 1 zu löschen.
4. Geben Sie für die PIN Länge die „0“ ein.
   ⇨ Bei korrekter Eingabe wird der betroffene User-PIN gelöscht.

12.2.4 Programmierung

Programmieren von Komponenten [▶ 13]

12.2.5 Montage & Batteriewechsel

Die PinCode-Tastatur kann über das beiliegende Montagematerial befestigt werden.

- Für eine einfache und schnelle Montage kann die PinCode-Tastatur direkt über das beiliegende Spezialklebepad angebracht werden.
- Für eine sichere Montage wird die Verwendung der beiliegenden Schrauben empfohlen. Hierfür wird ein Torx-Schraubendreher vom Typ "TX6" *(nicht im Lieferumfang enthalten)* benötigt, um das Gehäuse zu öffnen!

Montieren Sie die PinCode-Tastatur in einer Entfernung von maximal 20 cm zur Schließung.

Um die Batterien zu wechseln, muss das Gehäuse der PinCode-Tastatur geöffnet werden. Hierfür wird ein Torx-Schraubendreher vom Typ "TX6" *(nicht im Lieferumfang enthalten)* benötigt! Ersetzen Sie alle Batterien durch neue Sony-, Panasonic- oder Varta-Batterien vom Typ CR 2450 (3V).

Handbuch MobileKey

12.2.6 Bedienung

✓ Die PinCode-Tastatur wurde erfolgreich konfiguriert. (Master-Pin & User-Pin)

✓ Die PinCode-Tastatur wurde ordnungsgemäß programmiert.

✓ Mindestens ein User-PIN ist an der gewünschten Schließung berechtigt.

1. Eingabe eines User-PIN.
   ⇨ Zwischen den Eingaben der einzelnen Ziffern dürfen maximal 5 Sekunden verstreichen.
2. Die LED leuchtet grün und es ertönt ein Signalton "Piep, Piep".
   ⇨ Die Schließung kuppelt ein.

Leuchtet die LED der PinCode-Tastatur rot und es ertönt ein Signalton "Beeeeeep", wurde kein gültiger User-PIN eingegeben.

12.2.7 Technische Daten

PinCode-Tastatur	
Batterien:	2 x 3 V Lithium Typ CR 2032
Abmessungen in mm:	96 x 96 x 14
Schutzklasse:	IP 65
Einsatztemperatur:	-20°C bis +50°C
Signalelemente:	Grüne LED + Signaltöne

12.2.8 Konformitätserklärung

Dokumente wie Konformitätserklärungen und sonstige Zertifikate sind online unter www.my-mobilekey.com abrufbar.

12.3 Handbuch SmartBridge

12.3.1 Allgemein

HINWEIS Überprüfen Sie den Bestellcode auf der Verpackung, um sicherzustellen, dass Sie den richtigen Router verwenden!

System3060 / WaveNet: WNM.RN2.ER.IO

Im System 3060 kann der RouterNode 2 als WaveNet-Router eingesetzt werden. So können entsprechende Schließkomponenten untereinander vernetzt werden. Zusätzlich bietet der RouterNode 2 die Möglichkeit, externe Ein- und Ausgänge zu schalten.

Der RouterNode 2 darf nur für diesen vorhergesehen Zweck in einem SimonsVoss Funknetzwerk eingesetzt werden!

MobileKey: MK.SMARTBRIDGE.ER

Bei MobileKey kann die SmartBridge als Accesspoint für die Vernetzung von Schließungen eingesetzt werden.

Handbuch MobileKey

Die SmartBridge darf nur für diesen vorhergesehen Zweck im MobileKey-System eingesetzt werden!

12.3.2 Sicherheitshinweise

⚠ VORSICHT

Der Zugang durch eine Tür kann verweigert werden, wenn Komponenten fehlerhaft installiert oder programmiert wurden. Die SimonsVoss Technologies GmbH haftet nicht für die Folgen einer fehlerhaften Installation, wie beispielsweise der verweigerte Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder andere Schäden.

⚠ VORSICHT

Personen mit elektronischen medizinischen Implantaten (Herzschrittmacher, Hörgeräte usw.) müssen einen Mindestabstand von mindestens 30 cm zwischen dem Implantat und den Netzwerkkomponenten einhalten und sollten hierauf ausdrücklich hingewiesen werden. Im Interesse der Sicherheit sollten sich Personen mit elektronischen Implantaten bezüglich der potenziellen Gefahren der Funkkomponenten (868/915 MHz) medizinisch beraten lassen.

⚠ VORSICHT

Das Gehäuse darf nicht im Betrieb unter Spannung geöffnet werden! Trennen Sie immer die Stromversorgung (Netzkabel bzw. Netzwerk-Kabel bei POE-Betrieb), bevor Sie das Gehäuse öffnen.

⚠ VORSICHT

Im POE-Betrieb (Versorgungsspannung über Ethernet) kann die Temperatur der Platine sehr hoch sein! Lassen Sie den Router abkühlen, bevor Sie das Gehäuse öffnen.

HINWEIS

Die SimonsVoss Technologies GmbH behält sich das Recht vor, das Produkt ohne vorherige Ankündigung zu ändern. Deshalb können Beschreibungen und Darstellungen in diesem Handbuch von den aktuellsten Versionen des Produkts oder der Software abweichen. Grundsätzlich gilt im Zweifelsfall die deutsche Fassung. Irrtümer und Rechtschreibfehler vorbehalten.

HINWEIS

Weitere Informationen über die Produkte aus MobileKey von SimonsVoss finden Sie im Internet unter: www.my-mobilekey.com

Weitere Informationen über MobileKey finden Sie im Internet unter: www.my-mobilekey.com

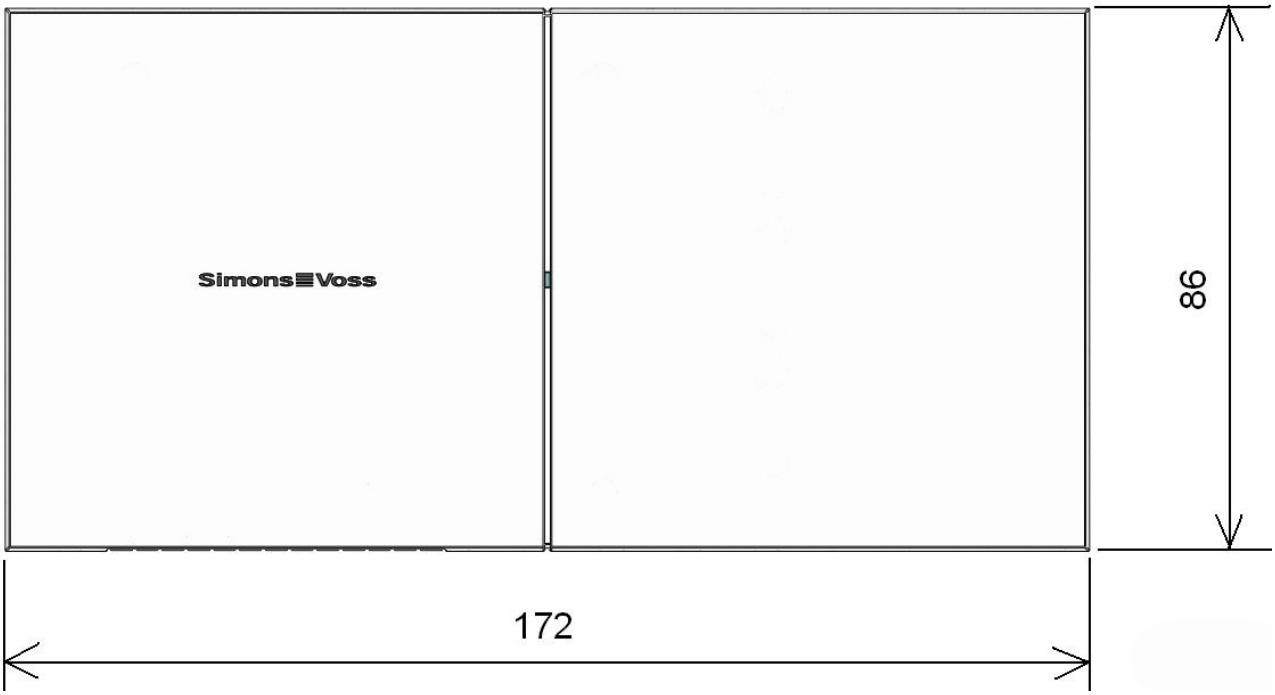
HINWEIS

Lesen Sie sich alle Handbücher der einzelnen SimonsVoss-Komponenten sorgfältig durch.

Handbuch MobileKey

12.3.3 Gehäuse

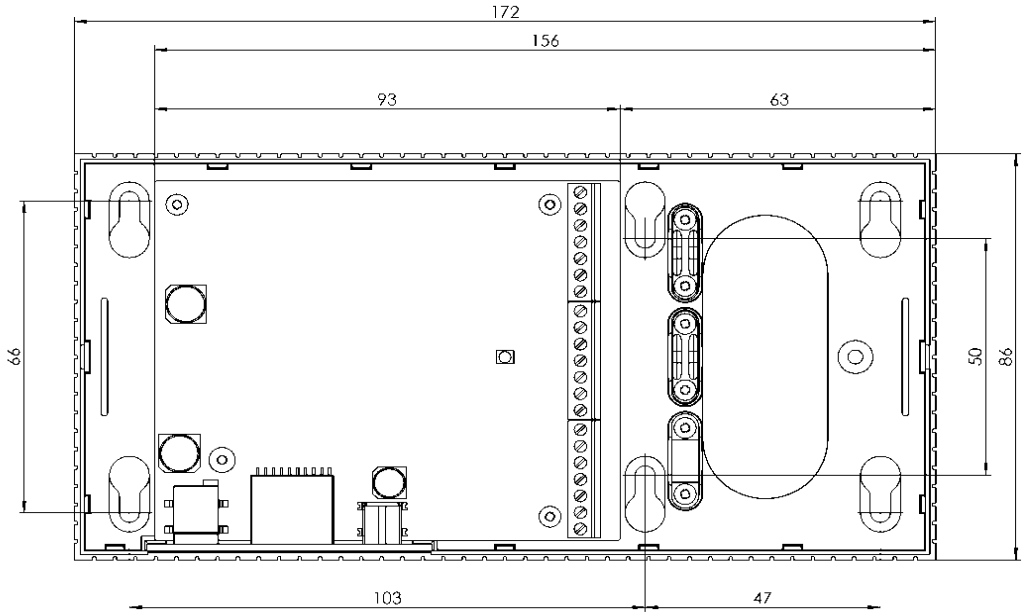
12.3.3.1 Bilder und Abmessungen



(Maße in mm)

Handbuch MobileKey

12.3.3.2 Abmessungen der Gehäuseunterschale



12.3.3.3 Öffnen des Gehäusedeckels

Die Oberschale kann ohne Hilfe von Werkzeug geöffnet werden. Hierzu muss mittig an der Grundplatte auf der linken oder rechten Seite ein leichter Druck ausgeübt werden und die Oberschale kann entfernt werden.

12.3.4 Aufputz Leitungszuführung

Die Rippen an der Gehäuseunterschale vorsichtig mit einer Säge beidseitig auftrennen und den Steg nach oben und unten bewegen damit dieser abbricht. Eventuell scharfkantige Teile mit einer Feile nachbearbeiten.

Handbuch MobileKey

12.3.5 Konfiguration der IP-Settings

Mit dem SimonsVoss OAM-Tool (Ethernet Operations, Administration and Maintenance Tool) können die IP-Settings vorgenommen werden. Das SimonsVoss OAM-Tool steht unter www.my-mobilekey.com zum freien Download zur Verfügung.

HINWEIS

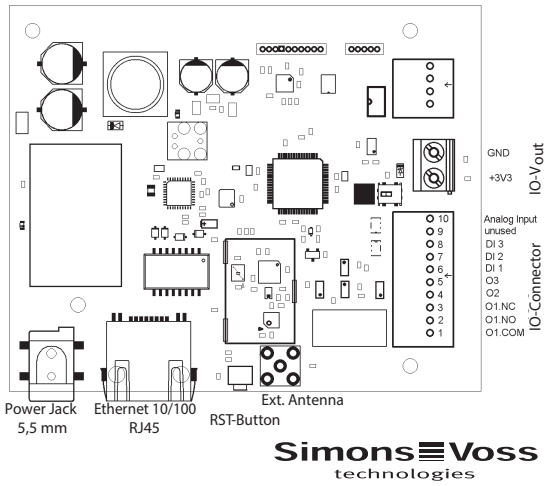
Standardeinstellungen:

IP-Adresse: 192.168.100.100

Benutzername: SimonsVoss | Passwort: SimonsVoss

12.3.6 Technische Anschlüsse

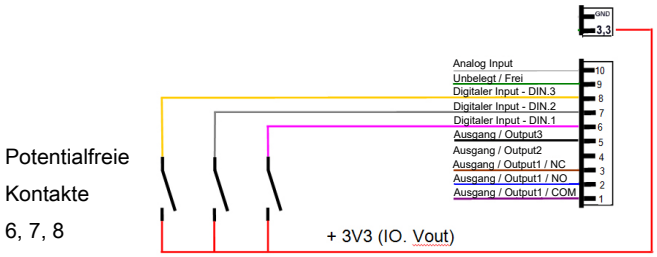
Die Beschaltung der Ein- und Ausgänge ist nur beim RouterNode2 (WNM.RN2.ER.IO) möglich.



12.3.7 Beschaltung IO-Connector

Die Beschaltung der Ein- und Ausgänge ist nur beim RouterNode2 (WNM.RN2.ER.IO) möglich.

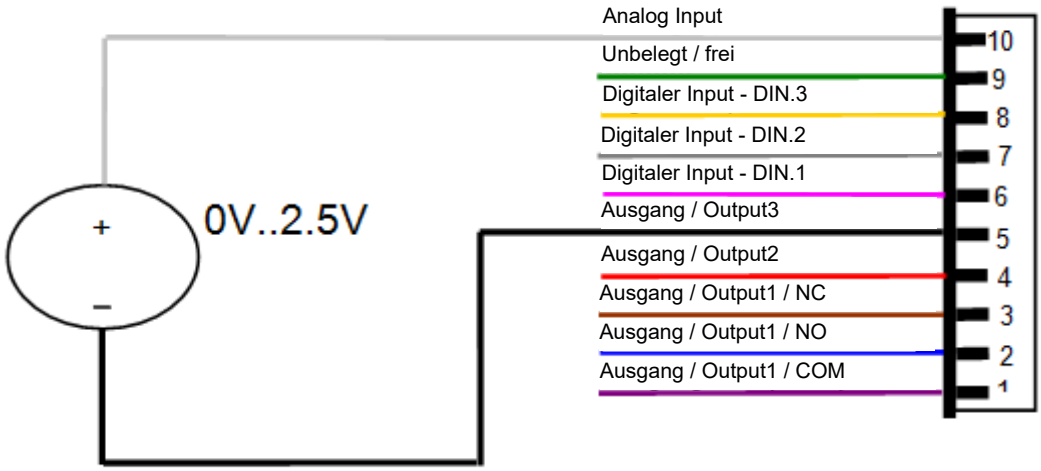
Einfache Kontaktauswertung



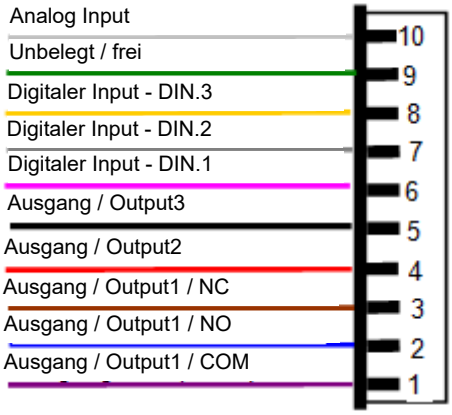
Handbuch MobileKey

Beschaltung digitaler Input (DIN 1 - 3): Zur Auswertung / Beschaltung potentialfreier Kontakte (Relais, Reedkontakte). Durch das Auslösen externer Kontakte können Inputänderungen bestimmte Funktionen ausführen.

Beschaltung analoger Input



Beschaltung Relaiskontakt (Ausgang 1)



Ausgang 1 (Relaisausgang potentialfrei)

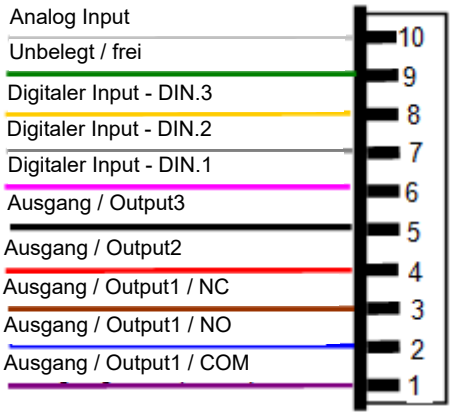
1 --> Common (Gemeinsamer)

2 --> Normally open (Schließer-Kontakt)

3 --> Normally closed (Öffner-Kontakt)

Handbuch MobileKey

Beschaltung Ausgänge 2/3



Ausgang 2/3

2 --> Masse-Kontakt

3 --> Masse-Kontakt

Dem Anwender stehen drei OpenDrain-Ausgänge zur Verfügung. Diese dürfen mit einem maximalen Strom von je 200 mA belastet werden. Beim Schalten von größeren Induktivitäten wird die Verwendung einer Freilaufdiode (z.B. 1N4148) empfohlen. Die Masse des Routers muss zwingend mit der Systemmasse verbunden sein. Maximale Leitungslänge der IO-Verdrahtung: 30 m. Gilt für DIN 1- 3 + Ausgang 2/3

Bezeichnung	**Erklärung**
Power Jack (5.5 mm)	Klinkenstecker von externer Quelle 9 – 24 VDC, polaritätsunabhängig
Abmessungen Platine (L*B)	93 x 76 mm (LxB)
RJ45 Ethernet 10/100	Ethernet Schnittstelle mit PoE 802.3af
RST-Button	Von außen zugänglicher Reset-Taster, mittels Büroklammer o.ä. auslösbar
IO-Connector	**Erklärung**
1. O1.COM	Ausgang 1: Relais C-Kontakt (C=Common), potentialfrei
2. O1.NO	Ausgang 1: Relais NO-Kontakt (Normally Open)
3. O1.NC	Ausgang 1: Relais NC-Kontakt (Normally Close)
4. O2	Ausgang 2: Open Collector
5. O3	Ausgang 3: Open Collector

Handbuch MobileKey

6. DI 1	Digitaler Input 1
7. DI 2	Digitaler Input 2
8. DI 3	Digitaler Input 3
9. Unbenutzt	Unbenutzt
10. Analog Input	Eingang für analoge Input-Signale

Bezeichnung	**Erklärung**
IO.Vout	Energieversorgung IO Connector
+3,3V	Pluspol max. 3,3V, kann als Input-Signal für DI1-3 verwendet werden
GND	Minuspol

Bezeichnung	**Erklärung**
RS485	Unbenutzt
V in	Spannungsversorgung von externer Quelle 9 – 24 VDC
GND	Minuspol
A	Datenleitung max. 900 m
B	Datenleitung max. 900 m

12.3.8 RouterNode zurücksetzen

Sehen Sie dazu auch

Konfiguration der IP-Settings [▸ 81]

12.3.8.1 Schließanlagen-Konfiguration zurücksetzen

Alle Schließanlageneinstellungen werden zurückgesetzt.

1. Spannungsversorgung entfernen *(ziehen des Netzsteckers)*.
2. 20 Sekunden warten.
3. Reset-Knopf drücken und gedrückt halten.
4. Spannung wieder zuführen *(anschließen des Netzsteckers)*.
5. Reset-Knopf nach 1 Sekunde loslassen.
6. Die Konfiguration wurde nun vollständig zurückgesetzt *(default)*.

12.3.8.2 IP-Konfiguration zurücksetzen

Alle IP-Konfigurationen (IP-Adresse, DHCP-Einstellungen und Hostname) werden auf die Werkseinstellungen [▸ 81] zurückgesetzt.

1. Spannungsversorgung entfernen *(ziehen des Netzsteckers)*.
2. 20 Sekunden warten.

Handbuch MobileKey

3. Reset-Knopf drücken und gedrückt halten.
4. Spannung wieder zuführen *(anschließen des Netzsteckers)*.
5. Reset-Knopf nach 5 Sekunden loslassen.
6. Die Konfiguration wurde nun vollständig zurückgesetzt *(default)*.

12.3.9 Technische Daten

Allgemein	
Gehäuse	ABS-Kunststoff, UV stabil,
Abmessungen (L*B*H)	172 x 86 x 33 mm (LxBxH)
Frequenzband	868,xx – 870 MHz
Farbe	9/118645 wie RAL 9016 (Verkehrsweiß)
Spannungsversorgung extern	geregeltes Netzteil 9 – 32 VDC, Klinkenstecker rund 5,5 mm
PoE	Power over Ethernet, unterstützt IEEE 802.3af
Leistung	max. 3 VA
Sendeleistung	10 dBm (ca. 10 mW) an Antennenbuchse
Leitungszuführung	Auf- oder Unterputzmontage möglich
Zugentlastung	3 x im Gehäuse
LED	In der Gehäusemitte
Wandmontage	Horizontale oder vertikale Gehäuseausrichtung möglich. Nicht auf Metall montieren. Von elektrischen bzw. magnetischen Störquellen fern halten.

Spannungsversorgung: Der Router (RouterNode 2 bzw. SmartBridge) kann die benötigte Versorgungsspannung über das Netzwerk beziehen (POE). Sollte im Netzwerk kein POE verfügbar sein, kann ein zusätzliches Netzteil angeschlossen werden.

Energieversorgung	
Externe Energieversorgung (Netzteil)	Eingangsspannung: 9 V DC min, 32 V DC max; (min. 3 W) Eingangsstrom: Abhängig von der Eingangsspannung (350 mA @ 8V) Polaritätsabhängig: Nein
PoE (Power over Ethernet)	IEEE802.3af, galvanisch isoliert, V_{in}:36 V to 57 V, P_{out} max. 10 W
Spannungsausgänge	1 x 3.0 – 3.3 V bei 200 mA max

Umwelt	
Temperatur	Betrieb: -10°C bis +55°C Lagerung: 0°C bis +30°C

Handbuch MobileKey

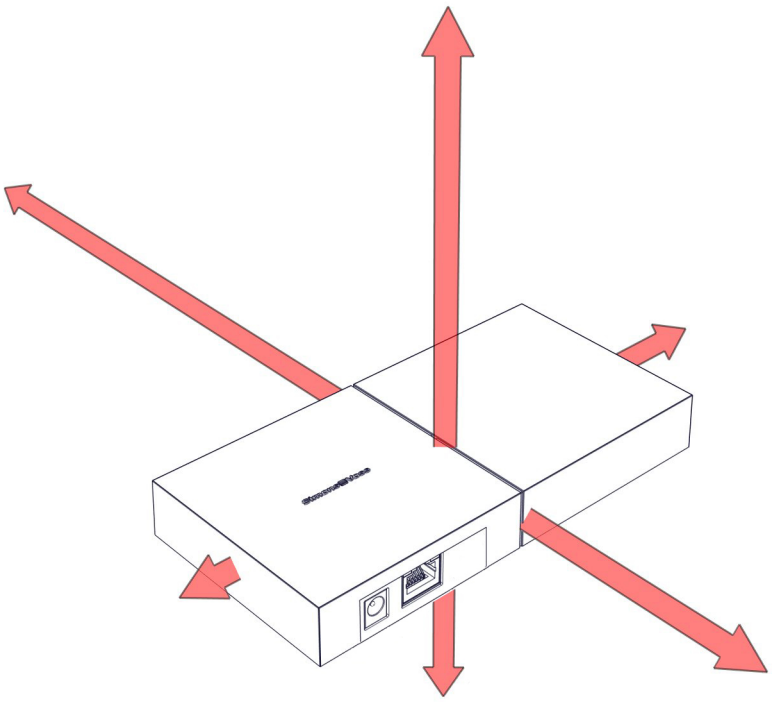
Luftfeuchtigkeit	Max. 90% ohne Kondensation
Umweltklasse	IP20
Schnittstellen	
TCP/IP	10T/100T, HP Auto_MDIX, DHCP Client, IPv4 TCP Service: 1x am Port 2101 UDP Service: 1x für Digi-Scan DHCP: on WebServer: enable Connector:RJ45
Frequenz	WaveNet 868 – 870 MHz, 10mW max. (10dBm)
Signalisiation	
LED	Eine dreifarbige LED: rot, grün, blau (in der Gehäusemitte)
Programmierung	
Schnittstellen	Über TCP/IP
Speicher	1MB intern
Relais für Ausgang 1 *(Nur WNM.RN2.ER.IO)*	
Anzahl	1 x
Betriebsart	Wechsler-Kontakt
Externer Ausgang über Relaiskontakt	1 x C, 1 x NO, 1 x NC. Max. Schaltspannung: 30 V DC, 24V AC (ohmsche Belastung) Max. Schaltstrom: 1A (ohmsche Belastung)
Digitale Eingänge (Inputs) *(Nur WNM.RN2.ER.IO)*	
Anzahl	3 x
Eingangsspannung	Low: 0 bis 0,5 V / High: 2 V bis 3.3 V max
Ext. Kontakt	Potentialfreier Kontakt kann zwischen Eingang (I1, I2, I3) und I_+ verbunden werden
Digitale Ausgänge (Outputs) *(Nur WNM.RN2.ER.IO)*	
Anzahl	2 x
Typ	Open Collector
Schaltspannung	12 V / 100mA max (ohmsche Belastung)
Energieversorgung	Ein “Pullup” Widerstand (ca... 1KOhm) kann zwischen jedem Ausgang und $Output_+$ verbunden werden ($V_{out} = V_{in} – 1V$)
Analoge Eingänge (Inputs) *(Nur WNM.RN2.ER.IO)*	

Handbuch MobileKey

Anzahl	1 x
Auflösung	12 bit
Eingangsspannung	0 bis 3,3V
Externe Antenne	
Ext. Antenne	Um die Reichweite zu erhöhen, kann über die SimonsVoss Technologies GmbH eine externe Antenne bestellt werden, welche direkt auf die Platine gesteckt wird.

12.3.10 Antenne

12.3.10.1 Antennenabstrahlung (interne Antenne)



12.3.10.2 Externe Antenne ANTENNA.EXT.868

Die Externe Antenne ANTENNA.EXT.868 ist als optionales Zubehör erhältlich!

Handbuch MobileKey

Die externe Antenne ANTENNA.EXT.868 ist für den Außeneinsatz ausgelegt, somit kann der Router im geschützten Bereich installiert werden und LockNodes im Außenbereich erreichen. Die Antenne wird über einen Anschluss auf der Platine des Routers angeschlossen.

Es ist keine weitere Konfiguration am Router oder in der Software nötig. Die interne Antenne wird durch den Anschluss der Antenne nicht deaktiviert.

Die Antenne hat einen Magnetfuß und wird inklusive Wandbefestigung, Dübel und Schrauben geliefert. Die Wandbefestigung dient der Befestigung des Magnetfußes der Antenne auf nichtmetallischem Untergrund.

12.3.10.3 Technische Daten ANTENNA.EXT.868 (Optional erhältlich)

Impedanz	50 Ohm
Polarisation	Linear
Verstärkung (max.)	2,2 dBi
VSWR	<3:1
Leistung	25W
Betriebstemperatur	-40°C bis +85°C
Höhe (max.)	71,95mm
Durchmesser (max.)	30,85mm
Kabellänge	ca. 5m

12.3.11 Spannungsversorgung

Spannungsversorgung: Das Gerät kann die benötigte Versorgungsspannung über das Netzwerk beziehen (POE). Sollte im Netzwerk kein POE verfügbar sein, kann ein zusätzliches Netzteil *(9 V bis 32 V DC, mindestens 3 W)* angeschlossen werden.

12.3.12 Konformitätserklärung

Dokumente wie Konformitätserklärungen und sonstige Zertifikate sind online unter www.my-mobilekey.com abrufbar.

12.3.13 Hilfe & Kontakt

Anleitungen

Detaillierte Informationen zum Betrieb und zur Konfiguration finden Sie auf der SimonsVoss-Homepage (www.simons-voss.com) im Supportbereich unter Infomaterial/Dokumente.

Hotline

Bei technischen Fragen hilft Ihnen die SimonsVoss Service-Hotline unter +49 (0) 89 99 228 333 (Anruf in das deutsche Festnetz, Kosten variieren je nach Anbieter).

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

hotline@simons-voss.com

Handbuch MobileKey

FAQ

Informationen und Hilfestellungen zu SimonsVoss-Produkten finden Sie auf der SimonsVoss-Homepage (www.simons-voss.com) im Supportbereich unter FAQ.

SimonsVoss Technologies GmbH
Feringastraße 4
85774 Unterföhring
Deutschland

12.4 Handbuch SmartRelais

12.4.1 Bestimmungsgemäßer Gebrauch

Bei den SimonsVoss SmartRelais handelt es sich um elektronische Schalter, welche mit entsprechenden Identmedien *(z.B. Transponder)* geschaltet werden können. Die Verwaltung der SmartRelais variiert je nach dem jeweiligen SmartRelais:

	VERWALTUNG	PROGRAMMIERUNG
3063	LSM-Basic, Business oder Professional	SMART.CD
	LSM-Starter	CD.STARTER *oder SMART.CD*
MobileKey	Web-Applikation	MK.CD.STARTER

Einige SmartRelais können optional über interne LockNodes mit entsprechenden Routern programmiert werden. Die Erstprogrammierung sollte in jedem Fall über ein Programmiergerät erfolgen.

SmartRelais dürfen nur für die in diesem Handbuch beschriebenen Zwecke eingesetzt werden. Ein anderer Gebrauch ist nicht zulässig und kann zur Beschädigung des SmartRelais führen.

HINWEIS SmartRelais sollten stets vor Einbau und Anschluss programmiert werden!

12.4.2 Sicherheitshinweise

⚠ WARNUNG Durch fehlerhaft installierte oder programmierte Schließungen kann der Zugang durch eine Tür versperrt werden. Für die Folgen fehlerhafter Installationen, wie nicht möglicher Zugang zu verletzten Personen, Sachschäden oder andere Schäden haftet die SimonsVoss Technologies GmbH nicht.

Handbuch MobileKey

⚠ WARNUNG

Die im digitalen SmartRelais eingesetzten Batterien können bei Fehlbehandlung eine Feuer- oder Verbrennungsgefahr darstellen. Die Batterien nicht aufladen, öffnen, erhitzen oder verbrennen! Batterien nicht kurzschließen!

HINWEIS

Für Beschädigungen der Türen oder anderen Komponenten durch fehlerhafte Montage übernimmt die SimonsVoss Technologies GmbH keine Haftung.

HINWEIS

Das SmartRelais darf nur für den vorgesehenen Zweck genutzt werden. Ein anderer Gebrauch ist nicht zulässig.

HINWEIS

Die Installation eines SimonsVoss Smart Relais setzt Kenntnisse in den Bereichen der Türmechanik, -zulassungen, Elektronikmontage und im Umgang mit der SimonsVoss Software voraus. Der Einbau darf nur durch geschultes Fachpersonal durchgeführt werden!

HINWEIS

Werden Smart Relais länger als eine Woche gelagert, ist die Backup Batterie zu entfernen.

HINWEIS

Die Installation der Smart Relais muss unter Einhaltung der ESD-Richtlinien (Elektrostatische Aufladung) vorgenommen werden. Insbesondere sind Berührungen der Platinen und der darauf befindlichen integrierten Schaltkreise zu vermeiden.

HINWEIS

Nach dem Einbau und oder dem Batteriewechsel des SmartRelais ist unbedingt ein Funktionstest durchzuführen!

HINWEIS

Änderungen bzw. technische Weiterentwicklungen vorbehalten.

HINWEIS

Die Dokumentation wurde nach bestem Wissen erstellt, evtl. Fehler können aber nicht ausgeschlossen werden. Hierfür kann keine Haftung übernommen werden.

HINWEIS

Sollten Abweichungen von Inhalten in Fremdsprachenversionen der Dokumentation bestehen, gilt im Zweifelsfalle das deutsche Original.

Handbuch MobileKey

HINWEIS Alle Anweisungen müssen beim Anschluss und Einbau des SmartRelais genau befolgt werden. Diese Anweisungen und jegliche Anweisungen bezüglich der Wartung sollten von der den Einbau vornehmenden Person an den Benutzer weitergegeben werden.

HINWEIS Der Batteriewechsel darf nur durch geschultes Fachpersonal durchgeführt werden!

HINWEIS Alte bzw. verbrauchte Batterien fachgerecht entsorgen, und nicht in Reichweite von Kindern aufbewahren!

HINWEIS Bei einem Batteriewechsel die Kontakte der neuen Batterien nicht mit den Händen berühren. Verwenden Sie hierzu saubere und fettfreie Handschuhe.

HINWEIS Es sind nur Batterien zu verwenden, welche von SimonsVoss freigegeben sind!

HINWEIS Ein Vertauschen der Polarität kann zu Beschädigungen des SmartRelais führen!

12.4.3 Allgemein

12.4.3.1 Versionen

SmartRelais sind in unterschiedlichsten Ausführungen für verschiedene Produktlinien ausgelegt. Prüfen Sie vor einer Bestellung genau, welches SmartRelais für Ihren Einsatz das Richtige ist.

SREL *(Schwarz)*		**SREL2** *(Weiß)*	
G1		**G2**	
SREL	SREL.G2	SREL.G2.W	Grundversion des SmartRelais 3063.
SREL.ZK	SREL.ZK.G2	SREL.ZK.G2.W	Wie die Grundversion des SmartRelais 3063, zusätzlich Zugangskontrolle und Zeitzonensteuerung.
SREL.ADV			Wie die ZK-Version des SmartRelais 3063, jedoch mit zusätzlichen Funktionen für die Ausgabe.

Handbuch MobileKey

		SREL2.G2.W	Grundversion des SmartRelais2 3063.
		SREL2.ZK.G2.W	Wie die Grundversion des SmartRelais2 3063, zusätzlich Zugangskontrolle und Zeitzonensteuerung.
		SREL2.ZK.MH.G2.W	Wie die ZK-Version des SmartRelais2 3063, zusätzlich Aufnahme eines internen MIFARE®-Kartenlesers sowie Anschlussmöglichkeit für maximal zwei weitere externe MIFARE®-Kartenleser.

Handbuch MobileKey

	SREL	SREL .ZK	SREL .ADV
Berechtigung bis zu 8.184 Transponder	X	X	X
Berechtigung für bis zu 64.000 Transponder			
Zugansgskontrolle		X	X
Erweiterte Anschlussmöglichkeiten			X
Mifare & Desfire Karten-Unterstützung			
Anschlussmöglichkeit für Externe Kartenleser			

	SREL .G2	SREL .ZK.G2	SREL .G2.W	SREL .ZK.G2.W
Berechtigung bis zu 8.184 Transponder				
Berechtigung für bis zu 64.000 Transponder	X	X	X	X
Zugansgskontrolle		X		X
Erweiterte Anschlussmöglichkeiten				
Mifare & Desfire Karten-Unterstützung				
Anschlussmöglichkeit für Externe Kartenleser				

	SREL2 .G2.W	SREL2 .ZK.G2.W	SREL2 .ZK.MH.G2.W
Berechtigung bis zu 8.184 Transponder			
Berechtigung für bis zu 64.000 Transponder	X	X	X
Zugansgskontrolle		X	X
Erweiterte Anschlussmöglichkeiten			
Mifare & Desfire Karten-Unterstützung			X
Anschlussmöglichkeit für Externe Kartenleser			X

Handbuch MobileKey

- **SmartRelais**

  Das SREL ermöglicht die reine Ja/Nein Berechtigung für maximal 8.184 verschiedene Transponder.

- **SmartRelais ZK**

  Wie die Basisversion (SREL), jedoch mit der Möglichkeit der getrennt zuschaltbaren Zutrittsprotokollierung der letzten 1.024 Zutritte (ab Firmwareversion 4.0.01.15) mit Datum und Uhrzeit, oder Tages – Zeitzonen für bis zu fünf Personengruppen sowie automatischer Ver- und Entriegelung.

- **Smart Relais Advanced Version**

  Wie die ZK-Version, jedoch mit folgenden zusätzlichen Funktionen:

  - Anschuss für externe Module über einen Drei-Draht-Bus.
  - Anschluss einer ausgelagerten Antenne.
  - Anschlüsse für serielle Schnittstellen zu externen Zeiterfassungsterminals oder Zutrittskontollesern.
  - Anschluss für externe LED oder Buzzer.

- **SmartRelais 2**

  Das SREL2.G2.W wird grundsätzlich mit Transpondern, also als rein „aktive“ Komponente betrieben. Es besteht aber auch die Möglichkeit, einen CompactReader zu verwenden, und somit das SREL2 mit Mifare Classic/DERFire®-Karten zu betreiben. Dieses SmartRelais ermöglicht die reine Ja/Nein Berechtigung für maximal 64.000 verschiedene Transponder.

- **SmartRelais 2 ZK**

  Wie die Basisversion (SREL2.G2), jedoch mit der Möglichkeit der getrennt zuschaltbaren Zutrittsprotokollierung der letzten 1.024 Zutritte mit Datum und Uhrzeit, oder Tages-Zeitzonen für bis zu 100 Personengruppen sowie automatischer Ver- und Entriegelung (Zeitumschaltung). Diese Version kann auch als Gateway in virtuellen Netzwerken eingesetzt werden.

- **SmartRelais 2 MH**

  Wie die ZK-Version. Zusätzlich können an diese Version zwei externe Kartenleser (SC.M.E.G2) sowie ein interner Kartenleser (SC.M.I.G2) angeschlossen werden. Mifare Classic/DERFire®-Karten können an diesem SREL2 betrieben werden.

12.4.3.2 Zubehör

SmartRelais können mit diversem Zubehör kombiniert werden. Prüfen Sie vor einer Bestellung genau, welches Kombinationsmöglichkeiten möglich sind.

Zubehör für SmartRelais 3063 G1

	SREL	SREL.ZK	SREL.ADV
MOD.SOM8			X

Handbuch MobileKey

SREL.AV			X
SREL.BAT	X	X	X

Zubehör für SmartRelais 3063 G2

	SREL.G2	SREL.ZK.G2	SREL.G2.W	SREL.ZK.G2.W
WNM.LNI.SREL.G2			X	X
SREL.BAT	X	X		
SREL.AV	X	X		
SREL2.COVER1			X	X

Zubehör für SmartRelais2 3063 *(G2)*

	SREL2.G2.W	SREL2.ZK.G2.W	SREL2.ZK.MH.G2.W
SREL.AV			X
WNM.LNI.SREL2.G2	X	X	X
SC.M.I.G2			X
SC.M.E.G2.W			X
SREL2.COVER1	X	X	X

– **SC.M.E.G2.W** *(SmartCard Mifare Extern G2 Weiß)*

  An ein SREL2.ZK.MH.G2.W oder SREL2.ZK.MH.G2.W.WP können maximal zwei externe Kartenleser (SC.M.E.G2.W) und ein interner Kartenleser (SC.M.I.G2) angeschlossen werden. Wenn zwei externe Kartenleser an ein SREL2 angeschlossen werden, dann muss an einem externen Kartenleser, ein Dip-Schalter auf Position „ON“ geschaltet werden! Der Dip-Schalter befindet sich auf dem Kartenleser rechts unterhalb des 26-poligen Steckers.

  Der Leitungstyp zum Verkabeln der Komponenten sollte z.B. CAT5 (FTP) oder besser entsprechen. Geschirmte Steuerleitungen können auch verwendet werden. Leitungslänge: max. 10m. Bei einer Leitungslänge > 3m für den externen Kartenleser, muss eine eigene Spannungsversorgung sowie eine eigene Leitungsführung gewählt werden.

– **SC.M.I.G2** *(SmartCard Mifare Intern G2)*

  Der interne Kartenleser wird direkt auf das SREL2 aufgesteckt.

– **SmartRelais 2 WP-Version**

  Wetterfeste Ausführung. Diese Option ist zusätzlich für alle SREL2 lieferbar. Die Leitungseinführung muss in Eigenverantwortung selbst abgedichtet werden. Hier empfiehlt es sich, geeignete Materialien wie z.B. Silikon oder andere beständige Dichtungsmittel zu verwenden. Das Gehäuse ist für IP65 ausgelegt.

Handbuch MobileKey

12.4.3.3 Spannungsversorgung

Für den Betrieb der digitalen SmartRelais 3063 wird eine stabile Spannungsversorgung benötigt. Netzteile sind nicht im Lieferumfang enthalten.

Optional können einige SmartRelais über Batterien (SREL.BAT) betrieben werden. In diesem Fall darf keine zusätzliche Spannungsversorgung angeschlossen werden!

	Gleichspannung	Wechselspannung
SREL	5V - 24V (max. 15W)	12V (max. 15W)
SREL2	9V - 24V (max. 15W)	Nicht möglich.

HINWEIS Setzen Sie keine Schaltnetzteile in der Nähe der Smart Relais ein!

12.4.3.4 Einbauposition festlegen

Die Reichweite Transponder zu Smart Relais (Lesereichweite) beträgt max. 1,5 m, kann aber durch metallene Umgebung (insbesondere durch starke Magnetfelder oder Aluminium) gedämpft werden.

Idealerweise wird ein Reichweitentest mit einem berechtigten Transponder und einem batteriebetriebenen SmartRelais vorgenommen.

12.4.3.5 Weitere Informationen

- Alle Kabel zum Anschluss an das Smart Relais sollen vom Typ IY(ST)Y ....x0,6 (paarig verdrilltes, abgeschirmtes Kabel) sein und eine maximale Kabellänge von 100m nicht überschreiten. Hierbei sind die Leitungsverluste bei der Dimensionierung der Spannungsversorgung zu berücksichtigen.
- Die technischen Daten der Ein- und Ausgänge sind zu berücksichtigen (siehe Technische Daten).
- Alle Kabel müssen entsprechend der Vorschriften des VDE verlegt und angeschlossen werden.

12.4.4 Inbetriebnahme

Überprüfung

1. Das SmartRelais auspacken und auf eventuelle Beschädigungen überprüfen.
2. Das SmartRelais an eine Spannungsversorgung oder Batterie anschließen.
3. Betätigen Sie das SmartRelais mit einem Transponder und testen Sie, ob das SmartRelais in irgendeiner Weise auf die Betätigung reagiert.

Handbuch MobileKey

Programmierung

Programmieren Sie das SmartRelais mit der entsprechenden Software, z.B. der LSM-Software bei SmartRelais 3063. Das SmartRelais muss für den Programmiervorgang mit einer Spannungsquelle verbunden sein. Details zur Programmierung in der LSM-Software finden Sie hier: Konfigurationen in der Software [▸ 100]

Anschluss und Einbau

✓ Das SmartRelais ist mit keiner Spannungsquelle verbunden und befindet sich im stromlosen Zustand.

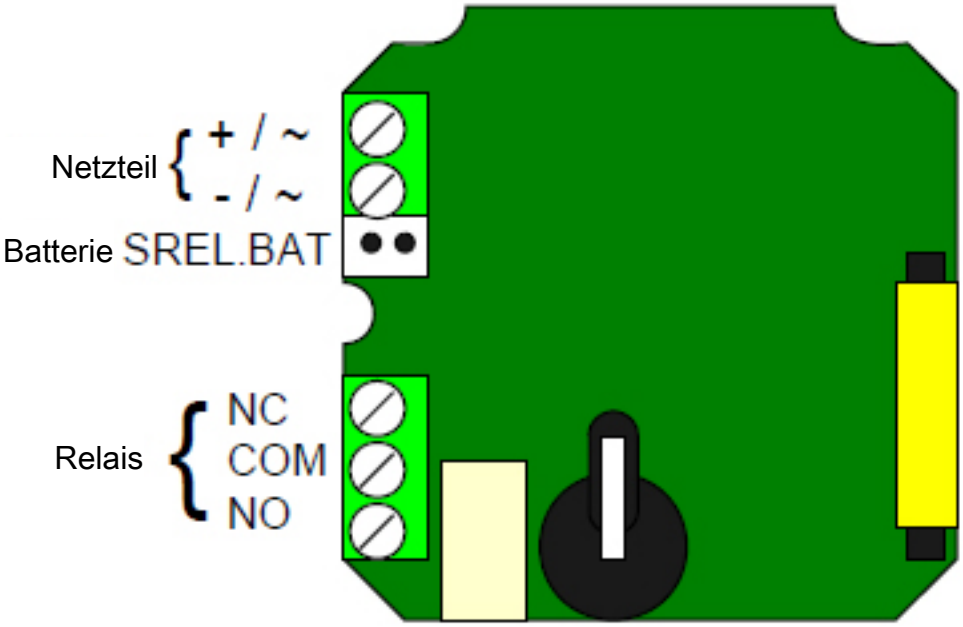
1. Backup-Batterie einsetzen: **Der Pluspol der 3V-CR1220-Batterie zeigt in jedem SmartRelais nach oben.**
2. Alle Kabel an die vorgesehenen Klemmen des Smart Relais anschließen (siehe Anschlüsse)
3. Die Spannungsversorgung einschalten (gegebenenfalls Stecker einstecken oder Batterie anklemmen).
4. Funktion des programmierten SmartRelais mit einem berechtigten Transponder testen.
5. SmartRelais einbauen.
   - ⇨ Bei Einbau in eine Unterputzdose ist das Gehäuse zu entfernen. Die Platinen der SmartRelais weisen zwei verschiedene Größen auf. Überprüfen Sie vor der Montage, ob die Platine des SmartRelais in Ihre Unterputzdose passt!
   - ⇨ Bei Aufputzmontage kann die Bodenplatte als Schablone für die Bohrungen (6 mm) verwendet werden.

HINWEIS Wenn das SmartRelais mit einer Batterie (SREL.BAT) betrieben wird, darf die Backup-Batterie nicht eingesetzt werden!

Handbuch MobileKey

12.4.5 Anschlüsse

12.4.5.1 SmartRelais (SREL)



NAME	SYMBOL	BESCHREIBUNG
Netzteil	+	Wahlweise Pluspol bei Anschluss einer Gleichspannung (5 bis 24 VDC) oder einer der beiden Wechselspannungsanschlüsse (12 VAC)
Netzteil	-	Wahlweise Minuspol bei Anschluss einer Gleichspannung (5 bis 24 VDC) oder der zweite Wechselspannungsanschluss (12 VAC)
Batterie		Steckeranschluss für eine Batterie (bei Betrieb ohne Netzteil) Bestellcode der Batterie inkl. Stecker SREL.BAT
Relais NC		Normally Closed Kontakt des Wechsler Relais. Dieser Kontakt ist im nicht geschalteten Fall geschlossen gegen Relais COM
Relais COM		Common Kontakt des Wechsler Relais. Dieser Kontakt wird entweder gegen Relais NC verdrahtet (Öffner) oder gegen Relais NO (Schließer)

Handbuch MobileKey

Relais NO	Normally Open Kontakt des Wechsler Relais. Dieser Kontakt ist im geschalteten Fall geschlossen gegen Relais COM

Handbuch MobileKey

12.4.5.2 Anschlussbemerkungen SREL2

SREL2.G2 mit drei Karteninterfaces

Es ist möglich, das SREL2 mit insgesamt 3 Karteninterfaces (1x intern und 2x extern) gleichzeitig zu betreiben. Für einen solchen Betrieb muss der Dip-Schalter auf dem internen Karteninterface auf 1 (ON)gestellt werden!

Externer Trigger für SREL2.G2

Wenn an F1 eine Spannung von +3 bis +24 Volt (DC) als Impuls angelegt wird, löst das SREL2 aus. Hierdurch kann beispielsweise die OMRON-Funktion realisiert werden.

Externe LED oder Buzzer an SREL2.G2

An den Anschlüssen F3 und PLUS (+) kann eine externe LED oder ein Buzzer angeschlossen werden. Die Spannung an F3 und PLUS entspricht der Versorgungsspannung. Deswegen muss die Spannung ggf. durch einen geeigneten Vorwiderstand herabgesetzt werden.

12.4.6 Konfigurationen in der Software

SmartRelais sind hardwarebedingt sehr spezifisch und können deshalb nur in der für sie vorgesehenen Umgebung betrieben werden.

<table>
<tr><th>Artikelnummer</th><th>Protokollgeneration</th><th>Software</th></tr>
<tr><td>SREL</td><td rowspan="3">G1: Nur Schließanlagen vom Typ "G1" oder "G2+G1"</td><td rowspan="10">LSM</td></tr>
<tr><td>SREL.ZK</td></tr>
<tr><td>SREL.ADV</td></tr>
<tr><td>SREL.G2</td><td rowspan="7">G2: Nur Schließanlagen vom Typ "G2"</td></tr>
<tr><td>SREL.ZK.G2</td></tr>
<tr><td>SREL.G2.W</td></tr>
<tr><td>SREL.ZK.G2.W</td></tr>
<tr><td>SREL2.G2.W</td></tr>
<tr><td>SREL2.ZK.G2.W</td></tr>
<tr><td>SREL2.ZK.MH.G2.W</td></tr>
<tr><td>MK.SREL2.ZK.G2.W</td><td rowspan="2">MobileKey</td><td rowspan="2">MobileKey</td></tr>
<tr><td>MK.SREL2.LN.ZK.G2.W</td></tr>
</table>

12.4.6.1 LSM

Die Einstellungen des SmartRelais können in den Eigenschaften der Schließung in der Registerkarte "Konfiguration/Daten" vorgenommen werden.

Schließungseigenschaften: Konfiguration/Daten: SmartRelais (G1)

Diese Registerkarte ist in zwei Seiten aufgeteilt:

– Die linke Seite zeigt den Soll-Zustand der Schließung - also der in der LSM Software konfigurierte und gewollte Zustand.

Handbuch MobileKey

– Auf der rechten Seite wird der Ist-Zustand der Schließung angezeigt - also der Zustand, der zuletzt programmiert wurde.

Folgende Merkmale können **je nach Schließungstyp** aktiviert werden:

– **Zugangskontrolle**

  Nur bei SREL.ZK und SREL.ADV möglich. Die jeweils letzten 1.024 Transponderbetätigungen werden mit Datum und Uhrzeit gespeichert.

– **Zeitzonensteuerung**

  Nur bei SREL.ZK und SREL.ADV möglich. Ein Zeitzonenplan kann geladen werden und die Transponder werden dann entsprechend ihrer Zeitzonengruppe zugelassen bzw. gesperrt.

– **Overlay**

  Ersatztransponder können ihre Ursprungstransponder überschreiben. Nach der erstmaligen Betätigung mit einem Ersatztransponder, ist der Ursprungstransponder gesperrt.

– **FlipFlop**

  Der Impulsmodus (Default Einstellung) wird abgeschaltet, die Impulsdauer spielt keine Rolle mehr. Das SmartRelais wechselt bei eingeschaltetem FlipFlop-Modus seinen Zustand bei jeder Transponderbetätigung von AN nach AUS oder umgekehrt. Dieser Modus empfiehlt sich zum Schalten von Licht oder Maschinen etc.

  Bei einer solchen Installation ist gegebenenfalls darauf zu achten, dass die Netzteile und Türöffner für Dauerstrombetrieb geeignet sind.

– **Repeater**

  Das SmartRelais empfängt ein Transpondersignal und sendet dieses verstärkt weiter. In dieser Funktion kann das SmartRelais verwendet werden, um größere Funkstrecken zu überbrücken. Die Entfernung zu einem anderen SmartRelais kann bis zu 2 m betragen.

– **Zeitumschaltung**

  Nur für SREL.ZK und SREL.ADV. Wenn die Zeitumschaltung aktiviert wird, muss ein Zeitzonenplan geladen werden, der eine generelle Freischaltung des SmartRelais während der markierten Zeiten (in Gruppe 5) ermöglicht. Also kann eine Tür tagsüber frei begehbar sein und nachts nur über Transponder geöffnet werden.

  Bei einer solchen Installation ist darauf zu achten, dass die Netzteile und Türöffner für Dauerstrombetrieb geeignet sind

– **OMRON**

  Nur für SREL.ADV. Viele Zutrittskontroll- und Zeiterfassungssysteme besitzen serielle Schnittstellen zum Anschluss von Kartenlesern. Über diese Schnittstellen ist auch der Anschluss eines SmartRelais möglich. Damit können Sie den SimonsVoss Transponder auch in Fremdsystemen benutzen.

Handbuch MobileKey

Möchten Sie, dass das SmartRelais die Transponderdaten zu einem Fremdsystem überträgt, und bei Freischaltung durch das Fremdsystem vom SmartRelais ein Fernöffnungsbefehl zu einem Zylinder gesendet wird, dann wählen sie diese Option sowohl am SmartRelais als auch am Zylinder.

Der Typ des externen Systems ist unter „Schnittstellen“ einzustellen. Klicken Sie hierfür auf die Schaltfläche "Erweiterte Konfiguration".

Über die Schalfläche "Erweiterte Konfiguration" können einige Einstellungen präzisiert werden:

- **Pulslänge**

  Hier geben Sie den Wert für die Impulsdauer des Schaltimpulses in Sekunden an. Der Wert kann 0,1 bis 25,5 Sekunden betragen. Wenn sie zum Beispiel 3 Sekunden eintragen, dann wird ein Türöffner für 3 Sekunden frei geschaltet, bevor er wieder sperrt.

- **Begrenzte Reichweite**

  Bei Auswahl dieser Option wird die Lesereichweite Transponder zu SmartRelais von ca. 1,5 m auf ca. 0,4 m begrenzt. Diese Option kann z.B. benutzt werden, wenn sich mehrere SmartRelais in unmittelbarer Nähe zueinander befinden, und einzelne Transponder an mehreren SmartRelais berechtigt sind.

- **Unberechtigte Zutrittsversuche protokollieren**

  Nur für SREL.ZK und SREL.ADV: Normalerweise werden nur berechtigte Transponderbetätigungen protokolliert. Wenn gewünscht wird, auch den Versuch der Türöffnung mit einem unberechtigten Transponder zu erfassen, muss diese Option gewählt werden.

- **Anzahl Erweiterungsmodule**

  Hier geben Sie die Anzahl der an das SmartRelais angeschlossenen externen Module an. Diese Module werden an die Klemmen RS-485 C OM, RS-485 A und RS-485 B angeschlossen.

- **Schnittstelle**

  Nur bei SREL.ADV: Für den Betrieb als Serielle Schnittstelle können Sie hier die Art des Kartenlesers einstellen, den das SmartRelais simulieren soll.

  Als Optionen stehen zur Verfügung:

  - Wiegand 33 bit
  - Wiegand 26 bit
  - Primion
  - Siemens
  - Kaba Benzing
  - Gantner Legic

Handbuch MobileKey

  - Isgus
- **Keine akustischen Programmierquittungen**

  Nur bei SREL.ADV: Wenn gewünscht wird, dass bei einer Programmierung des SmartRelais keine Programmierquittungen über einen angeschlossenen Buzzer/Piepser gegeben werden sollen, dann ist dieses Feld anzukreuzen.
- **Externer Piepser / Externe LED**

  Nur bei SREL.ADV: Hier wird angegeben, welche externe Baugruppe angeschlossen ist. Das SmartRelais erzeugt im FlipFlop-Mode bei einer externen LED ein Dauersignal im geschalteten Zustand, während bei einem angeschlossenen Piepser nur jeder Zustandswechsel kurz mit einem Tonsignal quittiert wird.
- **Interne / Externe Antenne**

  Nur bei SREL.ADV
  - **Autodetektion**

    Ist eine externe Antenne angeschlossen, wird nur diese benutzt. Das SmartRelais schaltet dann die interne Antenne aus. Wenn keine externe Antenne angeschlossen ist (Standardfall), dann arbeitet das SmartRelais mit der internen Antenne.
  - **Beide aktiv**

    Das SmartRelais kann Buchungen von Transpondern an beiden Antennen bewerten.

Schließungseigenschaften: Konfiguration/Daten: SmartRelais (G2)

Diese Registerkarte ist in zwei Seiten aufgeteilt:

- Die linke Seite zeigt den Soll-Zustand der Schließung - also der in der LSM Software konfigurierte und gewollte Zustand.
- Auf der rechten Seite wird der Ist-Zustand der Schließung angezeigt - also der Zustand, der zuletzt programmiert wurde.

Folgende Merkmale können **je nach Schließungstyp** aktiviert werden:

- **Pulslänge**

  Hier geben Sie den Wert für die Impulsdauer des Schaltimpulses in Sekunden an. Der Wert kann 0,1 bis 25,5 Sekunden betragen. Wenn sie zum Beispiel 3 Sekunden eintragen, dann wird ein Türöffner für 3 Sekunden frei geschaltet, bevor er wieder sperrt.
- **Zugangskontrolle**

  ZK und ADV möglich. Die jeweils letzten Transponderbetätigungen werden mit Datum und Uhrzeit gespeichert.
- **Zeitzonensteuerung**

Handbuch MobileKey

Nur bei ZK und ADV möglich. Ein Zeitzonenplan kann geladen werden und die Transponder werden dann entsprechend ihrer Zeitzonengruppe zugelassen bzw. gesperrt.

– **Unberechtigte Zutrittsversuche protokollieren**

  Nur für ZK und ADV: Normalerweise werden nur berechtigte Transponderbetätigungen protokolliert. Wenn gewünscht wird, auch den Versuch der Türöffnung mit einem unberechtigten Transponder zu erfassen, muss diese Option gewählt werden.

– **Gateway**

  Das SmartRelais kann als Gateway genutzt werden.

– **FlipFlop**

  Der Impulsmodus (Default Einstellung) wird abgeschaltet, die Impulsdauer spielt keine Rolle mehr. Das SmartRelais wechselt bei eingeschaltetem FlipFlop-Modus seinen Zustand bei jeder Transponderbetätigung von AN nach AUS oder umgekehrt. Dieser Modus empfiehlt sich zum Schalten von Licht oder Maschinen etc.

  Bei einer solchen Installation ist gegebenenfalls darauf zu achten, dass die Netzteile und Türöffner für Dauerstrombetrieb geeignet sind.

– **Interne Antenne immer an**

  Auch wenn eine externe Antenne angeschlossen, wird trotzdem die interne Antenne parallel weiter benutzt.

– **Nahbereichsmodus (nur bei interner Antenne)**

  Der Nahbereichsmodus wird aktiviert.

– **Zeitumschaltung**

  Nur für ZK und ADV. Wenn die Zeitumschaltung aktiviert wird, muss ein Zeitzonenplan geladen werden, der eine generelle Freischaltung des SmartRelais während der markierten Zeiten (in Gruppe 5) ermöglicht. Also kann eine Tür tagsüber frei begehbar sein und nachts nur über Transponder geöffnet werden.

  Bei einer solchen Installation ist darauf zu achten, dass die Netzteile und Türöffner für Dauerstrombetrieb geeignet sind

Über die Schalfläche "Erweiterte Konfiguration" können einige Einstellungen präzisiert werden:

– **Schnittstelle**

  Für den Betrieb als Serielle Schnittstelle können Sie hier die Art des Kartenlesers einstellen, den das SmartRelais simulieren soll.

  Als Optionen stehen zur Verfügung:

  – Wiegand 33 bit
  – Wiegand 26 bit
  – Primion

  - Siemens
  - Kaba Benzing
  - Gantner Legic
  - Isgus
- **Externer Piepser / Externe LED**

  Nur bei SREL.ADV: Hier wird angegeben, welche externe Baugruppe angeschlossen ist. Das SmartRelais erzeugt im FlipFlop-Mode bei einer externen LED ein Dauersignal im geschalteten Zustand, während bei einem angeschlossenen Piepser nur jeder Zustandswechsel kurz mit einem Tonsignal quittiert wird.
- **Ausgänge invertieren**

  Über diese Einstellungen können Sie den Relaisausgang invertieren.

12.4.6.2 MobileKey

In der Web-App von MobileKey kann ein (MK-) SmartRelais schnell konfiguriert werden. Im Regelfall wird nur zwischen einer Öffnungsdauer oder einer Daueröffnung (FlipFlop) unterschieden. Optional kann ein LockNode eingestellt werden, um das SmartRelais über eine SmartBride zu verbinden.

12.4.7 Signalisation

SREL

- LED leuchtet oder blinkt grün: Identmedium ist berechtigt und das SREL schaltet.
- Keine Reaktion der LED: Identmedium abgewiesen oder nicht erkannt.

SREL2

- LED leuchtet oder blinkt blau: Identmedium ist berechtigt und das SREL2 schaltet.
- LED blinkt rot: Identmedium abgewiesen.

12.4.8 Wartung

12.4.8.1 Batteriewarnung und Batteriewechsel bei Einsatz von SREL.BAT

Für den Fall, dass die Batteriekapazität nicht mehr ausreicht, kann ein SmartRelais eine Batteriewarnung wie folgt abgeben:

- **SREL, SREL.ZK und SREL.ADV**
  - Interne LED blinkt 8x bei jeder Transponderbetätigung und vor dem Schalten des SmartRelais.
  - Diese LED sollte im Falle des Batteriebetriebs von außen sichtbar sein.
- **Nur SREL.ADV**

Handbuch MobileKey

– Externe LED blinkt 8x oder externer Buzzer piepst 8x bei jeder Transponderbetätigung.

HINWEIS Nach einer Batteriewarnung sind noch ca. 100 Betätigungen möglich. Die Batterie muss schnellstens gewechselt werden!

12.4.8.2 Backup-Batterie

Eine entladene Backup-Batterie kann zu einem Stehenbleiben der internen Uhr bei SmartRelais führen. Daher wird empfohlen, in regelmäßigen Abständen die Uhrzeit zu überprüfen. Eine Backup-Batterie hält ohne Stromunterbrechung des SmartRelais ca. 10 Jahre. Falls das Smart Relais im Falle häufiger Stromausfälle die Backup-Batterie oft benötigt, sollte regelmäßig diese Batterie erneuert werden.

HINWEIS Wenn das SmartRelais mit einer Batterie (SREL.BAT) betrieben wird, darf die Backup-Batterie nicht eingesetzt werden!

12.4.9 Technische Daten

12.4.9.1 Technische Daten SREL

Gehäuse aus schwarzem Kunststoff: Abmessungen LxBxH	72 x 57 x 25,5 mm
Schutzart	IP 20 nicht für Außeneinsatz getestet
Temperatur	Betrieb bei: -22°C bis 55°C Lagerung bei: 0°C bis 40°C
Luftfeuchtigkeit	<95% ohne Betauung
Leiterplatte Abmessungen LxBxH	50 x 50 x 14 mm
Netzspannung	12 VAC oder 5-24VDC (kein Verpolungsschutz)
Leistungsbegrenzung	Netzteil muss auf 15 VA begrenzt sein
Ruhestrom	< 5 mA
Max. Strom	< 100 mA
Impulsdauer programmierbar	0,1 bis 25,5 Sekunden
Ausgangsrelais Typ	Wechsler
Ausgangsrelais Dauerstrom	Max. 1,0 A
Ausgangsrelais Einschaltstrom	Max. 2,0 A
Ausgangsrelais Schaltspannung	Max. 24 V
Ausgangsrelais Schaltleistung	10^6 Betätigungen bei 30 VA
Multifunktionsanschlüsse F1, F2, F3	Max. 24 VDC, max. 50 mA

Handbuch MobileKey

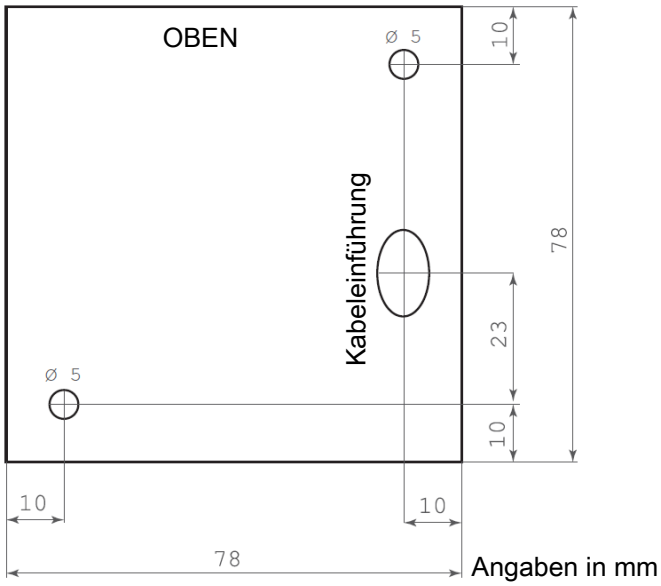
Vibrationen	15G für 11 ms, 6 Schocks nach IEC 68-2-27 nicht für den Dauereinsatz unter Vibrationen freigeben

12.4.9.2 Technische Daten SREL2

Gehäuse aus weißem Kunststoff: Abmessungen LxBxH Grundplatte semitransparent	ca. 78 x 78 x 19 mm
Schutzart	IP 20 nicht für Außeneinsatz getestet WP Version: IP65
Temperatur	Betrieb bei: -22°C bis 55°C Lagerung bei: 0°C bis 40°C
Luftfeuchtigkeit	<95% ohne Betauung
Leiterplatte Abmessungen LxBxH	50 x 50 x 14 mm
Netzspannung	9-24 V DC
Leistungsbegrenzung	Netzteil muss auf 15 VA begrenzt sein
Ruhestrom	< 100 mA
Max. Strom	< 300 mA
Impulsdauer programmierbar	0,1 bis 25,5 Sekunden
Ausgangsrelais Typ	Schließer
Ausgangsrelais Dauerstrom	Max. 1,0 A
Ausgangsrelais Einschaltstrom	Max. 2,0 A
Ausgangsrelais Schaltspannung	Max. 24 V
Ausgangsrelais Schaltleistung	10^6 Betätigungen bei 30 VA
Multifunktionsanschlüsse F1, F2, F3	Max. 24 VDC, max. 50 mA
Vibrationen	15G für 11 ms, 6 Schocks nach IEC 68-2-27 nicht für den Dauereinsatz unter Vibrationen freigeben

Handbuch MobileKey

12.4.9.3 Bohrbild SREL2 Weiß



12.5 Handbuch Programmierstick

12.5.1 Bestimmungsgemäßer Gebrauch

Der USB-Programmierstick ist ein kompaktes Programmiergerät, welches zur Programmierung von aktiven SimonsVoss Schließkomponenten *(z.B. Transponder oder Schließzylinder)* über einen Computer mit Windows-Betriebssystem dient.

- **CD.STARTER.G2**

  Für die Programmierung von Schließkomponenten aus dem System 3060 über die LSM STARTER.

- **MK.CD.STARTER.G2**

  Für die Programmierung von MobileKey-Schließkomponenten über die Web-Applikation. Der USB-Programmierstick kann außerdem an Android-Geräten (mit OTG-Funktion) betrieben werden.

12.5.2 Sicherheitshinweise

⚠ WARNUNG

Durch fehlerhaft installierte oder programmierte Schließungen kann der Zugang durch die Tür versperrt werden. Für die Folgen fehlerhafter Installation, wie nicht möglicher Zugang zu verletzten Personen, Sachschäden oder anderen Schäden, haftet die SimonsVoss Technologies GmbH nicht.

Handbuch MobileKey

HINWEIS Direkte Sonneneinstrahlung vermeiden.

HINWEIS Von magnetischen Störquellen fernhalten.

12.5.3 Lieferumfang

- CDStarter Programmiergerät
- USB-Kabel Stecker A / Buchse A
- Kurzanleitung

12.5.4 Inbetriebnahme

Der Treiber wird ab der Version 3.3 der LSM-Software automatisch installiert. Alternativ ist der Treiber auf der SimonsVoss-Homepage (www.simons-voss.com) im Supportbereich unter Infomaterial/Software-Downloads zu finden. Nach der Installation des Treibers ist das Programmiergerät einsetzbar.

12.5.5 Programmierung

Beachten Sie unbedingt das Systemhandbuch Ihres Systems:

- LSM Starter: www.simons-voss.com im Supportbereich unter Infomaterial/Dokumente.
- MobileKey: www.my-mobilekey.com im Infocenter unter Dokumente.

12.5.5.1 Programmierung über LSM STARTER

Auf dem Rechner muss eine aktuelle Version der LSM Starter installiert sein. Schließen Sie den Programmierstick an. Platzieren Sie die zu programmierenden Komponenten in einem Abstand von 10-30cm zum Programmiergerät und führen Sie die Programmierroutinen durch.

Sollten Sie eine Fehlermeldung bekommen, dass keine Hardware gefunden wurde, prüfen Sie zuerst ob der Programmierstick ordnungsgemäß angeschlossen ist und dann in der Software unter „Programmierung / Config Device testen“ ob der CDStarter erkannt wird. Bei einer weiteren Fehlermeldung ziehen Sie das Programmiergerät aus der USB Buchse und stecken Sie es erneut ein. Bei dieser Aktion wird der Treiber neu geladen.

Handbuch MobileKey

12.5.5.2 Programmierung über MobileKey

Melden Sie sich an der Web-App an und wählen Sie *"Menü/ Programmieren"*. Für die Programmierung über die Web-Applikation muss die Programmier-App installiert werden. Die Setupdatei wird über einen Link zum Download angeboten.

Sofern die Programmier-App bereits installiert ist, können Sie diese direkt über die Schaltfläche *"APP STARTEN"* starten und mit dem Programmieren beginnen.

12.5.5.3 Programmierdistanzen

- Der Abstand zwischen dem USB-Programmierstick und aktiver Komponente (z.B. Schließzylinder oder Transponder) sollte ca. 20 cm betragen.
- Achten Sie darauf, dass sich keine anderen aktiven Komponenten während des Programmier- oder Auslesevorgangs in unmittelbarer Nähe (Radius ca. 1,5 m zum USB-Programmierstick) befinden.

12.5.6 Technische Daten

Programmierung:	SimonsVoss Aktiv-Technologie 25kHz
LSM Version:	LSM Starter ab LSM 3.2 SP1
Betriebssystem:	Ab Windows XP SP3
USB Schnittstelle:	USB Typ A, USB 2.0
Abmessungen:	LxBxH 57(70)x19x13 mm
Reichweite:	10 - 30cm
Stromversorgung:	Via USB Stecker, keine interne Batterie
Schutzart:	IP40
Temperaturbereich:	-10 bis +60°C
Luftfeuchte:	95% (nicht kondensierend)