MobileKey

Handbuch

09.09.2019

SimonsVoss technologies

Inhaltsverzeichnis

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**
  - 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**

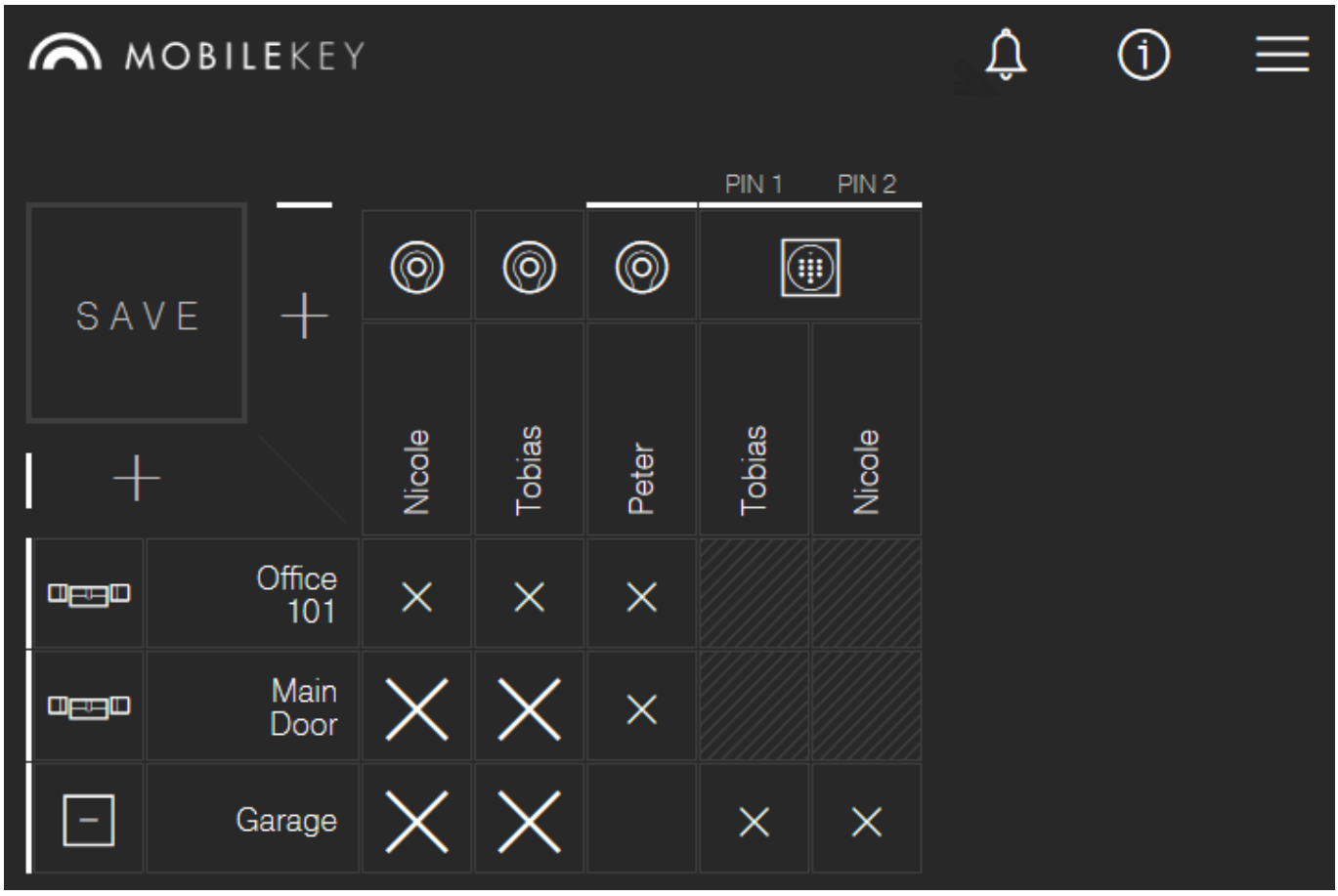
  Schlösser können auch online ohne USB-Programmierstick programmiert werden. Siehe *Programmieren von Komponenten [▸ 24]*. *In diesem Fall müssen nur noch die Transponder mit Hilfe des USB-Programmiersticks programmiert werden.*

  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 [▸ 43]*.

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.
×	**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 [▸ 38]*
- *Hilfe zur SmartBridge [▸ 37]*

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

Dieses Kapitel beschreibt die Einrichtung einer PinCode-Tastatur ohne Online-Erweiterung. Wenn Sie eine PinCode-Tastatur mit Online-Erweiterung haben, gehen Sie bitte wie im Kapitel *Online-PinCode-Tastatur anlegen [▸ 22]* beschrieben vor.

✓ PinCode-Tastatur bereits konfiguriert; siehe Konfiguration *(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 "PINCODE-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

Programmieren Sie jedes Schloss bzw. jede Online-PinCode-Tastatur vor dem Einbau!

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.

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 [▸ 5]*

Sehen Sie dazu auch

➡ *Programmierung [▸ 5]*

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 [▸ 5]*

Sehen Sie dazu auch

- *Programmierung [▸ 5]*

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 [▸ 5]*

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. MobileKey-Schließungen protokollieren bis zu 500 Zutritte. Wenn danach weitere Zutritte erfolgen, werden die ältesten Zutritte überschrieben. 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

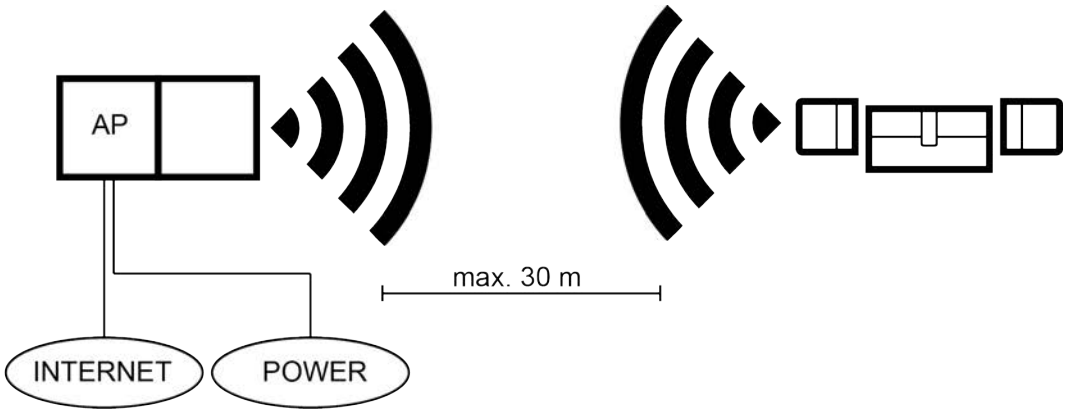
Beachten Sie, dass mit MobileKey maximal 10 SmartBridges eingesetzt werden können.

4.1.1 SmartBridges aufstellen

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

4.1.1.1 Eine SmartBridge

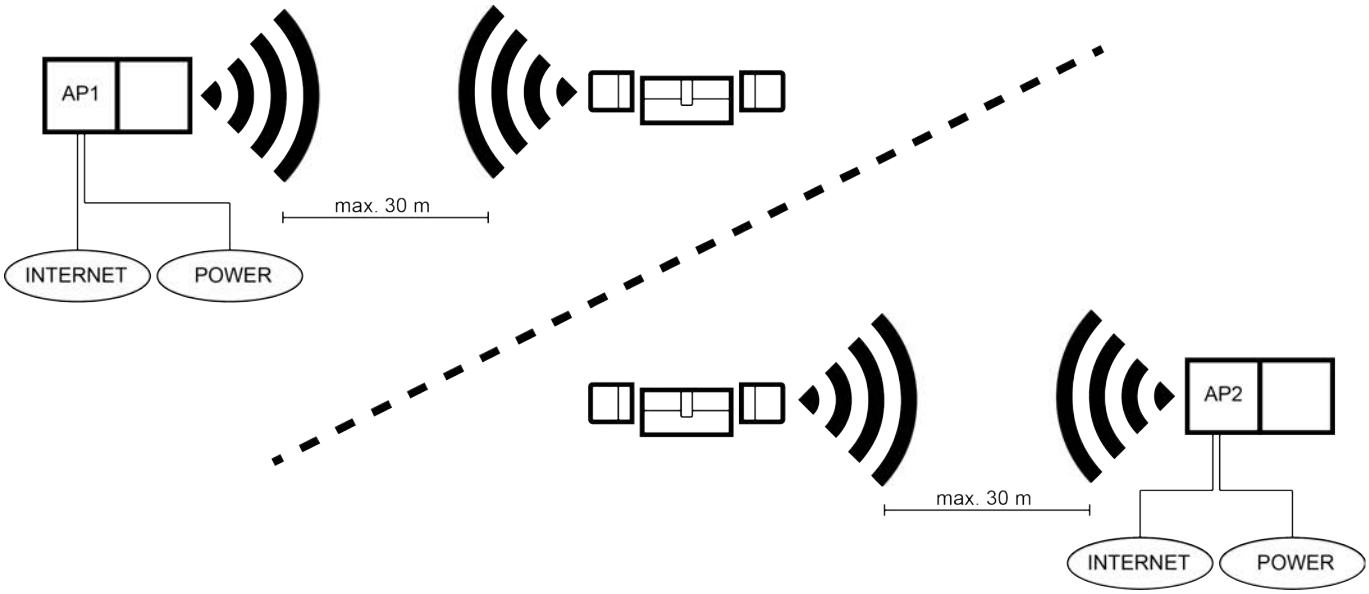
Der Einsatz einer als Accesspoint konfigurierten SmartBridge ist der einfachste Anwendungsfall für MobileKey ONLINE.



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 Smart-Bridges 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. 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) wird ausgeführt. Die SmartBridge kann 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 [▸ 19])*

✓ 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 [▸ 19])*
✓ 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-PinCode-Tastatur anlegen

✓ Online-PinCode-Tastatur bereits konfiguriert (siehe Konfiguration).
✓ Schloss für Online-PinCode-Tastatur bereits angelegt (siehe *Schloss mit Netzwerkknoten (LockNode) einrichten [▸ 20]*).
✓ Matrixansicht geöffnet.

1. Klicken Sie auf das Schlüssel-hinzufügen-Symbol (PLUS neben der "SAVE"-Schaltfläche).
2. Typ [PINCODE-Tastatur] auswählen.
3. Aktivieren Sie die Option ◉ ONLINE VERSION.
4. Geben Sie die Chip-ID ein.
5. Öffnen Sie das Dropdown-Menü ▼ Schloss.
6. Legen Sie das Schloss fest, an dem die Online-PinCode-Tastatur betrieben wird.
7. Geben Sie einen Namen für eine PIN ein, z.B. "Hans Müller".
8. Geben Sie eine User-PIN ein.
9. Geben Sie auf dieselbe Weise weitere PINs ein.

HINWEIS

Wenn Sie weitere User-PINs anlegen wollen, dann müssen Sie zuerst die entsprechende Checkbox aktivieren.

HINWEIS

Bis zu drei User-PINs können in der MobileKey Web-App eingerichtet und einem Schloss zugewiesen werden.

10. Klicken Sie auf die Schaltfläche SPEICHERN oder SPEICHERN + KOPIEREN.
    ↳ SPEICHERN speichert die Online-PinCode-Tastatur und navigiert zurück zur Matrixansicht.
    ↳ SPEICHERN + KOPIEREN speichert die Online-PinCode-Tastatur und bereitet gleich eine neue Online-PinCode-Tastatur mit denselben Eigenschaften vor.

↳ Online-PinCode-Tastatur ist angelegt.

HINWEIS

Wenn Sie die User-PINs anschließend bearbeiten wollen, dann klicken Sie auf den Eintrag in der Matrix und wählen Sie aus dem Menü die Schaltfläche BEARBEITEN aus.

ACHTUNG

Sperrung nach Falscheingaben

Nach sieben Falscheingaben einer User-PIN quittiert die SmartBridge weiterhin den Empfang, das System sperrt jedoch für drei Minuten die Verarbeitung von eingegebenen User-PINs. In der Web-App wird bei den Meldungen eine entsprechende Benachrichtigung angezeigt.

Sehen Sie dazu auch

- *Schloss anlegen [▸ 9]*

4.5 Online-PinCode-Tastatur löschen

✓ SmartBridge angelegt (Siehe *SmartBridges einrichten [▸ 19]*).
✓ Netzwerk eingerichtet und funktionsfähig (siehe *Online-Komponenten konfigurieren [▸ 24]*).
✓ Online-Status der zu löschenden Online-PinCode-Tastatur "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 die zu löschende Online-PinCode-Tastatur.
4. Klicken Sie auf die Schaltfläche "LÖSCHEN".
   ↳ Die Online-PinCode-Tastatur wird zum Löschen vorgemerkt.
5. Starten Sie die Netzwerkkonfiguration über die Schaltfläche KONFIGURATION STARTEN.
   ↳ Programmiervorgang *(in diesem Fall das Zurücksetzen)* wird ausgeführt.
   ↳ Online-PinCode-Tastatur kann nach vorherigem Zurücksetzen auf den Auslieferungszustand (siehe Auslieferungszustand setzen) anschließend in jeder MobileKey-Schließanlage neu eingebunden werden.

↳ Online-PinCode-Tastatur ist gelöscht.

4.6 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 [▸ 38]*.

4.7 Programmieren von Komponenten

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

HINWEIS

Programmieren Sie jedes Schloss bzw. jede Online-PinCode-Tastatur vor dem Einbau!

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 bzw. der Online-PinCode-Tastatur beim Anlegen 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)*

4.8 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 bzw. die Online-PinCode-Tastatur behält die Konfiguration und ist anschließend bis zu einer neuen Online-Einrichtung nur noch über den USB-Programmierstick erreichbar.

✓ Mindestens ein Online-Schloss bzw. eine Online-PinCode-Tastatur angelegt.
✓ Mindestens eine 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 bzw. auf die zu trennende Online-PinCode-Tastatur.
   ↳ 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 [▸ 38]*

4.9 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.

4.10 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.

4.10.1 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 [▸ 27].

HINWEIS

Das Zeitfenster von geteilten Schlüsseln ist auf sechs Monate beschränkt.

- Wenn Sie Freunden dauerhaft Zutritt gewähren wollen, dann verwenden Sie Transponder oder eine PinCode-Tastatur.

4.10.2 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.

4.11 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.
	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 [▸ 7])* 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), um weitere Hilfe zu erhalten. Wahrscheinlich muss Ihre Hardware ausgetauscht werden.

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 [▸ 24]*

VORSICHT

Riegel nicht überwacht

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

- 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 [▸ 38] für weitere Hilfe.*

Sehen Sie dazu auch

- *Hilfe zu Online-Schlössern [▸ 38]*
- *Programmieren von Komponenten [▸ 24]*

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 alle wichtigen Hinweise, Warnungen und Alarme 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 Stromversorgung unterbrochen wurde. Über den Zeitraum, in dem die SmartBridge nicht ordnungsgemäß online ist, gehen alle auftretenden Events verloren.

HINWEIS

Eine Benachrichtigung vom Typ "ALARM" wird in jedem Fall empfohlen. So können Sie dieses Event einrichten: *Regel vom Typ "Alarme" erstellen [▸ 32]*

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 [▸ 32]*

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.

- 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?
- **LAN-Verbindung** überprüfen.
- **Internetzugang** überprüfen.
  - Ist der Port 8883 (TCP/IP) der Firewall geöffnet? Fügen Sie ggf. entsprechende Ausnahmen hinzu, um die SmartBridge über den Port 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.
- 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.

HINWEIS

Zurücksetzen der SmartBridge

Die SmartBridge kann über einen Hardware-Reset auf die Werkseinstellungen zurückgesetzt werden (siehe RouterNode zurücksetzen).

6.6 Hilfe zur Online-PinCode-Tastatur

Führen Sie bei ein Problemen mit der Online-PinCode-Tastatur folgende Checkliste durch.

- Prüfen Sie den **Batteriezustand**. Führen Sie einen Batterietest durch (siehe Batterietest).
- Prüfen Sie, ob die **Chip-IDs** korrekt eingegeben wurden.
- Prüfen Sie die richtige Zuweisung des Schlosses zur Online-PinCode-Tastatur (siehe *Online-PinCode-Tastatur anlegen [▸ 22]*).

6.7 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!

6.8 Netzwerkfehler

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.

6.9 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 [▸ 25]*.

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 Stromversorgung!)

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.

VORSICHT

Batteriewechsel

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

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.simons-voss.com abrufbar.

10 Tipps & Tricks

10.1 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!

10.2 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.

10.3 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.

11 Hilfe und weitere Informationen

Infomaterial/Dokumente

Detaillierte Informationen zum Betrieb und zur Konfiguration sowie weitere Dokumente finden Sie auf der SimonsVoss-Homepage im Downloadbereich unter Dokumente (*https://www.simons-voss.com/de/downloads/dokumente.html*).

Software und Treiber

Software und Treiber finden Sie auf der SimonsVoss-Homepage im Downloadbereich unter Software-Downloads (*https://www.simons-voss.com/de/downloads/software-downloads.html*).

Konformitätserklärungen und Zertifikate

Konformitätserklärungen und Zertifikate zu diesem Produkt finden Sie auf der SimonsVoss-Homepage im Zertifikatsbereich (*https://www.simons-voss.com/de/zertifikate.html*).

Informationen zur Entsorgung

- Entsorgen Sie das Gerät (MobileKey) nicht mit dem Hausmüll, sondern gemäß der europäischen Richtlinie 2012/19/EU bei einer kommunalen Sammelstelle für Elektro-Sonderabfälle.
- Recyceln Sie defekte oder verbrauchte Batterien gemäß der europäischen Richtlinie 2006/66/EG.
- Beachten Sie örtliche Bestimmungen zur getrennten Entsorgung von Batterien.
- Führen Sie die Verpackung einer umweltgerechten Wiederverwertung zu.

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?

support@simons-voss.com

FAQ

Informationen und Hilfestellungen zu SimonsVoss-Produkten finden Sie auf der SimonsVoss-Homepage im FAQ-Bereich (*https://faq.simons-voss.com/otrs/public.pl*).

SimonsVoss Technologies GmbH
Feringastraße 4
85774 Unterföhring
Deutschland

Das ist SimonsVoss

SimonsVoss ist Technologieführer bei digitalen Schließsystemen.

Der Pionier funkgesteuerter, kabelloser Schließtechnik bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, mittlere und Großunternehmen sowie öffentliche Einrichtungen.

SimonsVoss-Schließsysteme verbinden intelligente Funktionalität, hohe Qualität und preisgekröntes Design made in Germany. Als innovativer Systemanbieter legt SimonsVoss Wert auf skalierbare Systeme, hohe Sicherheit, zuverlässige Komponenten, leistungsstarke Software und einfache Bedienung.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs. Das Unternehmen mit Hauptsitz in Unterföhring bei München und Produktionsstätte in Osterfeld (Sachsen-Anhalt) beschäftigt rund 300 Mitarbeiter in acht Ländern.

SimonsVoss ist ein Unternehmen der ALLEGION Group - ein global agierendes Netzwerk im Bereich Sicherheit. Allegion ist in rund 130 Ländern weltweit vertreten (www.allegion.com)

ALLEGION

SimonsVoss technologies