SmartIntego WO System description

Information

21.10.2021

SimonsVoss technologies

Contents

1 General safety instructions 6
2 SmartIntego 7
3 SmartIntego Tech Kit 8
4 Concept 9
5 Functions 10
5.1 Documentation 10
5.2 Communication between integrator system and locking devices 10
5.3 Error management 10
5.4 Event logging and log files 10
5.5 Battery management 11
5.6 System monitoring 11
5.7 Access authorisations 11
5.8 Offline functions (whitelists) 11
5.8.1 Construction site whitelist 12
5.8.2 Integrator whitelist 13
5.8.3 Emergency access or fire service cards with local inspection 14
5.9 Installation and start 14
5.10 Short-term engagement 15
5.11 Long-term opening/Flip-flop or static office mode 15
5.12 Office mode / Personal Office mode 16
5.13 DoorMonitoring 16
5.13.1 Possible (door) states 16
5.14 Escape & return 17
5.15 PIN code keypad 18
5.16 Shorter LockNode response times (short wake-up period) 18
5.17 IO-Node 19
5.18 Solution Guard 19
6 Components 20
6.1 Door 22
6.2 Storage mode 25
6.3 Types of SmartIntego locking devices 25
6.4 AXEOS operating system 27
6.5 Digital Cylinder AX 27
6.5.1 Structure 27

6.5.2 Variants and features ... 30
6.5.3 Installation ... 31
6.5.4 Tool ... 50
6.5.5 Cover contact ... 51
6.5.6 Technical specifications ... 52
6.6 Locking cylinder (TN4) ... 56
6.6.1 Structure ... 56
6.6.2 Variants and features ... 58
6.6.3 Installation ... 60
6.6.4 Tool ... 61
6.6.5 Technical specifications ... 61
6.6.6 Dimensional drawings cylinder ... 62
6.7 SmartHandle AX ... 64
6.7.1 Structure ... 65
6.7.2 Tool ... 65
6.7.3 Cover contact ... 66
6.7.4 Technical specifications ... 66
6.8 SmartHandle 3062 ... 78
6.8.1 Structure ... 78
6.8.2 Tool ... 81
6.8.3 Technical specifications ... 81
6.9 Padlock ... 85
6.9.1 Technical specifications ... 85
6.10 General signalling and processes for SmartIntego locking devices ... 88
6.11 IO-Node ... 92
6.11.1 Installation ... 93
6.11.2 Connections ... 93
6.11.3 Technical specifications ... 95
6.12 PIN code keypad ... 95
6.12.1 Intended use ... 95
6.12.2 Operation ... 96
6.12.3 Signals ... 96
6.12.4 Technical specifications ... 98
6.13 Batteries ... 98
6.13.1 Battery level measurement (locking cylinders and SmartHandles) ... 99
6.13.2 Battery replacement (locking devices and SmartHandles) ... 99
6.13.3 Battery level measurement (NodeIO and PIN code terminal) ... 100
7 Infrastructure ... 101
7.1 LockNodes ... 101
7.1.1 LockNode in locking devices (LNI) ... 101
7.1.2 LockNode in Node (LN) ... 101

7.2 GatewayNode (GN) ... 101
7.2.1 TCP ... 102
7.2.2 RS-485 ... 109
7.2.3 Signalling ... 113
7.2.4 Mercury Security Variant ... 114
7.2.5 External antenna ... 114
7.2.6 GatewayNode radio radio ... 115
7.3 WaveNet ... 117
7.3.1 Description ... 117
7.3.2 Frequency ... 117
7.3.3 Topology ... 118
7.3.4 Communication ... 120
7.3.5 Synchronization ... 123
7.3.6 Signal Quality Measurement ... 123
7.4 Programming Device (SI.SmartCD) ... 127
8 Software ... 129
8.1 SmartIntego Tool (WO) ... 129
8.2 SmartIntego Manager ... 130
8.3 OAM tool ... 130
8.4 QR code scanner (chip ID) ... 131
9 Passwords ... 132
9.1 Handling passwords ... 133
9.2 Project Password ... 134
9.3 Locking system password ... 134
9.4 WaveNet password ... 135
9.5 Card configuration password ... 136
9.6 Card data read key ... 136
9.7 Password for GatewayNode configuration website ... 136
9.8 AES encryption password ... 137
10 Cards ... 139
10.1 Card types (WirelessOnline) ... 139
10.2 Card settings ... 140
10.2.1 UID mode (Unique Identifier) ... 140
10.2.2 Password-protected data area ... 141
10.2.3 Calypso cards with serial number ... 143
10.2.4 ISO7816-4 cards ... 144
10.2.5 Return timeout after reading ... 144
11 Changelog ... 145

12 Help and other information 146

1 General safety instructions

Signal word (ANSI Z535.6)	Possible immediate effects of non-compliance
DANGER	Death or serious injury (likely)
WARNING	Death or serious injury (possible, but unlikely)
CAUTION	Minor injury
IMPORTANT	Property damage or malfunction
NOTE	Low or none

WARNING

Blocked access

Access through a door may stay blocked due to incorrectly fitted and/or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of blocked access such as access to injured or endangered persons, material damage or other damage!

Blocked access through manipulation of the product

If you change the product on your own, malfunctions can occur and access through a door can be blocked.

- Modify the product only when needed and only in the manner described in the documentation.

NOTE

Intended use

SmartIntego-products are designed exclusively for opening and closing doors and similar objects.

- Do not use SmartIntego products for any other purposes.

Qualifications required

The installation and commissioning requires specialized knowledge.

- Only trained personnel may install and commission the product.

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

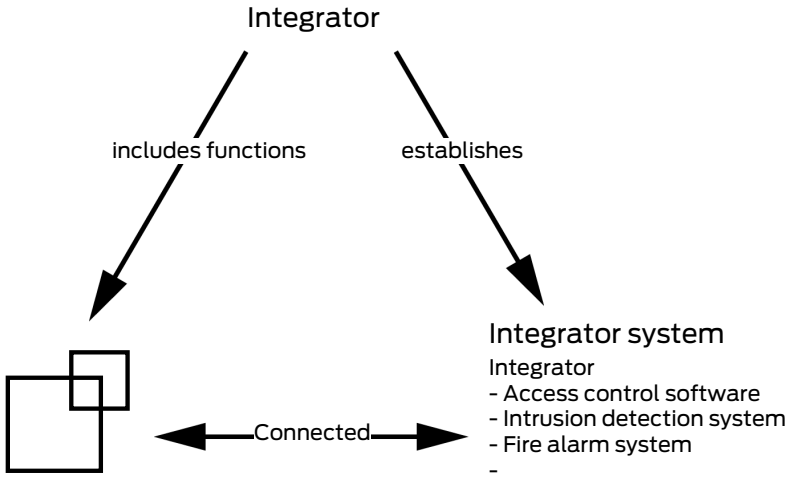
The German language version is the original instruction manual. Other languages (drafting in the contract language) are translations of the original instructions.

Read and follow all installation, installation, and commissioning instructions. Pass these instructions and any maintenance instructions to the user.

2 SmartIntego

SmartIntego is an independent product group from SimonsVoss. The SmartIntego components can be set up using the SimonsVoss configuration software and connected to an integrator system via the SmartIntego interface. The integrator is usually a manufacturer of building management software (access control software, EMEA solution, fire alarm system, etc.), in which the SimonsVoss SmartIntego locking devices are also managed. It develops the interface to his system independently and is also responsible for the connected functions. The SmartIntego interface is available in two versions:

- SmartIntego WirelessOnline (WO)
- SmartIntego Virtual Card Network (SVCN)



3 SmartIntego Tech Kit

The SmartIntego Tech-Kit helps you to perform the initial operation and operate your SmartIntego locking system.

It contains:

- Configuration Software
- System description
- Step-by-step instructions
- Current firmware versions
- Manuals

Versioning

You can recognise the current version in the file name (year month, e.g. 20-01). You can find the latest version of the SmartIntego-TechKit in the partner section of the SmartIntego website (*https://www.smartintego.com/int/home/home*).

4 Concept

SmartIntego Wireless Online (WO) is a networked SimonsVoss locking system based on cards and batteries. SMART.SURVEIL offers the following functions:

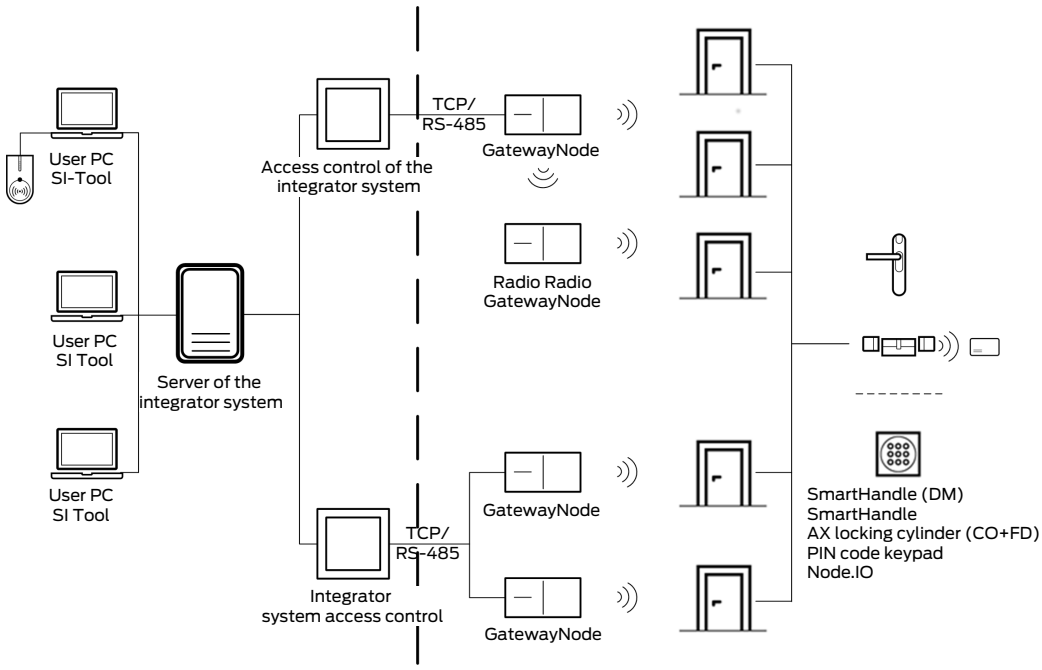
- Reading data from cards (identification number)
- Send read data to access control of the integrator system (board, computer, service...)
- Command received from access control (e.g. engage locking device)

A locking device connected to the access control system does not evaluate the read data itself. Instead, the locking device sends the data to the access control of the integrator system via a GatewayNode. Access control then evaluates the read data and responds to it (for example with the command to engage the locking device).

Depending on the integrator, the basis of the integrator system differs:

- Hardware base
- Software-based
- Mixed form

Ask your integrator to know the exact structure of the integrator system. This figure only shows the general structure:



5 Functions

5.1 Documentation

Each integrator develops their own integration system and provides information in their own documentation on topics such as:

- Before installation
- Description of Integrated Functions
- Details

The TechGuide only describes the general handling and configuration of SmartIntego components.

5.2 Communication between integrator system and locking devices

A technical acceptance test is carried out before certification of a new integrator. During this acceptance test, SimonsVoss and the integrator check whether the integrator system and SmartIntego components communicate perfectly with each other. Certified integration partners are listed on the SmartIntego website (*https://www.smartintego.com/int/home/home*).

5.3 Error management

Smartintego Wireless Online uses an 868-MHz radio network for wireless communication to the locking devices.

Wireless communication at 868 MHz is widespread. High utilization of the frequency range leads to temporary communication bottlenecks.

SmartIntego components are equipped with error correction routines that automatically intercept such bottlenecks.

Faults or bottlenecks that can no longer be intercepted by the SmartIntego components must either be intercepted by the integrator system with additional fault corrections and/or signalled with a display.

5.4 Event logging and log files

If the installer is to analyse a potential problem, an event log should be available in the integrator system.

The installer must be able to record and understand potential problems with this event log.

5.5 Battery management

The SmartIntego components send battery warnings to the integrator system, which then informs the locking system administrator of the weak batteries. A commissioned technician or the end customer is then responsible for the timely replacement of the batteries in the components.

5.6 System monitoring

The integrator system informs the locking system administrator of the network status of the SmartIntego GatewayNodes.

5.7 Access authorisations

The integrator system and its access control systems control the locking devices:

- Access authorisations
- Type of opening
  - Short-term engagement (3 to 25 seconds)
  - Long-term engagement (1 minute or more)
  - Office mode (Short: 3 to 25 seconds or long: 1 minute or more)
  - Denial of access
  - Automatic disengage
  - Time-controlled authorisations

5.8 Offline functions (whitelists)

Normally, the components of a SmartIntego wireless online system communicate directly with the integrator system, which processes all requests online.

In some cases, communication may be disrupted, for example:

- Power failure
- Network problems

SmartIntego locking devices then no longer reach the integrator system and vice versa. In this case, whitelists with authorised cards can be stored as a fallback level in the locking devices. With the whitelists, end users can continue to use the locking devices without uncontrolled access.

Whitelist definition

A whitelist is a pre-defined list of authorised cards. It is saved in the locking devices themselves. If a locking device does not reach the integrator system and the read card is stored in the whitelist, the locking device engages briefly (5 seconds).

Three types of whitelists are available to you:

- Construction site whitelist
- Integrator whitelist
- Integrator whitelist with local check (emergency access or fire service cards)

5.8.1 Construction site whitelist

The construction site whitelist is also known as a priority whitelist or temporary whitelist.

Sometimes it is necessary to install the locking devices on a construction site before the necessary infrastructure (power connections, IT equipment or integrator system) is available.

In this case, you can temporarily use your locking devices offline in advance until the network infrastructure is ready for use. To do so, release cards that can be used by construction site workers.

Unprogrammed SmartIntego locking devices can be opened with all cards that can be read by the locking device. The construction site whitelist restricts access authorisation to the cards you have approved (i.e. entered in the construction site whitelist). It should only be used temporarily during the construction phase. Always connect the locking devices to the integrator system later.

Construction site whitelist properties:

- Local verification of access authorisation by locking device
- No communication with integrator system
- Check access authorisation only with the unique ID (UID) of the card
- Restriction to 128 cards
- Same access authorisations for all saved cards (no restriction to individual locking devices: all cards on the construction site whitelist have access authorisations for all locking devices in which the construction site whitelist is stored)
- No access logging or access list
- Default value: Five seconds
- No battery warnings
- Exclusive management with SmartIntego tool
- No permanently engaged locking devices disengaged

The integrator system cannot change the construction site whitelist itself, but can delete the complete construction site whitelist in the locking devices.

NOTE

Transition to normal operation

The construction site whitelist does not expire or become ineffective by itself.

- When transferring to normal operation, the observer must delete the construction site whitelist from the locking devices and from the SmartIntego tool.

5.8.2 Integrator whitelist

The integrator whitelist is managed by the integrator himself and is the most important security mechanism in the SmartIntego locking system.

It acts as a fallback level if the integrator system is no longer reachable. Possible reasons for failure:

- Power failure
- Disruptions in the IT infrastructure
- Faults in the integrator system
- Hardware error

As soon as the locking devices no longer reach the integrator system, access authorisations can no longer be checked or received online. Authorised users would also no longer be able to open doors.

For this purpose, a whitelist is configured in the integrator system during the construction phase of a project and programmed into the locking devices.

Integrator whitelist properties:

- Local check by closing after return timeout (no response from integrator system within five seconds)
- No communication with integrator system
- Default value: Five seconds
- Prolonged card retention (approx. 5 seconds) also disengages permanently engaged locking devices
- Additional functions such as office mode or long-term engagement not available
- Whitelist authentication (offline) normally with the same card ID as online authentication. In special cases, a card can have an ID for online access and an ID for offline access.
- Limited to 250 cards per lock (see integrator system documentation)
- Individual, individual integrator whitelist for each lock

- Logging of offline accesses: Access list in the lock with 1,000 entries (overwritten on a rolling basis, WO Legacy 250)
- Access list readable with SmartIntego tool and WaveNet or local programming device
- No battery warnings
- Exclusive management by integrator system

NOTE

Whitelist for locking devices read on both sides

Locking devices with readers on both sides (FD or BL) only have a whitelist for both sides.

5.8.3 Emergency access or fire service cards with local inspection

These cards belong to the integrator whitelist, so they count towards their quota.

However, it differs in one important point for emergencies: As soon as the locking device detects that the card held is such a card, it engages for five seconds. Communication with the integrator system takes valuable time in an emergency and therefore only takes place retrospectively for these special cards. The integrator system is informed if there is a connection. The other functions and restrictions are identical to those of the integrator whitelist.

WARNING

Access for rescue personnel in the event of a system failure

Faults and failing systems often occur in emergencies such as a fire. The locking devices may then no longer be able to be opened centrally. With emergency access and fire service cards, ambulances can nevertheless penetrate very quickly.

- Create several emergency access or fire service cards and store them in a fire service key depot.

5.9 Installation and start

The SmartIntego tool manages the locking devices:

- add
- remove
- replacement

- or replace.

Changes made must be communicated to the integrator system. The procedure differs depending on the integrator system. This documentation therefore only describes the procedure in the SmartIntego tool.

5.10 Short-term engagement

Locking devices thus engage for a short period of time (3 to 25 seconds). During this time, users can operate the door mortise lock with the locking cylinder or SmartHandle.

As an alternative to an authorised card, the locking device can also be engaged differently:

- Remotely with the integrator system
- Time-controlled

5.11 Long-term opening/Flip-flop or static office mode

Depending on the integrator, this function is different:

- Long-term opening
- Flip-flop mode
- Static Office Mode

But it always means the same thing. Locking devices thus engage for a long period of time (one minute or longer). During this time, users can operate the door mortise lock with the locking cylinder or SmartHandle.

As an alternative to an authorised card, the locking device can also be engaged differently:

- Remotely with the integrator system
- Time-controlled

The engagement duration can be adjusted (one minute to infinite, i.e. permanently engaged). Combinations enable a wide range of requirements to be covered.

Example:

A locking device can be engaged using an authorised card:

- During office hours between 7:00 and 17:00, the door is heavily frequented:

  For convenience reasons, the locking device remains engaged for the long term and does not have to be engaged every time.
- Outside office hours between 17:00 and 7:00, there are a maximum of individual persons in the building.

For security reasons, the locking device remains engaged only for a short time.

This behaviour is often referred to as office mode. The locking device can be disengaged:

- Manual: With an authorised card
- Automatic: Through time control

For details, please refer to the documentation of the integrator system.

5.12 Office mode / Personal Office mode

This mode is similar to static office mode. However, the user can control the locking device's behaviour by holding the card briefly or long before the locking device.

Example:

- During working hours, other employees should be able to enter the office:

  The employee holds their card longer than two seconds before the locking device. This means that it engages the locking device for a long time and gives everyone access (one minute to permanently engaged).
- During the break, the employee does not want to be disturbed:

  The employee holds their card less than two seconds before the locking device. This means that it only engages the locking device for a short time.

Combinations enable a wide range of requirements to be covered.

The locking device can be disengaged:

- Manual: With an authorised card
- Automatic: Through time control

For details, please refer to the documentation of the integrator system.

5.13 DoorMonitoring

DoorMonitoring is SimonsVoss technology. SmartIntego locking devices with this option are equipped with sensors which monitor door status.

The use of DoorMonitoring in SmartIntego systems requires extended configuration and programming with the SmartIntego tool (WO).

For details, please refer to the documentation of the integrator system.

5.13.1 Possible (door) states

States may differ for different components.

5.13.1.1 Possible DoorMonitoring states of SmartHandles

- Door open/closed
- Door open for too long
- Locked (only for self-locking mortise locks)
- Handle in use/not in use

5.13.1.2 Possible DoorMonitoring states of SmartHandle AX

- Door open/closed (prepared, retrofittable)
- Door open for too long (prepared, retrofittable)
- Locked (only for self-locking mortise locks, retrofittable)
- Handle in use/not in use
- Sabotage detection

5.13.1.3 Possible states RouterNode 2 / GatewayNode 2

- Input active/inactive
- Analogue voltage input above/below threshold

5.14 Escape & return

This function makes it possible to return to a room for a short time after the door has already closed. This does not require a card.

A sensor on the inside of the SmartHandle detects when the handle has been actuated to open the door. SmartHandle then engages for a predefined return time and emits an acoustic/optical signal.

SmartHandle disengages automatically when the set return time expires. Alternatively, it can also be disengaged beforehand by holding a card in front of the SmartHandle reader for two seconds.

NOTE

Escape & Return: Legal situation

The Escape & Return Timeout can be between 30 s and 240 s. The use and configuration of Escape & Return may be subject to legal regulations (e.g. Norway).

- Inform yourself in advance about legal regulations.

5.15 PIN code keypad

The SmartIntego PIN code keypad is a battery-operated online PIN code keypad. Intelligence is not included in the PIN code keypad, but in the integrator system.

The PIN code keypad only stores one master PIN and the length of the user PINs for this PIN code keypad. Therefore, there is no limitation due to the available memory space and the number of user PINs is not limited by the hardware of the PIN code keypad.

Procedure:

✓ Master PIN defined.
✓ Length of user PINs defined for this PIN code keypad.

1. User enters PIN.
   ↳ PIN code keypad checks the length of the PIN entered (not the PIN itself!)
2. PIN code keypad sends PIN with valid length to integrator system.
3. Integrator system checks PIN for validity.
4. Integrator system responds to the PIN with one or more actions.
   ↳ For example, a door is opened next to the PIN code keypad.

Possible applications:

- Entering a PIN opens a door next to the PIN code keypad → Users can pass after entering them themselves.
- Entering a PIN opens one or more doors in the building → Users can pass other remote users by entering them.
- Entering a PIN and holding a card at the locking device opens the door → additional security (redundancy).

Requirements for PINs:

Master PIN requirements	Requirements for all user PINs
▪ Does not start with 0 ▪ Length exactly eight characters	▪ Does not start with 0 ▪ Same length (between one and nine characters)

5.16 Shorter LockNode response times (short wake-up period)

For all actions on locking devices initiated remotely by the integrator system, the network-related delays accumulate (see also *Communication between integrator system and locking devices [▸ 10]*). Such actions include, for example:

- Remote opening

- Openings with PIN code keypads
- Programming the whitelist

Up to 12 seconds or more may elapse between the initiation of the action and a visible reaction.

This time can be shortened. The LockNodes in the locking devices save energy by only "waking up" periodically and checking whether they are currently being addressed. These intervals can be shortened.

The wake-up interval of the locking device is shortened in the integrator system (short wake-up period). The locking device then senses more quickly that it is activated and reacts more quickly.

- This function can be activated or deactivated individually for each locking device (depending on the integrator).
- This function can also be activated or deactivated in a time-controlled manner (depending on the integrator, e.g. only switched on during office hours).
- The shorter wake-up interval increases power consumption. The standby battery life is reduced to 3.5 years with a permanently active shorter wake-up interval.

For details, please refer to the documentation of the integrator system.

5.17 IO-Node

SmartIntego IO Node is a battery-operated radio module with three inputs and an open drain output. The IO-Node can be used to monitor and control components by connecting to the integrator system.

For details, please refer to the documentation of the integrator system.

5.18 Solution Guard

The integrator can freely decide how to license their integration and how to protect their integration.

SimonsVoss Solution Guard can only be used for locking devices in integrator systems which have been registered centrally with the integrator. The integrator can also freely decide how to respond to unlicensed locking devices in their integration system.

Please refer to the description of your integrator system to see if Solution Guard is used.

6 Components

SmartIntego locking devices and components on the door are battery-operated and networked. All locking devices are passive (RFID technology with 13.56 MHz).

SmartIntego components available include:

Components on the door

	SI Digital Cylinder AX
	SI-Locking Cylinder
	SI.SmartHandle AX
	SI:SmartHandle

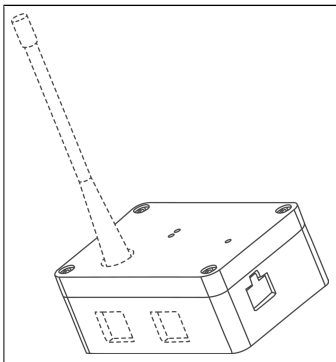
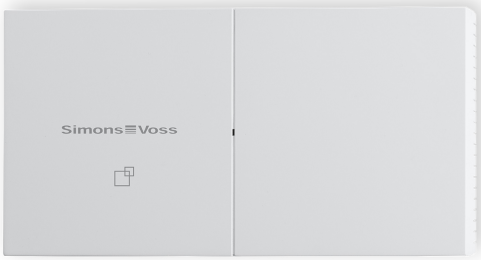
	SI Padlock AX
	SI-Padlock
	SI SmartLocker AX

Components on the door (no RFID)

	IO-Node

	SmartIntego PIN code keypad

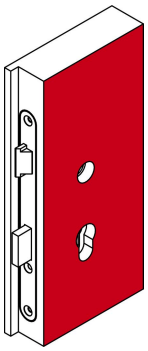
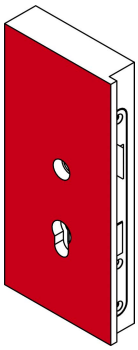
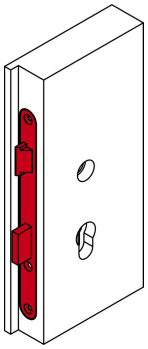
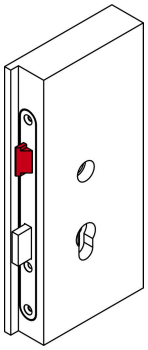
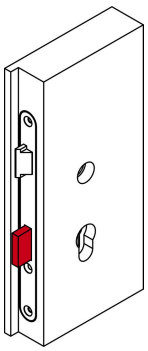
Infrastructure components

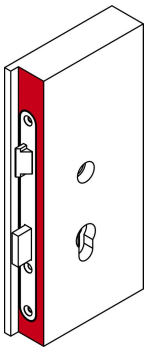
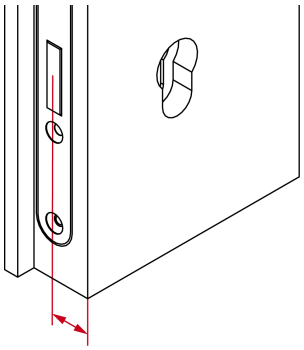
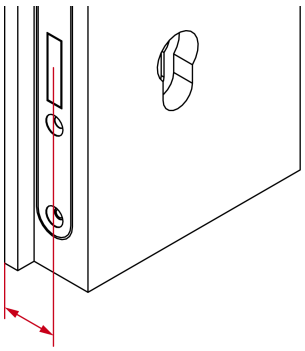
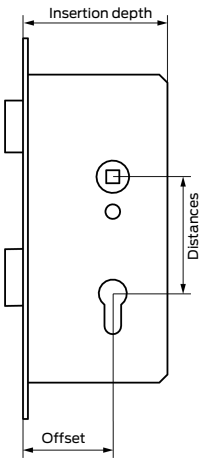
	GatewayNode 1
	GatewayNode 2
	Programming Device SI.SmartCD

Your integrator provides components with relay contact and reader with external power supply.

6.1 Door

The following drawings explain important technical terms relating to doors and mortise locks. You need these technical terms to use the correct SmartIntego locking devices.

	Outside (freely accessible area)
	Inside (secured area)
	mortise lock
	Latch
	Bolt/bolt block

	Door leaf
	Outside dimension (edge of the outside to the centre of the bolt with max. 3 mm projection)
	Inside dimension (inside edge up to the centre of the bolt)
	▪ Insertion depth ▪ Distances ▪ Offset

6.2 Storage mode

NOTE

Lack of access control in factory state

All SmartIntego locking devices are delivered unprogrammed. Unprogrammed locking devices respond to all readable cards (RFID frequency 13.56 MHz and existing ID). These cards can engage non-programmed locking devices for five seconds.

- Configure and programme the locking devices before using them in a productive system.

↳ After programming, access control in the integrator system takes over control of SmartIntego locking devices.

6.3 Types of SmartIntego locking devices

There are several types of SmartIntego locking devices:

SI Digital Cylinder AX  SI-Locking Cylinder 	Lock and unlock the door with the mortise lock dead bolt.

SI.SmartHandle AX  SI:SmartHandle 	Close and open the door with the latch of the mortise lock. SmartHandles can only lock doors in combination with a self-locking mortise lock.
SI Padlock AX  SI-Padlock 	Lock doors together with corresponding devices. The function is similar to mechanical padlocks but with the advantages of a digital locking device.

SI SmartLocker AX 	Lock furniture and locker doors. The function is similar to mechanical locker locks but with the advantages of a digital locking device.

6.4 AXEOS operating system

All SmartIntego locking devices are operated with a SimonsVoss operating system. SimonsVoss is introducing the latest operating system with SmartHandle AX: AXEOS.

SmartIntego components are generally backwards compatible. They can be used together with older SmartIntego components. Existing integration projects can generally be extended with AX components without additional integration effort if already integrated functions are used. Please refer to the integrator documentation to determine whether your integrator system supports the new AXEOS products.

The new AXEOS operating system has been revised as follows:

- New hardware components
- Longer battery life
- Platform flexibility for later functionality
- Omission of 3DES support for MIFARE DESFire

6.5 Digital Cylinder AX

The SI Digital Cylinder AX is an enhancement of the TN4 locking cylinder based on AXEOS technology.

The SI Digital Cylinder AX moves the mortise lock dead bolt. Use an SI Digital Cylinder AX if you want to lock doors.

Please refer to the manual of SI Digital Cylinder AX for more information.

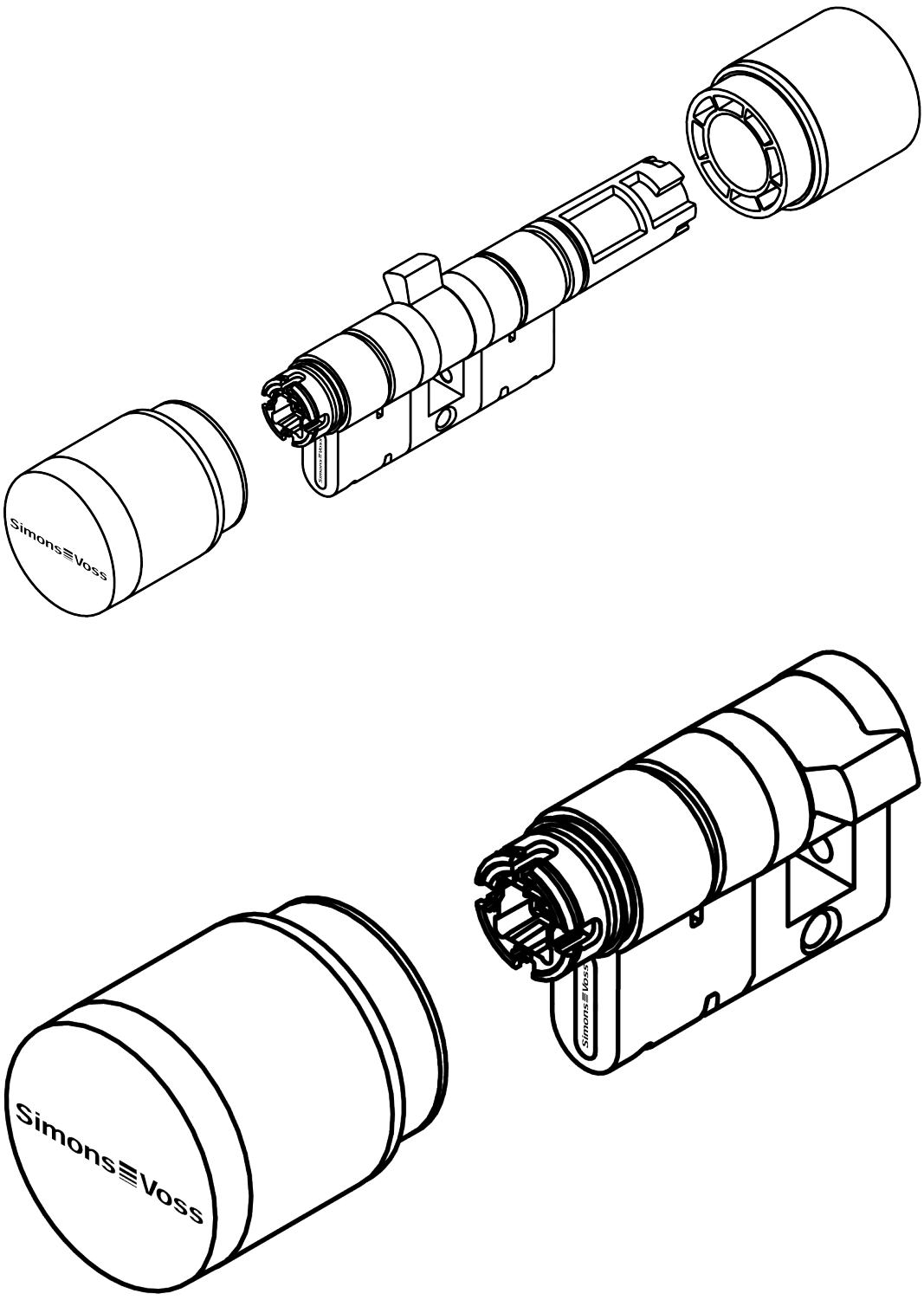
6.5.1 Structure

Comfort/half cylinder

In the case of the SI Digital Cylinder AX (Comfort and half cylinder), all electronics are located on the outside.

- Control Unit (CU)

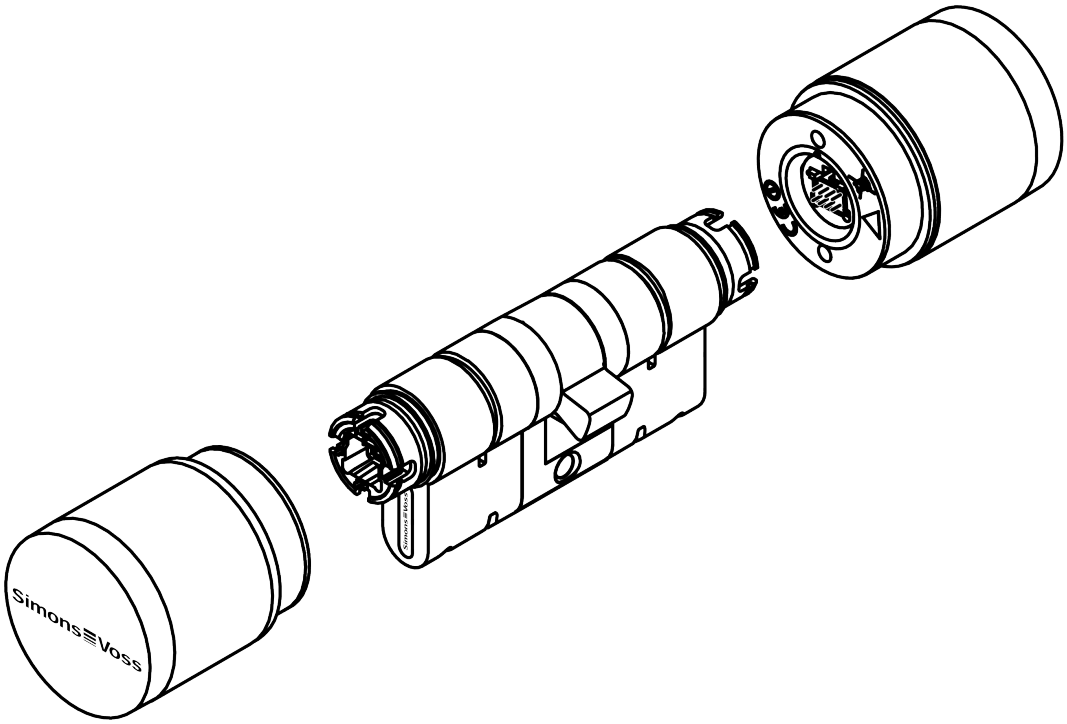
- Card Reader (CR)
- LockNode (LN)
- Batteries
- Secure element (SE) - in the profile core on the outer side



Freely rotating

In the case of the SI Digital Cylinder AX (freely rotating), each of the two reader thumb-turns is equipped with complete electronics.

- Control Unit (CU)
- Card Reader (CR)
- LockNode (LN)
- Batteries
- Secure element (SE) - in the profile core on the outer side



NOTE

Electronics for SI Digital Cylinder AX with reader on both sides

In the version with a reader on both sides, the SI Digital Cylinder AX is equipped with an electronic reader thumb-turn on the outside and an electronic reader thumb-turn on the inside. Both thumb-turns are independent of each other.

1. Create and configure the two electronic reader thumb-turns separately.
2. Program the two electronic reader thumb-turns separately.

Length modularity

The Euro Profile variant is modular and can be extended, shortened or otherwise adapted on site. See the length modularity manual for details.

6.5.2 Variants and features

The SI Digital Cylinder AX is available both as a version with a reader on one side (Comfort = CO) and as a version with a reader on both sides (freely rotating = FD).

The order number provides information about the variant and the equipment features:

General	SI	SmartIntego cylinder
	Z5	Technology level 5
	■ EU (Euro Profile/ EU) ■ SR (Swiss Round) ■ SR (Scandinavian Oval) ■ RS (Round Scandinavian)	Profile
	AXX-IXX	Exterior dimension Interior dimension
	M	**M**IFARE
Structure	CO	Comfort cylinder permanently engaged on the inside
	FD	Freely rotating - cylinder with two card readers (inside and outside) Different access authorisations possible (integrator-dependent)

Features	AP	Anti-panic function
	WP	Weatherproof version (IP 67), otherwise IP54
	MS	Brass version
	HZ	Half cylinder
	MR	Multi-point
Networking	■ WO (wireless online)	Networking technology

Further details on the individual variants and equipment features can be found in the manual for SI Digital Cylinder AX.

NOTE

Avoidance of incorrect orders through the order placement guide

SmartIntego components offer a wide variety of combinations. Not every combination makes sense and is actually available. A manual compilation of the product features can lead to combinations that are not available or to incorrect orders.

- Always use the order placement guide from the partner area of the SmartIntego website (*www.smartintego.com)*).

6.5.3 Installation

IMPORTANT

Unauthorised access by drilling on the inside

The outside of the AX locking cylinder is equipped with drilling protection on the outside, depending on the version.

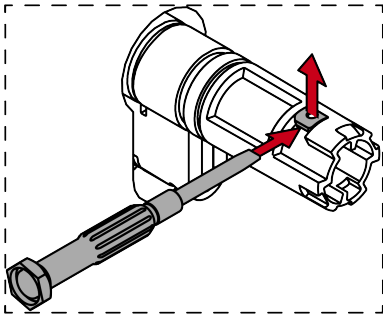
- If you find a mark on the inside (*IN*) of the cylinder body, mount the AX locking cylinder so that this side is in a protected area.

6.5.3.1 Brief descriptions (entire assembly)

Comfort cylinder/anti-panic cylinder (CO/AP, reader on one side)

Standard assembly/initial assembly

This is the easiest way to install the SI Digital Cylinder AX . You do not need any special tools for the initial assembly. Remove the red plastic assembly lock before initial assembly.



NOTE

Tool-free initial assembly

The mechanical thumb-turn is only clipped on when delivered. A thumb-turn lock (red plastic part) prevents the thumb-turn from engaging. You can install the mechanical thumb-turn of the AX locking cylinder without tools, but you cannot disassemble it without special tools. When the AX locking cylinder is installed for the first time, it is therefore not necessary to disassemble the mechanical thumb-turn. Instead, start by inserting the AX locking cylinder.

1. Dismantle the mechanical knob (see *Unmounting the thumb-turn (mech.) [▸ 37]*).
2. Insert the AX locking cylinder (see *Insert locking cylinder [▸ 48]*).
3. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder [▸ 49]*).
4. Fit the mechanical thumb-turn (see *Mounting thumb-turn (mech.) [▸ 36]*).
5. Carry out a functional test (see *Functional test [▸ 46]*).

↳ SI Digital Cylinder AX is fitted.

Fitting with clip-on covers

This option allows you to combine the SI Digital Cylinder AX with specific panels. Some cover plates are mounted on the cylinder and so are located between the thumb-turn and the door. If you want to use such panels, you have to dismantle both thumb-turns.

✓ Special tool available.

✓ 1.5 mm hexagonal wrench available.

1. Dismantle the mechanical knob (see *Unmounting the thumb-turn (mech.) [▸ 37]*).
2. Dismantle the electronic thumb-turn (see *Unmounting the thumb-turn (electr.) [▸ 42]*).
3. Insert the AX locking cylinder (see *Insert locking cylinder [▸ 48]*).

4. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder [▸ 49]*).
5. Fit the cover plates if required.
6. Fit the electronic knob (see *Mounting thumb-turn (electr.) [▸ 39]*).
7. Fit the mechanical thumb-turn (see *Mounting thumb-turn (mech.) [▸ 36]*).
8. Carry out a functional test (see *Functional test [▸ 46]*).

↳ SI Digital Cylinder AX is fitted with clip-on covers.

Freely-rotating cylinder (FD; reader on both sides)

Standard mounting

✓ Special tool available.
✓ 1.5 mm hexagonal wrench available.

1. Dismantle the electronic thumb-turn (see *Unmounting the thumb-turn (electr.) [▸ 42]*).
2. Insert the AX locking cylinder (see *Insert locking cylinder [▸ 48]*).
3. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder [▸ 49]*).
4. Fit the electronic knob (see *Mounting thumb-turn (electr.) [▸ 39]*).
5. Carry out a functional test (see *Functional test [▸ 46]*).

↳ SI Digital Cylinder AX is fitted.

Fitting with clip-on covers

✓ Special tool available.
✓ 1.5 mm hexagonal wrench available.

1. Dismantle the electronic thumb-turn (see *Unmounting the thumb-turn (electr.) [▸ 42]*).
2. Also disassemble the other electronic knob.
3. Insert the AX locking cylinder (see *Insert locking cylinder [▸ 48]*).
4. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder [▸ 49]*).
5. If necessary, attach the covers.
6. Fit the electronic knob (see *Mounting thumb-turn (electr.) [▸ 39]*).
7. Also fit the other electronic knob.
8. Carry out a functional test (see *Functional test [▸ 46]*).

↳ SI Digital Cylinder AX is fitted with clip-on covers.

Half cylinder (HZ, reader on one side)

Standard mounting

✓ Special tool available.
✓ 1.5 mm hexagonal wrench available.

1. Dismantle the electronic thumb-turn (see *Unmounting the thumb-turn (electr.) [▸ 42]*).
2. Insert the AX locking cylinder (see *Insert locking cylinder [▸ 48]*).
3. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder [▸ 49]*).
4. Fit the electronic knob (see *Mounting thumb-turn (electr.) [▸ 39]*).
5. Carry out a functional test (see *Functional test [▸ 46]*).

↳ Half cylinder AX is fitted.

Fitting with clip-on covers

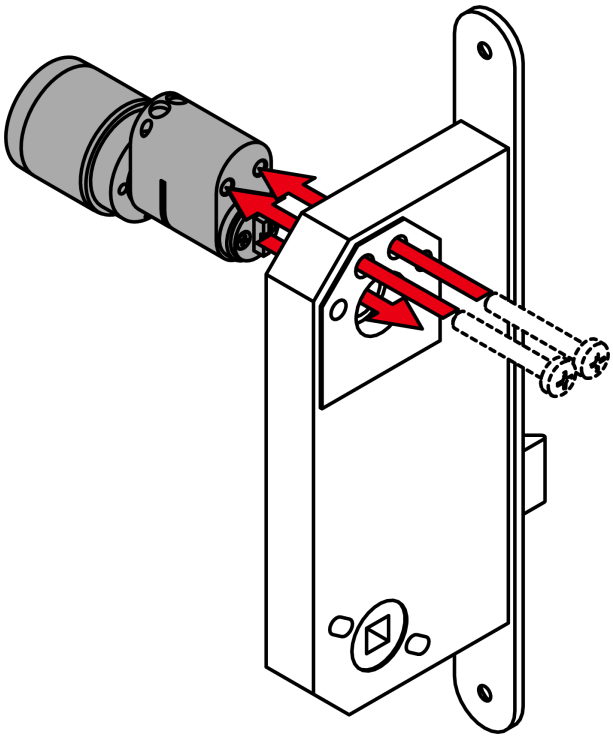
✓ Special tool available.
✓ 1.5 mm hexagonal wrench available.

1. Dismantle the electronic thumb-turn (see *Unmounting the thumb-turn (electr.) [▸ 42]*).
2. Insert the AX locking cylinder (see *Insert locking cylinder [▸ 48]*).
3. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder [▸ 49]*).
4. Fit the electronic knob (see *Mounting thumb-turn (electr.) [▸ 39]*).
5. Carry out a functional test (see *Functional test [▸ 46]*).

↳ Half cylinder AX is mounted with clip-on covers.

Scandinavian oval/round (SO/RS)

Installation



IMPORTANT

Unauthorised access by drilling on the inside

The outside of the AX locking cylinder is equipped with drilling protection on the outside, depending on the version.

- If you find a mark on the inside (*IN*) of the cylinder body, mount the AX locking cylinder so that this side is in a protected area.

✓ Rosettes may already be fitted.

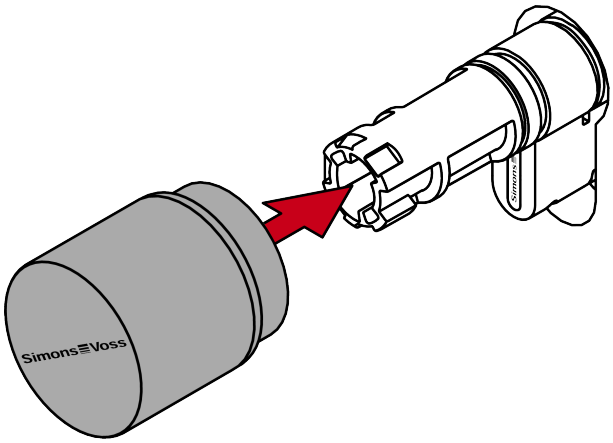
1. Insert the AX locking cylinder with the cam into the retainer of the mortise lock.
2. Screw the AX locking cylinder tight.
3. If necessary, install other fittings.

↳ AX programmed locking cylinder

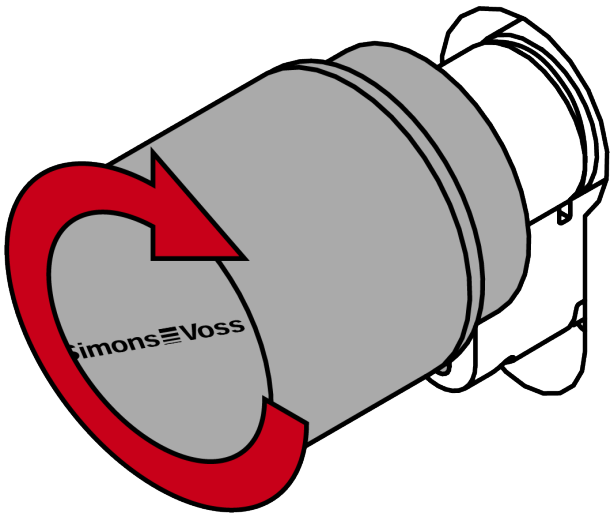
6.5.3.2 Detailed descriptions (individual steps)

Mounting thumb-turn (mech.)

1. Attach the thumb turn.



2. The thumb-turn snaps into place with one click.



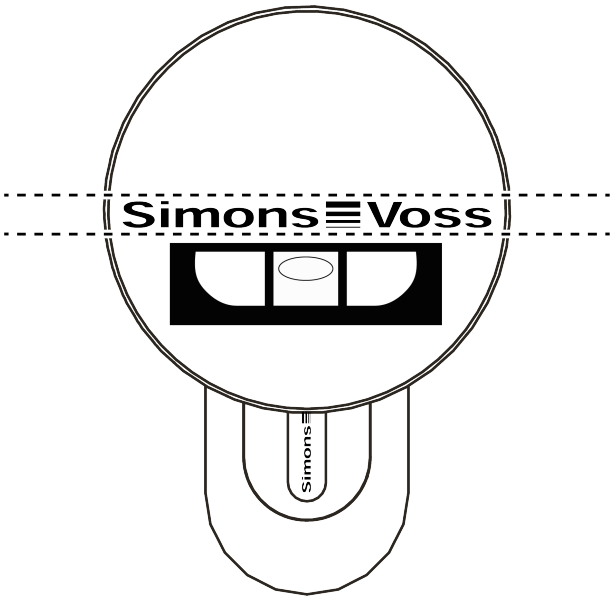
↳ Mechanical thumb-turn is installed.

↳ Disassembling the mechanical thumb-turn

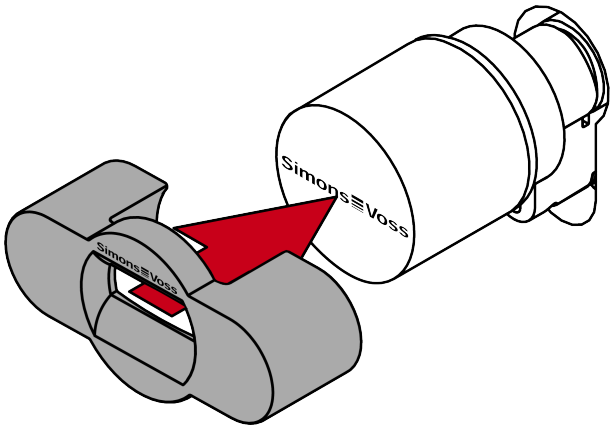
Unmounting the thumb-turn (mech.)

✓ Special tool available.

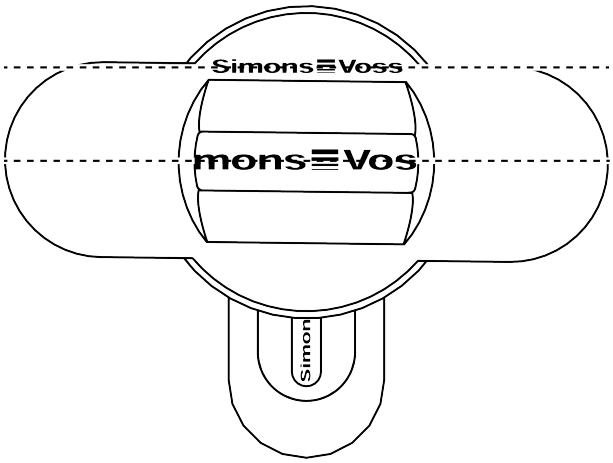
1. Align the thumb turn horizontally.



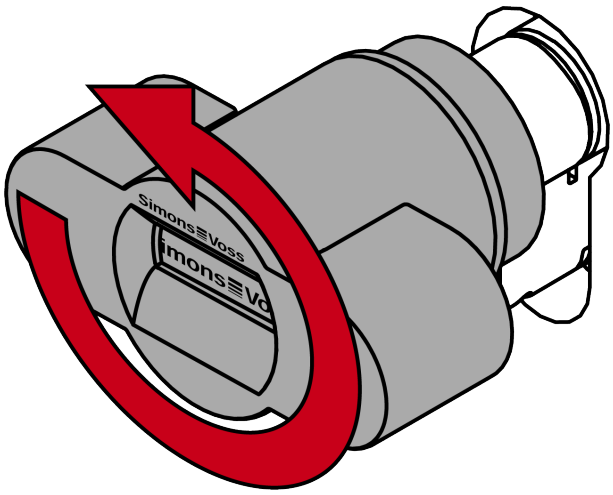
2. Attach the special tool.



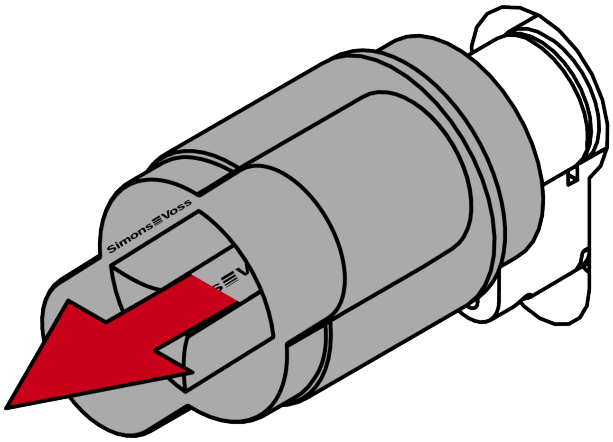
3. Align the special tool so that the logo is parallel to the recess.



4. At the same time turn the special tool and the thumb turn counter-clockwise.



5. Remove the special tool and the thumb turn at the same time.

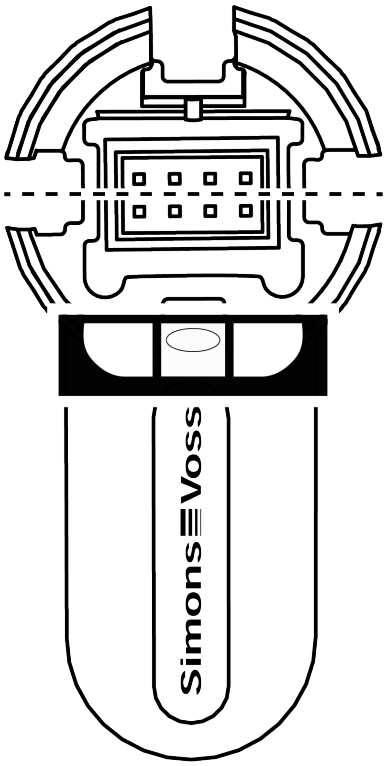


↳ The mechanical thumb turn is disassembled.

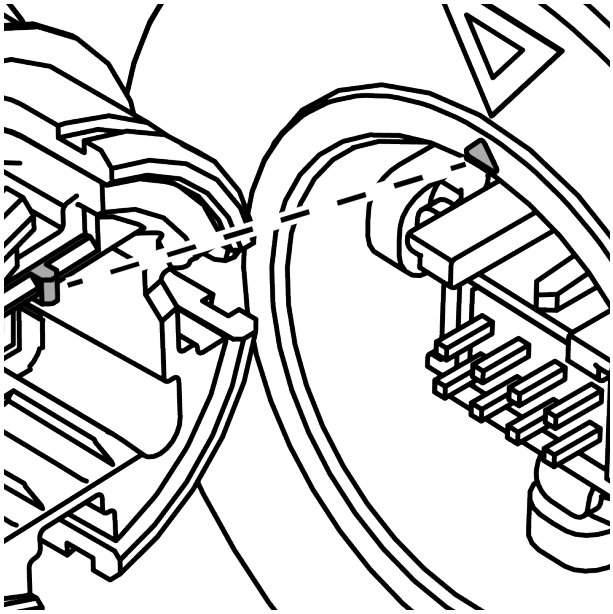
Mounting thumb-turn (electr.)

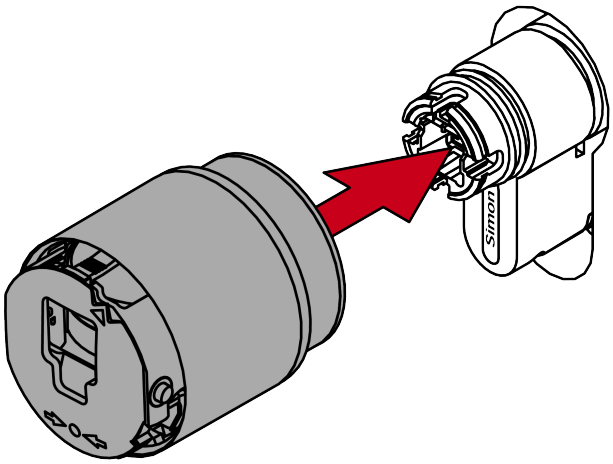
✓ 1.5 mm hexagonal wrench available.

1. Align the thumb turn mount horizontally.



2. Attach the thumb turn.





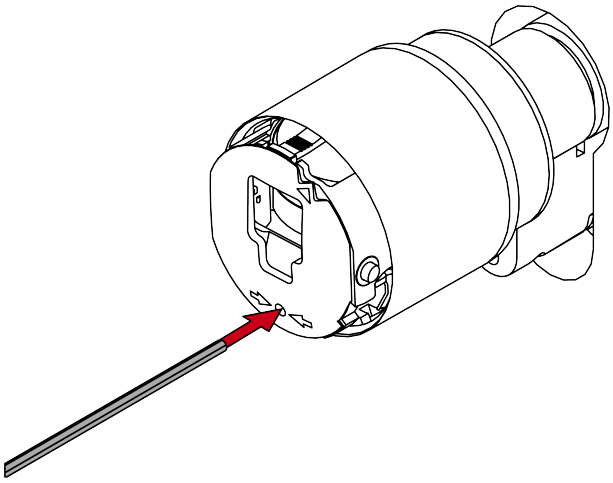
NOTE

Use the supplied hexagonal wrench.

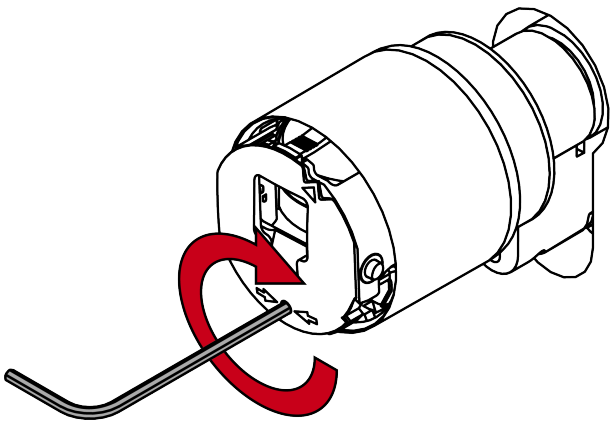
The special tool is supplied with a hexagonal wrench.

- Use this hexagonal wrench to mount and dismount the electronic thumb turn.

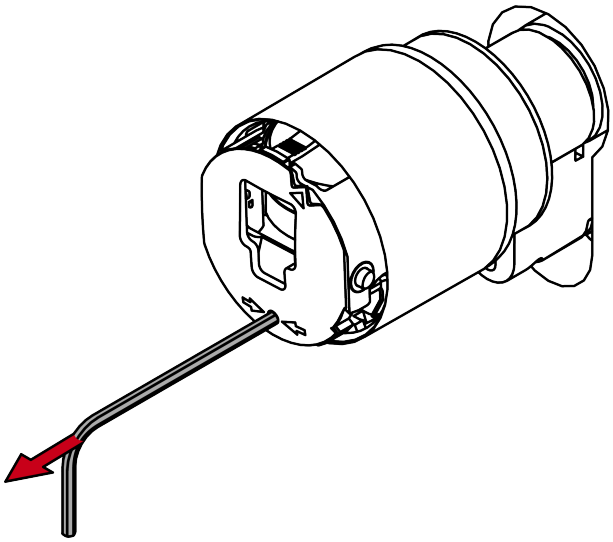
3. Insert the hexagonal wrench into the hole provided until it stops.



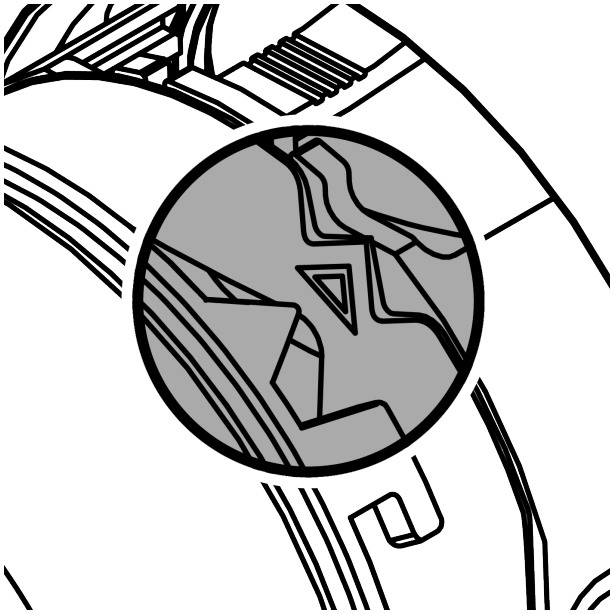
4. Turn the hex key 270 degrees clockwise.

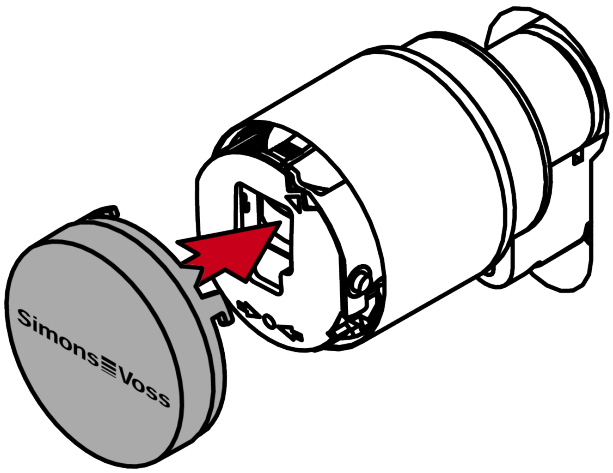


5. Pull out the hexagon wrench again.

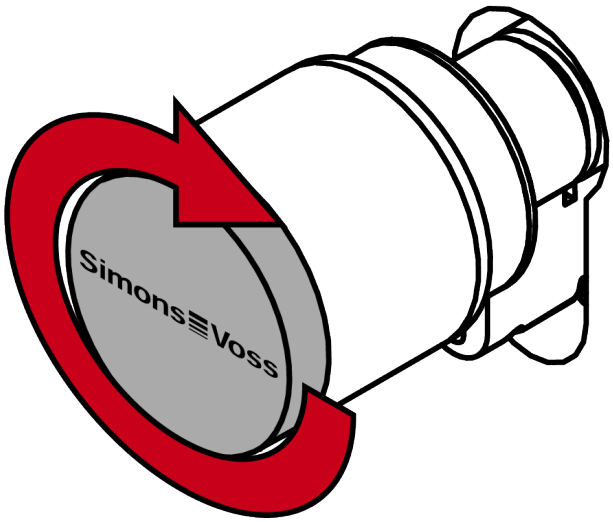


6. Put on the cover.





7. Turn the cover clockwise.



↳ The cover snaps into place with one click.

↳ The electronic thumb turn is installed.

Unmounting the thumb-turn (electr.)

NOTE

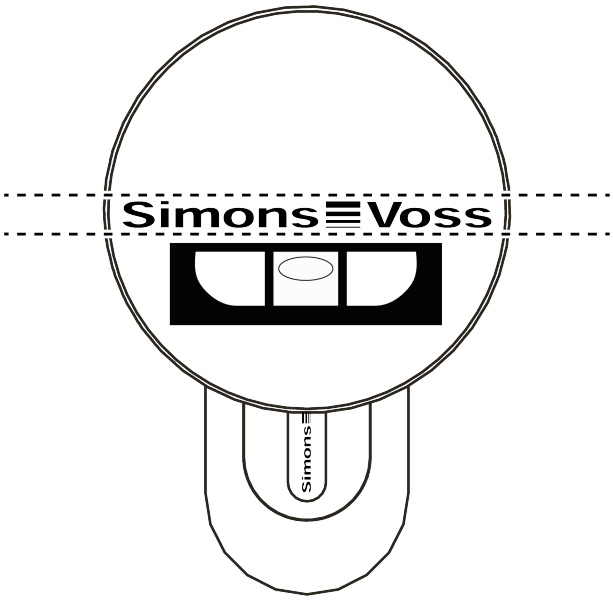
Use the supplied hexagonal wrench.

The special tool is supplied with a hexagonal wrench.

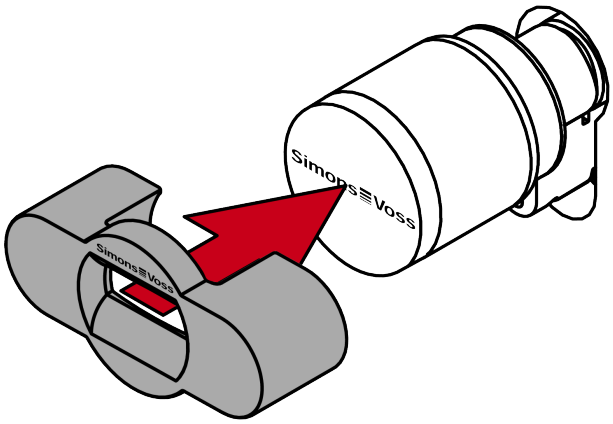
- Use this hexagonal wrench to mount and dismount the electronic thumb turn.

✓ Special tool available.
✓ 1.5 mm hexagonal wrench available.

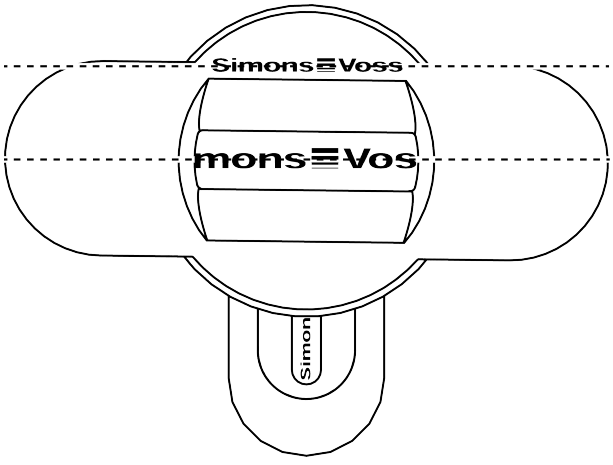
1. Align the thumb turn horizontally.



2. Attach the special tool.



3. Align the special tool so that the logo is parallel to the recess.



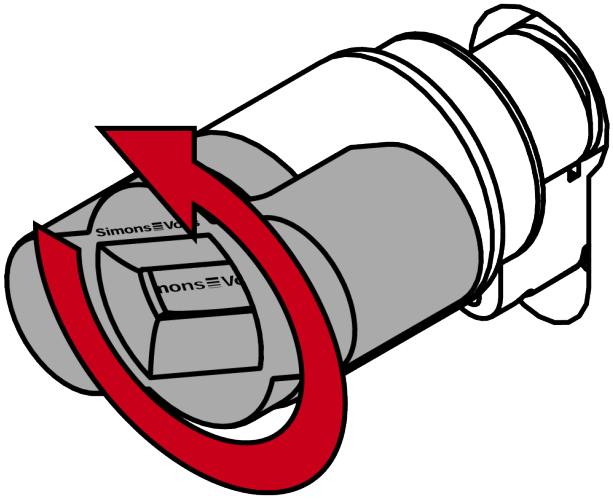
4. Hold the special tool and thumb turn cap firmly at the same time and turn them together 1-2° clockwise first and then counter-clockwise.

NOTE

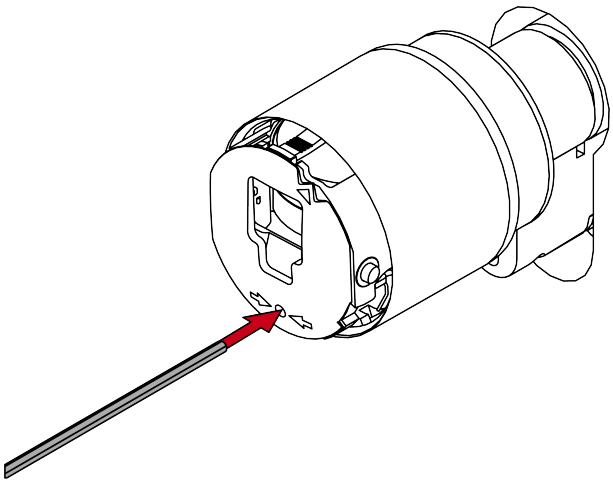
Slipping when turning

The surface of the thumb turn cap can be slippery and the cap can be difficult to turn (especially with WP versions, recognizable by the blue cylinder neck ring or the lasered marking on the inner side of the cylinder profile).

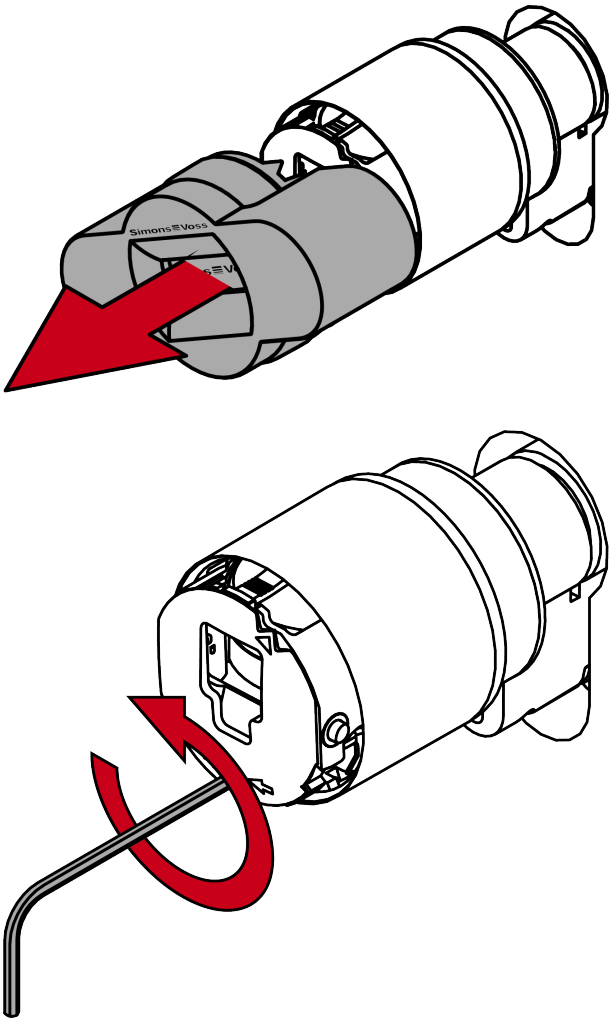
- Wear non-slip gloves.



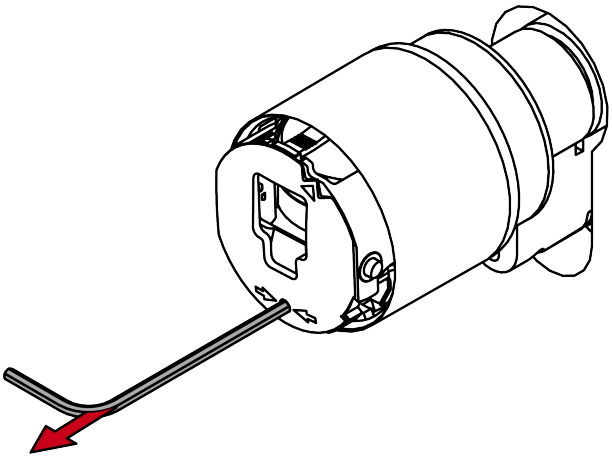
5. Remove the tool and cover.
6. Insert the hexagonal wrench into the hole provided until it stops.



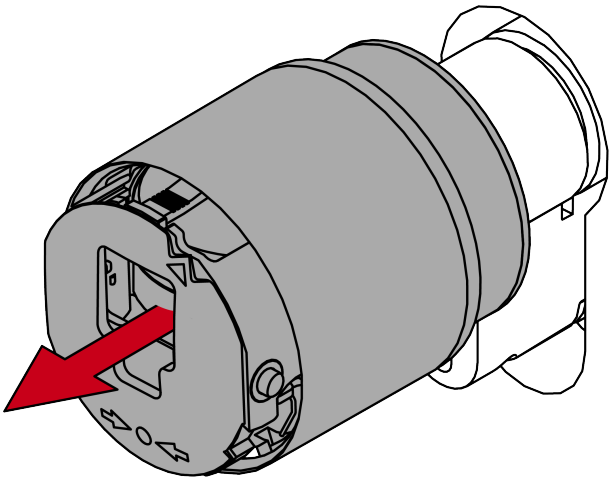
7. Turn the hex wrench 270 degrees counterclockwise.



8. Pull out the hexagon wrench again.



9. Pull off the thumb turn.



↳ Electronic thumb-turn is disassembled.

Functional test

Perform a function test after each installation and each battery change.

✓ Assembly or battery change completed
✓ SI Digital Cylinder AX programmed
✓ At least one identification medium authorised

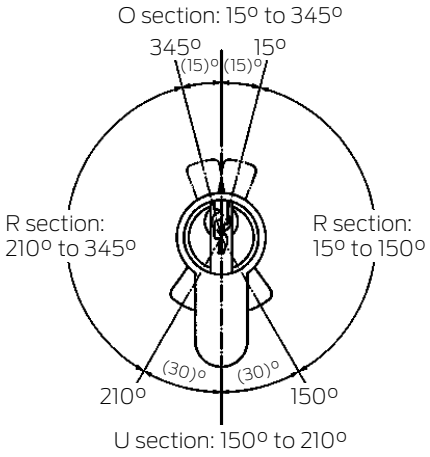
1. Pull hard on the electronic or mechanical thumb-turns.
2. Turn the electronic thumb-turns. The SI Digital Cylinder AX the AX locking cylinder must not be tight, nor rotate the tappet.
3. Activate an authorised identification medium.
4. Check that the SI Digital Cylinder AX engages and pushes out the locking bit.

↳ Mounting or battery change successfully completed.

AP functional test

Carry out a function test:

- After assembly
- After realignment
- After changes to the fastening screw



U section:	No restore force on the cam
R section:	Restore force section towards U section
O section:	Top dead point in dead bolt throw (no restore force on the cam)

✓ Functional test is carried out in escape direction.
✓ The dead bolt is retracted.

1. With the cylinder engaged, first turn the thumb-turn in the direction of locking as far as the dead bolt throw in the R section.
   ↳ Reset torque detectable...
2. Release the thumb-turn.
   ↳ Cylinder must automatically turn back into the U section.
3. Activate an authorised identification medium.
   ↳ Cylinder engages.
4. Turn the engaged thumb-turn in the locking direction of the lock through the R section into the O section.
   ↳ The dead bolt extends.
   ↳ No reset torque detectable.
5. Move the thumb-turn slightly over the threshold between the 'O' and 'R' section in the same direction of rotation.
6. Release the thumb-turn.
   ↳ The reset force must continue to turn the driver independently from this point to the U section.
   ↳ The dead bolt extends completely.
   ↳ If the thumb-turn does not automatically rotate as far as the 'U' section, either the fastening screw has been tightened too firmly or the locking device has been aligned incorrectly. The test is to be repeated after the fault has been eliminated. A fastening screw which has been tightened too firmly acts as a brake on the restoring force mechanism.

7. Lock the door and check that the locking device functions correctly by pressing the door fitting or panic bar in the direction of escape.
   ↳ The dead bolt must snap back.
   ↳ The door must open easily.
   ↳ If the dead bolt does not draw back when the handle is turned or the door fitting catches, either the locking cylinder or the locking device is incorrectly aligned or defective. The test is to be repeated after the fault has been eliminated as described above.

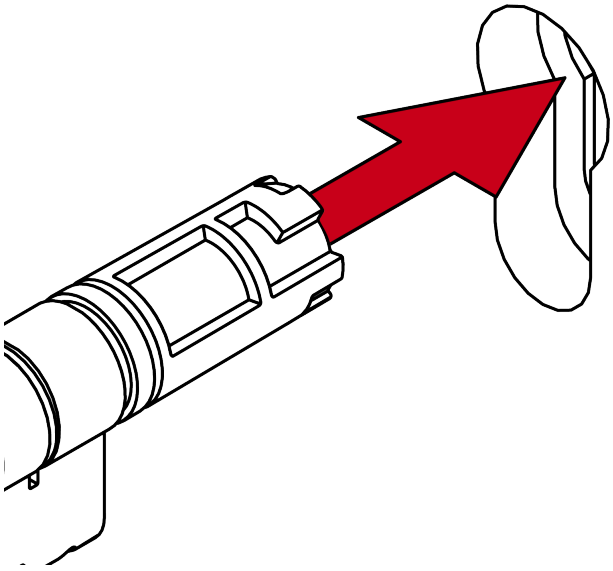
Insert locking cylinder

The SI Digital Cylinder AX is modular. You can disassemble both the mechanical and electronic thumb-turn. Accordingly, you have the choice:

- SI Digital Cylinder AX inserted with the mechanical side
- SI Digital Cylinder AX inserted with the electronic side

SI Digital Cylinder AX inserted with the mechanical side

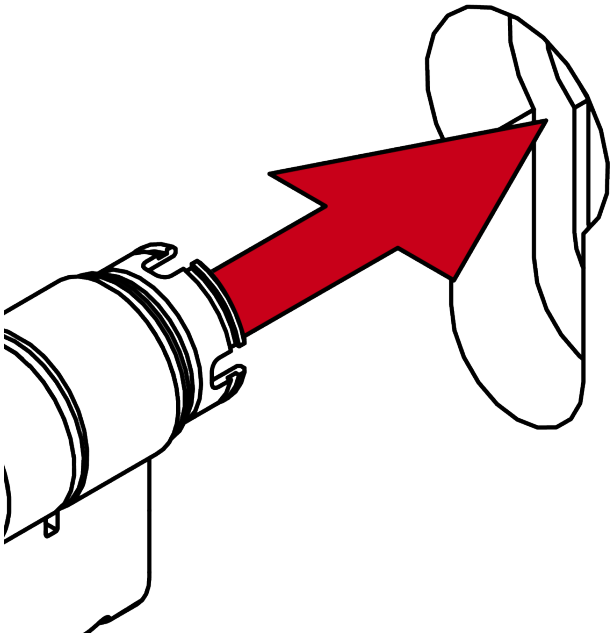
- Insert the locking cylinder AX with the thumb-turn-free side into the lock.



↳ AX locking cylinder is positioned in the lock.

SI Digital Cylinder AX inserted with the electronic side

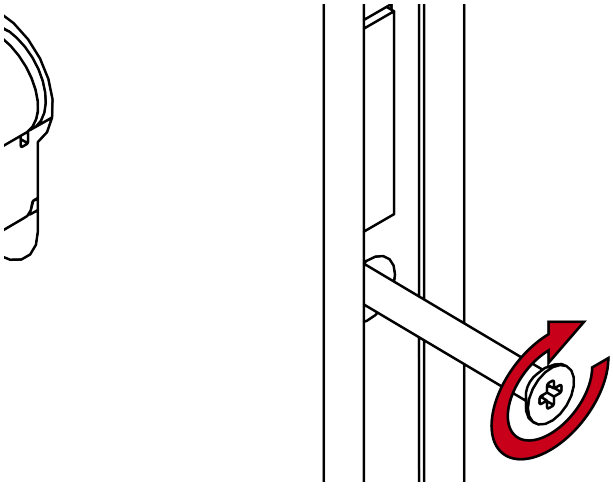
- Insert the locking cylinder AX with the thumb-turn-free side into the lock.



↳ You have positioned the AX locking cylinder in the lock.

Fixing the locking cylinder

- Screw the locking cylinder AX tight with the face plate screw.



↳ Locking cylinder AX is fixed in the lock.

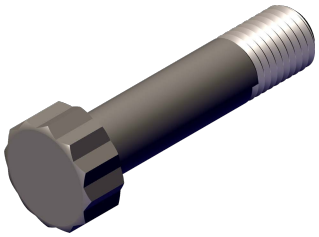
6.5.4 Tool

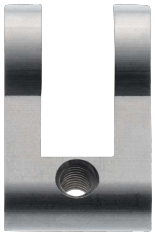
Installation	Battery replacement
Tools required: ■ Initial installation of Comfort variant without special tool ■ Further installation of the Comfort variant with special tool (in photo) ■ Installation of other variants with special tool ■ Always remove with special tool	Tools required: ■ Special tool (in photo)

The special tool shown can be obtained using order code Z5.TOOL.

The Euro Profile cylinder is modular (length modularity). Additional tools and components are required to change its length (for details see manual on length modularity):

Extractor (Z5.LIFTER)	SPACER (Z5.SPACER)	Terminal BLOCK (Z5.BLOCK)
		

Extension bolt	Core extension for the profile	Profile extension
 Z5.BOLT.XX (XX = required basic length)	 Z5.CORE.05: 5 mm Z5.CORE.10: 10 mm Z5.CORE.20: 20 mm	 Z5.PROFILE.05: 5 mm Z5.PROFILE.10: 10 mm Z5.PROFILE.20: 20 mm

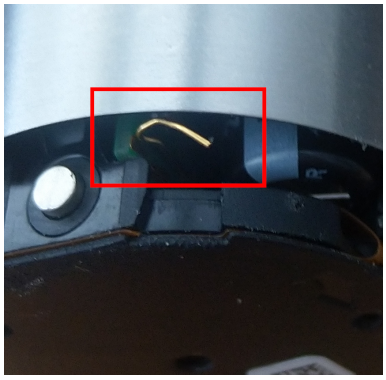
Clamps	Half cylinder centre piece	Cylinder centre piece
 Z5.CLAMPS Set contains 50 units.	 Z5.CNT.HZ	 Z5.CNT.EU

Cam (standard, WP)	Inside thumb-turn mount
 Z5.CAM.WP	 Z5.PR.IN

6.5.5 Cover contact

The SI Digital Cylinder AX uses a cover contact to detect whether the cap has been removed or placed in position. It detects every change, relays them in the system (WaveNet) and measures the battery level after it has been put back in position.

Also disengage SI Digital Cylinder AX those that are currently permanently engaged (permanent engaging, office mode or emergency opening).



6.5.6 Technical specifications

6.5.6.1 Euro Profile and SwissRound

Dimensions knob (Øxlength)	Ø 32 mm × 39.5 mm (electronic), Ø 32 mm × 37.5 mm (mechanical)
Basic length outside	30 mm, can be extended to 90 mm in 5 mm increments for Euro Profile (short cylinder: 25 mm, other lengths on request)
Basic length inside	30 mm, can be extended to 90 mm in 5 mm increments for Euro Profile (short cylinder: 25 mm, other lengths on request)
Material	Stainless steel
Colours	Standard: Brushed stainless steel, MS: Brass colour coated
Thumb-turn covers for reader thumb-turn	Plastic cap (passive/hybrid), metal ring cap (active), full metal cap (active)
VdS classification	Class BZ: applied for (Europrofile only)
SKG classification	In preparation (Europrofile only)
Weather protection	IP54 (standard), IP67 (.WP)
Temperature range (operation)	25 °C to +65 °C (according to DIN EN 15684)
Battery type	2x CR2450 3V (lithium) per reader thumb-turn, for battery thumb-turn: 6x
Approved battery manufacturers	Murata, Panasonic, Varta

Battery lifetime	Up to 12 years on standby or 100,000 activations (with battery knob: Up to 300,000 activations)
Signalisation	Audible signal (buzzer) and/or visual signal (LED – green/red)
Network capability	Yes (integrated LockNode can be ordered and retrofitted)
Opening modes	Pulse flip-flop
Upgradeability	Firmware upgradable via BLE
Frequency range; max. transmission power RFID (~13,56 MHz)	13.560006 MHz - 13.560780 MHz; 1.04 dBµA/m (3 m distance, depending on equipment)
Frequency range; max. transmission power (~868 MHz)	868.000 MHz - 868.600 MHz; <25 mW ERP (depending on equipment)
Frequency range; max. transmission power BLE	2402 MHz - 2480 MHz; 2.5 mW
Geographical restrictions within the EU	No

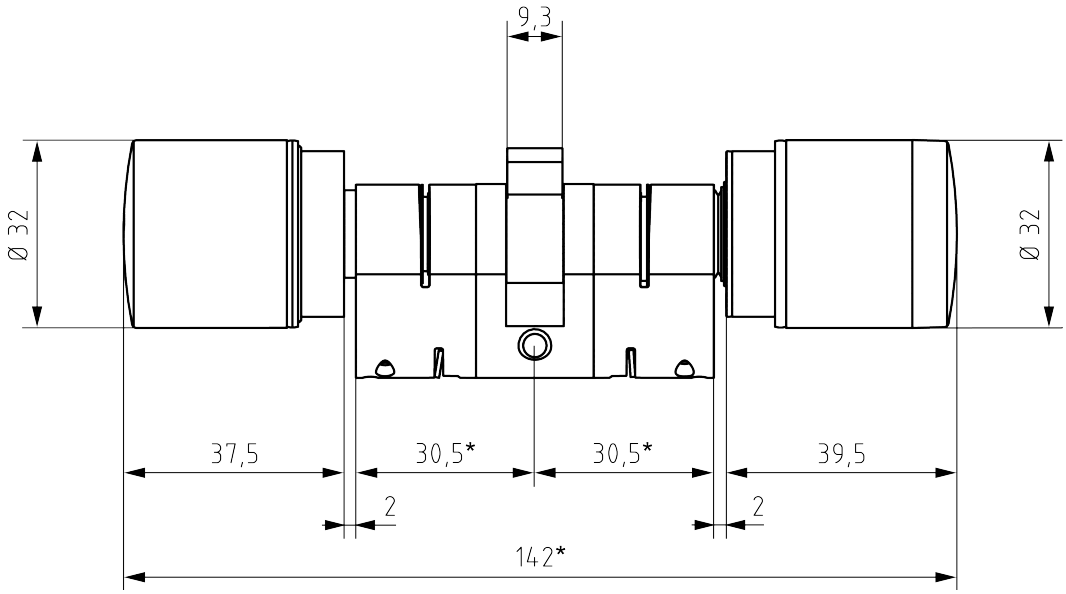
6.5.6.2 Scandinavian Oval Scandinavian Round

Dimensions knob (Øxlength)	Ø 32 mm × 39.5 mm (electronic), Ø 32 mm × 37.5 mm (mechanical)
Material	Stainless steel
Colours	Standard: Brushed stainless steel, MS: Brass colour coated
Thumb-turn covers for reader thumb-turn	Plastic cap (passive/hybrid), metal ring cap (active), full metal cap (active)
Weather protection	IP54 (standard), IP67 (.WP)
Temperature range (operation)	25 °C to +65 °C (according to DIN EN 15684)
Battery type	2x CR2450 3V (lithium) per reader thumb-turn, for battery thumb-turn: 6x
Approved battery manufacturers	Murata, Panasonic, Varta

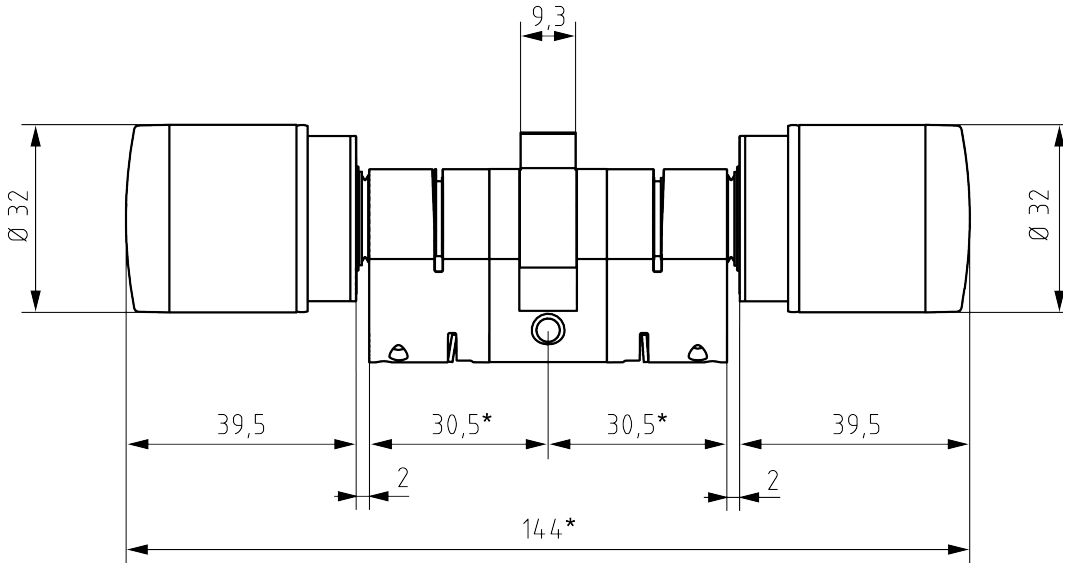
Battery lifetime	Up to 12 years on standby or 100,000 activations (with battery knob: Up to 300,000 activations)
Signalisation	Audible signal (buzzer) and/or visual signal (LED – green/red)
Network capability	Yes (integrated LockNode can be ordered and retrofitted)
Opening modes	Pulse flip-flop
Upgradeability	Firmware upgradable via BLE
Frequency range; max. transmission power RFID (~13,56 MHz)	13.560006 MHz - 13.560780 MHz; 1.04 dBµA/m (3 m distance, depending on equipment)
Frequency range; max. transmission power (~868 MHz)	868.000 MHz - 868.600 MHz; <25 mW ERP (depending on equipment)
Frequency range; max. transmission power BLE	2402 MHz - 2480 MHz; 2.5 mW
Geographical restrictions within the EU	No

6.5.6.3 Dimensions

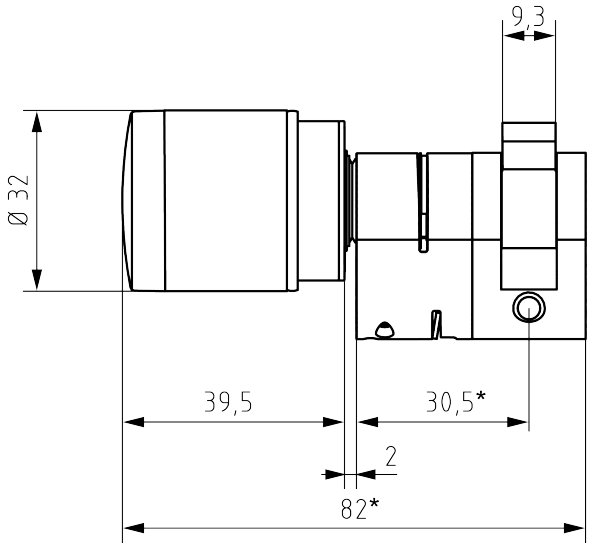
CO (comfort cylinder)



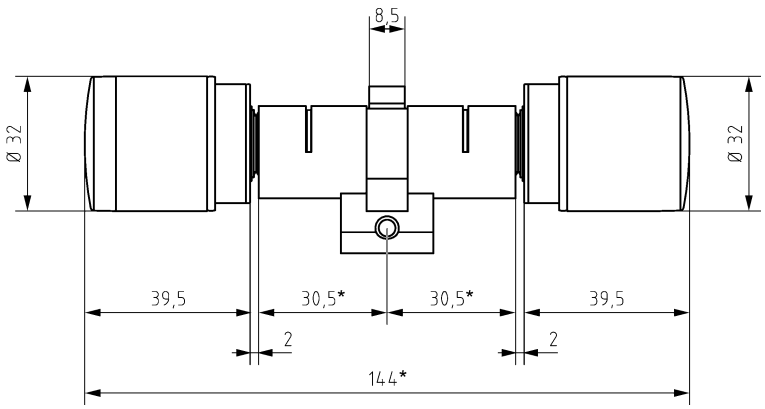
FD (free-rotating cylinder)



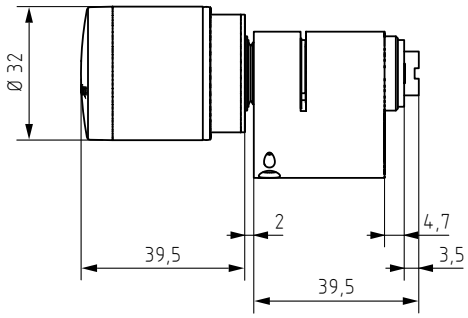
HZ (Half cylinder)



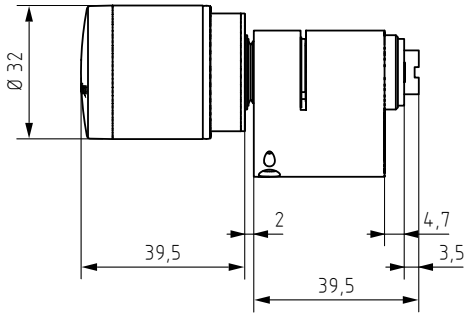
SR (Swiss round profile)



SO (Scandinavian Oval)



RS (Scandinavian Round)



6.6 Locking cylinder (TN4)

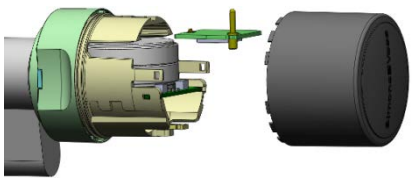
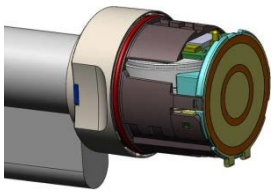
The locking cylinder moves the bolt of the mortise lock. Use a locking cylinder if you want to lock doors.

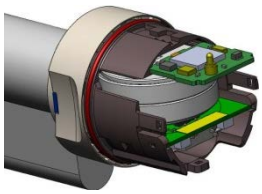
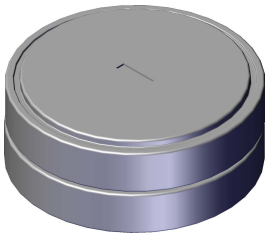
6.6.1 Structure

Locking cylinders basically consist of two halves:

Master (Central Unit = CU)	Slave
Thumb-turn cannot be removed.	Knob can be removed for installation.
Identifier: Black ring between thumb-turn and profile cylinder.	

Locking cylinders consist of several parts:

	Control Unit (CU): Assembly under the battery compartment of the master knob
	Card reader (Card Reader = CR): Master reader (for cylinders which can be read on both sides (FD and BL): additional slave reader)

	LockNode (LN): Assembly above the battery compartment of the master knob
	Batteries in the battery compartment of the master knob

The locking cylinder should always be installed with the inner side inside. You will find the marking on the inside:

- In the dimensional drawings (see *Dimensional drawings cylinder [▸ 62]*)
- On the profile housing (IN)

Comfort (CO)	Page	Behaviour (disengaged state)	Components	Batteries
Master	Outside	Freely rotating	▪ Control Unit ▪ Card reader	2
Slave	Inside	Permanently engaged	No electronics	None

Freely rotating (FD)	Page	Behaviour (disengaged state)	Components	Batteries
Master	Inside	Freely rotating	▪ Control Unit ▪ Card reader	2
Slave	Outside	Freely rotating	Second control unit	2

Anti-panic freely rotating (AP2 FD)	Page	Behaviour (disengaged state)	Components	Batteries
Master	Outside	Freely rotating	▪ Control Unit ▪ Card reader	2
Slave	Inside	Engage not possible	No electronics	None

Anti-panic, read on both sides (AP2 BL)	Page	Behaviour (disengaged state)	Components	Batteries
Master (inner)	Reversible	Freely rotating	▪ Control Unit ▪ Card reader ▪ LockNode	2
Slave (external)		Freely rotating	▪ Control Unit ▪ Card reader	2

NOTE

Programming error during interrupted or changed master-slave pairing

The master and slave are factory configured as belonging together. Replacing knobs will result in programming errors.

Master and slave communicate during programming.

- Make sure that the master and slave are physically connected during programming.

6.6.2 Variants and features

The order number provides information about the variant and the equipment features:

General	SI	SmartIntego cylinder
	Z4	Technology level 4
	AXX-IXX	Exterior dimension Interior dimension
	▪ MI (for SmartIntego WirelessOnline) ▪ M (for SmartIntego Virtual Card Network)	▪ **M**IFARE & LockNode **I**ntegrated (for SmartIntego Wireless Online) MIFARE Integrated is an abbreviation for *MIFARE technology with integrated LockNode*. ▪ **M**IFARE (for SmartIntego Virtual Card Network)

Structure	CO	Comfort cylinder permanently engaged on the inside
	FD (SmartIntego Wireless Online only)	Freely rotating - cylinder with two card readers (inside and outside) Different access authorisations possible (integrator-dependent)
Features	WP	Weatherproof version (IP 66), otherwise IP54
	AP2	Anti-panic function
	BL	Double-sided reading (only available together with anti-panic function for SmartIntego Wireless Online)
	DK	Removable thumb-turn (e.g. for installation behind panels without cylinder perforation, only available as half cylinder)
	HZ	Half cylinder
	MR	Multi-point version
	MS	Brass version
	OK	Without internal thumb-turn
	SL	Self-locking (only available as half cylinder)

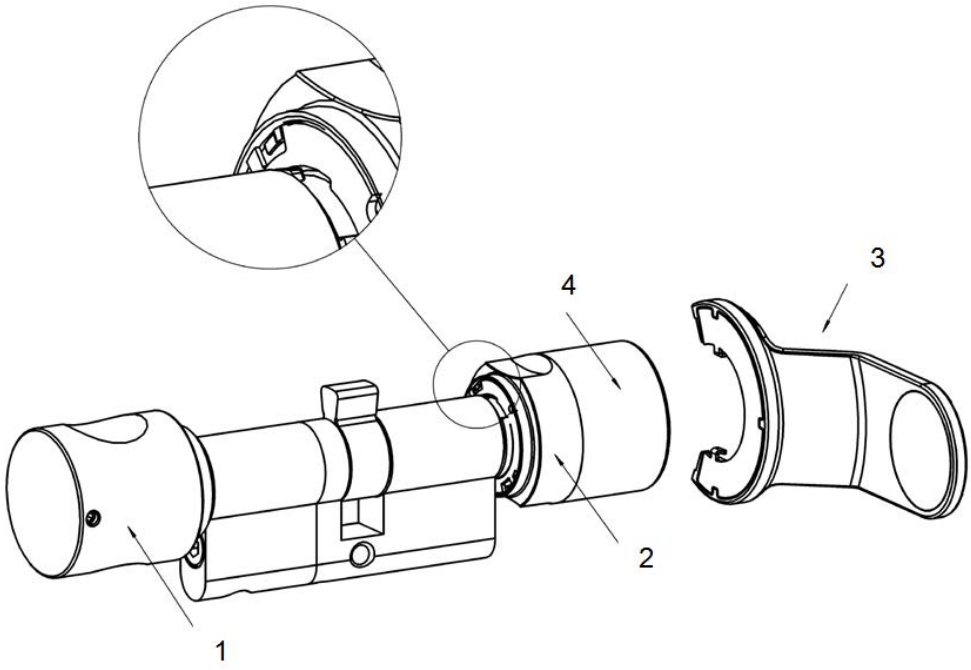
NOTE

Avoidance of incorrect orders through the order placement guide

SmartIntego components offer a wide variety of combinations. Not every combination makes sense and is actually available. A manual compilation of the product features can lead to combinations that are not available or to incorrect orders.

- Always use the order placement guide from the partner area of the SmartIntego website (*www.smartintego.com)*).

6.6.3 Installation



1. Inside thumb-turn
2. Recessed handle ring
3. Battery replacement key
4. Outer thumb-turn

The slave thumb-turn is installed with the installation or battery replacement key. The exact procedure is described in the short instructions supplied with the locking cylinder.

6.6.4 Tool

Installation	Battery replacement
Tools required: ■ Installation key ■ Battery replacement key (shown)	Tools required: ■ Battery replacement key (shown) and ■ Battery replacement card (see step-by-step instructions)

The illustrated battery replacement key is available with order number Z4.KEY.

6.6.5 Technical specifications

Profile cylinder

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

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

Ambient conditions

Operating temperature:	-25°C to +65°C
Protection class:	Standard protection rating IP54 (when installed); .WP variant: IP 66
Air humidity:	< 95%; non-condensing

Batteries

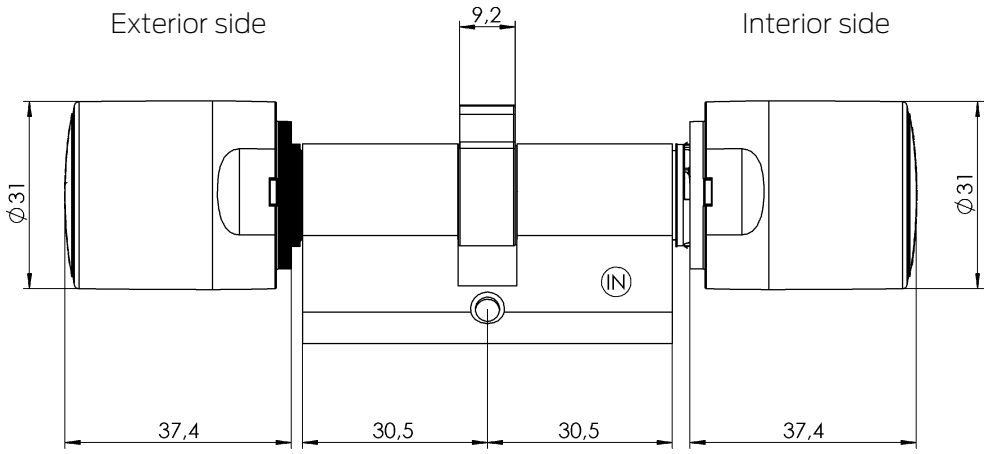
Type:	CR, 2450, 3 V
Manufacturer:	Murata, Panasonic, Varta

Quantity:	2 units
Battery life:	SmartIntego Wireless Online (WO): ■ Up to 5 years ■ Up to 80,000 activations Card SmartIntego Virtual Card Network (SVCN): ■ Up to 6 years ■ Up to 50,000 activations

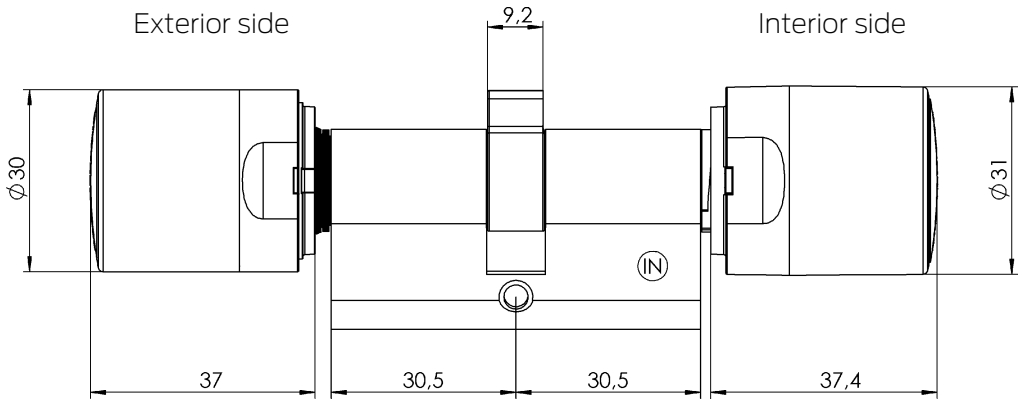
The cylinder provides acoustic and optical (blue/red LED) feedback.

6.6.6 Dimensional drawings cylinder

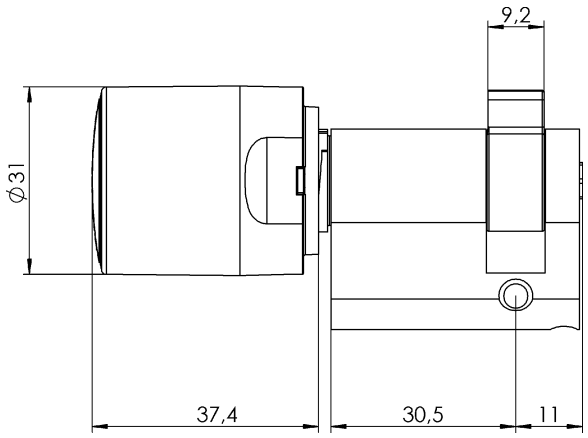
Comfort - Passive (CO MP)



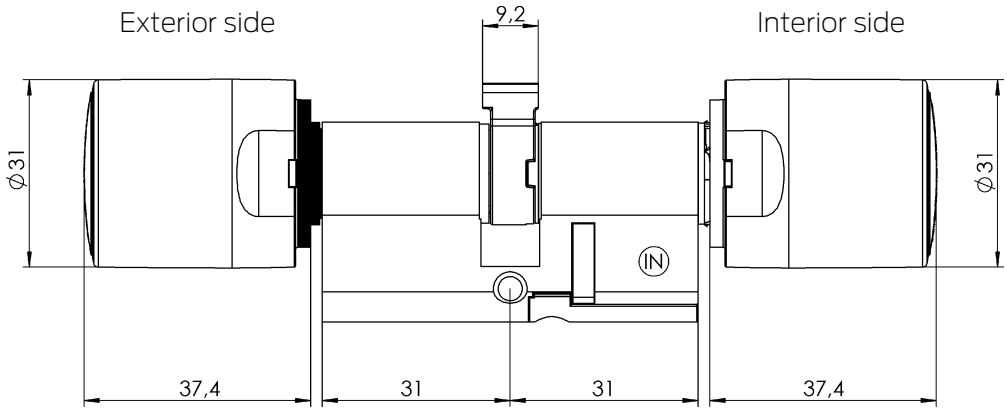
Freely rotating - Passive/hybrid (FD MP/MH)



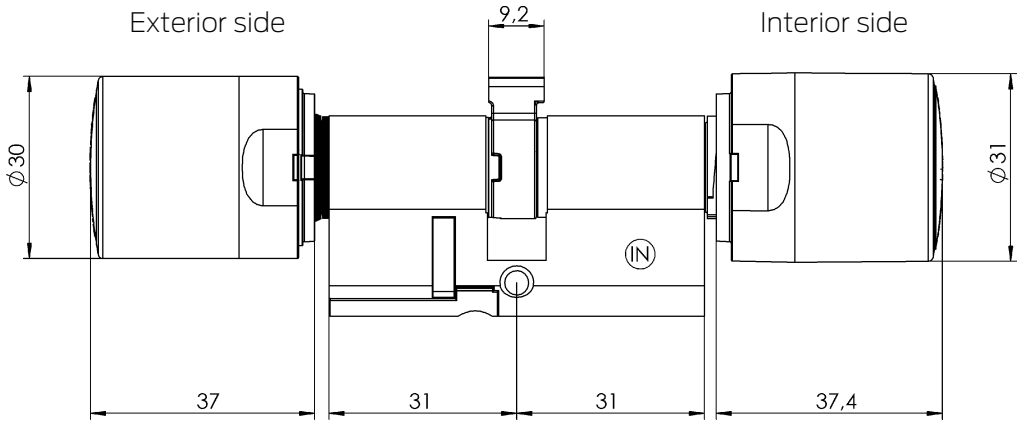
Half Cylinder - Passive (HZ MP)



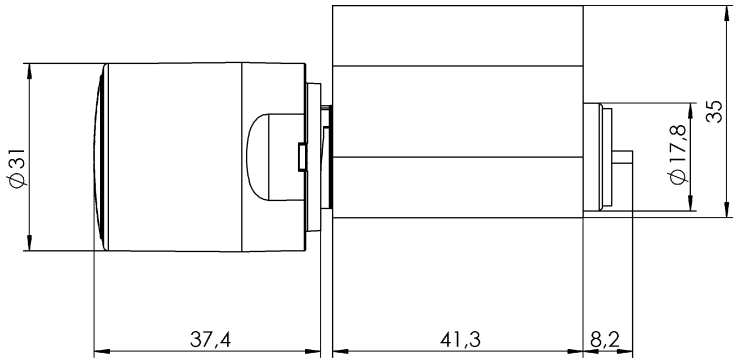
Anti-panic Free rotating - passive (AP2 FD MP)



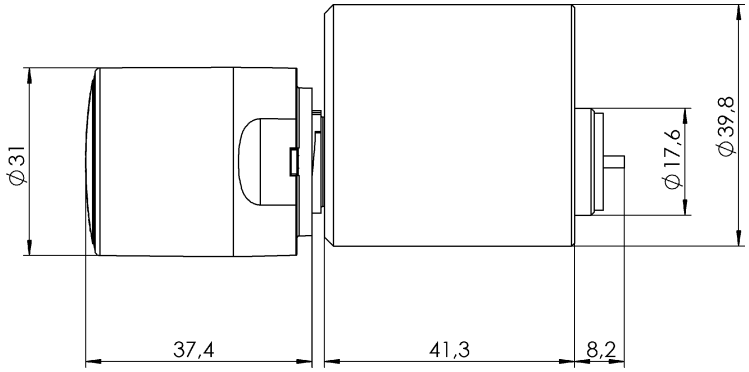
Anti-panic Reader on both sides - Passive (AP2 BL MP)



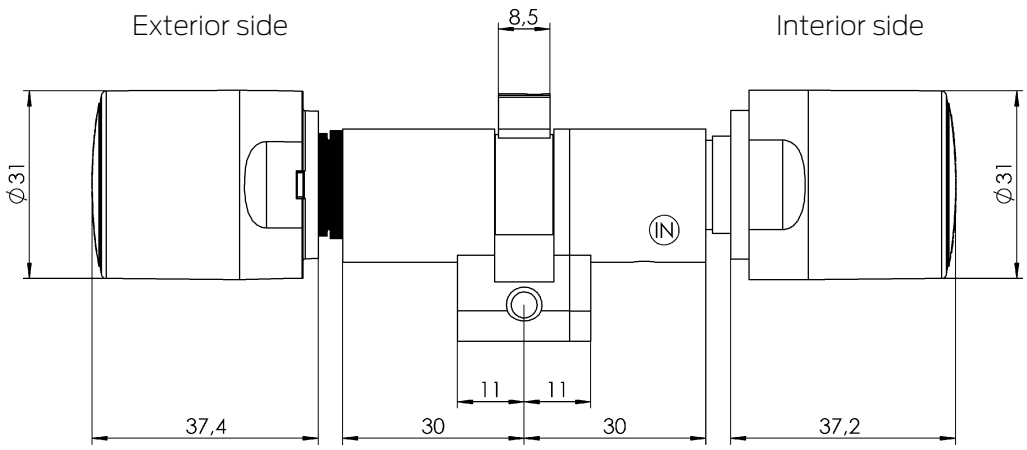
Scandinavian Oval - Passive (SO MP)



Scandinavian Round - Passive (RS MP)



Swiss Round Comfort - Passive (SR CO MP)



6.7 SmartHandle AX

SmartHandle AX moves the latch of the mortise lock. Use SmartHandle AX or SmartHandle 3062 if you only want to close doors (internal doors).

If doors are also to be locked, you can combine a SmartHandle with a self-locking mortise lock.

Variants, equipment features, assembly...

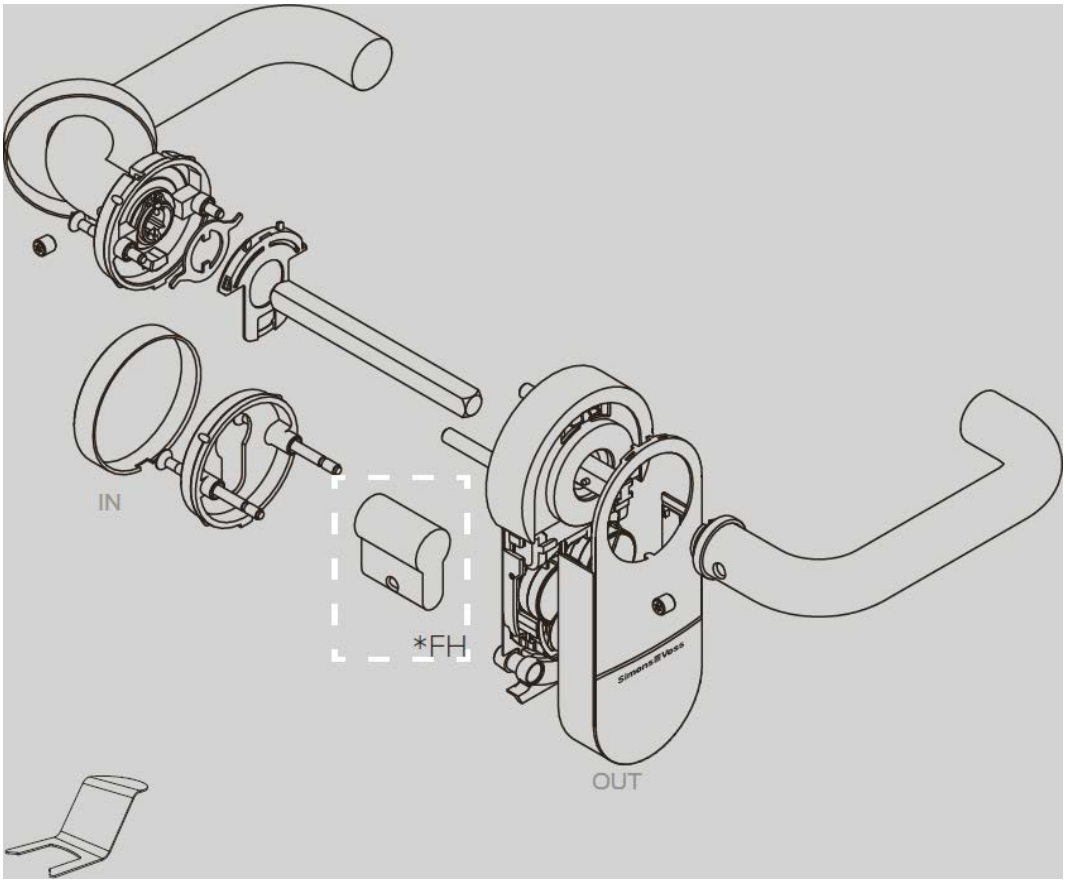
Please refer to the manual of SI.SmartHandle AX for more information.

6.7.1 Structure

SmartHandle AX contains all the electronics on the outside:

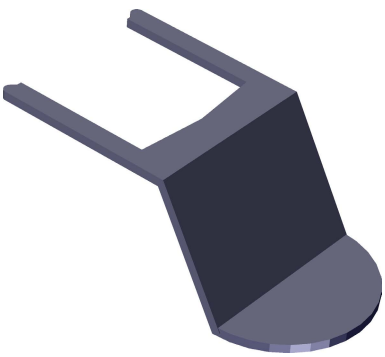
- Control Unit (CU)
- Card Reader (CR)
- LockNode (LN)
- Batteries

SmartHandle AX is available in several versions. The figure shows, for example, the structure with the suspended installation:



6.7.2 Tool

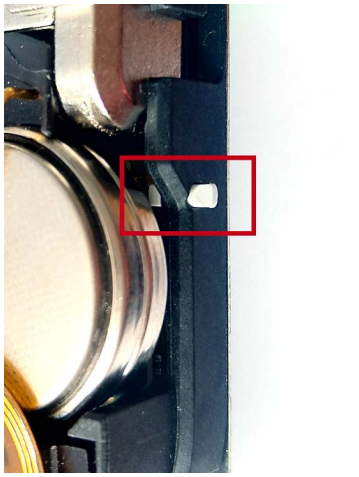
The supplied SmartHandle tool is required to remove the cover. For further tools required, please refer to the supplied quick guide.



6.7.3 Cover contact

The SI.SmartHandle AX uses a sabotage contact to detect whether the housing has been removed or fitted into position. It senses every change and forwards it (WaveNet) and measures the battery level after it has been restored.

Also disengage SI.SmartHandle AX those that are currently permanently engaged (permanent engaging, office mode or emergency opening).



6.7.4 Technical specifications

Types	■ Euro Profile cylinder ■ Scandinavian Oval ■ Swiss Round
Read systems	■ Passive ■ BLE ready
Supported cards (Wireless Online WO)	■ MIFARE® Classic ■ MIFARE DESFire® EV1/EV2 ■ UID (card serial number) according to ISO 14443 (e.g. MIFARE, Legic Advant, HID® SEOS)
Supported cards (SmartIntego Virtual Card Network SVCN)	■ MIFARE® Classic ■ MIFARE DESFire® EV1/EV2
Reading ranges	Near field
Power supply	
Battery type	4× CR2450 (3 V)

Battery manufacturer	■ Murata ■ Varta ■ Panasonic
Battery life (Wireless Online WO)	■ Up to 180,000 activations ■ Up to 9 years stand-by without operation
Battery life (SmartIntego Virtual Card Network SVCN)	■ Up to 150,000 activations ■ Up to 9 years stand-by without operation
Ambient conditions	
Temperature range	Operational: -25 °C to +50 °C
	In storage (temporary): -40 °C to +50 °C
	In storage (long-term): 0 °C to +30 °C
Protection rating	IP40
Feedback	
Signalling	■ Acoustic (beeper) ■ Optical (two-colour LED)
Administration and settings	
Networking capability	■ Wireless Online (WO): Integrated LockNode (LNI) ■ SmartIntego Virtual Card Network (SVCN): Not network-compatible
Other information	
Can be upgraded	Upgradeable firmware
Entrys in the access list	Max. 1,000

Radio emissions		
SRD (WaveNet)	868.000 MHz - 868.600 MHz	<25 mW ERP

There are no geographical restrictions within the EU.

6.7.4.1 Mechanical system

Dimensions

The dimensions refer to the side with the electronic fitting.

Height	■ A0 (standing) ■ A3 (tubular frame) ■ DS (reader on both sides)	120 mm
	A1 (suspended, short)	140 mm
	■ A2 (suspended, long) ■ E0/E1 (Scandinavian Oval)	174 mm
	A4 (panic bar)	■ BKS (centres distance: 72 mm): 193.4 mm ■ BKS (centres distance: 92 mm): 213.4 mm ■ CISA (centres distance: 72 mm): 224.4 mm (information with adapter plate)
Width	66 mm	

Depth	■ A0 (standing) ■ A1 (suspended, short) ■ A2 (suspended, long) ■ E0/E1 (Scandinavian Oval)	21 mm
	A3 (tubular frame)	26 mm (information with adapter plate)
	A4 (panic bar)	25 mm (information with adapter plate)
	DS (reader on both sides)	■ 21 mm (side without adapter plate) ■ 26 mm (side with adapter plate

You will find detailed dimension drawings at the end of the section.

Centres distances and door thicknesses

A* = Euro profile, B* = Swiss round, E* = Scandinavian Oval

Versions	Centres distance	Door thickness
A0/B0 Stationary	not relevant (stationary installation: Handle shaft axis and profile cylinder axis not connected at the fitting)	S: 38 - 60 mm
		M: 59 - 80 mm
		L: 79 - 100 mm
		X: 100–200 mm
A1/B1 Suspended, short	70 - 79 mm	S: 38 - 60 mm
		M: 59 - 80 mm
		L: 79 - 100 mm
		X: 100–200 mm
A2/B2 Suspended, long	70 - 110 mm	S: 38 - 60 mm
		M: 59 - 80 mm
		L: 79 - 100 mm
		X: 100–200 mm

Versions	Centres distance	Door thickness
A3 Metal frames	not relevant (stationary installation: Handle shaft axis and profile cylinder axis not connected at the fitting)	S: 38 - 57 mm
		M: 58 - 77 mm
		L: 78 - 97 mm
		X: 97 - 196 mm
A4 Panic bar	92 mm (BKS full-leaf door without plate) 72 mm (CISA full-leaf door, with plate or BKS full-leaf door without sign)	S: 38 - 60 mm
		M: 59 - 80 mm
		L: 79 - 100 mm
		X: 100–200 mm
DS Reader on both sides (double-sided)	not relevant (stationary installation: Handle shaft axis and profile cylinder axis not connected at the fitting)	S: 38 - 58 mm
		M: 59 - 78 mm
		L: 79 - 99 mm
		X: 100–200 mm
E0, E1 Scandinavian Oval	105 mm	S: 38 - 60 mm
		M:59 - 80 mm
		L: 79 - 100 mm
		X: 100–200 mm

Handle turning angle and colours

Handle turning angle		48° effective
Colours	Cover	■ Traffic white (RAL 9016) ■ Dark grey (RAL 7021) ■ Brass Also see Surface finishes for cover colours
	Escutcheon	■ Brushed nickel, coated ■ Brushed brass, coated
	Handle	■ Brushed stainless steel, painted ■ Brushed brass, coated

Dimensional drawings SmartHandle AX

NOTE

Height depends on the variant (see table).

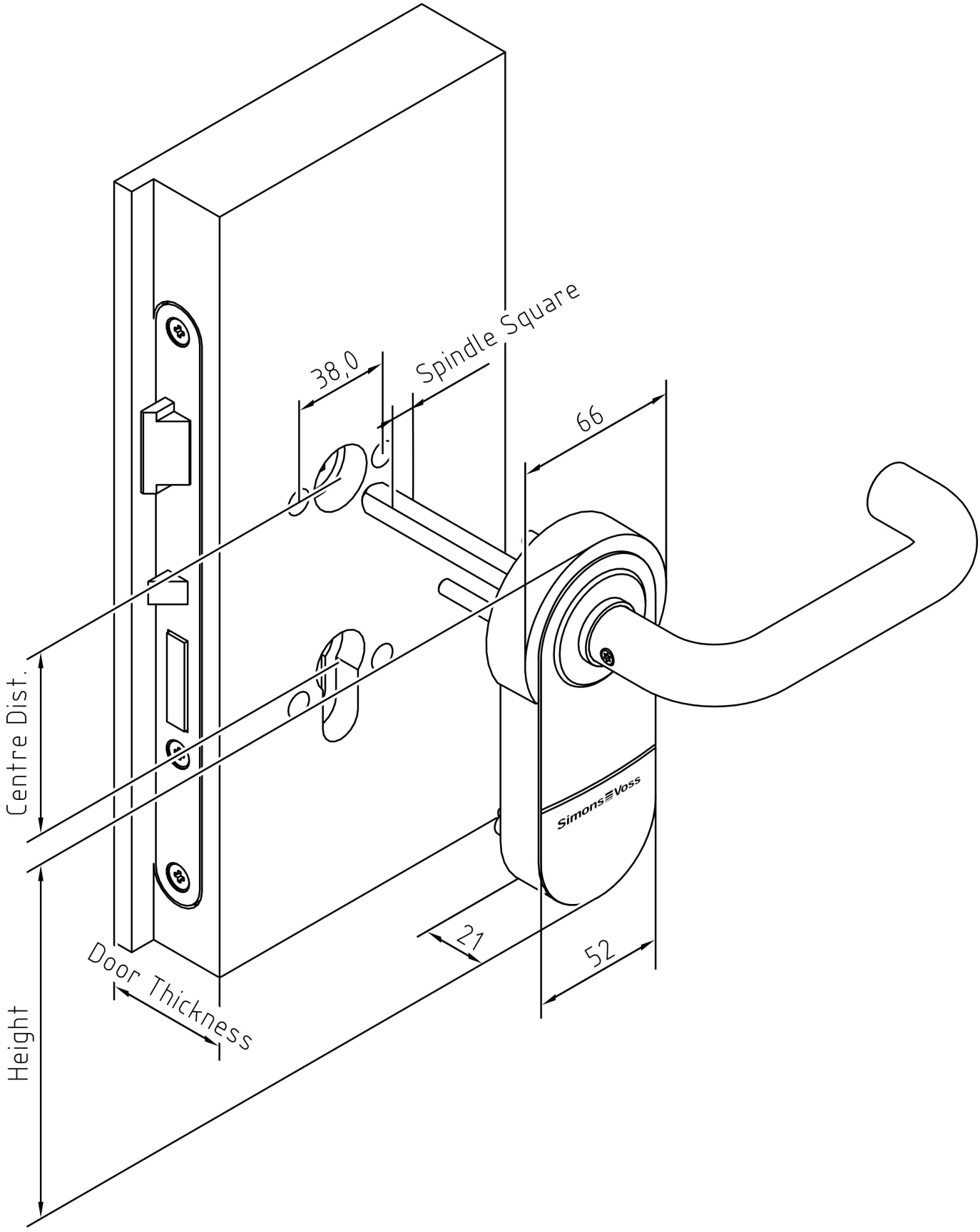


Fig. 1: Dimensioning SmartHandle AX suspended (A1, A2)

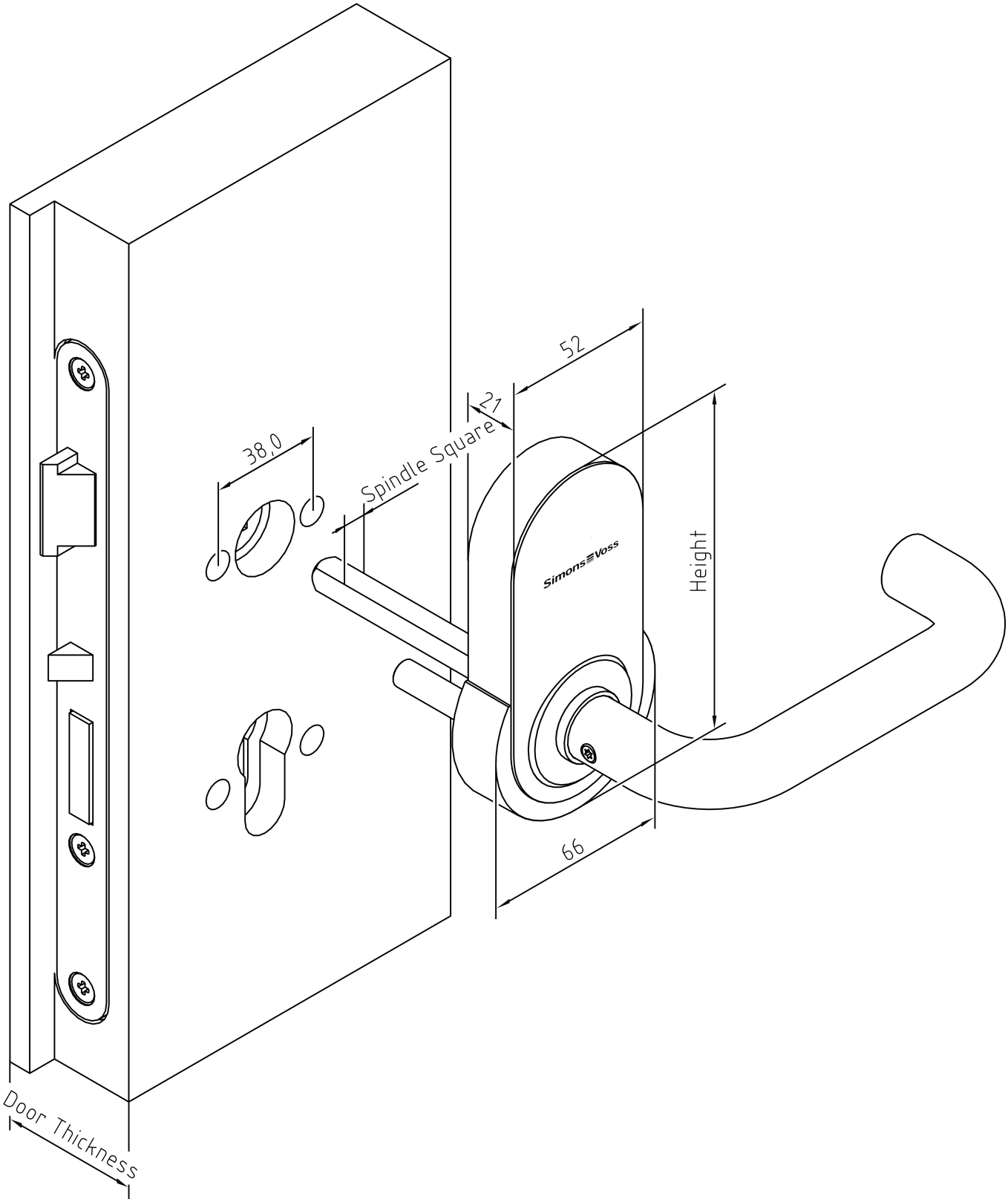


Fig. 2: Dimensioning SmartHandle AX stationary (A0)

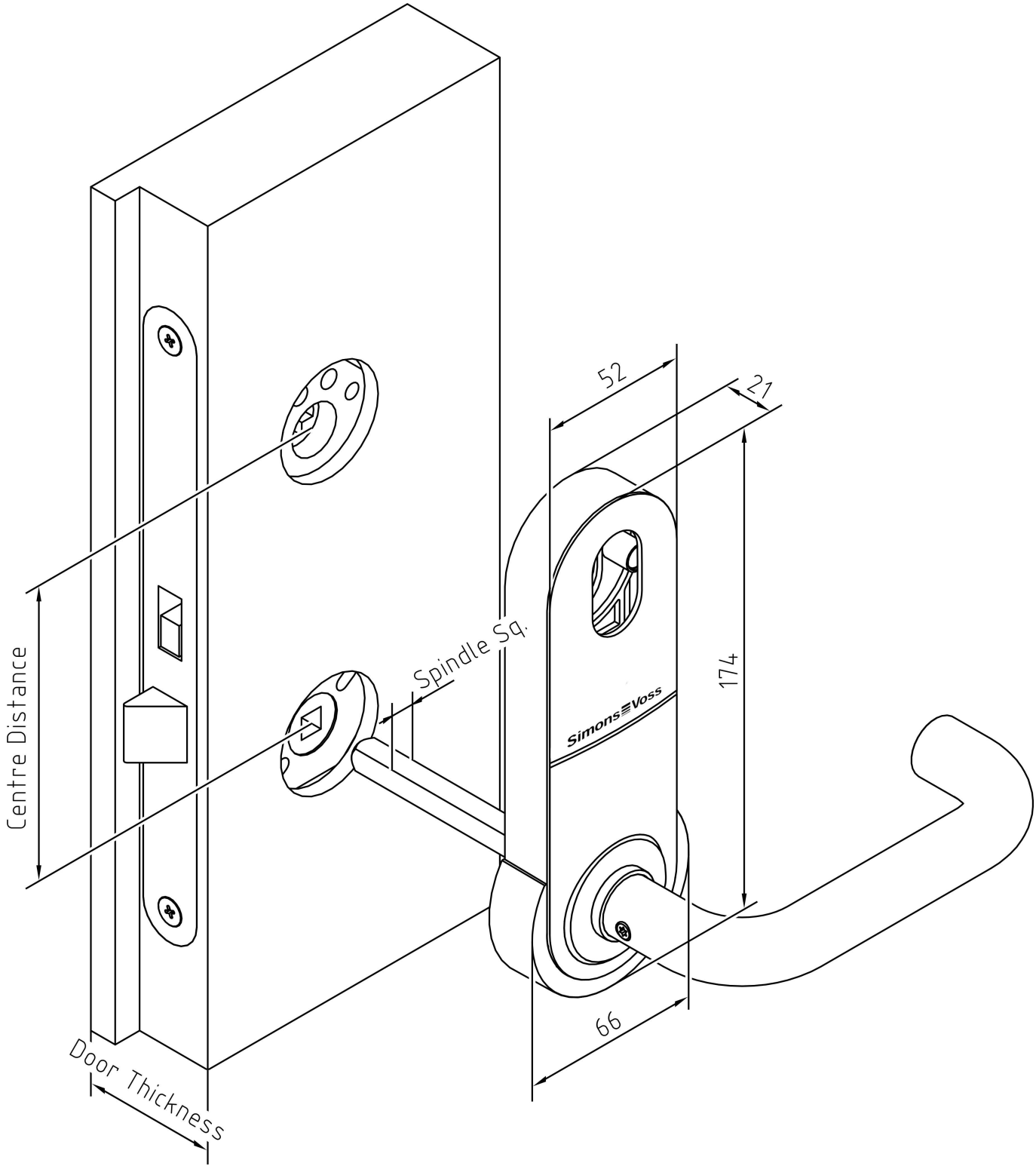


Fig. 3: Dimensioning SmartHandle AX Scandinavian Oval (E0, E1)

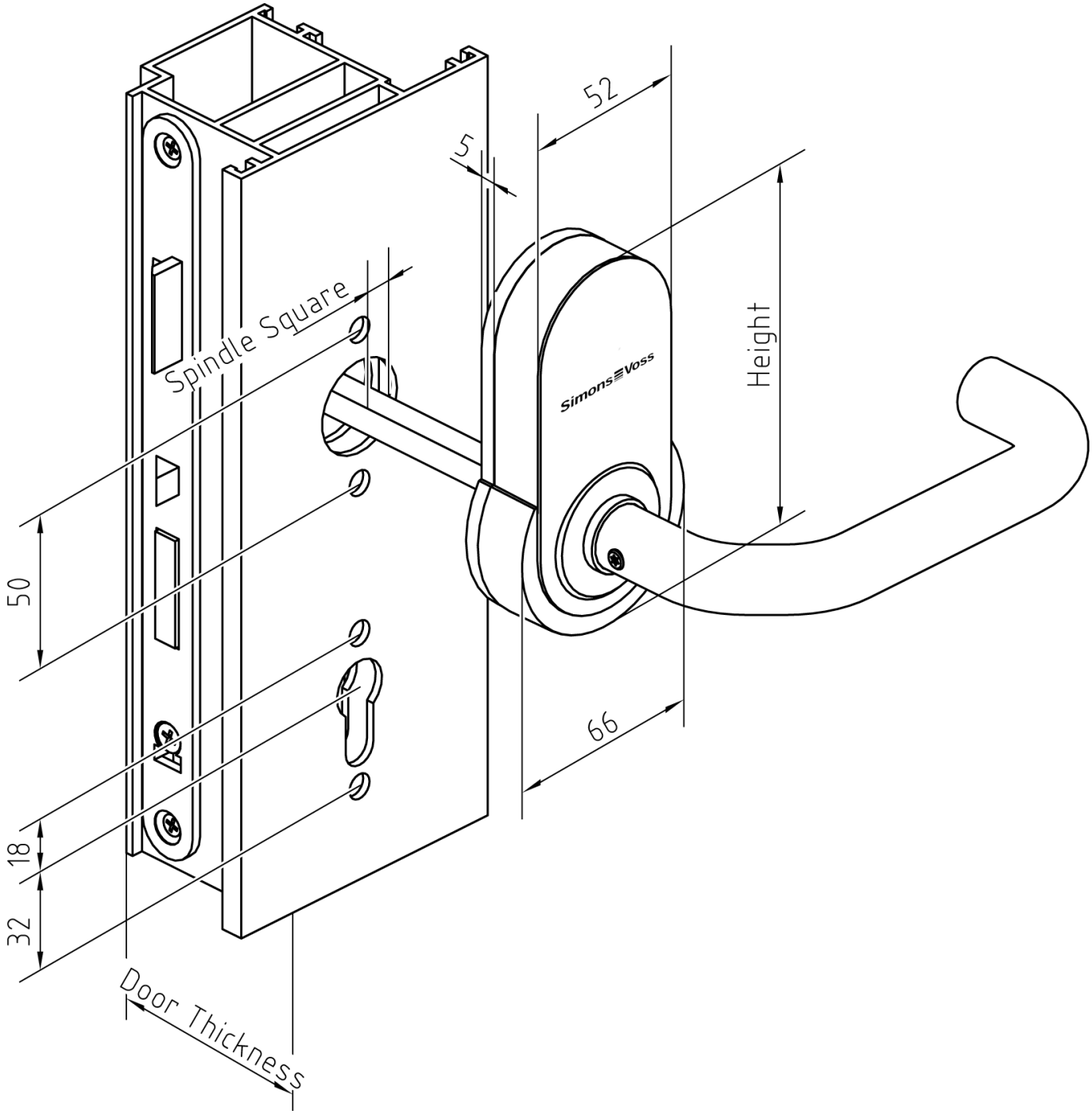


Fig. 4: Dimensioning SmartHandle AX metal frame (A3)

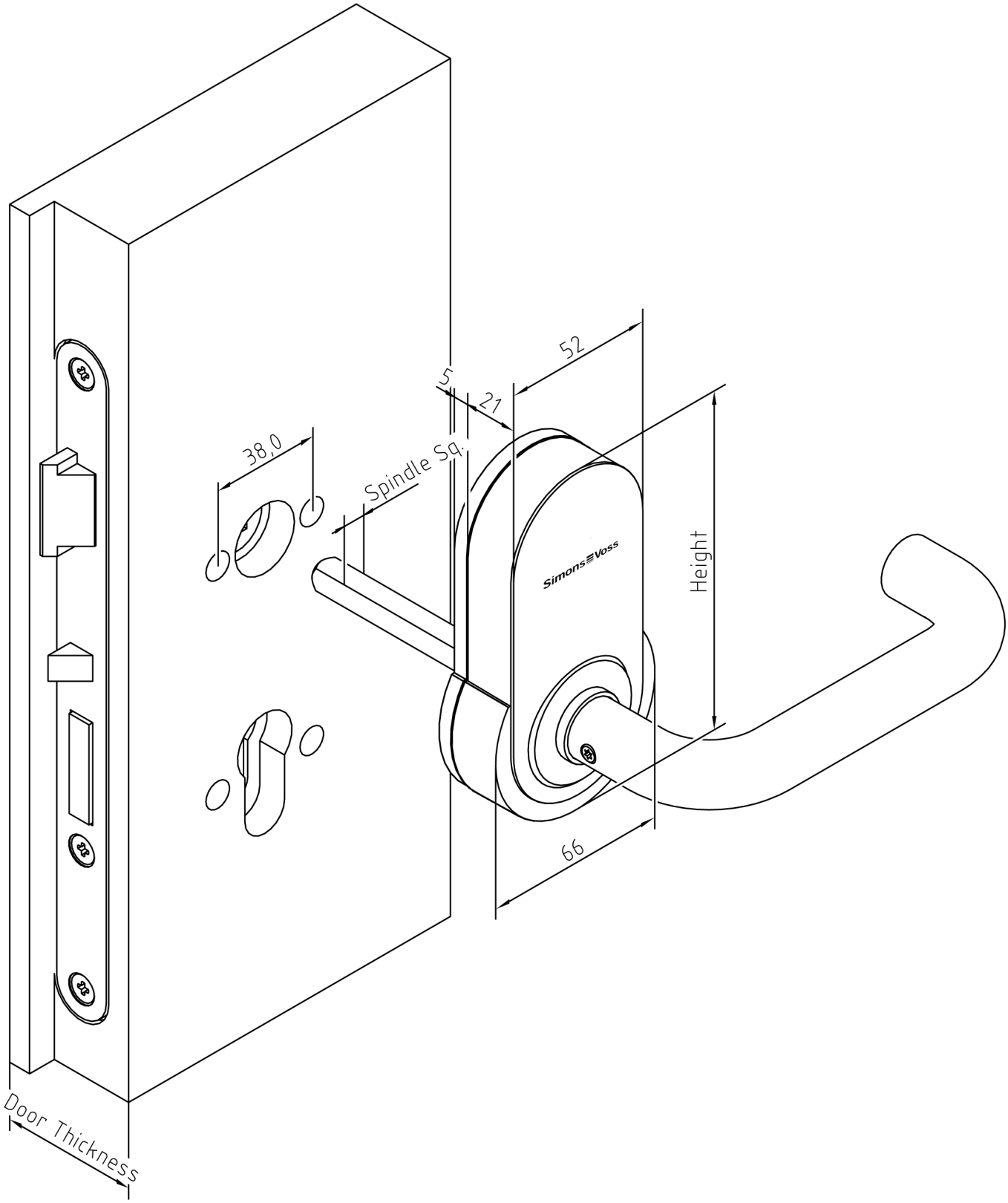
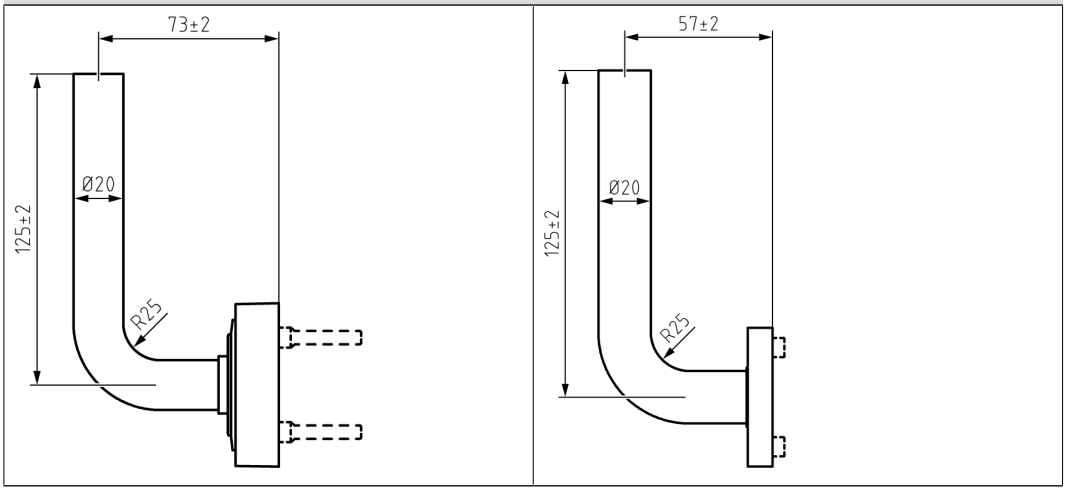


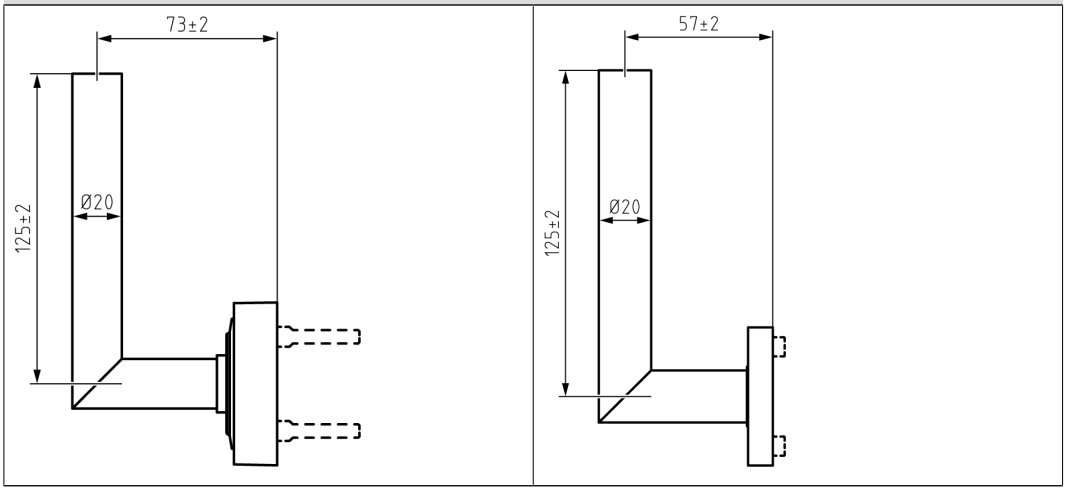
Fig. 5: Dimensioning SmartHandle AX BSL (DS)

Dimensional drawings handles

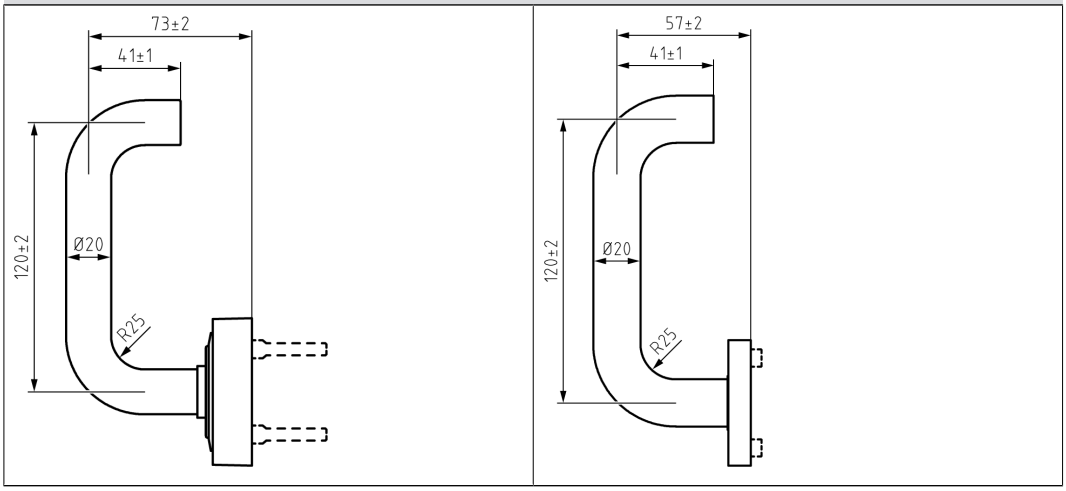
Shape A (Outside/Inside)

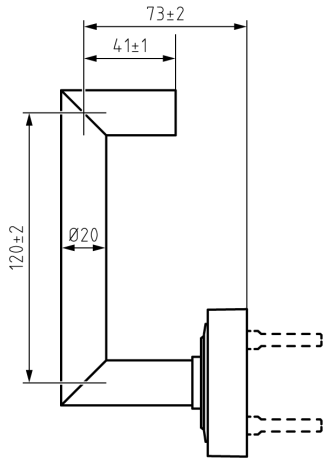
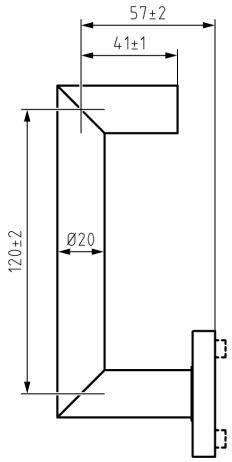
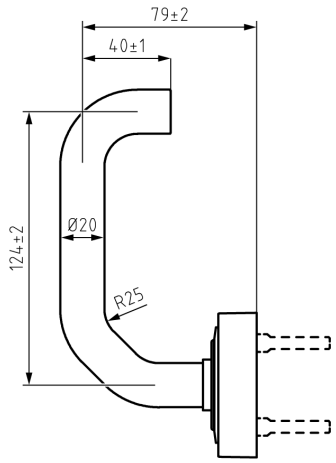
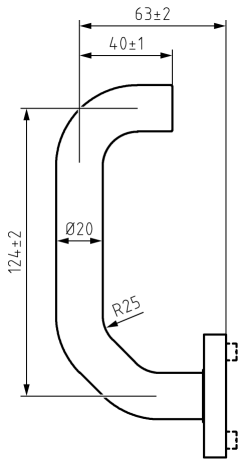


Shape B (Outside/Inside)



Shape C (Outside/Inside)



Shape D (Outside/Inside)	
	
Shape L (Outside/Inside)	
	

6.8 SmartHandle 3062

SmartHandle 3062 moves the latch of the mortise lock. Use SmartHandle AX or SmartHandle 3062 if you only want to close doors (internal doors).

If doors are also to be locked, you can combine a SmartHandle with a self-locking mortise lock.

Variants, equipment features, assembly...

Please refer to the manual of SI:SmartHandle for more information.

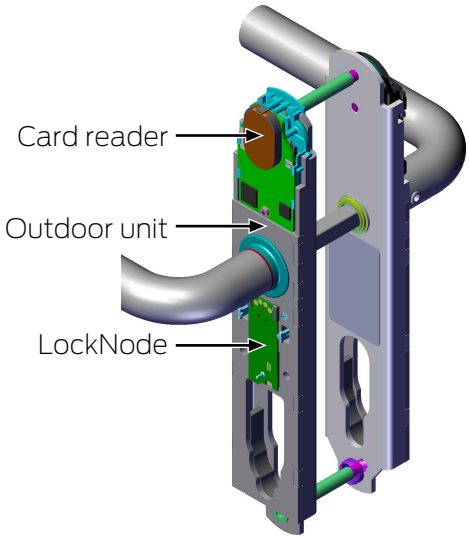
6.8.1 Structure

SmartHandle 3062 always consists of two sides:

Master (inner side)	Slave (outside)
■ Central Unit (= CU)	■ Card Reader (CR)
■ Batteries	■ LockNode (LN)

Master (inner side)	Slave (outside)
■ Always inside the door ■ Permanently engaged	■ Always on the outside of the door ■ Can only be engaged with identification medium

During installation, the two halves are separated from each other.



The body differs depending on the variant and equipment:

Escape&Return (.ER)

Master (inner side)	Slave (outside)
■ Central Unit (= CU) ■ Batteries ■ Sensors for Escape&Return	■ Card Reader (CR) ■ LockNode (LN)
■ Always inside the door ■ Permanently engaged	■ Always on the outside of the door ■ Can only be engaged with identification medium

DoorMonitoring (.DM)

DoorMonitoring SmartHandles use sensors to detect different door statuses.

Master (inner side)	Slave (outside)

■ Central Unit (= CU)
■ Batteries
■ Sensors for DoorMonitoring
  ■ Inside handle sensor
  ■ Bolt (only together with a self-locking mortise lock in which a SimonsVoss sensor or a third-party sensor is optionally installed - see list of compatible sensor locks)
  ■ Fastening screw sensor in mortise lock
	■ Card Reader (CR)
	■ LockNode (LN)

■ Always inside the door ■ Permanently engaged	■ Always on the outside of the door ■ Can only be engaged with identification medium

The sensitivity of the sensors is set in the SmartIntego tool. If one of the sensors detects a change, this change is immediately forwarded to the integrator system.

DoorMonitoring SmartHandle 3062 can detect the following statuses:

- Engaged/Disengaged
- Handle pressed/not pressed (inside handle and, if engaged, also outside handle)
- Door open
- Door closed
- Door open too long (adjustable timer in SmartHandle)
- Door closed after open too long
- Door locked (only together with a self-locking mortise lock)
- Door unlocked (only together with a self-locking mortise lock)
- Tampering attempt
  - Fastening screw
  - Intrusion attempt
  - Sensor malfunction
  - Manipulation of the handle

For details, please refer to the documentation of the integrator system.

NOTE

Programming error during interrupted or changed master-slave pairing

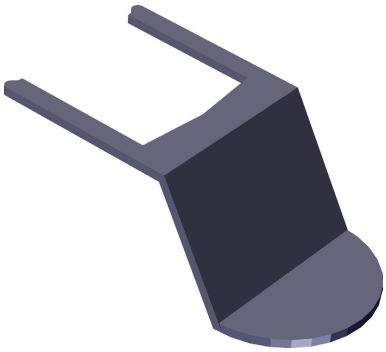
The master and slave are factory configured as belonging together. Replacing knobs will result in programming errors.

Master and slave communicate during programming.

- Make sure that the master and slave are physically connected during programming.

6.8.2 Tool

The supplied SmartHandle tool is required to remove the cover. For further tools required, please refer to the supplied quick guide.



6.8.3 Technical specifications

Dimensions, narrow (WxHxD)	41 x 224 x 14 mm
Dimensions, wide (WxHxD)	53 x 224 x 14 mm
Battery life (online network WO):	80,000 locking cycles, 5 years on standby
Battery life (offline networking or "virtual networking" SVCN):	50,000 locking cycles, 6 years on standby
Battery type:	CR2450 3V lithium, Murata (Panasonic, Varta)
Battery manufacturer	- Murata - Varta - Panasonic
Number of locking devices per GatewayNode:	16
Temperature range (operation)	-20 °C to +50 °C

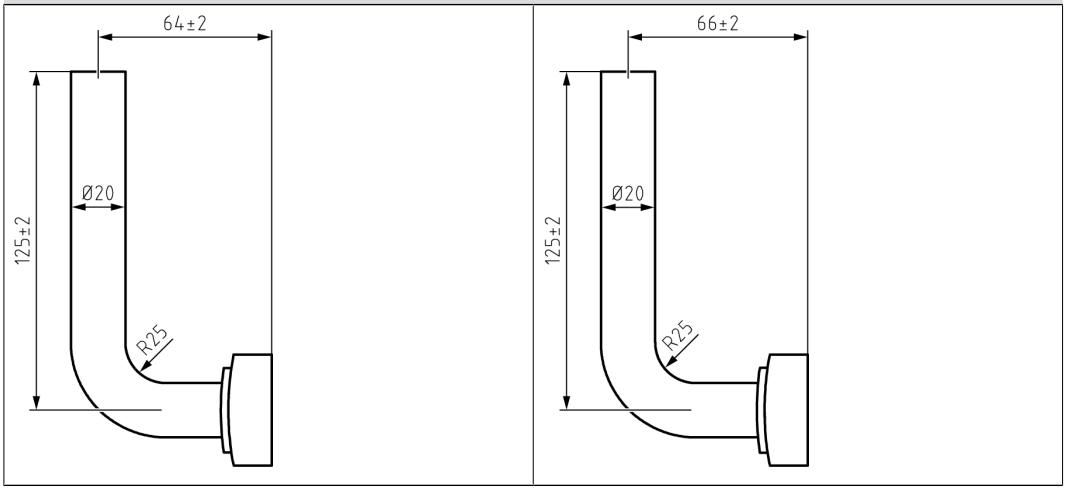
White list function:	250 offline cards
Entries in the access list	Max. 1,000 (WO: 250)
Protection rating	IP 40 (WP version: IP 45 for outside)
Online network: Card technology	■ MIFARE Classic ■ MIFARE DESFire EV1 ■ UID according to 14443 from MIFARE, LEGIC advant and HID iCLASS
Virtual (VN Offline): Card technology	■ MIFARE Classic ■ MIFARE DESFire EV1
Feedback signals:	Buzzer + LED (blue/red)
Directly networkable (only with SmartIntego Wireless Online)	Integrated LockNode

Radio emissions		
SRD (WaveNet)	868.000 MHz - 868.600 MHz	<25 mW ERP

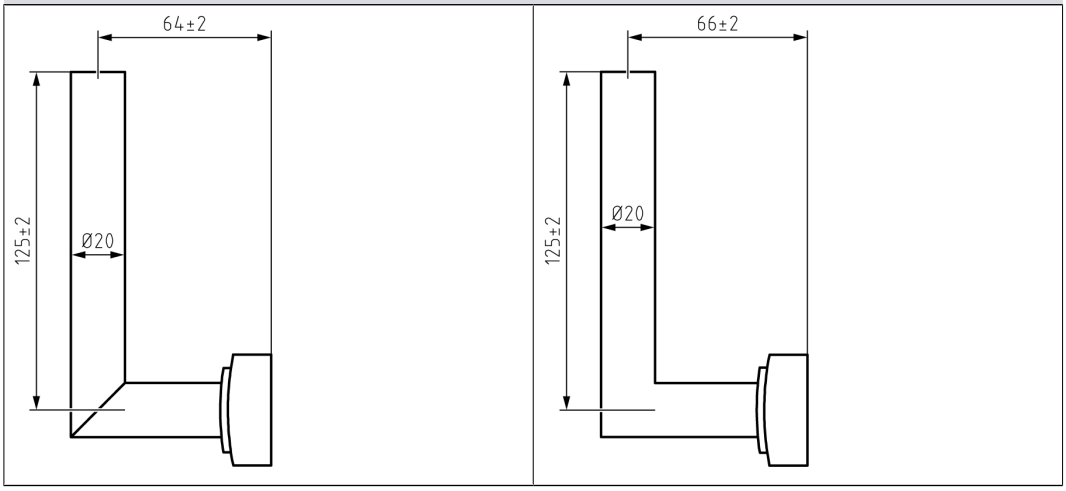
There are no geographical restrictions within the EU.

6.8.3.1 Dimensional drawings handles

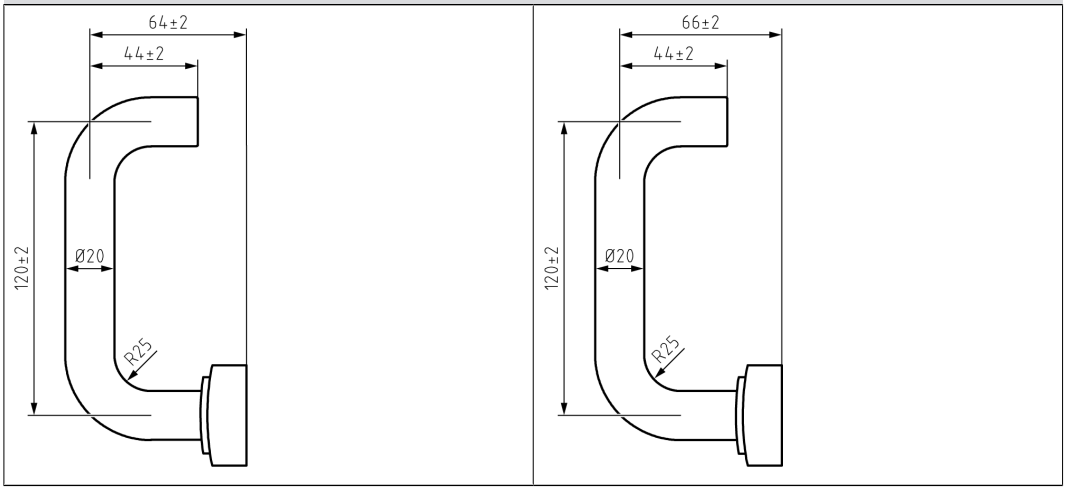
Shape A (Outside/Inside)



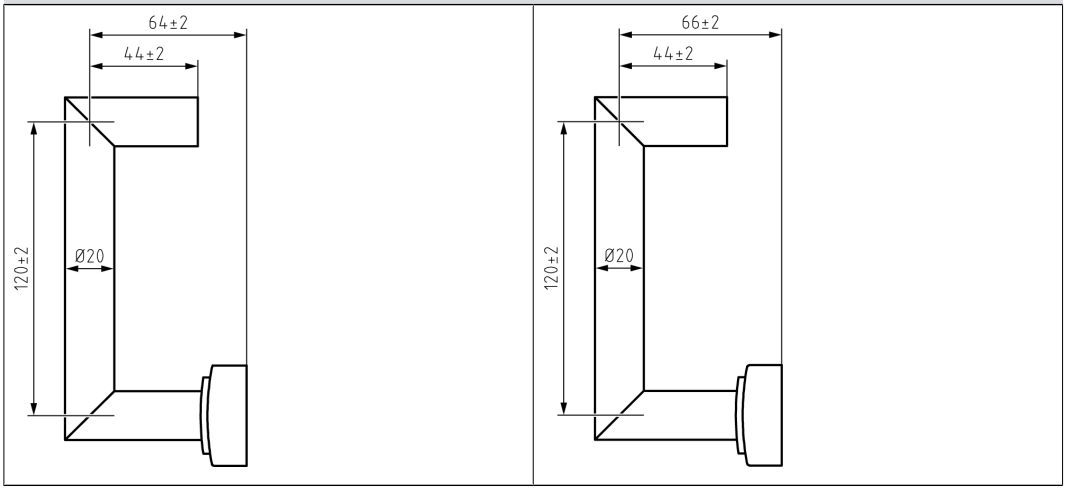
Shape B (Outside/Inside)



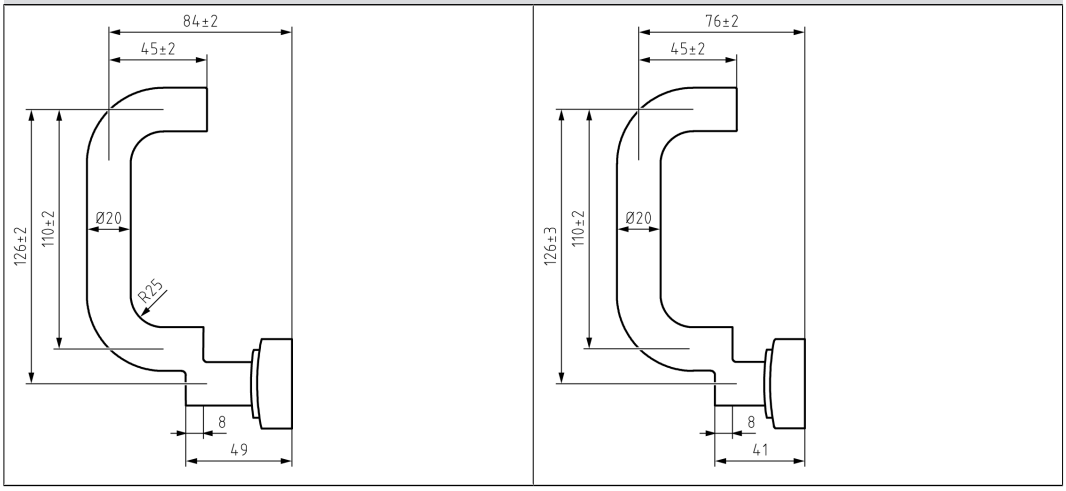
Shape C (Outside/Inside)



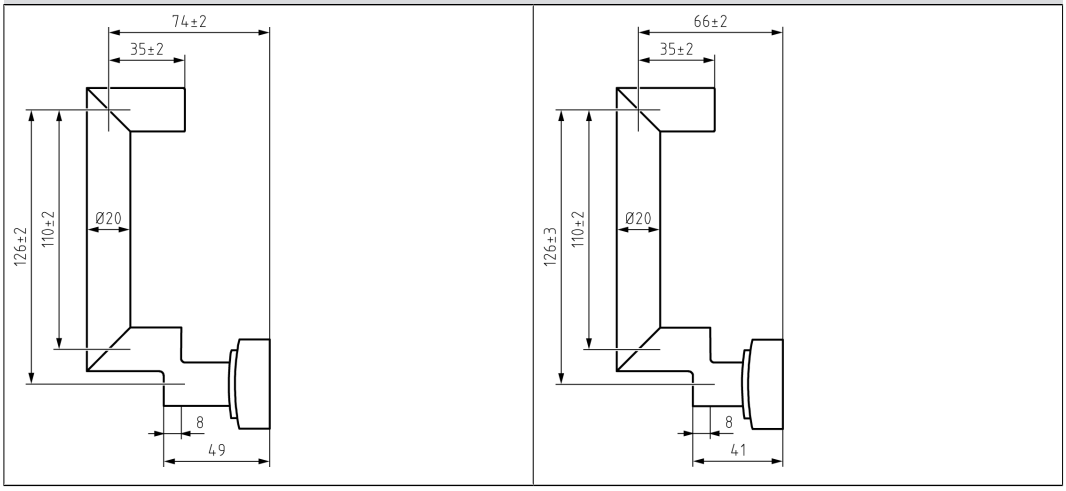
Shape D (Outside/Inside)



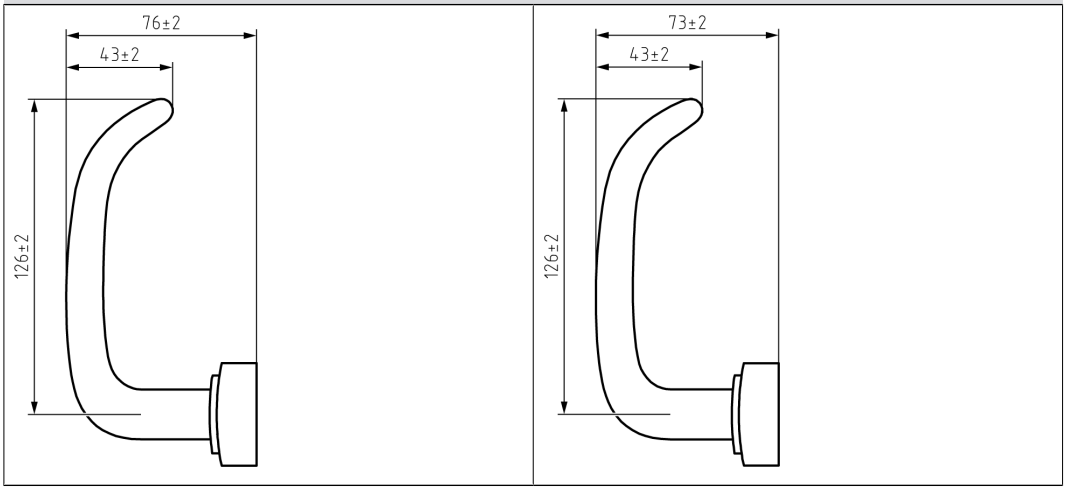
Shape E (Outside/Inside)

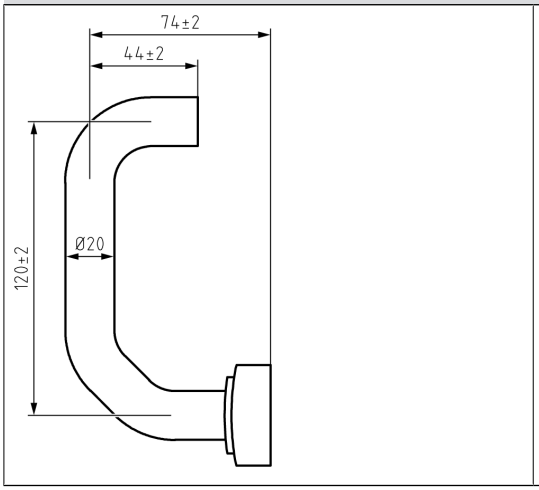
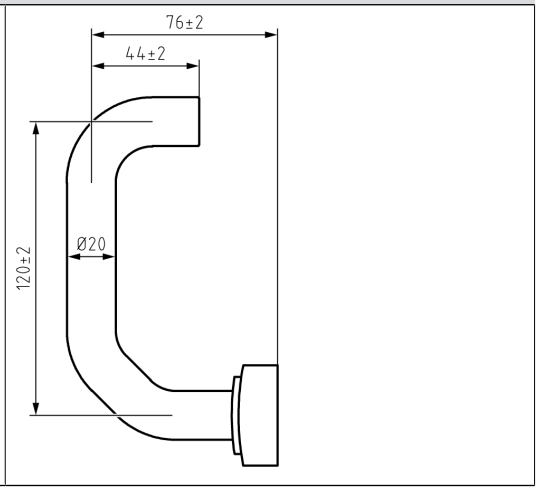


Shape F (Outside/Inside)



Shape G (Outside/Inside)



Shape H (Outside/Inside)	
	

6.9 Padlock

The SimonsVoss padlock functions like a normal mechanical padlock. However, it is unlocked and locked by an electronic thumb-turn and expands the functions of a mechanical padlock with the advantages of electronic locking devices.

6.9.1 Technical specifications

Padlock with shackle 8 mm in diameter	
Locking device dimensions (W x H x D)	51 x 70 x 25 mm *(without cylinder knob or shackle)*
Inside height of shackle	25 mm or 60 mm (manual locking or self-locking respectively)
Locking device protection class	Class 3 as per EN 12320

Padlock with shackle 11 mm in diameter	
Locking device dimensions (W x H x D)	60 x 72.5 x 25 mm *(without cylinder knob or shackle)*
Inside height of shackle	Manual locking: 35 mm Self-locking: 50 mm
Locking device protection class	Class 4 as per EN 12320

Technical specifications for the locking device	
Battery type	2x CR2450 3V lithium *(Murata, VARTA, Panasonic)*

Battery life SmartIntego	Wireless Online (WO): Up to 5 years standby or 80,000 activations SmartIntego Virtual Card Network (SVCN): Up to 6 years standby or 50,000 activations

Protection rating	IP66
Temperature range	Operational: -25°C to +65°C Storage: -35°C to +50°C
Loggable access events (.ZK in System 3060 resp. MobileKey)	Up to 3,000 System 3060 resp. MobileKey: Up to 3.000 SmartIntego: Up to 1.000 (WO: 250)
Time zone groups (.ZK)	100+1 (G2)

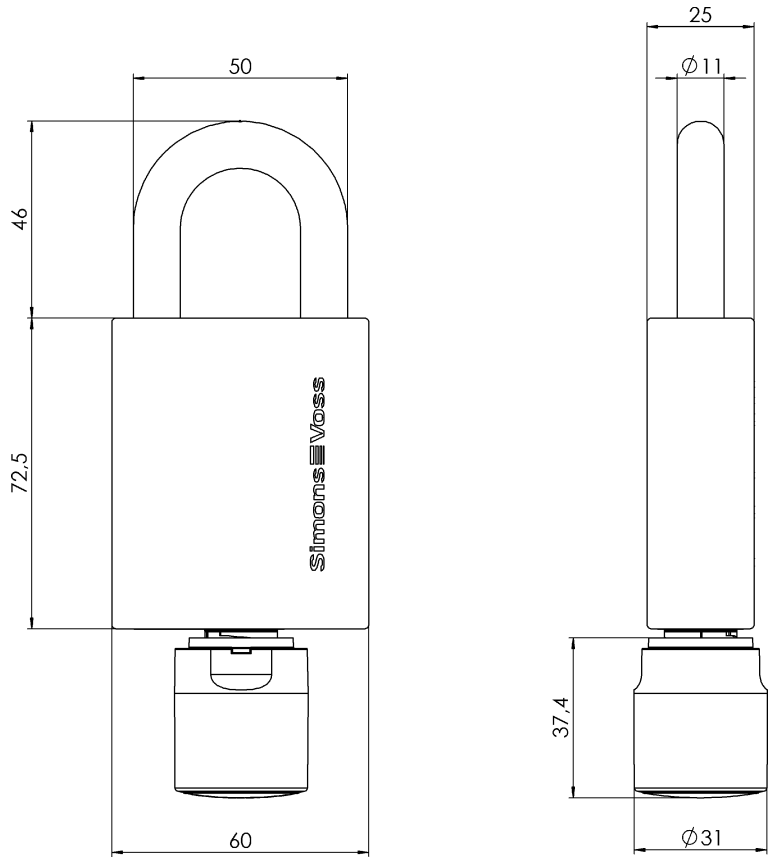
Number of media which can be managed per padlock	Transponders: up to 64,000 (G2) Smart cards (G2): up to 32,000 (depending on the configuration / template selected)
Networking capability	Directly network-ready with integrated LockNode; LockNode can be retrofit
Other information	Version with access control, time zone control and event logging
Permanent/open modes	Time-controlled flip-flop mode (time change-over) possible: time-controlled automatic or time-controlled manual engage and disengage (using transponder). A transponder can be optionally used to interrupt the engage procedure

Radio emissions		
SRD (WaveNet)	868.000 MHz - 868.600 MHz	<25 mW ERP

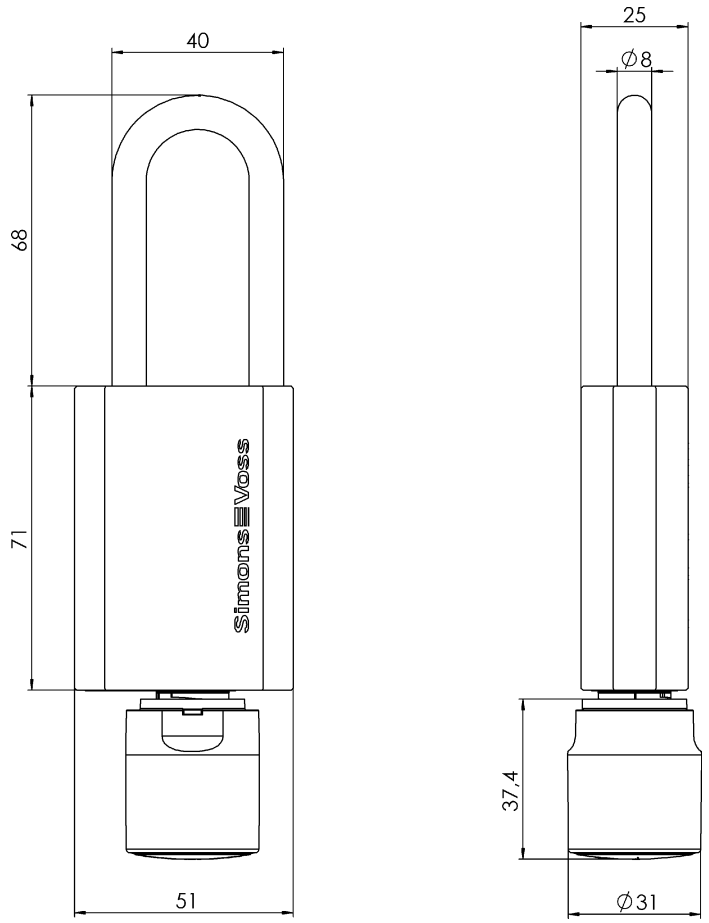
There are no geographical restrictions within the EU.

6.9.1.1 Dimensional drawings padlocks

Padlock 11 mm - Passive (PL MP)



Padlock 8 mm - Passive (PL MP)



6.10 General signalling and processes for SmartIntego locking devices

The signals are generally divided into the following schematic:

- Process
- Action/reaction of the locking device
- LED (number, colour, duration)
- Tones (number, duration)

Short-term couplings

Process	Action/Response	LED	Tones
Short-term engaging (card)	Read card	1× blue (short)	1× beeps (short)
	Engage	2× blue (short)	2× beeps (short)
	During engagement time (3 to 25 seconds)		
	Disengage		1× beeps (short)

Process	Action/Response	LED	Tones
Short-term engagement (remote command)	Engage	2× blue (short)	2× beeps (short)
	During engagement time (3 to 25 seconds)		
	Disengage		1× beeps (short)

Long-term cupolas

Process	Action/Response	LED	Tones
Long-term engagement / FlipFlop (card)	Read card	1× blue (short)	1× beeps (short)
	Engage	2× blue (short-long)	2× beeps (short-long)
	During engagement time (1 minute to continuous)	No response	
Long-term disengagement/FlipFlop (card)	Read card	1× blue (short)	1× beeps (short)
	Disengage	2x blue (long-short)	2x beeps (long-short)
Long-term engagement/FlipFlop (Remote Command)	Engage	2× blue (short-long)	2× beeps (short-long)
	During engagement time (1 minute to continuous)	No response	
Long-term disengagement/FlipFlop (remote command)	Disengage	2x blue (long-short)	2x beeps (long-short)
Long Term Engage/ FlipFlop (time controlled)	Engage	2× blue (short-long)	2× beeps (short-long)
	During engagement time (1 minute to continuous)	No response	
Long-term disengagement/FlipFlop (time-controlled)	Disengage	2x blue (long-short)	2x beeps (long-short)

Office mode

Process	Action/Response	LED	Tones
Activate office mode (keep card briefly available)	Read card	1× blue (short)	1× beeps (short)
	Engage	2× blue (short)	2× beeps (short)
	During engagement time (3 to 25 seconds)	No response	
	Disengage	2× blue (short)	2× beeps (short)
Activate office mode (hold card for a long time)	Read card	1× blue (short)	1× beeps (short)
	Engage	2× blue (short)	2× beeps (short)
	Wait until second reading	No response	
	Read card	1× blue (short)	1× beeps (short)
	During long-term engagement (1 minute to continuous)	No response	
Deactivate office mode (hold card for a long time)	Read card	1× blue (short)	1× beeps (short)
	Wait until second reading	No response	
	Reading and uncoupling the card	2x blue (long-short)	2x beeps (long-short)
Deactivate office mode (remote command)	Disengage	2x blue (long-short)	2x blue (long-short)
Deactivate office mode (time-controlled)	Disengage	2x blue (long-short)	2x blue (long-short)

Escape&Return

Process	Action/Response	LED	Tones
Escape&Return	Actuate and engage inside handle	2× blue (short-long)	2× beeps (short-long)
	During engagement time (continuous signal)	1x red (short)	1× beeps (short)
	Disengage	2x blue (long-short)	2x beeps (long-short)

Batteries

Process	Action/Response	LED	Tones
Battery warning		No response	
Battery replace-ment	Read card	1× blue (short)	1× beeps (short)
	During battery measurement	1× blue (2 seconds)	
	Completion of bat-tery measurement		1× beeps (short)

WaveNet test card

Process	Action/Response	LED	Tones
WaveNet test card successful	Read card	1× blue (short)	1× beeps (short)
	Communication successful	4× blue (short)	4× beeps (short)
WaveNet test card not successful	Read card	1× blue (short)	1× beeps (short)
	During the timeout wait time: Default value 5 seconds	No response	
	Communication not successful	1× red (long)	1× beeps (long)

Other information

Process	Action/Response	LED	Tones
Activate non-programmed locking device with card	Reading and engaging the card	2× blue (short)	2× beeps (short)
	During engage time (5 seconds)	No response	
	Disengage		1× beeps (short)
Timeout	Read card	1× blue (short)	1× beeps (short)
	During the timeout wait time: Default value 5 seconds	No response	
	Timeout signal	1× red (long)	1× beeps (long)
Deny access	Read card	1× blue (short)	1× beeps (short)
	Access denied signal	1x red (short)	1× beeps (short)
Card reader error		1x red (short)	1× beeps (short)
Card with different card configuration than in the locking device		No response	
Initialize LockNode		4× Red (short)	4× beeps (short)

6.11 IO-Node

SmartIntego IO Node is a battery-operated radio module with three inputs and an open drain output. The IO-Node can be used to monitor and control components by connecting to the integrator system. You will need the components shown:

- SI.N.IO
- WN.LN.SENSOR.CABLE

Examples of use:

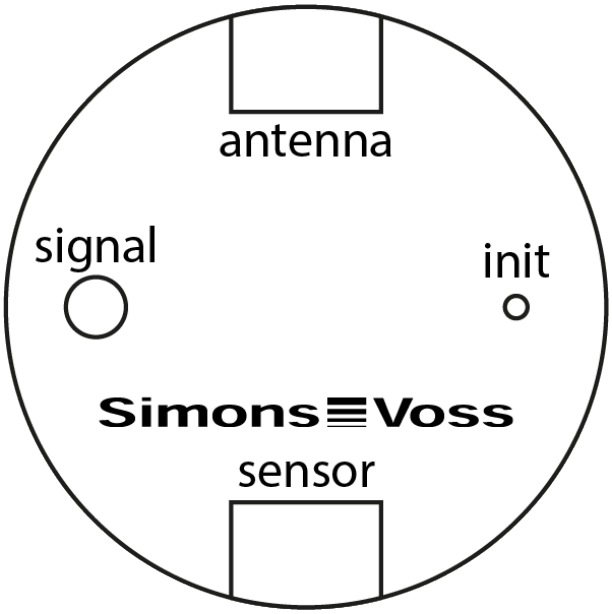
- Monitoring of doors with reed contacts from third-party manufacturers (use of inputs)
- Switching on surveillance cameras (using the output)

6.11.1 Installation

1. Unpack the LockNode.
2. Check if the LockNode is damaged.
3. If necessary, connect the WN.LN.SENSOR.CABLE.
4. If necessary, connect the WN.LN.SENSOR.CABLE to the components to be connected.
5. Connect the power supply or insert the batteries.

↳ LockNode is installed.

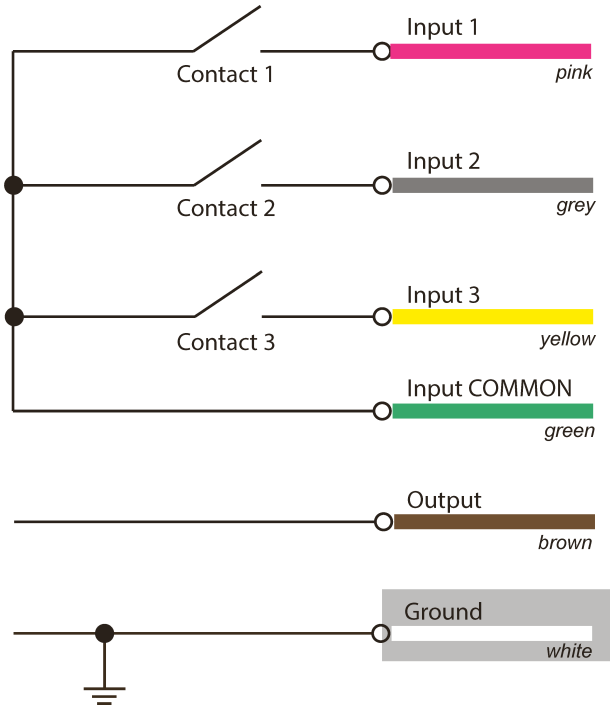
6.11.2 Connections



antenna	Direct connection for SREL.ADV (WN.KAB.WIRED-BF). Only for system 3060.

sensor	I/O panel (WN.LN.SENSOR.CABLE) ■ green (In-Common) ■ pink (input 1, connection with green = 1, otherwise 0) ■ grey (input 2, connection with green = 1, otherwise 0) ■ yellow (input 3, connection with green = 1, otherwise 0) ■ brown (open collector output) ■ white (ground)

The following figure shows the assignment of the sensor cable.



The signal LED indicates the operating status, the Init button can reset WNM-LockNodes (see Hardware reset of external LockNodes) or test the signal quality of WN-LockNodes.

SmartIntego

Your integrator provides the exact connection diagram of the inputs. Changes to the inputs are forwarded from the inputs to the integrator system (node IO events).

For details, please refer to the documentation of the integrator system.

6.11.3 Technical specifications

Dimensions	37xØ53 mm, suitable for standard flush-mounted box (DIN 49073 part 1)
Power supply	2 batteries, type 2/3 AA Lithium 3.6V (Tadiran SL-761)
Current consumption	■ Send: 32 mA ■ Receive: 18 mA ■ Standby: approx. 20 µA (depending on traffic and usage of the frequency band)
Battery life	approx. 6 years
Sensitivity	-95 dBm
Interfaces	■ Connection for SREL.ADV (only for system 3060) ■ Connections for digital inputs and outputs ■■ 3x Input, 1x Common-In ■■ 1x open collector output (max. 25 V_{DC}, 650 mA and up to 2 A peak, contact resistance 0.5 Ω)

Maximum transmission power	about 1 mW

6.12 PIN code keypad

6.12.1 Intended use

Use the SmartIntego PIN code keypad MobileKey to operate locking devices by entering an authorised User PIN (see section on *Operation [▸ 96]*). You need to change the Master PIN and assign a User PIN to do so.

You can programme the SmartIntego PIN code keypad using the MobileKey web app (SmartIntego: SmartIntego manager and integrator system). The SmartIntego PIN code keypad is added as a "key" with PINs and assigned to a lock.

The SmartIntego PIN code keypad contains a LockNode with a "Chip ID" and is assigned to the SmartBridge located within range when the network is configured. If a correct user PIN length has been entered, the PIN is transmitted to the server (SmartIntego: To integrator system) via WaveNet, where it is evaluated.

6.12.2 Operation

NOTE

Both the SmartIntego PIN code keypad and the lock must have a stable network connection, so that the SmartIntego PIN code keypad can send signals to the networked lock via the network.

Cancellation of actions

All actions can be cancelled by not making any further inputs. The SmartIntego PIN code keypad will cancel the action after a waiting period.

- ✓ SmartIntego PIN code keypad has been successfully configured. (Master PIN)
- ✓ The User PIN length has been programmed correctly.
- ✓ There is a stable network connection.

- ▪ Enter a User PIN. You have a maximum of 3 seconds to enter each individual number.
- ↳ SmartIntego PIN code keypad beeps and flashes green once after a User PIN with a valid length has been entered.

The SmartIntego PIN code keypad transmits the entered User PIN to the server (SmartIntego: Integrator system) for verification and triggers the following process:

1. The SmartIntego PIN code keypad sends a feedback signal accepting the User PIN length if the right User PIN length has been entered. See *Signals [▸ 96]* for more details.
2. The SmartIntego PIN code keypad transmits the User PIN entered to the SmartBridge (SmartIntego: Integrator system) via the network.
3. The SmartIntego PIN code keypad emits a positive feedback signal if the SmartBridge receives the PIN successfully (SmartIntego may differ). See *Signals [▸ 96]* for more details.
4. The networked lock is activated via the SmartBridge if it matches the User PINs specified in the web app (SmartIntego may differ).

6.12.3 Signals

Information on signaling the SmartIntego variant can also be found in the SmartIntego TechGuide.

LED colour	LED flashing	Buzzer	Event	Explanation
Red	8x	4 x	Power-on reset	Reset after battery replacement – batteries not OK
	1x	1x	Error	Error occurred
			User PIN length incorrect	Length of the User PIN entered not correct
			User PIN not received	Entered User PIN not received by SmartBridge
Orange	3x	3x	Abort	Current action has been cancelled
	4 x	4 x	Power-on reset	Reset after battery replacement in operating mode – batteries OK
Green	2x	2x	Master PIN changed	Master PIN successfully changed
			PIN length changed	Length of the User PIN successfully changed
			User PIN received	Entered User PIN received by SmartBridge
	1x	1x	User PIN length correct	Length of the User PIN entered correct

Tab. 1: General signals

LED colour	LED flashing	Buzzer	Event	Explanation
Red	4 x	4 x	Battery Warning 2	Battery very low
Orange	4 x	4 x	Battery Warning 1	Low battery
Green	3x	3x	Full capacity	Batteries fully charged
	1x	1x	Battery "OK"	Batteries OK

Tab. 2: Battery test

6.12.4 Technical specifications

SmartIntego PIN code keypad	
Batteries:	4 x 3 V lithium, type CR 2032 (Murata, Panasonic, Varta) *Always replace all four batteries with new, approved, brand-name batteries when changing them.*
Battery life:	up to 500,000 lock operations or up to 12 years on standby
Dimensions in mm:	96 x 96 x 14
Protection class:	IP65
Operating temperature:	-20 °C to +50 °C
Signal elements:	Different colour LEDs (red, green, orange) + audible signals
Marking:	PHI number (physical hardware identifier) = chipID
Housing:	Silver ABS polymer housing with semi-transparent rear/base plate
Main colour:	Similar to RAL 9007, using formula no. 19900841
Key labelling:	RAL 7016 Anthracite Grey

6.13 Batteries

All SmartIntego components are battery-powered:

- Locking cylinder
- Digital padlocks
- SmartHandles (AX and 3062)
- IO-Node
- PIN code keypad

A three-stage battery management system prevents unexpectedly fully discharged batteries:

1. Battery is OK
2. Battery is low (warning)

   Depending on use, up to thirty days remain. The locking device then switches to the last warning level.
3. Battery is very low (alarm)

Depending on use, up to twenty days remain.

6.13.1 Battery level measurement (locking cylinders and SmartHandles)

Your SmartIntego locking devices automatically measure the battery status daily between midnight and four o'clock in the morning (set time). The measurement takes a few seconds. The locking device cannot be opened during the measurement. The measurement is stored until the next measurement.

The determined battery warning level is transmitted to the integrator system as a card event or once a day (depending on the integrator system). The integrator system must display the battery status. The locking devices themselves do not indicate the battery status.

6.13.2 Battery replacement (locking devices and SmartHandles)

If the integrator system displays a battery warning, the batteries must be replaced:

✓ Battery replacement card created (see step-by-step instructions).

1. Replace all batteries in the affected locking device as described in the short instructions supplied.
   ↳ Locking device signals successful battery replacement (flashes several times).
2. Hold a battery replacement card in front of the locking device for the components (not required for AX).
   ↳ The locking device immediately measures the battery status.
   ↳ Battery status is transmitted to the integrator system the next time a card is activated.
   ↳ The integrator system no longer displays a battery warning for this locking device.
3. Test LockNode.

Detailed information can be found in the documentation for the respective component.

Recommended manufacturers

SimonsVoss only uses batteries from brand manufacturers:

- Murata
- Varta
- Panasonic
- Tadirane

Battery types

Locking devices	CR2450
PIN code keypad	CR2032
IO-Node	2/3AA (Tadiran)

6.13.3 Battery level measurement (NodeIO and PIN code terminal)

The battery status is continuously monitored.

The determined battery warning level is transmitted to the integrator system as an event or once a day (depending on the integrator system). The components themselves do not indicate the battery status.

7 Infrastructure

7.1 LockNodes

A LockNode is a network node that connects a locking device (lock) or a node (IONode or PIN code keypad) to the integrator system via a GatewayNode.

7.1.1 LockNode in locking devices (LNI)

LNI means LockNode Integrated. These are small printed circuit boards that are installed ex works on SmartIntego components.

A small metal pin on the circuit boards establishes contact with the thumb-turn covers (cylinders) or the cover (SmartHandles). The thumb-turn covers or cover thus serve as an extended antenna.

Without the thumb-turn covers or the cover as an extended antenna, the signal strength of the WaveNet connection is significantly worse and may no longer be sufficient.

Locking devices and LockNodes are configured independently of each other. However, the configurations build on each other.

Programme

1. Configure the ADS server.
2. Programme the locking device.

↳ LockNode and locking device are linked to each other after programming.

Reset

1. Reset the locking device.
2. If this the case, reset the LockNode.

↳ LockNode and locking device are separated again after resetting the locking device.

7.1.2 LockNode in Node (LN)

The PIN code keypad and the IO node are not components with an additional LockNode. The LockNode is permanently mounted on the circuit board of the respective component here.

7.2 GatewayNode (GN)

A GatewayNode connects several locking devices/LockNodes to the integrator system via WaveNet. From the perspective of LockNodes, this is an access point.

There are two options for connecting to the integrator system:

- Ethernet
- RS-485

7.2.1 TCP

On delivery, the GatewayNodes expect a DHCP server in the network to assign them an IP address. If there is no DHCP server on the network, GatewayNodes assign default credentials.

Interfaces

- Radio (WaveNet)
- Ethernet (TCP/IP)

Power supply

SI.GN.ER	SI.GN2.ER, SI.GN2.ER.M
WN.POWER.SUPPLY.PPP 	POWER.SUPPLY.2 
Power over Ethernet (PoE, IEEE802.af, galvanically isolated)	

Variants:

	- SI.GN2.ER - SI.GN2.ER.M (Mercury variant)

	SI.GN.ER (Ethernet)

Technical specifications:

SI.GN2.ER

General	
Dimensions	172 mm × 86 mm × 33 mm
Weight	About 100 g
Material	ABS plastic, UV-stable
Colour	White (like RAL 9016 "Traffic white")
Installation	■ horizontal ■ vertical ■ Wall mounting possible ■ Integrated strain relief (3x)
Connections	■ RJ45 (Network/PoE) ■ Round plug Ø 5.5 mm, Ø pin 2.0 mm (power supply) ■ Screw terminal block 2-pole, wire diameter 0.14 mm^2 to 1.5 mm^2 (power supply for external applications) ■ MCX socket (optional external antenna) Power supply via PoE and round plug possible simultaneously: round plug > 12 V_{DC} → Round plug used, round plug < 12 V_{DC} → PoE used
Environment	
Temperature	■ Operational: -10 °C to +55 °C ■ Storage: -20 °C to +60 °C
Humidity	Max. 90%, non-condensing

Standard protection rating	IP20
Electric	
Operating voltage	9 V_{DC} to 32 V_{DC} (reverse polarity protected) or PoE according to IEEE 802.3af Power supply via PoE and round plug possible simultaneously: round plug > 12 V_{DC} → Round plug used, round plug < 12 V_{DC} → PoE used
Output	max. 3 W
Output VOUT	3.0 V_{DC} to 3.3 V_{DC}, max. 200 mA
Relay output O1	▪ Max. switching voltage 30 V_{DC}/24V_{AC} (resistive load) ▪ Max. switching current 1 A (resistive load)
Interfaces	

RJ45	▪ Network interface
	▪ 10T/100T
	▪ HP Auto_MDX
	▪ DHCP-Client (DHCP: on)
	▪ IPv4
	▪ Service
	  ▪ TCP: 1x at Port 2101
	  ▪ UDP: 1x for Digi-Scan (OAM tool)
	▪ Web server: Enable

868 MHz radio	WaveNet interface, range up to 30 m
Analogue input	1x with 12-bit resolution from 0 to 3.3 V_{DC}
Relay contacts	1x change-over contact, potential-free.
Signalling	
LED	RGB LED (centre of housing)
Software	
Programming	via TCP/IP interface

Transfer media	Interfaces	Power supply	Dimensions
■ 868 MHz ■ Ethernet	■ RJ45 (Network/PoE) ■ Round plug Ø 5.5 mm, Ø pin 2.0 mm (power supply) ■ MCX socket (optional external antenna)	9 V_{DC} to 32 V_{DC} or PoE according to IEEE 802.3af Power supply via PoE and circular plug possible at the same time: Round plug > 12 VDC → Round plug used, round plug < 12 VDC → PoE used	172.1×85.9×32.8 mm

SI.GN.ER

Transfer media	Interfaces	Power supply	Dimensions
■ 868 MHz ■ Ethernet	■ Connecting terminals for an external plug-in power supply ■ RJ45 (Network/PoE) ■ FME socket (antenna)	9 V_{DC} to 24 V_{DC}, min. 3 VA	98×64×40 mm or 98×64×130 mm with antenna

7.2.1.1 Configuration and operation

In general, the use of an independent IP address range for the GatewayNodes is advisable. One way to do this is to have a virtual local area network (V-LAN) that works separately from the normal network.

A prerequisite for trouble-free operation is a permanent connection of the GatewayNodes to the integrator system. SmartIntego components can also be connected to the SmartIntego tool (WO) during setup.

TCP ports used

Port (TCP)	Direction	Description
80	Setup PC to GatewayNodes	Accessing the configuration website of the GatewayNodes

Port (TCP)	Direction	Description
2101	■ Setup PC to GatewayNodes ■ Integrator system to GatewayNodes	■ Communication between SmartIntego tool (WO) on setup PC to GatewayNodes ■ Communication between integrator system and GatewayNodes during operation
2153	Integrator system to GatewayNodes	Communication between integrator system and GatewayNodes in operation (if TLS encryption is used)

7.2.1.2 Configuration TCP GatewayNodes

The TCP GatewayNodes can be adapted to the respective IT infrastructure (see integrator documentation). For this purpose, the connected GatewayNodes in the network provide a website that can be opened via the IP or DNS name with a browser. The following setting options are available:

| SYSTEM INFORMATION |	[OVERVIEW]	Displays the IT settings.
	[WAVENET]	Displays the WaveNet settings.
	[CONNECTION]	Shows the active connection to the integrator system.
| CONFIGURATION |	[NETWORK]	Changes general network settings.
	[PORT]	Sets the port for TCP connection.
	[ETHERNET INTERFACE]	Sets the speed and IEEE802.1X.
	[WAVENET]	Resets WaveNet settings.

| ADMINISTRATION |	[PASSWORD]	Changes the login password.
	[AES]	Changes the AES settings (encryption password between GatewayNode and integrator system), binding the GatewayNode to the respective integrator system. Only visible when accessed via HTTPS.
	[CERTIFICATE]	Sets TLS encryption between GatewayNode and integrator system.
	[FACTORY]	Resets the GatewayNode to the factory settings.
	[REBOOT]	Restarts the GatewayNode (Depending on browser settings, this function may also be deactivated).

Open website

You receive the device with the following factory configuration:

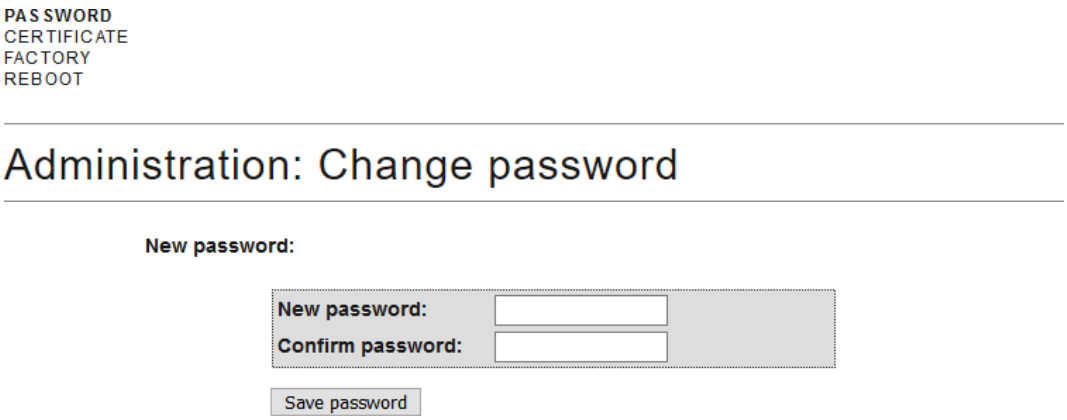
IP address	192.168.100.100 (if no DHCP server is found)
Subnet mask	255.255.0.0
User name	SimonsVoss
Password	SimonsVoss

In the address bar, type https://IP address (computer and GatewayNode must be on the same network). Then change the password.

Some browsers do not register any spaces included at the start of a password, so do not begin your password with spaces.

✓ Browser interface opened.

1. Open the [PASSWORD] tab using | ADMINISTRATION |.



2. Enter your new password.
3. Repeat your new password.
4. Click on the Save password button.

↳ Password is now changed.

IMPORTANT

Access via default password

Other people can access the product using the factory-set access data.

Some browsers do not transmit spaces at the beginning of the password.

1. Change the default password.
2. Do not start the password with spaces.

NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.

7.2.1.3 Encryption

Support GatewayNodes from firmware 40.X or later:

- AES encryption for data packets
- TLS encryption for the connection

Encryption

AES encryption stores a secret key in the settings of each GatewayNode.

The same key is stored in the integrator system.

This key links the GatewayNodes to the integrator system and encrypts the data packets with 128-bit ES.

Please refer to the integrator system documentation for details of the settings.

Encryption

Optional TLS encryption encrypts the active connection between a GatewayNode and the integrator system. For this purpose, it may be necessary to store your own certificates on the GatewayNodes via the GatewayNodes configuration website.

Please refer to the integrator system documentation for details of the settings.

7.2.2 RS-485

Interfaces

- Radio (WaveNet)
- RS-485
- Ethernet (TCP/IP) - only for the configuration device (SI.GN.CONFIG.EC)

Power supply

SI.GN.CR or SI.GN.CONFIG.EC can be supplied either via a WN.POWER.SUPPLY.PPP or via the terminals.

Variants:

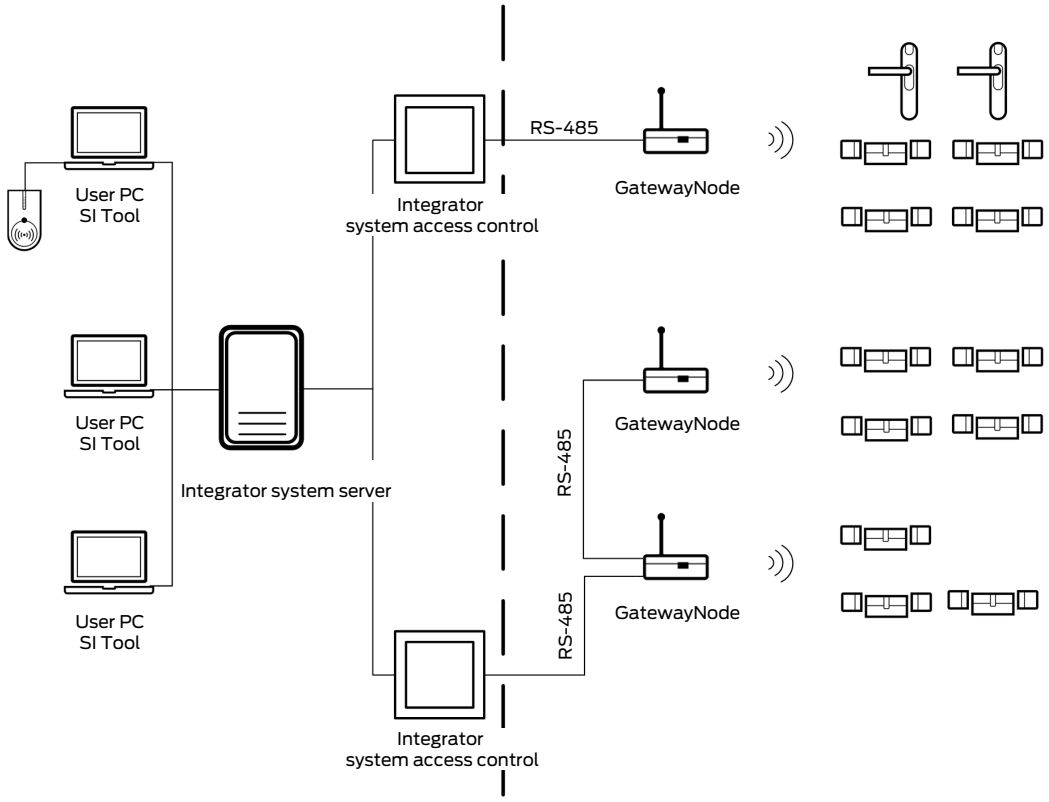
	SI.GN.CR (RS-485)
	SI.GN.CONFIG.EC

SI.GN.CR

Transfer media	Interfaces	Power supply	Dimensions
■ 868 MHz ■ RS-485	■ Connecting terminals for an external plug-in power supply ■ Terminals for RS-485 ■ FME socket (antenna)	9 V_{DC} to 24 V_{DC}, min. 3 VA	98×64×40 mm or 98×64×130 mm with antenna

7.2.2.1 Configuration and operation

During daily operation of the RS-485 network, all RS-485 Gateway Nodes (SI.GN.CR) are directly connected to the RS-485 interface of the integrator system.



The ConfigNode is only required for configuring the RS-485 Gateway Nodes and the associated locking devices. It represents the interface to the SmartIntego tool (WO).

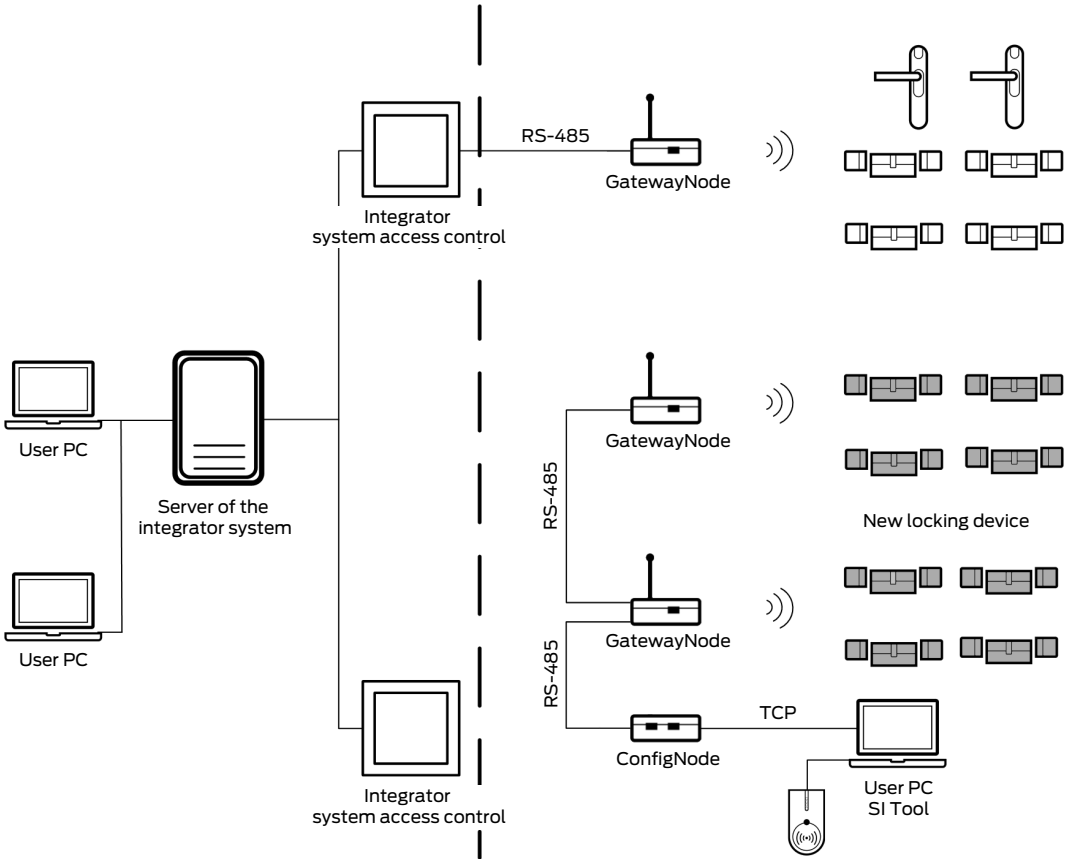
During configuration, the RS-485 connection between the integrator system and the GatewayNodes is disconnected. The GatewayNodes are instead connected to the ConfigNode (RS-485) and this is connected via Ethernet to the setup PC including the SmartIntego tool (WO).

NOTE

Locking devices offline during configuration

The locking devices are disconnected from the integrator system during configuration. The locking devices are therefore offline and only work with a previously stored whitelist.

- Make sure that a whitelist is stored in the locking devices before you disconnect the connection to the integrator system.



In this example, the grey locking devices are no longer connected to the integrator system and are offline.

A maximum of 255 addresses can be managed with a ConfigNode. Each LockNode uses one address of this quota, but each GatewayNode uses two. If there are more LockNodes or GatewayNodes in the system, a second ConfigNode must be used after the first one. Parallel operation of several ConfigNodes is not possible.

Several smaller projects can also be operated directly with a ConfigNode. Please note that the settings in ConfigNode must match the project:

- New projects must always be created with a new or reset ConfigNode. When the project is created, the appropriate settings are written to ConfigNode.

- If the ConfigNode is to be used in another project, it must be reset beforehand. SmartIntego Manager replaces the ConfigNode in the project with the option Replace with with a new or reset ConfigNode. The SmartIntego Manager writes the appropriate settings for the project in ConfigNode.
- This means that the same ConfigNode can be used for several projects, but must be reset as described for each project change before it can be used again.

7.2.2.2 ADDRESSING

Each ConfigNode can manage 255 addresses, each GatewayNode needs two. A ConfigNode can therefore configure a maximum of 127 GatewayNodes.

The addresses of the GatewayNodes are linked to the ConfigNode:

- SmartIntego Manager
- In ConfigNode itself

7.2.2.3 Physical connection

The GatewayNodes are connected to each other with a cable.

Smaller groups of GatewayNodes can be connected to a common line (daisy chain). However, several cables can also be used in a project (star-shaped). Both cabling techniques can also be combined (multiple daisy chains merged at one point). The structure and distribution is normally specified by the hardware controller of the integrator.

A ConfigNode is able to address several physical connections (cable lines).

7.2.2.4 Naming convention

GatewayNodes can be given their own names. The physical connections should be identifiable in the names.

Depending on the structure (if there are several ConfigNodes in the project), it is also helpful to include the logical connections to the ConfigNodes in the names.

Detailed system documentation is particularly important in this context in RS-485 projects.

7.2.3 Signalling

The GatewayNodes signal their current status with an LED in the housing:

LED	Status
Flashing slowly (1 s green, then 1 s pause)	No WaveNet configuration
Flashing fast (0.5 s green, then 05 s pause)	WaveNet configuration present
Very fast flashing (continuous for a maximum of 12 s)	Active data transfer

7.2.4 Mercury Security Variant

The Mercury variant (SI.GN2.ER.M) is technically identical to the normal GatewayNode (SI.GN2.ER). It differs in the assignment of device addresses (device addresses are linked to WaveNet addresses).

Mercury GatewayNodes are therefore only compatible with integrator systems based on a Mercury security controller, for example (list incomplete):

- Genetec
- Lenel
- Avigilon
- Keri Systems

Therefore, please note:

- Do not mix Mercury verifiers with non-Mercury variants.
- Use Mercury GatewayNodes only in integrator systems with Mercury Security Controller.
- The locking devices are not linked to their own device address. The WaveNet address is handled instead.

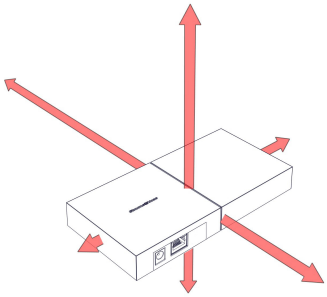
The difference between the device address and the WaveNet address affects handling in different situations in the system (see *Topology [▸ 118]*). If, for example, locking devices are relocated, the device address changes for Mercury variants.

Locking devices are not directly connected to the integrator system. Regular SmartIntego locking devices can therefore be used in Mercury systems and there is no Mercury version of SmartIntego locking devices.

7.2.5 External antenna

Sometimes a GatewayNode does not reach individual locking devices optimally. In these cases, an optional external antenna (order number: ANTENNA.EXT.868).

The dispersion characteristics are also significantly different, with which locking devices may be easier to achieve.

Beam characteristics	
Internal antenna	External antenna
	Approximate spherical dispersion characteristics  (850 MHz, Az=45, EL=45 shown)

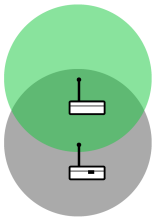
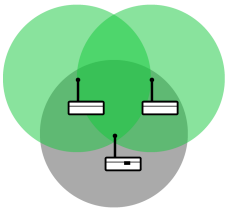
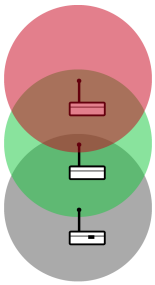
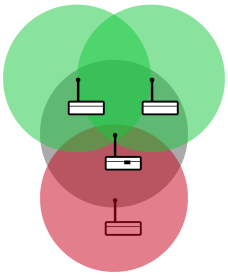
7.2.6 GatewayNode radio radio

Alternatively, if an external antenna is not sufficient to extend the range, a GatewayNode repeater (SI.GN.R) can be installed in the next segment.

The GatewayNode radio radio radio opens a new segment on an existing segment (via the radio interface). A normal segment can be extended a maximum of once with a repeater, but two independent GN.R can be connected to a normal segment (Y shape).

Other uses of repeaters are not possible.

Remember that all traffic in all extended segments "flows" over the original segment and therefore the original segment can become a bottleneck.

✓	✓	✕	✕
			
An existing segment (grey) that is physically connected (RS-485/TCP) is expanded with a repeater (green).	An existing segment (grey) that is physically connected (RS-485/TCP) is expanded with two repeaters (green).	An existing segment (grey) that is physically connected (RS-485/TCP) is expanded with a repeater (green). Another repeater in series to further expand the extended segment is not allowed (red).	An existing segment (grey) that is physically connected (RS-485/TCP) is expanded with two repeaters (green). A third repeater is not allowed (red).

Interfaces

- Radio (WaveNet)

Power supply

SI.GN.R is supplied with WN.POWER.SUPPLY.PPP.

7.2.6.1 Configuration

The repeater (SI.GN.R) is managed exclusively by SmartIntego Manager.

7.3 WaveNet

7.3.1 Description

The WaveNet protocol is a SimonsVoss communication standard between Gateway and LockNodes:

- Frequency: 868 MHz
- Internal topology (addressing)
- Encrypted (AES-128-bit)

7.3.2 Frequency

WaveNet operates in the 868 MHz range and uses one of the two frequencies:

1. 868.099915 MHz
2. 868.0999151999512 MHz

The channel distance is 199.951172 kHz. Frequency 1 is the default frequency. If other systems are present and the systems are disturbing, the second frequency can be compensated for. This change affects all components in WaveNet and is only possible during the first setup.

7.3.3 Topology

Chip ID

The chip ID is a unique number that is permanently programmed into the LockNode. Each LockNode can be clearly addressed with the chip ID (comparable to the MAC address of an IT component). In SmartIntego Manager, the option can be used to Find Chip ID search for a chip ID and thus for a specific LockNode. Chip IDs have eight digits in hexadecimal format, e.g. 00017FD8.

Net ID

The network ID (Net ID) is the name of the WaveNet network. It consists of eight digits in hexadecimal format, e.g. 2DA9. SmartIntego Manager automatically generates the network ID as soon as the first GatewayNode is added to the project (this GatewayNode must be new or reset!). After this, the network ID can no longer be changed and is stored on all components of this WaveNet. Projects with the same network ID must not be within radio range of each other and should therefore generally be avoided.

WaveNet address

WaveNet address is an individual network address for each component. It is used for internal communication between Gateway and LockNodes within the WaveNet. SmartIntego Manager automatically generates WaveNet addresses when Gateway or LockNodes are added to the project.

Normally, the integrator system and LockNodes can communicate with each other without knowing which LockNode has which WaveNet address. Mercury systems trade addressing differently and therefore represent a special case (see *Mercury Security Variant [▸ 114]*).

Network mask

The WaveNet address range includes 65535 addresses. This address range is divided into two groups:

1. Addresses for GatewayNodes
2. Addresses for LockNodes

The division is determined by the network mask:

Network mask	GatewayNode addresses (GatewayNodes in the project)	LockNode addresses (= segment addresses) (LockNodes per GatewayNode)
8_8	2^8 = 256	2 = 256
11_5	2^{11} = 2048	2^5 = 32
12_4	2^{12} = 4096	2^4 = 16

In each segment, the first six and last addresses are reserved for internal use.

Some addresses for GatewayNodes are also reserved for internal purposes and therefore cannot be used.

WaveNet forms the backbone for SmartIntego wireless online projects. The WaveNet quality guidelines for SmartIntego stipulate a maximum of 16 LockNodes per GatewayNode.

Device address

The *device address* is an identification attribute of the LockNodes and GatewayNodes with which they are identified by the integrator system. SmartIntego Manager generates the device address when LockNodes and GatewayNodes are linked and then assigns them individually to LockNodes and GatewayNodes.

Each LockNode and each GatewayNode has a unique device address in the project.

	Device Address	Mercury Device Address
Structural address	■ 0100 ■ 0200 ■ 0300 ■ and so on.	Depending on WaveNet segment: ■ 002100 ■ 002600 ■ 002700 ■ and so on.
Create locking device	Assigned from a pool of free device addresses.	Assigned free WaveNet addresses from a pool.

	Device Address	Mercury Device Address
Replace locking device	Device address changes.	Device address can change. The first free WaveNet address is always used and assigned as the device address.
Replace locking device	Device address remains unchanged.	Device address remains unchanged.
Relocate locking device	Device address remains unchanged.	Device address can change. The first free WaveNet address is always used and assigned as the device address.
Delete locking device	Device address is detached from the component and no longer used for new components.	Device address is detached from the component and can be used for new components.

Import with CSV file

The described topology properties, i.e. the SmartIntego system structure, can be imported automatically into the integrator system (CSV file). If the desired integrator system does not support this function, please contact the integrator who provides the integrator system.

7.3.4 Communication

Each GatewayNode in WaveNet expands its own segment and manages LockNodes within its segment. The WaveNet quality guidelines stipulate a maximum of 16 LockNodes per GatewayNode. A maximum of two repeaters (SI.GN.R) are permitted per wired (Ethernet/RS-485) (see *GatewayNode radio radio [▸ 115]*).

Communication between GatewayNode and LockNode is limited to one active communication per segment. A GatewayNode can therefore only communicate with one LockNode at a time. During this communication, no other communication between the GatewayNode and another LockNode can take place in this segment.

All communication is event-based. If there is nothing to share, then no connection is established either.

GatewayNodes, whose radio ranges overlap, so-called overlapping segments (crosstalk), are also affected by this.

Communication between GatewayNode and LockNode for engaging usually takes a maximum of 500 ms. As a result of this short duration, limiting the connection to a maximum of one active connection is normally not a problem. Larger processes such as extensive programming of locking device configurations (e.g. after updating a whitelist with many entries) can reduce the available bandwidth in WaveNet and lead to temporary disruptions. The integrator system is responsible for sequential processing here.

All components use a list-before-talk procedure. Before sending, the components always check first whether communication is currently taking place within their segment.

- A new communication is only established if no communication is currently taking place in the segment (i.e. the segment is free).
- If communication is ongoing in the segment (i.e. the segment is not free), the component waits and tries to send the data packet up to three times. After the third unsuccessful attempt, the data packet is discarded.

There are three types of communication between the integrator system and LockNode:

1. LockNode to GatewayNode: Events (e.g. reading the card)
2. GatewayNode to LockNode: Commands (e.g. engage locking device)
3. LockNode to GatewayNode: Answers to commands (e.g. successful or why not successful)

In order to extend the battery life of battery-operated locking devices, the following components of the locking device are always in standby mode:

- Card reader
- LockNode

They only become active when they are needed. The LockNode checks every three seconds for a very short time whether a GatewayNode is currently trying to communicate with it. The frequency of these tests can be adjusted (see *Shorter LockNode response times (short wake-up period) [▸ 18]*).

Example: A user opens a door with their card

Event	1. A user holds their card in front of the locking device. 2. The locking device registers an event. 3. The locking device immediately activates the LockNode. 4. The LockNode sends the event immediately via WaveNet. 5. The LockNode remains active for a few seconds in order to receive commands from the integrator system.
Command	1. The integrator system receives the event via WaveNet. 2. The integrator system decides on the opening. 3. The integrator system sends an opening command via WaveNet to the LockNode of the locking device.
Answer	1. The LockNode receives the opening command via WaveNet and forwards the opening command to its locking device. 2. The locking device will engage. 3. The locking device transmits the result of executing the command to the integrator system via its LockNode and WaveNet.

Example: A is opened without an event (e.g. remote opening from the integrator system)

Command	1. The integrator system sends an opening command to the lock. 2. The corresponding GatewayNode attempts to establish contact with the locking device LockNode for a maximum of 12 seconds. (Wake-up signal with interruptions according to 868 MHz specifications)

Answer	1. The LockNode checks every three seconds (adjustable) whether a GatewayNode is currently contacting it. 2. The LockNode receives the opening command from the GatewayNode and forwards it to its locking device. 3. The locking device will engage. 4. The locking device transmits the result of executing the command to the integrator system via its LockNode and WaveNet.

It may take up to twelve seconds between sending a command that comes directly from the integrator system and not responding to an event at the locking device and the corresponding response at the locking device. In a few cases (high frequency utilisation, faults), several attempts may be necessary until a command arrives at the locking device. This process is controlled by the integrator system.

7.3.5 Synchronization

During a communication in WaveNet, the data packages are verified several times internally in order to additionally secure the communication.

The connection between GatewayNodes and the integrator system can be interrupted, for example by restarting the GatewayNodes or the integrator system. Some checksums need to be synchronized again after the connection has been lost.

The integrator system and SmartIntego components automatically synchronize the checksums. If the checksums have not been synchronized automatically, synchronization is performed at the latest during the first active communication. The user must then hold their card again in front of the reader.

7.3.6 Signal Quality Measurement

Signal quality can be measured at different times using different methods:

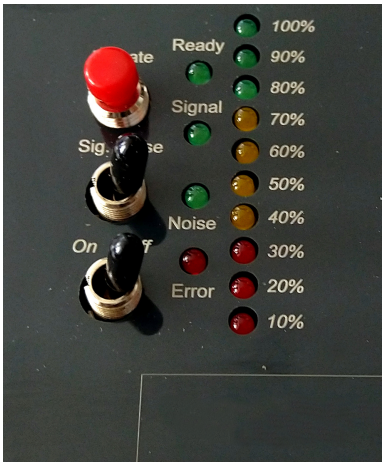
1. Before the project with BAMO
2. During installation with SmartIntego Manager
3. Ongoing measurement during operation and display in the integrator system

The signal quality depends on various influences, for example:

- Other electronic devices that are poorly shielded or communicate by radio

- Environmental obstacles (metal fire doors, new walls with residual moisture...)
- Distance between Gateway and LockNode

Measurement before the project (BAMO)

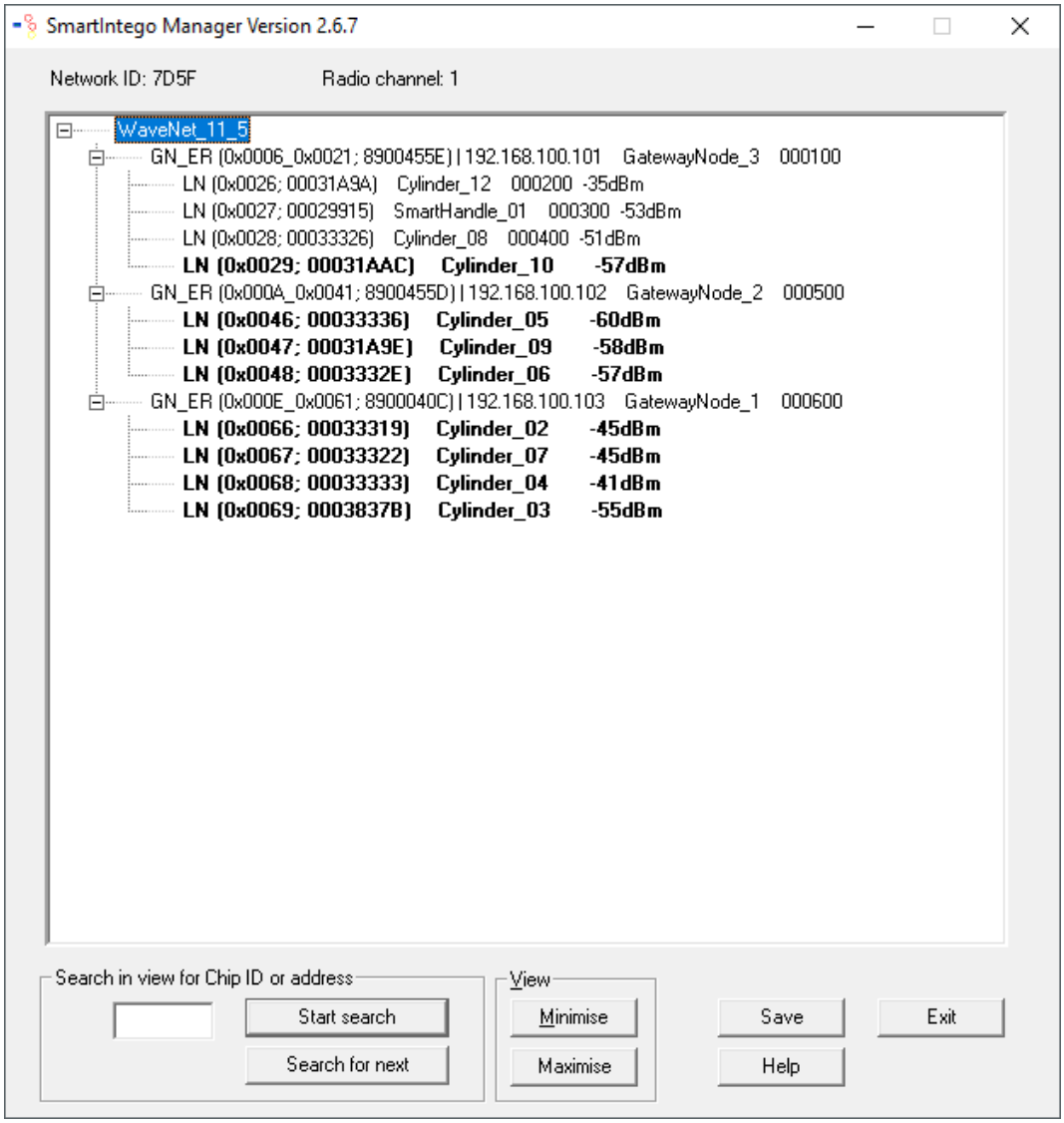


The SimonsVoss WaveNet test tool (BAMO.EU) can be used to take stock of the situation during measurement. The object in which the project is to be implemented should no longer be changed after the measurement. Therefore, measurement in an unfinished building or in a bodyshell is not recommended. The BAMO provides three values with two measurements:

1. Measurement	■ Signal strength (at least 70%) ■ Data packets successfully sent (at least 80%)
2. Measurement	■ Interference signals (0%)

Measurement during installation (SmartIntego Manager)

During installation, SmartIntego Manager displays the RSSI (Received Signal Strength Indication) values measured between GatewayNode and LockNode.



This value in dBm (decibels milliwatts) is:

- Current: An assessment of the status during installation (last packet of communication between SmartIntego Manager and LockNode).
- Logarithmic: In practice, an improvement of 10 dBm means twice the signal strength.
- Negative: The theoretical best value is 0 dBm and is only achieved by cable connections. The closer the value is to 0 dBm, the better reception.

The value displayed in SmartIntego Manager should not be less than -75 dBm for safe operation. Ambient conditions and thus the measured values change during normal operation. The displayed values are therefore only valid together with defined ambient conditions. These environmental conditions must be included and documented:

- Location of GatewayNodes
- Position of locking devices (doors open or closed)

- Interference influences (no moving obstacles between the locking device and the GatewayNode)

Measurement during normal operation (QoS value in the integrator system)

After each communication between the GatewayNode and LockNode in which a packet has been sent and received, the signal quality is calculated as a QoS value (Quality of Service) and sent to the integrator system. This quality index is an average of:

- Packets Received Successfully
- Packets sent successfully
- Number of all packets
- Packets lost or defective
- ACKs not received (internal responses in WaveNet)
- Number of channels used (communication blocked by other communication)

The integrator system can display the received QoS value. Due to the composition and averaging, the QoS value is a long-term calculated value. It is not suitable for detecting short-term signal quality deflections. Short-term faults can be detected with a WaveNet test card (see step-by-step instructions) or SmartIntego Manager.

Improvements in signal quality can only be seen in the QoS values after some time.

A PowerOn reset on the locking device also deletes the QoS value.

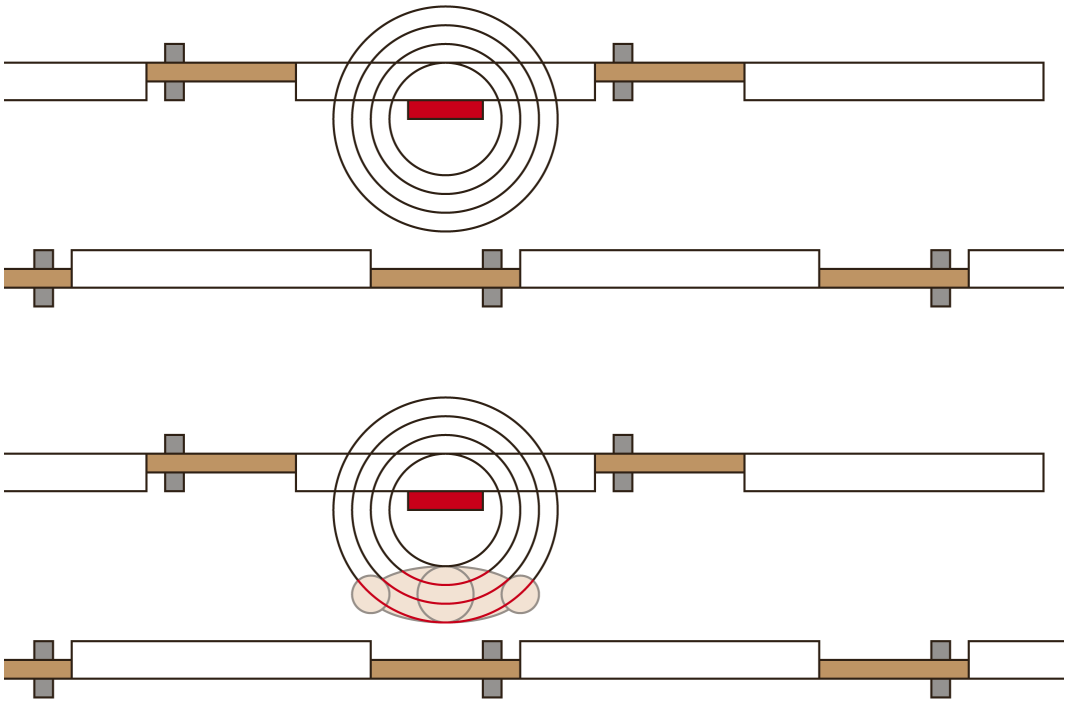
WaveNet quality guidelines for operation with SmartIntego

The quality of WaveNet is viewed more critically for SmartIntego compared to other SimonsVoss products. WaveNet is the backbone of a SmartIntego wireless online system and opening doors largely depends on WaveNet and its infrastructure.

The recommended limits contain a buffer. Reason: The GatewayNode is often positioned in such a way that it reaches as many locking devices as possible without any obstacles:

- GatewayNode in progress
- Locking devices with LockNodes on the outside of the doors

Persons who open the doors normally stand directly in front of the doors and thus shield the LockNode with their body. This significantly impairs the signal quality. The degradation of the signal quality by opening the door is taken into account in the recommended limit value of -75 dBm.



7.4 Programming Device (SI.SmartCD)

The SI.SmartCD is a local USB programming device and is used by the SmartIntego tool:

- Programming of locking devices
  - Via WaveNet (SI.SmartCD remains connected to the configuration PC)
  - Direct
- Emergency opening

- Read-out of offline accesses (also possible via WaveNet)
- Read-out of locking devices (also possible via WaveNet)

The SI.SmartCD requires a direct physical connection to the locking device with which communication is to take place. Due to the short range (near field), the distance between the SI.SmartCD and the card reader of the locking device may only be a few millimetres.

During programming via WaveNet, the SI.SmartCD only needs to be connected to a free USB port until the first locking device has been programmed. The configuration is then fully saved in the SmartIntego tool and the SI.SmartCD can be removed. However, as soon as the card configuration has been changed, the SI.SmartCD must be connected once. It can then be removed again after programming the first locking device.

8 Software

These programs are required to set up a SmartIntego WirelessOnline system:

- SmartIntego tool (WirelessOnline WO)
- SmartIntego Manager (included in SmartIntego tool WO)
- Integrator system (example: SmartIntego Config Tool)

Additional helpful features:

- OAM tool
- Firmware update tool
- SV-QR code scanners (chip IDs)

8.1 SmartIntego Tool (WO)

The SmartIntego tool (WO) is used to manage SmartIntego system configuration and locking devices.

Configurable:

- Passwords
- Card configurations
- Construction site whitelist
- Locking devices (equipment features and configuration beep)
- WaveNet configuration (with the included SmartIntego Manager)

This data is stored in a separate project file (*.ikp) for each locking system. This file is therefore important and must be handled according to the following rules.

1. Only work with a single copy of the project file.
   - ↳ The configuration status in the software and locking devices must match what is actually programmed.
   - ↳ Older project files with a different status are an administrative and security risk!
2. Save the file in a secure and managed IT environment.
3. Backup the project file.

For further information, please refer to the LSM-Mobile manual.

To avoid mixing different projects and systems, a separate project file with a separate password must be created for each customer project.

NOTE

Multiple project files for an integration project

Using a separate project file for each hardware controller of the integrator system significantly increases the administrative effort for the installer.

1. SimonsVoss advises against this type of administration.
2. If necessary, ensure that the integrator system supports the use of multiple project files.

Loss of the project file (*.ikp)

If the project file is lost despite a backed up environment and backup, you will no longer be able to continue working with the existing project.

1. Reset the locking devices with the locking system password.
2. If necessary, reset the LockNodes with a hardware reset.
3. If necessary, reset the GatewayNodes with a hardware reset.
4. Then reprogram the entire locking system.

8.2 SmartIntego Manager

SmartIntego Manager is included in the SmartIntego tool (WO) and configures WaveNet (GatewayNodes and LockNodes) together with it. SmartIntego Manager only works together with the SmartIntego tool (WHO).

The following data is generated:

- WaveNet configuration
- LockNode configuration
- LockNode configuration

When SmartIntego Manager is closed, it transfers this data to the SmartIntego tool (WHO). From there, they are saved in the project file (*.ikp).

The SmartIntegoManager is opened via | Tools | and SmartIntego-Manager - SmartIntego-Manager.

8.3 OAM tool

The OAM tool can:

- change the IP settings of a GatewayNode
- open the configuration website of a GatewayNode
- open HTTPS configuration website of a GatewayNode (required for AES encryption settings)

- update firmware of a GN2

The following chapters describe the procedure in more detail. Some of them are written for RouterNode 2 (System 3060). The procedure for GatewayNode 2 is the same.

To ensure secure operation in the IT infrastructure, it is necessary that some settings are made directly via the configuration website of the GatewayNodes (see *Configuration TCP GatewayNodes [▸ 106]*).

8.4 QR code scanner (chip ID)

The QR code scanner is an auxiliary tool for setting up the locking system. SimonsVoss components supplied must be assigned to the correct doors before configuration to ensure that their size and properties match.

Normally, the name of the door on which the locking device is to be used is written to the packaging of the locking device on the basis of a name list. There is also a data matrix code on the packaging containing the chip ID. This code can be scanned with a data matrix code-capable reader (USB). This step links the doors and GatewayNodes with the chip IDs (and thus also with the LockNodes and locking devices).

The exact procedure is also described in the step-by-step manual.

1. Open the name list (names of the doors and GatewayNodes) with the SimonsVoss QR code scanner.
2. Label the packaging of the locking devices and GatewayNodes with the names from the name list.
3. Scan the respective data matrix codes on the packaging.
   ↳ QR code scanner extracts chip IDs and stores them in the name list.
4. Proceed in the same way with the remaining SmartIntego components.
5. Save the name list with the read chip IDs.

↳ Name list will be used later in SmartIntego Manager.

9 Passwords

The locking system and the locking devices are protected with several passwords. The locking system operator is responsible for managing and storing passwords.

Careless use of passwords can impair the security of the locking system and/or render SmartIntego components unusable.

Locking devices

Password	Protection
Project Password	Protects against unauthorized reprogramming, reading or opening
Locking system password	Protects against unauthorized reprogramming, reading or opening
Card Reading Key	▪ Decides whether the locking device can read the card ▪ Safety-relevant for door opening

LockNodes

Password	Protection
Project Password	Protects system design from unauthorized changes
WaveNet password	Protects against accidental or unauthorized modification (effect e.g. offline device)

GatewayNode

Password	Protection
Project Password	Protects system design from unauthorized changes
WaveNet password	Protects against accidental or unauthorized modification (effect e.g. offline component)
GatewayNode Configuration Password	Protects against unauthorized configuration changes
AES encryption password	▪ Protects communication between GatewayNode and integrator system ▪ GN authentication on the integrator system

Integrator system

Password	Protection
AES encryption password	■ Protects communication between GatewayNode and integrator system ■ GN authentication on the integrator system

Project file

Password	Protection
Project Password	Protects against unauthorized opening of the file and its contents

Card configuration

Password	Protection
Project Password	Protects card configuration from unauthorized access or modification
Card configuration password	Additionally protects card configuration within the project file from unauthorized access or modification
Card Reading Key	Reading key is stored in card configuration of the locking device

9.1 Handling passwords

NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.

NOTE

Secure passwords

For all passwords described here, the generally applicable rules for handling passwords apply.

1. Use complex passwords.
2. Use individual passwords/keys for each project or customer.
3. Do not use passwords more than once (whether within a project or across projects).
4. Protect your passwords from loss and keep them safe.

9.2 Project Password

The SmartIntego tool stores global locking system data such as

- Card configuration
- Softwareconfiguration
- WaveNet topology
- ...

in a project file (*.ikp). The project file cannot be opened without the project password. This means that the project password protects the project data from unauthorised access.

Change/Loss

- Can be changed in SI tool
- No restoration possible in case of loss

9.3 Locking system password

The SmartIntego tool uses the locking system password to programme the configuration into the locking devices. The configuration can then only be read out from the locking devices with the locking system password. This means that the locking system password protects the locking device configuration from unauthorised access.

The locking system password is required for every programming. Once the locking system password has been entered, it can no longer simply be changed.

The project file (*.ikp) also contains the locking system password in encrypted form.

IMPORTANT

Loss of locking system password and project file

If you lose both the locking system password and the project file, components can no longer be reset or configured, even by SimonsVoss. The components are then unusable!

1. Write down your passwords.
2. Keep your passwords secure.
3. Backup your project file.

NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.

Change/Loss

1. Reset system (locking device and WaveNet).
2. Create a new project file.
3. Set up system with new password (locking device and WaveNet).

- If lost, the project file can be used (reset)
- Restoration not possible

If the project file and locking system password are lost, the locking system firmware must be replaced.

9.4 WaveNet password

The network configuration is stored on all SmartIntego WirelessOnline components. Regardless of access to the locking device configuration, the WaveNet password protects the network configuration from unauthorised access.

The SmartIntego Manager prompts you to assign a WaveNet password at the first start. During configuration of the WaveNet components, SmartIntego Manager saves the WaveNet password on the SmartIntego WirelessOnline components.

To change the WaveNet password, all components must first be reset with the configuration from the project file.

Change/Loss

1. Reset system (locking device and WaveNet).
2. Create a new project file.
3. Set up system with new password (locking device and WaveNet).

- If lost, the project file can be used (reset)

9.5 Card configuration password

The locking devices require the card configuration to be able to read the cards. The card configuration is saved in the project file (*.ikp).

Optionally, the card configuration can also be protected against inadvertent changes within the project file with the card configuration password.

The card configuration password can be changed using the SmartIntego tool.

Change/Loss

- Can be changed in SI tool

9.6 Card data read key

Depending on the card data to be read, it may be necessary to store the card data read key (DESFire: Reading key of the application/file or Classic: Reading key of the sector). The read key is part of the card configuration and is saved together with it in the project file (*.ikp) and in the locking devices.

The read key is used by the locking devices to read only the relevant part of the card's memory space.

The card manufacturer or other users of the card provide the card's reading key, for example as a template file (*.ikt) or directly in plain text. For information, see the step-by-step manual.

Change/Loss

- Can be changed in SI tool
- All locking devices and cards must be reprogrammed

9.7 Password for GatewayNode configuration website

TCP GatewayNode is an IT component. The TCP configuration is entered on the Gateway Node configuration website. The configuration website can only be accessed with a password.

You receive the device with the following factory configuration:

IP address	192.168.100.100 (if no DHCP server is found)
Subnet mask	255.255.0.0
User name	SimonsVoss
Password	SimonsVoss

IMPORTANT

Access via default password

Other people can access the product using the factory-set access data.

Some browsers do not transmit spaces at the beginning of the password.

1. Change the default password.
2. Do not start the password with spaces.

NOTE

Loss of passwords

Your passwords are the basis for managing your locking system. Lost or publicly known passwords are a serious security risk and/or lead to loss of control over the system.

1. Make a note of your passwords.
2. Store your passwords in a safe place.

Change/Loss

- Can be changed on the GatewayNode configuration website
- If lost, the GatewayNode can be reset

9.8 AES encryption password

The integrator system is normally connected to the GatwayNodes. Traffic over this connection should be encrypted using the secret AES password (see also description of the integrator system).

This password is stored on the GatewayNodes via the HTTPS configuration website and also in the integrator system itself.

The AES encryption password can be viewed and changed via the HTTPS configuration website.

Change/Loss

- Can be changed on the GatewayNode configuration website and in the integrator system

- If lost, the GatewayNode can be reset

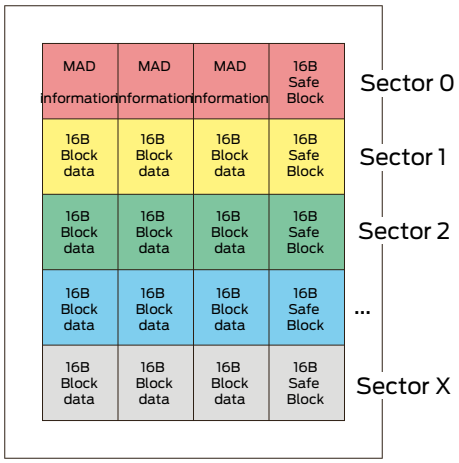
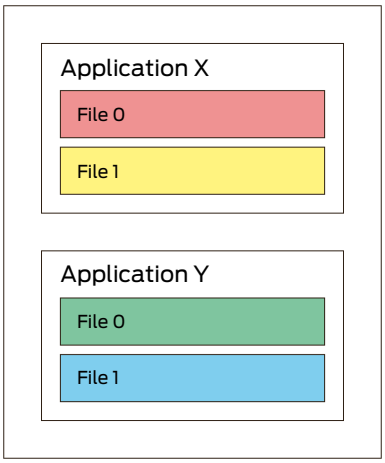
10 Cards

10.1 Card types (WirelessOnline)

- Frequency range: 13.56 MHz (RFID)
- Technologies:
  - ISO 14443-A
  - ISO 14443-B

Data Types	
■ Unique ID ■ Card Serial Number (CSN)	Card ID as data record
■ MIFARE Ultralight ■ MIFARE Classic (1K/4K/Mini) ■ MIFARE DESFire ■ Legic-advant (ISO 14443)	■ MIFARE Classic (Sectors or Mifare Application Directory=MAD) ■ MIFARE DESFire (application)
■ No pre-programming of the card required ■ Unsafe (skimming and duplication possible) ■ No parallel use with data on the card in the same system	■ Card pre-programming required ■ Safe ■ Up to five setups possible in one system

MIFARE Classic	MIFARE DESFire
■ Data stored in sectors ■ Addressing directly with sectors or Mifare Application Directory (=MAD) ■ Sector protection via key in MAD ■ MIFARE Classic encryption hacked and now insecure	■ Data saved in files ■ Addressing with application ID and file ID ■ File backed up by file read key ■ Card ID must be stored in an application file, read access to the file is required ■ Encryption with AES

MIFARE Classic	MIFARE DESFire
Distribution of the memory: 	Distribution of the memory: 

10.2 Card settings

SmartIntego WirelessOnline can read different cards.

Minimum requirements for using a card:

Frequency	13.56 MHz (RFID)
Supported Reading Technologies	ISO 14443-A ISO 14443-B
Unique Identifier/Card Serial Number	Static

10.2.1 UID mode (Unique Identifier)

In this mode, the card is only identified by the unique identifier or card serial number read out.

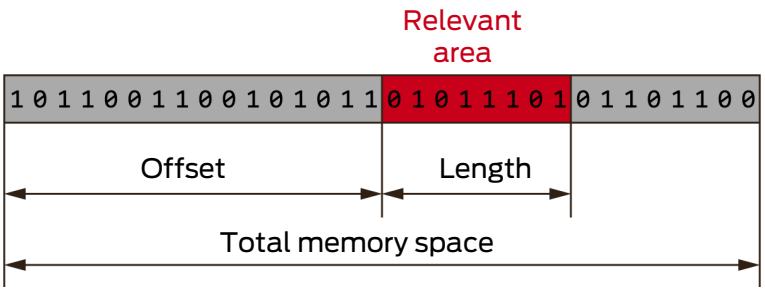
Neither the unique identifier nor the card serial number are protected in any way. Attackers can identify the card with its unique identifier and card serial number.

Frequency	13.56 MHz (RFID)
Supported Reading Technologies	ISO 14443-A ISO 14443-B
Unique Identifier/Card Serial Number	Static

Supported card types	■ MIFARE Classic ■ MIFARE DESFire ■ Legic-advant (ISO 14443) ■ HID iCLASS SEOS UID (ISO 14443)

In the area, "SI-Tool: Kartenkonfiguration - Custom portion [offen]" you specify which contiguous bytes of the identification number should be read out from the locking device. Normally, the entire identification number is evaluated; restrictions are specified by the card manufacturer or the integrator.

SI-Tool: Kartenkonfiguration - Offset Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Offset Whitelist (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Whitelist (Bytes) [offen]
■ Specifies from which byte the identification number is read. ■ Use for online access	■ Specifies how many bytes of the identification number are read. ■ Use for online access	■ Specifies from which byte the identification number is read. ■ Use for whitelist access	■ Specifies how many bytes of the identification number are read. ■ Use for whitelist access



The exact parameters can be found in the documentation of your integrator system.

Identification with a random ID (RID) is not possible.

10.2.2 Password-protected data area

If a data record is used on the card (with UID of the card or another unique ID), each card in the system has its own identification. This identification is stored in a password-protected area of the card.

Access rights to this area of the card are part of the card configuration and stored on the SmartIntego locking devices. After holding such a card, the locking device reads only this area.

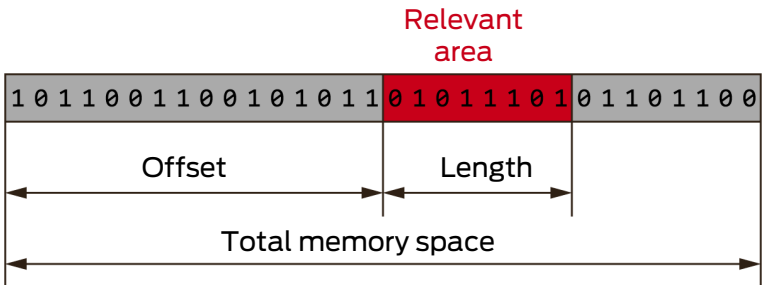
Frequency	13.56 MHz (RFID)
Supported Reading Technologies	ISO 14443-A
Unique Identifier/Card Serial Number	Static or Random
Supported card types including configuration settings	■ Mifare Classic: IsMad (0 or 1) KeyType (KEY A or KEY B) Key MadAid SectorList ■ Mifare Desfire: AppID (decimal) Communication Mode (Encrypted, plain or mac) CryptoMode (AES, 3DES - 3DES not AX-compatible, convert to AES beforehand if necessary) Datei-Nr. ReadKey No. ReadKey (hexadecimal)

Up to five such card configurations can be used simultaneously in a locking system. All card configurations are globally valid: All locking devices in the locking system use the same card configurations.

For each card configuration, it must be specified where the data relevant for the respective card configuration is located on the card.

The locking device should not read out the entire data record of the card. It only requires a number (max. 32 bytes) that uniquely identifies the card. In the area "SI-Tool: Kartenmanagement - LOcation if the data (e.g. card ID) [offen]" you specify which related data should be read out from the locking device.

SI-Tool: Kartenkonfiguration - Offset Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Online Connection (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Offset Whitelist (Bytes) [offen]	SI-Tool: Kartenkonfiguration - Length Whitelist (Bytes) [offen]
■ Specifies from which byte the data is read. ■ Use for online access	■ Specifies how many bytes of the data are read. ■ Use for online access	■ Specifies from which byte the data is read. ■ Use for whitelist access	■ Specifies how many bytes of the data are read. ■ Use for whitelist access



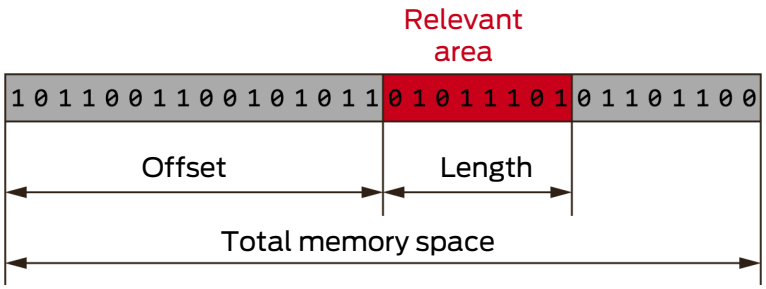
The exact parameters can be found in the documentation of your integrator system.

10.2.3 Calypso cards with serial number

The Calypso serial number is an application ID for a 1TIC.ICA application.

The system is preset to read and process the entire serial number of an 8-byte Calypso card.

Some integrator systems cannot handle the entire length of 8 bytes. In this case, the SmartIntego tool in the "SI-Tool: Kartenkonfiguration - Custom portion [offen]" area offers to specify an offset and the length of the relevant area. The full length of 8 bytes can then be shortened to, for example, one byte.



The exact parameters can be found in the documentation of your integrator system.

10.2.4 ISO7816-4 cards

- File type according to ISO 7816-4: Elementary
- Card type: ISO 14443-A or ISO 14443-B
- ReadCmd
- SelectCmd

The serial number of a card according to ISO 7816-4 is read out with a corresponding read command (ReadCmd) and selection command (SelectCmd). The serial number can then be processed.

These commands must be formatted according to the following structure (Application Protocol Data Unit (= APDU) of ISO 7816-4):

	APDU header (mandatory)				APDU body (optional)		
Case 1	CLA	INS	P1	P2			
Case 2	CLA	INS	P1	P2	Le		
Case 3	CLA	INS	P1	P2	Lc	Data	
Case 4	CLA	INS	P1	P2	Lc	Data	Le

The exact parameters can be found in the documentation of your integrator system.

10.2.5 Return timeout after reading

After a card event, the locking device waits a limited time for a response from the integrator system. This time span is the return timeout.

A response from the integrator system (e.g. an opening command) is only accepted and executed within this time span (online access). If the response is too late or not received at all, the locking device uses the locally saved whitelist after the return timeout expires. Cards on this whitelist then engage the locking device (offline access), all other cards are rejected.

In this case, the user has two options:

- Present card either again (new attempt)
- Use card included in whitelist

The return timeout is a global setting for all locking devices.

11 Changelog

Versions	Changes	Chapter
01.00	FIRST RELEASE	...
01.01	Preparation AX	*SmartHandle AX [▸ 64]*
01.02	Several preparation for AX	Documents
01.03	Bugfix AP2+FD Cylinder	*Locking cylinder (TN4) [▸ 56]*
	Adjustments regarding support for AX components	Documents
01.04	Internal bugfixing	Documents
01.05	Support SI Digital Cylinder AX	*Digital Cylinder AX [▸ 27]*

12 Help and other information

Information material/documents

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

www.smartintego.com/int/home/infocenter/documentation

Software and drivers

Software and drivers can be found on the website:

www.simons-voss.com/en/service/software-downloads.html

Declarations of conformity

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

www.simons-voss.com/en/certificates.html

Hotline

Our hotline 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.

si-support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

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.

ALLEGION

SimonsVoss technologies

Made in Germany