Manual
MobileKey Web-App

06.2017

ALLEGION

Simons Voss technologies

Manual
MobileKey Web-App

Contents

Manual
MobileKey Web-App

Manual
MobileKey Web-App

Manual
MobileKey Web-App

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.

NOTICE

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.

NOTICE

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

NOTICE

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

NOTICE

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

NOTICE

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

Manual
MobileKey Web-App

- 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 MobileKey.

    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 programming app to programme the MobileKey locking components.

- **Optional: Online via SmartBridge**

  Locking devices can also be programmed online with a USB config device. See Programming components [▶ 19]. *In this particular case, only the transponders need to be programmed with the aid of the USB config device.*

Manual
MobileKey Web-App

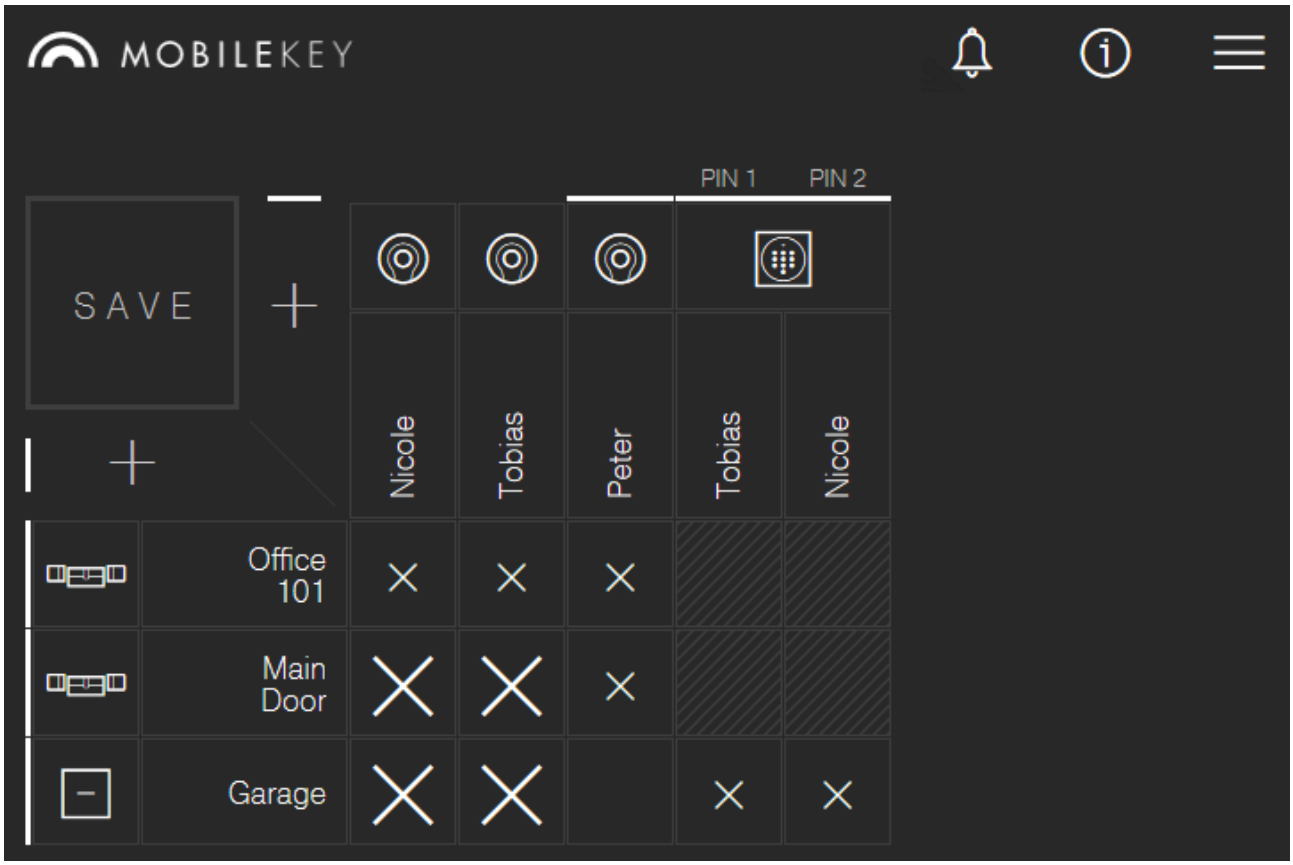
Tip:

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 locking devices at a later stage. See Using keys without the USB config device [▶ 34] for more information.

Manual
MobileKey Web-App

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.

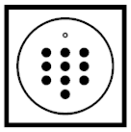
Authorisations

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

Manual
MobileKey Web-App

	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 about this

- Help for online locking devices [▶ 28]
- Help for SmartBridge [▶ 28]

Manual
MobileKey Web-App

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

1. Click on Add lock icon (PLUS symbol beneath the "SAVE" button).
2. Select locking device type, such as "Cylinder" for a normal locking cylinder.
3. Assign a name, such as front door.
4. Select mode.
   - ⇨ Click on "Opening interval in seconds" and specify the length of time that the locking device should remain engaged ready for use. (RECOMMENDED SETTING)
   - ⇨ Click on "Permanent opening" to activate the "Flip-flop mode". The locking device remains engaged ready for use until it is activated with the key again.
5. Save new locking device.
   - ⇨ "Save" saves the locking device and takes you back to the matrix screen.
   - ⇨ "Save + Copy" saves the locking device and prepares another locking device with the same properties.

NOTICE

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 open too long", are visible once the DM locking devices have been programmed for the first time.

NOTICE

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 "Configure relay contact/invert output" setting will then be visible in the SmartRelay properties. If you activate this option, the SmartRelay needs to be reprogrammed.

3.2 Add key

1. Click on Add-key icon (PLUS symbol on the right, next to the "SAVE" button).
2. Select key type, e.g. "Transponder"
3. Assign a name, e.g. "John Smith".
4. Optional: Indicate validity period.

⇨ "Valid from": Specify a date from when the key is to be authorised in the locking system.

⇨ "Valid until": Specify a date until when the key is to be authorised in the locking system.

5. Save new key.

⇨ "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.

3.3 Add PIN code keypad

✓ The PIN code keypad is already configured; see Configuration [▶ 66] *(Master PIN and at least one user PIN must be configured!)*

✓ First add the locking device on which the PIN code keypad is to be operated.

1. Click on Add-key icon (PLUS symbol on the right, 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. Save new key.

⇨ "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.

NOTICE

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.

NOTICE

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.

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

NOTICE 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 schedule: 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 program: 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:

1. Click on required key on the matrix screen.
2. Click on "Time plan".
3. Select type of time plan.
   ⇨ Weekly schedule: Select day and "Add time interval". Several time intervals can be selected on different days.
   ⇨ Daily program: Click on "Exclude weekend" if the schedule is to apply from Monday to Friday only. Then "Add time interval". Several time intervals can be added.
4. "Save" saves the key and takes you back to the matrix screen.

NOTICE 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

NOTICE It is strongly recommended that you programme each locking device before installation.

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

✓ There are programming tasks pending. These are displayed on the corresponding components in the matrix.

1. Select *Menu/Programme to launch* to launch programming app and carry out all pending tasks.
2. Optional: Log on to the programming app.
3. The task list will show you which components need programming. Click on the first component to start programming it. 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 [▶ 6]

3.6.2 IMPORTANT: Programming on an Android device

Download the free MobileKey programming 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 [▶ 6]

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.
2. Select the "Delete" option.
3. Select *Menü/Programme* to launch programming app and complete all tasks.

⇨ The component is also deleted in the locking plan once programming is completed successfully.

3.8 Forced component deletion

If a defective component cannot be reset without any difficulty (see Resetting components [▶ 13]), it is possible to delete it from the locking plan. A repeated deletion of the component leads to a forced deletion of the component.

✓ The component has already been deleted.

✓ The component has been programmed before.

1. Click on the component again.
2. Click on "Force deletion" and confirm.

NOTICE

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. Proceed as follows to display the access protocol:

1. Click on the ready-programmed locking device that you require in the matrix view.
2. Select "Access log".
3. Change the access log time period if necessary.
4. Click on "Read log".
   ⇨ The "Read access log" command is sent to the programming app as a task.
5. Select *Menu/Programme* to launch programming app and complete the task.
6. Close programming app.
7. Select "Display log".

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.

NOTICE

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

NOTICE

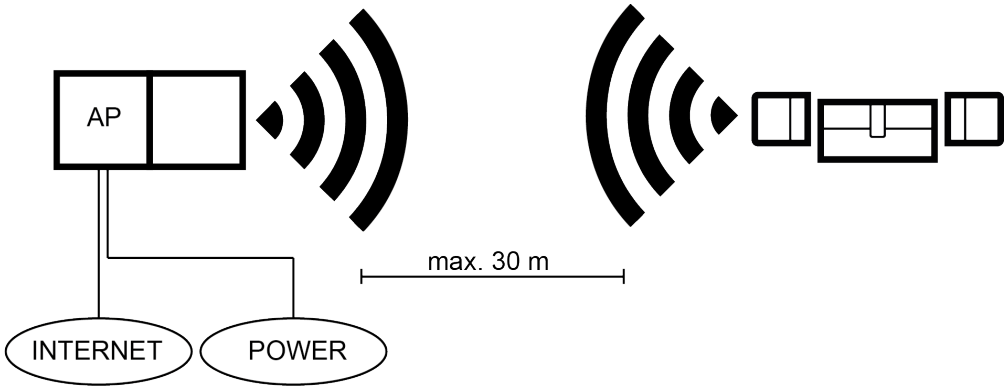
Note that a maximum of 10 SmartBridges can be used with MobileKey.

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

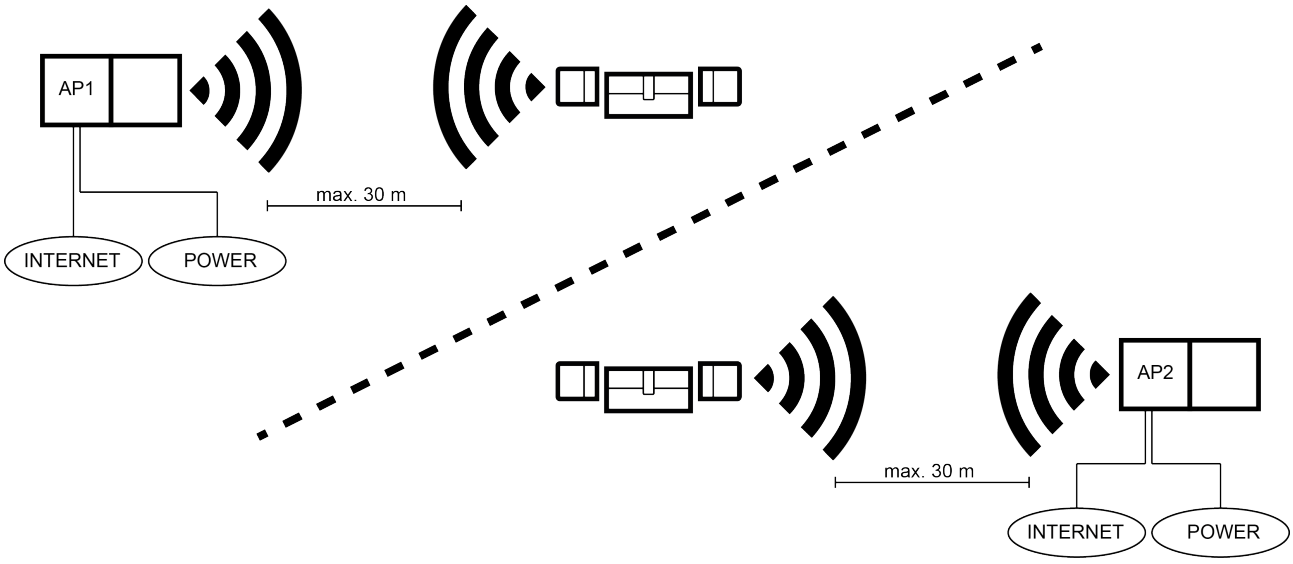
The simplest use for MobileKey ONLINE is as a SmartBridge configured as an access point.



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 option "Show assigned SmartBridge".



4.1.2 Setting up SmartBridges

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

1. Select "Menu / Network".
2. Add a new SmartBridge using the Plus symbol on SmartBridges.
   ⇨ A dialogue is launched to add a new SmartBridge.
3. Select type.

⇨ Select "STANDARD" to configure a SmartBridge as an access point.

4. Issue name.
   ⇨ Assign a unique name, such as "SmartBridge Office 2"
5. Enter MobileKey ID.
   ⇨ You will find the MobileKey ID on the packaging or the rear of SmartBridge.
6. Save.
   ⇨ Save your configuration. You return automatically to the "Network" menu.

4.1.3 Deleting SmartBridge

NOTICE

The LockNodes in locking devices can only be reset via the connected SmartBridge. If you delete the SmartBridge, all connected LockNodes are automatically reset. 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:

✓ Ensure that all connected locking devices display the status "ONLINE".

1. Select "Menu / Network".
2. Click on the SmartBridge to be deleted.
3. Select "DELETE".
   ⇨ The SmartBridge is flagged for deletion.
4. Press the "Launch configuration" button to start network configuration.
5. The programming process is performed (in this case: SmartBridge and all connected LockNodes reset). SmartBridge and LockNodes can then be re-incorporated into the MobileKey locking system.

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

NOTICE

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:

✓ A SmartBridge has already been added. *(See* Setting up SmartBridges [▸ 16]*)*

1. Click on Add lock icon (PLUS symbol beneath the "SAVE" button).
2. Select locking device type, such as "Cylinder" for a normal locking cylinder.
3. Assign a name, such as front door.
4. Select mode.
   ⇨ Click on "Opening interval in seconds" and specify the length of time that the locking device should remain engaged ready for use. (RECOMMENDED SETTING)
   ⇨ Click on "Permanent opening" to activate the "Flip-flop mode". The locking device remains engaged ready for use until it is activated with the key again.
5. Activate online extension.
   ⇨ Enter chipID. The chipID is printed on the packaging and on the internal of the thumb-turn cover.
6. Save new locking device.
   ⇨ "Save" saves the locking device and takes you back to the matrix screen.
   ⇨ "Save + Copy" saves the locking device and prepares another locking device with the same properties.

4.3 Delete locking devices with network node (LockNode)

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

✓ A SmartBridge has already been added. *(See* Setting up SmartBridges [▶ 16]*)*
✓ The network is set up and fully functional.
✓ The online status of the locking device that you wish to delete is "ONLINE".

1. Click on the locking device you wish to delete in the "Network" menu.
2. Select "DELETE".
   ⇨ The locking device is flagged for deletion.
3. Press the "Launch configuration" button to start network configuration.
   ⇨ The programming process is implemented *(in this case: reset)*. The locking device can then be re-incorporated into the MobileKey locking system.

4.4 Configure online components

✓ At least one SmartBridge has been added.
✓ The SmartBridge is connected to the Internet and ready for operation.
✓ At least one online locking device has been added with a chipID.

✓ The distance between SmartBridge and locking devices is less than about 30 cm. All components should be within the SmartBridge radio range at all times.

✓ At least one online locking device has been added.

1. Select "Menu / Network".
2. 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 [▶ 28]

4.5 Programming components

Online locking devices 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).

NOTICE It is strongly recommended that you programme each locking device before installation.

NOTICE 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:

✓ The locking device's chip ID was indicated when the locking device was added.

✓ The network has been successfully configured.

1. Click on the locking device you wish to programme.
2. Click on "Save".
   ⇨ The programming process will start automatically via the SmartBridge. A maintenance symbol is displayed in the matrix during the programming process.

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

4.6 Disconnecting connection to online components

Online components can be removed from the system again if required. If components are physically removed, by taking them out of the MobileKey radio range, for example, warning messages are activated. You should therefore always de-register the components concerned in the system. The

de-registration process resets the LockNode. The locking device 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 locking device or SmartBridge has been added.

1. Select "Menu / Network".
2. Simply click on a locking device to select.
3. Click on the "Disconnect connection" button in the menu.
4. Press the "Launch configuration" button to start online configuration.

Also see about this

Help for online locking devices [▶ 28]

4.7 Carrying out remote opening

✓ Your locking system is configured correctly.

✓ The access point is connected to the Internet.

✓ The locking device features a LockNode and has been configured correctly in the network.

1. Click on the locking device you wish to operate remotely.
2. Click on "Remote opening".
   ⇨ 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.

4.8 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.

4.8.1 Sharing keys

✓ Your locking system is configured correctly.

✓ The access point is connected to the Internet and thus online.

1. Click on the required locking device to select.
2. Select "Menu/Send Key4Friend".
3. Fill out the information as you wish.

4. Complete the recipient's details.
5. Restrict the key validity.
6. Send the key to your friend.
   ⇨ 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 [▶ 21]

NOTICE

Note that the time frame for shared keys is limited to 3 weeks. *Use transponders or a PIN code keypad to give friends access on a permanent basis.*

4.8.2 Managing keys

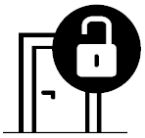
Select "Manage Key4Friends" in the main menu. You will find all the keys currently shared under "Active" type. Change the type to "All" to display all keys not currently shared.

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

4.9 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.

Manual
MobileKey Web-App

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.

Other warnings may be shown for a DoorMonitoring locking device *(see* The matrix [▶ 8]*)* 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 tempered 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 [▶ 33]) to receive further help. Your hardware probably needs to be replaced.

NOTICE

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 reprogrammed, so that it is reset and any future break-ins or manipulation can be recorded in access event logging.*See* Programming components [▶ 19]

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.

NOTICE

Please note that your MobileKey network must be configured correctly. The SmartBridge and DoorMonitoring locking device must both always be "ONLINE". *See* Help for online locking devices [▶ 28]*for further help.*

Manual
MobileKey Web-App

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 "Messages" in the MobileKey web application.

5.1 Viewing notifications on the web app

You display all notifications triggered by Event Management plus important information and warnings by selecting the "Messages" menu in the matrix

(can be accessed using the  symbol).

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. Select "Menu/Settings" to enter the "Settings" menu. Then click on the Plus symbol under "Event Management".

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 event type "Access".
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.

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 event type "DoorMonitoring".
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.

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 event type "Alarm".
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.

5.3 Important information

NOTICE

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.

NOTICE

An "Alarm"-type notification is recommended in all cases. This is how you can configure this event: Creating an "Alarm"-type rule [▶ 24]

NOTICE

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 "Messages".

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".

1. Look for the key concerned in the locking plan and cancel all authorisations for the locking devices. Save changes.
2. Click on key in the locking plan and select the "Delete" option.
   ⇨ The key is now flagged for resetting. This task is completed in the programming app at a later stage.
3. Lost, stolen or defective key: Click on key in the locking plan and select the option "Force deletion".
   ⇨ The key has now been deleted; however, it is not yet deactivated for the locking device.
4. Optional: Add new keys, create authorisations and save.
5. Select *Menü/Programme* to launch programming app and complete 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.

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

NOTICE Important: re-programme all authorised keys immediately if the key is lost for security reasons.

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 reprogramme 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:

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 locking device concerned in the locking plan and select the "Delete" option.
   ⇨ The locking device is flagged for reset. This task is completed in the programming app at a later stage.
3. If the locking device is defective: Click on the locking device and select "Force deletion".
   ⇨ The locking device is permanently deleted in the locking plan.
4. Add new locking device, create authorisations and save.
5. Select *Menü/Programme* to launch programming app and complete all tasks.

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:

1. Add the corresponding component (e.g. key or transponder) to the locking plan again.
2. Select *Menü/Programme* to launch programming app and complete all tasks.
   ⇨ The initial attempt to re-programme is acknowledged with an error message.
3. Carry out the task again.
   ⇨ The 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. Select *Menu/Programme* to launch programming app.
2. Click on "Read" button.
3. Select the component that you wish to read.

A feedback message shows, for example, the name of the key (John Smith) or whether a MobileKey component is in non-programmed 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?
- Is the **distance** between the SmartBridge and locking device 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.
- Check **Internet access**.
  - Is the Firewall Port 8883 open? If necessary, add suitable exceptions to allow the SmartBridge to communicate to the outside world via Ports 1883 and 8883.
  - Is the DHCP server configured in such a way that a device is able to register on the network?

    You can also optionally access SmartBridge on a Windows PC using the **SimonsVoss OAM Tool** *(www.simons-voss.com / Infocenter / Downloads / WaveNet Manager | 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.
- Check that the **chip IDs and MobileKey IDs** have been entered correctly.

6.6 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.

6.7 Network error

Network errors do not necessarily always mean a serious problem. Check that your Internet connection is stable if several network errors occur within 24 hours.

NOTICE

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.

6.8 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 [▶ 19]

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:

1. Locking cylinder: Audible signal (4 beeps).
2. 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

NOTICE

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

NOTICE

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

Clean the MobileKey components with a soft, moist cloth if necessary.

Only use disinfectants explicitly suitable for the disinfection of sensitive metal surfaces and plastic.

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

Manual
MobileKey Web-App

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.

Manual
MobileKey Web-App

10 Help & Contact

Instruction manuals

You will find detailed information on MobileKey components online at www.my-mobilekey.com

Hotline

The SimonsVoss service hotline is available to help you on +49 (0) 89 99 228 333

Email

You may prefer to send us an email.

hotline@simons-voss.com

FAQs

You will find information and help for MobileKey in the public FAQs section.

SimonsVoss Technologies GmbH
Feringastrasse 4
85774 UnterföhringGermany
Germany

Manual
MobileKey Web-App

11 Tips & Tricks

11.1 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!

11.2 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:

✓ You need to be using the ONLINE extension and all locking devices need to be networked online.

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. Indicate a validity period for the key if you wish.
7. Click on the "Save" button and return to the matrix.
8. Authorise the key for all required locking devices.
9. Programme all locking devices for which the key needs to be authorised. (Click on locking device and select "Programming").
   ⇨ Programming takes place online via the SmartBridge.

Manual
MobileKey Web-App

12 Attachment: manuals for the individual components

The following product manuals are designed for use with the LSM Software to a certain extent. The MobileKey web app is used to manage and programme in MobileKey. The MobileKey web app offers simple handling with special functions supported, such as access event logging, time schedules and DoorMonitoring functions.

12.1 Locking cylinder manual

12.1.1 Intended use

SimonsVoss digital MobileKey-Locking Cylinder are installed in designated door locks (such as DIN mortise locks) to integrate them into a digital locking system. Digital half cylinders can also be operated in the optional SimonsVoss padlocks.

Digital MobileKey-Locking Cylinder may only be used for its intended purpose in a designated door. No other use is permitted.

Digital MobileKey-Locking Cylinder is available in various lengths. The selection of the proper size is of significance. The length of the locking cylinder is printed on the packaging and can be measured at any time. If the cylinder is too short, the handles cannot be fitted. If the cylinder is too long, it may be ripped out of the lock. The cylinder may not protrude more than 3 mm on each side of the door to ensure proper operation.

The product may not be changed in any way, other than in compliance with the changes described in the instructions.

12.1.2 Safety instructions

Warning:

- Access through a door may be blocked due to an incorrectly installed or incorrectly programmed MobileKey-Locking Cylinder. SimonsVoss Technologies GmbH is not liable for consequences of incorrect installation, such as blocked access to injured persons, physical damage or any other losses.
- The batteries used in the digital MobileKey-Locking Cylinder may pose a fire or burn hazard if handled incorrectly. Do **not** recharge, open, heat or burn these batteries. Do not short-circuit batteries.
- When used in combination with panic locks, after installation, you must ensure that all parts of the locking system are fully functional and the mortise lock panic function is guaranteed to work.
- The anti-panic cylinder may only be fitted into locks in which it is expressly approved for use. Please also refer to the lock manufacturer's information/documentation.

Manual
MobileKey Web-App

– If the anti-panic lock is used in non-approved locks, the escape door function may malfunction and no longer be triggered. Contact SimonsVoss Technologies GmbH for more information on use in anti-panic locks.

– Do not activate the anti-panic lock before it is fitted as there is a risk of injury from the cam springing back.

– As per European standard EN 179, Appendix C, all components in the anti-panic cylinder locking mechanism must be checked at intervals no greater than one month to ensure that all parts in the locking mechanism are in satisfactory working order as part of locking device maintenance.

Important:

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

– The SimonsVoss MobileKey-Locking Cylinder may only be used for its intended purpose: opening and locking doors. No other use is permitted.

– Only trained specialists may install the cylinder.

– Do **not** allow the cylinder to come into contact with oil, paint or acids.

– Use the .WP version when installing outdoors.

– The inside MobileKey-Locking Cylinder thumb-turn features a protection rating of IP40. This is why it is important to ensure that the inside thumb-turn does not come into contact with water.

– Both knobs are freely rotating in anti-panic cylinders and can only be engaged using an authorised ID medium.

– When used outdoors, the anti-panic cylinder is no longer guaranteed to function at temperatures under - 20 °C or over + 50 °C.

– A functions test must be performed without fail after installing the anti-panic cylinder or replacing its batteries.

– The WP variant must be installed when an anti-panic cylinder is used outdoors.

– We reserve the right to make modifications or further technical developments.

– This documentation has been compiled in accordance with the best knowledge available to us. However, errors cannot be ruled out. No liability is accepted in such cases.

– Should there be differences in the content of other language versions of this documentation, the German version applies in cases of doubt.

Manual
MobileKey Web-App

– All instructions must be followed precisely during installation. The person installing the system should hand these instructions as well as any maintenance instructions over to the user.

– For security reasons, the locking system password must consist of at least 8 characters. The code length for digital locking cylinders in both *System 3060/3061 and MobileKey* is 2^{168} bit.

Instructions on battery replacement

– Only trained specialists may replace the battery.

– Damage may be caused to the MobileKey-Locking Cylinder if you reverse the polarity.

– **Only** use batteries which have been **approved** by SimonsVoss.

– The cylinder must always be operated with two batteries.

– Dispose of old and used batteries in the proper manner and store them out of children's reach.

– Always replace both batteries when changing batteries.

– Do not touch the contacts on the new batteries with your hands when replacing the old ones. Use clean gloves free of fat or grease to handle the battery.

– When replacing the batteries, make sure that the electronics are not subject to mechanical load and are not damaged in any other way.

– Only use the SimonsVoss installation/battery key (Z4.KEY) to replace the battery.

12.1.3 General information

12.1.3.1 Product description

The SimonsVoss Digital Locking System is an electronic version of a mechanical locking system with the functions of a typical access control system.

The digital locking cylinder and the digital half cylinder are a main component in the locking and access control system, where radio communication replaces the mechanical authentication of a conventional key.

This product description details both the locking cylinder and the half cylinder. The design and operating mode of the two products are comparable in many respects. Any differences between the two products and different versions are pointed out in the corresponding sections.

'Locking cylinder' is taken to mean both 'locking cylinder' and 'half cylinder' in this document unless explicitly stated otherwise or taken out of context.

The data for authentication is transmitted with a transponder (25 kHz inductive).

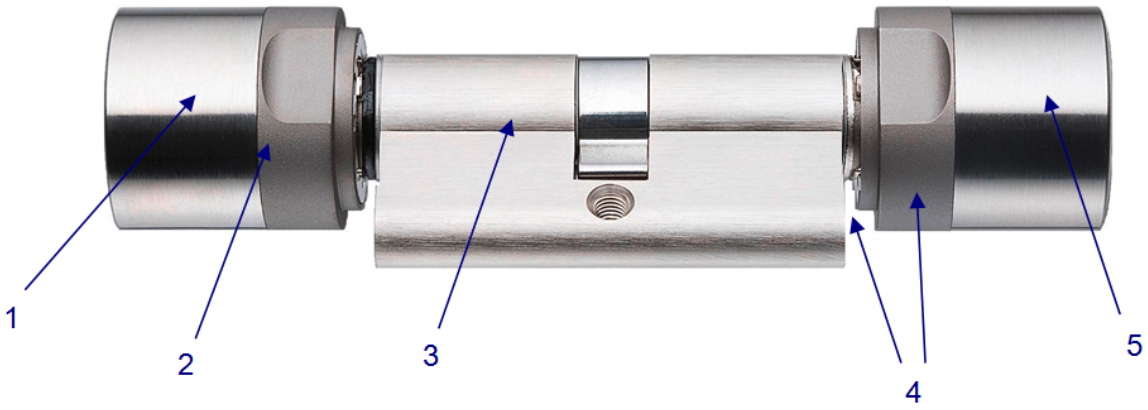
Manual
MobileKey Web-App

Digital locking cylinders are powered by two batteries in a redundant system. Cylinders operate as stand-alone components thanks to this integrated power supply, which also means there is no need to wire doors. An intelligent battery warning system also increases reliability.

The SimonsVoss system elements are not configured before delivery from the factory. They are first assigned to a locking system during initial programming. This makes it easier for stock keeping and makes product management simpler.

Thanks to modularity, all locking cylinders are seamlessly integrated into the SimonsVoss systems and, like all SimonsVoss components, they can be programmed using the relevant locking plan software *(e.g. LSM or MobileKey web app)* . Other different authentication media *(e.g. a PIN code keypad)* can be connected with the need for wiring. If the system is extended at a later stage, cylinders can be networked without wiring (e.g. for WaveNet or MobileKey ONLINE) and managed in an online interconnected system.

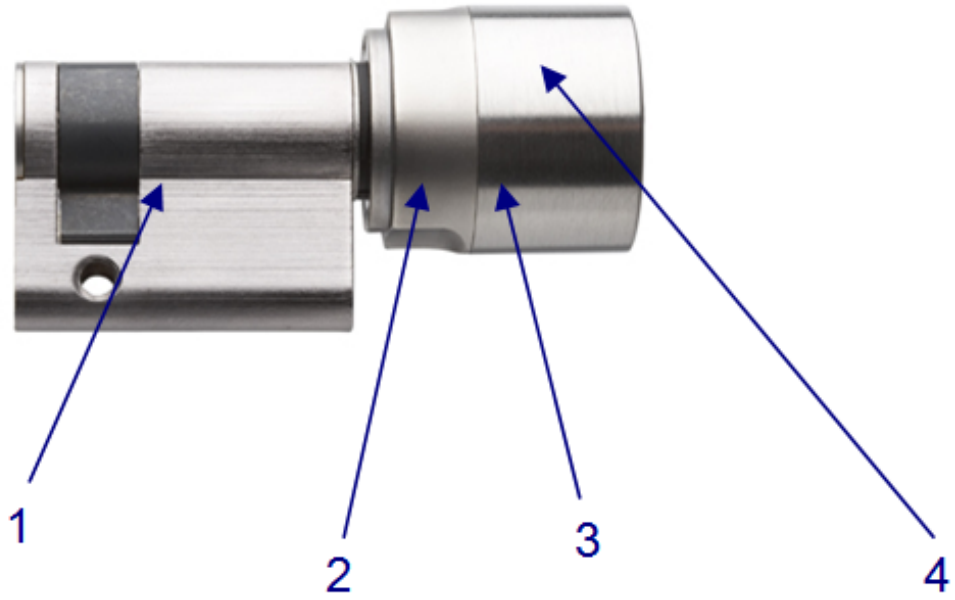
12.1.3.2 Locking cylinder design



1. Inside thumb-turn
2. Batteries/electronics
3. Actuator
4. Drilling protection
5. Outside thumb-turn

Manual
MobileKey Web-App

12.1.3.3 Half cylinder design



1. Actuator
2. Electronic systems
3. Batteries
4. Thumb-turn

12.1.3.4 Opening and locking from the outside

With freely rotating locking cylinders (FD)

The outer and inside thumb-turn rotate freely when not activated in the freely rotating MobileKey-Locking Cylinder, meaning it is not possible to open or lock the door without a valid ID medium. Identify yourself with your valid ID medium on the outer thumb-turn to activate the cylinder. If the ID medium is authorised, an audible signal will sound twice, the blue LED will flash twice and the locking cylinder will engage ready to open. Turn the outer thumb-turn in the direction of locking or opening. You have about five seconds to do so. The engage time can be configured. A single audible signal will then sound and the outer or inside thumb-turn will rotate freely again. Ensure that the outside or inside locking cylinder thumb-turn rotates freely again after the thumb-turn has been engaged ready for use.

NOTICE

If the user has an ID medium which is not authorised for use at that particular moment due to the time zone plan, a single audible signal will sound. The cylinder will not engage, so the outer or inside thumb-turn continues to rotate freely and the user cannot open the door. You need to configure this response separately in third-party systems.

Manual
MobileKey Web-App

12.1.3.5 Opening and locking from the inside

With freely rotating locking cylinders (FD)

The outer and inside thumb-turn rotate freely when not activated in the freely rotating MobileKey-Locking Cylinder, Doors can also only be opened or locked on the outside using an ID medium.

With non-freely rotating locking cylinders (FD)

MobileKey-Locking Cylinder which are permanently engaged for use on the inside can be operated from the inside without a ID medium. In this case, the door can be opened and closed using the inside thumb-turn without an authorised ID medium.

12.1.4 Versions

12.1.4.1 FD version (Standard)

Freely rotating MobileKey-Locking Cylinder on both sides

The .FD double thumb-turn cylinder is available from a length of 30-30 mm.

12.1.4.2 HZ version (Standard)

The standard version of the half cylinder.

12.1.4.3 TS version

Design as for standard version, but with the additional option of allowing the cylinder to engage without an identification medium. This cylinder version can be engaged mechanically with the aid of two buttons on the inside knob. This means that no transponder is needed when the user is on the inside. The cylinder will then engage for five seconds (configurable) and the door can be opened or locked. Once this time interval expires, the cylinder rotates freely again on both sides.

The .TS version cannot be retrofit.

12.1.4.4 AP2 Version

A cylinder with an anti-panic function must be fitted to all doors where the lock's panic function may be adversely affected by the position of the cam. This version contains an integrated spring mechanism which places the locking cam in a non-critical position, meaning a panic lock's panic function cannot be blocked.

You install this version in the same way as a normal MobileKey-Locking Cylinder.

The following aspects should be taken into consideration for doors along rescue routes which have been installed after April 1, 2003 (exit devices as per DIN EN 179 or DIN EN 1125): All MobileKey-Locking Cylinder models may be used for all exit devices where their approval states that the MobileKey-Locking Cylinder has no impact on the lock's function. The MobileKey-Locking Cylinder type .AP2 (anti-panic cylinder) must be used

for all exit devices where the MobileKey-Locking Cylinder cam position affects the lock's function. This must be stated in the lock manufacturer's approval.

⚠ DANGER Due to the structural design of panic locks, it is not permitted to turn the MobileKey-Locking Cylinder thumb-turn to the stop position when the door is locked since this may affect the lock's panic function.

12.1.4.5 WP Version (FD)

The protection rating is increased from IP 54 to IP 65 in the WP version (weatherproof) of the MobileKey-Locking Cylinder . This version is thus suitable for use outdoors or on external doors even if the cylinder is not exposed to direct splash water.

Anti-panic cylinder: The WP version is specifically designed for outdoor areas and should be fitted if the outside knob comes into contact with water (e.g. rainwater). The WP version features greater resistance to water, meaning the cam should not come into contact with water.

This version is available from a length of 30-35 mm and as .FD, .ZK, .MS and .FH models.

12.1.4.6 WP version (HZ/CO/AP)

The electronic knob is sealed in the WP version of the half, comfort and anti-panic cylinders, thus providing an increased protection rating of IP65. This version is thus suitable when the electronics side is outdoors, i.e. the electronic knob is exposed to rain, for example. Water must not enter through the door.

12.1.4.7 DM version (DoorMonitoring locking cylinder)

General information

This manual is a supplementary document for the "Digital Locking Cylinder and Digital Half Cylinder (TN4)" manual. The aforementioned document describes the installation, operation and battery replacement for the TN4 cylinder generation, which is also used for the DoorMonitoring (DM) cylinder. The safety instructions are also listed in the document, which are also valid for the DM Cylinder.

This particular document describes the DM Cylinder's functions. When the basic functions are used, the DM Cylinder behaves in exactly the same way as a SimonsVoss digital locking cylinder. For this reason, this product description only deals with the special features of the DM Cylinder. Reference is made to the product manual for "Digital Locking and Half Cylinder (TN4)", its installation and handling.

Manual
MobileKey Web-App

Description

The Door Monitoring Cylinder (DM Cylinder) is an electronic locking cylinder with integrated door monitoring. The integrated door monitoring system in the DM Cylinder is fitted without any wiring to the door.

Sensors within the DM Cylinder monitor the rotation of the cam. Sensors in the intelligent fastening screw monitor the door's opening status.

The DoorMonitoring Cylinder logs access events (access lists) and monitors the door status and changes to door status (open, closed, locked, securely locked, manipulation attempt and forced entry).

The following door statuses are logged:

– Door – open or closed
– Cam rotated once/twice (maximum four times) - door - unlocked / locked / securely locked
– Alarm

These door statuses can be transmitted to the software or web app via the network, where they can be displayed, so that the user can see the transmitted status easily.

Specifications

NOTICE

DM cylinders must not be used in multi-lock systems with gears (gear locking devices).

Standard design

The DM Cylinder is supplied in the following standard configuration:

– .DM DoorMonitoring
– .ZK access control, time zone management and events logging

The following accessories must be ordered with the standard configuration:

– Z4.DM.dd.SCREW.n Fastening Screw

NOTICE

You must indicate the backset when ordering the fastening screw

The fastening screw is manufactured to match the backset and is a few millimetres longer

Information is only correctly transferred to the cylinder if the fastening screw is the right length.

dd refers to the locking device's backset. Standard fastening screws are supplied for backsets between 25 and 110 mm at increments of 5 mm. Greater lengths are possible at increments of 5 mm.

Installation lengths

The DM Cylinder is supplied at 30-35mm and larger (outside – inside).

Manual MobileKey Web-App

Order codes

Refer to the respective current price list or the current product catalogue for the corresponding product codes.

Initial operation

Overview

Different functions are available, depending on the configuration:

	Offline	Online
Tracking to identify who last locked/ unlocked a door	Read access list using USB config device	Read access list using USB config device or the wireless network
Door status monitoring	no	Yes
Transmission of alarms to the matrix	no	Yes. Display in matrix
Generate events, such as a pop-up window	no	no
Incorporate locking device with profile cylinder profile	Yes	Yes
Monitoring of an SLP* locking device	no	no

Installation instructions

Installation and fitting

The DM Cylinder is installed in the same way as any other SimonsVoss digital cylinder.

Batteries are already installed when the product is delivered. The cylinder is ready for immediate use.

When installing the digital locking cylinder, ensure that there are no sources of low-frequency interference in the surrounding area. Typical sources are:

- Switch-mode power supply units
- High-voltage power lines
- Generators
- Frequency converters

Locking cylinders should be installed at least 0.5 m from one another while SmartRelays or activation units should be 1.5 m from one another

Manual
MobileKey Web-App

The locking cylinder housing may only project a maximum of 3 mm from the door in outdoor areas; a profile cylinder escutcheon or fitting should be used if necessary

You must not strike the thumb-turns when installing the cylinder

NOTICE

The DoorMonitoring Cylinder must not be fitted with conventional fastening screws

Conventional fastening screws may permanently damage the cylinder

a) The DM Cylinder must be fitted with a fastening screw especially manufactured for the cylinder

b) The fastening screw is not included in the supply package and must be ordered separately

The standard fastening screw is available for a backset between 25 mm and 110 mm at 5 mm increments. You must indicate the locking device backset when you order. If you use a fastening screw which is too short, the screw will not be able to provide a firm grip; if you use one which is too long, you cannot screw it fully within the door leaf

The head of the fixing screw features a sensor. The screw is tightened using a special screwdriver or adapter. If a conventional slot screwdriver is used, it could permanently damage the screw and the sensor

Lock standards specify that the hole diameter for the fastening screw must be at least 5.4mm. Some locking devices are supplied with a smaller drill hole. If this is the case, you can make it larger with a 5.5-mm steel drill bit

Installation

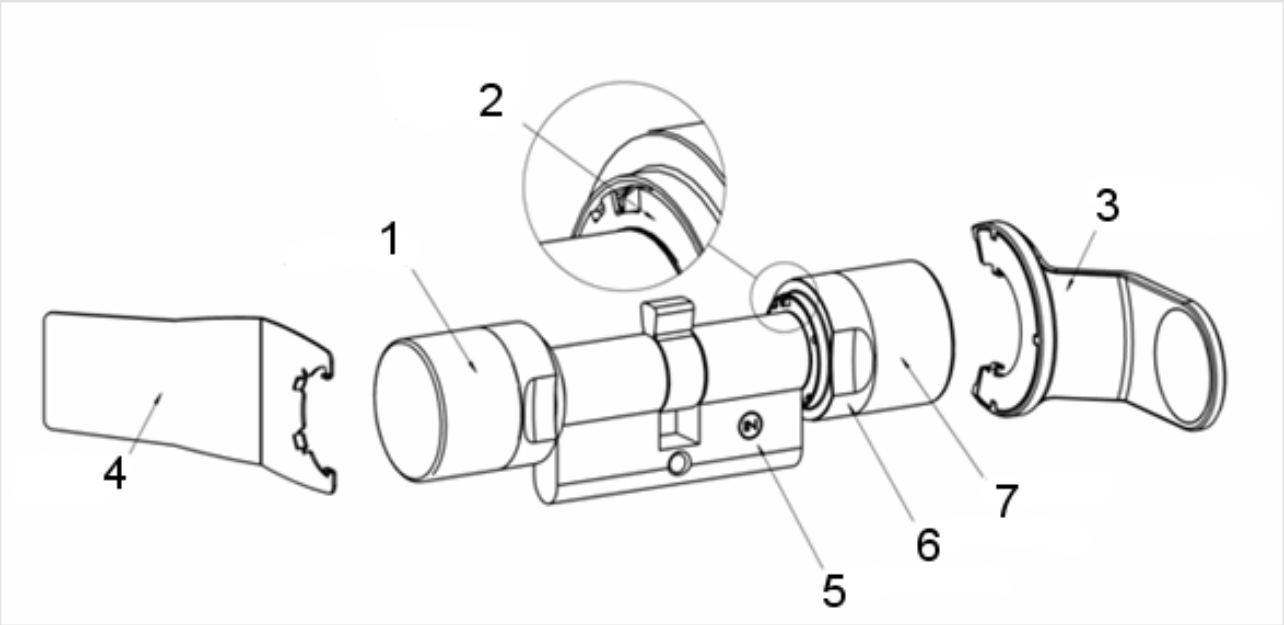
There is a thumb-turn with electronics and a thumb-turn without electronics in digital locking cylinders. The thumb-turn electronics must be removed for installation. The electronics thumb-turn is on the inside for almost all cylinders. The few exceptions are:

- Comfort Cylinder: .CO
- Swiss Round Cylinder: .SR

The word 'IN' is engraved on the cylinder body on inside of the cylinder

The thumb-turn without electronics is merely attached in position when delivered and can be easily removed

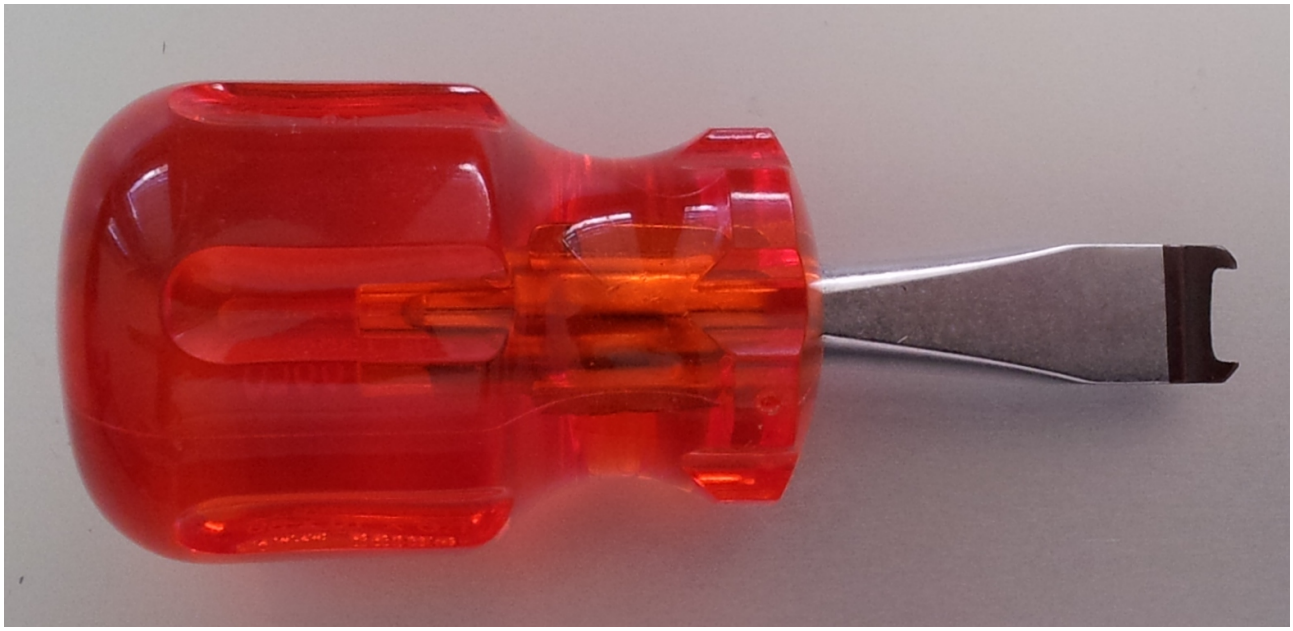
Manual
MobileKey Web-App



1. Outside thumb-turn (without electronics)
2. Locking disc with opening
3. Installation and battery key
4. Installation key (not for battery replacement)
5. Side marking
6. Recessed grip ring
7. Inside thumb-turn (with electronics)

1. Remove the thumb-turn without electronics
2. Insert the cylinder through the locking device

Manual
MobileKey Web-App



3. Fasten the cylinder with the appropriate fastening screw. Do not fasten screw tightly. Use the correct screwdriver only

NOTICE

If you tighten the fastening screw too firmly, this may cause the locking cylinder to malfunction in the locking device (e.g. it may jam).

Tighten the fastening screw firmly by hand (max. 3.5 Nm)

Do not use a battery-operated screwdriver

NOTICE

A conventional screwdriver can damage the sensor in the fastening screw

Tighten the fastening screw with the appropriate screwdriver only

4. Replace the thumb-turn and rotate until the thumb-turn grips into the indents in the flange
5. Place the installation key on the outer thumb-turn in such a way that the two teeth locking device into the outer thumb-turn; if necessary, turn the thumb-turn until both teeth engage into the locking disc
6. Lock the thumb-turn into position again by rotating it 30° in a clockwise direction

Magnet installation

The magnetic plates which come with the fastening screw must be affixed to the door frame for door monitoring. The magnets act as a signalling mechanism for the sensor in the fastening screw. A functions test should be carried out after installation

Manual MobileKey Web-App

One or more magnetic plates need to be affixed, depending on the door and frame material and the gap width

1. Loosely affix the magnetic plates to the door frame, so that the plates are positioned opposite the head of the fastening screw
2. Carefully close the door, so that the latch almost engages
3. If the display in LSM switches from 'Open' to 'Closed' when the door is almost closed:
   - Reduce the number of magnetic plates
   - Move the plate further towards the centre of the frame
   - Make the plate smaller
4. Close door. The display in LSM must change from 'Open' to 'Closed.' If this is not the case, the magnetic field is too weak for the sensor. Affix another plate to the frame and repeat the test

If the magnetic field is too big (too many plates), this will cause the sensor to overreach, so that it no longer responds

Use in escape doors

Use in an escape door locking device

Panic locking devices can be unlocked and opened from the inside by pushing the door handle. The locking device unlocks without the cam rotating. Some locking devices require an anti-panic cylinder since the cam can cause the locking device to jam when in certain positions. You need to clarify with the locking device manufacturer whether an AP cylinder must be used or not. Different issues need to be clarified in advance when the DM Cylinder is used in escape door locking devices:

– SLP locking device or non-SLP locking device

– Use of an AP cylinder required to prevent the locking device from jamming

– Typical usage behaviour of the door.

Is the door normally opened with an authorised transponder or by pressing the inside handle? The DM Cylinder records the cam's movements and detects the locking device status based on rotations and the direction of rotation. It does not record retraction of the bolt and, consequently, does not register the unlocking of the door either. Cam monitoring is deactivated in the DM.AP2 Cylinder. Manual locking is not monitored.

NOTICE

You must comply with the requirements in DIN EN 179 or EN 1125 when fitting an escape door locking device.

Manual MobileKey Web-App

Use in an SLP locking device

An SLP (self-locking panic) locking device can be opened on the inside by pressing the door fitting and locked when the door is closed. This means that the DM Cylinder does not reliably indicate the bolt position (at all). The DM.AP2 does not monitor the bolt position. This means that only the door's opening status can be monitored.

Day-to-day operation

You can display the key information about your locking system directly in the locking plan. The DM Cylinder's door statuses can be shown directly on the locking plan

The door statuses are displayed using different icons in the matrix

Icon	Status	Information
	Door securely locked	Door is locked and cam has been rotated to [securely locked] position
	Closed	Door is closed and bolt retracted
	Open	Door open
	Error message - undefined status / warning / alarm	This icon has different meanings: Door open too long Fastening screw has been manipulated (no longer addresses, has been removed) Magnetic field manipulation (magnetic field on the fastening screw is too extensive) Door has been forced open (door is opened despite locking)
	Status unknown	Undefined status – the status is unknown due to a malfunction or a non-logical change to the system

Table 1: Door monitoring icons in the matrix

Unknown status

The 'Unknown status' icon and the alarm icon do not change automatically if the reason for the malfunction disappears (an exception is the 'Door open too long alarm' which does not disappear when the door is closed).

Error message	Action
Undefined door status	Door must be opened, then closed again. The cylinder detects the status and transmits it to the software or web app.

Manual
MobileKey Web-App

Error message	Action
Door open too long	Close door
Fastening screw has been manipulated (has been removed)	Check fastening screw. Reset the error once it has been eliminated; see section on Cylinder
Magnetic field manipulation (fastening screw magnetic field too extensive)	Check door. Reset error; see section on Cylinder
Door has been forced open (door is opened despite locking)	Check door. Reset error

NOTICE

Resetting the alarm signals

Important alarm signals (intrusion) must be reprogrammed by hand to reset in offline mode. This is why we **always** recommend networking using WaveNet or MobileKey ONLINE.

Batteries

Battery life

The battery life depends on the DM Cylinder configuration settings and the use behaviour. The following affect the battery life:

- The fastening screw sampling interval
- Number of activations
- Reading the access list
- Changes to programming
- Number of tasks

The number of activations totals up to 50,000.
The battery life depends on the fastening screw setting:

Sampling interval	Battery lifetime
Fixed	Up to 4 years

Table 2: Sampling intervals and battery life

The indicated battery life serves as a guide. A battery warning is not emitted when the aforementioned service life expires, but is based on the measured battery capacity instead.

Battery warning levels

Warning Level 1	Warning Level 2
8 short audible signals before engaging	Eight short audible signals 30 seconds long with one second pause each time before engaging
Up to 15,000 access events or up to 9 months on standby	Up to 50 access events or up to 30 days

Table 3: DM Cylinder battery warning levels

Manual
MobileKey Web-App

NOTICE

The cylinder's monitoring function is deactivated from Warning Level 2. Changes to the cylinder status are not logged or transmitted.

Once Warning Level 2 has been emitted for the first time, the door can be opened with a transponder around 50 times.

Error diagnosis

Symptom	Cause	Solution
Fastening screw cannot be fully tightened	Fastening screw too long	Re-measure backset. Order fastening screw according to backset size You must not shorten the fastening screw under any circumstances. This will permanently damage the sensor
Fastening screw does not grIPwhen turned	Fastening screw too short	Re-measure backset Order fastening screw according to backset size
Door status is not shown in the web app	Connection between cylinder and web app is malfunctioning	Check whether the error also occurs when the cam bit rotates. If it does, the connection is malfunctioning. Check network Is the cylinder (network cover) integrated into the network?
	Magnetic field around fastening screw sensor too weak	Affix additional magnetic plate
	The sensor does not detect the magnetic field if it is too weak	Reduce gap between door and frame
	Magnetic field around fastening screw sensor too strong	Remove magnet plate
	The sensor overreaches if the magnetic field too strong	Increase gap between door and frame

Manual
MobileKey Web-App

Symptom	Cause	Solution
	Fastening screw too short.	Re-measure backset
	No contact between the sensor in the fastening screw and the cylinder	Order fastening screw according to backset size
	DM Cylinder configured incorrectly	Check DM Cylinder configuration. Is there a check mark against 'Door open' in the access list? Is transmission via network configured? Is sampling interval configured for fastening screw?
		Flip-flop mode or time switch-over configured? > The bolt status cannot be checked
	Defective cylinder	Replace cylinder
	DM Cylinder activated in flip-flop mode or time switch-over	DM Cylinder cannot be operated in flip-flop mode or time switch-over. Change mode and open and close door, so that cylinder returns to a defined status
	Defective cylinder	Replace cylinder
	Network connection unstable	Examine surroundings for sources of interferences, such as fluorescent tubes, dim switches, generators, mains adapters

Forward events

Check the network settings if the door statuses are not displayed correctly.

Accessories

Battery set

There is a set of batteries with replacement batteries available for the cylinder. The set consists of 10 CR2450 batteries.

Order code: Z4.BAT.SET

Manual
MobileKey Web-App

Fastening screw

The DM Cylinder requires a special fastening screw with an integrated door opening sensor.

Order code: Z4.DM.xx.SCREW.n

Fastening screw xx indicates the locking device's backset and should not be confused with the fastening screw length. Standard fastening screws are supplied for backsets between 25 and 70mm at increments of 5 mm. Special lengths available on request.

Screwdriver

The screw head on the fastening screw rises in the middle, so that the fastening screw cannot be fastened with a normal slot screwdriver. A screwdriver is available as a tool.

Order code: Z4.DM.SCREWDRIVER

WaveNet network cover LN.I

The WaveNet network cover is a replacement cover and contains the electronics required to connect the DM Cylinder with the network.

Technical specifications

Cylinder model	Euro Profile DoorMonitoring Cylinder as per DIN 18252/ EN1303, stainless steel, freely rotating on both sides
Protocol generations	G2 or MobileKey
Thumb-turn diameter	30 mm
Basic installation length	30-35 mm (external/inside dimension)
Protection rating	IP54 (when installed)
Air humidity:	95%; (non-condensing)
Battery type	2 x lithium, CR2450, 3 V
Battery life	Up to 50,000 actuations or 4 years on standby with a fastening screw sampling interval of 2 seconds
Temperature range	Operational: -25 °C to +65 °C In storage: -35 °C to +70 °C
Access memory	About 1,000 door statuses can be stored
Time zone groups	100+1 *(time zone groups are not supported in MobileKey)*
Number of transponders per locking cylinder	Up to 64,000 or 100 for MobileKey
Network	Network-ready with integrated LockNode (Network Thumb-Turn Cover WNM.LN.I)

Table 4: Technical specifications - DoorMonitoring Cylinder

Manual
MobileKey Web-App

12.1.5 Installation instructions

12.1.5.1 General instructions

When installing the digital MobileKey-Locking Cylinder, ensure that there are no sources of low-frequency radio interference in the surrounding area.

The profile cylinder housing should be fitted flush in outside areas; it should project a maximum of 3 mm and a profile cylinder escutcheon or security fitting should be installed if necessary. It is also important to ensure that no water is able to penetrate the cylinder via the cam section.

You must not strike the thumb-turns when installing the cylinder.

Both thumb-turns are locked into place with a bayonet mount.

The inner side of the MobileKey-Locking Cylinder is laser-engraved with the letters IL for inside length on the profile cylinder housing; the electronics side is identifiable by the black plastic ring between the thumb-turn and the profile cylinder housing.

Batteries are already installed before delivery.

All the tasks listed in this section can also be carried out using the installation/battery key.

12.1.5.2 Programming

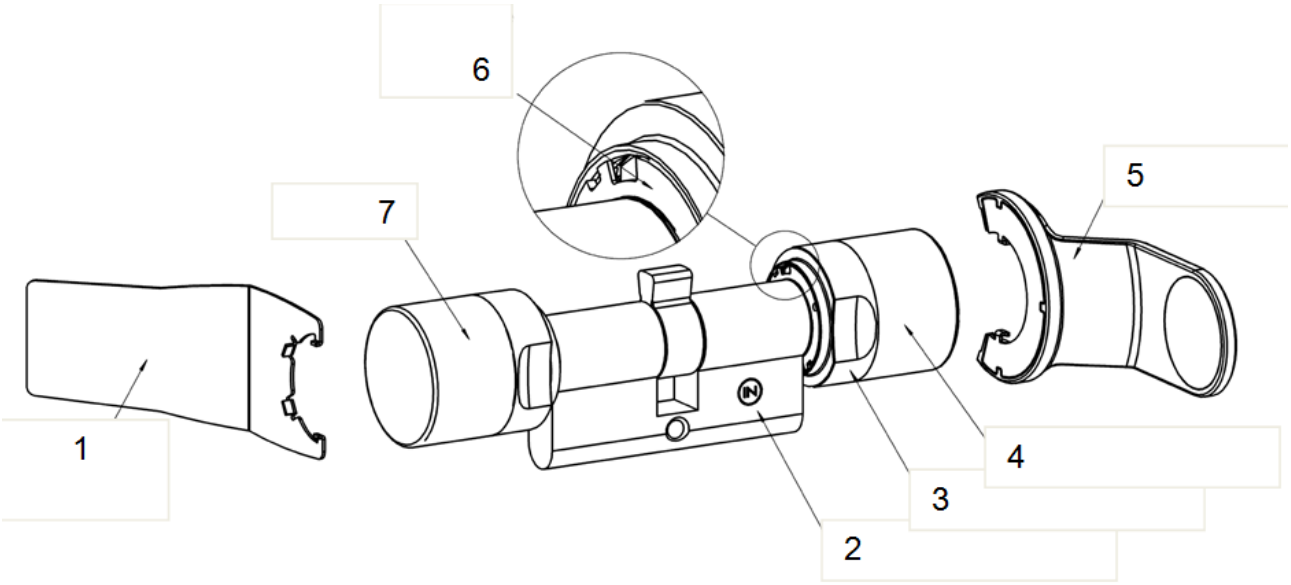
Both the digital and the associated identification media must be programmed before installation.

Programming MobileKey-Locking Cylinder in MobileKey: See Programming components [▶ 13]

Manual
MobileKey Web-App

12.1.5.3 Installation variants

Installation of double thumb-turn cylinders (except types .AP/.SKG/.VdS)



1. Installation key
2. Side marking
3. Recessed grip ring
4. Inside thumb-turn
5. Battery replacement key
6. Locking disc with opening (identical on outside)
7. Outside thumb-turn

Removing the outside thumb-turn

Place the installation key on the outside thumb-turn in such a way that its two teeth engage into the outside thumb-turn; if necessary, turn the thumb-turn until both teeth lock into the locking disc.

NOTICE

The installation tool must be placed flat on the inside front surface of the thumb-turn to ensure that the tool can lock into the locking disc.

Hold the outside thumb-turn firmly and carefully turn the installation tool about 30° in a clockwise direction (until you hear a click). Detach door thumb-turn.

Manual
MobileKey Web-App

Fastening the digital cylinder into the lock

Turn the cam until it is vertical and pointing downwards. Insert the digital locking cylinder through the lock in such a way that the inside thumb-turn (see diagram above) is facing the inner side of the door. Fasten the cylinder into the mortise lock with the fastening screw.

NOTICE

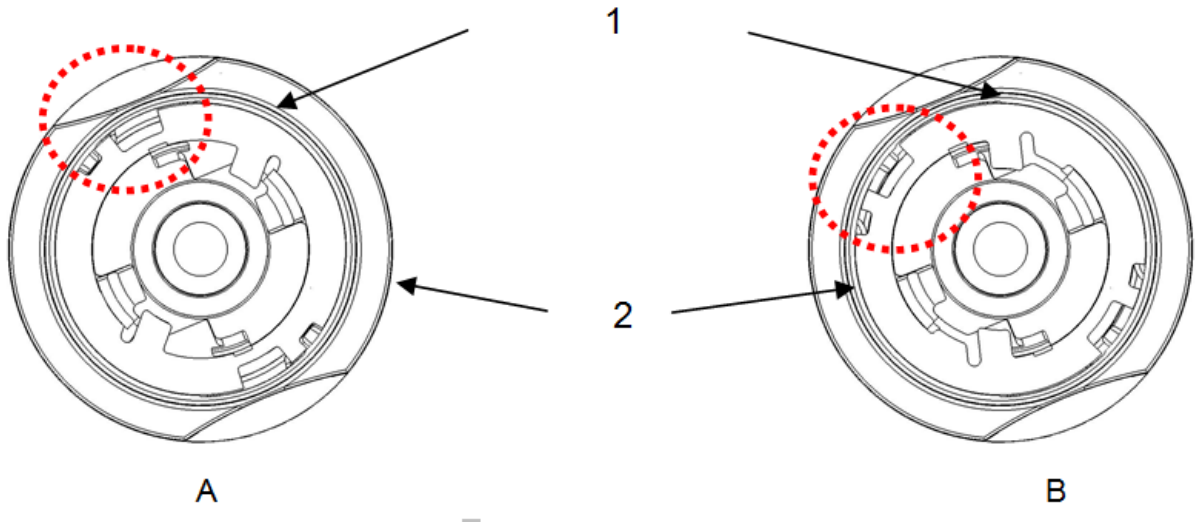
You must not strike the thumb-turns when installing the cylinder. Do not allow the cylinder to come into contact with oil, grease, paint or acids.

Fastening the outside thumb-turn

Replace the thumb-turn and turn in an anti-clockwise direction while applying slight pressure until the outer thumb-turn grips into the indents in the flange. Possibly place the thumb-turn in this position by pressing it towards the profile cylinder housing.

NOTICE

Turning the bayonet disc when not installed may prevent the thumb-turn from being fastened into position. In such a case, push the disc back into the original 'bayonet disc open' position using the installation tool. (see diagrams)



1. Bayonet disc
2. Thumb-turn
3. Bayonet disc closed
4. Bayonet disc open

Manual
MobileKey Web-App

Place the installation key on the outside thumb-turn in such a way that its two teeth engage into the outside thumb-turn; if necessary, turn the thumb-turn until both teeth lock into the locking disc. Lock the thumb-turn into position again by rotating it 30° in a clockwise direction.

Carry out a function test

1. Engage cylinder using a valid ID medium and turn the thumb-turn in both the locking and opening direction with the door open. The thumb-turn must be able to rotate easily when you do so.
2. Close the door and repeat the process. If the locking cylinder should be stiff, you need to align the door or modify the strike plate.

Fitting an anti-panic cylinder

Removing the inside thumb-turn

Loosen the inside thumb-turn's threaded pin (see diagram above) using an Allen key. Do not unscrew completely. Hold the cam firmly and then turn the inside thumb-turn anti-clockwise or, in the case of a freely rotating AP cylinder, remove the thumb-turn after loosening the threaded pin.

Fastening the digital cylinder into the lock

Turn the cam until it is vertical and pointing downwards. Insert the digital locking cylinder through the lock from the outside in such a way that the outside thumb-turn is facing the outer side of the door. Fasten the cylinder into the mortise lock with the fastening screw.

NOTICE

You must not strike the thumb-turns when installing the cylinder. Do not allow the cylinder to come into contact with oil, paint or acids.

Fastening the inside thumb-turn

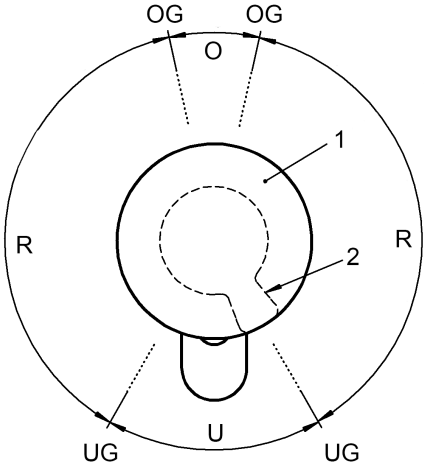
Screw the inside thumb-turn onto the thread until it locks into place as it comes up against the cam in the lock. Pull on the inside thumb-turn, or push on the inside thumb-turn of a freely rotating AP cylinder, until it locks into position. Fasten the threaded pin tightly using the Allen key.

Functions test

– To verify that the AP2 cylinder functions correctly in an anti-panic lock, you must check that the cam moves easily and that the door opens correctly using the procedure described below.
– Carry out the functions test in the direction of escape.

Manual
MobileKey Web-App

– You must carry out a functions test whenever the cylinder or the fastening screw is repositioned.
– You will need an authorised identification medium to carry out the functions test.
– Withdraw the deadbolt before testing.



U section:	No restore force on the cam
R section:	Restore force section towards U section
O section:	Top dead point in deadbolt throw - no restore force on the cam
OG:	Top threshold section
UG:	Lower threshold section
1:	Thumb-turn
2:	Cam position (concealed)

1. With the cylinder engaged, first turn the thumb-turn in the direction of locking as far as the deadbolt throw in the 'R' section.
   ⇨ You will feel the restore force. When you release the thumb-turn in this position, it must turn back to the 'U' section of its own accord.
2. Lock the lock and check the restore force. To do so, turn the engaged thumb-turn in the direction of locking through the 'R' section and into the 'O' section.
   ⇨ The deadbolt extends. There is no restore force in the 'O' section.
3. Move the thumb-turn slightly over the threshold between the 'O' and 'R' section in the same direction of rotation.
   ⇨ The deadbolt will extend. The restore force must turn the thumb-turn automatically from this point as far as the 'U' section if it is released.

Manual
MobileKey Web-App

⇨ If the knob does not automatically rotate as far as the 'U' section, either the fastening screw has been tightened too firmly or the lock has been aligned incorrectly. The test is to be repeated after the fault has been eliminated. A fastening screw which has been tightened too firmly acts as a brake on the restoring force mechanism.

4. Lock the door and check that the lock functions correctly by pressing the handle or panic bar in the direction of escape.
   ⇨ The deadbolt must spring back and it must be possible to open the door easily.
   ⇨ If the deadbolt does not draw back when the handle is turned or the handle catches, either the locking cylinder or the lock is incorrectly aligned or defective. The test is to be repeated after the fault has been eliminated as described above.

If you cannot ensure that the lock will function correctly after the functions test, please contact the SimonsVoss hotline.

12.1.6 Audible signals

The MobileKey-Locking Cylinder emits an audible signal to indicate its status and an authorisation. The table below lists what the audible signals mean.

2 short audible signals before engaging and a short tone after disengaging.	Normal activation	None
1 short audible signal: cylinder does not engage.	Attempted entry with a transponder listed in the locking system, but: – used outside time zone.	None
Battery Warning Level 1: 8 short audible signals before engaging.	Batteries are low.	Replace batteries in the cylinder.
Battery Warning Level 2: 8 short audible signals 30 seconds long with one second pause each time before engaging.	Batteries are almost completely empty.	Replace batteries in the cylinder immediately.
8 short audible signals after disengaging.	Transponder battery is low.	Have transponder battery replaced.

Manual
MobileKey Web-App

12.1.6.1 Battery warnings

A battery management system has been implemented in locking cylinders and transponders which warns the user in good time that the battery capacity is diminished. This prevents the batteries from becoming fully discharged. The individual battery warning levels are described below.

The locking cylinder batteries feature a redundant system. If one of the batteries fails or its capacity falls below a certain level, the system emits a battery warning.

– Warning Level 1: Low batteries

  If the charged capacity falls below 25% in one of the batteries, Battery Warning Level 1 is activated. After you activate the transponder, you will hear eight brief audible signals in rapid succession before the cylinder engages. You must replace the batteries.

– Warning Level 2: Extremely low batteries

  If the locking cylinder batteries discharge even further, short audible signals are heard in rapid succession for about 30 seconds before the cylinder engages after the transponder is activated. The cylinder does not engage until the audible signals have finished. The batteries should be replaced as quickly as possible.

	WARNING LEVEL 1	WARNING LEVEL 2
Active cylinder:	8 short audible signals before engaging	Eight short audible signals 30 seconds long with one second pause each time before engaging
	Up to 15,000 access events or up to 9 months on standby	Up to 50 access events or up to 30 days

12.1.6.2 Battery warning for transponders

When the transponder battery is low, short audible signals are heard in rapid succession on the locking cylinder (not the transponder) after the locking cylinder disengages each time the transponder is used.

12.1.7 Battery replacement

12.1.7.1 General instructions

Only trained personnel may replace batteries.

You must wear clean gloves made of cloth and free of fat or grease when replacing the batteries to prevent the batteries being contaminated by fingerprints. Fingerprints on batteries may reduce battery life considerably.

Only use batteries which have been approved by SimonsVoss.

Manual
MobileKey Web-App

NOTICE

Damage may be caused to the MobileKey-Locking Cylinder if you reverse the polarity. The batteries used in this device may pose a fire or burn hazard if handled incorrectly. Do not recharge, open or burn batteries, or heat them to over 100° C.

NOTICE

Dispose of lithium batteries properly immediately after they have discharged. Store them out of children's reach; do not open and do not throw into a fire. Always replace both batteries when changing batteries. Please note safety instructions.

The locking cylinder retains its status, programming and saved protocols even without power supply.

12.1.7.2 Battery life

Battery life is different for each locking cylinder version as power consumption varies when the cylinder is activated or a data connection is established.

VERSION	BATTERY LIFE	NUMBER OF ACTIVATIONS	NUMBER OF BATTERIES
Standard cylinder and versions	Up to 10 years	Up to 300,000	2
WN (LNI / LockNode)	Up to 5 years	Up to 150,000	2

The specified battery life is for guidance only. A battery warning is not emitted when the aforementioned battery life expires, but is based on the measured battery status instead.

12.1.7.3 Procedure

1. Place the installation/battery key on the inside thumb-turn in such a way that the two teeth lock into the openings in the locking disc; if necessary, turn the thumb-turn until both teeth engage into the locking disc.

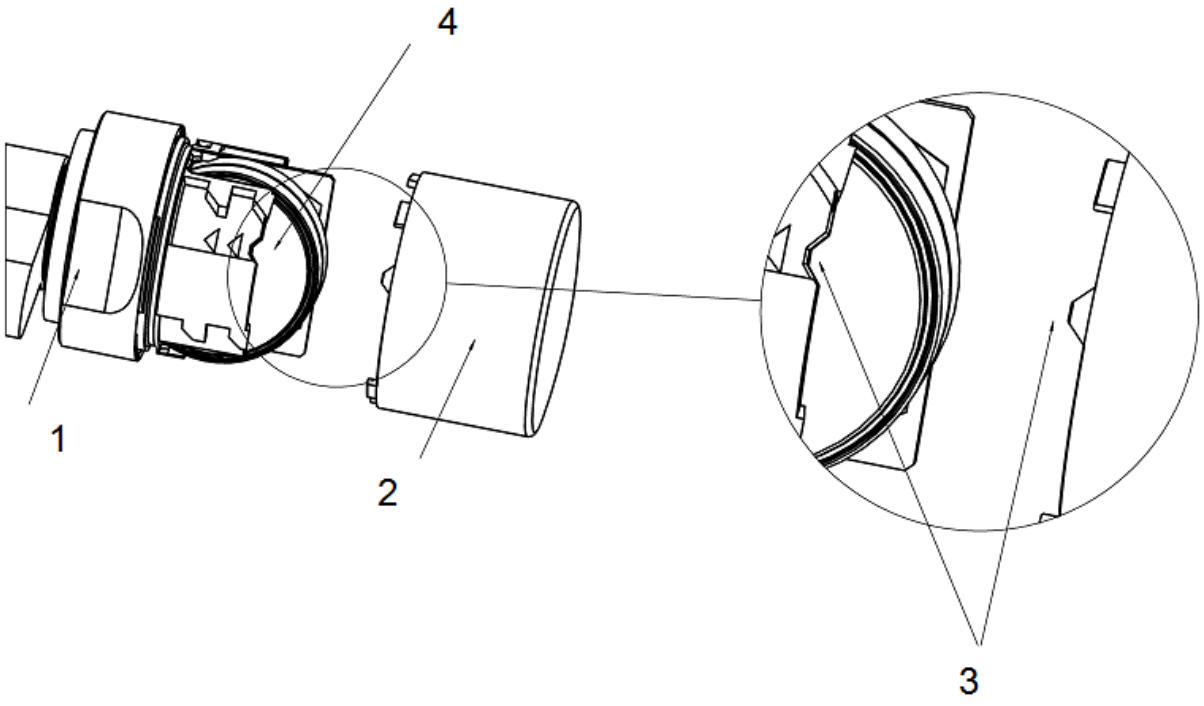
NOTICE

The tool must be placed flat on the inside front surface of the recessed grip ring to ensure that the installation/battery key can engage into the locking disc.

2. Hold the inside thumb-turn firmly and carefully turn the installation/battery key about 30° in a clockwise direction (until you hear a click).
3. Remove installation/battery key from the thumb-turn.
4. Push recessed grip ring backwards towards the door, so that it comes away from the thumb-turn.

Manual
MobileKey Web-App

5. Hold recessed grip ring firmly and turn thumb-turn about 10° in an anti-clockwise direction and remove.
6. For MH cylinders only: Carefully fold antenna upwards.
7. Carefully remove both batteries from the holder.
8. Insert the new batteries into the holder at the same time with the positive poles next to each other; change the batteries as quickly as possible. Use clean gloves free of fat or grease to handle new batteries.



9. For MH cylinders only: Lock antenna back into place.
10. Replace the thumb-turn (align the triangle mark as in the diagram), hold the recessed grip firmly and fasten the inside thumb-turn by turning in a clockwise direction (about 10°). (Diagram may differ slightly from the purchased product)
11. Push recessed grip ring back onto the thumb-turn, so that the thumb-turn and ring close together in a flush fit.
12. Place the installation/battery key on the inside thumb-turn in such a way that the two teeth lock into the openings in the locking disc; if necessary, turn the thumb-turn until both teeth engage into the locking disc.
13. Close the thumb-turn again by turning it about 30° in a clockwise direction (until you hear a click).

Manual
MobileKey Web-App

Then activate an authorised ID medium and check that it functions.

12.1.8 Maintenance, cleaning and disinfection

NOTICE

Digital locking cylinders MUST not come into contact with oil, grease, paint or acids.

NOTICE

The use of unsuitable or aggressive disinfectants can damage the locking cylinder.

Clean the locking cylinder if necessary with a soft, moist cloth.

Only use disinfectants explicitly suitable for the disinfection of sensitive metal surfaces and plastic.

NOTICE

HZ.SL:*In the case of frequent use of automatic locking, we recommend applying some lubrication to the latching edge on the control cabinet lever hold.*

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

Carry out a new functions test after changing the batteries in anti-panic cylinders.

12.1.9 Areas of use

12.1.9.1 General information

The digital locking cylinder is compatible with locks for Euro profile cylinder as per DIN 18252 and EN1303.

12.1.9.2 Fire doors

As a general rule, this cylinder can be fitted into fire doors. However, you must check that it is actually approved for use in fire doors.

12.1.9.3 Doors along rescue routes

Type .AP should be installed for use in doors with an anti-panic function in which the position of the cam may have an effect on the lock's functioning. This must be specified in the lock manufacturer's approval. Also see industrial standards EN 179 and EN 1125 and the individual lock manufacturers' data sheets.

Manual
MobileKey Web-App

12.1.9.4 Installation outdoors

If you are unable to ensure that no water will come through the door, we recommend using the respective .WP versions. The outside knob is completely sealed in the anti-panic cylinder model and the whole cylinder is sealed in the double cylinder model.

12.1.10 Accessories

12.1.10.1 Knobs

The following special knobs are available as accessories:

- Outside knob in a TN4 design
- Outside knob, 42 mm in diameter with recessed grips
- Inside knob, 36 mm in diameter for a .TS cylinder
- Outside knob, shortened
- Brass knob, matt (inside and outside knob)

These knobs can replace the original locking cylinder knobs at any time. See Installation instructions or Battery replacement for knob installation.

12.1.10.2 Core extraction protection adapter (Z4.KA.SET)

This adapter is compatible with all SKG/VdS cylinders manufactured up to 2010 and all .FD cylinders.

There is a mechanical extension for core extraction protection fittings as the profile cylinder profile is not cut out of these fittings. The extension is 8 mm long and can be retrofitted at any time.

12.1.10.3 Tool

In addition to the installation tool, a battery replacement key is also included in the supply package. You can use this tool to install or remove outside thumb-turns and replace batteries.

12.1.10.4 Battery set

A new set of batteries can be ordered, which contains ten CR2450 batteries. Only ever use batteries approved by SimonsVoss.

12.1.11 Data sheets

12.1.11.1 Locking cylinder

Profile cylinder

Basic length:	Outside 30 mm, inside 30 mm (AP/WP 35mm)

Manual
MobileKey Web-App

Installation lengths in 5 mm increments, overall length up to 140 mm (max. 90 mm on one side); special lengths on request.

Batteries

Type:	CR, 2450, 3 V
Manufacturer:	Sony, Panasonic, Varta
Quantity:	2 units
Battery life:	up to 300,000 lock operations or up to 10 years on standby

Ambient conditions

Operating temperature:	-25 °C to +65 °C
Storage temperature:	-35°C to +65°C
Protection class:	IP54 (when installed); .WP variant: IP65

Features

- 3,000 access events can be logged (ZK)
- Network-ready with integrated LockNode (WN)
- LockNode can be retrofitted
- Max. number of transponders per cylinder: 100
- Different permanent/open modes

Thumb-turns

Material:	Stainless steel
Colours:	stainless steel, brushed
Diameter:	30 mm
Length:	37 mm (from front surface of profile)

12.1.11.2 Half cylinder

Thumb-turns

Material:	Stainless steel
Colours:	stainless steel, brushed
Diameter:	30 mm
Length:	37 mm (from front surface of profile)

Profile cylinder

Basic length:	outside 30 mm, inside 10 mm

Installation lengths in 5 mm increments (no installation kit) an overall length of up to 100 mm with a maximum length of 90 mm on the outer side of the cylinder. Greater lengths on request.

Batteries

Type:	CR, 2450, 3 V
Manufacturer:	Sony, Panasonic, Varta
Quantity:	2 units
Battery life:	up to 300,000 lock operations or up to 10 years on standby

Features

- 3,000 access events can be logged (ZK)

Manual
MobileKey Web-App

– Network-ready with integrated LockNode (WN)
– LockNode can be retrofitted
– Different permanent/open modes

Ambient conditions

Operating temperature:	-25 °C to +65 °C
Storage temperature:	-35 °C to +65 °C
Protection class:	IP54 (when installed); .WP variant: IP66 (thumb-turn)

12.2 PIN code keypad manual

12.2.1 Intended use

The PIN code keypad can be used to activate SimonsVoss locking devices, *such as locking cylinders, SmartHandles or SmartRelays* by entering a numerical code.

The PIN code keypad is integrated into the locking system using the corresponding locking system software.

– The PIN code keypad can store up to 3 User PINs, which can be regarded as 3 separate transponders.
– User PINs may contain between 4 and 8 characters.
– You can configure User PINs directly on the PIN code keypad by entering the Master PIN first.

12.2.2 Safety instructions

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

⚠ CAUTION The batteries used in this product may pose a fire or burn hazard if handled incorrectly. Do not recharge, open or burn these batteries, or heat them to over 100°C.

⚠ CAUTION The products/systems described in this manual may only be operated by persons who are qualified to perform the related tasks. Qualified staff are capable of identifying any risks associated with handling these products/systems and avoiding potential hazards thanks to their knowledge and skills.

Manual
MobileKey Web-App

NOTICE

The Master PIN is a main, integral component of the PIN code keypad security concept. You must ensure that the Master PIN is kept in a safe, secure place and can be consulted at any time. Losing the Master PIN will significantly impair locking system operation.

NOTICE

Ensure that you do not get the PIN code keypad dirty or scratch it. You must not let the PIN code keypad drop onto the floor or expose it to any other type of strong impact.

NOTICE

SimonsVoss Technologies GmbH reserves the right to make changes to the product without prior notification. For this reason, descriptions and illustrations in these documents may differ from the latest versions of products and software. The original German version should be taken as a reference in cases of doubt. Errors and spelling mistakes excepted. You can obtain more information about SimonsVoss products online at: www.simons-voss.com

NOTICE

You should dispose of batteries in compliance with local and national regulations.

12.2.3 Configuration

12.2.3.1 Changing the master PIN

You only need to carry out this step if no new Master PIN has been programmed yet.

1. Enter 0 0 0 0
2. Enter old Master PIN: 1 2 3 4 5 6 7 8
3. Enter new Master PIN
   ⇨ The new Master PIN must consist of 8 characters which must not be consecutive or identical and must not begin with 0.
4. Re-enter the new Master PIN

NOTICE

The Master PIN is essential to use the PIN code keypad and cannot be imported, read or regenerated. Make a note of the Master PIN and keep it in a safe, secret place.

The Master PIN can be changed at any time. No programming is required to make a change.

Manual
MobileKey Web-App

12.2.3.2 Programming a user PIN

Up to three User PINs can be issued in the PIN code keypad. The User PIN may consist of between 4 and 8 digits, which must not be consecutive or identical.

An aid to better understanding: Each User PIN *behaves as a separate transponder. As a result, these individual* User PINs *must be programmed in the respective (internal) transponders (1, 2 & 3).*

1. Enter 0
2. Enter Master PIN
3. Enter User PIN – e.g. 1 for User PIN 1
4. Enter the length of the User PIN – e.g. 4 for a 4-digit User PIN
5. Enter User PIN

Repeat the process to programme otherUser PINs into the PIN code keypad.

12.2.3.3 Deleting a user PIN

User PINs can be deleted by setting the length of the PIN to 0 characters:

1. Press '0' to switch to programming mode.
2. Enter the 'Master PIN'.
3. Press the button '1' on the PIN code keypad to delete the user PIN 1, for example.
4. Enter '0' for the PIN length.
   ⇨ The User PIN will then be deleted if the input has been entered correctly.

12.2.4 Programming

Programming components [▶ 13]

12.2.5 Assembly & battery exchange

The PIN code keypad can be installed using the supplied installation accessories.

– You can use the enclosed special adhesive pad to affix thePIN code keypad making installation quick and easy.
– We recommend using the supplied screws to secure the component. For this, a "TX6" Torx screwdriver *(not contained in the scope of delivery)* is required to open the housing!

Install the PIN code keypad at a distance of up to 20 cm from the locking device.

Manual
MobileKey Web-App

To exchange the batteries, the housing of the PIN code keypad must be opened. For this, a "TX6" Torx screwdriver *(not contained in the scope of delivery)* is required to open the housing! Replace all batteries with new Sony, Panasonic or Varta batteries of the type CR 2450 (3V).

12.2.6 Operation

✓ The PIN code keypad has now been successfully configured. (master PIN & user PIN)

✓ The PIN code keypad has been programmed correctly.

✓ At least one User PIN is authorised for use on the locking device concerned.

1. Enter a User PIN.
   ⇨ You have a maximum of 5 seconds to enter each individual number.
2. The LED will light up green and an audible "beep, beep" will sound when you enter numbers.
   ⇨ The locking device will engage.

If the PIN code keypad LED lights up red and a long audible "beep" sounds, no valid User PIN has been entered.

12.2.7 Technical specifications

PIN code keypad	
Batteries:	2 x 3 V lithium, type CR 2032
Dimensions in mm:	96 x 96 x 14
Protection class:	IP65
Operating temperature:	-20 °C to +50 □
Signal elements:	Green LED + audible signals

12.2.8 Declaration of Conformity

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

12.3 SmartBridge manual

12.3.1 General information

NOTICE Check the order code on the packaging to ensure that you have used the right router.

Manual
MobileKey Web-App

System3060 / WaveNet: WNM.RN2.ER.IO

RouterNode 2 can be used as a WaveNet router in System 3060. This allows corresponding locking components to be networked with one another. RouterNode 2 also offers the option of connecting inputs and outputs.

RouterNode 2 may only be used for this designated purpose in a SimonsVoss wireless network.

MobileKey: MK.SMARTBRIDGE.ER

With MobileKey, the SmartBridge can be used as an access point for networking locking devices.

The SmartBridge may only be used for this designated purpose in a MobileKey system.

12.3.2 Safety instructions

⚠ CAUTION

Access through a door may be denied if components are installed or programmed incorrectly. SimonsVoss Technologies GmbH is not liable for the consequences of incorrect installation, such as denied access to injured persons or those at risk, physical damage or any other losses.

⚠ CAUTION

People who have electronic, medical implants such as pacemakers and hearing aids must maintain a minimum distance of 30 cm between the implant and network components and should be expressly informed of this requirement. In the interests of safety, people wearing electronic implants should seek medical advice regarding the potential hazards of radio components (868/915 MHz).

⚠ CAUTION

The housing may not be opened under voltage while in operation! Always disconnect from the power supply (mains lead or network cable in the case of PoE operation) before opening the housing.

⚠ CAUTION

During PEO operation (power supply over ethernet), the temperature of the circuit board can be very high! Let the router cool down before you open the housing.

NOTICE

SimonsVoss Technologies GmbH reserves the right to modify the product without prior notification. As a result, the descriptions and images in this manual may differ from the latest version of the product or software. The German version of this manual takes precedence in cases of doubt. Errors and spelling mistakes excepted.

Manual
MobileKey Web-App

NOTICE

You will find more information about products in the SimonsVoss online at: www.simons-voss.com

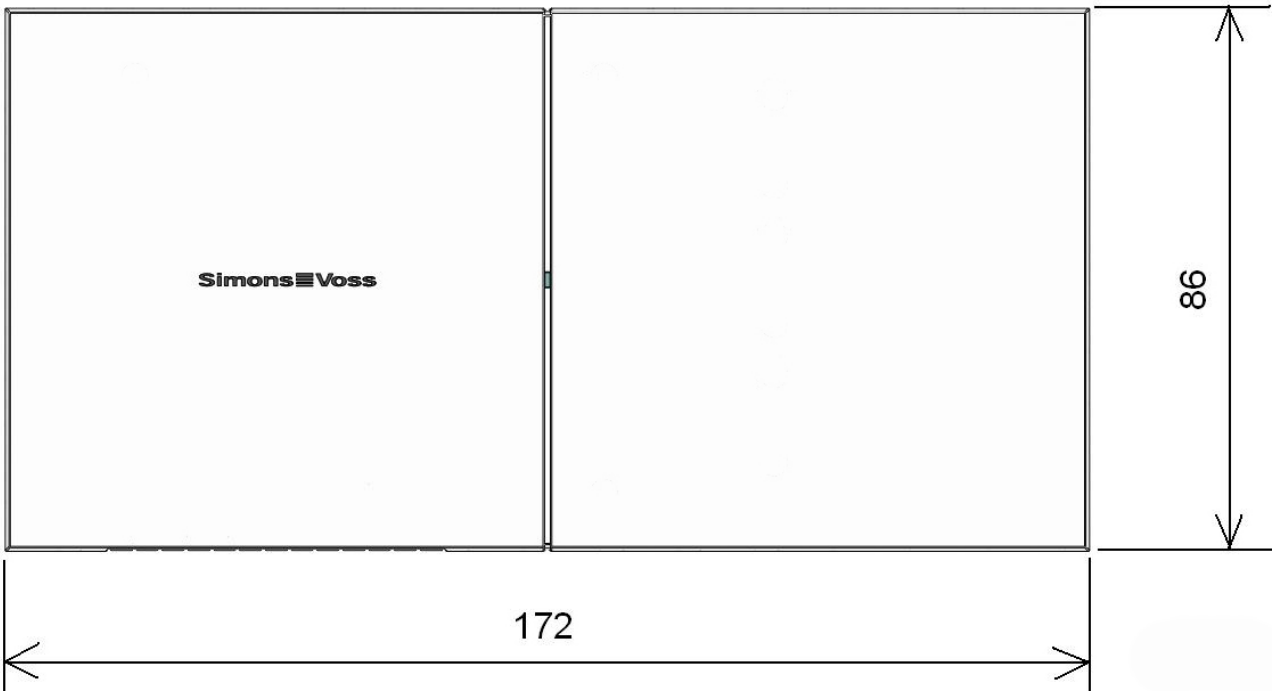
You can find more information about MobileKey online at: www.my-mobilekey.com

NOTICE

Read all manuals for the individual SimonsVoss components carefully.

12.3.3 Housing

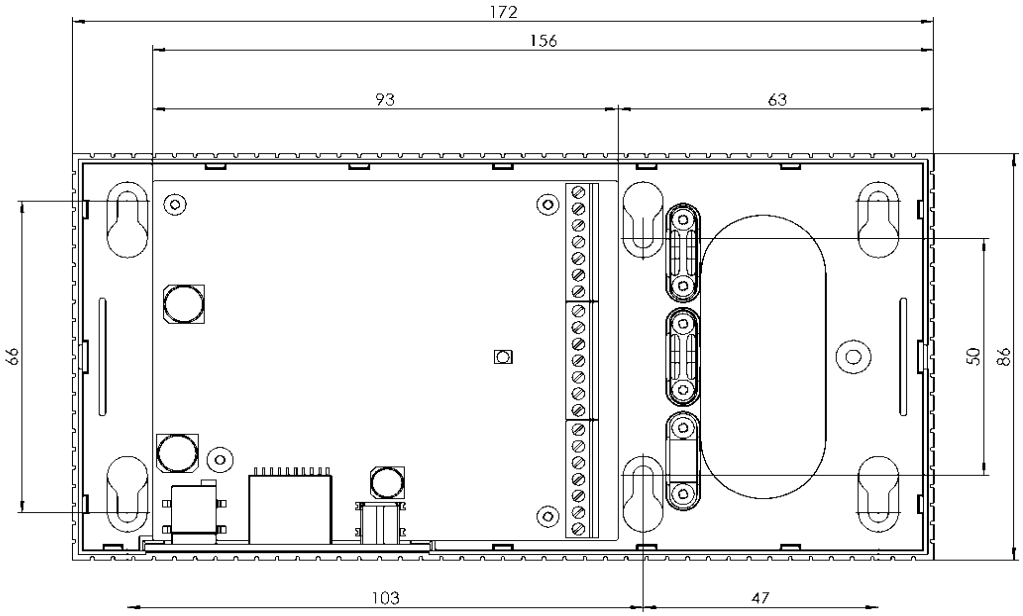
12.3.3.1 Images and dimensions



(dimensions in mm)

Manual
MobileKey Web-App

12.3.3.2 Dimensions of lower housing shell



12.3.3.3 Opening the housing lid

You do not need a tool to open the upper housing section. Apply slight pressure to the centre of the base plate on the left- or right-hand side and then you can remove the upper section.

12.3.4 Surface installation of wiring

Carefully separate the ribs on the lower housing shell from one another with a saw and move the web up and down until it breaks off. Remove any sharp edges with a file.

Manual
MobileKey Web-App

12.3.5 Configuration of IPsettings

You can use the SimonsVoss OAM tool (Ethernet operations, administration and maintenance tool) to make the IPsettings. The SimonsVoss OAM tool is available for download free of charge at www.simons-voss.com.

NOTICE

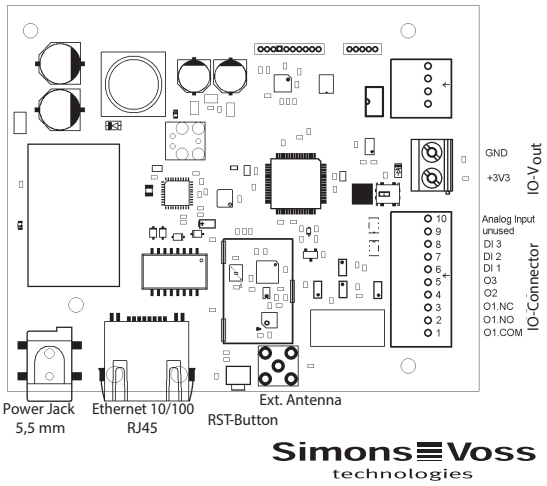
Standard settings:

IP address: 192,168,100,100

User name: SimonsVoss | Password: SimonsVoss

12.3.6 System connections

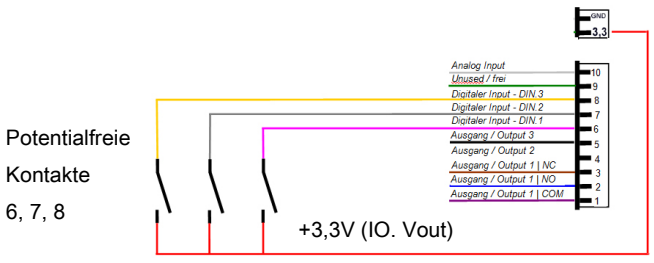
Inputs and outputs can only be connected with RouterNode2 (WNM.RN2.ER.IO).



12.3.7 IO connector wiring

Inputs and outputs can only be connected with RouterNode2 (WNM.RN2.ER.IO).

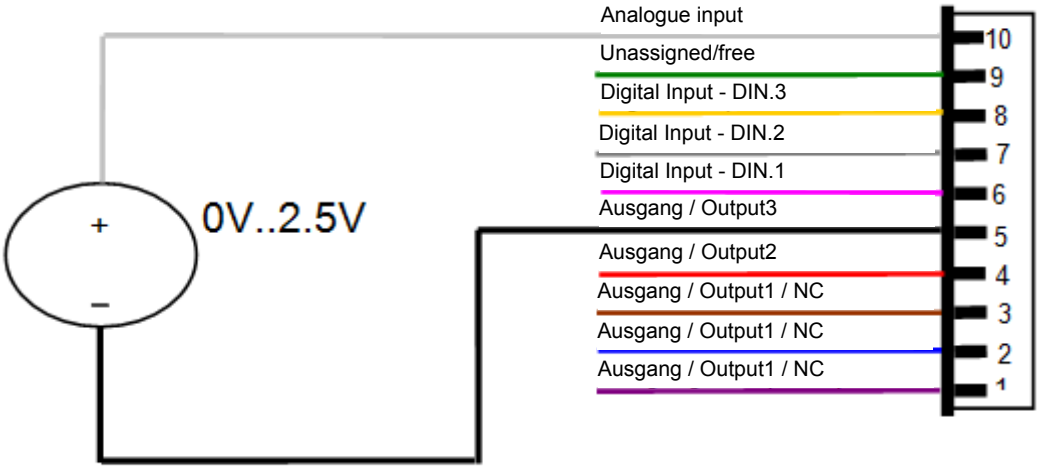
Simple contact analysis



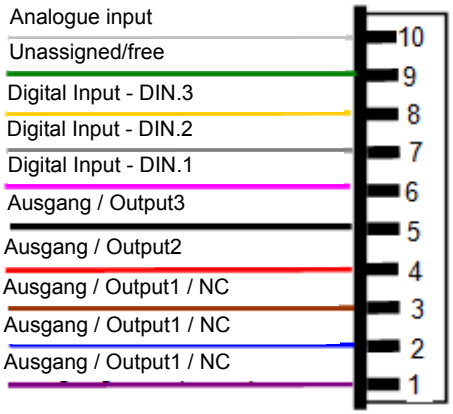
Manual
MobileKey Web-App

Wiring for digital input (DIN 1-3): to analyse/wire isolated contacts (relay, reed contacts). Opening external contacts can change inputs to carry out certain functions.

Analogue input wiring



Relay contact wiring (Output 1)



Output 1 (isolated relay output)

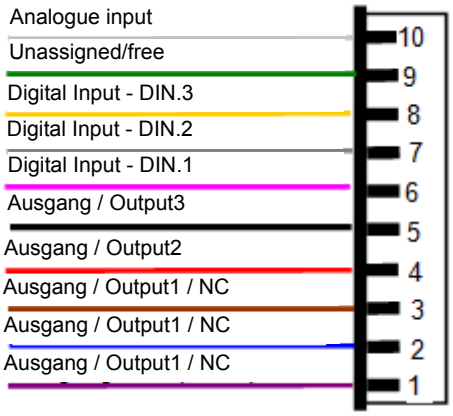
1 --> Common

2 --> Normally open

3 --> Normally closed

Manual
MobileKey Web-App

Wiring for Outputs 2/3



Output 2/3

2 --> Ground contact

3 --> Ground contact

The user has three open drain outputs at their disposal for use. These may be exposed to a maximum current of 200 mA each. We recommend using a recovery diode, such as a 1N4148, when connecting larger inductances. The router's earth must be connected to the system earth without fail. Maximum line length of the IO wiring: 30 m. Applies to DIN 1-3 + Output 2/3

Item	Explanation
Power jack (5.5 mm)	Jack plug from external source, 9-24 VDC, polarity-independent
Circuit board dimensions (L x W)	93 x 76 mm (L x W)
RJ45 Ethernet 10/100	Ethernet interface with PoE 802.3af
RST button	Reset button accessible from outside; can be tripped using paper clip or similar

IO connector	Explanation
1. O1.COM	Output 1: C-contact relay (C = common), isolated
2. O1.NO	Output 1: NO-contact relay (normally open)
3. O1.NC	Output 1: NC-contact relay (normally closed)
4. O2	Output 2: Open collector
5. O3	Output 3: Open collector
6. DI 1	Digital Input 1
7. DI 2	Digital Input 2

Manual
MobileKey Web-App

8. DI 3	Digital Input 3
9. Not in use	Not in use
10. Analogue input	Input for analogue input signals

Item	**Explanation**
IO.Vout	IO connector for power supply
+3.3V	Positive contact max. 3.3 V; can be used as an input signal for DI1-3
GND	Negative contact

Item	**Explanation**
RS485	Not in use
V in	Power supply from external source 9-24 VDC
GND	Negative contact
A	Data cable, max. 900 m
B	Data cable, max. 900 m

12.3.8 Resetting configuration

Reset locking system configuration

All locking system settings will be reset.

1. Disconnect power supply *(remove mains plug)*.
2. Wait 20 seconds.
3. Press reset button and hold pressed down.
4. Reconnect to power supply *(connect the mains plug)*.
5. Release reset button after 1 second.
6. The configuration has now been fully reset *(default)*.

Reset IP configuration

All IP configurations (IP address, DHCP settings and host name) are reset to the factory settings [▶ 72].

1. Disconnect power supply *(remove mains plug)*.
2. Wait 20 seconds.
3. Press reset button and hold pressed down.
4. Reconnect to power supply *(connect the mains plug)*.
5. Release reset button after 5 seconds.
6. The configuration has now been fully reset *(default)*.

12.3.8.1 Reset locking system configuration

All locking system settings will be reset.

1. Disconnect power supply *(remove mains plug)*.

Manual
MobileKey Web-App

2. Wait 20 seconds.
3. Press reset button and hold pressed down.
4. Reconnect to power supply *(connect the mains plug)*.
5. Release reset button after 1 second.
6. The configuration has now been fully reset *(default)*.

12.3.8.2 Reset IP configuration

All IP configurations (IP address, DHCP settings and host name) are reset to Factory settings [▶ 72] .

1. Disconnect power supply *(remove mains plug)*.
2. Wait 20 seconds.
3. Press reset button and hold pressed down.
4. Reconnect to power supply *(connect the mains plug)*.
5. Release reset button after 5 seconds.
6. The configuration has now been fully reset *(default)*.

12.3.9 Technical specifications

General information	
Housing	ABS plastic, UV-stable,
Dimensions (L x W x H)	172 x 86 x 33 mm (L x W x H)
Frequency range	868.xx-870 MHz
Colour	9/118645, same as RAL 9016 (Traffic white)
External power supply	Regulated mains adapter, 9-32 VDC, jack plug, round, 5.5 mm
PoE	Power-over-Ethernet, supports IEEE 802.3af
Output	Max. 3 VA
Transmitting capacity	10 dBm (about 10 mW) to the antenna socket
Wiring to device	Surface or flush mount possible
Strain relief clamp	3 x in housing
LED	In centre of housing
Wall mount	Housing can be mounted in horizontal or vertical position. Do not install on metal. Keep away from electric or magnetic sources of interference.

Power supply: The Router (RouterNode 2 or SmartBridge) can draw the required power supply via the network (PoE). If there is no PoE available, you can connect an additional mains adapter.

Power supply

Manual
MobileKey Web-App

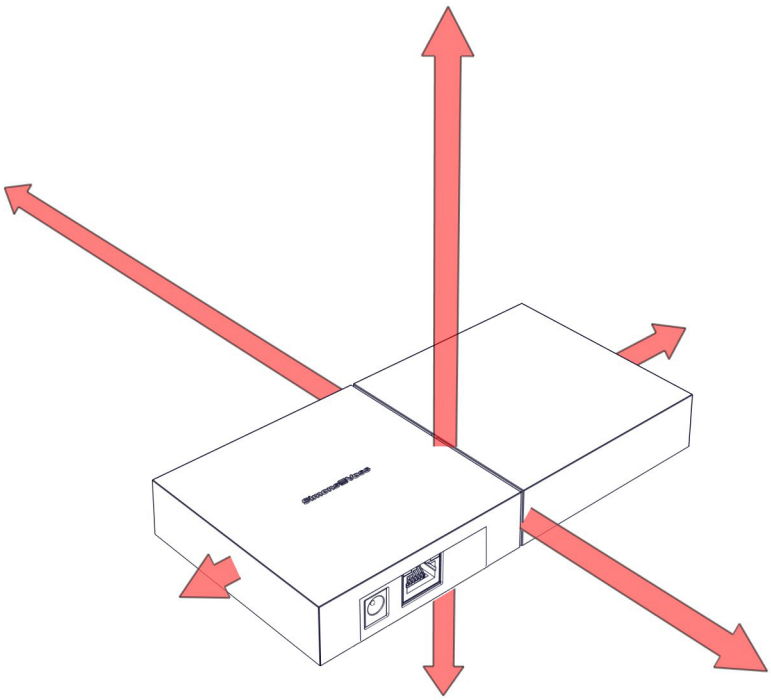
External power supply (mains adapter)	Input voltage: 9 V DC min., 32 V DC max.; (min. 3 W) Input current: depends on the input voltage (350 mA @ 8V) Polarity-dependent: no
PoE (power-over-Ethernet)	IEEE802.3af, floating, V_{in}:36 V to 57 V, P_{out} max. 10 W
Power outputs	1 x 3.0 – 3.3 V at 200 mA max.
Environment	
Temperature	Operational: -10°C to +55°C Storage: 0°C to +30°C
Humidity	Max. 90%, non-condensing
Environmental Class	IP20
Interfaces	
TCP/IP	10T/100T, HP Auto_MDIX, DHCP client, IPv4 TCP service: 1x at Port 2101 UDP service: 1x for Digi-Scan DHCP: on WebServer: enable Connector: RJ45
Frequency	WaveNet 868-870 MHz, 10 mW max. (10 dBm)
Signalling	
LED	A three-colour LED: red, green, blue (in centre of housing)
Programming	
Interfaces	Via TCP/IP
Memory	1 MB, internal
Relay for Output 1 *(WNM.RN2.ER.IO only)*	
Quantity	1 x
Operating mode	Changeover contact
External output via relay contact	1 x C, 1 x NO, 1 x NC. Max. switching voltage: 30 V DC/24 V AC (ohmic load) Max. switching current: 1A (ohmic load)
Digital inputs *(WNM.RN2.ER.IO only)*	
Quantity	3 x
Input voltage	Low: 0 to 0.5 V / high: 2 V to 3.3 V max

Manual
MobileKey Web-App

Ext. Contact	Isolated contact can be connected between output (I1, I2, I3) and I_+
Digital outputs *(WNM.RN2.ER.IO only)*	
Quantity	2 x
Type	Open collector
Switching voltage	12 V DC/100mA (max. ohmic load)
Power supply	A pull-up resistor (about 1 KOhm) can be connected between each output and output$_+$ (V_{out} = V_{in} – 1V)
Analogue inputs *(WNM.RN2.ER.IO only)*	
Quantity	1 x
Resolution	12 bit
Input voltage	0 to 3.3V
External antennas	
Ext. Antenna	You can order an external antenna from SimonsVoss Technologies GmbH to extend the read range. This antenna is plugged directly into the circuit board.

12.3.10 Antenna

12.3.10.1 Antenna emission (internal antenna)



12.3.10.2 External antenna ANTENNA.EXT.868

The external antenna ANTENNA.EXT.868 is available as an optional accessory.

The external antenna ANTENNA.EXT.868 is designed for outdoor use, allowing the router to be installed within a protected area, yet still reach LockNodes in the outdoor area. The antenna is connected via a connection to the router circuit board.

No further configuration is required on the router or in the software. The internal antenna is not deactivated when the external antenna is connected.

The antenna has a magnetic base and is supplied with a wall mount, wall plug and screw. The wall mount is used to fasten the antenna's magnetic foot to the non-metallic support surface.

Manual
MobileKey Web-App

12.3.10.3 Technical specifications for ANTENNA.EXT.868 (available as option)

Impedance	50 Ohm
Polarisation	Linear
Gain (max.)	2.2 dBi
VSWR	<3:1
Output	25W
Operating temperature	-40°C to +85°C
Height (max.)	71.95mm
Diameter (max.)	30.85mm
Cable length	about 5 m

12.3.11 Power supply

Power supply: the device can draw the required power supply via the network (PoE). If there is no PoE available in the network, you can connect an additional mains adapter *(9 V to 32 V DC; at least 3 W)*.

12.3.12 Declaration of conformity

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

12.3.13 Help & Contact

Instruction manuals

You will find detailed information on operation and configuration online under INFOCENTER > DOWNLOADS on our homepage at www.simons-voss.de

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.

hotline@simons-voss.com

FAQs

You will find information and help for SimonsVoss products in the FAQ section
www.simons-voss.de
in INFO CENTRE > FAQ SECTION

SimonsVoss Technologies GmbH, Feringastrasse 4, 85774 Unterföhring, Germany

Manual
MobileKey Web-App

12.4 SmartRelay manual

12.4.1 Intended use

SimonsVoss SmartRelay is an electronic switch which can be activated with suitable ID media *such as transponders*. SmartRelay administration varies depending on the SmartRelay in question:

	ADMINISTRATION	PROGRAMMING
3063	LSM Basic, Business or Professional	SMART.CD
	LSM Starter	CD.STARTER *or* *SMART.CD*
MobileKey	Web application	MK.CD.STARTER

Some SmartRelays can be optionally programmed via internal LockNodes with suitable routers. However, a programming device should always be used to perform initial programming.

SmartRelays may only be used for the purposes described in this manual. No other use is permitted as it may cause damage to the SmartRelay.

NOTICE SmartRelays should always be programmed before installation and connection

12.4.2 Safety instructions

Warning:

⚠ WARNING Access through a door may be denied if locking devices are installed or programmed incorrectly. SimonsVoss Technologies GmbH is not liable for consequences of incorrect installation, such as denied access to injured persons, physical damage or any other losses.

⚠ WARNING The batteries used in SmartRelay may pose a fire or burn hazard if handled incorrectly. Do **not** recharge, open, heat or burn these batteries. Do not short-circuit batteries.

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

NOTICE SmartRelay may only be used for its intended purpose. No other use is permitted.

Manual
MobileKey Web-App

NOTICE Specialist knowledge in door mechanics, door approvals, electronic system installation and the use of SimonsVoss software is required when installing a SimonsVoss SmartRelay. Only trained specialists may install the cylinder.

NOTICE If SmartRelays are placed in storage for longer than a week, the backup battery is to be removed.

NOTICE SmartRelays must be installed in compliance with the ESD (electrostatic discharge) directive. You should particularly ensure that you do not touch the circuit boards and their integrated circuits.

NOTICE You **must** perform a functions test without fail after installing SmartRelay or replacing its batteries.

NOTICE We reserve the right to make modifications or further technical developments.

NOTICE This documentation has been compiled in accordance with the best knowledge available to us. However, errors cannot be ruled out. No liability is accepted in such cases.

NOTICE Should there be differences in the content of other language versions of this documentation, the German version applies in cases of doubt.

NOTICE You must follow all instructions precisely when connecting and installing SmartRelay. The person installing the system should hand these instructions as well as any maintenance instructions over to the user.

NOTICE Only trained specialists may replace the battery.

NOTICE Dispose of old and used batteries in the proper manner and store them out of children's reach.

NOTICE Do not touch the contacts on the new batteries with your hands when replacing the old ones. Use clean gloves free of fat or grease to handle the battery.

Manual
MobileKey Web-App

NOTICE

Only use batteries which have been **approved** by SimonsVoss.

NOTICE

You may **damage** SmartRelay if you reverse the polarity.

12.4.3 General information

12.4.3.1 Versions

SmartRelays are available in an extensive variety of versions for different product lines. Carefully check which SmartRelay is the right one for your use before placing an order.

SREL *(black)*		**SREL2** *(white)*	
G1		**G2**	
SREL	SREL.G2	SREL.G2.W	Basic version of SmartRelay 3063.
SREL.ZK	SREL.ZK.G2	SREL.ZK.G2.W	As the basic version of SmartRelay 3063, plus access control and time zone control.
SREL.ADV			As the access control version of SmartRelay 3063, but with additional functions for issuing.
		SREL2.G2.W	Basic version of SmartRelay2 3063.
		SREL2.ZK.G2.W	As the basic version of SmartRelay2 3063, plus access control and time zone control.
		SREL2.ZK.MH. G2.W	As the access control version of SmartRelay2 3063, but also with support for an internal MIFARE® card reader and connection options for a maximum of three external MIFARE® card readers.

	SREL	SREL .ZK	SREL .ADV
Authorisation for up to 8,184 transponders	X	X	X

Manual
MobileKey Web-App

Authorisation for up to 64,000 transponders				
Access control			X	X
Extended connection options				X
Mifare & Desfire card support				
Connection option for external card readers				

	SREL G2	SREL ZK.G2	SREL G2.W	SREL ZK.G2.W
Authorisation for up to 8,184 transponders				
Authorisation for up to 64,000 transponders	X	X	X	X
Access control		X		X
Extended connection options				
Mifare & Desfire card support				
Connection option for external card readers				

	SREL2 G2.W	SREL2 ZK.G2.W	SREL2 ZK.MH.G2.W
Authorisation for up to 8,184 transponders			
Authorisation for up to 64,000 transponders	X	X	X
Access control		X	X
Extended connection options			
Mifare & Desfire card support			X
Connection option for external card readers			X

– **SmartRelay**

  The SREL provides simple yes/no authorisation for a maximum of 8,184 different transponders.

– **SmartRelay ZK**

  Similar to the basic version (SREL), but with the option of access event logging connected separately for the last 1,024 accesses (firmware version 4.0.01.15 and higher) with date and time, or day-time zones for up to five user groups and automatic locking and unlocking.

– **SmartRelay Advanced version**

  Similar to the ZK version but with the following additional functions:

Manual MobileKey Web-App

- Connection for external modules via a three-wire bus.
- Connection to an external antenna.
- Connections for serial ports to external time-and-attendance terminals or access control readers.
- Connection for external LED or buzzer.

– **SmartRelay 2**

The SREL2.G2.W is basically used with transponders, i.e. as purely "active" components. There is also the option of using a CompactReader and thus operating the SREL2 with Mifare Classic/ DERFire® cards. This SmartRelay provides simple yes/no authorisation for a maximum of 64,000 different transponders.

– **SmartRelay 2 ZK**

The same as the basic version (SREL2.G2), but with the option of access event logging with date and time connected separately for the last 1,024 accesses, or day time zones for up to 100 user groups and automatic locking and unlocking (time-controlled switch-over). This version can also be used as a gateway in a virtual network.

– **SmartRelay 2 MH**

As the ZK version. Two external card readers (SC.M.E.G2) and an internal card reader (SC.M.I.G2) can be connected to this version. Mifare Classic/DERFire® cards can be operated on this SREL2.

12.4.3.2 Accessories

SmartRelay can be combined with a variety of accessories. Carefully check which combinations can be used before placing an order.

Accessories for SmartRelay 3063 G1

	SREL	SREL.ZK	SREL.ADV
MOD.SOM8			X
SREL.AV			X
SREL.BAT	X	X	X

Accessories for SmartRelay 3063 G2

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

Accessories for SmartRelay 3063 *(G2)*

	SREL2.G2.W	SREL2.ZK.G2.W	SREL2.ZK.MH.G2.W
SREL.AV			X

WNM.LNI.SREL2.G2	X	X	X
SC.M.I.G2			X
SC.M.E.G2.W			X
SREL2.COVER1	X	X	X

– **SC.M.E.G2.W** *(Mifare smart card, external, G2 white)*

  A maximum of two external card readers (SC.M.E.G2.W) and an internal card reader (SC.M.I.G2) can be connected to a SREL2.ZK.MH.G2.W or SREL2.ZK.MH.G2.W.WP. If two external card readers are connected to an SREL2, then a dip switch placed at the "on" position must be connected to an external card reader. The dip switch is found on the right-hand side beneath the 26-pin plug connector on the card reader.

  The cabling type used to wire components should be CAT5 (FTP) or a higher quality. Shielded control cabling may also be used. Cable length: max. 10 m. An own power supply and own wiring should be installed if the cable line length is > 3m for the external card reader.

– **SC.M.I.G2** *(Mifare smart card, internal G2)*

  The internal card reader is plugged directly into the SREL2.

– **SmartRelay 2 WP version**

  Weatherproof design. This option is also available for all SREL2s. You must seal the bushing yourself under your own responsibility. We recommend using suitable materials such as silicon or other resistant sealing materials. The housing features an IP65 design.

12.4.3.3 Power supply

A stable power supply is required to operate Digital SmartRelay 3063. Mains adapters are not included in the delivery package.

Some SmartRelays can be operated using batteries (SREL.BAT) as an option. **No additional power supply** may be connected in such cases.

	Direct current	Alternative current
SREL	5 V-24 V (max. 15 W)	12 V (max. 15 W)
SREL2	9V-24 V (max. 15 W)	Not possible.

NOTICE

Do not use switched-mode power supplies near SmartRelays.

Manual
MobileKey Web-App

12.4.3.4 Determining installation position

The transponder transmission range for SmartRelay (read range) is a max. of 1.5 m, but may be reduced in environments containing metals, especially in magnetic fields or where aluminium is present.

Ideally, you should perform a read range test with an authorised transponder and a battery-operated SmartRelay.

12.4.3.5 More information

- All cabling used to connect SmartRelay should be type IY(ST)Y ....x0.6 – twisted pair, shielded cable – and should not exceed 100m in length. Power losses should be taken into account when dimensioning the power supply.
- The technical data regarding inputs and outputs are to be taken into account (see Technical Data).
- All cabling must be installed and connected as per VDE regulations (VDE = German Association of Electro-technology, Electronics & Information Technology).

12.4.4 Initial operation

Check

1. Unpack SmartRelay and check for any damage.
2. Connect SmartRelay to a power supply or a battery.
3. Activate the SmartRelay with a transponder and test whether the SmartRelay responds to activation in some way or other.

Programming

Programme the SmartRelay with the appropriate software, e.g. LSM Software for SmartRelay 3063. The SmartRelay must be connected to a power source for the programming process. You will find the details on programming in the LSM Software here: Configurations in the software [▶ 89]

Connection and installation

✓ The SmartRelay is not connected to any power source and is in a de-energised state.

1. Use backup battery: **The positive terminal on the 3V-CR1220 battery faces upwards in all SmartRelays.**
2. Connect all cables to their designated terminals on the SmartRelay (see Connections)
3. Switch on the power supply (connect the plug or battery if required).
4. Use an authorised transponder to test the programmed SmartRelay.
5. Install SmartRelay.

Manual
MobileKey Web-App

⇨ Remove the housing if you install in a flush-fitted masonry box. The SmartRelay circuit boards have two different sizes. Check whether the SmartRelay circuit board fits into its flush-fitted box **before** installation.

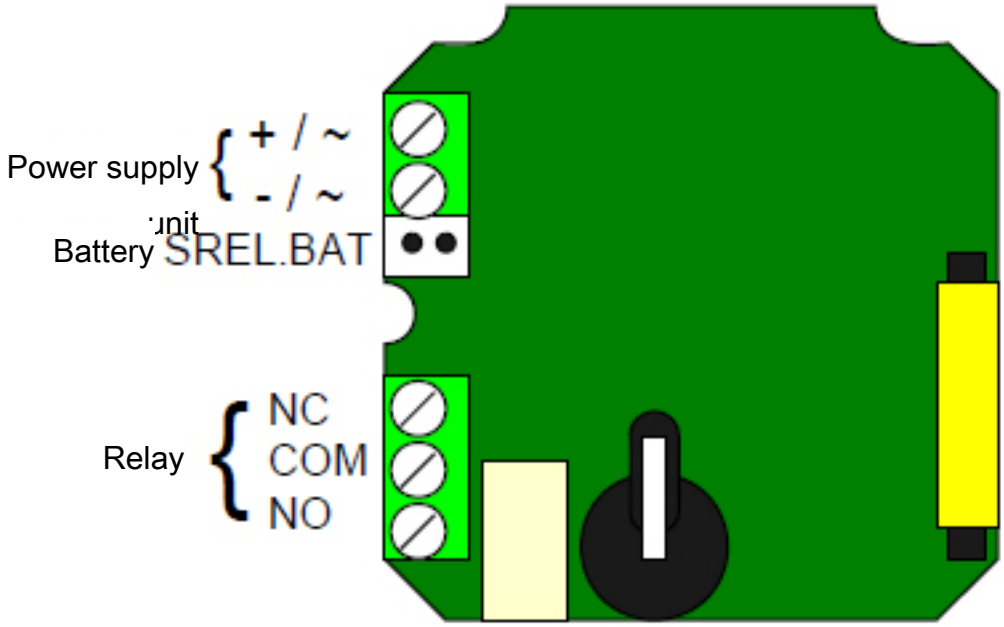
⇨ If mounted on the surface, the base plate can be used as a template for the drill holes (6 mm).

NOTICE

The backup battery must not be used if SmartRelay is powered by a battery (SREL.BAT).

12.4.5

12.4.5.1 SmartRelay (SREL)



NAME	SYMBOL	DESCRIPTION
Power supply unit	+	Either positive terminal when connected to a direct current (5 to 24 V DC) or one of the two alternative current connections (12 V AC)
Power supply unit	-	Either minus terminal when connected to a direct current (5 to 24 V DC) or the second alternative current connections (12 V AC)

Manual
MobileKey Web-App

Battery	Connector for a battery when operated without a power supply unit; order code for battery, including SREL.BAT connector
Relay NC	Normally closed contact in the relay changeover contact. This contact is closed against Relay COM when not connected
Relay COM	Common contact in the relay changeover contact. This contact is wired either against an NC relay (break contact) or against a NO relay (closing contact)
NO relay	Normally open contact in the relay changeover contact. This contact is closed against Relay COM when not connected

12.4.5.2 Notes on SREL2 connection

SREL2.G2 with three card interfaces

It is possible to operate the SREL2 with a total of 3 card interfaces at the same time (1 x internal and 2 x external). The dip switch **must** be set to 1 (ON) on the internal card interface for such operation.

External trigger for SREL2.G2

The SREL2 is triggered if a current of +3 to +24 Volt (DC) is added to F1 as a pulse. This configuration can be used to implement the OMRON function, for example.

External LED or buzzer to SREL2.G2

An external LED or buzzer can be connected to the F3 and PLUS (+) connections. The voltage at F3 and PLUS is the same as the supply voltage. If necessary, the voltage must thus be reduced by a suitable series resistor.

12.4.6 Configurations in the software

SmartRelays are very specific due to their hardware and can therefore only be operated in environments designated for them.

Item order code	Protocol generation	Software
SREL	G1: Type G1 or G2 + G1 locking systems only	LSM
SREL.ZK		
SREL.ADV		
SREL.G2	G2: Type G2 locking systems only	
SREL.ZK.G2		
SREL.G2.W		
SREL.ZK.G2.W		
SREL2.G2.W		
SREL2.ZK.G2.W		
SREL2.ZK.MH.G2.W		

Manual
MobileKey Web-App

MK.SREL2.ZK.G2.W MK.SREL2.LN.ZK.G2.W	MobileKey	MobileKey

12.4.6.1 LSM

The SmartRelay's settings can be adjusted in the "Configuration/Data" tab in the locking device's properties.

Locking device properties: Configuration/Data: SmartRelay (G1)

This tab is divided into two sides:

– The left side shows the target status of the locking device – i.e. the desired status configured in the LSM software.

– The right side shows the locking device's current status – i.e. the status which was last programmed.

The following features can be enabled **depending on the locking device type**:

– **Access control**

Only possible in SREL.ZK and SREL.ADV versions. The 1,024 most recent transponder transactions are logged with the date and time.

– **Time zone control**

Only possible in SREL.ZK and SREL.ADV versions. A time zone plan can be uploaded and the transponders are approved or blocked according to their time zone group.

– **Overlay**

Replacement transponders can overwrite their corresponding original transponders. The original transponder is blocked once the replacement transponder is used for the first time.

– **Flip flop**

Pulse mode (default setting) is switched off and the pulse duration no longer plays a role. When flip flop mode is activated, SmartRelay changes its status from on to off or vice versa each time it is activated using a transponder. This mode is ideal for switching lights, machines and other systems on and off.

Where applicable, you should ensure that mains adapters and electric strikes are suitable for continuous current operation in such an installation.

– **Repeater**

The SmartRelay receives a transponder signal, which it amplifies and forwards. This function allows SmartRelay to be used to bridge longer radio transmission paths. The distance to the next SmartRelay can be up to 2 m.

– **Time switch-over**

Manual
MobileKey Web-App

For SREL.ZK and SREL.ADV only. A time zone plan needs to be uploaded when the time switch-over is activated. This allows the locking cylinder to remain unlocked during the indicated times (in Group 5). During the day, the door can be used freely while only a transponder will open the door at night.

You should ensure that mains adapters and electric strikes are suitable for continuous current operation in such an installation

– **OMRON**

For SREL.ADV only. Many access control and time-and-attendance systems feature serial interfaces to connect card readers. A SmartRelay can also be connected via these interfaces, thus also allowing you to use SimonsVoss transponders in third-party systems.

Select this option on both the SmartRelay and the cylinder if you wish the SmartRelay to transmit transponder data to a third-party system and a remote opening command to be sent from SmartRelay to a cylinder after clearance by the third-party system.

Set the type of external system under 'Interfaces'. Click on the "Extended configuration" button to do so.

Some settings can be specified using the "Extended configuration" button:

– **Pulse length**

This is where you indicate the number of seconds for the duration of switch pulse. The value can be set at 0.1 to 25.5 seconds. If you enter 3 seconds, for example, an electric strike is released for 3 seconds before it locks again.

– **Limited range**

If you select this option, the reader range from the transponder to the SmartRelay is reduced from 1.5 m to about 0.4 m. This option can be used when several SmartRelays are in close proximity to one another and individual transponders are authorised for use on several SmartRelays, for example.

– **Logging unauthorised attempted access events**

For SREL.ZK and SREL.ADV only: Normally, only authorised transponder operations are logged. You need to select this option if you also wish to record attempts to open the door with non-authorised transponders.

– **Number of extension modules**

This is where you indicate the number of external modules connected to the SmartRelay. These modules are connected to the terminals RS-485 C OM, RS-485 A and RS-485 B.

– **Interface**

For SREL.ADV only: You can enter the type of card reader here which the SmartRelay is to simulate for operation as a serial interface.

Manual
MobileKey Web-App

The following options are available:

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

– **No audible programming acknowledgement signals**

For SREL.ADV only: You should check this field if you do not want audible programming confirmation signals to be emitted from a connected buzzer or beeper while you are programming SmartRelay.

– **External LED/external beeper**

For SREL.ADV only: This indicates which external component group is connected. In flip flop mode, SmartRelay emits a permanent signal when switched on if there is an external LED; in the case of a beeper, an audible signal is only emitted when there is a change of status.

– **Internal/external antennas**

For SREL.ADV only

- **Auto-detection**

  If an external antenna is connected, this is the one which is used. SmartRelay switches off the internal antenna in such cases. If no external antenna is connected (standard case), SmartRelay functions with the internal antenna.

- **Both active**

  SmartRelay is able to use both antennas to verify transponder bookings.

Locking device properties: Configuration/Data: SmartRelay (G2)

This tab is divided into two sides:

– The left side shows the target status of the locking device – i.e. the desired status configured in the LSM software.

– The right side shows the locking device's current status – i.e. the status which was last programmed.

The following features can be enabled **depending on the locking device type**:

– **Pulse length**

Manual
MobileKey Web-App

This is where you indicate the number of seconds for the duration of switch pulse. The value can be set at 0.1 to 25.5 seconds. If you enter 3 seconds, for example, an electric strike is released for 3 seconds before it locks again.

– **Access control**

ZK and ADV possible. The most recent transponder transactions are logged with the date and time.

– **Time zone control**

Only possible in ZK and ADV versions. A time zone plan can be uploaded and the transponders are approved or blocked according to their time zone group.

– **Logging unauthorised attempted access events**

For ZK and ADV only: Normally, only authorised transponder operations are logged. You need to select this option if you also wish to record attempts to open the door with non-authorised transponders.

– **Gateway**

SmartRelay can be used as a gateway.

– **Flip flop**

Pulse mode (default setting) is switched off and the pulse duration no longer plays a role. When flip flop mode is activated, SmartRelay changes its status from on to off or vice versa each time it is activated using a transponder. This mode is ideal for switching lights, machines and other systems on and off.

Where applicable, you should ensure that mains adapters and electric strikes are suitable for continuous current operation in such an installation.

– **Internal antenna always on**

Even if an external antenna is connected, the internal antenna is still used at the same time.

– **Close range mode (for internal antennas only)**

Close range mode is activated.

– **Time switch-over**

For ZK and ADV only. A time zone plan needs to be uploaded when the time switch-over is activated. This allows the locking cylinder to remain unlocked during the indicated times (in Group 5). During the day, the door can be used freely while only a transponder will open the door at night.

You should ensure that mains adapters and electric strikes are suitable for continuous current operation in such an installation

Some settings can be specified using the "Extended configuration" button:

Manual
MobileKey Web-App

– **Interface**

You can enter the type of card reader here which the SmartRelay is to simulate for operation as a serial interface.

The following options are available:

– Wiegand, 33 bit
– Wiegand, 26 bit
– Primion
– Siemens
– Kaba Benzing
– Gantner Legic
– Isgus

– **External LED/external beeper**

For SREL.ADV only: This indicates which external component group is connected. In flip flop mode, SmartRelay emits a permanent signal when switched on if there is an external LED; in the case of a beeper, an audible signal is only emitted when there is a change of status.

– **Invert outputs**

You can use these settings to invert the relay output.

12.4.6.2 MobileKey

A (MK) SmartRelay can be quickly configured in the MobileKey web app. As a general rule, distinction is only made between an opening interval and a permanent opening (flip-flop). A LockNode can be configured as an option to connect the SmartRelay via a SmartBridge.

12.4.7 Signalling

SREL

– LED lights up or flashes green: ID medium is authorised and the SREL activates.
– No response from the LED: ID medium rejected or not recognised.

SREL2

– LED lights up or flashes blue: ID medium is authorised and the SREL2 activates.
– LED flashes red: ID medium rejected.

12.4.8 Maintenance

12.4.8.1 Battery warning and battery replacement when SREL.BAT is used

A SmartRelay can emit a battery warning as follows when the battery capacity is depleted:

– **SREL, SREL.ZK and SREL.ADV**

- Inside LED flashes 8x each time a transponder is used and before the SmartRelay switches.
- This LED should be visible from the outside in the case of battery-powered operation.

– **SREL.ADV only**

- External LED flashes 8x or external buzzer beeps 8x each time a transponder is used.

NOTICE

Around another 100 activations are possible after a battery warning. Transponder battery must be replaced as soon as possible.

12.4.8.2 Backup battery

A discharged backup battery may lead to the internal clock stopping in SmartRelays. We therefore recommend checking the time on the clock at regular intervals. A backup battery will last for about ten years if the power supply to the SmartRelay is not interrupted. This battery should be replaced on a periodical basis if SmartRelay draws on the backup battery at regular intervals due to frequent power failures.

NOTICE

The backup battery must not be used if SmartRelay is powered by a battery (SREL.BAT).

12.4.9 Technical specifications

12.4.9.1 Technical data for SREL

Housing made of black plastic: dimensions l x w x h	72 x 57 x 25.5 mm
Protection rating	IP20, not tested for outside use
Temperature	When operating: -22°C to 55°C In storage: 0 °C to 40 °C
Humidity	< 95% without condensation
Circuit board dimensions l x w x h	50 x 50 x 14 mm
Mains voltage	12 V AC or 5-24 V DC (no reverse voltage protection)
Power limitation	Mains adapter must be limited to 15 VA
Standby current	< 5 mA
Max. current	< 100 mA
Pulse duration programmable	0.1 to 25.5 seconds
Output relay type	Changeover contact

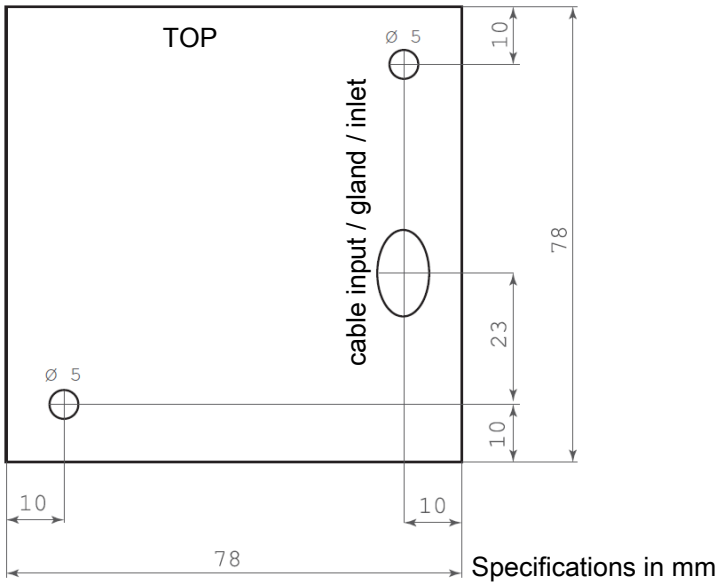
Output relay continuous current	Max. 1.0 A
Output relay switch-on current	Max. 2.0 A
Output relay switching voltage	Max. 24 V
Output relay switching power	10^6 activations at 30 VA
Multi-function connections F1, F2, F3	Max. 24 V DC, max. 50 mA
Vibrations	15 G for 11 ms, 6 shocks as per IEC 68-2-27 Not approved for use when subject to permanent vibrations

12.4.9.2 Technical specifications for SREL2

Housing made of white plastic: Dimensions LxWxH Base plate semi-transparent	About 78 x 78 x 19 mm
Protection rating	IP20, not tested for outside use WP version: IP65
Temperature	When operating: -22 °C to 55 °C In storage: 0 °C to 40 °C
Humidity	< 95% without condensation
Circuit board dimensions l x w x h	50 x 50 x 14 mm
Mains voltage	9-24 V DC
Power limitation	Mains adapter must be limited to 15 VA
Standby current	< 100 mA
Max. current	< 300 mA
Pulse duration programmable	0.1 to 25.5 seconds
Output relay type	NO contact
Output relay continuous current	Max. 1.0 A
Output relay switch-on current	Max. 2.0 A
Output relay switching voltage	Max. 24 V
Output relay switching power	10^6 activations at 30 VA
Multi-function connections F1, F2, F3	Max. 24 V DC, max. 50 mA
Vibrations	15 G for 11 ms, 6 shocks as per IEC 68-2-27 Not approved for use when subject to permanent vibrations

Manual
MobileKey Web-App

12.4.9.3 SREL2 drilling template, white



12.5

12.5.1 Intended use

The USB config device is a compact programming device which is used to programme active SimonsVoss components *such as transponders or locking cylinders* using a Windows-based computer.

– **CD.STARTER.G2**

  Used to programme System 3060 locking components with LSM STARTER.

– **MK.CD.STARTER.G2**

  Used to programme MobileKey locking components with the web application. The USB config device can also be operated on Android devices (with an OTG function).

12.5.2 Safety instructions

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

NOTICE Avoid placing in direct sunlight.

Manual
MobileKey Web-App

NOTICE Keep away from sources of magnetic interference.

12.5.3 Included in supplied package

- CD.Starter Config Device
- USB cable connector A / socket A
- Quick installation guide
- Driver CD

12.5.4 Initial operation

Install the associated driver by executing the set-up file. The set-up file is located in the "System" subdirectory on the LSM Starter CD and distinguishes between a driver for 32-bit and 64-bit Windows operating systems. Follow the instructions in the installation wizard. You can also find the driver under Downloads on the SimonsVoss website. Once the driver is installed, the programming device is ready for use.

12.5.5 Programming

Please observe the system manual for your system:

- LSM Starter: under "Infocenter/Downloads/Software" at http://www.simons-voss.com/
- MobileKey: under "Infocenter/Downloads" at http://www.my-mobilekey.com/

12.5.5.1 Programming with LSM STARTER

The current version of LSM 3.2 or higher must be installed on your computer. Connect the USB programmer. Place the components to be programmed at a distance of 10-30 cm from the config device and implement the programming routines.

If you should receive an error message stating that no hardware has been found, first check that the USB programmer is connected properly and then verify whether the CD.Starter has been detected under 'Programming / Config device' in the software. If there is still an error message, remove the config device from the USB socket and plug it in again. The driver will then be reloaded.

12.5.5.2 Programming with MobileKey

Log on to the web application and select *"Menu/Programme"*. The programming app must be installed to programme with the web application. The set-up file is provided for download via a link.

Manual
MobileKey Web-App

If the programming app is already installed, you can launch it directly using the *"START APP"* button and then begin programming.

12.5.5.3 Programming distance

– The distance between the USB config device and active components, such as locking cylinders or transponders, should be about 20 cm.

– Ensure that no other active components are in the immediate surrounding area during the programming or read process (radius of about 1.5 m around the USB config device).

12.5.6 Technical specifications

Programming:	SimonsVoss Active Technology, 25kHz
LSM version:	LSM Starter LSM 3.2 SP1 or higher
Operating system:	Windows XP SP3 and higher
USB port:	USB type A, USB 2.0
Dimensions:	LxWxH 57(70)x19x13 mm
Read range:	10-30cm
Power supply:	via USB connector, no internal battery
Protection rating:	IP40
Temperature range:	-10 to +60°C
Humidity:	95% (non-condensing)