MobileKey

Handbuch

22.01.2024

Simons Voss technologies

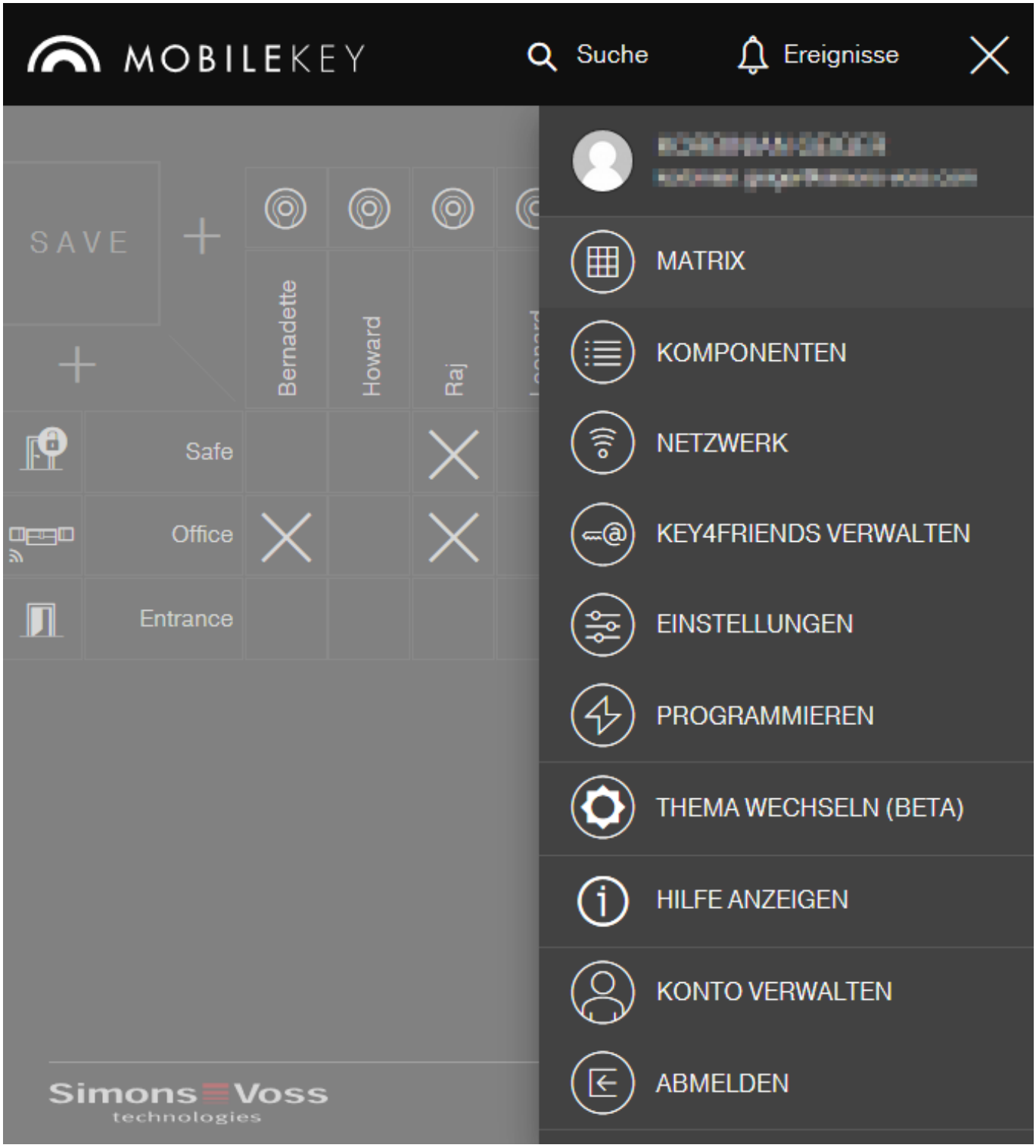
Inhaltsverzeichnis

1. Einleitung

MobileKey ist eine unabhängige Produktkategorie für kleine Schließanlagen. Sie können bis zu 100 Schlüssel *(Transponder)* und 20 Schlösser *(Schließzylinder und SmartRelais)* verwalten.

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 Systemvoraussetzungen

1.1.1 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.

1.1.2 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 mit Online-Erweiterung [▸ 45]*. *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 [▸ 71]*.

2. Allgemeine Sicherheitshinweise

Signalwort: Mögliche unmittelbare Auswirkungen bei Nichtbeachtung
WARNUNG: Tod oder schwere Verletzung (möglich, aber unwahrscheinlich)
VORSICHT: Leichte Verletzung
ACHTUNG: Sachschäden oder Fehlfunktionen
HINWEIS: Geringe oder keine

WARNUNG

Versperrter Zugang

Durch fehlerhaft montierte und/oder programmierte Komponenten kann der Zutritt durch eine Tür versperrt bleiben. Für Folgen eines versperrten Zutritts wie Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss Technologies GmbH nicht!

Versperrter Zugang durch Manipulation des Produkts

Wenn Sie das Produkt eigenmächtig verändern, dann können Fehlfunktionen auftreten und der Zugang durch eine Tür versperrt werden.

- Verändern Sie das Produkt nur bei Bedarf und nur in der Dokumentation beschriebenen Art und Weise.

Batterie nicht einnehmen. Verbrennungsgefahr durch gefährliche Stoffe

Dieses Produkt enthält Lithium-Knopfzellen. Wenn die Knopfzelle verschluckt wird, können schwere innere Verbrennungen innerhalb von gerade einmal zwei Stunden auftreten und zum Tode führen.

1. Halten Sie neue und gebrauchte Batterien von Kindern fern.
2. Wenn das Batteriefach nicht sicher schließt, dann benutzen Sie das Produkt nicht mehr und halten Sie es von Kindern fern.
3. Wenn Sie meinen, dass Batterien verschluckt wurden oder sich in irgendeinem Körperteil befinden, suchen Sie unverzüglich medizinische Hilfe auf.

Explosionsgefahr durch falschen Batterietyp

Das Einsetzen falscher Batterietypen kann zu einer Explosion führen.

- Verwenden Sie ausschließlich die in den technischen Daten spezifizierten Batterien.

VORSICHT

Feuergefahr durch Batterien

Die eingesetzten Batterien können bei Fehlbehandlung eine Feuer- oder Verbrennungsgefahr darstellen.

1. Versuchen Sie nicht, die Batterien aufzuladen, zu öffnen, zu erhitzen oder zu verbrennen.
2. Schließen Sie die Batterien nicht kurz.

ACHTUNG

Beschädigung durch elektrostatische Entladung (ESD)

Dieses Produkt enthält elektronische Bauteile, die durch elektrostatische Entladungen beschädigt werden können.

1. Verwenden Sie ESD-gerechte Arbeitsmaterialien (z.B. Erdungsarmband).
2. Erden Sie sich vor Arbeiten, bei denen Sie mit der Elektronik in Kontakt kommen könnten. Fassen Sie dazu geerdete metallische Oberflächen an (z.B, Türzargen, Wasserrohre oder Heizungsventile).

Beschädigung durch Öle, Fette, Farben und Säuren

Dieses Produkt enthält elektronische und/oder mechanische Bauteile, die durch Flüssigkeiten aller Art beschädigt werden können.

- Halten Sie Öle, Fette, Farben und Säuren vom Produkt fern.

Beschädigung durch aggressive Reinigungsmittel

Die Oberfläche dieses Produkts kann durch ungeeignete Reinigungsmittel beschädigt werden.

- Verwenden Sie ausschließlich Reinigungsmittel, die für Kunststoff- bzw. Metalloberflächen geeignet sind.

Beschädigung durch mechanische Einwirkung

Dieses Produkt enthält elektronische Bauteile, die durch mechanische Einwirkung aller Art beschädigt werden können.

1. Vermeiden Sie das Anfassen der Elektronik.
2. Vermeiden Sie sonstige mechanische Einwirkungen auf die Elektronik.

Beschädigung durch Überstrom oder Überspannung

Dieses Produkt enthält elektronische Bauteile, die durch zu hohen Strom oder zu hohe Spannung beschädigt werden können.

- Überschreiten Sie die maximal zulässigen Spannungen und/oder Ströme nicht.

Beschädigung durch Verpolung

Dieses Produkt enthält elektronische Bauteile, die durch die Verpolung der Spannungsquelle beschädigt werden können.

- Verpolen Sie die Spannungsquelle nicht (Batterien bzw. Netzteile).

Störung des Betriebs durch Funkstörung

Dieses Produkt kann unter Umständen durch elektromagnetische oder magnetische Störungen beeinflusst werden.

- Montieren bzw. platzieren Sie das Produkt nicht unmittelbar neben Geräten, die elektromagnetische oder magnetische Störungen verursachen können (Schaltnetzteile!).

Störung der Kommunikation durch metallische Oberflächen

Dieses Produkt kommuniziert drahtlos. Metallische Oberflächen können die Reichweite des Produkts erheblich reduzieren.

- Montieren bzw. platzieren Sie das Produkt nicht auf oder in der Nähe von metallischen Oberflächen.

HINWEIS

Bestimmungsgemäßer Gebrauch

SimonsVoss-Produkte sind ausschließlich für das Öffnen und Schließen von Türen und vergleichbaren Gegenständen bestimmt.

- Verwenden Sie SimonsVoss-Produkte nicht für andere Zwecke.

Funktionsstörungen durch schlechten Kontakt oder unterschiedliche Entladung

Zu kleine/verunreinigte Kontaktflächen oder unterschiedliche entladene Batterien können zu Funktionsstörungen führen.

1. Verwenden Sie nur Batterien, die von SimonsVoss freigegeben sind.
2. Berühren Sie die Kontakte der neuen Batterien nicht mit den Händen.
3. Verwenden Sie saubere und fettfreie Handschuhe.
4. Tauschen Sie immer alle Batterien gleichzeitig aus.

Abweichende Zeiten bei G2-Schließungen

Die interne Zeiteinheit der G2-Schließungen hat eine technisch bedingte Toleranz von bis zu ± 15 Minuten pro Jahr.

Qualifikationen erforderlich

Die Installation und Inbetriebnahme setzt Fachkenntnisse voraus.

- Nur geschultes Fachpersonal darf das Produkt installieren und in Betrieb nehmen.

Fehlerhafte Montage

Für Beschädigungen der Türen oder der Komponenten durch fehlerhafte Montage haftet die SimonsVoss Technologies GmbH nicht.

Änderungen bzw. technische Weiterentwicklungen können nicht ausgeschlossen und ohne Ankündigung umgesetzt werden.

Die deutsche Sprachfassung ist die Originalbetriebsanleitung. Andere Sprachen (Abfassung in der Vertragssprache) sind Übersetzungen der Originalbetriebsanleitung.

Lesen Sie alle Anweisungen zur Installation, zum Einbau und zur Inbetriebnahme und befolgen Sie diese. Geben Sie diese Anweisungen und jegliche Anweisungen zur Wartung an den Benutzer weiter.

3. Produktspezifische Sicherheitshinweise

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.

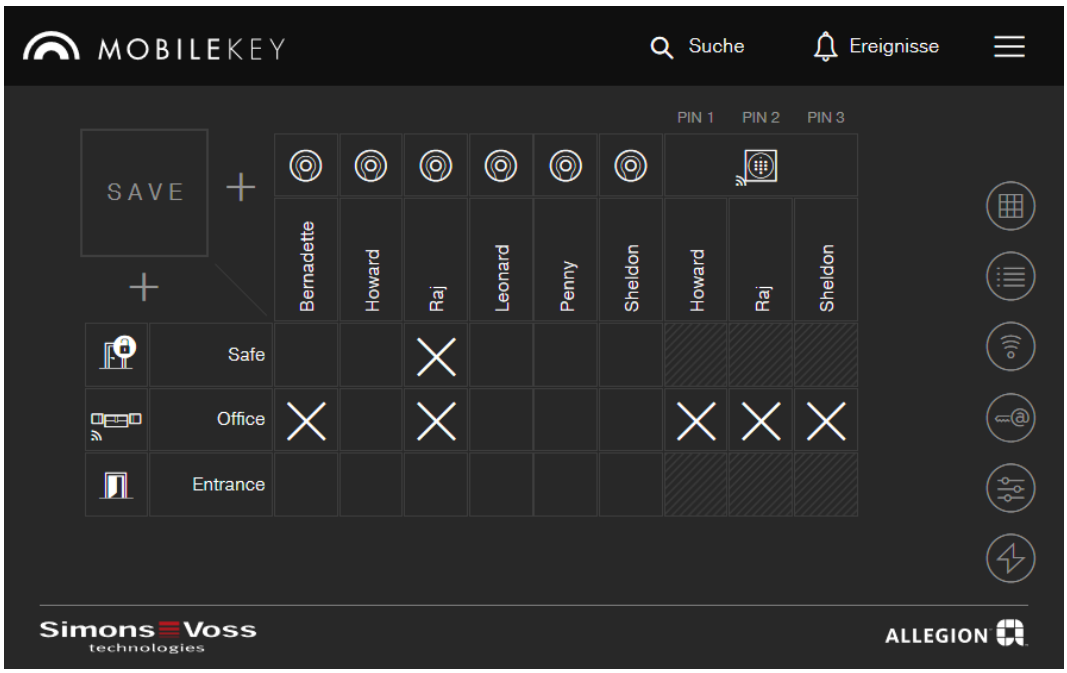
4. Bedeutung der Textformatierung

Diese Dokumentation verwendet Textformatierung und Gestaltungselemente, um das Verständnis zu erleichtern. Die Tabelle erklärt die Bedeutung möglicher Textformatierungen:

Beispiel	Schaltfläche
☑ Beispiel ☐ Beispiel	Checkbox
◉ Beispiel	Option
[Beispiel]	Registerkarte/Tab
"Beispiel"	Name eines angezeigten Fensters
| Beispiel |	Obere Programmleiste
Beispiel	Eintrag in der ausgeklappten oberen Programmleiste
Beispiel	Kontexmenü-Eintrag
▼ Beispiel	Name eines Dropdown-Menüs
"Beispiel"	Auswahlmöglichkeit in einem Drop-down-Menü
"Beispiel"	Bereich
Beispiel	Feld
Beispiel	Name eines (Windows-)Dienstes
Beispiel	Befehle (z.B. Windows-CMD-Befehle)
Beispiel	Datenbank-Eintrag
[Beispiel]	MobileKey-Typauswahl

5. Die Matrix

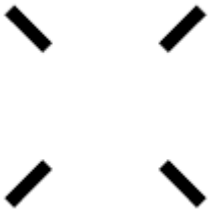
Die Matrix stellt die gesamte Schließanlage übersichtlich dar. Somit ist diese Ansicht der Mittelpunkt aller Funktionen. Horizontal werden alle Schlüssel (z.B. Transponder) und vertikal alle Schlösser (z.B. Schließzylinder) dargestellt. Wichtige Menüs sind über die Schaltflächen Suche, Ereignisse und aufrufbar.



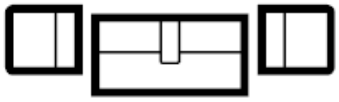
Um die Matrix so übersichtlich wie möglich zu halten, werden verschiedene Symbole eingesetzt.

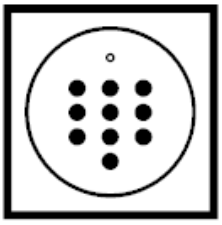
Berechtigungen

Symbol	Beschreibung
	**Berechtigungskreuz: Neu** Die Berechtigung wurde gesetzt; allerdings noch nicht programmiert.
	**Berechtigungskreuz: Gesetzt** Die Berechtigung wurde gesetzt und ist aktiv.

Symbol	Beschreibung
	**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, dass eine Online-Erweiterung vorhanden ist.*
	**Schloss: SmartRelais** Bei dieser Komponente handelt es sich um ein SmartRelais. *Ein zusätzliches Funksymbol in der linken, unteren Ecke zeigt an, dass eine Online-Erweiterung vorhanden ist.*
	**Schlüssel: Transponder** Bei dieser Komponente handelt es sich um einen Transponder.

Symbol	Beschreibung
	**Schlüssel: PinCode-Tastatur** Bei dieser Komponente handelt es sich um eine PinCode-Tastatur. *Ein zusätzliches Funksymbol in der linken, unteren Ecke zeigt an, dass eine Online-Erweiterung vorhanden ist.*

Suchfunktion

Aufruf weiterer Funktionen

Aus der Matrixansicht rufen Sie auch weitere Funktionen auf.

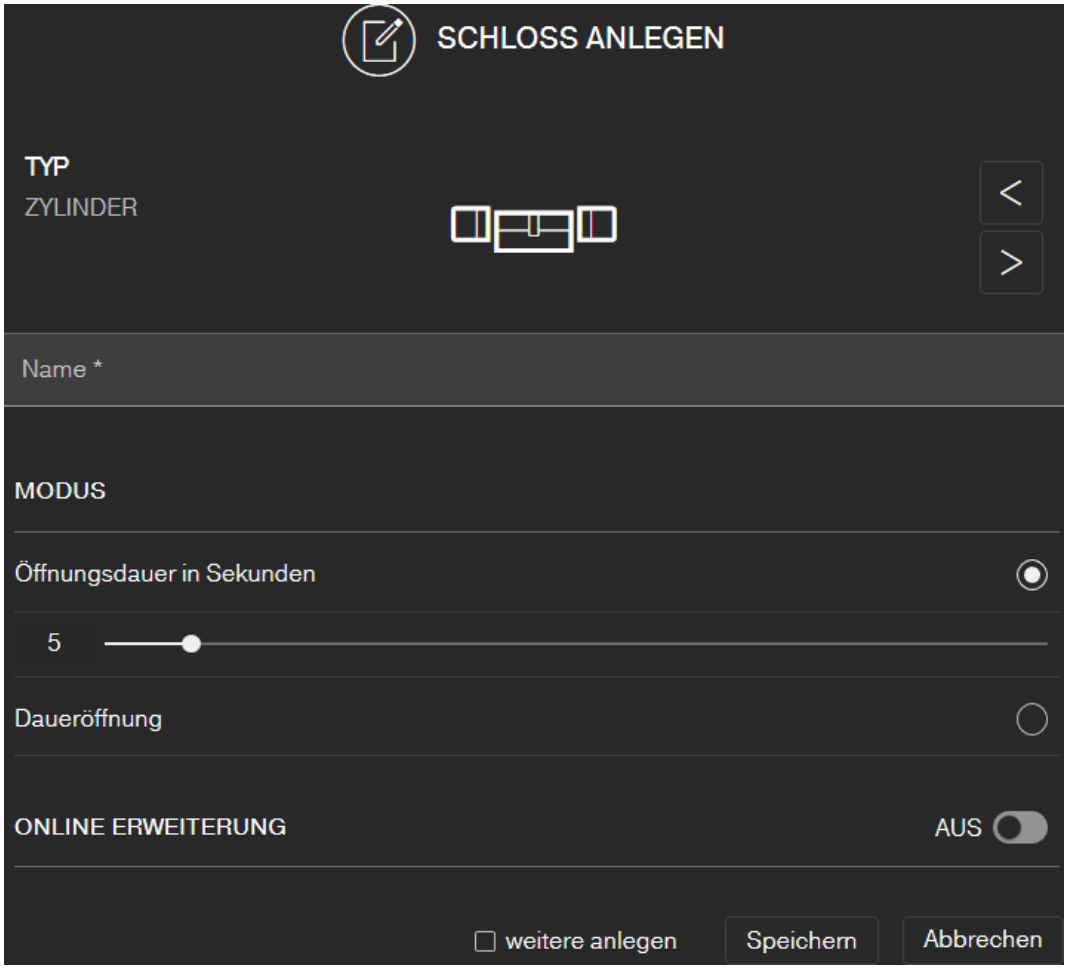
Symbol	Beschreibung
	**Suche** Mit einem Klick auf die Schaltfläche Suche rufen Sie eine Suchfunktion auf. Diese findet: - Schlösser (Schließzylinder bzw. SmartRelais, siehe *Schloss anlegen [▸ 17]*) - Schlüssel (Transponder, siehe *Schlüssel anlegen [▸ 18]*) - Key4Friends (siehe *Key4Friends [▸ 48]*) Sie können die gefundenen Einträge anschließend aufrufen und bearbeiten.
	**Ereignisse** Sie können einstellen, ob Sie bei bestimmten Ereignissen benachrichtigt werden wollen. Wenn eine Benachrichtigung für Sie vorliegt, dann wird Ihnen das hier angezeigt (siehe *Ereignismanagement [▸ 55]*).

Symbol	Beschreibung
	**Menü** Sie können hier auf alle Funktionen von MobileKey zugreifen (siehe *Grundfunktionen [▸ 17]*und *MobileKey Online-Erweiterung [▸ 35]*): ▪ Matrix ▪ Komponenten ▪ Netzwerk ▪ Key4Friends verwalten ▪ Einstellungen ▪ Programmieren ▪ Thema wechseln ▪ Hilfe anzeigen ▪ Konto verwalten ▪ Abmelden Über eine Schnellstartleiste auf der rechten Seite der Matrixansicht können Sie folgende Funktionen auch zeitsparend ohne Menü aufrufen: ▪ Matrix ▪ Komponenten ▪ Netzwerk ▪ Key4Friends verwalten ▪ Einstellungen ▪ Programmieren

6. 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.

6.1 Schloss anlegen



✓ Matrixansicht geöffnet.

1. Klicken Sie auf das Schloss-hinzufügen-Symbol ⊕ (unterhalb der SA-VE -Schaltfläche).
2. Wählen Sie den Schloss-Typ aus, z.B. "ZYLINDER" für einen normalen Schließzylinder.
3. Vergeben Sie einen Namen, z.B. Haustür.
4. Wählen Sie eine der Optionen: ◉ Öffnungsdauer in Sekunden oder ◉ Daueröffnung.
   ↳ Wenn Sie ◉ Daueröffnung gewählt 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. Wenn Sie ein weiteres Schloss anlegen wollen, dann markieren Sie die Checkbox ☑ weitere anlegen.
   ↳ Mit dieser Checkbox bleiben Sie nach dem Speichern in dieser Ansicht und können sofort ein weiteres Schloss anlegen.
6. Klicken Sie auf die Schaltfläche Speichern.

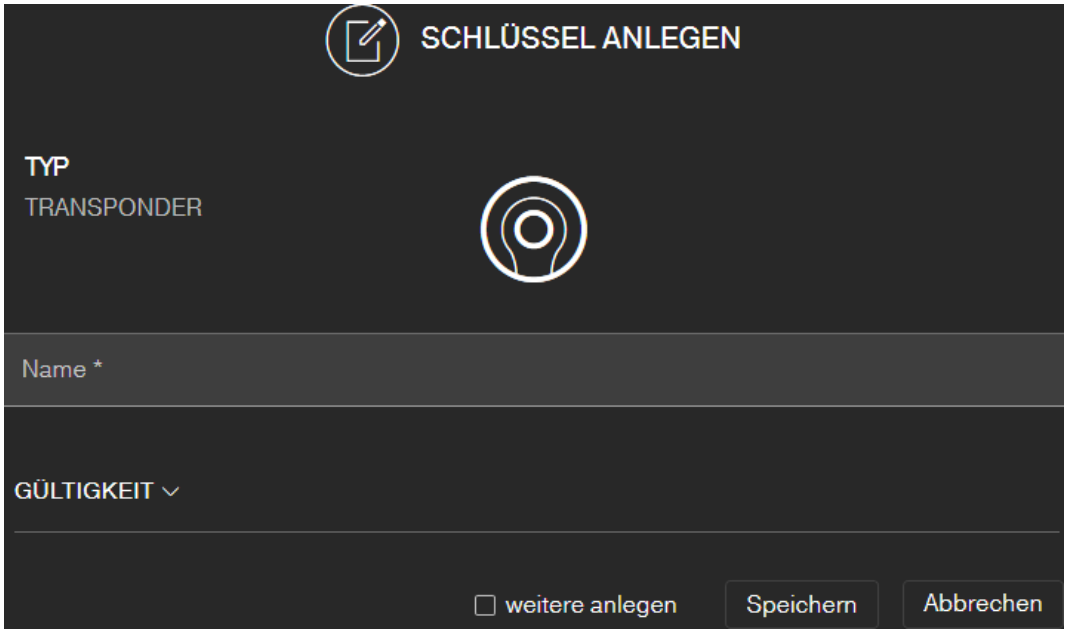
↳ Schloss ist angelegt.

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.

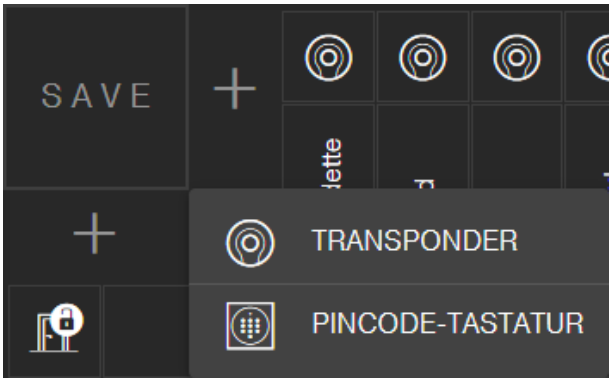
Beim **SmartRelais 2** ist es möglich, den **Ausgang (Relaiskontakt) zu invertieren**. Hierfür muss erst ein SmartRelais angelegt und programmiert werden. Anschließend wird die Einstellung "RELAISKONTAKT KONFIGURIEREN" mit der Option "Ausgang invertieren" in den Eigenschaften des SmartRelais sichtbar.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

6.2 Schlüssel anlegen



✓ Matrixansicht geöffnet.

1. Klicken Sie auf das Schlüssel-hinzufügen-Symbol ⊕ (neben der SA-VE -Schaltfläche).
   ↳ Kontextmenü öffnet sich.



2. Wählen Sie den Schlüssel-Typ TRANSPONDER aus.
3. Vergeben Sie einen Namen, z.B. "Hans Müller".
4. Bestimmten Sie gegebenenfalls die Gültigkeit.
   ↳ "Gültig von": Ab diesem Datum ist der Schlüssel in der Schließanlage berechtigt.
   ↳ "Gültig bis": Ab diesem Datum ist der Schlüssel in der Schließanlage nicht mehr berechtigt.
5. Wenn Sie einen weiteren Schlüssel (Transponder) anlegen wollen, dann markieren Sie die Checkbox ☑ weitere anlegen.
6. Klicken Sie auf die Schaltfläche Speichern .

↳ Schlüssel ist angelegt.

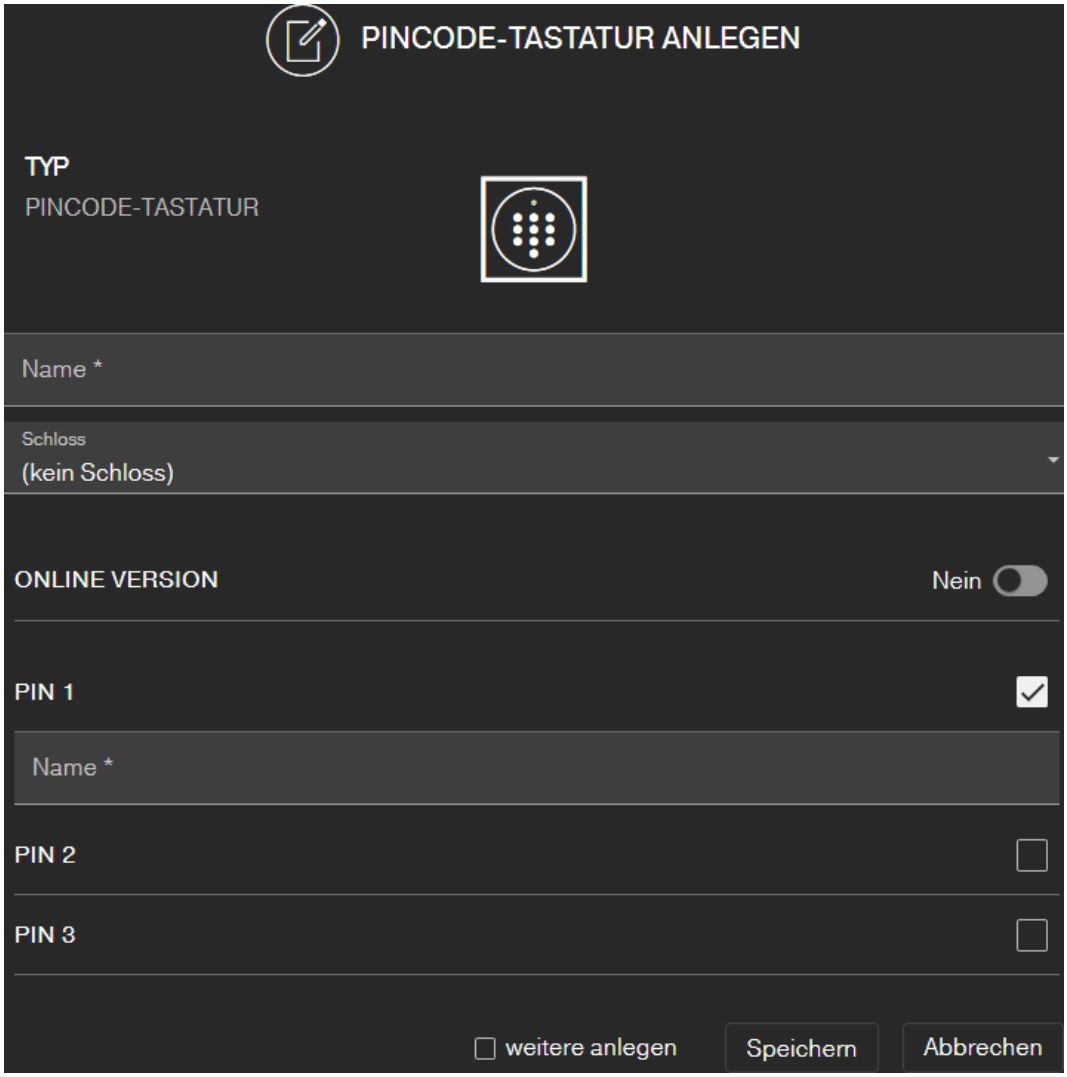
HINWEIS

Zuordnung der Schlüssel (Transponder) mit Komponentenliste

Viele nacheinander programmierte Transponder sind schwierig zuzuordnen. Sie müssen diese Transponder nicht markieren. Auf jedem Transponder ist eine einzigartige ID eingraviert. Diese ID ist dem von Ihnen angegebenen Namen zugeordnet. Sie sehen diese Zuordnung in der Komponentenliste (siehe *Komponentenliste exportieren [▸ 28]*).

6.3 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 *PinCode-Tastatur mit Online-Erweiterung anlegen [▸ 43]* beschrieben vor.



- ✓ PinCode-Tastatur bereits konfiguriert; siehe mitgelieferte Kurzanleitung *(Master-Pin und mindestens eine User-Pin müssen eingerichtet sein!)*
- ✓ Schloss für PinCode-Tastatur angelegt (siehe *Schloss anlegen [▸ 17]* oder *Schloss mit Online-Erweiterung anlegen [▸ 40]*)
- ✓ Matrixansicht geöffnet.

1. Klicken Sie auf das Schlüssel-hinzufügen-Symbol ⊕ (neben der SA-VE -Schaltfläche).
2. Wählen Sie den Typ PINCODE-TASTATUR aus.
3. Legen Sie das Schloss fest, an welchem die PinCode-Tastatur betrieben wird.
4. Vergeben Sie einen Namen für die PIN 1 *(entspricht User-Pin 1)*, z.B. "Hans Müller". Die weiße Checkbox für PIN 1 ist bereits aktiviert.
5. Wenn Sie eine zweite und dritte PIN verwenden wollen, markieren Sie die Checkboxen. Verfahren Sie dann ebenso wie bei PIN 1.

6. Wenn Sie eine weitere PinCode-Tastatur anlegen wollen, dann markieren Sie die Checkbox ☑ weitere anlegen.
   ↳ Mit dieser Checkbox bleiben Sie nach dem Speichern in dieser Ansicht und können sofort eine weitere PinCode-Tastatur anlegen.
7. Klicken Sie auf die Schaltfläche Speichern.

↳ PinCode-Tastatur ist angelegt.

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.

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.

6.4 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 und sind noch nicht gespeichert. Beim Programmieren werden diese Änderungen nicht übernommen.

- Übernehmen Sie die Änderungen vor dem Programmieren mit einem Klick auf die Schaltfläche SAVE.

Alle Änderungen und Berechtigungen der Komponenten müssen programmiert werden (siehe *Programmieren von Komponenten [▸ 25]*), bevor sie tatsächlich in Kraft treten.

6.5 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.

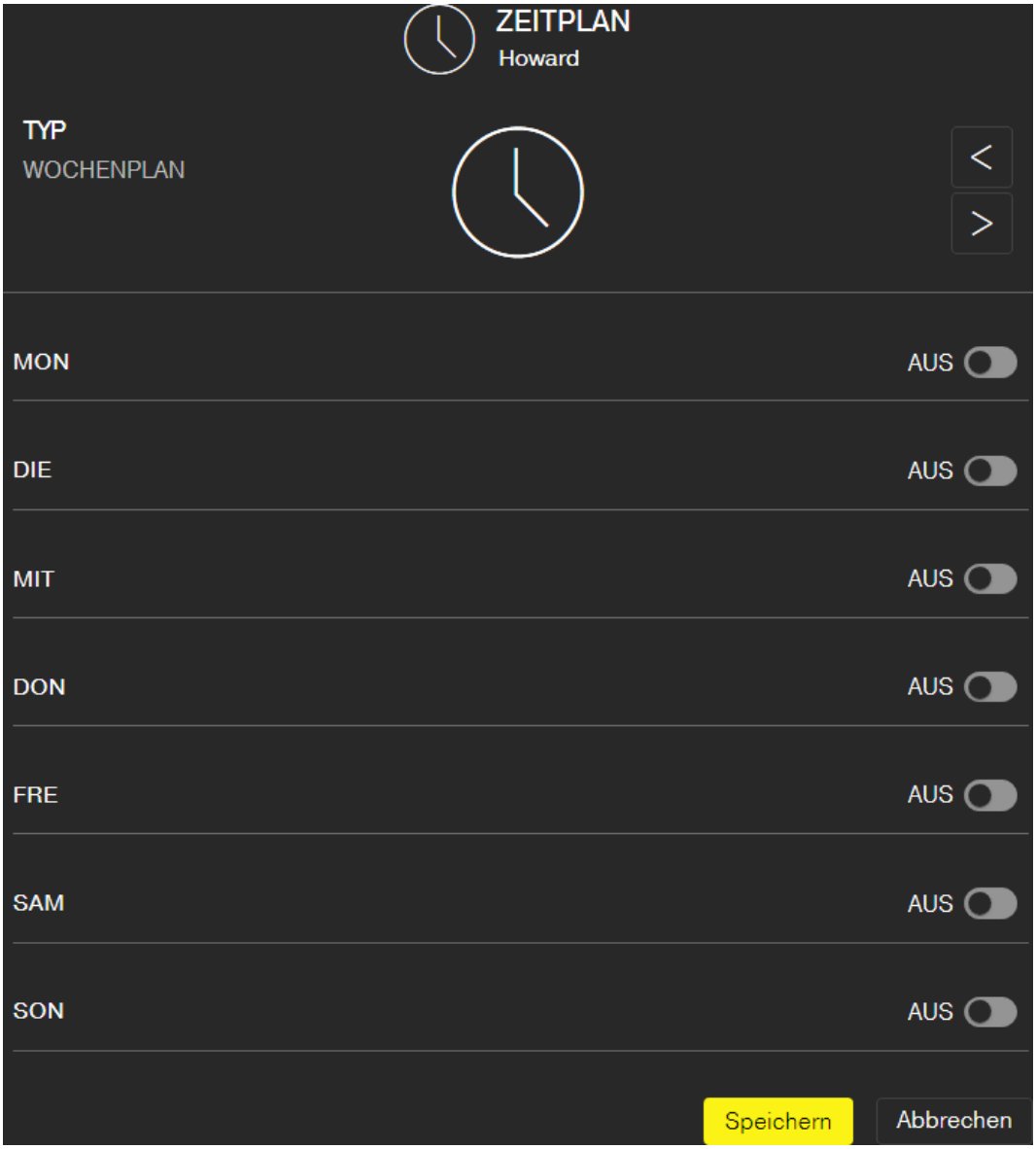
  BEISPIEL: Mitarbeiter John Dorian ist von Mo. bis Fr. von 07:00 bis 19:00 Uhr an den Schlössern berechtigt.

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

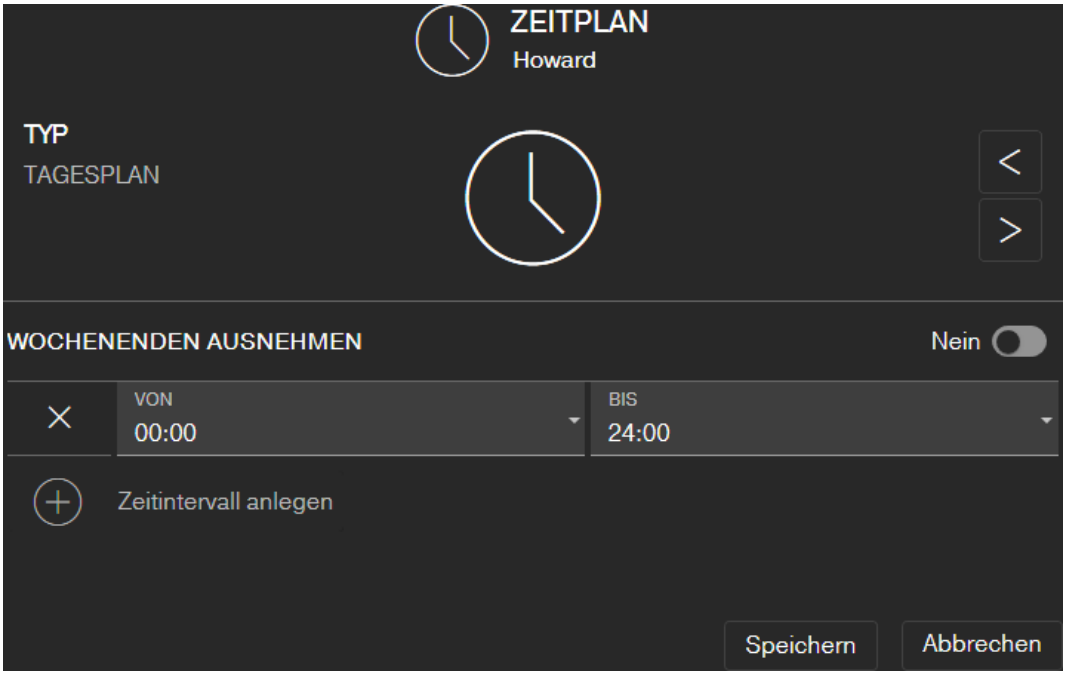
✓ Matrixansicht geöffnet.

1. Klicken Sie auf den gewünschten Schlüssel in der Matrixansicht.
   ↳ Kontextmenü 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.

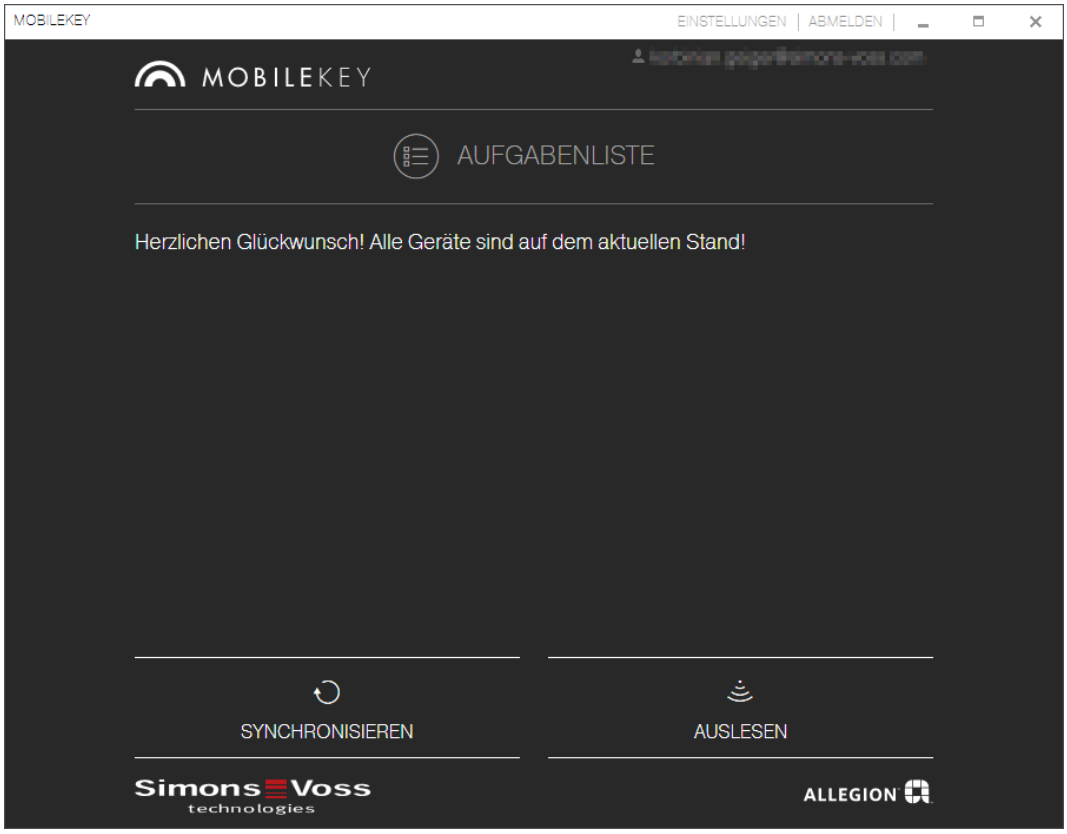
HINWEIS

Zeitintervalle um Mitternacht

Überschreitet ein Zeitintervall Mitternacht, dann kann es nicht mit einem Tag programmiert werden. Sie müssen ein solches Zeitintervall auf zwei Tage aufteilen:

1. Legen Sie ein Zeitintervall von "Zeit vor Mitternacht" bis "Mitternacht" an.
2. Legen Sie ein zweites Zeitintervall von "Mitternacht" bis "Zeit nach Mitternacht" an.

6.6 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.

6.6.1 HINWEIS: Programmieren über ein Windows-Gerät

Sie müssen die Programmier-App einmalig heruntergeladen und installieren. Danach melden Sie sich an. Für die Programmierung muss der USB-Programmierstick mit dem USB-Anschluss des Computers verbunden sein.

Auf diese Installation wird hingewiesen, sobald Sie auf Menü und PROGRAMMIEREN klicken. Der Download der Installationsdatei beginnt nach dem Klick auf Installieren/Reparieren. Installieren Sie die Programmier-App (Administratorrechte erforderlich).

Beachten Sie die Hardwareanforderungen: *Programmierung [▸ 6]*

6.6.2 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. Sie benötigen ggfs. ein separat erhältliches USB-On-The-Go-Kabel (OTG):

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

Beachten Sie die Hardwareanforderungen: *Programmierung [▸ 6]*

6.6.3 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.

6.7 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.

6.8 Erzwungenes Löschen von Komponenten

Kann eine defekte Komponente nicht problemlos zurückgesetzt werden (siehe *Zurücksetzen von Komponenten [▸ 27]*) 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 die Schaltfläche LÖSCHEN ERZWINGEN und bestätigen Sie die Eingabe.

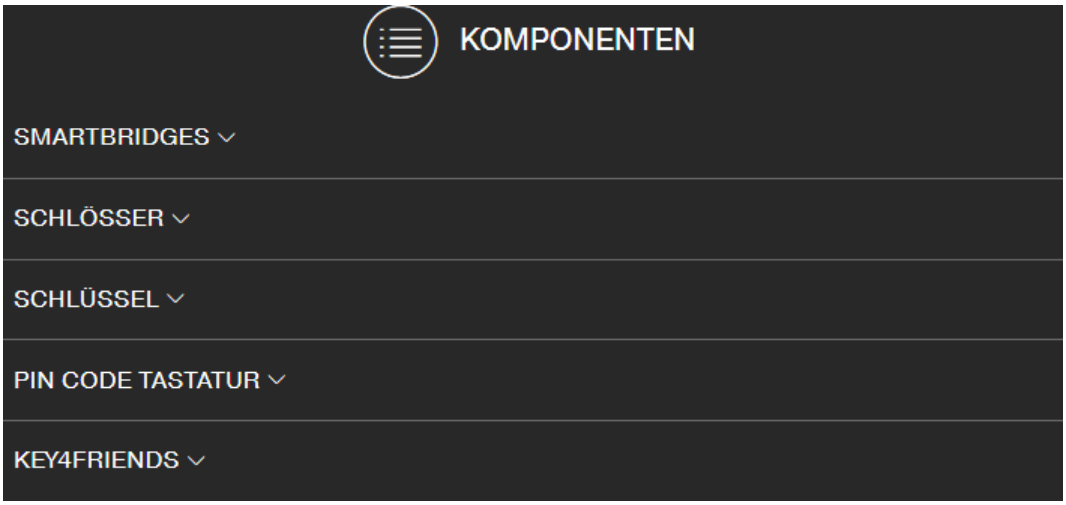
HINWEIS

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

- Sie können die Komponenten durch die Programmier-App zurücksetzen (siehe *Gelöschte Komponenten zurücksetzen oder wiederverwenden [▸ 64]*).

6.9 Komponentenliste exportieren

Sie können über Menü und Komponenten sehen, was in Ihrem MobileKey-Schließplan vorhanden ist:



Sie können mit dem Aufklappen der Dropdown-Menüs die Komponenten sehen:

- ▼ SMARTBRIDGES
- ▼ SCHLÖSSER
- ▼ SCHLÜSSEL
- ▼ PIN CODE TASTATUR
- ▼ KEY4FRIENDS

Mit der Schaltfläche PDF generieren erstellen Sie ein PDF mit detaillierten Informationen:

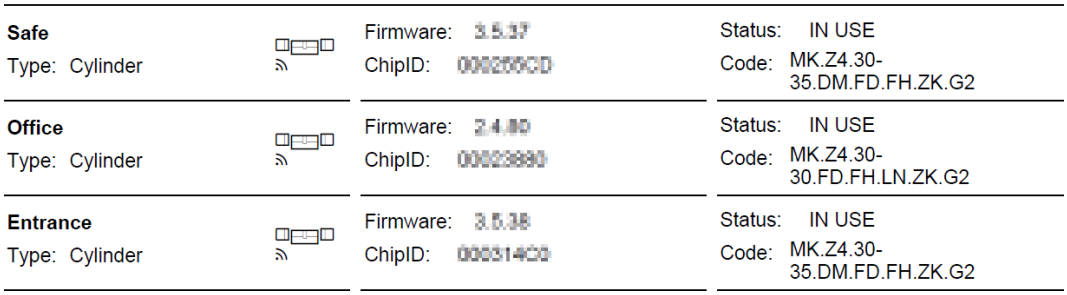
Standort und Konto

Angabe	Bedeutung
Standort	Standort der Komponenten (Hier wird die Standortangabe in den Einstellungen verwendet, siehe *Einstellungen [▸ 59]*).
Konto	Konto, zu dem die Komponenten gehören.

SMARTBRIDGES

Angabe	Bedeutung
Typ	Standardeintrag ohne weitere Bedeutung.
Firmware	Firmwareversion der SmartBridge.
MobileKeyID	MobileKey-ID der SmartBridge.
Zustand	Mögliche Zustände:

SCHLÖSSER



Angabe	Bedeutung
Typ	Gibt an, ob es sich um einen Zylinder oder ein SmartRelais handelt.

Angabe	Bedeutung
Firmware	Firmware des verwendeten Schlosses. Wenn das Schloss nicht programmiert ist, dann wird -- angezeigt.
ChipID	Chip-ID des verwendeten Netzwerkknotens (LockNode). Wenn das Schloss nicht programmiert ist, dann wird -- angezeigt.
Zustand	Mögliche Zustände:
Code	Artikelnummer des Zylinders. Sie können mit dieser Artikelnummer denselben Zylinder nachbestellen. Bei technischen Problemen können Sie dem Support diese Artikelnummer zur Identifizierung mitteilen. Wenn das Schloss nicht programmiert ist, dann wird -- angezeigt.

SCHLÜSSEL

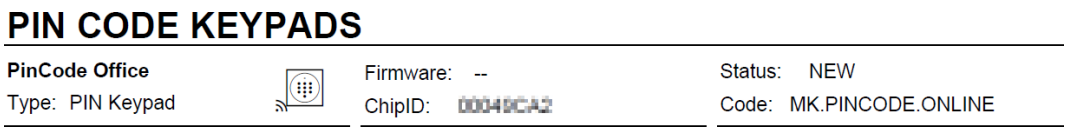
LIST OF KEYS

Bernadette Type: Transponder		Firmware: 3.2.19 Serial number: 2U4G3M2	Status: IN USE Code: MK.TRA2.G2
Howard Type: Transponder		Firmware: 3.2.17 Serial number: 1UHL3L	Status: IN USE Code: MK.TRA2.G2
Raj Type: Transponder		Firmware: 3.2.19 Serial number: 2U039M	Status: IN USE Code: MK.TRA2.G2
Leonard Type: Transponder		Firmware: 3.2.19 Serial number: 2U4P7M	Status: IN USE Code: MK.TRA2.G2
Penny Type: Transponder		Firmware: 3.2.19 Serial number: 0XK3C4	Status: IN USE Code: MK.TRA2.G2
Sheldon Type: Transponder		Firmware: 2.3.5 Serial number: 06137T	Status: IN USE Code: MK.TRA2.G2

Angabe	Bedeutung
Typ	Standardeintrag ohne weitere Bedeutung.
Firmware	Firmware des Transponders.

Angabe	Bedeutung
Seriennummer	Seriennummer des Transponders. Sie finden diese Seriennummer auch auf der Rückseite des Transponders eingraviert. Verwenden Sie diese Seriennummer, um physische Transponder eindeutig den Transpondern im Schließplan zuzuordnen.
Zustand	Mögliche Zustände:
Code	Artikelnummer des Transponders. Bei technischen Problemen können Sie dem Support diese Artikelnummer zur Identifizierung mitteilen.

PIN CODE TASTATUR



Angabe	Bedeutung
Typ	Standardeintrag ohne weitere Bedeutung.
Firmware	Firmware der verwendeten PinCode-Tastatur. Wenn die PinCode-Tastatur nicht programmiert ist, dann wird **--** angezeigt.
ChipID	Chip-ID des verwendeten Netzwerkknotens (LockNode). Wenn kein LockNode vorhanden ist, dann wird **--** angezeigt.
Zustand	Mögliche Zustände:
Code	Artikelnummer der PinCode-Tastatur. Sie können mit dieser Artikelnummer dieselbe PinCode-Tastatur nachbestellen. Bei technischen Problemen können Sie dem Support diese Artikelnummer zur Identifizierung mitteilen.

Sie können alternativ auch die Komponenten auslesen (siehe *Komponenten auslesen [▸ 64]*).

6.10 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. Klicken Sie auf die Schaltfläche PROTOKOLL AUSLESEN.

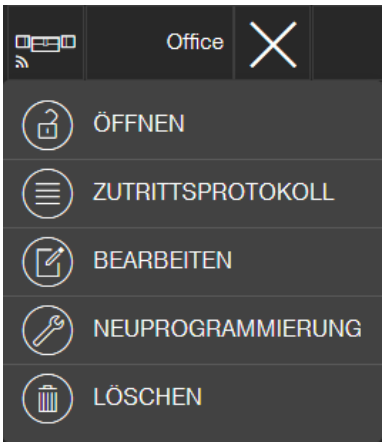
HINWEIS

Auslesen von Schlössern mit Online-Erweiterung

Schlösser mit Online-Erweiterung werden über die SmartBridge automatisch ausgelesen. Sie müssen diese Schlösser nicht mit der Programmier-App und dem USB-Stick auslesen.

   ↳ Der Befehl "Zutrittsprotokoll auslesen" wird als Aufgabe an die Programmier-App gesendet.
4. Klicken Sie auf die Menü-Schaltfläche.
   ↳ Menü öffnet sich.
5. Klicken Sie auf die Schaltfläche PROGRAMMIEREN.
   ↳ Programmier-App startet.
6. Führen Sie die Programmieraufgabe durch.
7. Öffnen Sie die Matrix.

8. Klicken Sie auf das Schloss, dessen Protokoll Sie auslesen wollen.
   ↳ Menü öffnet sich.



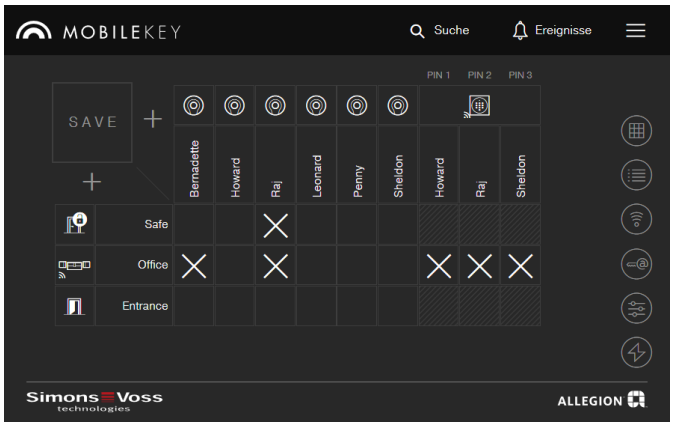
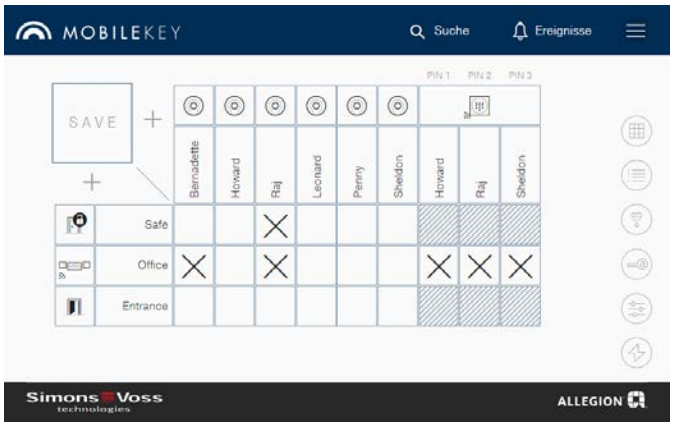
9. Klicken Sie auf die Schaltfläche ZUTRITTSPROTOKOLL.
   ↳ Zutrittsprotokoll wird angezeigt.
10. Filtern Sie bei Bedarf die Einträge.

↳ Gefiltertes Zutrittsprotokoll wird angezeigt.

6.11 Farbschema wechseln

Ihnen stehen zwei Farbschemata zur Verfügung:

Dunkel	Hell
Helle Schrift und Symbole auf dunkelgrauem Grund (Standard nach Login oder Aktualisieren der Seite)	Dunkle Schrift und Symbole auf weißem Grund

Dunkel	Hell
	

Je nach Ihrer persönlichen Präferenz können Sie zwischen den Themes wechseln:

1. Klicken Sie auf die Menü-Schaltfläche .
   ↳ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche Thema wechseln.

↳ Thema ist geändert.

7. MobileKey Online-Erweiterung

Über eine SmartBridge (welche als Accesspoint dient) können Sie Schlösser und PinCode-Tastaturen mit Online-Erweiterung vernetzen, um direkt mit der Web-App zu kommunizieren. Sie profitieren von folgenden Vorteilen:

- Programmieren Sie Schlösser und PinCode-Tastaturen mit Online-Erweiterung plattformunabhängig.
- Verfolgen Sie in Echtzeit Türzustände (offen, geschlossen, verriegelt).
- Lesen Sie die Zutrittslisten der Schlösser von überall auf der Welt aus.
- Teilen Sie mit Key4Friends Ihre Schlüssel mit Freunden.
- Öffnen und schließen Sie Ihre Schlösser aus der Ferne.

Komponenten für die Online-Erweiterung

Für die Nutzung dieser Funktionen sind spezielle Komponenten erforderlich:

- SmartBridge: Als Accesspoint ist sie dauerhaft mit dem Internet verbunden.
- Schloss mit Online-Erweiterung: 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.
- PinCode-Tastatur mit Online-Erweiterung: Diese PinCode-Tastatur ist über einen Netzwerkknoten (LockNode) mit der SmartBridge verbunden.

Hinweis zur Netzwerkabhängigkeit und Offline-Rückfallebene

MobileKey ist eine web-basierte Lösung zur Verwaltung eines Schließplans mit Schlössern und Schlüsseln, die nach der Programmierung selbstständig und unabhängig arbeitet (offline).

Die beschriebene Online-Erweiterung ist von einer dauerhaften und zuverlässigen Internetverbindung zu unserem Server abhängig. Sie bietet zum Beispiel folgende Funktionen:

- Fernöffnungen
- Key4Friends
- Online-PinCode-Tastatur
- Unmittelbares Versenden von Benachrichtigungen

Fernöffnungen ermöglichen Personen ohne eigenes physikalisches Identifikationsmedium unmittelbaren Zutritt an vernetzten Schließungen. Im Gegensatz dazu berechtigen Key4Friends Personen ohne eigenes physikalisches Identifikationsmedium temporär zum selbständigen Zutritt. Solche Personen sind zum Beispiel:

- Freunde
- Diensleister
- Nachbarn
- Lieferanten

HINWEIS

Offline-Rückfallebene für vernetzte Schließungen

Alle Funktionen der Online-Erweiterung (einschließlich Key4Friends) sind nur als Erweiterung und nicht als Ersatz der Offline-Funktionen ausgelegt. Sie sind kein Ersatz für Personen mit dauerhaften Berechtigungen oder als ausschließliche Zutrittsberechtigung an sicherheitskritischen Türen und Zugängen geeignet.

- Stellen Sie daher bei der Online-Erweiterung unseres Standardsystems (Offline), insbesondere bei der Verwendung mit Key4Friends oder Fernöffnungen, immer ein oder mehrere Offline-Backups zur Verfügung (PinCode-Tastatur (offline), Transponder).

↳ Diese physikalischen Identifikationsmedien kommunizieren direkt mit den Schlössern. Sie stellen jederzeit und netzwerkunabhängig den Zutritt an entsprechenden Türen und Zugängen sicher.

7.1 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.

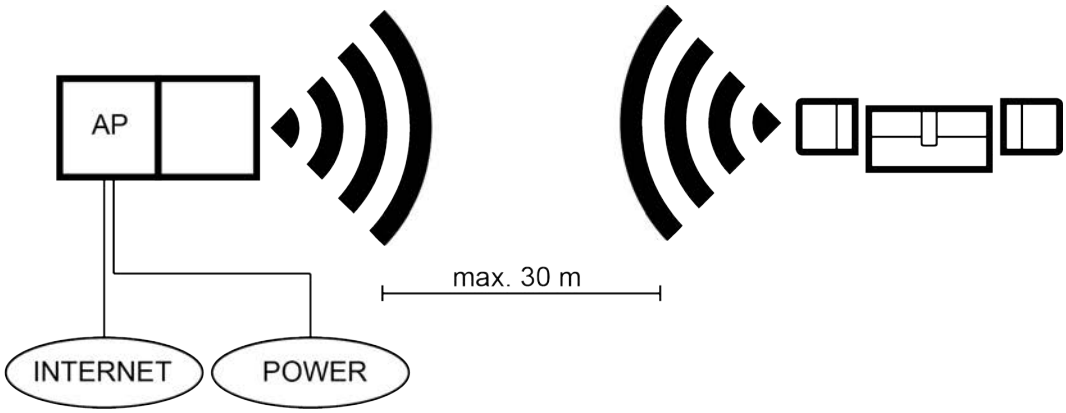
Beachten Sie, dass mit MobileKey maximal 10 SmartBridges eingesetzt werden können.

7.1.1 SmartBridges aufstellen

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

7.1.1.1 Eine SmartBridge

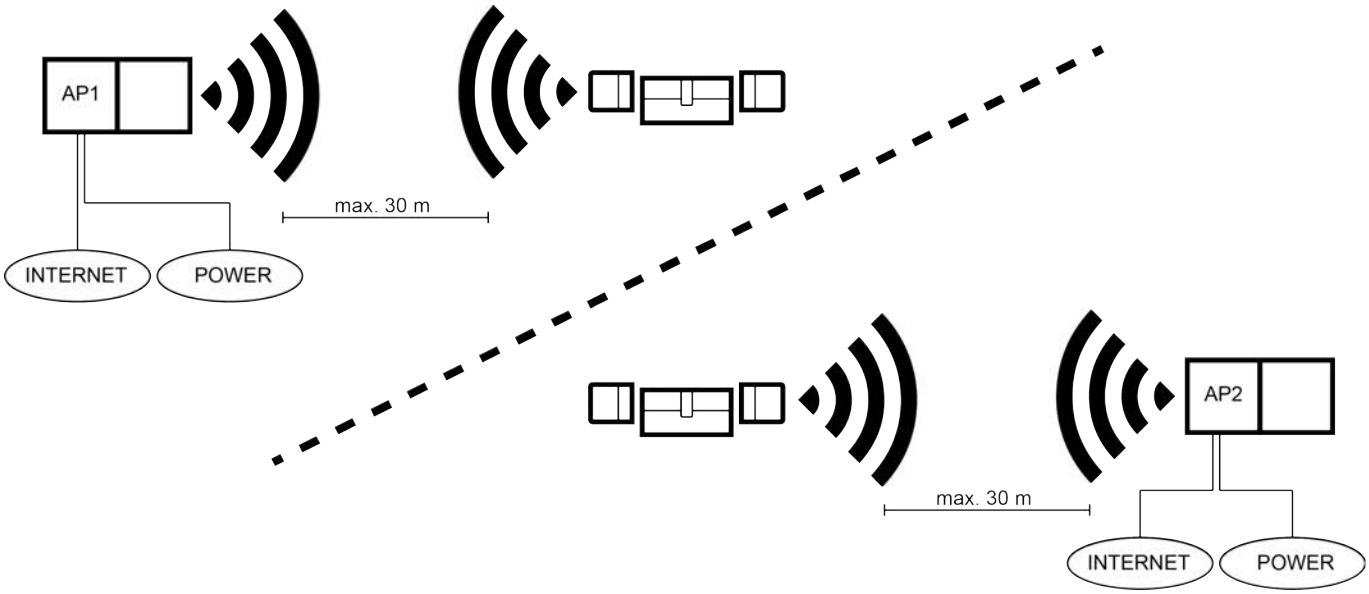
Der Einsatz einer als Accesspoint konfigurierten SmartBridge ist der einfachste Anwendungsfall für MobileKey ONLINE.



7.1.1.2 Zwei oder mehrere SmartBridges

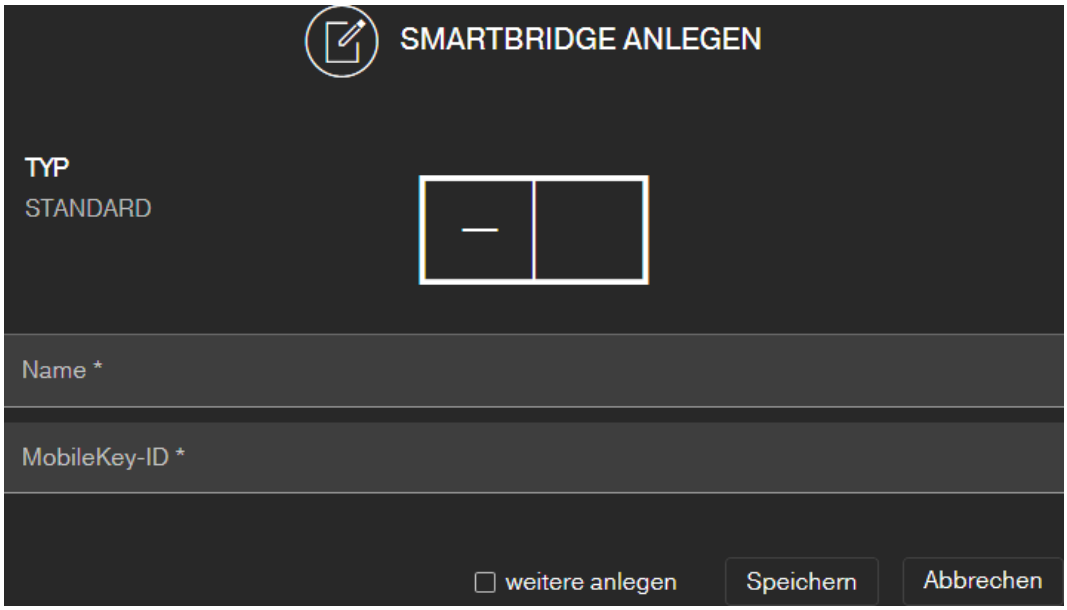
MobileKey ONLINE kann mehrere Accesspoints verwalten. Auf diese Weise können mehrere Standorte oder sehr weit entfernte Schlösser mit dem MobileKey ONLINE Netzwerk abgedeckt werden.

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.



7.1.2 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.
   ↳ Netzwerkansicht öffnet sich.
3. Fügen Sie eine neue SmartBridge über die ⊕-Schaltfläche bei Smart-Bridges hinzu.
   ↳ Dialog zum Hinzufügen einer neuen SmartBridge startet.
4. Vergeben Sie einen eindeutigen Namen (z.B. "SmartBridge Büro 2").
5. Geben Sie die MobileKey-ID ein (Siehe Verpackung oder Rückseite der SmartBridge, Format XXXX-XXXX-XXXX-XXXX).
6. Wenn Sie eine weitere SmartBridge anlegen wollen, dann markieren Sie die Checkbox ☑ weitere anlegen.
   ↳ Mit dieser Checkbox bleiben Sie nach dem Speichern in dieser Ansicht und können sofort eine weitere SmartBridge anlegen.
7. Klicken Sie auf die Schaltfläche Speichern.
   ↳ SmartBridge ist angelegt.

HINWEIS

SmartBridge-Verbindung zum Server

Ihre SmartBridge baut etwa alle 15 Sekunden eine Verbindung zum Server auf. Wenn Sie unmittelbar nach dem Einrichten der SmartBridge die Netzwerkkonfiguration starten, dann kann der Server die SmartBridge noch nicht identifizieren und die Netzwerkkonfiguration schlägt fehl.

- Warten Sie nach dem Einrichten der SmartBridge etwa zwanzig Sekunden, bevor Sie die Netzwerkkonfiguration starten.

Standardpasswort ändern

Unbefugter Zugriff mit Standard-Zugangsdaten

1. Ändern Sie das frei einsehbare Webserver-Standardpasswort. Unbefugte können zwar keinen Zutritt erlangen, aber die Konfiguration ändern. In diesem Fall erreichen Sie das Gerät nicht mehr und müssen es zurücksetzen.
2. Verwenden Sie keine Leerzeichen am Anfang oder am Ende (werden von manchen Browsern nicht übertragen).

Ändern Sie das Standardpasswort Ihrer SmartBridge:

1. Ermitteln Sie mit dem OAM-Tool die IP-Adresse Ihrer SmartBridge.
2. Rufen Sie mit einem Browser die Weboberfläche Ihrer SmartBridge auf (Benutzername: SimonsVoss, Passwort: SimonsVoss).
3. Vergeben Sie ein neues Passwort.

Detaillierte Informationen zum OAM-Tool und zu Ihrer SmartBridge finden Sie im OAM-Tool-Handbuch, in der Kurzanleitung Ihrer SmartBridge und dem SmartBridge-Handbuch.

7.1.3 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.

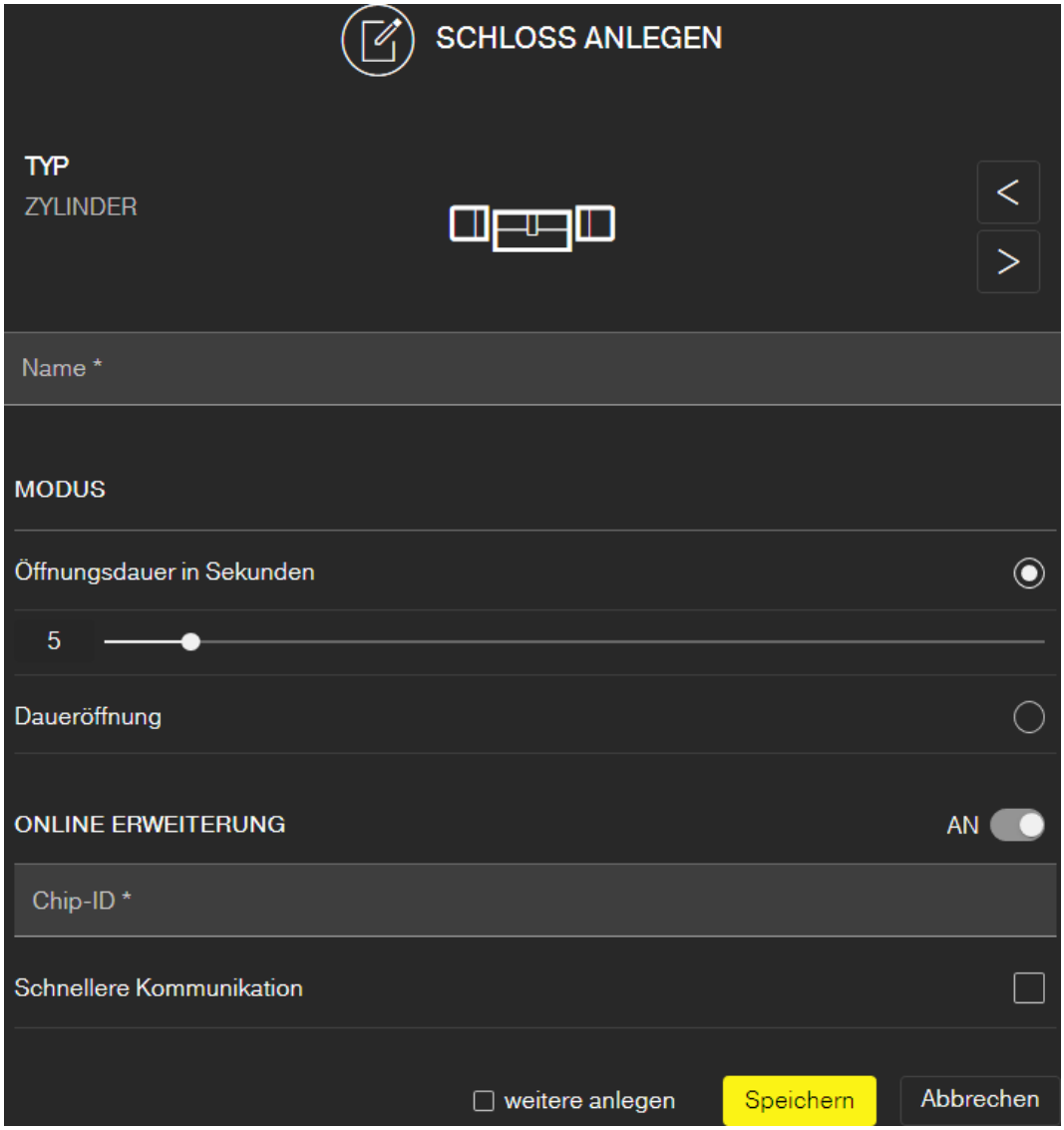
1. Klicken Sie auf die Menü-Schaltfläche ☰.
   ↳ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche NETZWERK.

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.

7.2 Schloss mit Online-Erweiterung anlegen

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. Informationen zum Austausch finden Sie in der Kurzanleitung des LockNodes. 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 [▸ 38]*).

✓ Matrixansicht geöffnet.

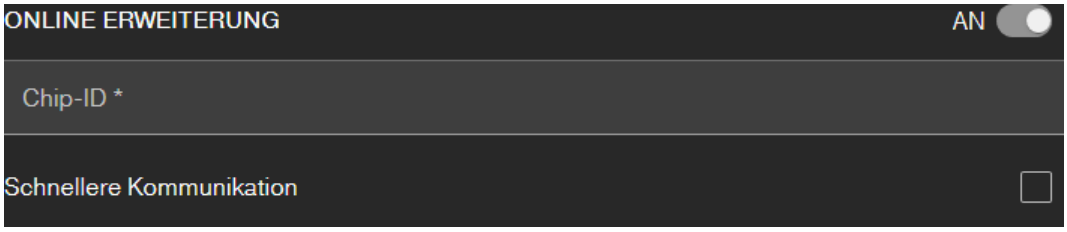
1. Klicken Sie auf das Schloss-hinzufügen-Symbol ⊕ (unterhalb der SA-VE -Schaltfläche).
2. Wählen Sie den Schloss-Typ aus, z.B. "ZYLINDER" für einen normalen Schließzylinder.
3. Vergeben Sie einen Namen, z.B. Haustür.

VORSICHT

Sicherheitsrisiko durch Daueröffnung

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

4. Wählen Sie eine der Optionen: ◉ Öffnungsdauer in Sekunden oder ◉ Daueröffnung.
   ↳ Wenn Sie ◉ Daueröffnung gewählt haben, dann bleibt das Schloss solange eingekuppelt, bis es erneut mit einem Schlüssel oder per Fernöffnung betätigt wird.
5. Aktivieren Sie die Online-Erweiterung.



6. Tragen Sie die Chip-ID ein (Siehe Verpackung oder Knaufinnenseite, Format XXXXXXXX).

HINWEIS

Geringere Batterielaufzeit

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

7. Aktivieren Sie optional die Checkbox ☑ Schnellere Kommunikation.
8. Wenn Sie ein weiteres Schloss mit Online-Erweiterung anlegen wollen, dann aktivieren Sie die Checkbox ☑ weitere anlegen.
   ↳ Mit dieser Checkbox bleiben Sie nach dem Speichern in dieser Ansicht und können sofort ein weiteres Schloss mit Online-Erweiterung anlegen.
9. Klicken Sie auf die Schaltfläche Speichern.

↳ Schloss mit Online-Funktion (LockNode) angelegt.

7.3 Schloss mit Online-Erweiterung löschen

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

✓ SmartBridge angelegt *(Siehe SmartBridges einrichten [▸ 38])*
✓ 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.

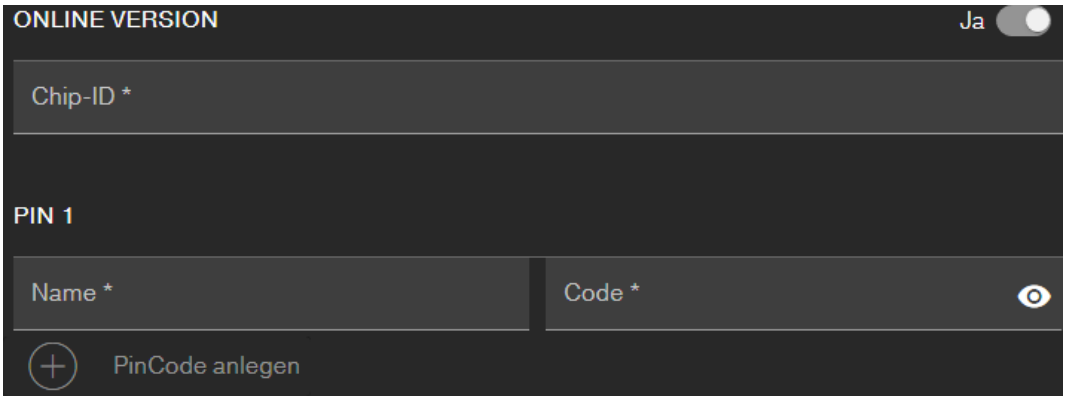
4. Klicken Sie auf die Schaltfläche LÖSCHEN.
   ↳ Das Schloss wird zum Löschen vorgemerkt.
5. Starten Sie die Netzwerkkonfiguration über die Schaltfläche "Konfiguration starten".
   ↳ Programmiervorgang *(in diesem Fall das Zurücksetzen)* wird ausgeführt.
   ↳ Schloss kann anschließend in jeder MobileKey-Schließanlage neu eingebunden werden.

↳ Schloss ist gelöscht.

7.4 PinCode-Tastatur mit Online-Erweiterung anlegen

✓ Online-PinCode-Tastatur bereits konfiguriert (siehe mitgelieferte Kurzanleitung).
✓ Schloss für Online-PinCode-Tastatur bereits angelegt (siehe *Schloss mit Online-Erweiterung anlegen [▸ 40]*).
✓ Matrixansicht geöffnet.

1. Klicken Sie auf das Schlüssel-hinzufügen-Symbol (neben der SAVE-Schaltfläche).
2. Geben Sie einen Namen für die PinCode-Tastatur ein, z.B. "Bürotür".
3. Öffnen Sie das Dropdown-Menü ▼ Schloss.
4. Legen Sie das Schloss fest, an dem die Online-PinCode-Tastatur betrieben wird.
5. Aktivieren Sie die Online-Erweiterung.



6. Geben Sie die Chip-ID ein (Siehe Verpackung oder Rückseite, Format: XXXXXXXX).
7. Geben Sie einen Namen für die erste PIN ein, z.B. "Hans Müller".
8. Geben Sie eine PIN ein (Mit der Sichtbar-Schaltfläche sehen Sie die PIN im Klartext).
9. Legen Sie ggfs. bis zu zwei weitere PINs an (Schaltfläche PinCode anlegen).

10. Wenn Sie weitere PinCode-Tastaturen mit Online-Erweiterung anlegen wollen, dann aktivieren Sie die Checkbox ☑ weitere anlegen.
    ↳ Mit dieser Checkbox bleiben Sie nach dem Speichern in dieser Ansicht und können sofort eine weitere PinCode-Tastatur mit Online-Erweiterung anlegen.
11. Klicken Sie auf die Schaltfläche Speichern.

↳ 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.

7.5 PinCode-Tastatur mit Online-Erweiterung löschen

✓ SmartBridge angelegt (Siehe *SmartBridges einrichten [▸ 38]*).
✓ Netzwerk eingerichtet und funktionsfähig (siehe *Netzwerk konfigurieren [▸ 45]*).
✓ 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 mitgelieferte Kurzanleitung) anschließend in jeder MobileKey-Schließanlage neu eingebunden werden.

↳ Online-PinCode-Tastatur ist gelöscht.

7.6 Netzwerk 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: *Schloss mit Online-Erweiterung funktioniert nicht [▸ 67]*.

7.7 Programmieren von Komponenten mit Online-Erweiterung

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

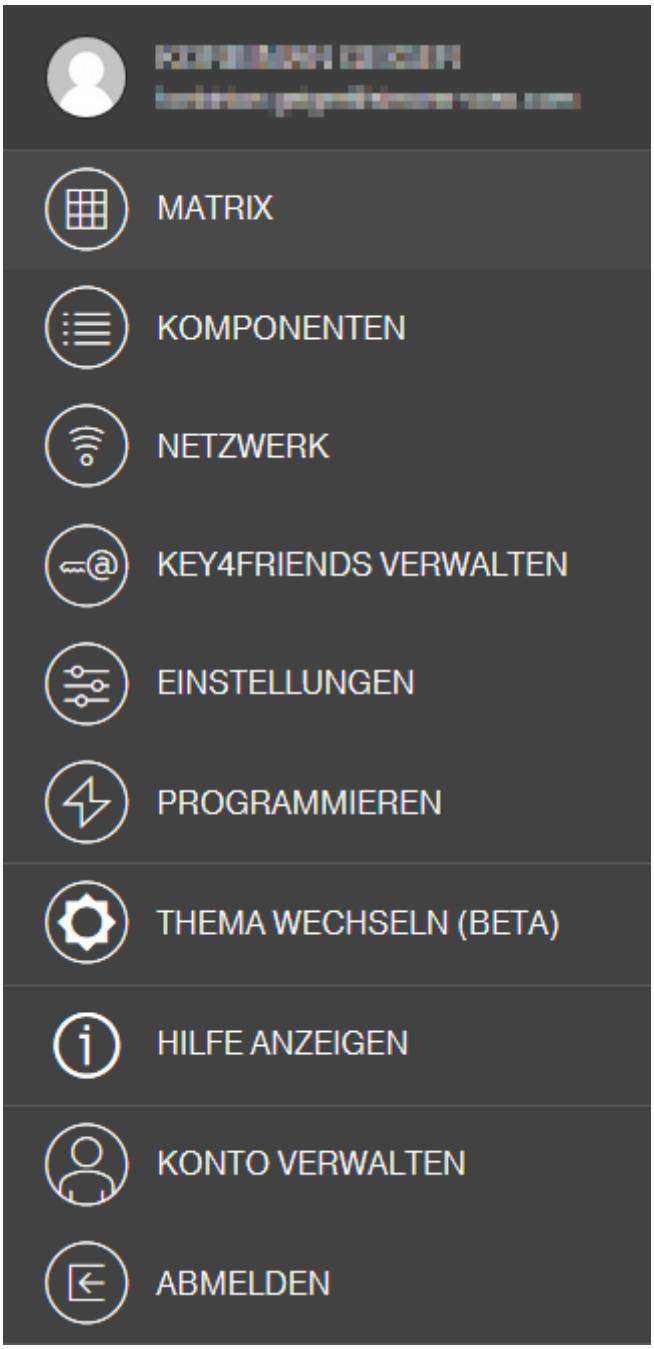
Programmieren Sie jedes Schloss bzw. jede Online-PinCode-Tastatur vor dem Einbau!

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.
- ✓ SmartBridge erfolgreich konfiguriert (siehe *Netzwerk konfigurieren [▸ 45]*).
- ✓ Matrixansicht geöffnet.

1. Legen Sie eine Komponente an.
2. Vergeben Sie gegebenenfalls Berechtigungen (wenn Sie Berechtigungen ändern wollen).
3. Klicken Sie auf die Menü-Schaltfläche (☰).
   - ↳ Menü öffnet sich.
   - ↳ Programmiervorgang startet über die SmartBridge.



4. Klicken Sie auf die Schaltfläche NETZWERK.
   ↳ Netzwerkübersicht öffnet sich.
5. Klicken Sie auf die Schaltfläche Konfiguration starten.
   ↳ Konfiguration mit neuer Komponente startet.
   ↳ Abschluss der Konfiguration wird über einen schnellen, sich dreimal wiederholenden Ton signalisiert (*Piep-Piep-Piep*).
   ↳ Der anschließend automatisch startende Programmiervorgang wird über die untere Message-Bar angezeigt.

↳ Programmierung abgeschlossen.

7.8 Verbindung zu Komponenten mit Online-Erweiterung trennen

Online-Komponenten können bei Bedarf wieder aus dem System entfernt 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.

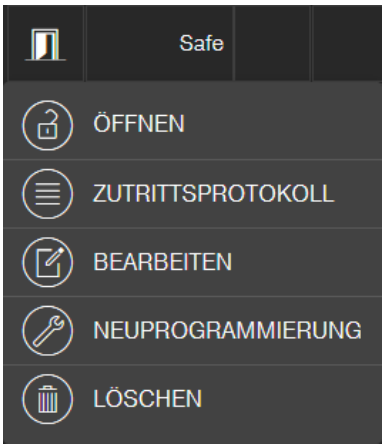
✓ Mindestens ein Online-Schloss bzw. eine Online-PinCode-Tastatur angelegt.
✓ Mindestens eine SmartBridge angelegt.

1. Klicken Sie auf die Menü-Schaltfläche.
   ↳ Kontextmenü 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 auf die Schaltfläche BEARBEITEN.
   ↳ Bearbeitungsmenü des Schlosses bzw. der PinCode-Tastatur öffnet sich.
5. Deaktivieren Sie die Checkbox ☐ ONLINE VERSION.
6. Klicken Sie auf die Schaltfläche Speichern.
7. Starten Sie die Onlinekonfiguration über die Schaltfläche Konfiguration starten.

7.9 Fernöffnung durchführen

- ✓ Schließanlage ordnungsgemäß konfiguriert.
- ✓ SmartBridge mit Internet verbunden.
- ✓ Fernzuöffnendes Schloss mit Online-Erweiterung.
- ✓ Fernzuöffnendes Schloss ordnungsgemäß konfiguriert (siehe *Schloss mit Online-Erweiterung anlegen [▸ 40]*).
- ✓ Matrixansicht geöffnet.

1. Klicken Sie auf die Schließung, die sie aus der Ferne öffnen wollen.
   ↳ Kontextmenü öffnet sich.



2. Klicken Sie auf die Schaltfläche ÖFFNEN.
   ↳ Der Befehl wird direkt über die SmartBridge zum Schloss geschickt. Wenn Sie diesen Befehl an ein geöffnetes Schloss im Daueröffnungs-Modus schicken, dann wird dieses Schloss geschlossen.

↳ Schloss wird geöffnet/geschlossen.

7.10 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.

HINWEIS

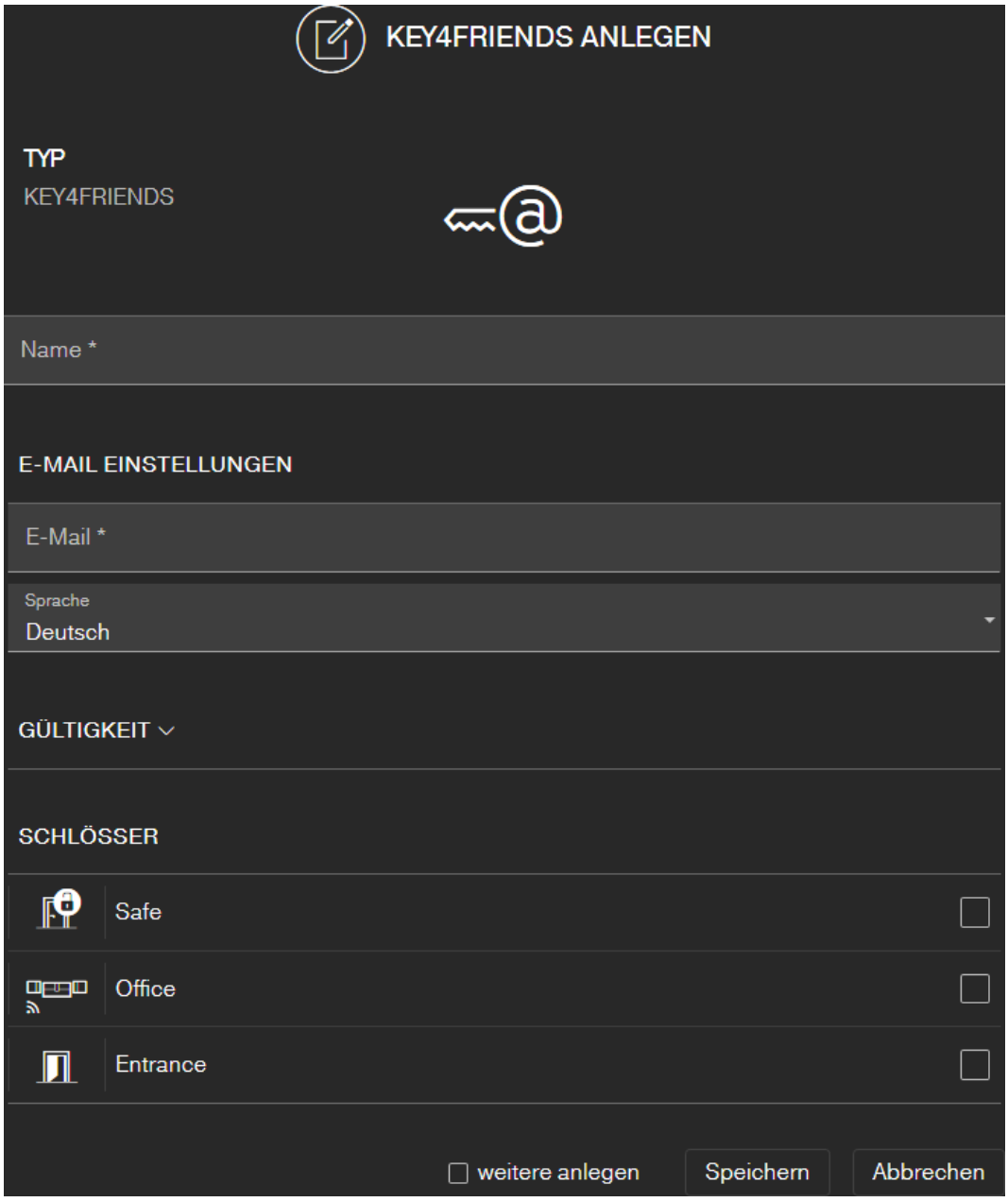
Offline-Rückfallebene für vernetzte Schließungen

Alle Funktionen der Online-Erweiterung (einschließlich Key4Friends) sind nur als Erweiterung und nicht als Ersatz der Offline-Funktionen ausgelegt. Sie sind kein Ersatz für Personen mit dauerhaften Berechtigungen oder als ausschließliche Zutrittsberechtigung an sicherheitskritischen Türen und Zugängen geeignet.

- Stellen Sie daher bei der Online-Erweiterung unseres Standardsystems (Offline), insbesondere bei der Verwendung mit Key4Friends oder Fernöffnungen, immer ein oder mehrere Offline-Backups zur Verfügung (PinCode-Tastatur (offline), Transponder).

↳ Diese physikalischen Identifikationsmedien kommunizieren direkt mit den Schlössern. Sie stellen jederzeit und netzwerkunabhängig den Zutritt an entsprechenden Türen und Zugängen sicher.

7.10.1 Schlüssel teilen



Die E-Mail enthält den in den Einstellungen angegebenen Namen (siehe *Einstellungen [▸ 59]*).

✓ Schließanlage ordnungsgemäß konfiguriert.
✓ Matrixansicht geöffnet.

1. Klicken Sie auf die Menü-Schaltfläche ☰.
   ↳ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche KEY4FRIENDS VERWALTEN.
   ↳ Komponentenübersicht öffnet sich.
3. Klicken Sie auf die Schaltfläche ⊕ Key4Friends anlegen.
4. Geben Sie den Namen und die E-Mail-Adresse des Empfängers ein.

5. Wählen Sie im Dropdown-Menü ▼ **Sprache** die Sprache der E-Mail aus (Dänisch, Niederländisch, Englisch, Französisch, Deutsch, Italienisch oder Schwedisch).
6. Schränken Sie ggfs. die Gültigkeit des Schlüssels ein.
7. Markieren Sie alle Schlösser, an denen der Schlüssel gültig sein soll.

HINWEIS

Key4Friends nur mit Online-Erweiterung

Die Key4Friends-App sendet über die SmartBridge einen Fernöffnungsbefehl (vergleiche *Fernöffnung durchführen [▸ 48]*) und funktioniert nur mit Online-Erweiterung. Deshalb können Sie hier nur Schlösser mit Online-Erweiterung markieren.

8. Aktivieren Sie optional die Checkbox ☑ weitere anlegen.
   ↳ Mit dieser Checkbox bleiben Sie nach dem Speichern in dieser Ansicht und können sofort ein weiteres Schloss mit Online-Erweiterung anlegen.
9. Klicken Sie auf die Schaltfläche Speichern.

↳ 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 [▸ 51].

HINWEIS

Das Zeitfenster von geteilten Schlüsseln ist auf sechs Monate beschränkt.

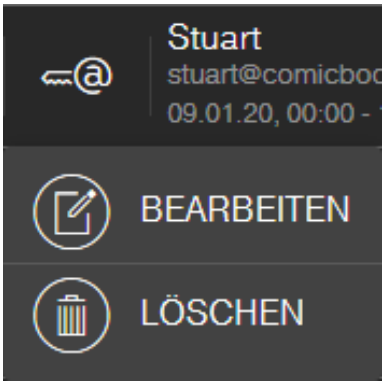
- Wenn Sie Freunden dauerhaft Zutritt gewähren wollen, dann verwenden Sie Transponder oder eine PinCode-Tastatur.

7.10.2 Schlüssel verwalten

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

✓ Schließanlage ordnungsgemäß konfiguriert.
✓ Matrixansicht geöffnet.

1. Klicken Sie auf die Menü-Schaltfläche ☰.
   ↳ Menü öffnet sich.
2. Klicken Sie auf die Schaltfläche KEY4FRIENDS VERWALTEN.
   ↳ Komponentenübersicht öffnet sich. Sie sehen in der Rubrik KEY4FRIENDS alle Key4Friends.
3. Klicken Sie auf den Key4Friend, den Sie bearbeiten oder löschen wollen.
   ↳ Kontextmenü öffnet sich.



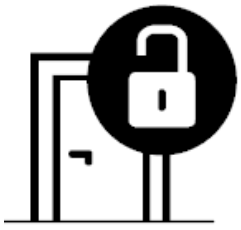
4. BEARBEITEN oder LÖSCHEN Sie den Key4Friend.

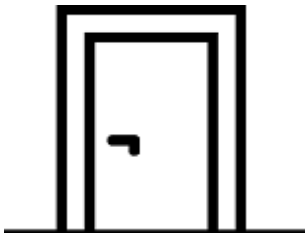
BEARBEITEN	LÖSCHEN
Damit bearbeiten Sie die Eigenschaften des Key4Friends: ■ Name ■ Gültigkeit ■ Schlösser, für die der Key4Friend gilt	Damit löschen Sie den Key4Friend. Mit diesem Key4Friend kann dann kein Schloss mehr geöffnet werden.

7.11 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.

Symbol	Beschreibung
	Tür sicher geschlossen und Schloss verriegelt.
	Tür zu lange geöffnet. Legen Sie die Zeit nach der Erstprogrammierung (siehe *Programmieren von Komponenten mit Online-Erweiterung [▸ 45]*) in den Schlosseinstellungen (siehe *Schloss mit Online-Erweiterung anlegen [▸ 40]*) fest: ■ Nie ■ 30 Sekunden ■ Eine Minute ■ Zwei Minuten ■ Fünf Minuten
	Tür geschlossen. Verriegelungszustand nicht überwacht.

Zusätzlich können bei Ihrem DoorMonitoring-Schloss weitere Warnungen angezeigt.

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 mit Online-Erweiterung [▸ 45]*

VORSICHT

Riegel nicht überwacht

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

- Verzichten Sie auf den Daueröffnungs-Modus, wenn Sie den Riegel ebenfalls überwachen wollen.

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

Bitte beachten Sie, dass Ihr MobileKey-Netzwerk erfolgreich konfiguriert sein muss! Die Status von Smartbridge und DoorMonitoring-Schloss müssen beide stets "ONLINE" sein. *Siehe Schloss mit Online-Erweiterung funktioniert nicht [▸ 67] für weitere Hilfe.*

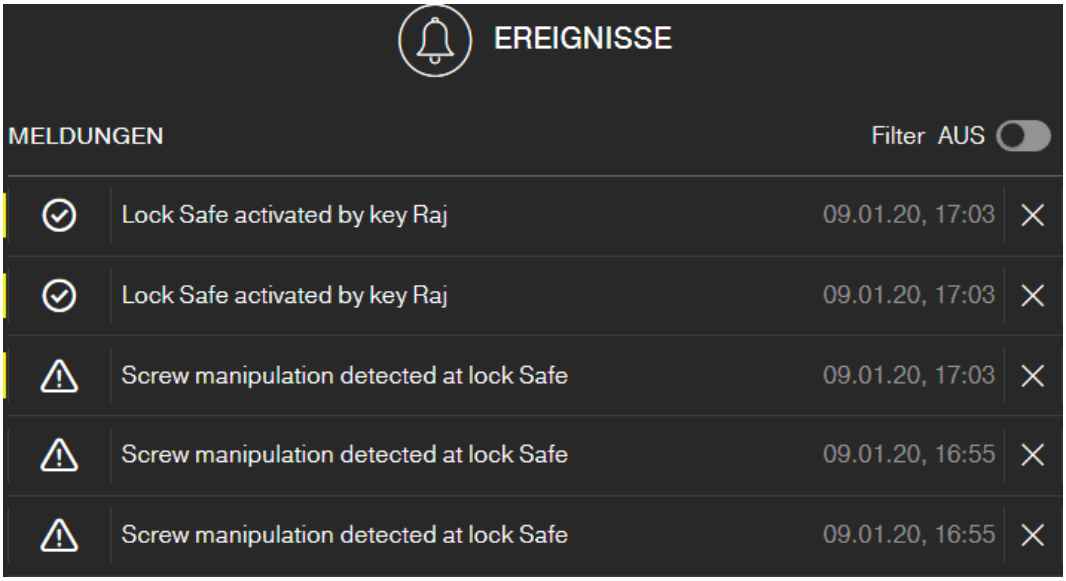
8. Ereignismanagement

Lassen Sie sich mit dem MobileKey-Ereignismanagement bei bestimmten, von Ihnen festgelegten, Ereignissen benachrichtigen:

Ereignistyp	Bedeutung
Zutritt	Wählen Sie Schlüssel, Schlösser und einen Zeitraum aus. Wenn einer dieser Schlüssel innerhalb des Zeitraums an einem dieser Schlösser benutzt wird, dann erhalten Sie eine Benachrichtigung.
DoorMonitoring	Wählen Sie DoorMonitoring-Ereignisse, Schlösser und einen Zeitraum aus. Wenn eines dieser DoorMonitoring-Ereignisse (siehe *DoorMonitoring Schloss - Angezeigte Schlosszustände [▸ 52]*) innerhalb des Zeitraums an einem dieser Schlösser auftritt, dann erhalten Sie eine Benachrichtigung.
Alarm	Wählen Sie aus, über welche Probleme Sie benachrichtigt werden wollen: ▪ Batterie schwach ▪ Netzwerkfehler ▪ Einbruch ▪ Hardwareproblem

Sie erhalten diese Benachrichtigungen über verschiedene Kanäle:

- E-Mail-Versand an verschiedene Adressen
- Push-Benachrichtigungen auf Ihr Smartphone (nur bei laufender MobileKey-App)
- MobileKey-Web-App (Klick auf die Schaltfläche Ereignisse)



An diesem Symbol wird Ihnen auch angezeigt, wenn neue Ereignisse vorliegen, die Sie noch nicht gesehen haben.

Filtern

Sie können die angezeigten Ereignisse filtern. Aktivieren Sie dazu den Filter und stellen Sie Ihn nach Bedarf ein.

8.1 Regeln erstellen

Erstellen Sie individuelle Ereignisse:

✓ Matrixansicht geöffnet.

1. Klicken Sie auf die Schaltfläche Ereignisse.
   ↳ Ereignisübersicht öffnet sich.
2. Klicken Sie auf die Schaltfläche Regeln verwalten.
   ↳ Regelverwaltung öffnet sich.
3. Klicken Sie auf die Schaltfläche Regel anlegen.
4. Folgen Sie dem Assistenten.

↳ Regel angelegt. Sie erhalten bei Eintritt des von Ihnen festgelegten Ereignisses eine Benachrichtigung.

Übersicht über die zur Verfügung stehenden Ereignistypen

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.

DoorMonitoring

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.

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.

Auslöser	Beschreibung
Einbruch	Eine Benachrichtigung wird verschickt, sobald ein DoorMonitoring-Schloss einen Einbruchsversuch detektiert.
Hardwarefehler	Eine Benachrichtigung wird verschickt, sobald ein Hardwarefehler erkannt wird.

8.2 Wichtige Hinweise

HINWEIS

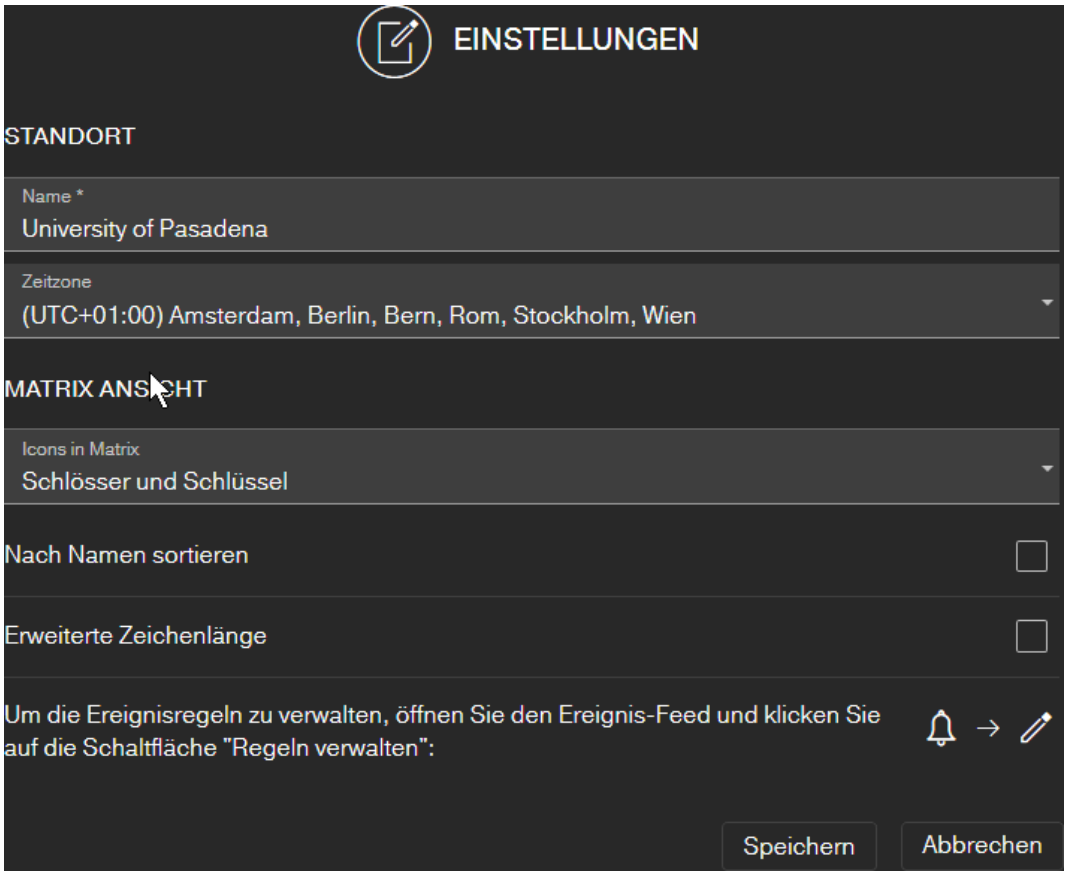
Alle Events werden über die SmartBridge übertragen. Sie erhalten keine Benachrichtigungen über Events, wenn die Internetverbindung gestört oder die Stromversorgung unterbrochen wurde. Über den Zeitraum, in dem die SmartBridge nicht ordnungsgemäß online ist, gehen alle auftretenden Events verloren.

Eine Benachrichtigung vom Typ "ALARM" wird in jedem Fall empfohlen. So können Sie dieses Event einrichten: *Regeln erstellen [▸ 56]*

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.

9. Einstellungen

Rufen Sie die Einstellungen über die Menü-Schaltfläche ☰ und die Schaltfläche ⚙ EINSTELLUNGEN auf:



Standort der Schließanlage

Geben Sie hier den *Namen des Standorts* (z.B. Büro) und die *Zeitzone des Standorts* an.

Die Standortangabe wird auch in der exportierten Komponentenliste verwendet (siehe *Komponentenliste exportieren [▸ 28]*).

Matrixansicht

Passen Sie hier die Darstellung Ihrer Matrix an:

Einstellung	Auswirkung
Icons in Matrix	Wählen Sie zwischen folgenden Darstellungsmöglichkeiten: ▪ Schlösser und Schlüssel (Standard) ▪ Nur Schlösser ▪ Alle ausgeblendet

Einstellung	Auswirkung
Nach Namen sortieren	Wenn die Checkbox ☑ Nach Namen sortieren aktiviert ist, dann werden die Einträge in der Matrix alphabetisch sortiert. Wenn die Checkbox ☐ Nach Namen sortieren nicht aktiviert ist, dann werden die Einträge in der Matrix in der Reihenfolge angezeigt, in der sie erstellt wurden.
Erweiterte Zeichenlänge	In der Matrix werden der besseren Übersicht halber nur 16 Zeichen der Komponentennamen angezeigt. Wenn Sie die Checkbox ☑ Erweiterte Zeichenlänge aktivieren, dann werden in der Matrix 22 Zeichen der Komponentennamen angezeigt.

10. Fehlerbehebung

Im Folgenden werden Hilfestellungen zu möglichen Alltagsproblemen gezeigt.

10.1 Schlüssel verloren, beschädigt oder gestohlen

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 Programmierung aller Schlösser.

So ersetzen Sie einen nicht mehr vorhandenen oder defekten Schlüssel:

✓ Matrixansicht geöffnet.

1. Suchen Sie den betroffenen Schlüssel im Schließplan.
2. Klicken Sie den Schlüssel im Schließplan an.
   ↳ Kontextmenü öffnet sich.

3. Klicken Sie auf die Schaltfläche LÖSCHEN.
   ↳ Schlüssel wird zum Zurücksetzen vorgemerkt.
   ↳ Aufgabe wird später in der Programmier-App abgearbeitet.
4. Klicken Sie auf den betroffenen Schlüssel im Schließplan.
   ↳ Kontextmenü öffnet sich.

5. Klicken Sie auf die Schaltfläche "LÖSCHEN ERZWINGEN".
   ↳ Schlüssel ist im Schließplan gelöscht.
   ↳ Schlüssel ist noch nicht im Schloss gesperrt.
6. Legen Sie gegebenenfalls einen neuen Schlüssel an (siehe *Schlüssel anlegen [▸ 18]*).
7. Vergeben Sie gegebenenfalls nötige Berechtigungen (siehe *Berechtigung vergeben und abspeichern [▸ 21]*).
8. Klicken Sie auf die Schaltfläche SAVE.
   ↳ Änderungen sind gespeichert (Schlösser mit Online-Erweiterung werden bei bestehender Netzwerkverbindung automatisch programmiert).
9. Klicken Sie auf die Menü-Schaltfläche ☰.
   ↳ Menü öffnet sich.
10. Klicken Sie auf die Schaltfläche PROGRAMMIEREN.
    ↳ Programmier-App startet.
11. 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 der Schlüssel gelöscht wurde und die Schlösser neu programmiert wurden.

- Programmieren Sie bei Schlüsselverlust sofort alle berechtigten Schlösser neu.

10.2 Schloss defekt

Schlösser bzw. Schließzylinder können unter Umständen einen Defekt erleiden. Wechseln Sie zunächst die Batterien des Schlosses (siehe mitgelieferte Kurzanleitung). Versuchen Sie dann erneut, das Schloss zu programmieren.

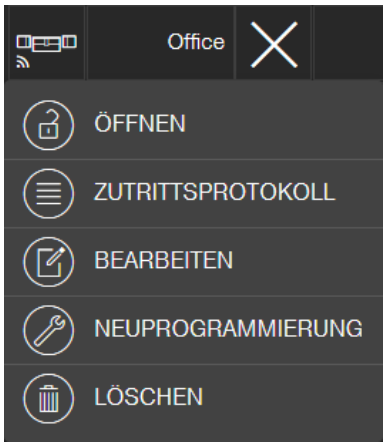
Funktioniert das Schloss immer noch nicht korrekt, muss dieses ausgetauscht werden.

Tauschen Sie das Schloss auch einfach aus, wenn Sie ein Schloss mit anderen Eigenschaften verwenden wollen.

Gehen Sie folgendermaßen vor, um ein Schloss auszutauschen:

✓ Matrixansicht geöffnet.

1. Entfernen Sie das betroffene Schloss aus der Tür.
   Es ist unter Umständen schwierig, ein Schloss aus einer verschlossenen Tür zu entfernen. Fragen Sie ggfs. den Fachhändler, der Ihnen die SimonsVoss-Produkte installiert hat, um Rat.
2. Klicken Sie im Schließplan auf das betroffene Schloss.
   ↳ Kontextmenü 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.
   ↳ Kontextmenü öffnet sich.
5. Klicken Sie auf die Schaltfläche LÖSCHEN ERZWINGEN".
   ↳ Schloss wird im Schließplan unwiderruflich gelöscht.
6. Legen Sie ein neues Schloss an (siehe *Schloss anlegen [▸ 17]* oder *Schloss mit Online-Erweiterung anlegen [▸ 40]*).
7. Vergeben Sie nötige Berechtigungen (siehe *Berechtigung vergeben und abspeichern [▸ 21]*).
8. Klicken Sie auf die Schaltfläche SAVE.

9. Klicken Sie auf die Menü-Schaltfläche .
   ↳ Menü öffnet sich.
10. Klicken Sie auf die Schaltfläche PROGRAMMIEREN.
    ↳ Programmier-App startet.
11. Führen Sie alle Aufgaben durch.

↳ Programmierung wird durchgeführt.

10.3 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.

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

10.4 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.

So lesen Sie MobileKey-Komponenten aus:

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.

Sie können alternativ die Komponentenliste exportieren (siehe *Komponentenliste exportieren [▸ 28]*).

10.5 SmartBridge funktioniert nicht

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.
  - Sind die **Ports 1883 und 8883** (TCP/IP) der Firewall geöffnet?

    Fügen Sie ggf. entsprechende Ausnahmen oder Weiterleitungen in Ihrem Router hinzu, um die SmartBridge über die Ports 1883 und 8883 nach außen kommunizieren zu lassen. Suchen Sie nach *Portfreigaben*, *Portweiterleitungen*, *Speziellen Anwendungen* oder ähnlichem.

HINWEIS

Portfreischaltung geräteabhängig

Im Regelfall erkennen Router selbständig, dass die SmartBridge über den Port 8883 kommunizieren will und gibt den Port frei.

- In Ausnahmefällen oder in höher gesicherten Netzwerken müssen Sie den Port manuell freigeben (siehe folgende Beispiele).

Liste "Spezielle Anwendungen"

Name	Status	Trigger-Port	Trigger-Protokoll	Protokoll öffnen	Port öffnen	Optionen
TCP2	An	8883	TCP/UDP	TCP/UDP	8883	Bearbeiten Löschen

Hinzufügen

Freigaben

Status	Bezeichnung	Protokoll	IP-Adresse im Internet	Port extern vergeben		
	MobileKey	TCP	IPv4	8883 (8883)		

Neue Freigabe

- Ist der DHCP-Server so konfiguriert, dass sich ein Gerät im Netzwerk anmelden kann?

  Sie erreichen über einen Windows-PC 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*) in den Software-Downloads.

  Detaillierte Informationen zum OAM-Tool finden Sie im Handbuch zum OAM-Tool.

HINWEIS

Verwendung fester IP-Adressen

Standardmäßig ist DHCP aktiviert. Die IP-Adresse wird automatisch vergeben. Alternativ können Sie auch eine feste IP-Adresse vergeben.

- Wenn Sie eine feste IP-Adresse verwenden, dann tragen Sie einen DNS (Domain Name Service) über das OAM-Tool ein.

- 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. Platzieren Sie ggfs. weitere SmartBridges.

HINWEIS

Zurücksetzen der SmartBridge

Die SmartBridge kann über einen Hardware-Reset auf die Werkseinstellungen zurückgesetzt werden (siehe mitgelieferte Kurzanleitung bzw. Handbuch).

10.6 PinCode-Tastatur mit Online-Erweiterung funktioniert nicht

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

1. Prüfen Sie den **Batteriezustand**. Führen Sie einen Batterietest durch (siehe mitgelieferte Kurzanleitung).
2. Prüfen Sie, ob die **Chip-IDs** korrekt eingegeben wurden.
3. Prüfen Sie die richtige Zuweisung des Schlosses zur Online-PinCode-Tastatur (siehe *PinCode-Tastatur mit Online-Erweiterung anlegen [▸ 43]*).

10.7 Schloss mit Online-Erweiterung funktioniert nicht

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

1. Prüfen Sie, ob die **Chip-IDs** der Schlösser alle korrekt eingegeben wurden.
2. Prüfen Sie den **korrekten Einbau der Netzwerkknaufkappe (LockNode)**. Siehe auch mitgelieferte Kurzanleitung.
   ↳ Nach dem korrekten Einbau der Netzwerkknaufkappe hören Sie vier kurze Töne.
3. Prüfen Sie bei der Nachrüstung oder dem Austausch von Netzwerkknaufkappen die richtige Zuweisung der Schlösser!

10.8 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.

10.9 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 Komponenten mit Online-Erweiterung trennen [▸ 47]*.

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.

11. Wartung, Reinigung und Desinfektion

ACHTUNG

Beschädigung der Oberflächen

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

1. Halten Sie Öl, Farbe, Fett oder Säure von Ihren MobileKey-Komponenten fern.
2. Verwenden Sie nur Desinfektionsmittel, die ausdrücklich zur Desinfektion empfindlicher metallischer Oberflächen bzw. Kunststoffe vorgesehen sind.

VORSICHT

Batteriewechsel

Leere Batterien müssen stets durch neue, von SimonsVoss freigegebene, Batterien ersetzt werden (Siehe jeweilige Kurzanleitung). Alte Batterien sind stets fachgerecht zu entsorgen!

12. 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.*

13. Tipps & Tricks

13.1 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!

13.2 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.
   ↳ Die Programmierung erfolgt online über die SmartBridge.

↳ Schlüssel sind an gewählten Schlössern berechtigt.

13.3 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 die Schaltfläche KONTO VERWALTEN.
   ↳ Kontoübersicht öffnet sich
3. Klicken Sie im oberen Bereich der Kontoübersicht auf die Schaltfläche SPRACHEN.
   ↳ Auswahlmenü für Sprachen wird geöffnet.
4. Wählen Sie Ihre gewünschte Sprache aus.

↳ Sprache ist eingestellt.

Kehren Sie mit der Schaltfläche HOME zurück zur Matrix.

14. Hilfe und weitere Informationen

Infomaterial/Dokumente

Detaillierte Informationen zum Betrieb und zur Konfiguration sowie weitere Dokumente finden Sie auf der Homepage:

https://www.simons-voss.com/de/dokumente.html

Software und Treiber

Software und Treiber finden Sie auf der Website:

https://www.simons-voss.com/de/service/software-downloads.html

Konformitätserklärungen und Zertifikate

Konformitätserklärungen und Zertifikate finden Sie auf der Homepage:

https://www.simons-voss.com/de/zertifikate.html

Technischer Support

Unser technischer Support hilft Ihnen gerne weiter (Festnetz, Kosten abhängig vom Anbieter):

+49 (0) 89 / 99 228 333

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

support-simonsvoss@allegion.com

FAQ

Informationen und Hilfestellungen finden Sie im FAQ-Bereich:

https://faq.simons-voss.com/otrs/public.pl

Adresse

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Deutschland

Das ist SimonsVoss

SimonsVoss, der Pionier funkgesteuerter, kabelloser Schließtechnik, bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, kleine und große Unternehmen 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. Damit wird SimonsVoss als ein Technologieführer bei digitalen Schließsystemen angesehen.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs.

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).

Made in Germany

Für SimonsVoss ist „Made in Germany“ ein ernsthaftes Bekenntnis: Alle Produkte werden ausschließlich in Deutschland entwickelt und produziert.

© 2024, SimonsVoss Technologies GmbH, Unterföhring

Alle Rechte vorbehalten. Texte, Bilder und Grafiken unterliegen dem Schutz des Urheberrechts.

Der Inhalt dieses Dokuments darf nicht kopiert, verbreitet oder verändert werden. Technische Änderungen vorbehalten.

SimonsVoss und MobileKey sind eingetragene Marken der SimonsVoss Technologies GmbH.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION