

30
60

System 3060

System description

18.08.2022

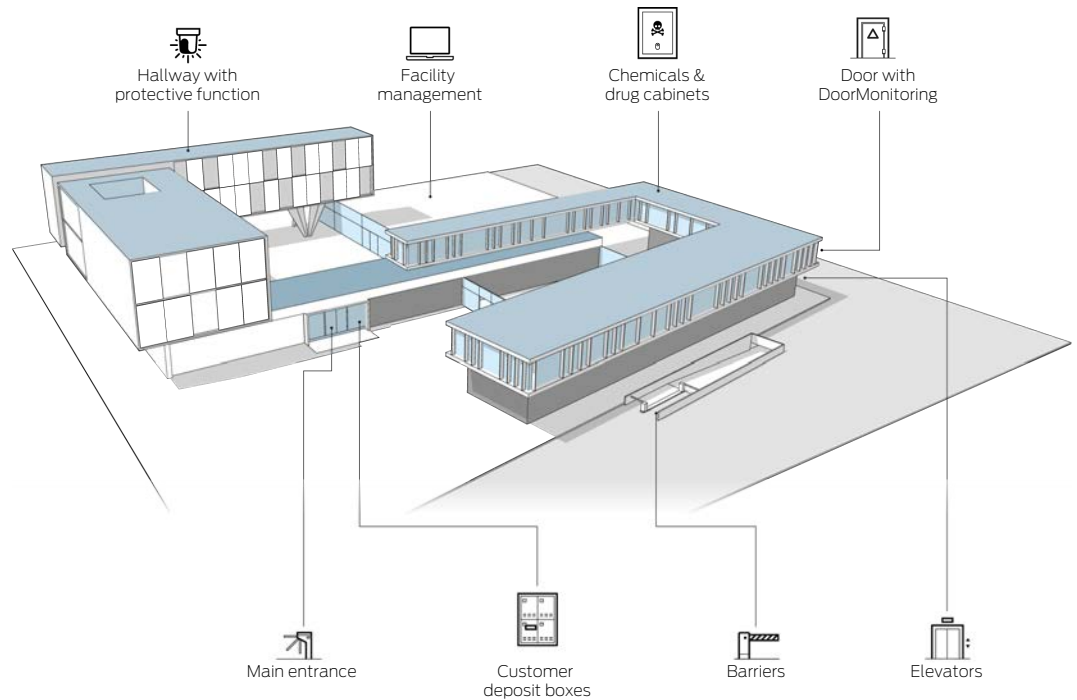
Simons Voss
technologies

Contents

1	General operation	3
2	Components	5
2.1	Software	5
2.1.1	Locking System Management (LSM).....	5
2.1.2	Additional software	6
2.1.3	Protocol generation	8
2.2	Programming devices	8
2.2.1	Active.....	8
2.2.2	Passive.....	9
2.3	Locking devices	9
2.3.1	Locking cylinder.....	10
2.3.2	SmartHandle.....	11
2.3.3	SmartRelais	12
2.3.4	Digital padlocks.....	14
2.3.5	Furniture locks	14
2.4	Identification media	15
2.4.1	Transponder (active)	15
2.4.2	RFID (passive)	15
2.4.3	CompactReader (hybrid).....	16
2.4.4	PINCode.....	17
2.4.5	Block lock.....	18
3	Functions and equipment	19
3.1	Access event logging.....	19
3.2	Time zone control	19
3.3	DoorMonitoring.....	20
4	Networking	22
4.1	Offline.....	23
4.2	WaveNet.....	24
4.2.1	Event management	25
4.3	Virtual	25
5	Help and other information	27

1 General operation

The 3060 digital locking and access control system has a modular structure. It ranges from a simple locking system for individual doors to a complex computer-controlled access control system.



Identification media

Conventional mechanical keys are replaced by digital identification media:

- Transponder
- RFID media
- PIN code keypad

Each user will normally have their own transponder or RFID medium. Compared to mechanical keys, digital keys are a better solution in the long term: They have more functions and offer greater operational security. A lost digital key can be blocked in just a few minutes and can no longer be misused.

Locking devices

These identification media open and close the locks (generic term: locking devices), e.g. on:

- Doors
- Gates
- Barriers
- Furniture
- Lifts

Communication between identification media and locking devices is protected by multiple state-of-the-art encryption methods. External attacks are thus prevented technically. Digital locking devices also offer advantages compared to mechanical locking devices: For example, a digital lock can be temporarily deactivated during the arming of an alarm system and no one can open it during this time ("Block lock function", see [Block lock \[► 18\]](#)).

Permissions

Each identification medium is individually programmed for a locking system. Each locking system contains a locking plan which you can use to control the permissions of identification media for the locking devices.

You can grant permissions for each employee individually or for several employees at once (e.g. for all employees in a department).

Full control

Then keep an eye on everything with the various functions of your locking system:

- Who may open which locking device when?
- Who opened which locking device when?
- When was which door opened for how long?
- Which doors are open, which are closed and which are locked?

Future security

SimonsVoss locking systems are future-proof. Modify and extend the system according to your personal needs. Construct your personal locking system from the System 3060 portfolio.

2 Components

2.1 Software

2.1.1 Locking System Management (LSM)



The locking plan software (LSM for short) is the brain of your locking system. It can run on Windows from version 7 (a Windows server is required depending on the extension stage). You can find the exact system requirements in the LSM manual ([SimonsVoss website](http://www.simonsvoss.com)). LSM allows you free programming of all components.

A locking system can be very comprehensively equipped:

- 64,000 identification media
- 64,000 locking devices

Not enough for you yet? Use each of your transponders in up to four locking systems.

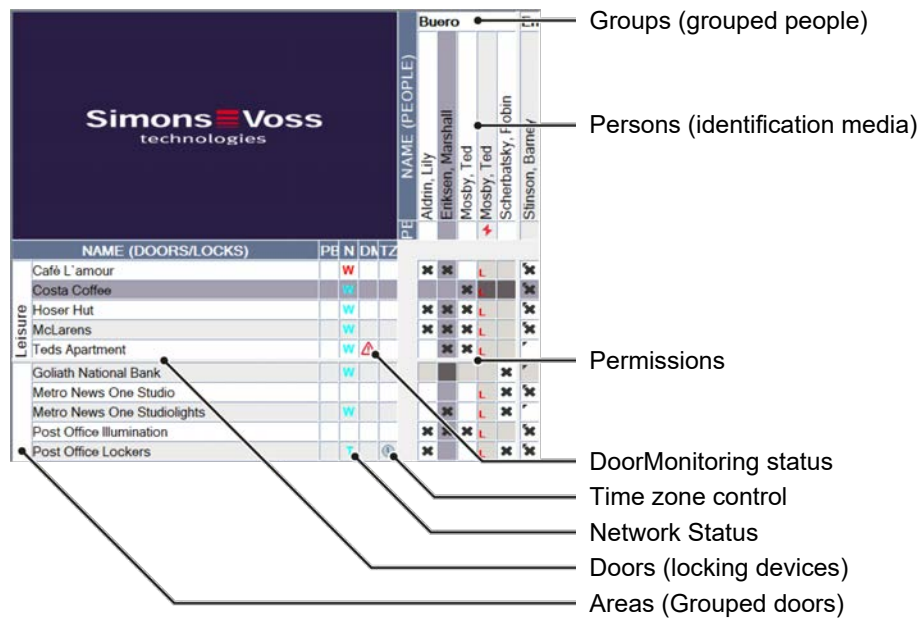
Four locking systems per transponder are not enough for you either? With superordinate locking levels, you can use the same transponders in even more locking systems.

Easy control

At the same time, issuing and changing authorisations is very easy:

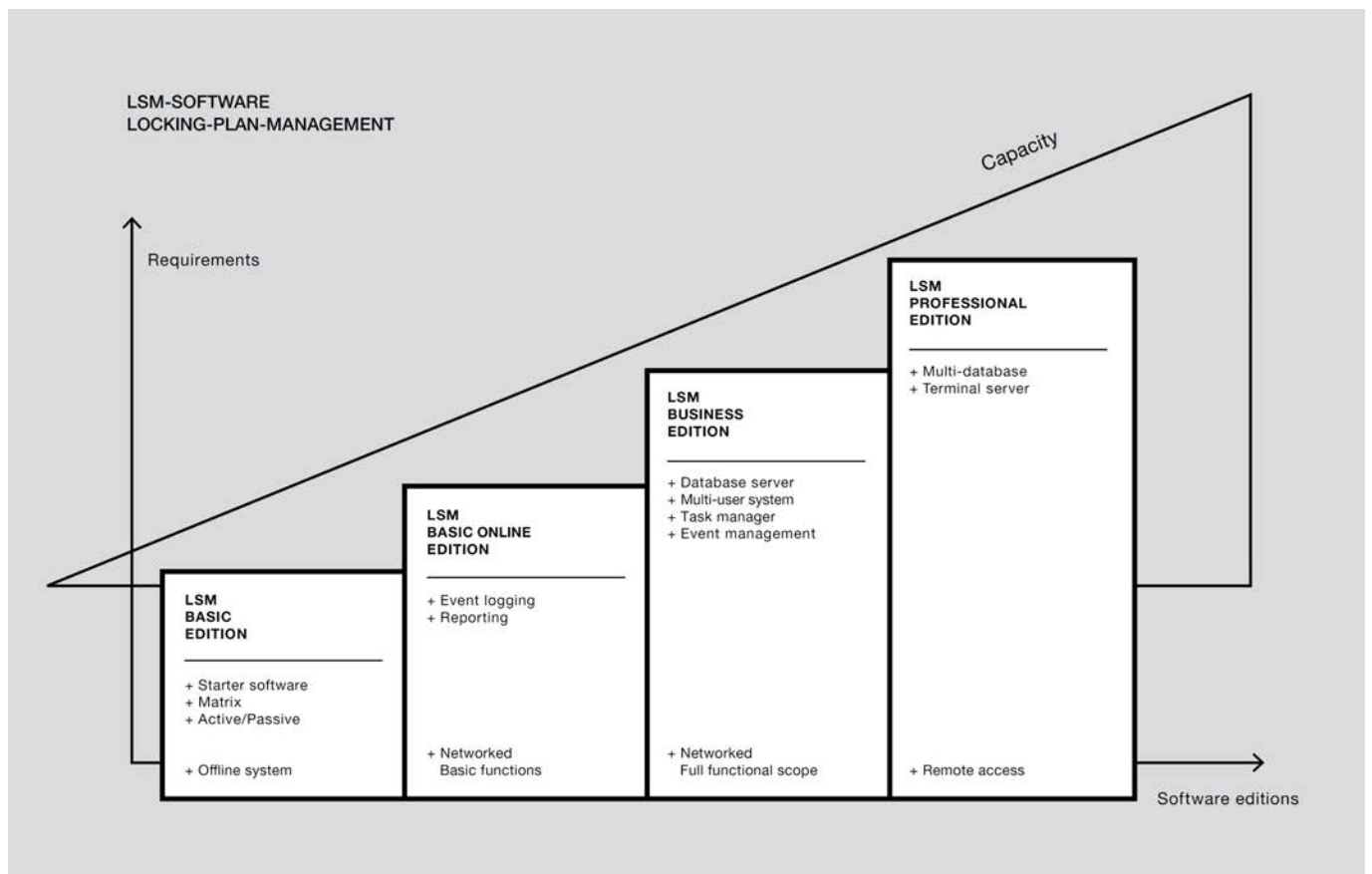
1. Click the mouse.
2. Program.
3. And it's done.

Areas, groups and filters are available to give you an overview even of large locking systems. Display columns or rows as required. In the example, columns on network status, door monitoring status and time zone control are displayed:



Editions

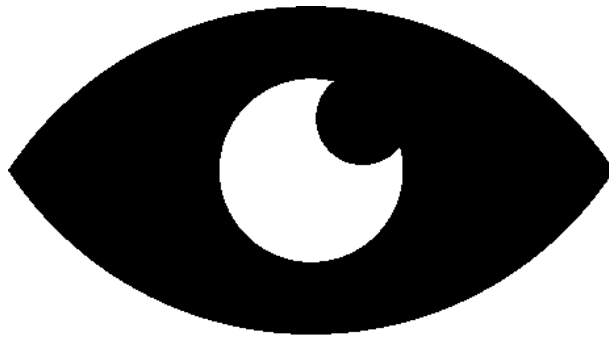
LSM is available in various editions that build on each other. The simplest edition is LSM Starter, which only supports active technology (transponders).



2.1.2 Additional software

SimonsVoss makes your life even easier with smart software:

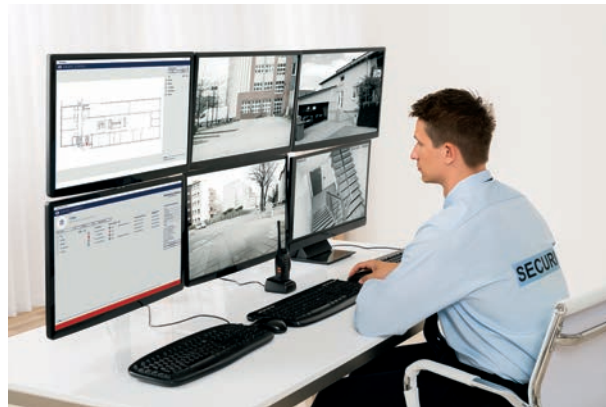
Smart.Surveil



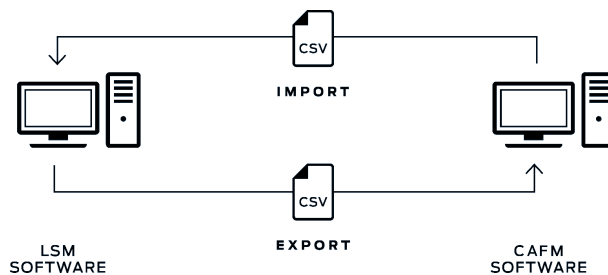
Smart.Surveil is a monitoring tool which allows you to monitor your networked doors with DoorMonitoring locking devices even without LSM and to control them remotely (see *DoorMonitoring* [▶ 20]).

Example

Smart.Surveil is suitable for use in a monitoring room. Together with a camera system, you always know what's going on.



Smart.XChange



Smart.XChange is an interface for automated data transfer between LSM and a third-party system (e.g. a personnel management system).

2.1.3 Protocol generation

```
01110001 00001100 10101001 01100000 01001101 10110111
00111011 01111100 00111101 01111101 10000011 10100110
11010110 00010111 10011101 00000011 01010001 00000001
00010110 01011111 10111101 10001000 01011110 01100111
```

SimonsVoss protocols for regulation of communication between the locking device and identification medium, are already in the second generation. Compared to the first generation, G2 protocols are:

- More powerful: G2 allows you to manage a much greater number of locking devices and identification media.
- More flexible: One major advantage is the freedom of choice for new permissions. Unlike G1, you can now save permissions either on the locking device or on the identification medium. This saves a lot of time, especially in spatially extended locking systems.

SimonsVoss attaches great importance to investment security, so it goes without saying that you can mix G1 and G2 components and thus continue to use G1 components already in place.

2.2 Programming devices

You can save permissions from your locking plans to your identification media and locking devices with the programming devices. You can use different programming devices according to the type of identification media:

- *Active* [▶ 8]: Transponder
- *Passive* [▶ 9]: RFID identification media


All programming is wireless and encrypted. In networked systems, you can also conveniently program changes via WaveNet from your workstation.

2.2.1 Active





SmartCD.G2:

SmartCD.G2 can be used from LSM Basic onwards and programs transponders and active or hybrid locking devices.

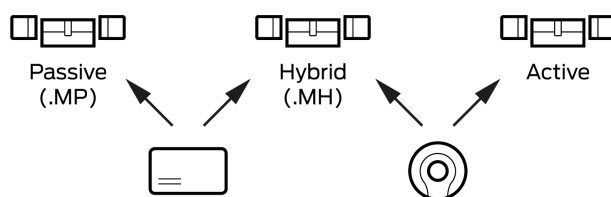
	<p>CD.Starter.G2: CD.Starter.G2 can only be used in LSM Starter and programs transponders and active locking devices.</p>
---	---

2.2.2 Passive

	<p>SmartCD.MP: SmartCD.MP programs your RFID identification media and passive or hybrid locking devices.</p>
	<p>SmartCD.HF: SmartCD.HF quickly programs your RFID identification media.</p>

2.3 Locking devices

In the System 3060, a "locking device" is anything that can be opened and closed or switched using an identification medium. There are three basic types of locking device:



- Active locking devices (25 kHz): Can only be operated with active identification media, e.g. with a transponder.
- Passive locks (13.56 MHz): Can only be operated with passive identification media, e.g. with a card.
- Hybrid locks (25 kHz and 13.56 MHz): Can be operated with active and/or passive identification media.

You will receive many locking devices with additional features available. Some of these features are described in the chapter *Functions and equipment* [▶ 19]. Further details can be found in the documentation and the product catalogue. All SimonsVoss locking devices have different opening modes, including:

- Timed opening for a freely selectable duration (locking device then disengages again)
- Flip-flop mode (locking device only opens and closes when the identification medium is presented again)

2.3.1 Locking cylinder



Locking Cylinder 3061 is the classic SimonsVoss locking device. Identify yourself with an identification medium and simply turn the knob instead of using a mechanical key.

- The cylinder profile is similar to a mechanical locking cylinder: Locking Cylinder 3061 is mechanically fully compatible.
- The batteries for power supply are integrated into the knob: Complicated wiring is no longer needed.

This makes installation so easy that it can be completed in just a few minutes:

1. Remove old locking cylinder.
2. Install Locking Cylinder 3061.
3. And it's done.
4. Locking Cylinder 3061 is available in many versions, including:

- Permanently engaged on the inside
- Half cylinder
- Freely rotating on both sides
- Weatherproof
- VdS-compliant
- Brass colours
- With button on the inside
- Design for panic locks
- Easy-grip knobs
- ...

There is a very long battery life of up to 300,000 activations or 10 years on stand-by. If the batteries do eventually lose power, a multi-stage battery warning system will alert you in good time, even directly in the LSM for networked locking systems.

2.3.2 SmartHandle

SmartHandle 3062



SmartHandle 3062 is the digital replacement for your door handle. Identify yourself with an identification medium and operate the handle to open the door.

With its broad portfolio, SmartHandle is suitable for many installation situations - especially exterior areas.

Long battery life allows long maintenance-free operation until the battery warning system warns of low batteries (up to 150,000 activations or up to ten years on stand-by in the active version).

SmartHandle AX



SmartHandle AX is a further development of SmartHandle 3062. With its adaptive design, it can be mounted on existing escutcheon patterns with no drilling in accordance with DIN 18251. The combination with metal elements is also an eye-catching feature.

SmartHandle AX is also very intelligent and future-proofed with functions such as BLE* and Phone2Door* (with expected availability from 2021).

Here, too, the broad portfolio offers solutions for a great number of installation situations.

SmartHandle AX has an outstanding battery life (up to 300,000 activations or up to ten years on stand-by in the active version). This also has an integrated battery warning system.

2.3.3 SmartRelais



The SimonsVoss SmartRelais product range is a series of electronic switches which can be operated using identification media or via the network.

You simply assign authorisations for identification media in LSM just like with any locking device.

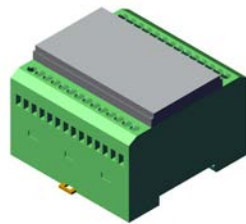


SmartRelais:

This SmartRelais is so small that it can even be hidden in a cavity wall box. You can still manage it conveniently with the LSM.

 A single, compact, light grey rectangular housing for the SmartRelais 2. The text "Simons Voss" is visible on the front face.	<p>SmartRelais 2:</p> <p>The SmartRelais 2 housing is elegant, compact and optionally weatherproof.</p> <p>It can also read passive identification media.</p>
 Three light grey rectangular housings for the SmartRelais 3, shown in a staggered arrangement to show their depth and design.	<p>SmartRelais 3:</p> <p>SmartRelais 3 sets new standards of performance. Due to the PoE-capable Ethernet interface, even large amounts of data can be transferred quickly and there is no need for irritating mains power cables.</p>

If you require a large number of outputs, you can connect SmartOutput modules to a SmartRelais or SmartRelais 3. You can connect up to 15 modules, giving you up to 115 individually controllable outputs.



2.3.4 Digital padlocks



The SimonsVoss padlock can be operated like a 3061 locking cylinder. This means that you can also secure basement sections or garden sheds, for example, without bothering with mechanical keys.

It is available as a manual or self-locking version and with different shackle diameters. A security chain prevents it from falling or being stolen.

There is a very long battery life of up to 300,000 activations or 10 years on stand-by. If the batteries do eventually lose power, a multi-stage battery warning system will alert you in good time, even directly in the LSM for networked locking systems.

2.3.5 Furniture locks


You can also manage your furniture in System 3060 with furniture locks.

Program permissions as normal, open with transponders and optionally record who opened what and when.



Shooting bar lock:

The shooting bar lock is suitable for single-leaf or multi-leaf hinged door cabinets.

	<p>Locker lock: The shooting bar lock is suitable for lockers, cabinets or drawers.</p>
---	---

2.4 Identification media

In System 3060, an "identification medium" is anything that can open and close or operate a locking device.



2.4.1 Transponder (active)



Transponder 3064, as the most well-known SimonsVoss product, is also managed and authorised in the LSM. It then opens contactlessly and encrypts all active or hybrid locking devices. It not only replaces your mechanical keys, it also takes on the functions of an identification card.

The transponder is supplied with a blue button as standard. On request, however, you can also select brown or red and make your transponders RFID enabled.

2.4.2 RFID (passive)

	<p>SmartCard: MIFARE® Classic, MIFARE Plus® and MIFARE® DESFire® SmartCards can also be used in System 3060. This is particularly advantageous where a company already has cards which are used, for example, as a company ID or for recording time and attendance.</p>
	<p>SmartTag: Would you prefer SmartTags to SmartCards? MIFARE® Classic, MIFARE Plus® and MIFARE® DESFire® SmartTags can also be used in System 3060.</p>

2.4.3 CompactReader (hybrid)



With the CompactReader, in no time at all you can turn your active locking devices into hybrid locking devices which can also read passive RFID identification media, such as a card. The CompactReader is permanently linked to the locking device during programming. It reads the card and forwards the data to the locking device.

Installation is quick and easy with only two screws and no cables. Alternatively, simply stick the CompactReader in place.

After that, you don't have to worry about anything for up to 80,000 activations or up to 6 years on standby. The CompactReader warns you in good time when the batteries run out.

2.4.4 PINCode



SimonsVoss offers two products in System 3060 into which a PIN can be entered:

- PinCode *keypad*
- PinCode *Terminal*

The main difference is that the PinCode terminal requests a second feature in addition to the PIN (two-factor authentication).

After programming and easy installation (gluing or screwing), you no longer have to worry about anything else for both products until you get a warning of weak batteries (up to 100,000 activations or up to ten years on stand-by).

PinCode keypad

You can create up to three user PINs with a freely selectable master PIN. You can authorise these user PINs independently of each other at a locking device in the LSM. After entry of an authorised user PIN, the corresponding locking device opens.

The use of a PIN code keypad is particularly useful if it is impractical to work with physical identification media, e.g. at a conference.

PinCode terminal

Depending on the operating mode, the PinCode terminal requires the following to open:

- Entry of a freely selectable user PIN and transponder ID
- Activation of the identification medium and entry of a freely selectable user PIN

- Activation of the identification medium and entering a fixed user PIN

LSM is used to set up the PinCode terminal operating mode. A single PinCode terminal supports up to 500 user PINs.

Two-factor authentication increases security in the system. Potential thieves, for example, don't just need to have the transponder, they must also enter the corresponding user PIN.

2.4.5 Block lock



The block lock is practical if you are using an alarm system. The block lock is also available as VdS construction.

Set your alarm system from a central point. At this point, the block lock deactivates all monitored doors and thus also blocks them for authorised identification media. This prevents annoying and expensive false alarms.

After the monitoring period, turn the alarm system back off at the central point and simultaneously reactivate the monitored doors.

3 Functions and equipment

3.1 Access event logging

Locking devices with access event logging (.ZK) record attempted access by authorised and optionally unauthorised identification media.

You can read the access list and view it in the LSM. There are have several options for reading out:

- Reading out with a programming device
- Read-out via WaveNet (networked locking devices)
- Read-out via the network connection (SmartRelais 3)

The number of storable accesses depends on the specific locking device. For each access or attempted access, the following is recorded:

- Date
- Time
- Transponder ID

After it has been read out, the LSM compares the read out with the internal access list and only adds new entries to the internal access list. 10,000 access events can be saved per locking device in LSM.



NOTE

Access logging and time zone control cannot be retrofitted

The .ZK feature cannot be retrofitted.

- If you require access logging and/or time zone control, please order .ZK locking devices.

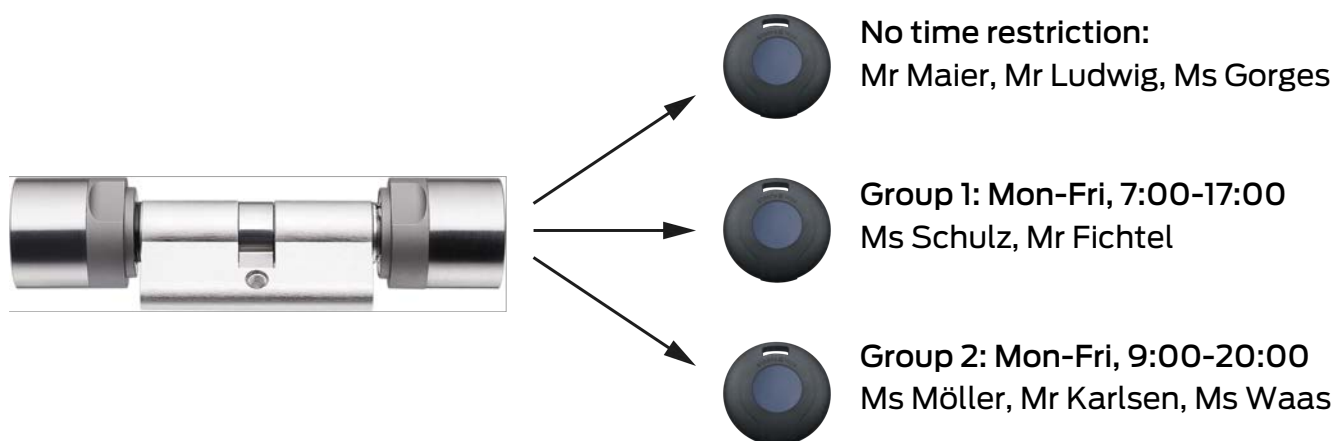
3.2 Time zone control

Time zone-capable locking devices can be controlled both via the matrix and also via the date and time:

- Automatically engage and/or disengage at a specific time
- Groups of transponders are only authorised at certain times.

A total of 100 time groups are available for controlling the time-related authorisations of transponders.

An example of application would be, for example, authorisations with different time restrictions for different groups of users for the same locking device. Some users can always open the locking device, some only from 7:00 to 17:00 and some only from 9:00 to 20:00:



Sundays or public holidays can, of course, also be taken into account.



NOTE

Access logging and time zone control cannot be retrofitted

The .ZK feature cannot be retrofitted.

- If you require access logging and/or time zone control, please order .ZK locking devices.

3.3 DoorMonitoring

DoorMonitoring is your miniature electronic monitor. With a combination of sophisticated integrated sensors, the locking device can detect, e.g., the following statuses:

- Door is open.
- Door is closed.
- Door is locked.
- Door is securely (doubled) locked.
- Handle pressed / not pressed (SmartHandle, SmartHandle AX)
- Cover removed / not removed (SmartHandle AX, SmartRelais 3)

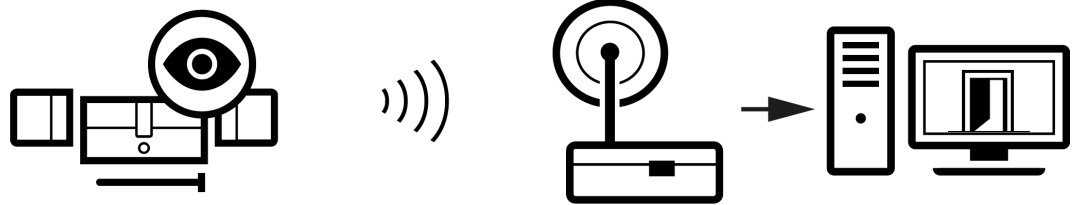
You can monitor three inputs as a DoorMonitoring event even in SmartRelais 3.

DoorMonitoring is cable-free and needs no drilling.

LSM and networked locking devices allow you to respond immediately to different door statuses and to be notified, for example, if a door is open for too long (see *Event management* [▶ 25]). Smart.Surveil is also available (see *Additional software* [▶ 6]). With this you can see the status of all doors at a glance: Available as a list or directly in the building plan.

Example

After lessons, all doors should be closed. Your networked locking devices recognise that the door is open. You forward this information to the LSM database via WaveNet. From there, the information is displayed in the LSM or Smart.Surveil.



4 Networking

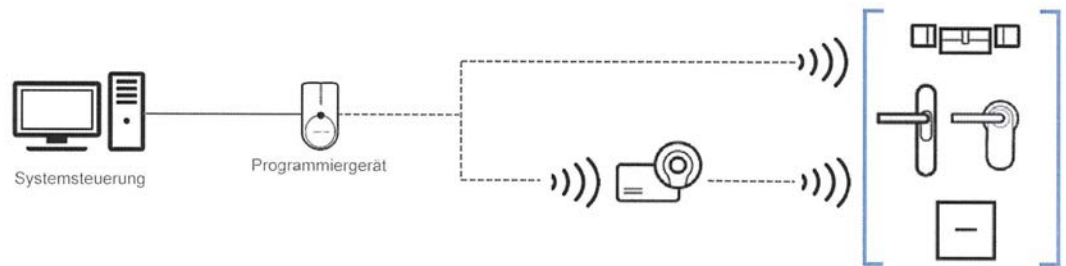
Networked locking devices mean less work, but more functions. You can choose between two networking concepts, which you can of course also combine:

	WaveNet (online)	Virtual networking (virtual)	Offline (no networking)
Functional principle	Data transmission with networked WaveNet devices. (See <i>WaveNet</i> [▶ 24])	Data transmission with identification media (except programming data). (See <i>Virtual</i> [▶ 25])	Data transmission with programming devices. (See <i>Offline</i> [▶ 23])
Propagation	WaveNet devices are linked via various transmission media. All types of data are transmitted using these transmission media.	In the virtual network, certain data is transferred to the identification media using a gateway (entries in the blacklist). If you then operate these identification media on a virtually networked locking device, the data is transferred to the locking device.	Locking devices that are not networked can only exchange data with the programming device. You must go to the locking devices with the programming device.
Programming effort	Low.	Low.	Effort depends on the size of the locking system. <ul style="list-style-type: none"> ■ Small locking system: Low effort. ■ Medium locking system: Medium effort. ■ Large locking system: Extensive effort.
Transmission speed of the data exchange	Immediate. Data exchange with different transmission media.	Speed between gateway and locking devices highly dependent on the intensity of use of the locking devices. Identification media are transmission media - no data transmission without identification.	Slow.

	WaveNet (online)	Virtual networking (virtual)	Offline (no networking)
Central activation/deactivation of locking devices	Possible.	Not possible.	Not possible.
Activation/deactivation centrally traceable	Possible.	Not possible.	Not possible.
Remote opening	Possible.	Not possible.	Not possible.
Remote monitoring (Door-Monitoring, see <i>DoorMonitoring</i> [▶ 20])	Possible.	Not possible.	Not possible.
Event management	Possible.	Not possible.	Not possible.
Access lists centrally retrievable	Possible.	Not possible (except SREL 3).	Not possible.
Software/server independent protective functions	Possible.	Not possible.	Not possible.
Immediate locking device system-wide response to critical situations (availability of protective functions).	Possible.	Not possible.	Not possible.

4.1 Offline

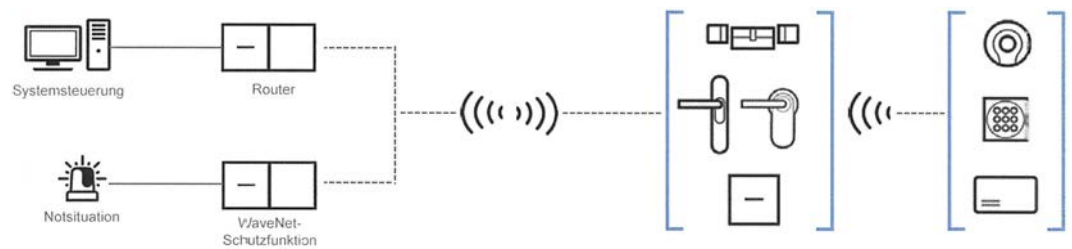
Operation without networking is primarily suitable for small systems. You program everything with your programming device, i.e. either the identification medium or the locking device.



To read out information from your locking devices, you must go to the corresponding door and read the locking device with the programming device.

Effort in this operating mode increases significantly as the locking system grows. Networked or virtually networked operation is ideal for this purpose.

4.2 WaveNet



In direct networking, you establish an 868 MHz radio network with base stations ("RouterNode") and network boards integrated in the locking device ("LockNode"). Your locking devices and the software can communicate directly with each other via the RouterNodes:

- Programme
- Remote opening
- Notifications of events

It is significantly more convenient than non-networked systems: Most of this can be done conveniently from the workplace.

The WaveNet configures itself automatically and does not need to be wired to the door.

Additional functions

The optional protective functions of your WaveNet further increase the overall security in the system.

There are also many other interesting functions and setting options available:

- Central activation/deactivation of locking devices
- Remote opening of locking devices
- Emergency release of locking devices

- gunman attack function

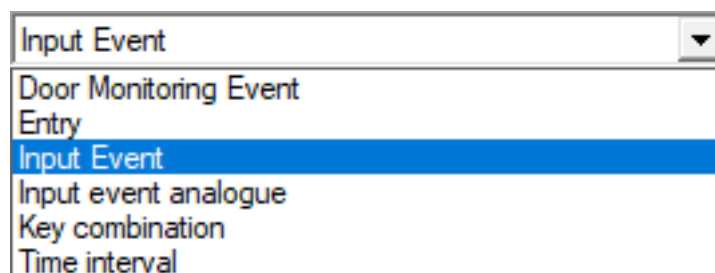
Please refer to the WaveNet manual for more detailed information.

4.2.1 Event management

System 3060 can also act without your intervention and perform a wide range of tasks for you. These tasks can be started in two ways:

- Time-controlled
 - One-time: Start on a specific date
 - Periodically: Start at specific time intervals
- Event-controlled: A configurable event (e.g. a door that is open too long) triggers any desired number of configurable tasks.

Choose from a variety of events that trigger a task.



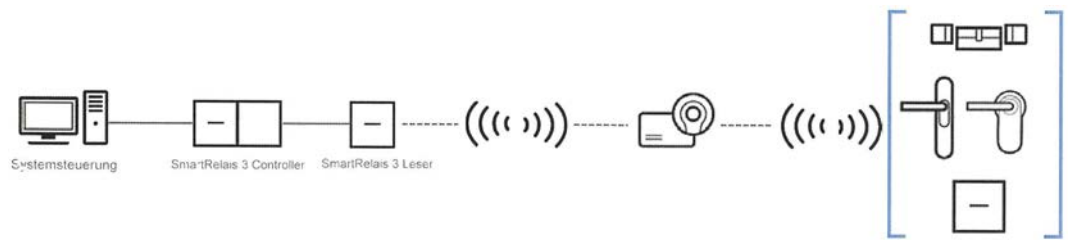
Example

A person with an unauthorised transponder attempts to enter the school building. The locking device detects the unauthorised attempted access and sends this information via the network. Event management is used to switch a networked SmartRelais, which in turn activates a camera.

4.3 Virtual

A direct networking ("WaveNet") requires a network board ("LockNode") at each locking device to be networked and sufficient base stations ("RouterNode") to reach all LockNodes.

Alternatively, the virtual network is available to you. The virtual network does not use radio for data transmission, but exploits the fact that users with writeable identification media are moving within a locking system. The data is written to the identification media at some central points ("gateways") and is carried by users to all locking devices throughout the day. Users also carry data from the locking devices to the gateways at the same time with their identification media.



The gateways are the only components with a direct connection to the LSM database and are always up to date. They function as a simplified, outsourced programming device.

If an identification medium is presented, the gateway checks whether:

- data is available in the database which must be transported to the locking device (e.g. "block transponder 1").
- data from the locking device is available in the identification medium that is to be written to the database (e.g. "Transponder 1 is blocked").

You can also create a stock of transponders. Program some transponders and place them in a box. If someone is to receive a transponder, the transponder just needs to be given to that person. The gateway recognises the transponder and programs the permissions assigned in the LSM onto the transponder.

5 Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

<https://www.simons-voss.com/en/documents.html>

Declarations of conformity

You will find declarations of conformity and other certificates on the website:

<https://www.simons-voss.com/en/certificates.html>

Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

Email

You may prefer to send us an email.

support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

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

Address

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germany



This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

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

Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

© 2022, SimonsVoss Technologies GmbH, Unterföhring

All rights are reserved. Text, images and diagrams are protected under copyright law.

The content of this document must not be copied, distributed or modified. More information about this product can be found on the SimonsVoss website. Subject to technical changes.

SimonsVoss and MobileKey are registered brands belonging to SimonsVoss Technologies GmbH.

SimonsVoss
technologies

Made in Germany

A BRAND OF


ALLEGION™