MobileKey

Manual

09.09.2019

SimonsVoss technologies

Contents

1 Introduction

MobileKey is a separate product category for small locking systems. Up to 100 keys *(transponders)* and 20 locking devices *(locking cylinders and SmartRelays)* are supported.

IMPORTANT

The locking plan is managed using the MobileKey web application only. You can access the application at *www.my-mobilekey.com*. Just click on "Login web app" to access the application directly. Here, you simply create a free user account to work with MobileKey.

1.1 Safety instructions

CAUTION

Access through a door may be blocked due to incorrectly installed or incorrectly programmed SimonsVoss components. SimonsVoss Technologies GmbH is not liable for consequences of incorrect installation, such as blocked access to injured persons, physical damage or any other losses.

IMPORTANT

SimonsVoss Technologies GmbH accepts no liability for damage caused to doors or components due to incorrect fitting or installation.

IMPORTANT

SimonsVoss components may only be used for its intended purpose: opening and locking doors. No other use is permitted.

IMPORTANT

Modifications or further technical developments cannot be excluded and may be implemented without prior notice.

IMPORTANT

All options in the online extension require a correctly configured MobileKey radio network. You can only perform any of the online functions if a stable Internet connection and power supply are guaranteed.

1.2 System requirements

1.2.1 Locking system management

The locking plan can be **displayed and edited** using any standard browser, irrespective of the platform. Basically, no special hardware is required, although the terminal device should support the latest version of one of the following browsers:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome
- Apple Safari
- Opera

You also need to have a permanent internet connection at all times. A high-speed Internet access is required to work without interruption.

1.2.2 Programming

You can programme the MobileKey locking components with the USB config device with the following devices:

- **Windows device**
  - Operating system: Windows Server 7, 8 or 10.
  - Hardware: USB port to connect the USB config device.

    No special hardware configurations are required for programming. The operating system must be stable and run free of errors.
  - The current version of Microsoft .NET Framework (at least Version 3.5) must be installed on the computer.

  Follow the instructions on programming app installation to programme the MobileKey locking components.

- **Android device**
  - You need to install the programming app from the Google Play Store to use the MobileKey app.

    Changes to the locking plan are made in the browser, such as the MobileKey web app.
  - The USB config device can be connected directly to the Android device or using an OTG cable available separately.

The Android device must support the OTG function in such a case. If you are not sure whether your Android device supports OTG or not, you can use a suitable app from Google Play to check this function. Search for "OTG check", for example.

Important: Such apps have nothing to do with SimonsVoss Technologies GmbH. We therefore accept no liability for any damages or problems caused by such apps.

Use the MobileKey web app to launch the MobileKey app to programme the MobileKey locking components.

- **macOS device**
  - Operating system: OS X 10.11 El Capitan or higher
  - Hardware: USB port to connect the USB config device.

    No special hardware configurations are required for programming. The operating system must be stable and run free of errors.
- **Optional: Online via SmartBridge**

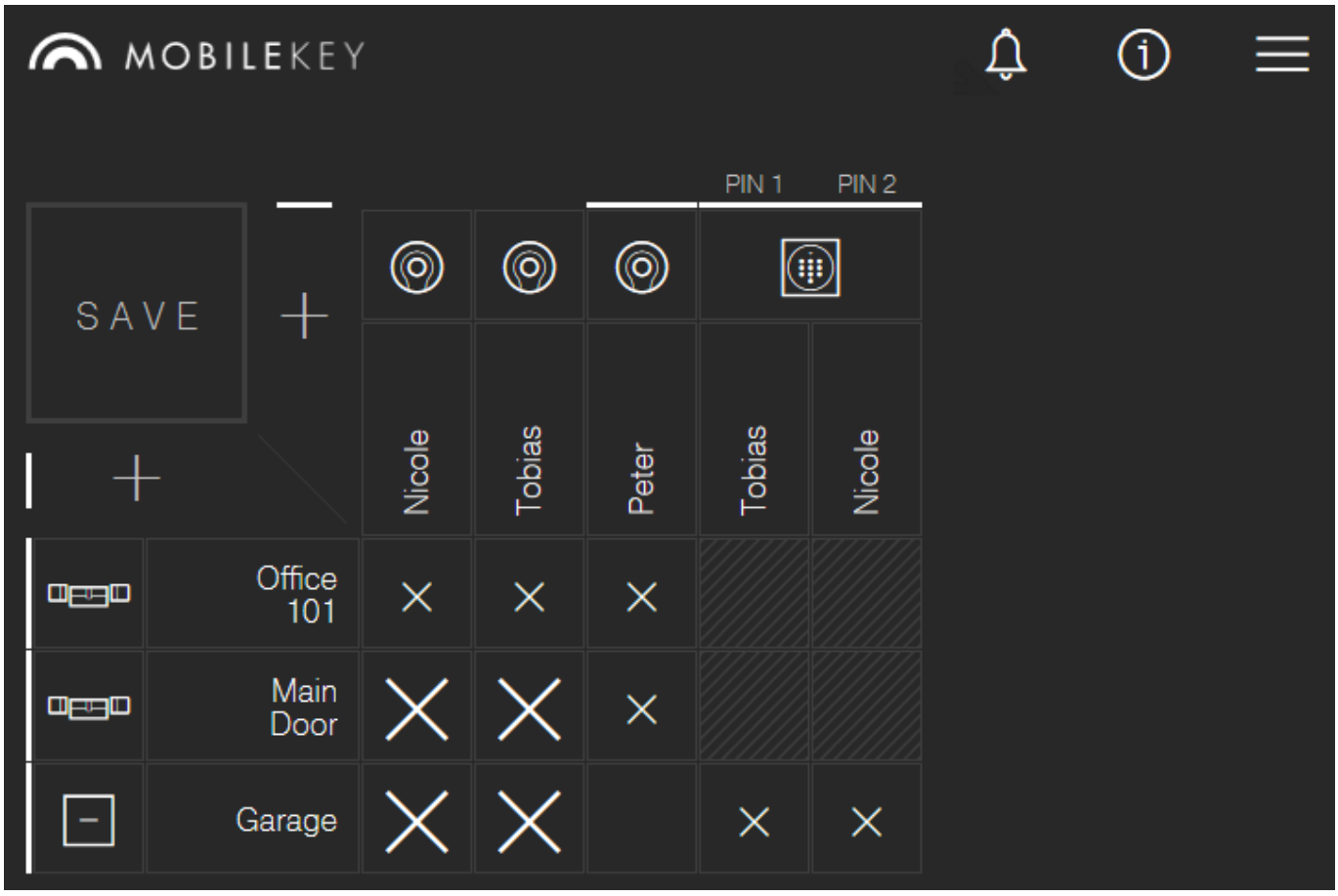
  Locking devices can also be programmed online with a USB config device. See *Programming components [▸ 22]*. *In this particular case, only the transponders need to be programmed with the aid of the USB config device.*

  Tip:

  If there should be no Windows or Android devices available for programming new keys, it is recommended to programme additional transponders as a reserve. These can then be assigned to networked online locks at a later stage. See Using keys without the USB config device [▸ 40] for more information.

2 The matrix

The matrix provides a clearly arranged view of the entire locking system. This view is thus the centre point for all functions. All keys (e.g. transponders) are displayed horizontally and all locking devices (e.g. locking cylinders) vertically. You can use the "Message centre", "Help" and "Menu" icons to access key menus.



Different systems are used to keep the matrix as straightforward as possible.

Authorisations

SYMBOL	DESCRIPTION
×	**Authorisation cross: New** Authorisation has been configured, but not programmed yet.
×	**Authorisation cross: Set** The authorisation has been set and is active.
×	**Authorisation cross: Remove** Authorisation has been configured, but not programmed yet.

	Authorisation cross: No authorisation If none of the previous three crosses are displayed, there is currently no authorisation at this position.

Locking devices & keys

SYMBOL	DESCRIPTION
	**Locking device: Locking device** This component is either a locking device or a locking cylinder. *An additional wireless symbol in the bottom, left-hand corner indicates whether the locking device features a LockNode for MobileKey ONLINE or not.*
	**Locking device: SmartRelay** This component is a SmartRelay. *An additional wireless symbol in the bottom, left-hand corner indicates whether the locking device features a LockNode for MobileKey ONLINE or not.*
	**Key: Transponder** This component is a transponder.
	**Key: PIN code keypad** This component is a PIN code keypad.

Also see

- *Help for online locking devices [▸ 35]*
- *Help for SmartBridge [▸ 34]*

3 Basic functions

A setup wizard will appear the first time that you log on to a MobileKey account, making it easy to configure. This wizard will help you to add locking devices and keys quickly and conveniently.

3.1 Creating a lock

✓ Matrix screen open

1. Click on the Add lock icon (plus sign beneath the "SAVE" button).
2. Select the lock type, e.g. "CYLINDER" for a normal locking cylinder.
3. Assign a name, e.g. front door.
4. Click on the "Opening duration in seconds" or "Permantently open" button.
   ↳ If you have activated "Permantently open", the lock will remain engaged ready for use until it is actuated again with a key or by remote opening.

CAUTION

Security risk with permanent opening

A door which is permanently open may pose a security risk. SimonsVoss Technologies GmbH therefore recommends limiting the opening time interval.

5. Click on the "SAVE" or "SAVE + COPY" button.
   ↳ "SAVE" saves the lock and takes you back to the matrix screen.
   ↳ "SAVE + COPY" saves the lock device and prepares another locking device with the same properties.

IMPORTANT

Extended network settings are shown first if at least one SmartBridge has been added and configured. Further online options, such as the interval for "Door left open", are visible once the DM locking devices have been programmed for the first time.

IMPORTANT

In the case of **SmartRelay 2**, it is possible **to invert the output (relay contact)**, but you need to add and programme a SmartRelay first. The "OUTPUT CONFIGURATION" setting will then be visible with the "Invert output" option in the SmartRelay properties. If you activate this option, the SmartRelay needs to be reprogrammed.

3.2 Add key

✓ Matrix screen open

1. Click on the Add lock icon (plus sign next to the "SAVE" button).
2. Select the key type, e.g. "TRANSPONDER".
3. Assign a name, e.g. "John Smith".
4. Specify the validity if necessary.
   ↳ "Valid from": Specify a date from when the key is to be authorised in the locking system.
   ↳ "Valid to": Specify a date until when the key is to be authorised in the locking system.
5. Click on the "SAVE" or "SAVE + COPY" button.
   ↳ "SAVE" saves the key and takes you back to the matrix screen.
   ↳ "SAVE + COPY" saves the key and prepares another key with the same properties.

↳ New key is added.

3.3 Add PIN code keypad

This section describes how to set up a PIN code keypad without an online extension. If you have a PIN code keypad with an online extension, proceed as described in the section *Create Online PIN Code Keypad [▸ 20]*.

✓ PIN code keypad already configured; see Configuration *(master PIN and at least one user PIN must be configured!)*
✓ Lock added for PIN code keypad
✓ Matrix screen open

1. Click on the Add lock icon (plus sign next to the "SAVE" button).
2. Select "PIN CODE KEYPAD" type.
3. Select locking device on which the PIN code keypad is to be operated.
4. Assign a name for PIN 1 *(corresponds to user PIN 1)* , e.g. "John Smith". The white checkbox for PIN 1 is already active.
5. Also issue names for PIN 2 and 3 if you wish. You first need to activate the white check boxes to activate the PINs.
6. Click on the "SAVE" or "SAVE + COPY" button.
   ↳ "SAVE" saves the key and takes you back to the matrix screen.
   ↳ "SAVE + COPY" saves the key and prepares another key with the same properties.

IMPORTANT

Up to 3 user PINs can be configured directly on the PIN code keypad. These user PINs must be activated in the web app when the PIN code keypad is assigned to a locking device.

IMPORTANT

Individual user PINs for an existing PIN keypad can be changed by clicking on the corresponding button in the matrix and selecting 'EDIT'.

3.4 Issue authorisation and save

Authorisations can be issued or withdrawn on the matrix screen.

- Authorising key at locking device: Click on the empty field at the intersection point between the key and locking device to add a cross.

  The cross is displayed reduced in size until the new authorisation has been programmed. Once programming is successfully complete, the cross fills the entire matrix square.

- Revoking a key's authorisation for a locking device: Click on the empty field at the intersection point between the key and locking device to remove the authorisation cross.

  The cross is not shown completely until the new change has been programmed. The authorisation cross will not disappear completely until programming is successfully complete.

IMPORTANT

Changes are displayed with yellow borders. These must be saved (or applied) before programming using the 'SAVE' button.

IMPORTANT

All component changes and authorisations must be programmed using the programming app before they actually come into effect.

3.5 Assign time plan

This additional function is optional, so you don't necessarily need to use it.

There are basically two types of time plans:

- Weekly: Individual time intervals can be assigned to each day of the week. EXAMPLE: The housekeeper only has access on certain days and at certain times – e.g. Mondays 8 a.m. to noon and Thursdays 1 p.m. to 3.30 p.m.
- Daily: A general time zone plan can be created for an entire week. EXAMPLE: Employee John Dorian is authorised to activate locking devices between 7 a.m. and 7 p.m. from Mon to Fri.

Proceed as follows to assign a time plan to a key:

✓ Matrix screen open

1. Click on the required key on the matrix screen.
   ↳ Menu opens.
2. Click on the "TIME SCHEDULE" button.
3. Select the time schedule type.
   ↳ Weekly: Select day and "Create time interval". Several time intervals can be selected on different days.
   ↳ Daily: Click on "exclude weekends" if the schedule is to apply from Monday to Friday only. Then a "Create time interval". Several time intervals can be added.
4. Click on the "SAVE" button.
   ↳ Key is saved.
   ↳ Matrix screen is displayed.

↳ Key is assigned to the time schedule.

IMPORTANT

If a time interval extends beyond midnight, you need to add two time intervals: One time interval for "Time before midnight to midnight" and "Midnight to the time after midnight".

3.6 Programming components

IMPORTANT

Programme each lock or Online PIN Code Keypad before installing it.

Proceed as follows to launch the programming app from the MobileKey web app and thus complete the individual programming tasks:

✓ Programming tasks pending (shown on respective components in matrix)

1. Click on the menu button.
   ↳ Menu opens.
2. Click on the button PROGRAMMING.
   ↳ The programming app launches.
3. Log on if required.
   ↳ Task list shows components requiring programming.
4. Execute all pending tasks.
5. Click on the first component to start programming it.

6. Then follow the instructions in the programming app.

3.6.1 IMPORTANT: Programming on a Windows device

You need to download and install the programming app once. You also need to enter the user name and password. The USB config device must be connected to the computer's USB port to programme.

You will be directed to this installation as soon as you click on Menu/ Programme. The message which appears will display the direct download link. Install the programming app. You will need administrator rights to install it.

Take hardware requirements into account: *Programming [▸ 5]*

Also see

- *Programming [▸ 5]*

3.6.2 IMPORTANT: Programming on an Android device

Download the free MobileKey app from the Google Play Store and connect the config device to the Android device, using an OTG cable available separately if necessary.

Launch the app one time to enter your user name and password.

Take hardware requirements into account: *Programming [▸ 5]*

Also see

- *Programming [▸ 5]*

3.6.3 IMPORTANT: Programming on a macOS device

You need to install a service one time for programming in macOS. A prompt will appear if the service has not yet been installed or has not been launched. You must not quit the browser when the service is running. Devices with an activated online extension do not need to be programmed. There are two options for programming keys and locks without an online extension in macOS.

Take hardware requirements into account: *Programming [▸ 5]*

Programming in the menu

The first option is to programme using the context menu. This method is suitable if few keys or locks have been changed.

1. Click on the components which need to be programmed.
   ↳ Menu opens.
2. Click on the button PROGRAMMING.
   ↳ Programming window opens.

3. Follow the instructions on the screen.

↳ Programming is complete.

Programming with programming list

The second option is to programme using the programming list. This method is suitable if many keys or locks have been changed in the matrix.

✓ Matrix screen open

1. Click on the menu button.
   ↳ Menu opens.
2. Click on the button PROGRAMMING.
   ↳ Programming list opens.
3. Click on a component in the list which needs to be programmed.
4. Follow the instructions on the screen.
   ↳ Component is programmed.
5. Click on the next component in the list to programme it.

↳ Programming is complete.

3.7 Resetting components

Components can be easily reset. After a reset, they are in storage mode and can be used in another system.

1. Click on the component you require.
   ↳ Menu opens.
2. Click on the "DELETE" button.
3. Click on the button PROGRAMMING.
   ↳ The programming app launches.
4. Complete all tasks.
   ↳ Component has been deleted from locking plan after successful programming.

3.8 Forced component deletion

If a defective component cannot be reset easily (see *Resetting components [▸ 14]*), it is still possible to delete it from the locking plan. A repeated deletion of the component leads to a forced deletion of the component.

✓ Component already deleted.

✓ Component programmed previously.

1. Click on the component again.
2. Click on "FORCE DELETE" and confirm the input.

IMPORTANT

Forced deletion disables a (still) programmed component, so it can no longer be used. You should only use this procedure on defective components!

3.9 Read access event log

All access events with a key are logged in the locking device. MobileKey locks log up to 500 accesses. If further accesses take place afterwards, the oldest accesses are overwritten. Proceed as follows to display the access protocol:

✓ Matrix screen open

1. Click on the required ready programmed lock to read its log.
   ↳ Menu opens.
2. Click on the button AUDIT TRAIL.
3. Change the time period for the access event log.
4. Click on the button READ AUDIT TRAIL.
   ↳ The "Read access log" command is sent to the programming app as a task.
5. Click on the menu button.
   ↳ Menu opens.
6. Click on the button PROGRAMMING.
   ↳ The programming app launches.
7. Execute the programming task.
8. Close the programming app.
9. Open the matrix.
10. Click on the required lock to read its log.
    ↳ Menu opens.
11. Click on the button AUDIT TRAIL.

↳ Access event log is displayed.

4 MobileKey ONLINE extension

Locking devices can be networked via a SmartBridge, which acts as an access point, to communicate directly with the web app. This provides a few new functions, such as the following:

- Locking devices can be programmed independently of the platform.
- Door statuses (open, closed, locked) can be tracked in real time.
- Locking device access lists can, in principle, be read from anywhere in the world.
- Keys can be shared with friends using Key4Friends.
- The web app can be used to open doors remotely.

Special components are required to use these functions:

- SmartBridge: as an access point, SmartBridge is permanently connected to the Internet.
- Online-capable locking device: All MobileKey locking devices can be equipped with a special network node *(SmartRelay* with suitable circuit board) to retrofit online functions. This where we refer to what are known as LockNodes. Locking devices with a "DoorMonitoring configuration" also feature soPHIsticated sensor technology. These locking devices can determine door statuses (open, closed, locked) and inform the web app.

4.1 SmartBridges

At least one SmartBridge must be operated as an access point. This connected to the Internet and thus guarantees connection to the server and web app.

IMPORTANT

Extended network settings *(e.g. when a locking device is added)* are not shown until at least one SmartBridge has been added.

IMPORTANT

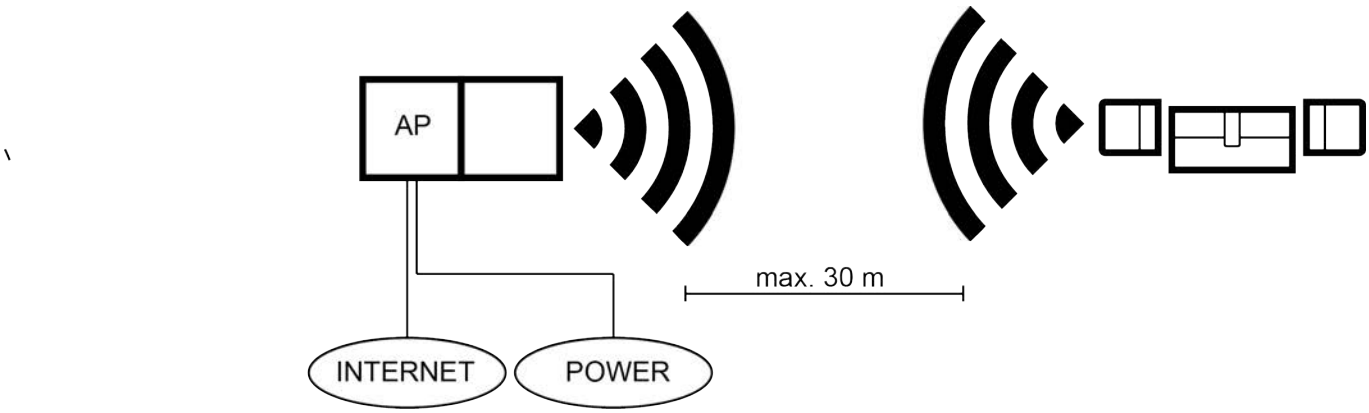
Note that a maximum of 10 SmartBridges can be used with MobileKey.

4.1.1 Setting up SmartBridges

SmartBridges can be operated in different ways depending on their use and configuration. The key scenarios are shown below.

4.1.1.1 A SmartBridge

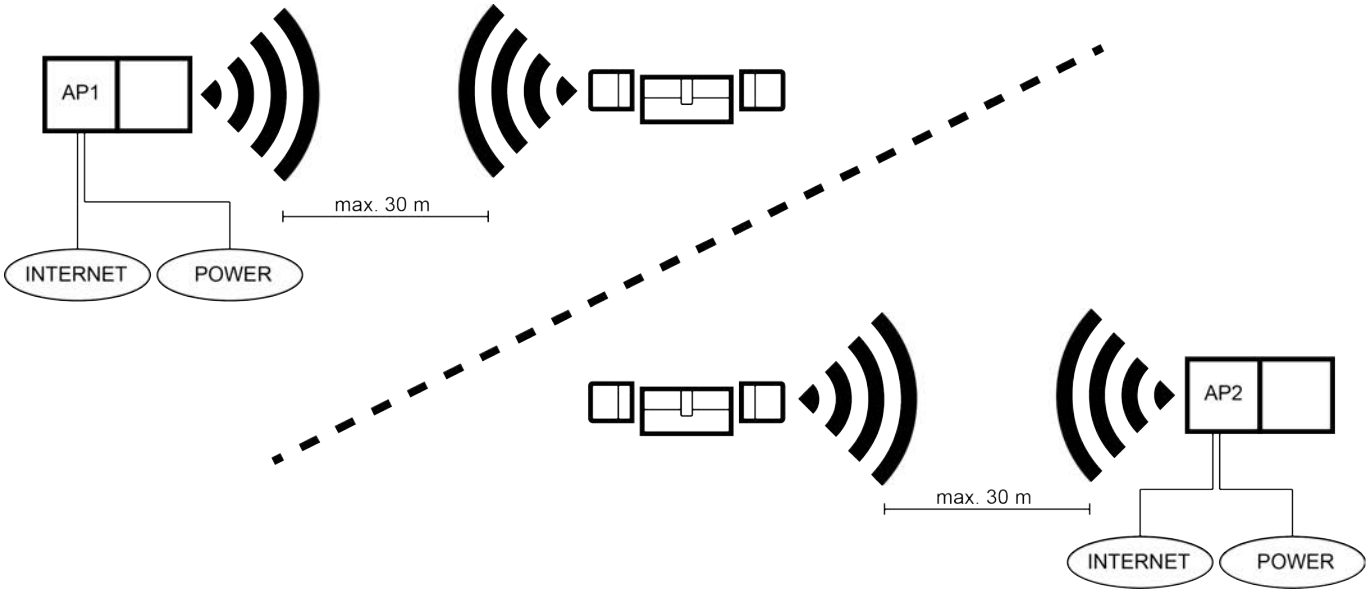
The simplest use for MobileKey ONLINE is as a SmartBridge configured as an access point.



4.1.1.2 Two or more SmartBridges

MobileKey ONLINE can manage a number of access points. This allows several locations or very distant locking devices to be covered with the MobileKey ONLINE network.

MobileKey ONLINE automatically determines which particular locking device is addressed by which particular access point based on the signal strength. You can trace the communication path in the "NETWORK" menu by activating the "Show Uplink" option.



4.1.2 Setting up SmartBridges

This how you add a new SmartBridge to the web app:

1. Click on the menu button.
   ↳ Menu opens.
2. Click on the "NETWORK" button.

3. Add a new SmartBridge using the Plus symbol on SmartBridges.
   ↳ Dialogue to add a new SmartBridge is launched
4. Select a type.
   ↳ Select "STANDARD" to configure a SmartBridge as an access point.
5. Assign a name.
   ↳ Assign a unique name, such as "SmartBridge Office 2"
6. Enter the MobileKey ID.
   ↳ You will find the MobileKey ID on the packaging or the rear of SmartBridge.
7. Click on the "SAVE" button.
   ↳ Configuration is saved. You return automatically to the "NETWORK" menu.

4.1.3 Deleting SmartBridge

IMPORTANT

The LockNodes in locking devices can only be reset via the connected SmartBridge. If locking devices are not flagged for deletion, they will retain their configuration. However, the locking devices can now only be accessed via a new SmartBridge or the programming device.

This is how you delete your SmartBridge in the web app:

✓ Connected locks indicate "ONLINE" status

1. Click on the menu button.
   ↳ Menu opens.
2. Click on the "NETWORK" button.
3. Click on the SmartBridge to be deleted.
4. Click on the "DELETE" button.
   ↳ The SmartBridge is flagged for deletion.
5. Use the "START CONFIGURATION" button to launch the network configuration.
6. The programming process is implemented (in this case: the SmartBridge is reset). The SmartBridge can then be re-incorporated into the MobileKey locking system.

4.2 Setting up a locking device with network node (LockNode)

IMPORTANT

Locking devices which have already been installed and programmed without an online function can also be integrated into MobileKey ONLINE retroactively. To do so, you merely need to replace the thumb-turn cover

(inside thumb-turn cover on FD locking devices, outer thumb-turn cover on CO locking devices or added circuit board in SmartRelay) with an online thumb-turn cover containing a LockNode. The new chipID for the LockNode can then be added to the locking device in the web app.

This how you add a new online locking device:

✓ SmartBridge added *(see Setting up SmartBridges [▸ 17])*

✓ Matrix screen open

1. Click on the Add lock icon (plus beneath the "SAVE" button).
2. Select the lock type, e.g. "CYLINDER" for a normal locking cylinder.
3. Assign a name, e.g. front door.

CAUTION

Security risk with permanent opening

A door which is permanently open may pose a security risk. SimonsVoss Technologies GmbH therefore recommends limiting the opening time interval.

4. Click on the "Opening duration in seconds" or "Permantently open" button.
   ↳ If you have activated "Permantently open", the lock will remain engaged ready for use until it is actuated again with a key or by remote opening.
5. Enter the chip ID (printed on the packaging and on the inside of the thumb-turn cover).

IMPORTANT

Low battery life

The locking device checks whether an action needs to be performed more often when fast wake-up is activated. This reduces the response time, but it also shortens the battery life by up to 30%.

6. Activate fast wake-up as an option.
7. Click on the "SAVE" or "SAVE + COPY" button.
   ↳ "SAVE" saves the lock and takes you back to the matrix screen.
   ↳ "SAVE + COPY" saves the lock and prepares another lock with the same properties.

↳ Lock with online function (LockNode) created.

4.3 Delete locking devices with network node (LockNode)

This is how you delete an existing online locking device via the SmartBridge:

✓ SmartBridge added *(see Setting up SmartBridges [▸ 17])*
✓ Network set up and functioning
✓ The online status of the lock that you wish to delete "ONLINE"

1. Click on the menu button.
   ↳ Menu opens.
2. Click on the "NETWORK" button.
3. Click on the lock you wish to delete in the "NETWORK" menu.
4. Click on the "DELETE" button.
   ↳ The locking device is flagged for deletion.
5. Use the "START CONFIGURATION" button to launch the network configuration.
   ↳ Programming process is implemented *(in this case: reset)*.
   ↳ The lock can then be re-incorporated into the MobileKey locking system.

↳ Lock is deleted.

4.4 Create Online PIN Code Keypad

✓ Online PIN Code Keypad already configured (see Configuration).
✓ Lock for Online PIN Code Keypad already added (see *Setting up a locking device with network node (LockNode) [▸ 18]*).
✓ Matrix screen open

1. Click on the Add lock icon (plus sign next to the "SAVE" button).
2. Select [PIN CODE KEYPAD] type.
3. Enable the ◉ ONLINE VERSION option.
4. Enter the chip ID.
5. Open the ▼ **Lock** drop-down menu.
6. Identify the lock which will be used to operate the Online PIN Code Keypad.
7. Enter a name for a PIN – e.g. "Mark Smith".
8. Enter a user PIN.
9. Enter other PINs in the same way.

IMPORTANT

If you wish to add other user PINs, you first need to enable the corresponding checkbox.

IMPORTANT

Up to three user PINs can be set up in the MobileKey web app and assigned to a lock.

10. Click on the SAVE or SAVE + COPY button.
    - ↳ SAVE saves the Online PIN Code Keypad and brings you back to the matrix screen.
    - ↳ SAVE + COPY saves the Online PIN Code Keypad and prepares a new Online PIN Code Keypad with the same characteristics.

↳ Online PIN Code Keypad is added.

IMPORTANT

If you subsequently wish to edit the user PINs, click on the entry in the matrix and select the EDIT button from the menu.

ATTENTION

Blocking after incorrect inputs

If a user PIN is entered incorrectly seven times, the SmartBridge continues to reset reception, but the system blocks processing of entered user PINs for three minutes. A relevant notification is displayed in the messages on the web app.

Also see

- *Creating a lock [▸ 9]*

4.5 Delete Online PIN Code Keypad

✓ SmartBridge added (see *Setting up SmartBridges [▸ 17]*).

✓ Network set up and functioning (see *Configure online components [▸ 22]*).

✓ Online status of the "ONLINE" Online PIN Code Keypad to be deleted.

1. Click on the menu button.
   - ↳ Menu opens.
2. Click on the "NETWORK" button.
3. Click on the Online PIN Code Keypad you wish to delete in the "NETWORK" menu.
4. Click on the "DELETE" button.
   - ↳ The Online PIN Code Keypad is flagged for deletion.

5. Use the START CONFIGURATION button to launch the network configuration.
   ↳ Programming process is implemented *(in this case: reset)*.
   ↳ The Online PIN Code Keypad can be incorporated into any MobileKey locking system after it has been reset to storage mode (see Set to storage mode).

↳ Online PIN Code Keypad is deleted.

4.6 Configure online components

✓ At least one added SmartBridge
✓ SmartBridge connected to Internet and ready for operation
✓ At least one lock with online chip ID added
✓ The distance between SmartBridge and locking devices is less than 30 m. *All components should be within the SmartBridge radio range at all times.*

1. Click on the menu button.
   ↳ Menu opens.
2. Click on the "NETWORK" button.
3. Click on the "START CONFIGURATION" button.
   ↳ The MobileKey network is configured fully automatically.

↳ The status of SmartBridges and locking devices must be set to "ONLINE" when configuration is complete.

Go through the following check list if the automatic configuration was not successful: *Help for online locking devices [▸ 35]*.

4.7 Programming components

Online locking devices or Online PIN Code Keypads can also be programmed using the SmartBridge. Keys or transponders must be programmed using the USB config device since they do not have a network node (LockNode).

IMPORTANT

Programme each lock or Online PIN Code Keypad before installing it.

IMPORTANT

The access list stored in the locking device is reprogrammed every time that the device is reprogrammed. Only accesses already imported into the web app are conserved.

This how you complete programming using the SmartBridge:

✓ Indicate the lock's or the Online PIN Code Keypad's chip ID when you add it.
✓ Network successfully configured
✓ Matrix screen open

1. Add a component.
2. Issue authorisations if necessary.
3. Click on "SAVE".
   ↳ Programming process will start automatically via the SmartBridge.
   ↳ Maintenance symbol is displayed in matrix during the programming process.

3 brief audible signals will indicate that locking device programming is complete. *(beep, beep, beep)*

4.8 Disconnecting connection to online components

Online components can be removed from the system again if required. Warning messages are activated if components are physically removed – when they are taken outside the MobileKey radio range, for example. You should therefore always de-register the components concerned in the system. The de-registration process resets the LockNode. The lock or the Online PIN Code Keypad retains its configuration and can then only be accessed using the USB config device until it is set up online again.

✓ At least one online lock or one Online PIN Code Keypad added.
✓ At least one SmartBridge added.

1. Click on the menu button.
   ↳ Menu opens.
2. Click on the "NETWORK" button.
3. Click on the lock or the Online PIN Code Keypad to be disconnected.
   ↳ Menu opens.
4. Click on the "DISCONNECT" button in the menu.
5. Use the "START CONFIGURATION" button to launch the online configuration.

Also see

➡ *Help for online locking devices [▸ 35]*

4.9 Carrying out remote opening

- ✓ Locking system configured correctly
- ✓ Access point connected to Internet
- ✓ Lock has LockNode
- ✓ Lock configured correctly
- ✓ Matrix screen open

1. Click on the locking device you wish to open remotely.
2. Click on "OPEN LOCK".
   - ↳ The command is sent directly to the locking device via the SmartBridge. A door can also be locked in the same way, as you would expect.

↳ Lock is opened/closed.

4.10 Key4Friends

Key4Friends allows users to share keys using smartphones. Keys can be shared with friends very easily using Key4Friends.

Your friend receives an email informing them that you wish to share a key with them. The email describes exactly how this shared key can be used with the help of the Key4Friends app.

Your friend installs the Key4Friends app and uses their email address and telephone number to register quickly and easily. This unique combination is the only way to ensure that your key can only be used by your friend's telephone.

4.10.1 Sharing keys

- ✓ Locking system configured correctly
- ✓ Access point connected to Internet and online
- ✓ Matrix screen open

1. Click on the lock whose key you wish to share.
   - ↳ Menu opens.
2. Click on the "NEW KEY4FRIENDS" button.
3. Fill out the values as you wish.
4. Complete the recipient's details.
5. Restrict the key validity.
6. Click on the "SEND" button.

↳ Your friend will then receive an email. The email describes exactly how they can use the key.

All settings and details for shared keys can be changed or revoked at any time; see Managing keys [▸ 25].

IMPORTANT

The time window for shared keys is limited to six months.

- If you want to give friends permanent access, use transponders or a PIN code keypad.

4.10.2 Managing keys

1. Click on the menu button.
   ↳ Menu opens.
2. Click on the "MANAGE KEY4FRIENDS" button.
   ↳ You will find all the keys currently shared under "Active" type.
   ↳ You will also find all the keys not currently shared under "All" type.

You can click on each shared key to edit or revoke it.

4.11 DoorMonitoring locking device - displayed locking statuses

Locking devices with a DoorMonitoring option use a special fastening screw to communicate door statuses. These locking devices are ready designed for use with MobileKey ONLINE as they already feature what is known as a LockNode.

The following door statuses for the DoorMonitoring locking device are displayed using a corresponding icon in the web application matrix with combined statuses shown at times:

SYMBOL	DESCRIPTION
	Door open.
	Door closed but not locked.
	Door securely closed and locking device locked.
	Door open too long. *The time can be configured in the locking device settings after the DM locking device has been programmed for the first time.*
	Door closed. Locking status not monitored.

Other warnings may be shown for a DoorMonitoring locking device *(see The matrix [▸ 7])* in addition to standard warnings:

SYMBOL	DESCRIPTION
	**Break-in** A break-in attempt has been reported at the door. Someone may have tried to force the door open.
	**Manipulation of magnet** Someone has tampered with the door or the magnetic plate.

	Manipulation of screw Someone has tampered with the door or the fastening screw.
	Hardware error Problems may arise with sensors in rare cases. Contact your specialist retailer or SimonsVoss Technologies GmbH directly (see Help & Contact) to receive further help. Your hardware probably needs to be replaced.

IMPORTANT

If there has been a break-in or deliberate manipulation of the DoorMonitoring locking device, the corresponding door must be checked immediately. Look for any damage to the door or locking device. The locking device must then be reset. *See Programming components [▸ 22]*

CAUTION

Dead bolt not monitored

If flip-flop mode is set, then the dead bolt's status is not monitored.

- Do not use flip-flop mode if you also want to monitor the dead bolt.

IMPORTANT

The access list stored in the locking device is reprogrammed every time that the device is reprogrammed. Only accesses already imported into the web app are conserved.

IMPORTANT

Please note that your MobileKey network must be configured correctly. The SmartBridge and DoorMonitoring lock must both always be "ONLINE". *See Help for online locking devices [▸ 35] for further help.*

Also see

- *Help for online locking devices [▸ 35]*
- *Programming components [▸ 22]*

5 Event management

Targeted notifications can be generated, triggered by individual rules (events). These notifications can be forwarded to different email addresses and also sent directly to smartphones in push notifications. All notifications are also displayed under "EVENT FEED" in the MobileKey web app.

5.1 Viewing notifications on the web app

The "EVENT FEED" menu in the matrix (use the icon to open menu) displays all notifications triggered by event management plus all important information, warnings and alarms.

The messages symbol on the main matrix screen keeps you informed of the latest events at all times. All events can be filtered or reset.

5.2 Creating rules

Individual events can be generated in the locking system settings.

1. Click on the menu button.
   ↳ Menu opens.
2. Click on the "SETTINGS" button.
3. Click on the Plus button under "EVENT-MANAGEMENT".

↳ Wizard to create new rules launches.

5.2.1 Creating an "Access"-type rule

ACCESS TYPE

TRIGGER	DESCRIPTION
Remote opening	A notification is sent for all remote opening events.
Key4Friends	A notification is forwarded for one opening event or all opening events actuated with Key4Friends.
Transponders/PINs	A notification is sent for one or all opening events actuated with a key (transponder) or PIN code.

Click on the "NEXT" button after each step. You can use the "SAVE" button to activate the event once all settings have been adjusted.

1. Select the "ACCESS" event type.
2. Specify the keys which are to trigger the event.
   ↳ Deactivate the slider to restrict the selection of keys and Key4Friends on an individual basis.
3. Specify the locking devices where the event is to be triggered.
   ↳ Deactivate the slider to restrict the selection of locking devices on an individual basis.

4. Specify a time period when events are to be triggered.
   ↳ All time periods are selected by default, so that events can be triggered at any time. You can restrict the selection as you wish.
5. Assign a suitable name to the event.
6. Indicate how you wish to be notified of events.
7. Click on the "SAVE" button.

↳ Event is activated.

5.2.2 Creating a "DoorMonitoring"-type rule

DOOR MONITORING TYPE

TRIGGER	DESCRIPTION
Door open	A notification is sent as soon as the door is physically opened.
Door closed	A notification is sent as soon as the door is physically closed.
Door open too long	A notification is sent as soon as the door is physically open for too long.
Door closed after being open too long	A notification is sent as soon as the door is closed again after being physically open for too long.
Door unlocked	A notification is sent as soon as the door is unlocked.
Door locked	A notification is sent as soon as the door is properly locked.

Click on the "NEXT" button after each step. You can use the "SAVE" button to activate the event once all settings have been adjusted.

1. Select the "DOOR MONITORING" event type.
2. Specify the events which are to trigger the event.
3. Specify the DoorMonitoring locking devices where the event is to be triggered.
   ↳ Deactivate the slider to restrict the selection of locking devices on an individual basis.
4. Specify a time period when events are to be triggered.
   ↳ All time periods are selected by default, so that events can be triggered at any time. You can restrict the selection as you wish.
5. Assign a suitable name to the event.
6. Indicate how you wish to be notified of events.
7. Click on the "SAVE" button.

↳ Event is activated.

5.2.3 Creating an "Alarm"-type rule

ALARM TYPE

TRIGGER	DESCRIPTION
Low battery	A notification is sent as soon as the battery level in a locking device is low.
Network error	A notification is sent as soon as a network error occurs.
Break-in	A notification is sent as soon as a DoorMonitoring locking device detects an attempted break-in.
Hardware problem	A notification is sent as soon as a hardware problem is detected.

Click on the "NEXT" button after each step. You can use the "SAVE" button to activate the event once all settings have been adjusted.

1. Select the "ALARM" event type.
2. Specify the alarms which are to trigger the event.
3. Assign a suitable name to the event.
4. Indicate how you wish to be notified of events.
5. Click on the "SAVE" button.

↳ Event is activated.

5.3 Important information

IMPORTANT

All events are transmitted via the SmartBridge. You will not receive any notifications about events if the Internet connection is malfunctioning or the power supply has been interrupted. All events which occur during the time period when the SmartBridge is not properly online.

IMPORTANT

An "ALARM"-type notification is recommended in all cases. This is how you can configure this event: *Creating an "Alarm"-type rule [▸ 29]*

IMPORTANT

Notifications of events are reported in real time only if the locking devices have been networked with SmartBridge. Alarms are also recorded for non-networked locking devices when a programming task is carried out on the locking device concerned. All events and alarms can be displayed, filtered and reset under "EVENT FEED".

Also see

- *Creating an "Alarm"-type rule [▸ 29]*

6 Help

Help for possible day-to-day problems are shown below.

6.1 Help with keys (transponders)

Keys or transponders may get lost, stolen or damaged at some point. Whatever the case, the old key needs to be deleted in the locking plan and a replacement key needs to be created. The deleted key's authorisations must be removed from all locking devices for security reasons. You can do this by reprogramming all locking devices.

Use the following procedure to replace a defective key or one which is "no longer available".

✓ Matrix screen open

1. Search for the key concerned in the locking plan.
2. Cancel all authorisations.
3. Click on the "SAVE" button.
   ↳ Changes have been saved.
4. Click on the key in the locking plan.
   ↳ Menu opens.
5. Click on the "DELETE" button.
   ↳ Key is now flagged for reset.
   ↳ Task will be completed in the programming app at a later stage.
6. Lost, stolen or defective key: Click on the key concerned in the locking plan.
   ↳ Menu opens.
7. Click on the "FORCE DELETE" button.
   ↳ Key is deleted in the locking plan.
   ↳ Key is not yet deactivated in the lock.
8. Create a new key if necessary.
9. Issue required authorisations if necessary.
10. Click on the "SAVE" or "SAVE + COPY" button if necessary.
    ↳ "SAVE" saves the key and takes you back to the matrix screen.
    ↳ "SAVE + COPY" saves the key and prepares another key with the same properties.
11. Click on the menu button.
    ↳ Menu opens.
12. Click on the button PROGRAMMING.
    ↳ The programming app launches.

13. Carry out all tasks.
    ↳ The following programming tasks can be expected: Removing authorisations for the deleted key from all locking devices and authorise a new key for the locking devices if required.

↳ Programming is performed.

CAUTION

Unauthorised access after theft

A stolen key is still authorised for use in the locking system until all authorisations have been removed and the locking devices reprogrammed.

- Re-programme all authorised keys immediately if a key is lost.

6.2 Help with locking devices (e.g. locking cylinders)

Locking devices or locking cylinders may present a defect. Replace the batteries in the locking device first and try to re-programme it. If the locking device still doesn't work correctly, it needs to be replaced.

If a locking device with different properties is required, it can simply be replaced.

Proceed as follows to replace a locking device:

✓ Matrix screen open

1. Remove the locking device concerned from the door.
   ↳ *It may be difficult to remove a locking device from a closed door. If necessary, ask the specialist who installed the SimonsVoss products for advice.*
2. Click on the lock concerned in the locking plan.
   ↳ Menu opens.
3. Click on the "DELETE" button.
   ↳ The lock is flagged for reset.
   ↳ Task will be completed in the programming app at a later stage.
4. If the locking device is defective: Click on the lock.
   ↳ Menu opens.
5. Click on the "FORCE DELETE" button.
   ↳ Lock is permanently deleted in the locking plan.
6. Create a new key.
7. Issue necessary authorisations.
8. Click on the "SAVE" or "SAVE + COPY" button.
   ↳ "SAVE" saves the key and takes you back to the matrix screen.
   ↳ "SAVE + COPY" saves the key and prepares another key with the same properties.

9. Create a new lock.
10. Issue necessary authorisations.
11. Click on the "SAVE" or "SAVE + COPY" button.
    ↳ "SAVE" saves the key and takes you back to the matrix screen.
    ↳ "SAVE + COPY" saves the key and prepares another key with the same properties.
12. Click on the menu button.
    ↳ Menu opens.
13. Click on the button PROGRAMMING.
    ↳ The programming app launches.
14. Carry out all tasks.

↳ Programming is performed.

6.3 Reset or re-use deleted components

If you delete a SimonsVoss component, such as a key or locking device, from the locking system without resetting it correctly beforehand, you can still continue to use it:

✓ Matrix screen open

1. Add the component concerned (e.g. key or transponder) to the locking plan again.
2. Click on the menu button.
    ↳ Menu opens.
3. Click on the button PROGRAMMING.
    ↳ The programming app launches.
4. Complete all tasks.
    ↳ The initial attempt to re-programme is acknowledged with an error message.
5. Carry out the task again.

↳ Component is now reprogrammed.

Always reset the components correctly to prevent this problem.

6.4 Read components

You can read all MobileKey components to see what their purpose is. This might be important if you find a key, such as a transponder, to which you are unable to assign to a user, for example.

MobileKey components can be quickly read:

1. Click on the menu button.
    ↳ Menu opens.
2. Click on the button PROGRAMMING.
    ↳ The programming app launches.

3. Click on the "READ DEVICE" button.

IMPORTANT

Reading in macOS/Android

The programming interface opens directly in the application itself instead of a programming app. There is no "READ DEVICE" button. Click on the wireless icon button.

4. Select the component that you wish to read.

↳ Feedback message shows, for example, the name of the key (John Smith) or whether a non-programme MobileKey component is in storage mode.

6.5 Help for SmartBridge

Go through the following check list if the automatic configuration was not successful due to a problem with SmartBridge:

- Check **power supply**.
  - Is the SmartBridge LED flashing?
- Check **LAN connection**.
- Check **Internet access**.
  - Is the Firewall Port 8883 (TCP/IP) open? If necessary, add suitable exceptions to allow the SmartBridge to communicate to the outside world via Port 8883.
  - Is the DHCP server configured in such a way that a device is able to register on the network?

    You can also optionally use a Windows PC to reach the SmartBridge with the **SimonsVoss OAM Tool**. The OAM Tool allows you make additional settings to SmartBridge, such as assigning a fixed IP address or configuring the integrated DHCP server settings. You will find the OAM Tool under Software downloads in the Support section on the SimonsVoss website (*www.simons-voss.com*).

IMPORTANT

Using fixed IP addresses

A DNS (domain name service) must also be entered in the OAM tool when using a fixed IP address.

- Check that the **chip IDs and MobileKey IDs** have been entered correctly.
- Is the **distance** between the SmartBridge and lock more than 1.5 m and less than about 30 m?

- Test the set-up if there is a clear linear distance of 3 m without any obstacles.
- Environmental influences, walls, objects and many other factors have a considerable effect on signal quality. Network coverage up to about 30 m cannot be guaranteed.

IMPORTANT

Resetting the SmartBridge

You can reset the SmartBridge to factory settings using a hardware reset (see Reset RouterNode).

6.6 Help for Online PIN Code Keypad

Go through the following checklist if you have a problem with the Online PIN Code Keypad.

- Check the **battery status**. Perform a battery test (see Battery test).
- Check that the **chip IDs** have been entered correctly.
- Check that the lock is assigned to the Online PIN Code Keypad correctly (see *Create Online PIN Code Keypad [▸ 20]*).

6.7 Help for online locking devices

Go through the following check list if the automatic configuration was not successful due to **problems with online locking devices**:

- Check that the different locking device **chip IDs** have all been entered correctly.
- Check that the **LockNode** has been **installed correctly**.

  4 short audible signals must be emitted if the contact between the LockNode and locking device has been established correctly.
- Check that locking devices are **correctly** assigned when LockNodes are retrofit or replaced.

6.8 Network error

Check that your Internet connection is stable if several network errors occur within 24 hours.

IMPORTANT

Many standard Internet routers obtain a new IP address at specific intervals, which may lead to a brief interruption in the Internet connection. A error message will be generated *(mainly at night)* if this process is longer than 30 seconds.

6.9 Manual resetting of LockNodes

A programmed online locking device consists of two separately programmed components: the locking device and the LockNode. Both components are matched to one another and cannot be used in another locking system when programmed. Always use the web app to reset the LockNode; see *Disconnecting connection to online components [▸ 23]*.

If this step is not possible, the LockNode configuration can only be reset with the help of a locking device which does not form part of the locking system. Fit the LockNode temporarily to an unknown locking device for this purpose. The system signals that the LockNode is reset after a few seconds:

- Locking cylinder: Audible signal (4 beeps)
- SmartRelay: Optical signalling by LED. (Ensure the power supply is correct)

The LockNode can be connected to any SmartBridge again once it has been reset.

7 Maintenance, cleaning and disinfection

Damage to surfaces

The use of unsuitable or aggressive disinfectants can damage MobileKey components.

MobileKey components MUST NOT come into contact with oil, grease, paint or acids.

Only use disinfectants explicitly suitable for disinfecting delicate metal surfaces and plastic.

CAUTION

Battery replacement

Empty batteries always must be replaced by new ones approved for use by SimonsVoss. Always dispose of old batteries in the proper manner.

8 MobileKey apps

The MobileKey app is available from iOS and Android app stores and supports the following functions:

- Overview of door statuses (if DM cylinder is used).
- Remote opening.
- Sending of Key4Friends authorisations.
- Reading and display of the access list.
- Reception of push messages from event management.
- Use of touch ID for security-related actions (remote opening, Key4Friends, deactivating push messages).
- Programming of keys and locking devices using the USB config device. *Only available with Android devices with OTG function and OTG cable.*

9 Declaration of conformity

You can access documents such as declarations of conformity and other certificates online at www.simons-voss.com.

10 Tips & Tricks

10.1 Link to the web app

A direct link to the MobileKey web app can be established on all devices. The web app can be launched particularly quickly and conveniently on your desktop or home screen, even on smartphones and tablet PCs. Try it out!

10.2 Using keys without the USB config device

All keys (transponders) must be programmed using the USB config device at the moment. This makes things particularly difficult when there is no access to a Windows or Android device. You will find below a way in which you can assign pre-programmed keys with any supported end device without needing to use a USB config device:

- ✓ Locks with online extension
- ✓ Locks with "ONLINE" status
- ✓ Matrix screen open

1. First of all, create a number of keys, such as Key Extra1, Extra2, Extra3 and so on.
   ↳ These keys are not assigned authorisations to begin with.
2. Programme all keys once with the USB config device and make them with a name if required.
   ↳ A key can obviously also be read at a later point in time.
3. Instead of adding a new key and programming it with the USB config device, simply change the properties of a key that you added previously, such as "Extra1".
4. Click on the key previously added, such as "Extra1", and select "EDIT".
5. Change the name.
6. Enter data for "Valid from" and "Valid to" if you wish.
7. Click on the "SAVE" button and return to the matrix.
   ↳ Key is saved.
8. Authorise the key for all required locking devices.
9. Click on the "SAVE" button.
   ↳ Matrix screen is opened.
10. Click on the lock for which the key needs to be authorised.
    ↳ Menu opens.
11. Click on the button
12. Click on the button PROGRAMMING.
    ↳ Programming takes place online via the SmartBridge.
13. Repeat this step until you have programmed all locks.

↳ Keys are authorised on selected locks.

10.3 Setting the language

You can very easily set the language for the web app. The following are available:

- English
- Danish
- German
- French
- Italian
- Dutch
- Swedish

Procedure:

✓ Matrix screen open

1. Click on the menu symbol.
   ↳ Menu on the right launches.
2. Click on the entry with your name.
   ↳ Menu changes.
3. Click on the "MANAGE ACCOUNT" button.
   ↳ Account data. menu is shown.
4. Click on the "LANGUAGES" button.
   ↳ Selection menu for languages is opened.
5. Select the language that you require.

↳ Language is set.

11 Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents under Informative material/Documents in the Download section on the SimonsVoss website (*https://www.simons-voss.com/en/downloads/documents.html*).

Software and drivers

You will find software and drivers in the Download section on the SimonsVoss website (*https://www.simons-voss.com/en/downloads/software-downloads.html*).

Declarations of conformity

You will find declarations of conformity for this product in the Certificate section on the SimonsVoss website (*https://www.simons-voss.com/en/certificates.html*).

Information on disposal

- Do not dispose the device (MobileKey) in the household waste. Dispose of it at a collection point for electronic waste as per European Directive 2012/19/EU.
- Recycle defective or used batteries in line with European Directive 2006/66/EC.
- Observe local regulations on separate disposal of batteries.
- Take the packaging to an environmentally responsible recycling point.

Hotline

If you have any questions, the SimonsVoss Service Hotline will be happy to help you on +49 (0)89 99 228 333 (German fixed network; call charges vary depending on the operator).

Email

You may prefer to send us an email.

support@simons-voss.com

FAQs

You will find information and help for SimonsVoss products in the FAQ section on the SimonsVoss website (*https://faq.simons-voss.com/otrs/public.pl*).

SimonsVoss Technologies GmbH
Feringastrasse 4
85774 Unterföhring
Germany

This is SimonsVoss

SimonsVoss is a technology leader in digital locking systems.

The pioneer in wirelessly controlled, cable-free locking technology delivers system solutions with an extensive product range for SOHOs, SMEs, major companies and public institutions.

SimonsVoss locking systems unite intelligent functions, optimum quality and award-winning German-made design. As an innovative system provider, SimonsVoss attaches great importance to scalable systems, effective security, reliable components, high-performance software and simple operation.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners. With its headquarters in Unterföhring, near Munich, and its production site in Osterfeld, eastern Germany, the company employs around 300 staff in eight countries.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

ALLEGION

SimonsVoss technologies