

# LSM 3.4 SP2 SmartUserGuide

---

## Manual

29.10.2019

## Contents

<b>1</b>	<b>Basic functions .....</b>	<b>4</b>
1.1	Add new locking system.....	4
1.2	Add new transponder group.....	4
1.3	Add new transponder .....	4
1.4	Assign transponder to a transponder group at later point in time .....	5
1.5	Add new area.....	5
1.6	Add new locking device .....	5
1.7	Assign locking device to an area.....	5
1.8	Issue/withdraw authorisation.....	6
1.9	Working in compliance with data protection regulations GDPR .....	6
1.9.1	Export data.....	7
1.9.2	Deleting Data.....	9
1.10	Add PIN code Keypad.....	11
1.10.1	Configure PIN code Keypad .....	11
1.10.2	Add PIN code Keypad to the locking plan .....	12
1.10.3	Programme PIN code Keypad .....	12
1.11	Search matrix.....	12
1.12	Execute group actions .....	13
1.13	Programme transponder .....	14
1.14	Programme locking device.....	14
1.15	Define time zone plan (with public holidays and company holidays .....	15
1.16	Resetting components.....	16
1.17	Replace defective locking device.....	17
1.18	Replace defective, lost or stolen transponders .....	17
1.19	Check and evaluate the battery level in the locking devices.....	19
1.20	Common locking level .....	21
1.20.1	Add common locking level .....	21
1.20.2	Link locking devices.....	22
1.20.3	Link transponders.....	22
1.20.4	Authorise transponders.....	23
1.21	Create fire service transponders.....	24
1.22	Setting up DoorMonitoring components.....	24
1.23	Programme using LSM Mobile .....	25
1.23.1	With pocket PC/PDA.....	25
1.23.2	With laptop, netbook or tablet PC.....	26
1.24	Reset storage mode in G1 locking devices.....	27

1.25	Access administration .....	27
1.26	Administer users (BUSINESS).....	28
1.27	Card management .....	28
1.27.1	Change configuration .....	29
1.27.2	Overview .....	31
<b>2</b>	<b>Performing standard WaveNet-based tasks in LSM Business .....</b>	<b>33</b>
2.1	Creating a WaveNet radio network and incorporating a locking device .....	33
2.1.1	Preparing the LSM software .....	33
2.1.2	Initial programming of the locking components.....	33
2.1.3	Preparing hardware.....	34
2.1.4	Creating communication nodes.....	34
2.1.5	Setting up the network and importing into LSM.....	35
2.2	Putting the DoorMonitoring locking cylinder into operation .....	36
2.2.1	Adding a DoorMonitoring locking cylinder.....	36
2.2.2	Incorporating a DoorMonitoring cylinder into the network .....	37
2.2.3	Transmitting the WaveNet configuration .....	37
2.2.4	Assigning a locking device's LockNode .....	38
2.2.5	Activating the locking device's input events .....	38
2.3	Setting up a RingCast .....	38
2.3.1	Preparing RouterNode for RingCast .....	39
2.3.2	Adding a RingCast.....	40
2.3.3	RingCast function test .....	42
2.4	Setting up event management .....	45
2.4.1	Setting up an email server .....	45
2.4.2	Setting up Task services .....	45
2.4.3	Forwarding input events via the RouterNode2 .....	45
2.4.4	Forward input events via the SREL3 ADV system .....	46
2.4.5	Creating a response .....	48
2.4.6	Creating an event .....	48
2.5	Managing the virtual network (VN) .....	49
2.5.1	Setting up a locking system .....	49
2.5.2	Setting up a VN service .....	49
2.5.3	Add components and set up the LSM software.....	49
2.5.4	Exporting authorisation changes.....	50
2.5.5	Importing authorisation changes .....	51
2.5.6	Tips on VN.....	51
2.6	Sabotage detection .....	52
2.7	DoorMonitoring (SmartHandle) - Door handle events .....	52
<b>3</b>	<b>Help and other information .....</b>	<b>53</b>

## 1 Basic functions

This section describes the basic processes in the LSM software. LSM software frequently offers a number of ways to access the function that you require. These basic functions mostly show you the quickest and easiest way.

The SimonsVoss Smart User Guide uses an understandable example to describe in detail how a locking system is created and managed.

### 1.1 Add new locking system

- ✓ Installation has been completed correctly and a backup has been created.
- 1. Select *Edit/New locking system* in the menu bar.
- 2. Define the required locking system options.
  - ➔ Select a colour from "Use as common locking level" for the common locking levels. *Common locking levels act as additional levels to existing standard locking systems. See Common locking level.*
- 3. Click on the "Apply" button.
- 4. Click on the "Finish" button.

### 1.2 Add new transponder group

- ✓ A locking system has already been added.
- 1. Right-click on transponder groups in the "Groups area" in the LSM software.
- 2. Click on "New".
- 3. Give the new transponder group a name and make other settings if necessary.
- 4. Click on the "Apply" button.
- 5. Click on the "Finish" button.

### 1.3 Add new transponder

- ✓ A locking system has already been added.
- 1. Select *Edit/New transponder*.
- 2. Fill out all attributes and use the "Configuration" button to make further settings if necessary.
- 3. Click on the "Save & next" button.
- 4. Click on the "Finish" button.

#### 1.4 Assign transponder to a transponder group at later point in time

- ✓ The transponder has already been created and a transponder group has been added.
- 1. Open the locking system settings, using the *Edit/Properties* menu bar, for example: *Locking system*.
- 2. Select the "Transponder" tab.
- 3. Select the transponder from the table with which you wish to correlate a transponder group.
- 4. Select the required transponder group which is to be correlated with the transponder from the drop-down list in "Change assignment to transponder groups".
- 5. Click on the "Execute" button.
- 6. Click on the "Apply" button.
- 7. Click on the "Finish" button.

*If a transponder is being newly added, it can be immediately assigned to an existing transponder group.*

#### 1.5 Add new area

- ✓ A locking system has already been added.
- 1. Right-click on areas in "Areas-area" in the LSM software.
- 2. Click on "New".
- 3. Give the new area a name and make other settings if necessary.
- 4. Click on the "Apply" button.
- 5. Click on the "Finish" button.

#### 1.6 Add new locking device

- ✓ A locking system has already been added.
- 1. Select *Edit/New locking device*.
- 2. Fill out all attributes and use the "Configuration" button to make further settings if necessary.
- 3. Click on the "Save & next" button.
- 4. Click on the "Finish" button.

#### 1.7 Assign locking device to an area

- ✓ The locking device has already been created and an area has been added.
- 1. Open the locking system settings, using the *Edit/Properties* menu bar, for example: *Locking system*.
- 2. Select the "Doors" tab.

3. Select the door from the table with which you wish to correlate an area.
4. Select the required area which is to be correlated with the door from the drop-down list in "Change assignment to area".
5. Click on the "Execute" button.
6. Click on the "Apply" button.
7. Click on the "Finish" button.

*If a locking device is being newly added, it can be immediately assigned to an existing transponder area.*

## 1.8 Issue/withdraw authorisation

You can use the matrix to issue and withdraw authorisations. You only need to click on an authorisation field to change the authorisation in the default setting.

*You can only issue or withdraw authorisations between a locking device and a transponder.*

Observe the two views:

### ■ View/Doors and persons

In this view, the authorisations are changed for the transponder concerned.

### ■ View/Areas and transponder groups

In this view, the authorisations are changed for entire groups.

## 1.9 Working in compliance with data protection regulations GDPR

Since 25 May 2018, the General Data Protection Regulation has been valid throughout Europe. It regulates the handling of personal data in order to ensure their protection and at the same time their free movement within the European internal market. First of all, access to the database via the graphical user interface is only possible with a password and corresponding user rights. Additional "Exceptions in time zone management": In addition, no "special categories" of personal data pursuant to Art. 9 GDPR are stored within the LSM software. The mandatory fields used for a person are used exclusively for the unique assignment of identification media within the locking plan. The obligatory data are only required by the system for the duration of the occupation of an identification medium (e.g. company affiliation). The duration of data storage in logs can be changed at will by the locking system administrator himself (see Options/Logging).

## 1.9.1 Export data



### IMPORTANT

#### Other language texts

The same language as in the LSM software is used for texts in the exported files.

#### Persons

You can export the saved personal data of people in the locking system as CSV files. Three files are generated during this process:

Person	This file contains personal data which can be used to identify the person (for example, surname, address or photo).
PersonHistory	This file contains the dates that the data record was created and erased.
PersonLog	This file contains different processing steps which have been performed on the person in question's data record, such as changes to authorisations and programming processes.

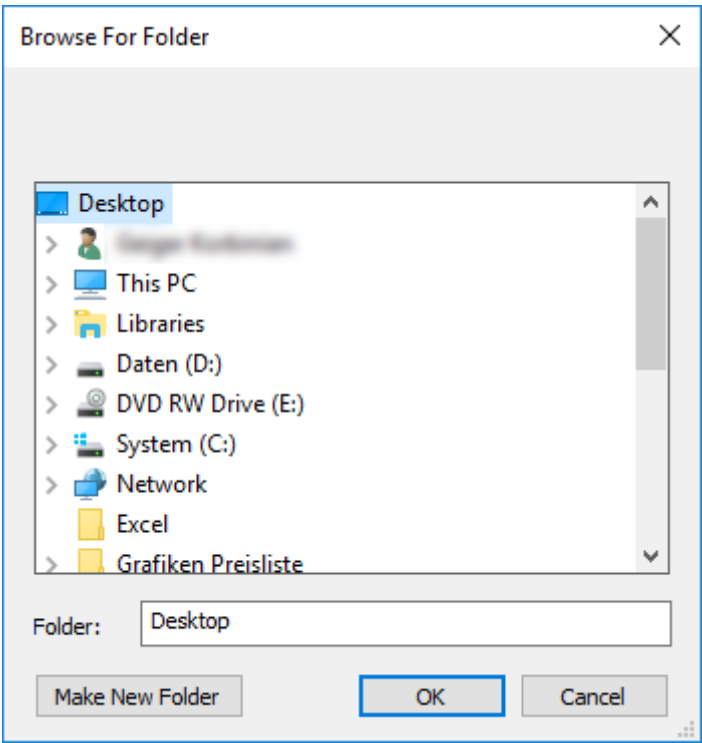


### IMPORTANT

The GDPR functions access HR Management for this purpose. As a result, the functions need to be assigned to a user group which is authorised to access HR Management.

✓ LSM open.

1. Use | Options | to select the **GDPR functions** item.  
↳ The "GDPR functions" window will open.
2. Highlight the entry for the person whose data needs to be exported in the "People" section.
3. Click on the **Export personal data** button in the "People" section.  
↳ The "Search Folder" window will open.



- 4. Indicate the folder where the files are to be exported.
- 5. Click on the **OK** button.
- ➔ Data is exported.

**Users**

You can export the users' saved personal data as CSV files in the LSM software. Two files are generated during this process:

User	This file contains the data which refers to the user, such as user name and user group.
UserLog	This file contains different processing steps which the user has carried out, such as creating a new locking device.



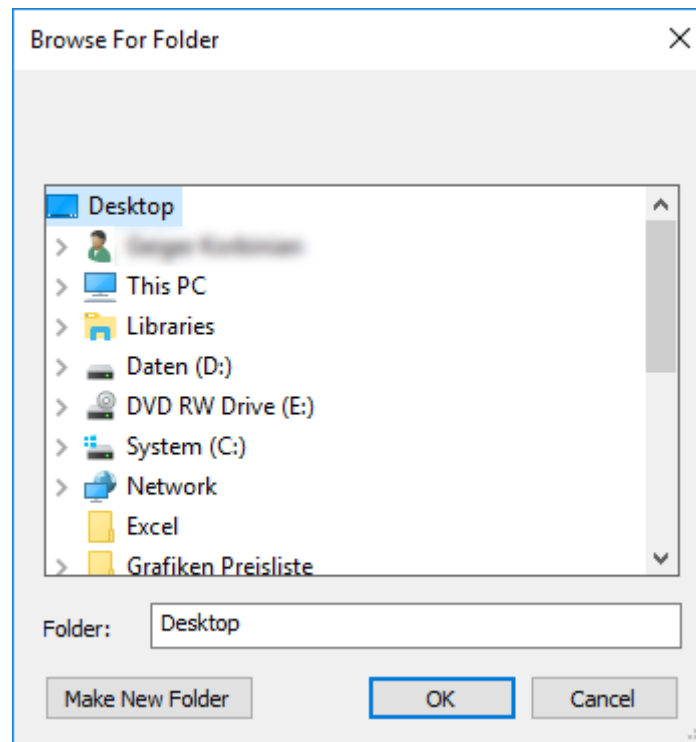
**IMPORTANT**

The GDPR functions access administration functions for this purpose. As a result, they need to be assigned to a user group which is authorised to access Administration.

- ✓ LSM open.
- 1. Use | Options | to select the **GDPR functions** item.
  - ➔ The "GDPR functions" window will open.
- 2. Highlight the entry for the user whose data needs to be exported in the "Users" section.



3. Click on the **Export personal data** button in the "Users" section.  
↳ The "Search Folder" window will open.



4. Indicate the folder where the files are to be exported.
5. Click on the **OK** button.  
↳ Data is exported.

## 1.9.2 Deleting Data

You can also use the GDPR module to easily erase personal data.

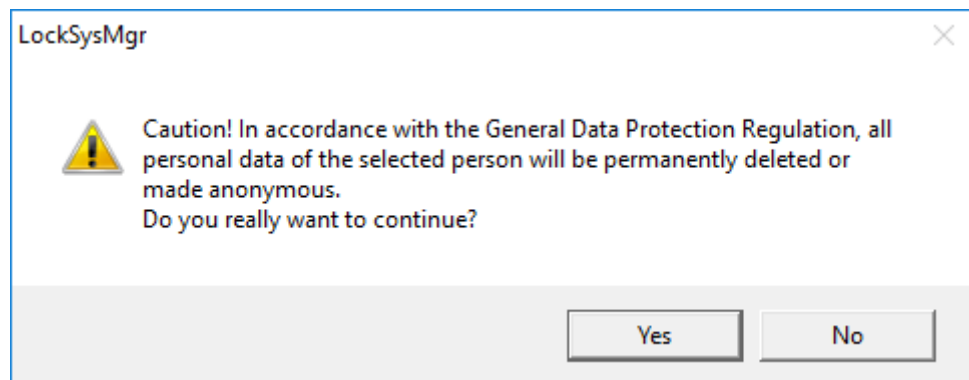
### Persons



#### IMPORTANT

The GDPR functions access HR Management for this purpose. As a result, the functions need to be assigned to a user group which is authorised to access HR Management.

- ✓ LSM open.
1. Use | Options | to select the **GDPR functions** item.  
↳ The "GDPR functions" window will open.
2. Highlight the entry for the person whose data needs to be erased in the "People" section.
3. Click on the **Permanently delete personal data** button in the "People" section.  
↳ The "LockSysMgr" window will open.



4. Click on the **Yes** button.

↳ The highlighted person's personal data is erased or anonymised.



### IMPORTANT

#### Erasure of remaining data from previous deletions

You can also use the **✕** button in the [Name] tab in the assigned identification media to erase personal data. Unlike erasure using the GDPR module, this button does not delete logs, which will remain in the system. This means that only a part of personal data is erased. People who are deleted in this way are no longer displayed in the GDPR module. Please use the **Delete** button in the "Database" section to meet GDPR requirements and also remove such files.

### Users



### IMPORTANT

The GDPR functions access administration functions for this purpose. As a result, they need to be assigned to a user group which is authorised to access Administration.

✓ LSM open.

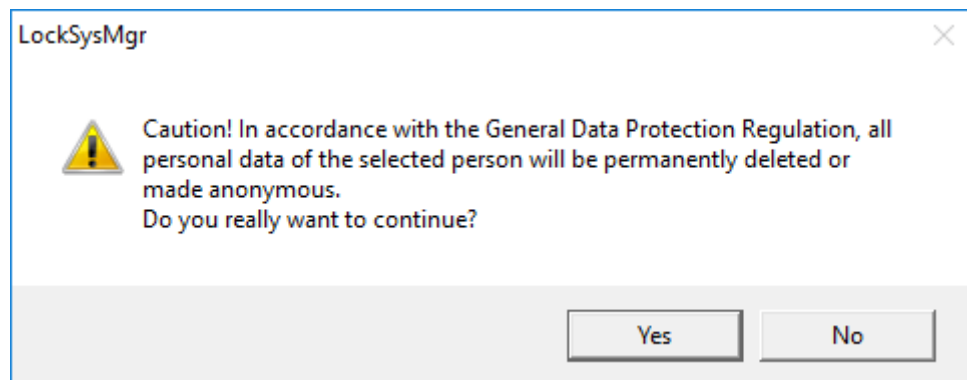
1. Use | Options | to select the **GDPR functions** item.

↳ The "GDPR functions" window will open.

2. Highlight the entry for the user whose data needs to be erased in the "Users" section.

3. Click on the **Permanently delete personal data** button in the "Users" section.

↳ The "LockSysMgr" window will open.



4. Click on the **Yes** button.

↳ The highlighted user's personal data is erased or anonymised.

## 1.10 Add PIN code Keypad

A PIN code keypad cannot be operated in pure G2 locking systems. The three user PINs act in the same way as G1 transponders.

### 1.10.1 Configure PIN code Keypad

#### 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-entering the new master PIN



#### IMPORTANT

The master PIN is essential for using 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. *Anyone who knows the master PIN can open or block PIN code Keypad locking devices by creating new user PINs themselves.*

#### Programming a user PIN

You can issue up to three user PINs for a PIN code Keypad. The user PIN can 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 user PIN length – e.g. 4 for a 4-digit user PIN
5. Enter User PIN

Repeat the process to programme other user PINs into the PIN code Keypad.

#### 1.10.2 Add PIN code Keypad to the locking plan

You **must** make a new entry for each user PIN.

1. Select *Edit / New transponder* from the menu bar.
2. Select the "G1 PinCode" entry in Type from the drop-down list and complete the other information.
  - ↳ The entry can be edited in detail in the same way as a transponder at a later point in time.
3. Select *Save & continue*
4. Select *End*

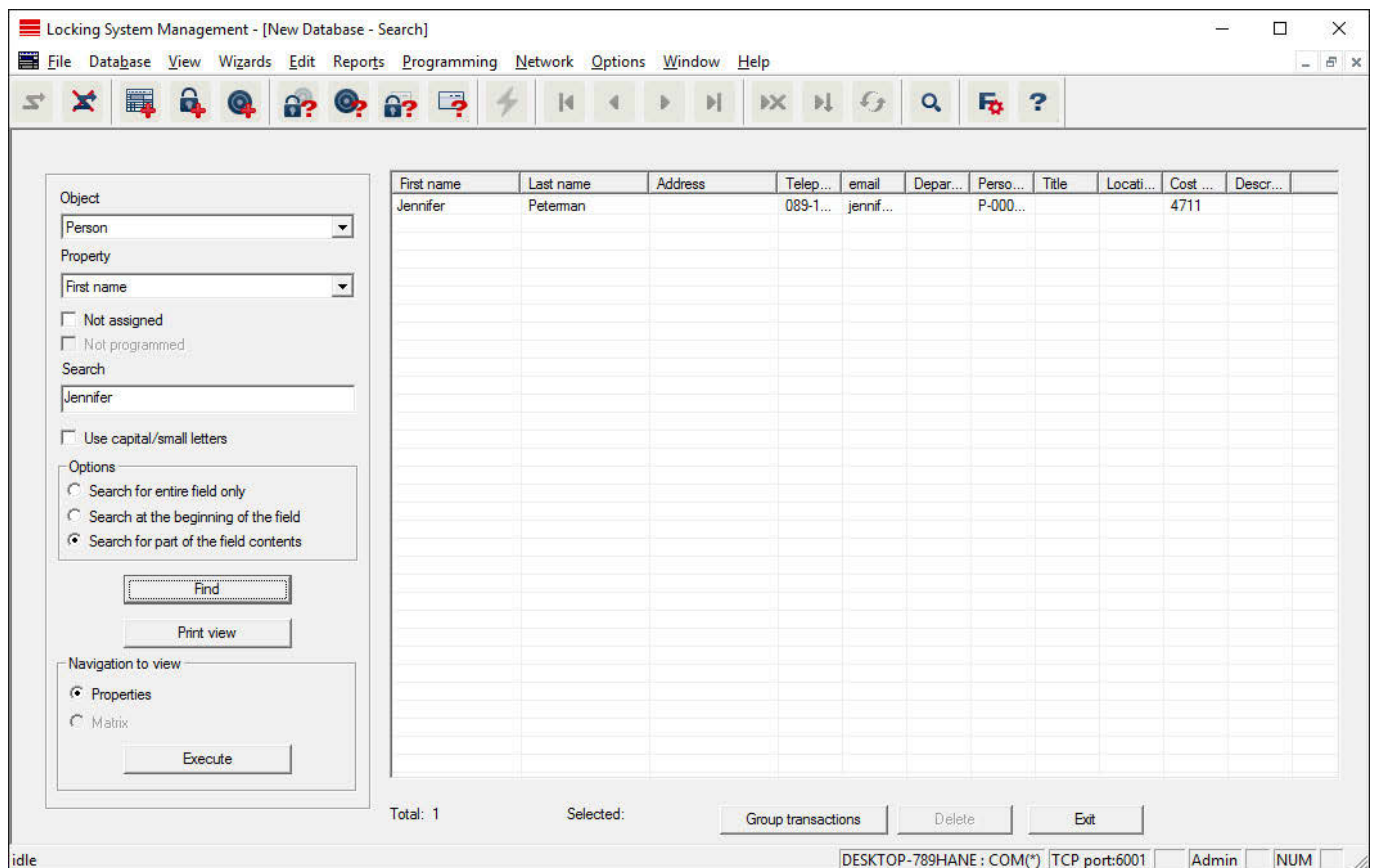
#### 1.10.3 Programme PIN code Keypad

1. LSM: right-click on the transponder/PIN code in the locking plan and select *Programme*.
  - ↳ The 'Programme transponder' window opens.
2. PIN code Keypad: Enter 0 0 + master PIN
3. LSM: Select *Programme*.
  - ↳ The programming process starts.
4. PIN code Keypad: Press user PIN, e.g. 1 for User PIN 1/ Internal Transponder 1, as soon as LSM displays the instruction 'Press the transponder button briefly once now'.
  - ↳ The programming process is now complete.

Repeat the process to programme other user PINs into the locking plan.

### 1.11 Search matrix

The search enables you to search easily for different items, such as a specific door or a specific transponder.



✓ Elements have already been added to the locking system, which you can search for.

1. Click on the magnifier icon in the icon bar.
2. Select the object that you wish to look for, such as persons, transponders, doors or locking devices.
3. Select a characteristic of the object that you are looking for, such as a last name or first name.
4. Enter a search term into the search field.
5. Click on the "Search" button to start the search process.

## 1.12 Execute group actions

Settings for a number of components can be made in just one single step. In this example, the properties of several G2 locking devices (*e.g. enable access control*) are to be changed all at once.

1. Click on the magnifier icon in the icon bar.
2. Search for all "Locking device"-type objects, for example.
  - ➡ No details need to be added in the "Search" field when searching for all locking devices.
3. Select a number of locking devices by filtering by type or area.

4. Click on the "Group actions" button.
  - ↳ If only G2 locking devices were selected in the preceding step, the correct parameters (*"Configuration changes to G2 locking devices" and "G2 locking cylinders active/hybrid"*) have already been selected.
5. Press on "Execute" button to start the changes to the selected locking devices.
6. Make the changes as you wish.
7. Click on the "Finish" button to save the new settings.



#### IMPORTANT

This process allows you to change many settings quickly and easily. Take into account that each changed component must be reprogrammed.

### 1.13 Programme transponder

- ✓ A transponder has been added to the locking system and is visible in the matrix.
1. Right-click on the transponder concerned.
  2. Click on Programme.
  3. Follow the instructions in the LSM software.

*Ensure that you select the right programming device.*

You can use the "TIDs to deactivate" button to open a list from which you can select one or two transponder IDs which are to be deactivated (see *Replace defective, lost or stolen transponders* [▶ 17]).



#### IMPORTANT

##### Automatically recognise G2 cards

It is not always possible to distinguish between cards as ID media. If there are a number of cards, the card which is to be programmed now needs to be read first to select the right card to be programmed in LSM. This step is omitted if the "Automatically recognise G2 card" box is checked. If LSM already knows the card, its data record is selected and programmed automatically.

### 1.14 Programme locking device

- ✓ A locking device has been added to the locking system and is visible in the matrix.
1. Right-click on the locking device concerned.

2. Click on Programme.
3. Follow the instructions in the LSM software.

*Ensure that you select the right programming device.*



#### IMPORTANT

Only one locking device may be near the programming device at any time.

### 1.15 Define time zone plan (with public holidays and company holidays)




#### IMPORTANT

##### Different times for G2 locks

The internal time unit of the G2 locks has a technical tolerance of up to  $\pm 15$  minutes per year.

It is recommended to apply time zone plans to entire areas and transponder groups. However, it is also possible to link time zone plans directly with locking devices and transponders.

- ✓ Locking devices (or areas) and transponders (or transponder groups) have already been created.
1. Click on *Edit/Time zone plan* in the menu bar.
    - ↳ An "empty time zone plan" will open up. If an existing time zone plan is displayed, click on the "New" button to create a new, empty time zone plan.
  2. Fill out the "Name" and "Description" fields.
  3. Select a public holiday list for your region if required. This is how to proceed if you wish to define one-time company holidays:
    - ↳ Click on the "... field" next to the holiday day drop-down selection.
    - ↳ Click on the "New holiday day" button.
    - ↳ Assign a name: e.g. "Company holiday 2017"
    - ↳ Newly defined holidays may contain a time period. The "Leave" field must be activated for this purpose. You can then enter a time period (From - To).
    - ↳ Select how the new holiday day should be treated: e.g. as "Sunday".
    - ↳ Click on the "Apply" button and then on the "Finish" button.
    - ↳ Click on the "Holiday administration" button.
    - ↳ Use the "Add" button in the holidays list (*in the right-hand column*) to add the newly created holiday (*in the left-hand column*).
    - ↳ Click on the "OK" button and then on the "Finish" button to return to the main time zone plan menu.

4. Select a group in the table and edit the weekly schedule for the group.
  - ↳ A blue bar indicates an authorisation for this time period.
  - ↳ You can click on fields individually or select them together.
  - ↳ Each time that you click on a field or area, you reverse the authorisation status.
  - ↳ 
5. Click on the "Apply" button.
6. Click on the "Finish" button.

Assign the time zone plan to an area:

1. Right-click on the area to which you wish to assign the time plan.
2. Select "Properties".
3. Select the corresponding time zone plan from the drop-down list in "Time zone".
4. Click on the "Apply" button.
5. Click on the "Finish" button.

*It is also possible to assign the time zone plan to a locking device directly.*

Assign a transponder group to the time group:

1. Right-click on the transponder group which is to be assigned to the time group.
2. Select "Properties".
3. Select the corresponding time group from the drop-down list in "Time zone group".
4. Click on the "Apply" button.
5. Click on the "Finish" button.

*It is also possible to assign the time group directly to a transponder.*

## 1.16 Resetting components

All SimonsVoss components can be reset at any time. You can even reset SimonsVoss components which do not belong to the locking system. In such a case, you need the corresponding locking system password.

Resetting components is an effective solution in many scenarios. It is advisable to reset and reprogramme the components in question particularly if they may not be functioning correctly.

1. Use *Programming/Read components* to read the components concerned.
2. Select the "Reset" button to start the reset process.



3. Follow the instructions in the LSM software.
  - ↳ If necessary, you will be requested to enter the locking system password or select the dataset to be deleted.

### 1.17 Replace defective locking device

Locking devices may become damaged or contain a defect.

Proceed as follows to replace a defective locking device with a new one:

1. Remove the defective locking device from the door.
  - ↳ It may be difficult to remove a cylinder from a closed door. If necessary, ask the specialist who installed the SimonsVoss products for advice.
2. Acquire a replacement locking device.
  - ↳ Double-click on the defective locking device in the LSM software to find all details on the locking device in the "Features" tab.
3. Carry out a software reset on the locking device in the LSM software.
  - ↳ Double-click on the defective locking device to open the "Configuration/Data" button, where you will see the "Software reset" button.
  - ↳ Once the software reset is complete, the software indicates a programming requirement for the defective locking device.
4. Carry out a programming process on the replacement locking device.
5. Fit the replacement locking device into the door and check that it functions correctly.



#### IMPORTANT

If a fault or error occurs, first try to reset the locking device itself by implementing a readout. After resetting the locking device, you can then possibly reprogramme it.



#### IMPORTANT

You must reset defective locking devices if at all possible before sending them to a retailer or SimonsVoss Technologies GmbH.

### 1.18 Replace defective, lost or stolen transponders

Transponders may get lost, stolen or damaged at some point. Whatever the case, the old transponder needs to be reset in the locking plan and a replacement transponder needs to be created.



### IMPORTANT

For security reasons, the deleted transponder's authorisations must be removed from all locking devices. You can do this by reprogramming all locking devices.

Proceed as follows to replace an "old" transponder with a new, non-programmed transponder.

1. Acquire a replacement transponder.
  - ↳ Double-click on the defective transponder in the LSM software to find all details on the transponder in the "Features" tab.
2. Right-click on the defective, lost or stolen transponder and select "Lost transponder".
  - ↳ The transponder concerned is prepared for blocking.
  - ↳ Indicate the reason why blocking is necessary. *When you select "Transponder lost/stolen", you can then programme a new transponder with the same authorisations directly afterwards. With the G2 protocol, this transponder blocks the lost transponder each time an authorised locking device is activated. However, all locking devices concerned still need to be reprogrammed.*
3. Implement all the newly appeared programming requirements on all components.

### Avoiding the need to reprogramme locking devices

Creating a new replacement transponder also entails a programming requirement for all locking devices. However, these special programming tasks can also be implemented directly with the new replacement transponder:

- ✓ The replacement transponder has been programmed correctly.
1. Activate the new replacement transponder on each locking device.
  2. Programme the new replacement transponder again. Activate the checkbox "Read deactivation acknowledgement/Battery warnings" in the "Programme transponder" window.
  3. Update the matrix. The programming requirement has now disappeared.

With LSM 3.4 SP2 and higher, it is possible to "inform" any number of transponders one or two other transponder IDs which need to be deactivated.

### Programme the TIDs to be disabled directly

The IDs to be disabled are saved on the transponder during the programming process.

- ✓ The transponder is physically available.
- ✓ The transponder's programming window is open.
- 1. Click on the "TIDs to deactivate" button.
  - ↳ The list will open.
- 2. Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.
- 3. Click on the **OK** button to confirm your input.
- 4. Continue with the programming.
- ↳ The checked TIDs will be saved to the transponder as TIDs to delete. When the transponder is authenticated on one of the locking devices concerned, the TIDs to be deleted are deactivated at the locking device.

#### **Add the TIDs to be blocked to the properties**

The IDs to be deactivated are saved on the transponder either during the next programming process or the next booking on a gateway.

- ✓ The transponder's properties window is open.
- 1. Change to the "Configuration" tab.
- 2. Click on the "TIDs to deactivate" button.
  - ↳ The list will open.
- 3. Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.
- 4. Click on the **OK** button to confirm your input.
- ↳ The checked TIDs are saved on the transponder either during the next programming process or the next booking on a gateway.

### **1.19 Check and evaluate the battery level in the locking devices**

There are different ways to query a locking device's battery level. In regular offline locking systems (and VN), the battery levels must first be transmitted to the LSM software before they can be evaluated in different ways.

#### **Transmitting battery levels to the LSM software**

##### **Fast & efficient: "collect" battery levels using a transponder**

1. Take a transponder which is authorised for use on all locking devices. Activate this transponder on each locking device.
2. Re-programme the transponder. Activate the checkbox "Read deactivation acknowledgement/Battery warnings" in the "Programme transponder" window.

#### **Importing battery levels by reading the locking device**

Select "Programme/read locking device" to read the required locking devices separately.

### **Transmitting battery levels to the LSM software using LSM Mobile**

You can use LSM Mobile to read battery levels directly or transmit them to the LSM software. Follow the instructions in the LSM Mobile manual. You will find it under Documents in the Support section on the SimonsVoss website ([www.simons-voss.com/en](http://www.simons-voss.com/en)).

### **Displaying battery levels**

#### **Basic procedure for all LSM versions:**

- ✓ The current battery warnings in the locking devices concerned have been transmitted to the LSM software.
- 1. Double-click on a locking device to display the locking device properties.
- 2. Select the "Status" tab.
- 3. The battery level will be displayed in the "Status at last readout".

### **Displaying battery warnings collectively in LSM BASIC Online and LSM BUSINESS:**

*Generate a list which displays all locking devices with battery warnings.*

- ✓ The current battery warnings in the locking devices concerned have been transmitted to the LSM software.
- 1. Select from the "Reports/Building structure" menu bar.
- 2. Select the "Locking devices with battery warnings".
- 3. Click on the "Display" button.

### **Displaying battery warnings automatically in LSM Business**

*Create a warning which displays battery warnings directly.*

- ✓ The current battery warnings in the locking devices concerned have been transmitted to the LSM software.
- 1. Selecting from the "Reports/Warnings" menu bar
- 2. Create a new warning using the "New" button.
- 3. Create the warning as you wish. Select "Locking device battery warning" as the type.
- 4. Do not forget to assign the locking devices concerned to this warning. The "Locking devices" field should not be empty.
- 5. Click on the "OK" button to confirm the new warning.

6. Click on the "Exit" button to close the dialogue.

## 1.20 Common locking level

Common locking levels can only be operated with active components. You cannot use passive card technology or smart tags for common locking levels.

### 1.20.1 Add common locking level

You must take the following into account for common locking levels:

- Common locking levels must use the same protocol generations.
- The red locking level should only be used for the fire service or other emergency services since it has been specifically optimised for this particular use.

In principle, a common locking level is used in the same way as any other locking system, e.g. using the "New locking system" button in the icon bar:

- Select any colour in "Use as common locking level".

The screenshot shows the 'Locking System Management - [SmartXChange - New locking system]' window. The interface includes a menu bar (File, Database, View, Wizards, Edit, Reports, Programming, Network, Options, Window, Help) and a toolbar with various icons. The main area contains the following fields and options:

- Name:** A text input field.
- Use as general locking level:** A dropdown menu currently set to 'Green'.
- Description:** A large text area.
- Protocol generation:** Radio buttons for G1, G2, and G2+G1 (selected). A checkbox for 'Automatically assign G1 TID' is checked.
- Inheritance in the hierarchy:** Checkboxes for 'Transponder group hierarchy' and 'Area hierarchy', both checked.
- Overlay Mode:** A checkbox that is currently unchecked.
- G1 Section:**
  - Old Password: [password field]
  - New Password (to protect file): [password field]
  - Confirm Password: [password field]
  - Quality: A color bar (orange to green) and '78 bits'.
- G2 Section:**
  - Old Password: [password field]
  - New Password: [password field]
  - Confirm Password: [password field]
  - Quality: A color bar (orange to green) and '98 bits'.
- Buttons:** 'Apply', 'Exit', and 'Help' at the bottom.

The status bar at the bottom shows 'idle', 'SANTABARBARA : COM3', 'TCP port:6000', 'Admin', and 'NUM'.

### 1.20.2 Link locking devices

- ✓ A common locking level has already been created.
- 1. Right-click on an area in the common locking level and select "Properties".
- 2. Select "Door management" button.
- 3. The right-hand table shows all locking devices in all locking systems in the project. Use the "Add" button to select the locking devices required.

[illegible]

### 1.20.3 Link transponders

*Transponders should only be linked to non-common locking levels.*

- ✓ Transponders or transponder groups have already been added.
- 1. Right-click on the transponder group and select "Properties".
- 2. Select the "Automatic" button in transponder allocation.

3. The right-hand table shows all transponders in all other locking systems in the project. Use the "Add" button to select the transponders required.

[illegible]

#### 1.20.4 Authorise transponders

As in each common locking level, selected transponder groups can also be authorised for all locking devices in the "red level" with just a few mouse clicks. This function is particularly suitable for fire service transponders.

- ✓ You have now already added a red common locking level.
- 1. Open red common locking system.
- 2. Create transponder group which should be authorised for all areas relevant for the fire service.
- 3. Click on the "Authorisations" button in the transponder group properties in Administration.
- 4. Use the checkboxes to select all the areas/locking devices required to grant access through all doors to the transponder group.

### 1.21 Create fire service transponders

- ✓ You have already created at least one locking system.
- 1. Create a new "red" common locking level, using *Edit/New locking system*, for example.
- 2. Add a new area, such as "All locking devices", and use "Door administration" to assign all the locking devices required to this area.
- 3. Add a new "Fire service" transponder group to the common locking level.
- 4. Click on the "Authorisations" button in the properties for the "Fire service" transponder group.
- 5. Enable the "All systems" checkbox to authorise this transponder group for all locking devices in general.
- 6. Click on the "OK" button to save the settings.
- 7. Add a new transponder – "Fire service transponder 1", for example – to the transponder group and programme it. *All locking devices also need to be reprogrammed. Note the new programming requirement which has now appeared.*

The "Fire service transponder 1" fire service transponder created in this step is authorised for all locking devices. Even deactivated locking devices can be opened in the red level, making it markedly different from "green" and "blue" levels.

### 1.22 Setting up DoorMonitoring components

The DoorMonitoring function is an add-on feature to display door statuses in the LSM software. SmartHandles and locking cylinders with the DoorMonitoring function are installed in the LSM software in exactly the same way as regular locking components.

- Add new DoorMonitoring locking cylinder: Select "G2 DoorMonitoring cylinder" as the locking device type from the drop-down list.
- Add new DoorMonitoring SmartHandle: Select "G2 DoorMonitoring SmartHandle" as the locking device type from the drop-down list.

#### Tab: Configuration/Data

Use the "Monitoring configuration" button to make further settings.

#### Tab: DoorMonitoring status

This tab shows the door's current status. The status is shown real time.



*A direct connection is required between the LSM software and locking components (e.g. via WaveNet) to ensure that this status display is always up to date. You will find more detailed information on setting up a WaveNet wireless network in the WaveNet manual.*

### 1.23 Programme using LSM Mobile

You can use LSM Mobile to carry out programming tasks directly on a locking device using mobile devices. This programming takes place as follows:

1. A list with components which indicate a programming requirement is exported to the LSM Mobile device from the LSM software, *either directly on the pocket PC or as a file for a notebook, netbook or tablet units*
2. LSM Mobile is launched on the mobile device. You can start the programming of components with the export from the LSM software.
3. The LSM software must then be informed which components have been programmed using LSM Mobile. This achieved using an import or synchronisation from LSM Mobile to the LSM software.

#### 1.23.1 With pocket PC/PDA



#### IMPORTANT

Programming with LSM Mobile will only work in the G1 protocol with a pocket PC or PDA.

This how you programme with the help of LSM Mobile:

- ✓ There are components in the LSM software which require programming.
  - ✓ Initial programming has already been completed on the components requiring programming.
  - ✓ LSM Mobile has been correctly installed on the mobile device. The version numbers are identical.
  - ✓ The SMARTCD.G2 programming device is charged and connected to the PDA via Bluetooth.
  - ✓ The pocket PC drivers have been correctly installed on the computer and a connection has been established.
1. Select *Programming/LSM Mobile/Export to LSM Mobile/LSM Mobile PDA*.
  2. Follow the instructions in the LSM software and transfer the programming tasks to the PDA.
  3. Launch LSM Mobile on the PDA and log on to the locking system concerned.

4. Use the programming device to carry out the programming processes on the components concerned.
5. Select *Programming/LSM Mobile/Import from LSM Mobile/LSM Mobile PDA*.
6. Follow the instructions in the LSM software and synchronize the programming tasks.

*The programming tasks have been completed using the PDA.*

*Synchronisation in the last step ensures that the programming flash icons indicating a programming requirement disappear from the LSM software.*

### **1.23.2 With laptop, netbook or tablet PC**

This how you programme with the help of LSM Mobile:

- ✓ There are components in the LSM software which require programming.
  - ✓ Initial programming has already been completed on the components requiring programming.
  - ✓ LSM Mobile has been correctly installed on the mobile device. The version numbers are identical.
  - ✓ The drivers have been correctly installed in the SMARTCD.G2 and SMARTCD.MP programming devices (depending on requirements).
1. Select *Programming/LSM Mobile/Export to LSM Mobile/LSM Mobile PC*.
  2. Follow the instructions in the LSM software and export the programming tasks in a file.
  3. Launch LSM Mobile on the mobile PC and import the file with the programming tasks into LSM Mobile.
  4. Follow the instructions in LSM Mobile.
  5. Use the programming device to carry out the programming processes on the components concerned.
  6. Export the status of the programming tasks.
  7. Select *Programming/LSM Mobile/Import from LSM Mobile/LSM Mobile PC*.
  8. Follow the instructions in the LSM software and import the file from LSM Mobile.

*The programming tasks have been completed using the external device.*

*The import in the last step ensures that the programming flash icons indicating a programming requirement disappear from the LSM software.*

## 1.24 Reset storage mode in G1 locking devices

If battery warnings are ignored in G1 locking devices, the locking devices concerned switch to storage mode. This prevents the batteries from being fully discharged. Storage mode can be terminated by reprogramming the locking device. The locking device must then be opened with an authorised transponder and the batteries replaced immediately.

## 1.25 Access administration

The reading of access and physical access lists can be greatly restricted to protect privacy. In LSM Basic, the "AdminAL" (Admin Access List) user is added as standard for this purpose. In LSM BUSINESS, you can add a suitable user manually; see *Administer users (BUSINESS)* [▶ 28].

*The following scenario is described in this section: Only an authorised person (e.g. Works Council logged on as the AdminAL) should be able to read access lists and physical access lists. The general locking system administrator is not given this right.*

### Configure AdminAL and permit reading of access lists

1. Use the "Admin" user name and your password to log on to your project.
2. Select "Edit/User group" to open user group administration.
3. Use the navigation arrow to scroll to the "Access lists administration" user group (or to any previously added user group in LSM Business).
4. Ensure that the "Access lists administration" and "Manage access lists" rights are activated in the "Role" section.
5. Click on the "Edit" field beneath "Role" section.
6. Activate the required locking systems in transponder groups and areas. If you have added areas or transponder groups, you must activate all required areas and transponder groups separately.
7. Click on the "OK" button to close the mask.
8. Confirm the settings that you made by pressing on the "Apply" and "Finish" buttons.
9. Select "Database/Log off" to log off from your current project.

### Remove rights to read access lists from Admin



#### IMPORTANT

The "Access lists administration" right must always be assigned to a user/user group and must not be withdrawn from both.

1. Use the "AdminAL" user name to log on to the project.
  - ↳ The default password in LSM BASIC is "system3060".
  - ↳ Change this password immediately.
2. Select "Edit/User group" to open user group administration.
3. Use the navigation arrow to scroll to the "Admin" user group.
4. Deactivate the "Access lists administration" and "Administer access lists" roles.
5. Confirm the settings that you made by pressing on the "Apply" and "Finish" buttons.
  - ↳ Configuration is now complete. Only the "AdminAL" user account may read or view access lists and physical access lists from now on.

## 1.26 Administer users (BUSINESS)

### Assign user to a user group

1. Click on "Edit/User group".
2. Use the navigation arrow to scroll to a user group (or use the "New" button to create a new user group).
3. Click on the "Edit" button.
4. Highlight the user that you require and use the "Add" button to assign them to the user group.
5. Click on the "OK" button to confirm the settings that you have made.
6. *Correct the roles if necessary.*
  - ↳ Click on the "Edit" field beneath "Role" section.
  - ↳ Activate the required locking systems in transponder groups and areas. If you have added areas or transponder groups, you must activate all required areas and transponder groups separately.
  - ↳ Click on the "OK" button to close the mask.
7. Confirm the settings that you made by pressing on the "Apply" and "Finish" buttons.

### Creating a new user

1. Click on "Edit/User".
2. Click on the "New" button to add a new user.
3. Issue a new user name and enter a password.
4. Confirm the settings that you made by pressing on the "Apply" and "Finish" buttons.

## 1.27 Card management

Below you can see the different card types and the distribution of memory in connection with the SimonsVoss locking system.

### ATTENTION

#### MIFARE DESFire recommended

Compared to MIFARE Classic, MIFARE DESFire uses microcontroller-based encryption based on AES-128, which has been further developed to meet increased security requirements.

- SimonsVoss recommends the use of transponders or MIFARE DESFire products.



### IMPORTANT

#### Different templates for AX products

If you want to use MIFARE products for SimonsVoss AX products, the templates used for writing and reading must be identical.

#### 1.27.1 Change configuration


You have two options for using cards.

- You can use cards that have already been used.
- You can use new cards.

In both cases, enter the card type, the configuration and, if necessary, the sectors to be described (see [Overview \[▶ 31\]](#)).

#### Configuring the card

- ✓ LSM open.

1. Switch to the locking system whose card management you want to change.
2. Click on the button to open the properties of the locking system .

3. Change to the tab [G2 card management].

NameLocksDoorsTransponderTransponder groupsAreasPasswordSpecial TIDSPIN-Code TerminalCard management G1G2 card management

Locking system: HIMYM

Level: Standard

Card type: Mifare Classic

Configuration: MC1000L\_AV

Memory space needed: 528

Bytes

Lock IDs: 128-1127

in card profile

Access instances in the log: 19

Virtual network: OK

Parameter:

Name	Value	Description
SectList	2,3,4,5,6,7,8,9,10,11,12,13,14,15	Sector List
TransportSectorT...	.....	Transport Settings

Print view

- 4. In the dropdown menu ▼ Card type select your card type.
- 5. In the dropdown menu ▼ Configuration select your configuration.
- 6. If necessary, enter further parameters such as sectors (e.g: 2,3,4,5,6,7,8,9,10,11,12,13,14,15).

Name	Value	Description	
SectList	2,3,4,5,6,7,8,9,10,11,12,13,14,15	Sector List	
TransportSectorT...	.....	Transport Settings	

- 7. Click on the Apply button.
- ➡ You have changed the configuration.

### 1.27.2 Overview

	MIFARE DESFire		MIFARE DESFire Predefined	MIFARE DESFire Predefined DB1
MDBasic	✓		✓	✗
MD1200L	✓		✓	✗
MD3800L	✓		✓	✗
MD2500L_AV	✓		✓	✗
MD4000L_AV	✓		✓	✗
MD10000L_AV	✓		✓	✗
MD32000L_AV	✓		✓	✗
MD2400L_AV	✗		✗	✓
MD3650L_AV	✗		✗	✓

	MIFARE Classic	MIFARE Classic Pre- defined A	MIFARE Classic Pre- defined B	MIFARE Classic + DESFire	MIFARE Plus S/X
MCBasic	✓	✓	✓	✗	✓
MC1200L	✓	✓	✓	✗	✓
MC3800L	✓	✓	✓	✗	✓
MC1000L_AV	✗	✓	✓	✗	✓
MC2400L_A V	✗	✓	✓	✗	✓
MC8000L_A V	✗	✓	✓	✗	✓
MBasic	✗	✗	✗	✓	✗
M1200L	✗	✗	✗	✓	✗
M3800L	✗	✗	✗	✓	✗
M1000L_AV	✗	✗	✗	✓	✗
M4000L_AV	✗	✗	✗	✓	✗
M8000L_AV	✗	✗	✗	✓	✗
M10000L_AV	✗	✗	✗	✓	✗

	G1/G2	Lock-IDs	Number of locks	Access list	Sectors	Required storage space	Virtual network
MCBasic	G1	✗	✗	✗	2-15	48	✗
MC1200L	G2	128-1327	1200	✗	2-15	192	✗

	G1/G2	Lock-IDs	Number of locks	Access list	Sectors	Required storage space	Virtual network
MC3800L	G2	128-3927	3800	✗	2-15	528	✗
MC1000L_AV	G2	128-1127	1000	19	2-15	528	✓
MC2400L_AV	G2	128-2527	2400	70	2-15 + 31-39	900	✓
MC8000L_AV	G2	128-8127	8000	125	2-15 + 31-39	2048	✓
MBasic	G1	✗	✗	✗	2-15	48	✗
M1200L	G2	128-1327	1200	✗	2-15	192	✗
M3800L	G2	128-3927	3800	✗	2-15	528	✗
M1000L_AV	G2	128-1127	1000	16	2-15	528	✓
M4000L_AV	G2	128-4127	4000	100	2-15 + 31-39	1600	✓
M8000L_AV	G2	128-8127	8000	124	2-15 + 31-39	2048	✓
M10000L_AV	G2	128-10127	10000	225	2-15 + 31-39	3048	✓
MDBasic	G1	✗	✗	✗	2-15	48	✗
MD1200L	G2	128-1327	1200	✗	2-15	192	✗
MD3800L	G2	128-3927	3800	✗	n.a. (DES-Fire)	528	✗
MD2500L_AV	G2	128-2627	2500	58	n.a. (DES-Fire)	1024	✓
MD4000L_AV	G2	128-4127	4000	100	n.a. (DES-Fire)	1600	✓
MD1000L_AV	G2	128-10127	10000	225	n.a. (DES-Fire)	3048	✓
MD3200L_AV	G2	128-32127	32000	470	n.a. (DES-Fire)	7000	✓
MD2400L_AV	G2	128-2527	2400	34	n.a. (DES-Fire)	830	✓
MD3650L_AV	G2	128-3777	3650	2	n.a. (DES-Fire)	830	✓



## 2 Performing standard WaveNet-based tasks in LSM Business

This example shows the key steps in setting up and administrating a WaveNet radio network in LSM Business. The examples are based on specific installations and are meant to help you become familiar with topics related to WaveNet.

### 2.1 Creating a WaveNet radio network and incorporating a locking device

This example describes how you can create a WaveNet radio network from scratch. The aim is to address a locking device via a RouterNode2.

#### 2.1.1 Preparing the LSM software

Note that the LSM software required to network SimonsVoss locking components must be properly installed and a corresponding network module licensed.

1. Install the CommNode server and ensure that the service has been started.
2. Install the current version of WaveNet Manager. (See Installation)
3. Open the LSM software and select "Network/WaveNet Manager".
  - ↳ Enter the WaveNet Manager installation directory and select a directory for the output file.
  - ↳ Use the "Launch" button to open WaveNet Manager.
4. Provide a password to increase your network's security.
  - ↳ WaveNet Manager launches and the settings are saved for the future. Exit WaveNet Manager to make further settings.

#### 2.1.2 Initial programming of the locking components

Before locking devices can be incorporated into the network, they first need to be programmed.

##### 2.1.2.1 Add new locking device

- ✓ A locking system has already been added.
1. Select *Edit/New locking device*.
  2. Fill out all attributes and use the "Configuration" button to make further settings if necessary.
  3. Click on the "Save & next" button.
  4. Click on the "Finish" button.

#### 2.1.2.2 Programme locking device

- ✓ A locking device has been added to the locking system and is visible in the matrix.

1. Right-click on the locking device concerned.
2. Click on Programme.
3. Follow the instructions in the LSM software.

*Ensure that you select the right programming device.*



#### IMPORTANT

Only one locking device may be near the programming device at any time.

#### 2.1.3 Preparing hardware

The current RouterNode2 is put into operation quickly and easily. Connect the RouterNode2 as described in the supplied quick guide. The RouterNode2 is pre-configured in the factory, so that it obtains its IP address from a DHCP server. You can quickly identify this IP address using the OAM tool (*available free of charge under Informative Material/ Software Downloads/Drivers in the Support section*).



#### IMPORTANT

Standard settings:

IP address: 192,168,100,100

User name: SimonsVoss | Password: SimonsVoss

If the locking device has not been equipped with a LockNode (LN.I) in the factory, you need to retrofit one with appropriate accessories.



#### IMPORTANT

Note down the RouterNode2's IP address and the locking device's chip ID after you have correctly prepared the hardware.

#### 2.1.4 Creating communication nodes

The communication node forms the interface between the CommNode server and the LSM software. You must launch the LSM software using an administrator account to add the configuration XMLs.

1. Open the LSM software.

2. Select "Network/Communication nodes".
3. Add "Name", "Computer name" and "Description",
  - ↳ e.g. *WaveNet\_Network\_123; Computer\_BS21; communication node for the WaveNet radio network 123*
4. Click on the "Config files" button
5. Ensure that the path links to the CommNode server's installation directory and click on the "OK" button.
6. Press "No" to reset the prompt and confirm your selection by clicking on "OK". *The three configuration XMLs (appcfg, msgcfg and netcfg) must be located directly in the CommNode server's installation directory.*
7. Click on the "Apply" button to save your settings.
8. Click on the "OK" button to close the prompt.
9. Click on the "Exit" button to close the dialogue.

## 2.1.5 Setting up the network and importing into LSM

### 2.1.5.1 Adding the WaveNet configuration

If all requisites have been met, you can start to configure the network:

- ✓ LSM has been installed correctly and a network module is licensed.
  - ✓ The CommNode server has been installed and the service launched.
  - ✓ The CommNode server's configuration files have been created.
  - ✓ The current version of WaveNet Manager has been installed.
  - ✓ A communication node has been created in the LSM software.
  - ✓ Initial programming of the locking device to be networked has been successfully completed.
  - ✓ RouterNode2 can be reached via the network and you know its IP address.
  - ✓ The programmed locking device features an installed LockNode and you know its chip ID.
1. Select "Network/WaveNet network" and press the "Launch" button to open WaveNet Manager.
  2. Enter the password.
  3. Right-click on "WaveNet\_xx\_x".
  4. Initialize the RouterNode2 first, e.g. using the option "Add: IP or USB router".
    - ↳ Follow the dialogue instructions and incorporate the RouterNode2 into your WaveNet radio network using its IP address.
  5. Initialize the locking device's LockNode by right-clicking on the newly added RouterNode2 and select the "Search by chip ID" option.
    - ↳ Follow the dialogue instructions and use the associated chip ID to assign the locking device or its LockNode to the RouterNode2.

6. Click on the "Save", "Exit" and "Yes" buttons one after another to close WaveNet Manager.
7. Import the new settings and assign them to the corresponding communication node.

#### 2.1.5.2 Transmitting the WaveNet configuration

The new settings still need to be transmitted to the CommNode server:

1. Select "Network/Communication nodes".
2. Select the RouterNode2 from the list of connections and click on the "Transmit" button.
3. Click on the "Apply" button to save your settings.
4. Click on the "Exit" button to close the dialogue.

#### 2.1.5.3 Assigning a locking device's LockNode

The initialized LockNode needs to be linked to a locking device. This is easiest to do using a collective command, particularly if there is more than one LockNode:

1. Select "Network/Collective commands/WaveNet nodes".
2. Select all LockNodes (*WNNode\_xxxx*) which have not been assigned yet. *Non-assigned LockNodes have no entry in the "Door" column.*
3. Click on the "Configure automatically" button.  
↳ The automatic configuration will start immediately.
4. Click on the "Exit" button to close the dialogue.

#### 2.1.5.4 Testing the WaveNet configuration

You can select "Right-click/Programme" to re-programme the locking device via the network at any time to test networking quickly. The network is working properly if programming is successful.

## 2.2 Putting the DoorMonitoring locking cylinder into operation

This example shows what settings need to be made to set up a DoorMonitoring locking cylinder. You will find the prerequisites for this process in "[Creating a WaveNet radio network and incorporating a locking device \[▶ 33\]](#)".

### 2.2.1 Adding a DoorMonitoring locking cylinder

The DM locking cylinder must first be added and programmed correctly in LSM.

1. Select the "Add locking device" button to launch the dialogue for a new locking device.

2. Select "G2 DoorMonitoring cylinder" as the locking device type and add all other information as you wish.
3. Exit the dialogue to add the locking device to the matrix.
4. Double-click to open the locking device properties and select the "Configuration/Data" tab.
5. Make the settings for the locking device's target status as you wish.
6. Click on the "Monitoring configuration" button and make the following settings (as a minimum):
  - ↳ Fastening screw sampling interval: e.g. 5 seconds. In this case, the door status is polled every 5 seconds.
  - ↳ Number of turns in lock: e.g. 1 turn This setting is important to identify the bolt status correctly.
7. Save the settings and return to the matrix.
8. Use a suitable programming device to carry out initial programming.

### 2.2.2 Incorporating a DoorMonitoring cylinder into the network

This is how you incorporate the DM cylinder into the WaveNet network:

- ✓ WaveNet Manager has already been set up.
  - ✓ The router to which the new locking device is to be assigned is already set up and "online".
  - ✓ A LockNode is correctly mounted on the DM locking cylinder and you know the chip ID.
1. Start WaveNet Manager.
  2. Initialize the locking device's LockNode by right-clicking on the newly added router and select the "Search by chip ID" option.
    - ↳ Follow the dialogue instructions and use the associated chip ID to assign the locking device or its LockNode to the RouterNode2.
  3. Right-click on the newly added DM LockNode.
  4. Activate the "I/O configuration" check box and click on the "OK" button.
  5. Activate the "Send all events to I/O router" check box and click on the "OK" button.
  6. Click on the "Save", "Exit" and "Yes" buttons one after another to close WaveNet Manager.
  7. Import the new settings and assign them to the corresponding communication node.

### 2.2.3 Transmitting the WaveNet configuration

The new settings still need to be transmitted to the CommNode server:

1. Select "Network/Communication nodes".
2. Select the RouterNode2 from the list of connections and click on the "Transmit" button.

3. Click on the "Apply" button to save your settings.
4. Click on the "Exit" button to close the dialogue.

#### 2.2.4 Assigning a locking device's LockNode

The initialized LockNode needs to be linked to a locking device. This is easiest to do using a collective command, particularly if there is more than one LockNode:

1. Select "Network/Collective commands/WaveNet nodes".
2. Select all LockNodes (*WNNode\_xxxx*) which have not been assigned yet. *Non-assigned LockNodes have no entry in the "Door" column.*
3. Click on the "Configure automatically" button.
  - ↳ The automatic configuration will start immediately.
4. Click on the "Exit" button to close the dialogue.

#### 2.2.5 Activating the locking device's input events

You need to make additional settings to ensure that door statuses are displayed correctly in the LSM software:

1. Selecting "Network/Collective commands/WaveNet nodes"
2. Select the DoorMonitoring cylinder (*or any locking cylinder which is to relay events*).
3. Click on the "Activate input events" button.
  - ↳ Programming is started immediately.
4. Click on the "Exit" button as soon as all locking devices have been programmed.

### 2.3 Setting up a RingCast

The description below tells you how to configure a RingCast. A RingCast allows a RouterNode2 input event to be relayed to other RouterNode2s in the same WaveNet radio network at the same time. In this example, an emergency release is to be implemented on locking devices. All connected locking devices should open as soon as a fire alarm system triggers Input 1 on a RouterNode2. Each locking device will then remain open until they receive an explicit remote opening command.

*Obviously, a RingCast can also be used to perform other tasks such a block lock function, remote opening and gunman attack function.*

This example requires a configured WaveNet radio network with two RouterNode2s. A locking device is connected to each RouterNode2. All locking devices should be opened immediately as soon as Input 1 on a RouterNode2 is actuated briefly. This gives people access to all rooms, so that they can seek protection from fire or smoke.



### IMPORTANT

If RouterNode2s are networked using Ethernet, RingCast is only supported by models which were supplied from about 2017. A RouterNode2 tries to establish an Ethernet connection to another RouterNode2 but fails. It then tries to establish the new connection wirelessly. The radio communication range is up to 30 m. This depends on the surroundings, so it cannot be guaranteed.

## 2.3.1 Preparing RouterNode for RingCast



### IMPORTANT

#### Firmware dependent availability of RingCast for RouterNodes

RingCast support is firmware dependent (see Firmware information).

- If necessary, update the firmware (see Updating firmware).

Prepare the RouterNodes for the RingCast:

- ✓ In the Wavenet radio network, at least two different RingCast-capable RouterNodes are configured and "online" (see Firmware information).
- ✓ At least one locking device is assigned to each RouterNode of the planned RingCast. Both locking devices are "online".

1. Open the WaveNet Manager.
2. Right-click on the first RouterNode 2.
  - ↳ Window "Administration" opens.



3. Select the option ☒ I/O configuration.
4. Click on the button **OK**.
  - ↳ Window "Administration" closes.
  - ↳ Window "I/O configuration" opens.
5. Optional: For example, for ▼ **Output 1** "Input receipt static", to be able to control a signal device during deactivation.
6. In the drop-down menu ▼ **Input** select the desired entry of the corresponding response (see RouterNode: Digital input).
7. In the drop-down menu ▼ **Delay [s]** select the entry "RingCast".
8. Click on the button **Select LN**.

9. Check whether all required LockNodes are selected. *(When the I/O configuration of the router is set up for the first time, all LockNodes are included.)*
10. Select your protocol generation from the drop-down menu ▼ **Protocol generation**



### IMPORTANT

#### Protocol generation in the LSM

The log generation is displayed in the LSM in the locking system properties on the tab page [Name] in the area "Protocol generation".

11. Enter the locking system password.
12. Click on the **OK** button.
13. Make the same settings on the other RouterNodes 2 as well.

### 2.3.2 Adding a RingCast



### IMPORTANT

#### Recalculating the RingCast

If you replace or delete a RouterNode in the RingCast or change its RingCast-relevant IO configuration, the RingCast is automatically recalculated after saving the changes and confirming the request.

- ✓ WaveNet Manager open (see Start).
- ✓ RouterNodes and LockNodes connected to power supply.
- ✓ Imported RouterNodes and LockNodes into WaveNet topology (see Finding and adding devices).
- ✓ RouterNodes prepared for RingCast (see [Preparing RouterNode for RingCast \[▶ 39\]](#)).

1. Right-click on the WaveNet entry in which you want to create a RingCast.
  - ↳ Window "Administration" opens.



2. Select the option ☒ RingCast.
3. Click on the button **OK**.
  - ↳ Window "Administration" closes.



→ Window "Edit radio domains" opens.



4. In the drop-down menu ▼ **Select domain** select an entry, for which, at ▼ **Delay [s]** you have selected the "RingCast".



→ In the field "selected routers" all RouterNode2 are shown, from which in this entry in ▼ **Delay [s]** you have selected the entry "RingCast" (=Domain).

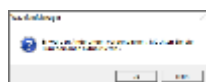


5. Click on the button **Save**.

6. Click on the button **Exit**.

→ Window "Edit radio domains" closes.

→ Window "WaveNetManager" opens.

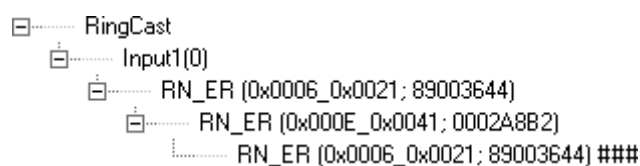


7. Click on the button **Yes**.

→ Window "WaveNetManager" closes.

→ Changes will be updated.

→ The RingCast is created and is visible in the WaveNet Manager after a brief period of time.



The settings have already been written to RouterNode2. Save the new settings and exit the WaveNet Manager.

### 2.3.3 RingCast function test

The settings made are effective immediately. The RingCast has no self-test function.



#### WARNING

##### Impairment or failure of protective functions due to changed conditions

The activation of the protection functions in RingCast is based on wireless connections and Ethernet connections. Especially wireless connections can be affected by changing environmental conditions (Radio network). This also influences the activation of the protective functions in the RingCast; and the safety of persons and property, which, for instance, are additionally protected by the protective functions in the RingCast, may be at risk.

1. Test the protective functions at least once a month (see [RingCast function test \[► 42\]](#)).
2. If necessary, also observe other directives or ordinances that are relevant for your locking system.



#### WARNING

##### Changing the sequence of emergency functions due to malfunctions

SimonsVoss and "Made in Germany" stand for maximum safety and reliability. In individual cases, however, malfunctions of your equipment cannot be ruled out. This may jeopardise the safety of persons and property that are additionally protected by the protective functions in the RingCast.

1. Test your devices at least once a month (see Device function test).
2. Test the protective functions at least once a month (see [RingCast function test \[► 42\]](#)).

Switch the corresponding input on the initiator and check:

- whether the locking devices are responding as required (see also RouterNode: Digital input).
- whether the output set on the RouterNode indicates the acknowledgement as required by switching (see also RouterNode: Digital output).



### IMPORTANT

#### Permanent emergency opening

A fire can damage the input cable or other parts. This would cause the locking devices to close again even though there is a fire. Persons could be locked up in the fire zone and rescue units could be prevented from entering.

Therefore, all locking devices stay in the emergency opening state (and thus passable) until an explicit remote opening command closes the locking devices again.

#### Test with central output router



### IMPORTANT

#### Central output router in RingCast with R/CR router nodes

The central output router receives the input acknowledgement of the participating router nodes exclusively via an Ethernet connection. The central output router therefore ignores the status of router nodes that are not Ethernet router nodes (.ER). If you are using the central output router and your RingCast also contains router nodes without an Ethernet interface, the central output router's input acknowledgement only means that all locking devices assigned to an Ethernet router node have received the command.

- Check the status of other router nodes (R/CR) independently of the central output router manually (see Test reachability (LSM) and RouterNodes or IO Status and LockNode responsiveness).

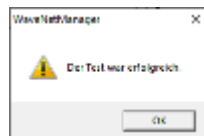
The use of a central output router (see Central output router) simplifies the testing of the RingCast considerably. Switch the corresponding input on the initiator and check whether the central output router issues an input acknowledgement or switches the corresponding output. If the output switches, then all locking devices have received the command. If the output does not switch, check which router nodes have caused problems:

- ✓ WaveNet Manager open (see Start).
- 1. Right-click on the entry of the RingCast you want to test.
- 2. In the drop-down menu ▼ **Select domain** select the input, whose RingCast you would like to test.
  - ➞ Window "Edit radio domains" opens.



3. Click on the button **Status**.

→ RingCast is being tested.



The RingCast was able to address all  
locking devices.

The RingCast could not be completed. Possible causes (see also Central output router):

- ❑ One or more router nodes did not receive the data packet.
- ❑ One or more RouterNodes have not reached one or more LockNodes.
- ❑ Ethernet connection to one or more RouterNodes is interrupted. The RouterNodes could have received the data packet remotely, but could no longer return their input acknowledgements due to the interrupted Ethernet connection.

1. Check the availability of the named RouterNodes (see RouterNodes and Test reachability (LSM)).
2. Check the accessibility of the LockNodes (see LockNodes and Test reachability (LSM)).
3. Check the last responses of the LockNodes (see IO Status and LockNode responsiveness)).

## 2.4 Setting up event management

Networking locking devices via a RouterNode2 brings many advantages. One decisive advantage is the permanent communication between the RouterNode2 and the locking device.

In this example, a pre-defined email is to be sent from the LSM software as soon as a transponder is activated on a specified locking device at night.

The following prerequisites need to be fulfilled for this requirement:

- A WaveNet radio network is set up as in the example *Creating a WaveNet radio network and incorporating a locking device* [▶ 33].
- Forwarding of locking device events has also been activated as in *Activating the locking device's input events* [▶ 38].

### 2.4.1 Setting up an email server

A rudimentary email client is set up to send emails in the LSM software. An own email account which supports SMTP format is required to forward emails.

1. Select "Network/Email notifications"
2. Click on the "Email" button.
3. Enter all SMTP settings for your email provider.
4. Click on the "OK" button.
5. Click on the "OK" button.

### 2.4.2 Setting up Task services

1. Select "Network/Task manager".
2. Select your communication node under Task services.
3. Click on the "Apply" button.
4. Click on the "Finish" button.

### 2.4.3 Forwarding input events via the RouterNode2

If events (*e.g. a transponder makes a booking on a networked locking device*) are to be forwarded to the CommNode server via the RouterNode2, this function needs to be activated in the router's I/O configuration.

1. Open WaveNet Manager.
2. Right-click the router and select "I/O configuration".
3. Select the "All LN events" option in the "Report events to management system" drop-down list.
4. Press OK to confirm and exit WaveNet Manager.

#### 2.4.4 Forward input events via the SREL3 ADV system

The SREL3 ADV system allows input entries to be forwarded to LSM.

##### 2.4.4.1 Evaluating controller inputs

The digital inputs on the SREL3 ADV system controller can be forwarded to LSM, where they may trigger actions.

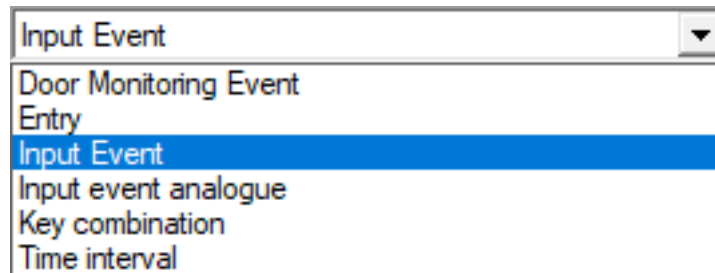
#### Adding an event

If you wish to use LSM or SmartSurveil (see SmartSurveil) to evaluate an input, you first need to create the corresponding input as an event in LSM. Only then will changes to the input also be saved in the LSM database.

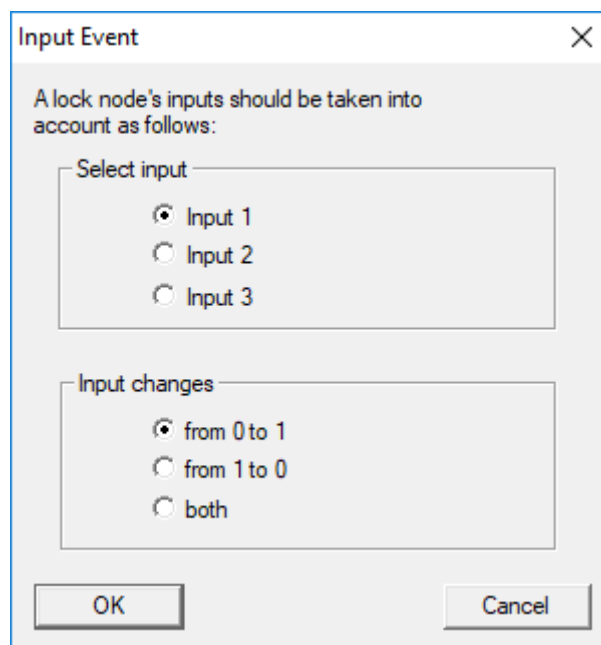
- ✓ LSM open.
  - ✓ SREL3 ADV System added to the matrix.
1. Use | Network | to select the **Event manager** item.  
↳ The "Network event manager" window will open.
  2. Click on the **New** button.  
↳ The "New Event" window will open.

3. Enter a suitable name for the event.
4. Enter an optional description for the event.
5. Enter an optional message.
6. Open the ▼ **Type** drop-down menu.

7. Select the "Input Event" item.



8. Click on the **Configure event** button.  
→ The "Input Event" window will open.



9. Select the required input in the "Select input" section.
10. Select the status change that the event should trigger in the "Input changes" section.
11. Click on the **OK** button.
12. Click on the **Select** button to assign a locking device to the event.  
→ The "Administration" window will open.
13. Highlight one or more locking devices.
14. Click on the **Add** button.
15. Click on the **OK** button.  
→ Window closes.  
→ Locking device is assigned to the event.
16. You can use the **New** or **Add** button to assign an action if you wish to configure an action.
17. Click on the **OK** button.  
→ Window closes.

- ↳ Event is displayed in the "Events" section.
- 18. Click on the **Exit** button.
  - ↳ Window closes.
- ↳ Input is added as an event and triggers an action.

#### 2.4.5 Creating a response

First create a response. This response can be selected at a later stage if a specific scenario arises.

1. Select "Network/Event manager".
2. Click on the "New" button under "Responses" on the right-hand side.
3. Add a name and description for the response.
4. Select "Email" as the type.
5. Click on the "Configure response" button.
6. Click on the "New" button.
7. Enter the recipient's email address, a subject and a message body. *You can use the "Test" button to test the email configuration immediately.*
8. Exit the dialogue by pressing the "OK" button three times. Press the "Exit" to return to the matrix.

#### 2.4.6 Creating an event

Once a response has been created, you can then go on to create an event.

1. Select "Network/Event manager".
2. Click on the "New" button under "Events" on the left-hand side.
3. Add a name and description for the response.
4. Select "Access" as the type.
5. Click on the "Configure event" button.
6. Activate the "Respond to all transponders" check box. *The event is to occur every time that a transponder is activated. Alternatively, you can restrict the event to a single transponder.*
7. You can adjust the action further in the "Time setting" section.
8. Click on the "OK" button.
9. Click on the "Select" button in the "Locking devices" section.
10. Add all locking devices which are to trigger the event when the transponder is activated and press OK to confirm your selection.
11. Click on the "Add" button in the "Associated actions" section.
12. Add the previously created response.
13. Click on the "Configure time" button.
14. Enter the night hour times. The event only becomes active within the pre-determined time frame here.



15. Exit the dialogue by pressing the “OK” button three times. Press the “Exit” to return to the matrix.

## 2.5 Managing the virtual network (VN)

Authorisations can also be quickly and conveniently modified and adjusted over a virtual network (VN network) without a full network. The authorisation for locking devices (and block IDs for blocked identification media) is saved directly to the ID medium and forwarded to locking devices each time a locking device is activated. In a virtual network, it is important to update all ID media at a gateway at regular intervals.

The main set-up of a virtual network is shown in this example.

### 2.5.1 Setting up a locking system

The “Virtual network” check box needs to be activated in an (exclusively) G2 locking system. A considerable programming requirement may arise if this setting is applied in an existing locking system.

### 2.5.2 Setting up a VN service

1. Select "Network/VN service".
2. Select the VN server (e.g. communication node).
3. Enter the installation path to the VN server. *The VN server is installed in a separate folder in the main directory for an LSM Business installation.*
4. Click on the "Apply" button.
5. Click on the "Finish" button.

### 2.5.3 Add components and set up the LSM software.

Before you begin with set-up, you need to make the key settings for operating a network in the LSM software and the RouterNode2 must be ready for use.

■ [Preparing the LSM software \[▶ 33\]](#)

■ [Preparing hardware \[▶ 34\]](#)

■ [Creating communication nodes \[▶ 34\]](#)

■ [Setting up Task services \[▶ 45\]](#)

1. Add the different ID media (e.g. transponders) and locking devices (e.g. active locking cylinders).
2. Implement initial programming of the added components.
3. Add a SmartRelay2 and authorise all ID media which are to receive new authorisations there at a later point in time.
  - ↳ The “Gateway” check box must be activated in the tab in the SREL2 locking device properties.

4. Carry out initial programming for the SREL2 and ensure that it features a properly connected LockNode.
5. Set up the RouterNode2 using WaveNet Manager and assign the gateway (or the SREL2) to it.
  - ↳ See *Setting up the network and importing into LSM* [▶ 35].

### 2.5.4 Exporting authorisation changes

Exporting authorisation changes only works if at least one change has been made. Withdraw authorisation for Locking Cylinder 1 from Transponder 1 to test, for example.

1. Select "Programming/Virtual network/Export to Vnetwork".
2. Select all SREL2s to which you intend to export/send data.
3. Check that you have selected the right locking system.
4. Clicking on the "Prepare" button
  - ↳ All changes which are to be exported will appear on the persons list.
5. Clicking on the "Export" button
  - ↳ The export process starts. The changes are exported to the gateway.

The authorisation change is now stored ready at the gateway. There are now two scenarios:

- Transponder 1 logs onto the gateway. Locking Device 1 will later recognise that Transponder 1 is no longer authorised and refuse access.
- Another transponder (not Transponder 1) logs onto the gateway first and authorises itself for use on Locking Device 1. Locking Cylinder 1 is notified of Transponder 1's block ID.

With LSM 3.4 SP2 and higher, it is possible to "inform" any number of transponders one or two other transponder IDs which need to be deactivated.

#### Programme the TIDs to be disabled directly

The IDs to be disabled are saved on the transponder during the programming process.

- ✓ The transponder is physically available.
  - ✓ The transponder's programming window is open.
1. Click on the "TIDs to deactivate" button.
    - ↳ The list will open.
  2. Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.
  3. Click on the **OK** button to confirm your input.

4. Continue with the programming.
  - ↳ The checked TIDs will be saved to the transponder as TIDs to delete. When the transponder is authenticated on one of the locking devices concerned, the TIDs to be deleted are deactivated at the locking device.

#### **Add the TIDs to be blocked to the properties**

The IDs to be deactivated are saved on the transponder either during the next programming process or the next booking on a gateway.

- ✓ The transponder's properties window is open.
- 1. Change to the "Configuration" tab.
- 2. Click on the "TIDs to deactivate" button.
  - ↳ The list will open.
- 3. Activate one or two check marks in the TID column to save the TIDs to be deleted on the transponder.
- 4. Click on the **OK** button to confirm your input.
  - ↳ The checked TIDs are saved on the transponder either during the next programming process or the next booking on a gateway.

#### **2.5.5 Importing authorisation changes**

Once the changes have been exported to the gateway, it is not possible to see which changes have already been collected from the gateway in the LSM software at first. They cannot be shown until an import is made.

1. Select "Programming/Virtual network/Import synchronisation".
  - ↳ The import process will launch immediately.
2. Clicking on the "Finish" button

#### **2.5.6 Tips on VN**

- It is important for all transponders to make bookings at short, regular intervals to quickly distribute changes throughout the locking system "offline". Time budgets can be used for this purpose:

The "Dynamic time windows" options in the locking system properties offer the possibility of imposing a time budget on transponders. This obliges a person to load the ID medium on the gateway on a regular basis; otherwise, the ID medium is blocked for the locking system in question.

- Import and export of changes to a gateway can be automated. These settings can be made under "Network/VN service".

## ATTENTION

### WaveNet capacity utilisation due to import and export

If many changes are imported and exported at the same time, full use is made of the WaveNet's capacity. This may affect other functions which also use the WaveNet.

## 2.6 Sabotage detection

From LSM 3.4 SP2 you can recognise sabotage attempts on the SmartHandle AX and on the SmartRelais 3 Advanced. When the enclosure used there is opened, the electronics detect this and send the information to LSM. If you want to evaluate the information, you can set up an event for it and respond to it (see *Setting up event management* [► 45]).

## 2.7 DoorMonitoring (SmartHandle) - Door handle events

From LSM 3.4 SP2 onwards, you can see the state of the handle on the SmartHandle AX. When the trigger is pressed, the electronics detect this and send the information to LSM. If you want to evaluate the information, you can set up an event for it and then respond to it (see (*Setting up event management* [► 45])).

## 3 Help and other information

### Information material/documents

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

### Software and drivers

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

### Declarations of conformity

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

### Hotline

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

### Email

You may prefer to send us an email.

[support@simons-voss.com](mailto:support@simons-voss.com)

### FAQs

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

SimonsVoss Technologies GmbH  
Feringastrasse 4  
85774 Unterföhring  
Germany



## This is SimonsVoss

SimonsVoss is a technology leader in digital locking systems.

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

SimonsVoss locking systems unite intelligent functions, optimum quality and award-winning German-made design. As an innovative system provider, SimonsVoss attaches great importance

to scalable systems, effective security, reliable components, high-performance software and simple operation.

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

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

© 2019, 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.

