

SmartIntego SVCN System description

Information

21.10.2021

Simons  Voss
technologies

Contents

1	General safety instructions.....	5
2	SmartIntego.....	7
3	SmartIntego Tech Kit.....	8
4	SmartIntego Virtual Card Network (SVCN)	9
4.1	Concept	10
4.2	Time budget in SVCN	10
5	Card structure	14
5.1	ID file.....	16
5.2	Access file.....	16
5.3	Upstream file.....	16
5.4	Types of cards by function	16
5.4.1	Access cards.....	17
5.4.2	Blacklist cards.....	17
5.4.3	Master card	17
5.4.4	Toggle cards	17
5.4.5	Emergency access or fire service cards.....	18
5.4.6	Upstream card.....	18
6	Locking device configuration	19
6.1	Description of locking device properties.....	19
6.2	Classification of locking device properties	20
6.3	Information and help.....	24
6.4	Access list	25
6.5	Event management	25
7	SVCN functions in the integrator system.....	27
7.1	Documentation.....	27
7.2	Handling passwords and backups	27
7.3	Battery management.....	27
7.4	Types of access	28
7.5	Office mode.....	29
7.6	Scheduled permissions (weekly schedule).....	29
7.7	Time-controlled authorisations (public holiday list)	29
7.8	Normal operation.....	29
7.9	Card loss.....	29
7.10	Escape&Return.....	30

8	Components	32
8.1	Door	33
8.2	Storage mode	36
8.3	Types of SmartIntego locking devices	36
8.4	AXEOS operating system	38
8.5	Digital Cylinder AX	38
8.5.1	Structure	38
8.5.2	Variants and features	41
8.5.3	Installation	42
8.5.4	Tool	61
8.5.5	Cover contact	62
8.5.6	Technical specifications	63
8.6	Locking cylinder (TN4)	67
8.6.1	Structure	67
8.6.2	Variants and features	68
8.6.3	Installation	71
8.6.4	Tool	71
8.6.5	Technical specifications	72
8.6.6	Dimensional drawings cylinder	73
8.7	SmartHandle AX	74
8.7.1	Structure	75
8.7.2	Tool	75
8.7.3	Cover contact	76
8.7.4	Technical specifications	76
8.8	SmartHandle 3062	88
8.8.1	Structure	88
8.8.2	Tool	89
8.8.3	Technical specifications	90
8.9	Padlock	94
8.9.1	Technical specifications	94
8.10	SmartLocker AX	96
8.10.1	Technical specifications	96
8.11	Batteries	102
8.11.1	Battery replacement (locking devices and SmartHandles)	103
9	Infrastructure	104
9.1	Update	104
9.2	Programming Device (SI.SmartCD)	104
9.3	Software	105
9.3.1	SmartIntego Tool (SVCN)	105
9.3.2	Integrator system (SmartIntego Config Tool)	108

10	Passwords.....	110
10.1	Handling passwords.....	110
10.2	Project Password.....	110
10.3	Locking system password	111
10.4	Card configuration password.....	112
10.5	Card data read key	112
10.6	Encrypting the transfer between SmartIntego tool (SVCN) and integrator system	112
11	Card Types (SVCN).....	115
11.1	MIFARE Classic.....	116
11.2	MIFARE DESFire.....	116
12	Changelog	118
13	Help and other information	119

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.

Different times for G2 locks

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

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.

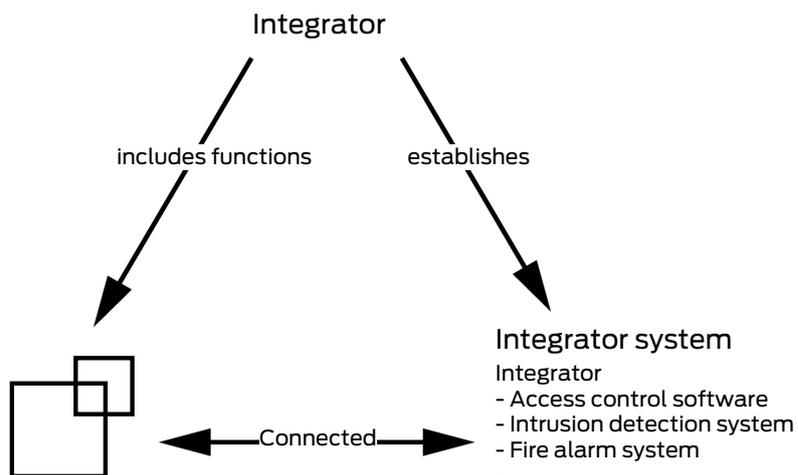
The German language version is the original instruction manual. Other languages (drafting in the contract language) are translations of the original instructions.

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
- 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>).

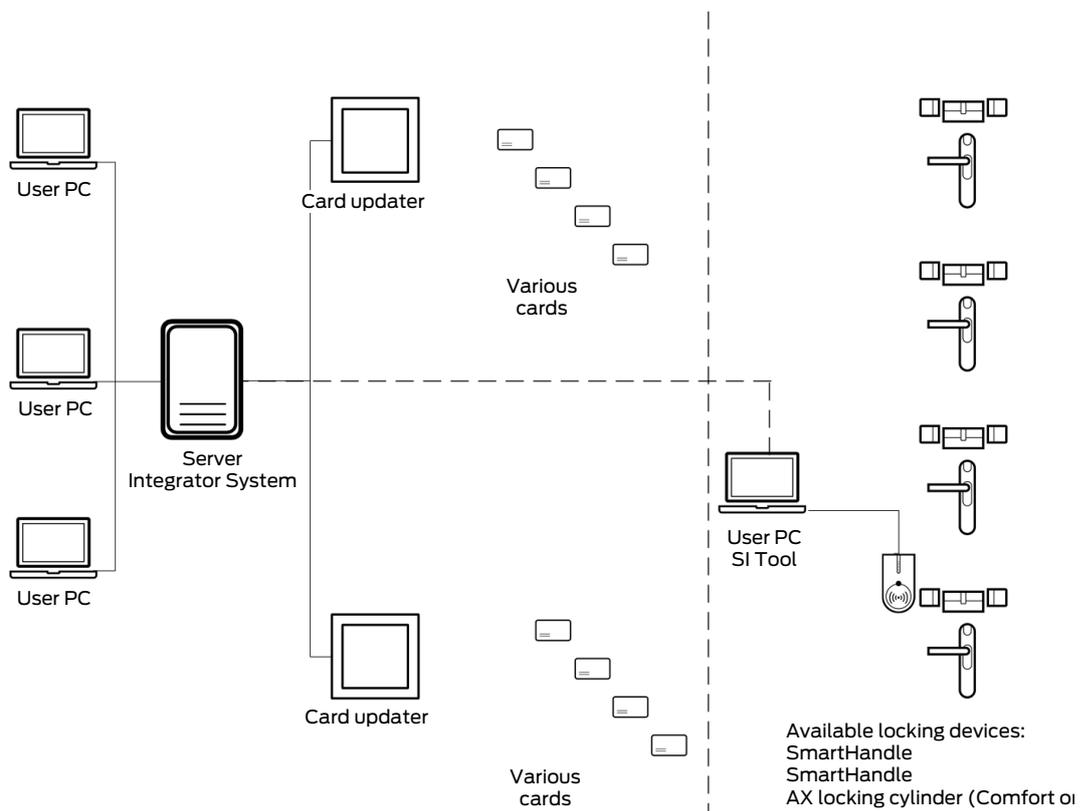
4 SmartIntego Virtual Card Network (SVCN)

The SmartIntego Virtual Card Network (SVCN) is a locking system which consists of cards and battery-operated locking devices and offers basic functions of an electronic locking system:

- Reading data from cards
- Process read data
- Carry out action on the locking device (e.g. engage)
- Optional: Write data to card

The locking devices are not directly connected to the integrator system. Instead, the cards are the carrier medium for communication between the locking devices and the updater (component provided by the integrator).

Project-specific settings are written to the locking devices using a local programming device (SI.SmartCD).



NOTE

Performance depends on the number of cards in circulation

The cards serve as a communication medium in a virtual network.

- The more cards actively participate in the system (i.e. regular use of updaters and locking devices, the better your virtual network will function.

4.1 Concept

All SmartIntego locking devices are part of a locking system and can read all cards and also describe them if required.

Each card contains its own individual data record, which allows it to use the locking devices. This includes:

- Identification of the card
- Authorisations
- Optional: Access list and/or information that writes the locking devices to the card

The updater is a component connected to the integrator system that can read and, if necessary, describe cards. Examples:

- Update terminal
- Punch/shoe
- Electric strike

It represents the connection of the virtual network to the integrator system.

The locking devices themselves only have individual basic information which is compared with the card data. The comparison determines:

- Granting access through the card
- Data transfer from card to locking device
 - Information about lost cards
 - No authorisation
 - Configurator
- Optional: Data transfer from locking device to card
 - Battery warnings
 - Access event log
 - ...

4.2 Time budget in SVCN

The access authorisations are stored on the card. For this reason, a time budget or an expiry date is set for the cards after which they become invalid. Users must therefore regularly hold their cards to the updaters in order to renew their time budgets. Frequent contact between cards and updaters effectively connects the virtual network to the integrator system. Through this connection, real status (locking system) and planned status (software) remain synchronous, including:

- Changes to authorisations

- Information about lost cards
- Card-specific access lists
- Status of locking devices

The time budget or expiry date is essential for most cards in the system. However, it must also be possible to create some cards that are excluded from this:

- Different general cards (time budget depending on customer)
- Emergency access or fire service cards
- Cards with special functions (switchover cards, blacklist cards, etc.)

For card types, see also *Card Types (SVCN)* [[▶ 115](#)].

Time budgets should always be used in offline systems. Otherwise, the cards are rarely or never held to the updaters and the connection of the virtual network to the integrator system is poor. This leads to different statuses in the software and locking system in the long term.

Recommended time budgets

This table is a guide to determine a suitable length for the time budget of the cards. Other *soft* factors should also be taken into account:

- Updater installation situation: Update terminal or door opener
- Building structure (cards use the updater unconsciously and automatically)
- Type of end customer (different operating times, e.g. schools and hospitals)

Different user groups can be assigned different time budgets.

Time budget	Note
≤ 8 hours	<ul style="list-style-type: none"> ■ Very safe ■ Information about lost cards not necessary (depending on customer) ■ Public holiday list possible ■ Implausible for the end user (time budget can expire during working hours)

Time budget	Note
8 hours to 24 hours	<ul style="list-style-type: none"> ❑ Very safe ❑ Information about lost cards not necessary (depending on customer) ❑ Public holiday list possible ❑ Practical for most end users
24 hours to 168 hours	<ul style="list-style-type: none"> ❑ Very safe to sufficiently safe ❑ Information about lost cards ❑ Blacklist card recommended (manual blacklist update: Securing critical doors, e.g. in the building envelope) ❑ Public holiday list possible ❑ Implausible for the end user (time budget top-up at updater is often forgotten)
≥ 168 hours	<ul style="list-style-type: none"> ❑ Unsafe (Lost cards can be found and then used for a long time) ❑ Information about lost cards recommended (but cards rarely on the updater, therefore information may be transferred slowly in the virtual network) ❑ Blacklist card strongly recommended (manual blacklist update: Securing critical doors, e.g. in the building envelope) ❑ Public holiday list not possible ❑ Implausible for the end user (time budget top-up at updater is often forgotten)



NOTE

Security risk due to lost cards

Lost cards can be found by unauthorized persons. These can then open locking devices until the blacklist in the locking devices has been extended with the lost card.

1. Use reasonable time budgets to always synchronize the system promptly.
2. Don't choose unnecessarily long time budgets. Cards whose time budget has expired and which are blocked in the system will normally no longer receive an extension from the integrator's updater.

5 Card structure

The integrator system controls the card structure. Therefore, the Integrator is responsible for:

- Card functions
- Card configuration
- General configuration of the SmartIntego Virtual Card Network (SVCN) with the given card format

This chapter explains the card structure using a MIFARE ESFire card. The SVCN uses three files on the card:

- ID file
- Access file
- Upstream file (optional)

Many entries in the card and the locking device must fit together for processing:

SVCN application (MIFARE DESFire) or reserved sectors (MIFARE Classic):

<i>ID file</i> [▶ 16]	<i>Access file</i> [▶ 16]		<i>Upstream file</i> [▶ 16]	
Identification of the card	Card configuration	<ul style="list-style-type: none"> ■ Area ■ Log level ■ Beeper ■ Long-term engagement ■ Engage Allowed ■ Toggle card ■ Upstream file configuration ■ Time budget: Start date and time Expiration date and time ■ Entry with full access list (indicates that the access list is full) 	Last unauthorized access attempts	2 entries
	Access profiles (several possible)	<ul style="list-style-type: none"> ■ Cups ■ Negative Exceptions ■ Doors ■ Weekly schedule (e.g. Monday to Friday) ■ Office mode 	Priority event list (optional)	<ul style="list-style-type: none"> ■ Up to 255 entries ■ Battery status feedback ■ Blacklist events
	Blacklist entries	<ul style="list-style-type: none"> ■ Card ID ■ Expiry week of the entered card ID 	Status list (optional)	<ul style="list-style-type: none"> ■ Up to 255 entries ■ Blacklist entries ■ Temperature
			Access list (optional)	<ul style="list-style-type: none"> ■ Up to 255 entries ■ Two accuracies (to Version 1: Accurate to 1 minute Version 2: Accurate to 2 minutes)

5.1 ID file

This file identifies the card. It is written directly when the card is created and is no longer changed.

5.2 Access file

This file contains the access authorisations for the card and all the information the locking device needs.

It is created during initial programming. The updater can change the contents of this file:

- Changes to authorisations
- Extensions or changes to the time budget

The locking device itself reads only this file.

5.3 Upstream file

This optional file stores information that is to be returned to the updater during communication with the locking device. Information in this file will return to the integrator system.

It is created during initial programming. Updaters and locking devices can change this file.

Four types of information can be returned with the upstream file:

1. Last unauthorized access attempts: Saves the last two rejected access attempts, the time of the access attempt and the reason for the rejection
2. Priority event list (optional): Saves all battery events and a warning if the blacklist in a locking device is more than 80% full (priority event list is not overwritten on a rolling basis and must be emptied regularly on the updater)
3. Status list (optional): Saves the number of blacklist entries and the locking device temperature
4. Access list (optional): Configurable rolling memory for logging access events

5.4 Types of cards by function

A special feature of the SmartIntego Virtual Card Network is that each card can have individual functions.

The following types of cards are a reference whose implementation depends on the (planned) scope of functionality of the integration.

- *Access cards* [[▶ 17](#)]
- *Blacklist cards* [[▶ 17](#)]

- *Master card [▶ 17]*
- *Toggle cards [▶ 17]*
- *Emergency access or fire service cards [▶ 18]*
- *Upstream card [▶ 18]*

5.4.1 Access cards

- For all end users
- With expiration date/time budget
- With all standard functions
- Largest share of all card types

5.4.2 Blacklist cards

- With information about all cards currently reported as lost
- Maximum 255 entries: If more than 255 cards are lost, a second blacklist card is required
- Must be kept available after each programming of a locking device
- For manually updating the blacklist in locking devices for important doors
- Used when there is no blacklist information stored on normal access cards

5.4.3 Master card

- For users who use the updater regularly (also possible without expiry date/time budget) - Example: As master key for caretakers
- With (long) expiration date/time budget
- With authorisation for all locking devices
- Recommended in order to ensure accessibility of the building in special cases (failure, support work, ...)

5.4.4 Toggle cards

The integrator system can support several types of switchover cards:

- Activation/deactivation cards: These cards activate and deactivate locking devices when present
- Flip-flop cards: These cards permanently engage and disengage locking devices

5.4.5 Emergency access or fire service cards

- For rescue personnel
- Without expiration date/time budget
- With authorisations for doors along escape routes
- Does not need to be updated on the updater

There are different types of fire service key cards. Refer to the integrator system documentation for information.



WARNING

Access for rescue personnel in the event of a system failure

Faults and failing systems often occur in emergencies such as a fire. 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.

5.4.6 Upstream card

- Contains upstream file
- Used when normal access cards do not contain an upstream file

6 Locking device configuration

Locking devices contain some configurations which are configured in the integrator system and programmed with the SmartIntego tool (SVCN).

Integrators can decide for themselves which functions and configurations they support. It is therefore possible that not all described functions are visible or adjustable in your integrator system.

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

6.1 Description of locking device properties

These settings are configured with the integrator system and transferred to the SmartIntego tool (SVCN).

Setting	Description
Area-ID	ID of the area in which the locking device is located
Locking device	ID of the locking device within the given range
Name	Name of the locking device (only for display in the software)
Door code	Unique identifier of the door/locking device (key value)
Group ID	Group profile ID
DLS	Daylight Saving (DLS) setting
Engage time (short)	Time that the locking device engages after reading an authorised card
Engage time (long)	Time that the locking device engages when the long-term coupling is activated after reading an authorised card (e.g. Handicap card)
Office mode	If TRUE: Office mode activated
Threshold for activation (office mode)	Time required for a card to be held in front of the locking device in accordance with Office mode
Override Threshold (Office Mode)	Time that a card must be held in front of the locking device for disengagement in accordance with office mode
Log level	Determined together with the min. Log level, whether an access event is also saved on the card. All access events are always logged on the locking device itself
Access protocol in the locking device	If TRUE: Access events are logged

Setting	Description
Shift Time Threshold	<p>Period of time a special card must be held in front of the locking device.</p> <p>Special cards:</p> <ul style="list-style-type: none"> ■ Changeover card for permanent engagement of the locking device ■ Toggle card to deactivate the locking device
Escape&Return	If TRUE: Escape&Return is activated
Escape & return signal	If TRUE: Locking device signals during active Escape & Return
Escape & Return Timeout	Time that the lock remains engaged after actuating the handle
Beeping enabled	If TRUE: Locking device beeps for signalling
Battery warnings enabled	If TRUE: Locking device displays battery warnings
Access enabled even with full access list	If TRUE: Access still possible when the locking device access list is full
Anti-tamper contact	If TRUE: Tamper contact is evaluated

6.2 Classification of locking device properties

Security

These settings are programmed with a local programming device (SI.SmartCD) and the SmartIntego tool (SVCN).

Value	Cylinders and Padlocks	SmartHandle 3062	SmartHandle 3062 with Escape&Return	SmartHandle AX	SmartHandle AX with Escape&Return
					

Value	Cylinders and Padlocks	SmartHandle 3062	SmartHandle 3062 with Escape&Return	SmartHandle AX	SmartHandle AX with Escape&Return
Locking system ID (Locking system ID)	✓	✓	✓	✓	✓
Locking system password Locking system password	✓	✓	✓	✓	✓
Card configuration Card configuration	✓	✓	✓	✓	✓

Authorisations

These settings are configured with the integrator system and transferred to the SmartIntego tool (SVCN).

Value	Cylinders and Padlocks	SmartHandle 3062	SmartHandle 3062 with Escape&Return	SmartHandle AX	SmartHandle AX with Escape&Return
					
Area ID (AreaID)	✓	✓	✓	✓	✓
Locking device (LockID)	✓	✓	✓	✓	✓

Value	Cylinders and Padlocks	SmartHandle 3062	SmartHandle 3062 with Escape&Return	SmartHandle AX	SmartHandle AX with Escape&Return
Door code (DoorCode) <i>e.g. B1-F5-D23 = "Building 1 - Floor 5 - Door 23"</i>	✓	✓	✓	✓	✓
Groups (Groups)	✓	✓	✓	✓	✓
GroupName (is not transmitted to locking device)	✓	✓	✓	✓	✓
Blacklist (Blacklist)	✓*	✓*	✓*	✓*	✓*

* Currently only transferable to the locking device via the card, not via the SmartIntego tool (SVCN).

Configuration

These settings are configured with the integrator system and transferred to the SmartIntego tool (SVCN).

Value	Cylinders and Padlocks	SmartHandle 3062	SmartHandle 3062 with Escape&Return	SmartHandle AX	SmartHandle AX with Escape&Return
					
Time (Time)	✓	✓	✓	✓	✓
Use daylight saving time (UseDLS)	✓	✓	✓	✓	✓

Value	Cylinders and Padlocks	SmartHandle 3062	SmartHandle 3062 with Escape&Return	SmartHandle AX	SmartHandle AX with Escape&Return
Engage time (short) (Coupling Time)	✓	✓	✓	✓	✓
Engage duration (long, e.g. handicap card) (Coupling Time Long)	✓	✓	✓	✓	✓
Office mode (OfficeMode)	✓	✓	✓	✓	✓
Threshold for activation (office mode) (OfficeMode Threshold)	✓	✓	✓	✓	✓
Override Threshold (Office Mode) (OfficeMode Threshold Release)	✓	✓	✓	✓	✓
Log level (LogLevel)	✓	✓	✓	✓	✓
Access protocol in the locking device (Audit trail On Lock)	✓	✓	✓	✓	✓
Enable / disable (Toggle Deactivation)	✓	✓	✓	✓	✓
Permanent engagement and disengagement (Toggle permanently open)	✓ (Firmware > 5.4.18)	✓ (Firmware > 5.4.18)	✓ (Firmware > 5.4.18)	✓	✓
Escape&Return (Escape Return)	✗	✗	✓	✗	✓
Escape & return signal (Escape Return Signal)	✗	✗	✓	✗	✓

Value	Cylinders and Padlocks	SmartHandle 3062	SmartHandle 3062 with Escape&Return	SmartHandle AX	SmartHandle AX with Escape&Return
Escape & Return Timeout (Escape Return Timeout)	✗	✗	✓	✗	✓
Beeping enabled (Beeping Enabled)	✓	✓	✓	✓	✓
Battery warnings enabled (BatteryWarningEnabled)	✓	✓	✓	✓	✓
Access enabled even with full access list (AccessAtAccessList-FullEnabled)	✓	✓	✓	✓	✓
Anti-tamper contact (Tamper contact)	✗	✗	✗	✓	✓

6.3 Information and help

This information can be transported from the locking device to the integrator system.

Setting	Description
PHI (Master)	Physical Hardware Identifier of the Master
PHI (Slave)	Hardware identifier of the slave (physical hardware identifier) (SmartHandle 3062 only)
OrderData	Equipment string
Version	Firmware version
CR version	Card reader firmware version

Setting	Description
Status	Possible states: <ul style="list-style-type: none"> ■ Programmed (IsProgrammed) ■ Error (IsErrorState) ■ Battery warning (IsBatteryWarningState) ■ Disabled (IsDisabledState) ■ Permanently Open

6.4 Access list

The locking device access list can be transported from the locking device to the integrator system. It can manage a maximum of 1000 entries and, depending on the configuration, overwrites old entries rolling when it is full.

Setting	Description
Index	Unique identifier
Card ID	Unique ID of the card
PC Time	UTC time of the computer when reading the access list
Closing time	UTC time of the locking device when reading out the access list
Access time	UTC time of access (attempt)
Reason for rejection	<ul style="list-style-type: none"> ■ Only in the event of a negative access attempt ■ From firmware master: 5.6.12 and slave: 5.7.14 Master: 5.4.19 and AX platform

6.5 Event management

During the programming of the locking devices, the time of the computer is transferred to the locking devices using the SmartIntego tool.

Alternatively, the time can also be transferred to the locking devices in the SmartIntego tool by carrying out a corresponding time-setting task.

An energy-saving clock is installed in the locking device, which continues the programmed time. Technically speaking, the clock can deviate by up to 15 minutes per year. You should therefore programme the locking devices once a year or set the time. The following functions depend on a correct time:

- Scheduled permissions (weekly schedules)
- Office mode permissions
- Access list on the card
- Access list in the locking device
- Blacklist
- Expiration Date/Time Budget

7 SVCN functions in the integrator system

The availability of the described functions depends on your integration system.

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

7.1 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.

7.2 Handling passwords and backups

Depending on the implementation of the project, different people may be responsible for managing the passwords:

- Integrator
- Installer
- End user

SimonsVoss is not responsible for loss of data or passwords.

7.3 Battery management

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.

Upstream file

The (optional) upstream file on the cards can be used to transport battery warnings in the virtual network to the updater. The integrator system can then alert the locking system administrator to the weak batteries.

Locking devices with the battery status Warning or Alarm write the battery status to the card held. The locking device does not overwrite the list even if it is full. Instead, the locking device waits for the next card with free space in the list. The list is always read and cleared on the updater. Important information cannot be lost as a result of normal inspections. Writing increases an internal counter in the locking device and after six times the

locking device no longer indicates its battery status. The counter first differentiates between the cards in AX components. So in older or mixed projects, it is possible that a single card is described six times.

The counter is reset when the battery is changed and the locking device can write the battery status back on cards the next time the batteries are low again.

Beeps

Beeping is an alternative/additional signalling of the battery status. The locking device will beep to indicate its battery status to the end user who activates the locking device:

- Battery status Ok: 2× beeps
- Battery status warning: 8 beeps before engaging
- Battery status alarm: Multiple beeps for 30 seconds before engaging



NOTE

Unnoticed battery depletion

In a system without any battery warning, the batteries in the locking devices are discharged unnoticed. The batteries can only be replaced "if suspected" and locking devices fail due to empty batteries.

1. The integrator should implement at least one of the two possible battery warnings (upstream file or beeps).
2. Please check the integrator documentation.

7.4 Types of access

Several access types are possible. They are managed by the integrator system:

- Short-term engagement (3 to 25 seconds)
- Office mode
 - Keep the card short: Short-term engagement (3 to 25 seconds)
 - Hold the card for a long time: Long-term opening/flip-flop (1 minute to 23 hours and 59 minutes)
 - Long engagement (e.g. for handicap card)
- Denial of access
- Time-controlled authorisations

7.5 Office mode

Engage for more than 25 seconds is implemented with Office mode. Office mode can engage a locking device for a maximum of 23 hours and 59 minutes

Permanent engagement is only possible with a special card (flip-flop card, see [Toggle cards \[▶ 17\]](#)).

7.6 Scheduled permissions (weekly schedule)

Cards authorisations can be limited in time, for example to office hours. For this purpose, a schedule is created in the integrator system. Please refer to the integrator system documentation for possible settings of this schedule.

The schedule on a card can be created for a maximum of one week (prerequisite: card has the corresponding time budget).

It is not possible to automatically engage locking devices in a time-controlled manner in a SmartIntego Virtual Card Network.

7.7 Time-controlled authorisations (public holiday list)

The public holiday lists are an optional part of the time control. Time control allows the integrator to offer public holiday lists on the card.

The schedule on a card can be created for a maximum of one week (prerequisite: card has the corresponding time budget).

7.8 Normal operation

The integrator system manages SmartIntego components together with the SmartIntego tool (SVCN):

- Add
- Remove
- Change
- Replace

7.9 Card loss

Lost cards can be blocked in the integrator system. In this case, the integrator must ensure the following:

- No extension of the expiration date or reloading of the lost card's time budget
- Share information about card loss with other cards (blacklist cards, access cards or other types of cards)
- Creation of a replacement card (with a different identification number)

- Optional: Make the lost card unusable on the updater
- Optional: Use the upstream file to inform SmartIntego locking devices that they should make the lost card unusable

The blacklist in the locking devices is dynamic and depends on the expiry date of the lost card. It can store a maximum of 500 entries. Information about lost cards is transferred to the locking devices via other cards in the system (card ID and expiry date). The locking device automatically deletes the lost card from the blacklist after it expires.

Cards that have been reactivated can be deleted from the locking device blacklist and used again as usual from the AX platform. Please refer to the integrator documentation for the necessary information.

The integrator system manufacturer is responsible for integrating the blacklist function.

The blacklist can only be transferred by cards. Therefore, transfer all information from the blacklist that has not yet expired to the locking devices after each programming.

7.10 Escape&Return

DoorMonitoring SmartHandles come with the Escape&Return function. This allows opening without the need to press an identification medium again, shortly after the door was closed.

The function is activated by selecting the corresponding check box and the specification of a time window in the integrator system. It must then be programmed with the SmartIntego tool.



Escape & Return:
Enabled:
Time: Sec
Supress Signal:



NOTE

Escape & Return: Legal situation

The Escape & Return Timeout can be between 30 s and 240 s (WO) respectively 1 s and 240 s (SVCN). The use and configuration of Escape & Return may be subject to legal regulations (e.g. Norway).

- Inform yourself in advance about legal regulations.

A sensor in the SmartHandle detects that the inside handle has been operated. The SmartHandle then engages for an adjustable time and signals this visually and acoustically.

Disengagement takes place after the previously defined time. The user can also disengage the locking device manually (thus canceling the escape and return function) by holding his card two seconds in front of the lock's card reader.

The signalling of the Escape&Return function can be switched off.

Example:

If a guest leaves their hotel room and smells smoke in the corridor, they can go back into their room immediately.

Example 2:

Student residence / retirement home: In many cases, the user notices that he forgot the card immediately after he or she closed the door. With Escape & Return the user can solve this problem himself.

8 Components

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

SmartIntego components available include:

Components on the door

		<p>SI Digital Cylinder AX</p>
		<p>SI-Locking Cylinder</p>
		<p>SI.SmartHandle AX</p>
		<p>SI:SmartHandle</p>

	<p>SI Padlock AX</p>
	<p>SI-Padlock</p>
	<p>SI SmartLocker AX</p>

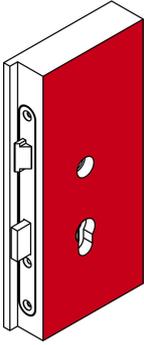
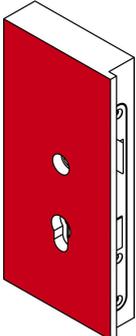
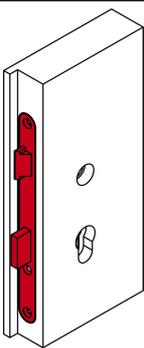
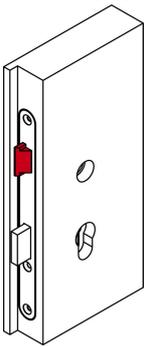
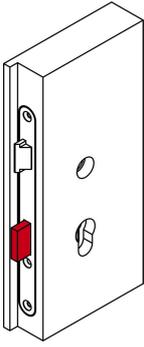
Infrastructure components

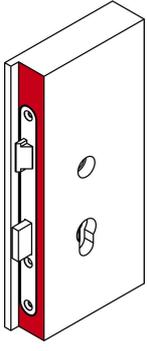
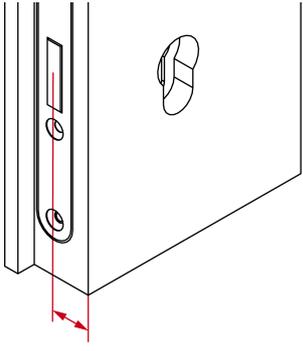
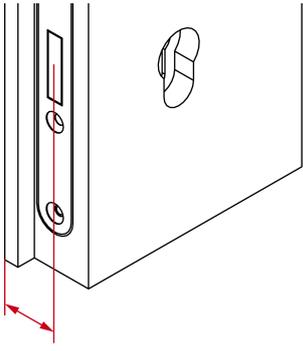
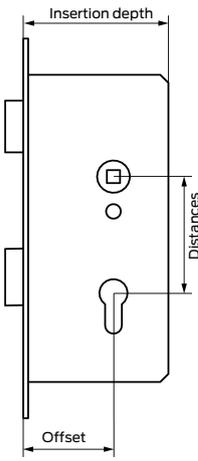
	<p>Programming Device SI.SmartCD</p>
---	--------------------------------------

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

8.1 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

	<p>Door leaf</p>
	<p>Outside dimension (edge of the outside to the centre of the bolt with max. 3 mm projection)</p>
	<p>Inside dimension (inside edge up to the centre of the bolt)</p>
	<ul style="list-style-type: none"> ■ Insertion depth ■ Distances ■ Offset

8.2 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.

8.3 Types of SmartIntego locking devices

There are several types of SmartIntego locking devices:

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

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

<p>SI SmartLocker AX</p>  A 3D rendering of the SI SmartLocker AX lock device. It is a dark grey, rectangular unit with a blue handle on the left side. The device is shown from a three-quarter perspective, highlighting its compact and industrial design.	<p>Lock furniture and locker doors. The function is similar to mechanical locker locks but with the advantages of a digital locking device.</p>
--	---

8.4 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.

In order to stabilise and further develop the basis, the AXEOS operating system behaves more strictly than its predecessor when dealing with configurations. This is why the new SmartIntego tool (SVCN) checks the current card configuration during the update and shows them whether it is compatible with AXEOS products. In the event of problems with existing systems, ask your integrator whether the current configuration is compatible with AXEOS products and, if applicable, what options are available to you.

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

8.5 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.

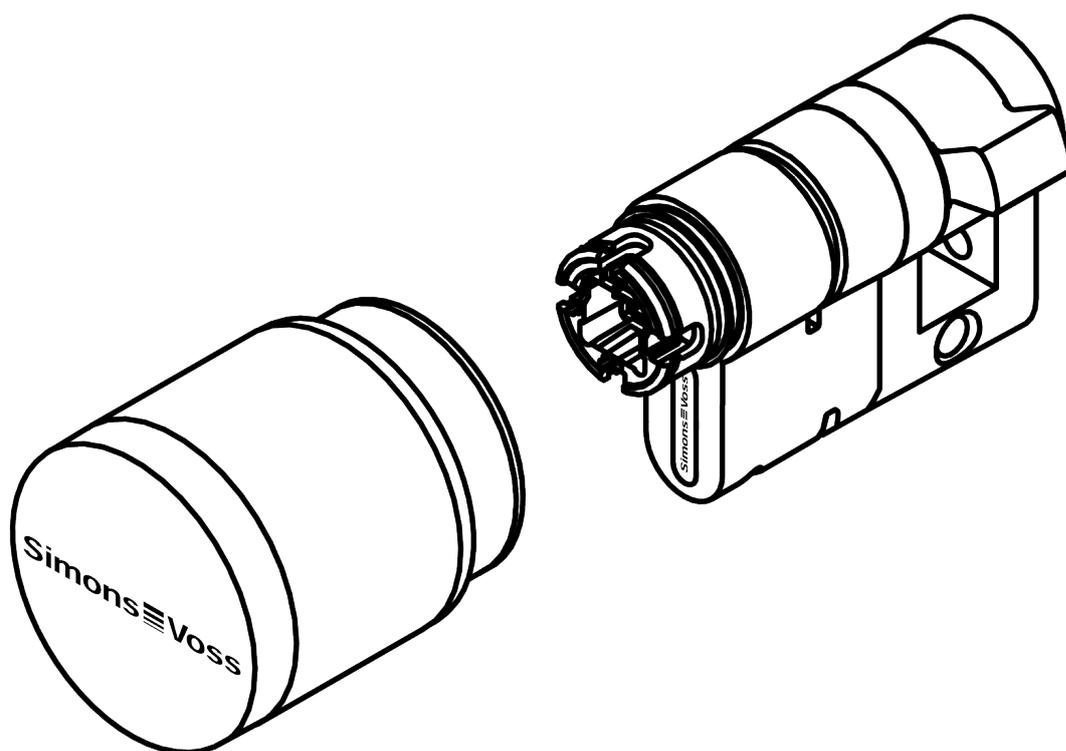
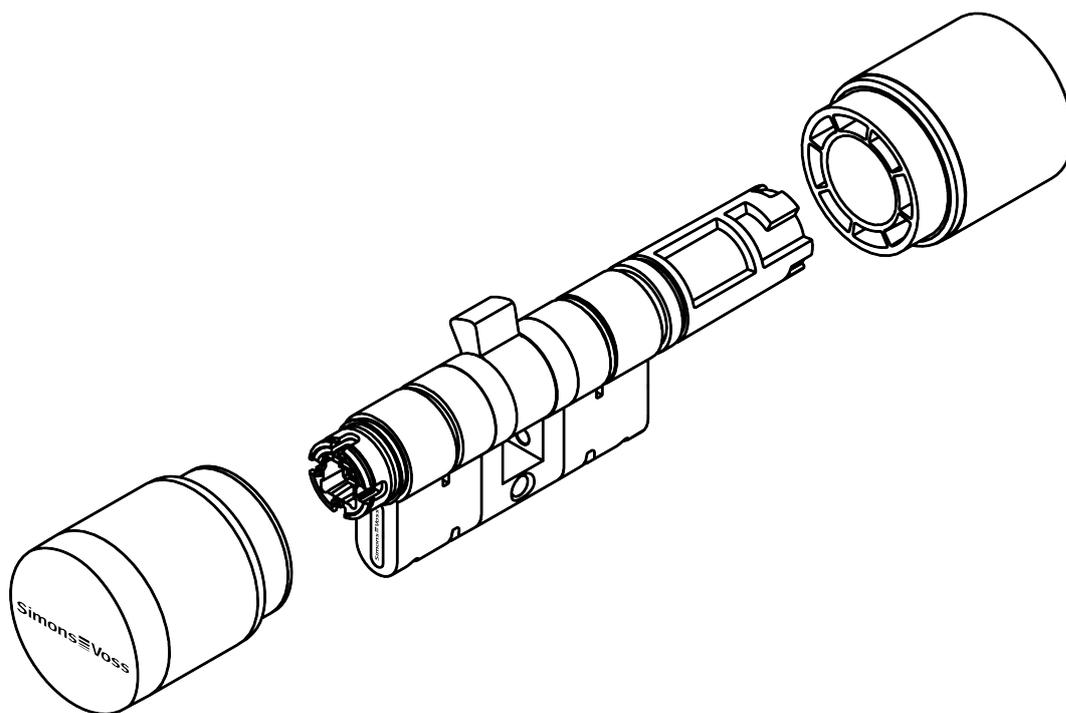
Please refer to the manual of SI Digital Cylinder AX for more information.

8.5.1 Structure

Comfort/half cylinder

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

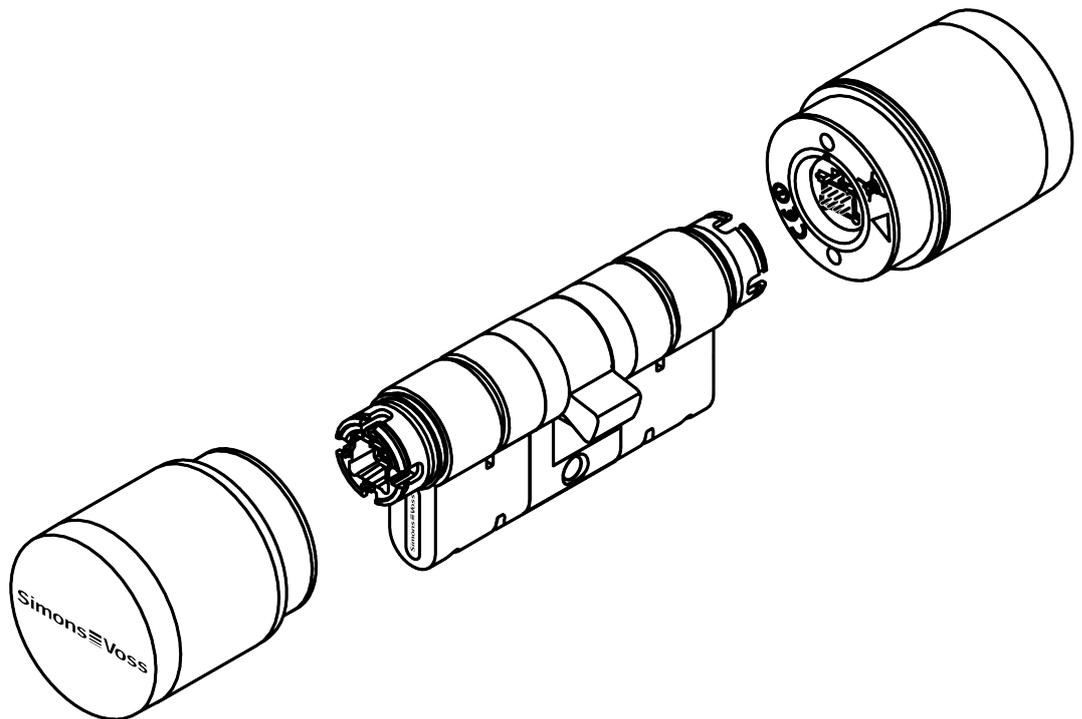
- Control Unit (CU)
- Card Reader (CR)
- Batteries
- Secure element (SE) - in the profile core on the outer side



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)
- 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.



8.5.2 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
	<ul style="list-style-type: none"> ■ EU (Euro Profile/ EU) ■ SR (Swiss Round) ■ SR (Scandinavian Oval) ■ RS (Round Scandinavian) 	Profile
	AXX-IXX	Exterior dimension Interior dimension
	M	MIFARE
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	<ul style="list-style-type: none"> ■ VCN (SmartIntego Virtual Card Network) 	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).

8.5.3 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.

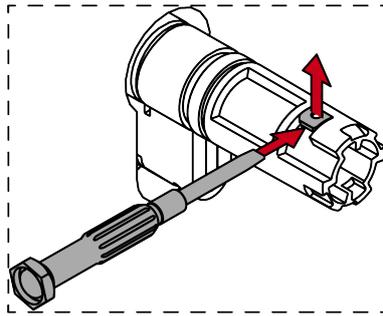
- If you find a mark on the inside (*I/N*) of the cylinder body, mount the AX locking cylinder so that this side is in a protected area.

8.5.3.1 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.)* [▶ 48]).
 2. Insert the AX locking cylinder (see *Insert locking cylinder* [▶ 59]).
 3. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder* [▶ 60]).
 4. Fit the mechanical thumb-turn (see *Mounting thumb-turn (mech.)* [▶ 47]).
 5. Carry out a functional test (see *Functional test* [▶ 57]).
- ↳ 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.)* [▶ 48]).
 2. Dismantle the electronic thumb-turn (see *Unmounting the thumb-turn (electr.)* [▶ 53]).
 3. Insert the AX locking cylinder (see *Insert locking cylinder* [▶ 59]).

4. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder* [▶ 60]).
 5. Fit the cover plates if required.
 6. Fit the electronic knob (see *Mounting thumb-turn (electr.)* [▶ 50]).
 7. Fit the mechanical thumb-turn (see *Mounting thumb-turn (mech.)* [▶ 47]).
 8. Carry out a functional test (see *Functional test* [▶ 57]).
- ↳ 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.)* [▶ 53]).
 2. Insert the AX locking cylinder (see *Insert locking cylinder* [▶ 59]).
 3. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder* [▶ 60]).
 4. Fit the electronic knob (see *Mounting thumb-turn (electr.)* [▶ 50]).
 5. Carry out a functional test (see *Functional test* [▶ 57]).
- ↳ 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.)* [▶ 53]).
 2. Also disassemble the other electronic knob.
 3. Insert the AX locking cylinder (see *Insert locking cylinder* [▶ 59]).
 4. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder* [▶ 60]).
 5. If necessary, attach the covers.
 6. Fit the electronic knob (see *Mounting thumb-turn (electr.)* [▶ 50]).
 7. Also fit the other electronic knob.
 8. Carry out a functional test (see *Functional test* [▶ 57]).
- ↳ SI Digital Cylinder AX is fitted with clip-on covers.

Half cylinder (HZ, reader on one side)

Standard mounting

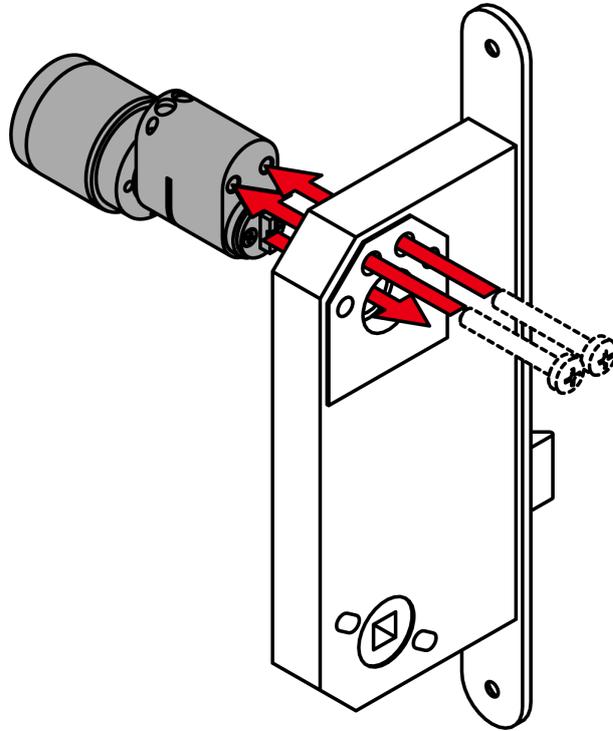
- ✓ Special tool available.
 - ✓ 1.5 mm hexagonal wrench available.
 - 1. Dismantle the electronic thumb-turn (see *Unmounting the thumb-turn (electr.)* [▶ 53]).
 - 2. Insert the AX locking cylinder (see *Insert locking cylinder* [▶ 59]).
 - 3. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder* [▶ 60]).
 - 4. Fit the electronic knob (see *Mounting thumb-turn (electr.)* [▶ 50]).
 - 5. Carry out a functional test (see *Functional test* [▶ 57]).
- ↳ 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.)* [▶ 53]).
 - 2. Insert the AX locking cylinder (see *Insert locking cylinder* [▶ 59]).
 - 3. Secure the AX locking cylinder with the face plate screw (see *Fixing the locking cylinder* [▶ 60]).
 - 4. Fit the electronic knob (see *Mounting thumb-turn (electr.)* [▶ 50]).
 - 5. Carry out a functional test (see *Functional test* [▶ 57]).
- ↳ 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.

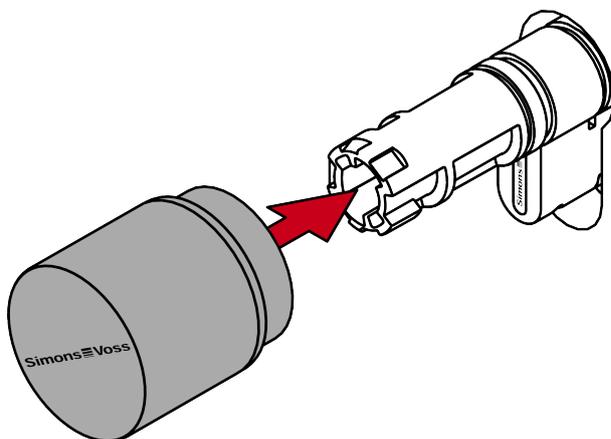
- If you find a mark on the inside (*IN*) of the cylinder body, mount the AX locking cylinder so that this side is in a protected area.

- ✓ 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

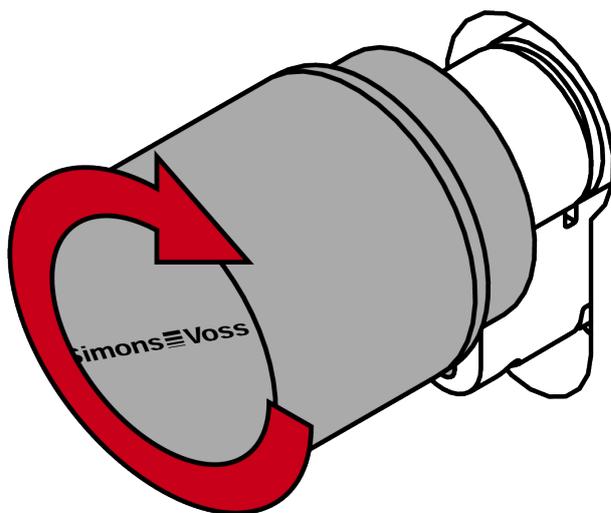
8.5.3.2 Detailed descriptions (individual steps)

Mounting thumb-turn (mech.)

1. Attach the thumb turn.



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

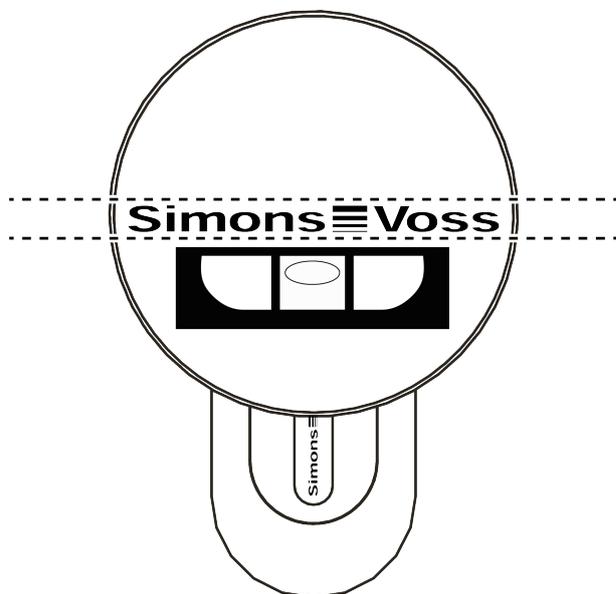


- ↳ Mechanical thumb-turn is installed.
- ↳ Disassembling the mechanical thumb-turn

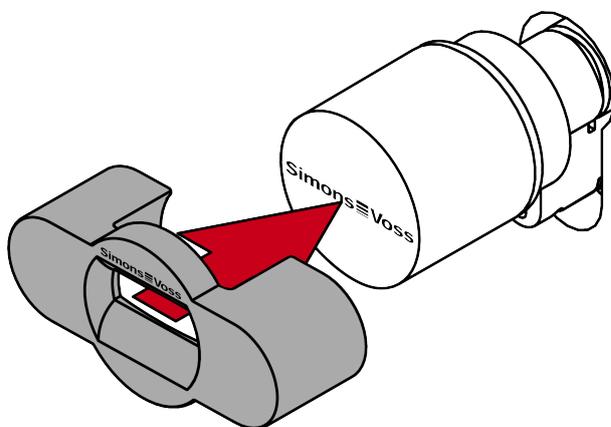
Unmounting the thumb-turn (mech.)

✓ Special tool available.

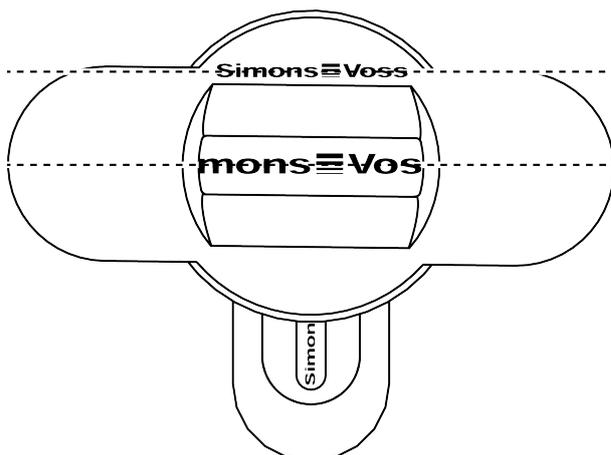
1. Align the thumb turn horizontally.



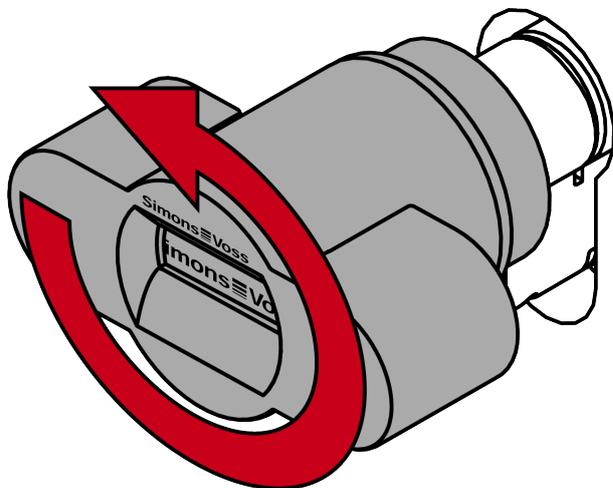
2. Attach the special tool.



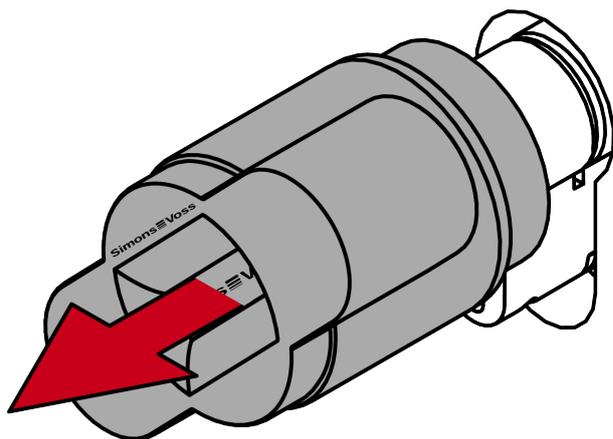
3. Align the special tool so that the logo is parallel to the recess.



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.

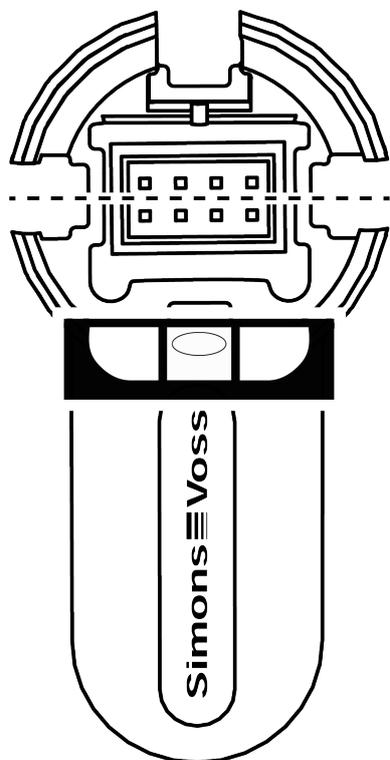


- ↳ The mechanical thumb turn is disassembled.

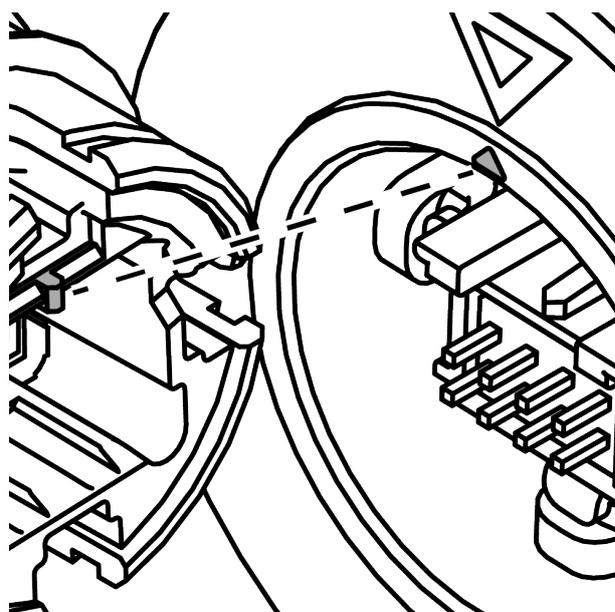
Mounting thumb-turn (electr.)

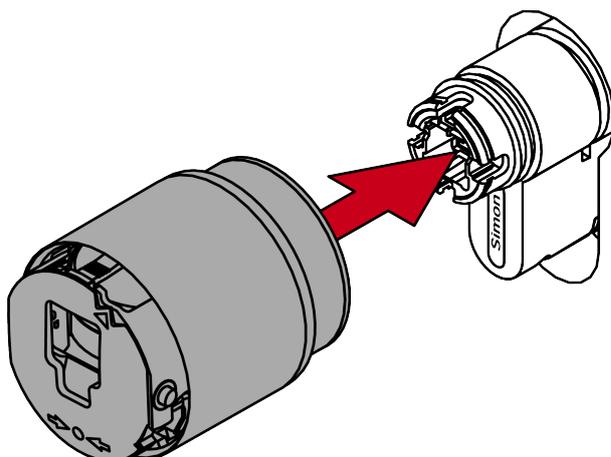
✓ 1.5 mm hexagonal wrench available.

1. Align the thumb turn mount horizontally.



2. Attach the thumb turn.





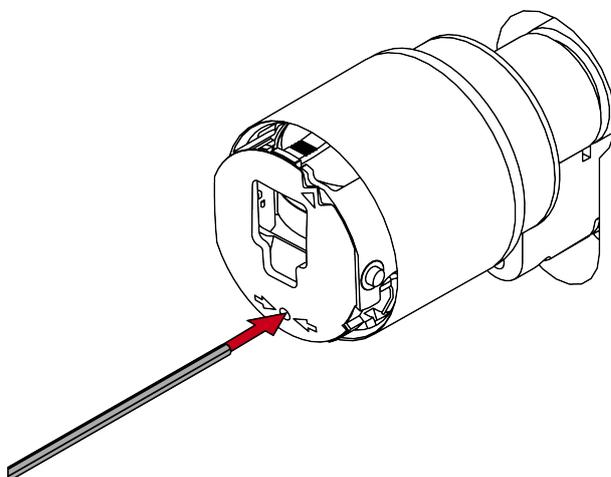
NOTE

Use the supplied hexagonal wrench.

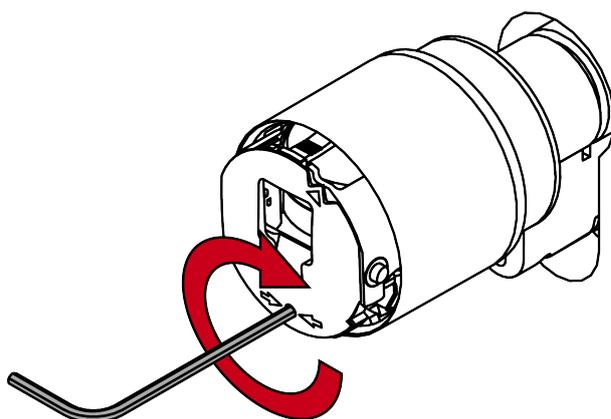
The special tool is supplied with a hexagonal wrench.

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

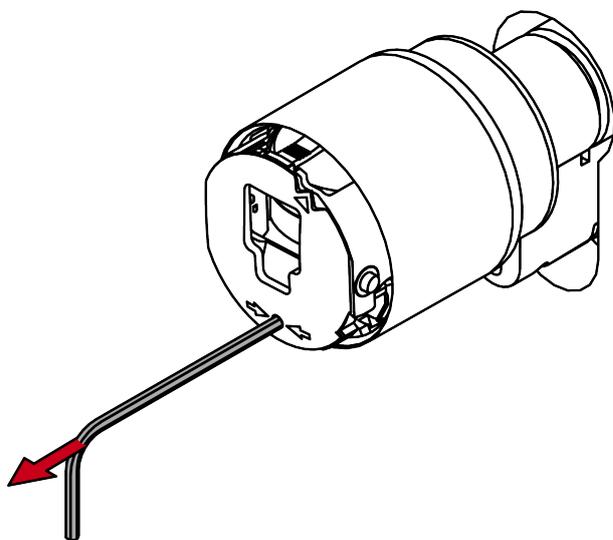
3. Insert the hexagonal wrench into the hole provided until it stops.



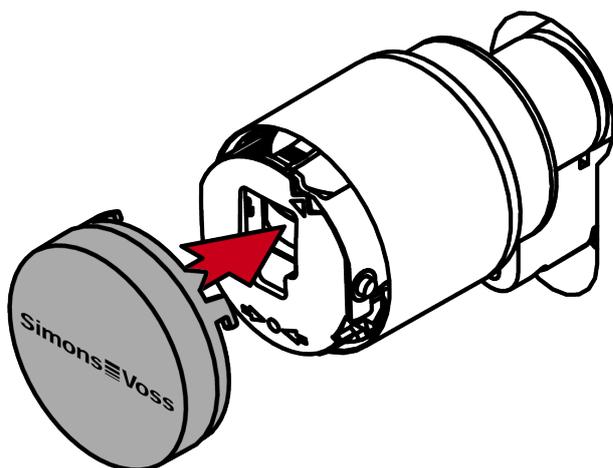
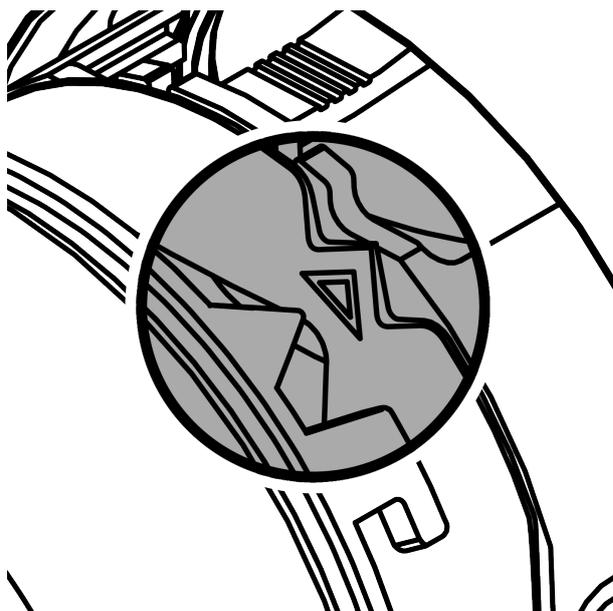
4. Turn the hex key 270 degrees clockwise.



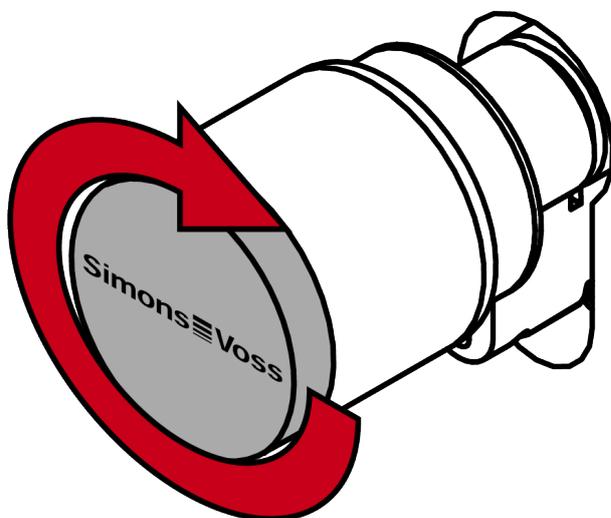
5. Pull out the hexagon wrench again.



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

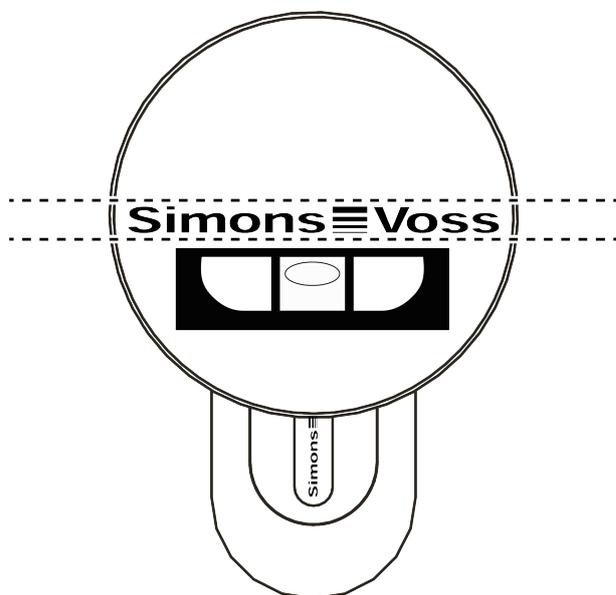
Use the supplied hexagonal wrench.

The special tool is supplied with a hexagonal wrench.

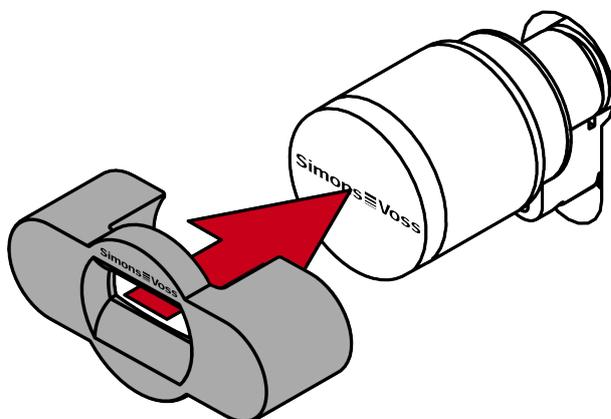
- Use this hexagonal wrench to mount and dismount the electronic thumb turn.

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

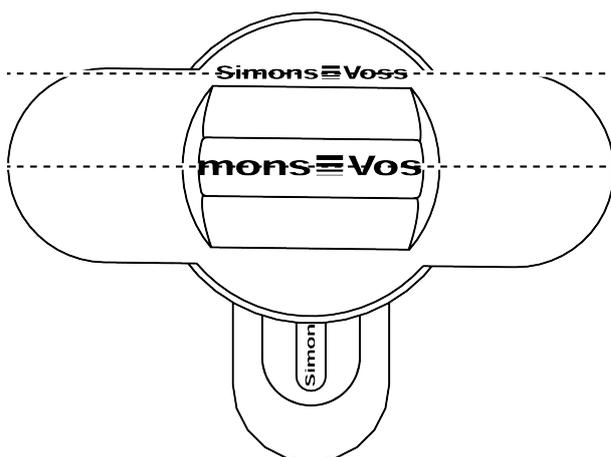
1. Align the thumb turn horizontally.



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.

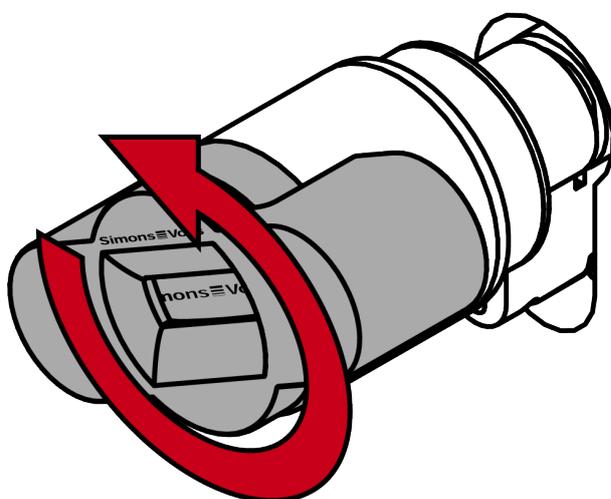


NOTE

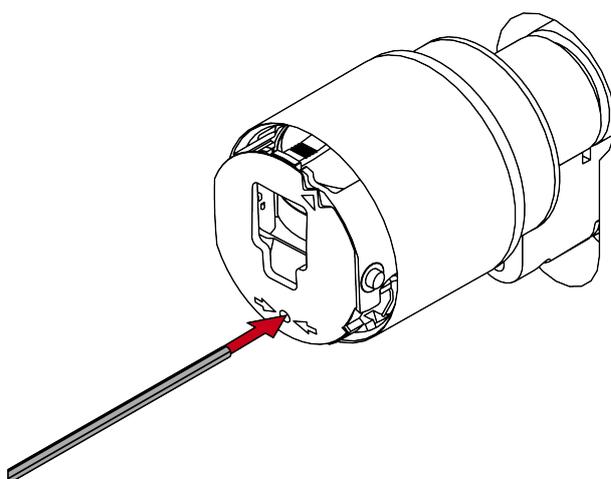
Slipping when turning

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).

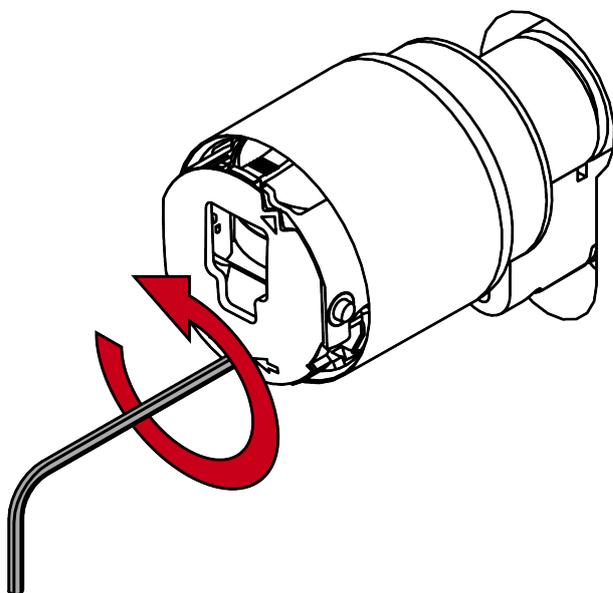
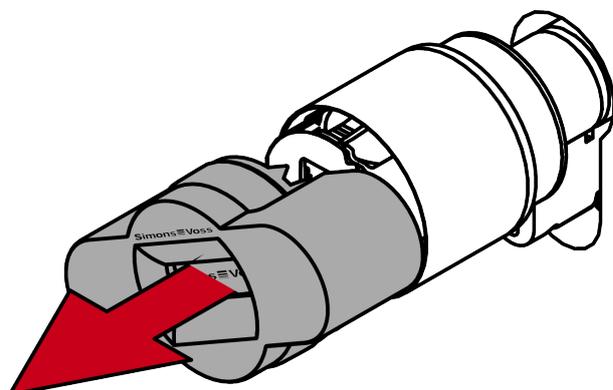
- Wear non-slip gloves.



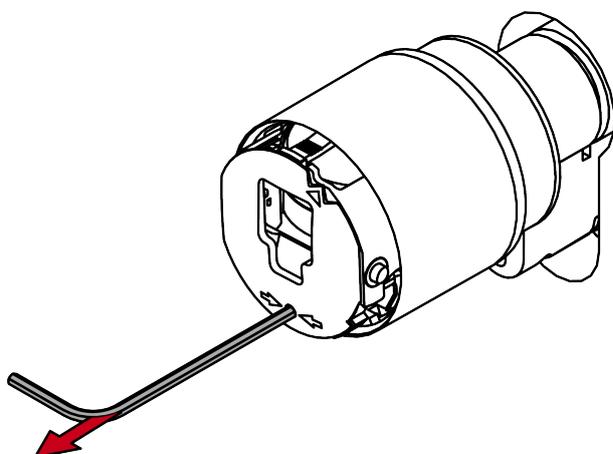
5. Remove the tool and cover.
6. Insert the hexagonal wrench into the hole provided until it stops.



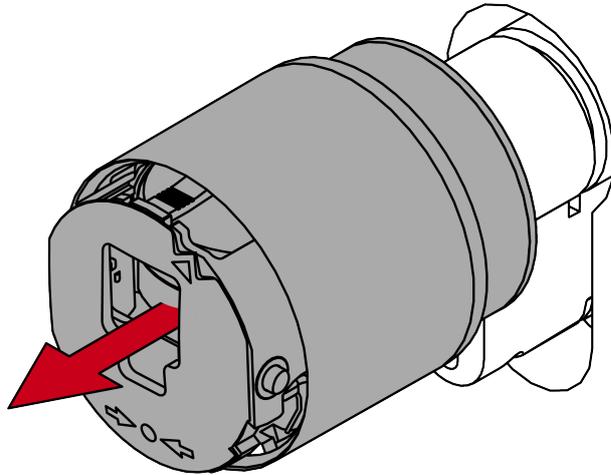
7. Turn the hex wrench 270 degrees counterclockwise.



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

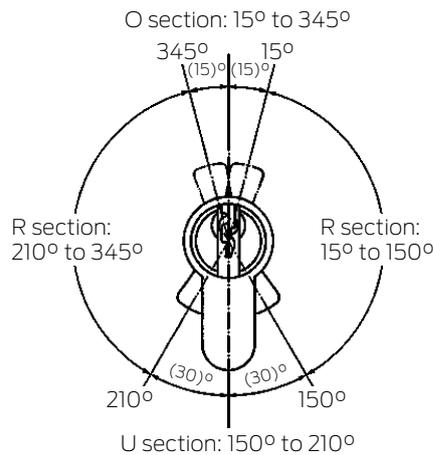
1. Pull hard on the electronic or mechanical thumb-turns.
2. Turn the electronic thumb-turns. The SI Digital Cylinder AX the AX locking cylinder must not be tight, nor rotate the tappet.
3. Activate an authorised identification medium.
4. Check that the SI Digital Cylinder AX engages and pushes out the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

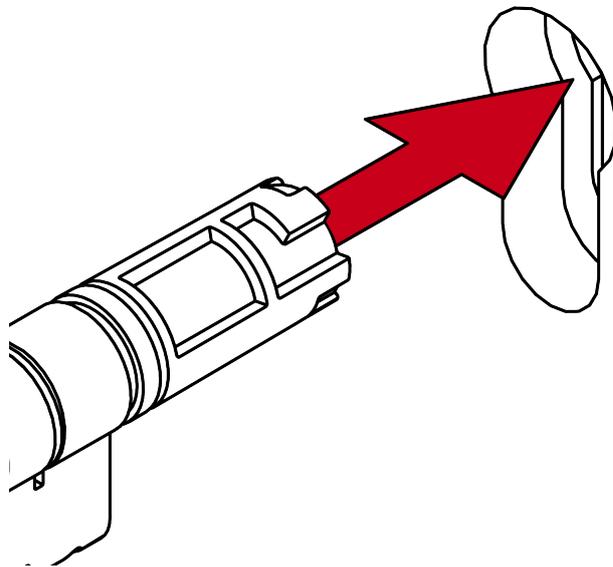
Insert locking cylinder

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

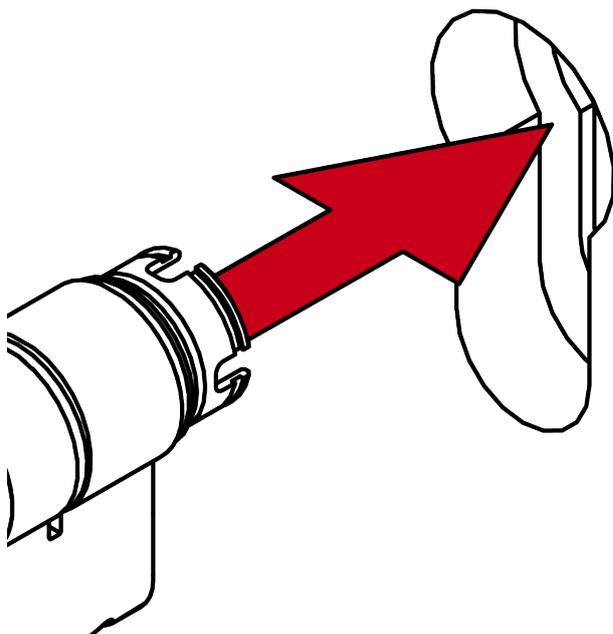
- Insert the locking cylinder AX with the thumb-turn-free side into the lock.



- ↳ AX locking cylinder is positioned in the lock.

SI Digital Cylinder AX inserted with the electronic side

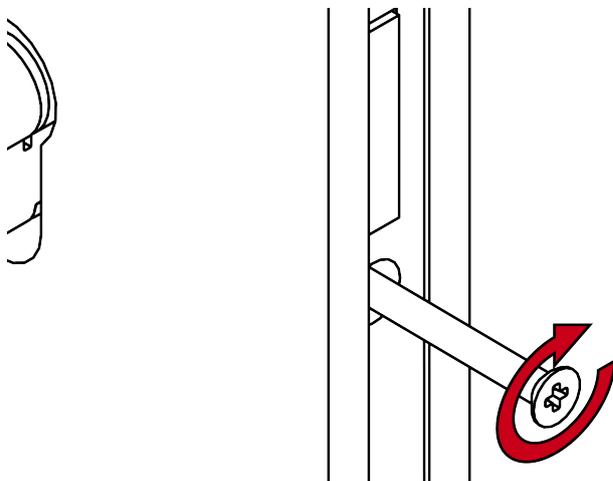
- Insert the locking cylinder AX with the thumb-turn-free side into the lock.



↳ 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.

8.5.4 Tool



Installation	Battery replacement
<p>Tools required:</p> <ul style="list-style-type: none"> ■ 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 	<p>Tools required:</p> <ul style="list-style-type: none"> ■ 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
 <ul style="list-style-type: none"> ■ Z5.BOLT.XX (XX = required basic length) 	 <ul style="list-style-type: none"> ■ Z5.CORE.05: 5 mm ■ Z5.CORE.10: 10 mm ■ Z5.CORE.20: 20 mm 	 <ul style="list-style-type: none"> ■ Z5.PROFILE.05: 5 mm ■ Z5.PROFILE.10: 10 mm ■ Z5.PROFILE.20: 20 mm
Clamps	Half cylinder centre piece	Cylinder centre piece
 <ul style="list-style-type: none"> ■ Z5.CLAMPS <p>Set contains 50 units.</p>	 <ul style="list-style-type: none"> ■ Z5.CNT.HZ 	 <ul style="list-style-type: none"> ■ Z5.CNT.EU
Cam (standard, WP)	Inside thumb-turn mount	
 <ul style="list-style-type: none"> ■ Z5.CAM.WP 	 <ul style="list-style-type: none"> ■ Z5.PR.IN 	

8.5.5 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).



8.5.6 Technical specifications

8.5.6.1 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 dB μ A/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

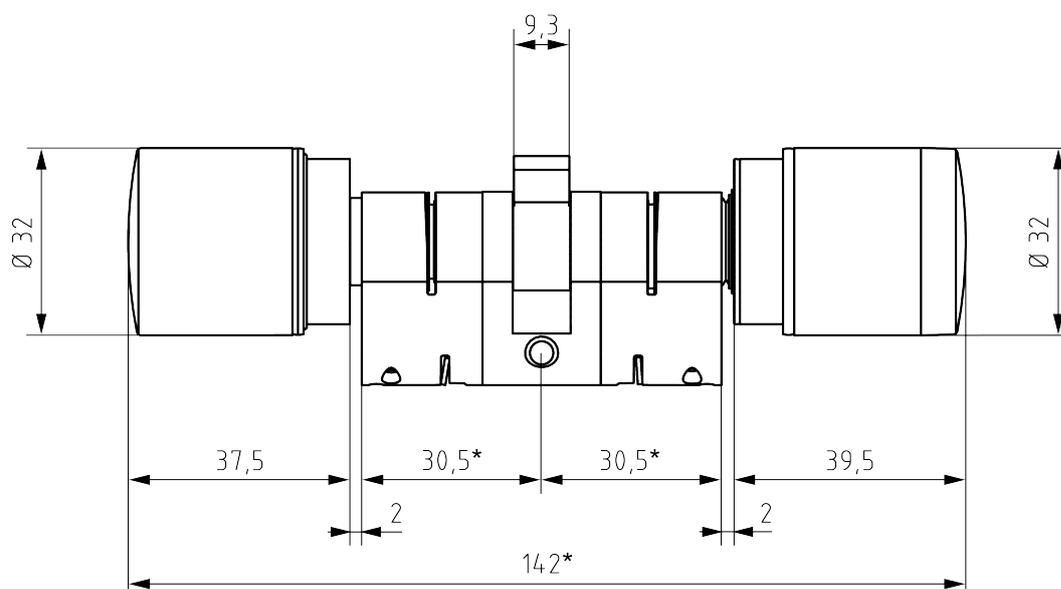
8.5.6.2 Scandinavian Oval Scandinavian Round

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

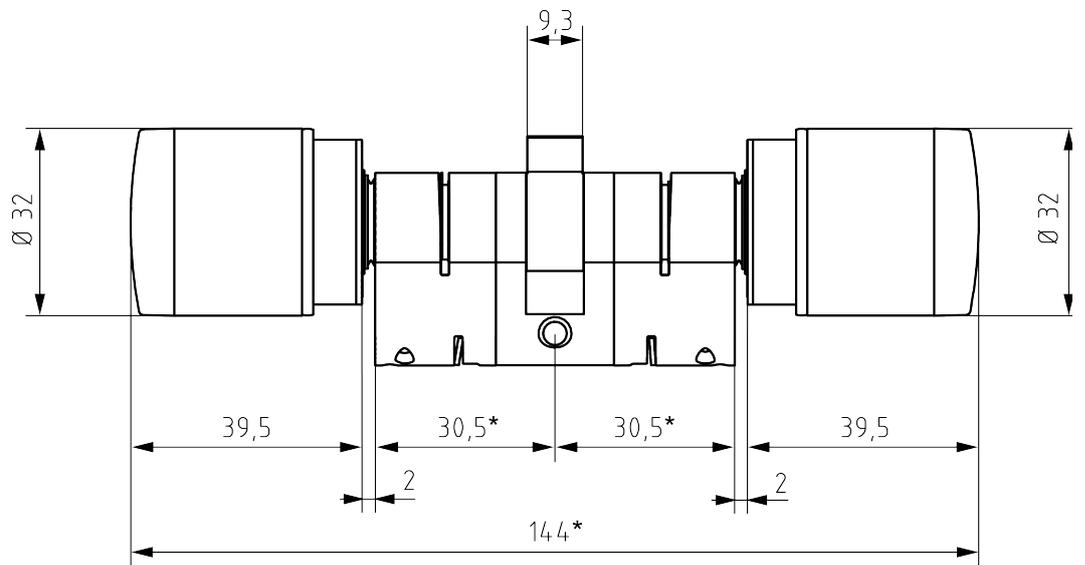
Battery lifetime	Up to 12 years on standby or 100,000 activations (with battery knob: Up to 300,000 activations)
Signalisation	Audible signal (buzzer) and/or visual signal (LED – green/red)
Network capability	Yes (integrated LockNode can be ordered and retrofitted)
Opening modes	Pulse flip-flop
Upgradeability	Firmware upgradable via BLE
Frequency range; max. transmission power RFID (~13,56 MHz)	13.560006 MHz - 13.560780 MHz; 1.04 dB μ A/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

8.5.6.3 Dimensions

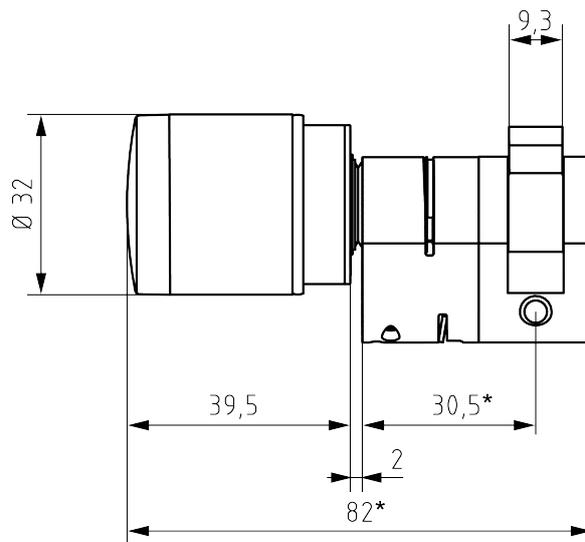
CO (comfort cylinder)



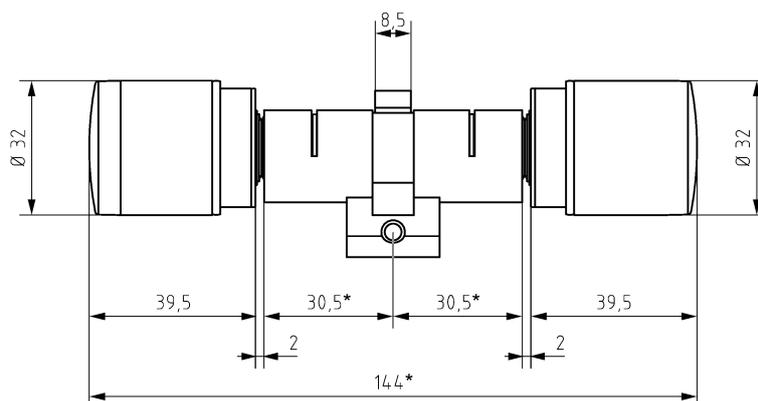
FD (free-rotating cylinder)



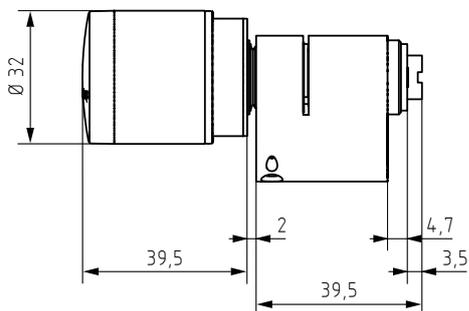
HZ (Half cylinder)



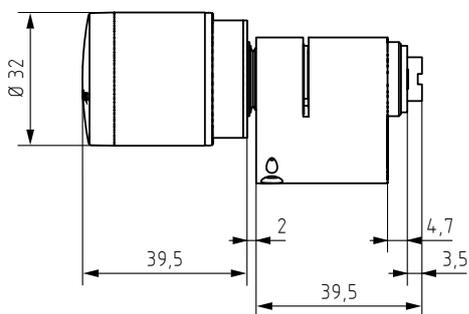
SR (Swiss round profile)



SO (Scandinavian Oval)



RS (Scandinavian Round)



8.6 Locking cylinder (TN4)

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

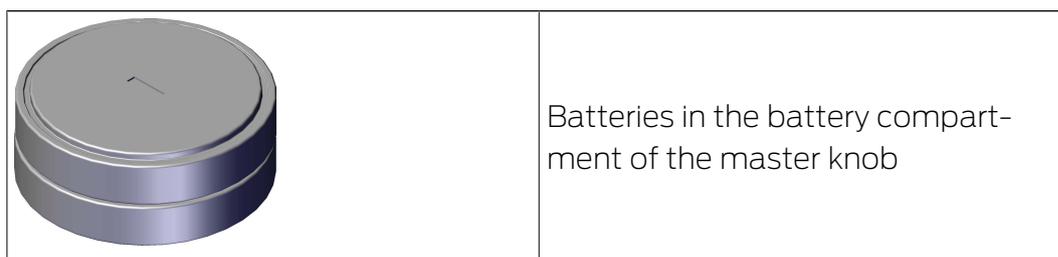
8.6.1 Structure

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)



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* [[▶ 73](#)])
- On the profile housing (IN)

Comfort (CO)	Page	Behaviour (dis-engaged state)	Components	Batteries
Master	Outside	Freely rotating	<ul style="list-style-type: none"> ■ Control Unit ■ Card reader 	2
Slave	Inside	Permanently engaged	No electronics	None

Anti-panic freely rotating (AP2 FD)	Page	Behaviour (dis-engaged state)	Components	Batteries
Master	Outside	Freely rotating	<ul style="list-style-type: none"> ■ Control Unit ■ Card reader 	2
Slave	Inside	Engage not possible	No electronics	None

8.6.2 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
	<ul style="list-style-type: none"> ■ MI (for SmartIntego WirelessOnline) ■ M (for SmartIntego Virtual Card Network) 	<ul style="list-style-type: none"> ■ MIFARE & LockNode Integrated (for SmartIntego Wireless Online) MIFARE Integrated is an abbreviation for <i>MIFARE technology with integrated LockNode</i>. ■ MIFARE (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)



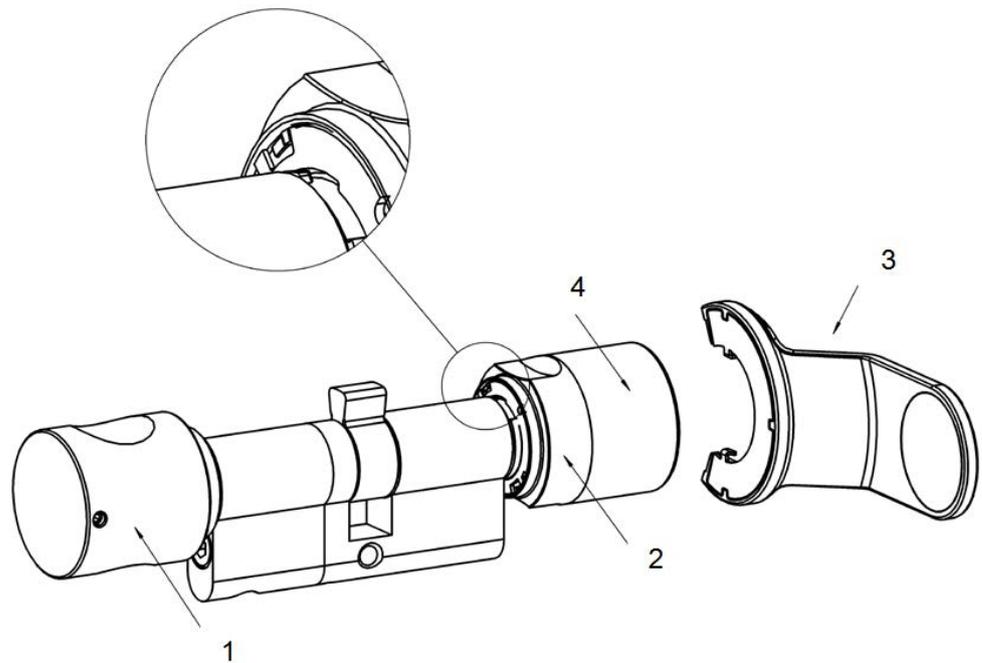
NOTE

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).

8.6.3 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.

8.6.4 Tool



Installation	Battery replacement
Tools required: <ul style="list-style-type: none"> ■ Installation key ■ Battery replacement key (shown) 	Tools required: <ul style="list-style-type: none"> ■ 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.

8.6.5 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

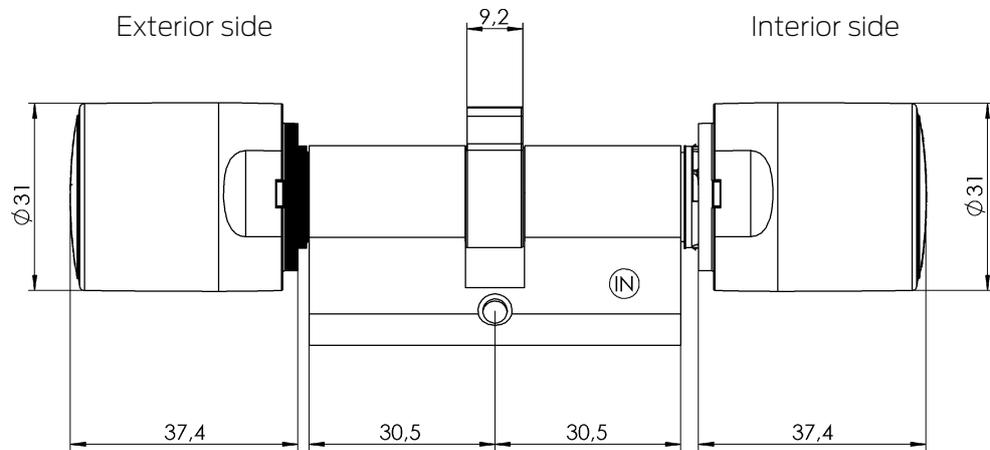
Batteries

Type:	CR, 2450, 3 V
Manufacturer:	Murata, Panasonic, Varta
Quantity:	2 units
Battery life:	SmartIntego Wireless Online (WO): <ul style="list-style-type: none"> ■ Up to 5 years ■ Up to 80,000 activations Card SmartIntego Virtual Card Network (SVCN): <ul style="list-style-type: none"> ■ Up to 6 years ■ Up to 50,000 activations

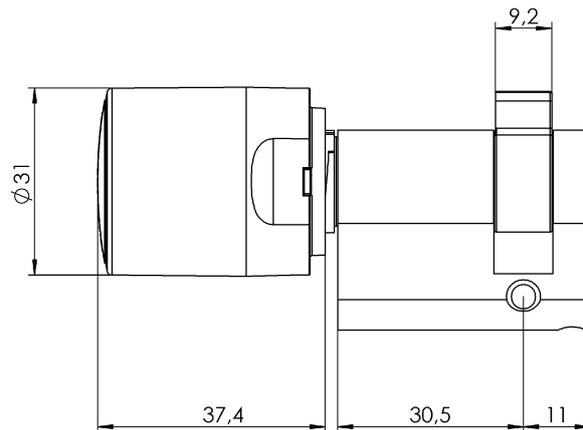
The cylinder provides acoustic and optical (blue/red LED) feedback.

8.6.6 Dimensional drawings cylinder

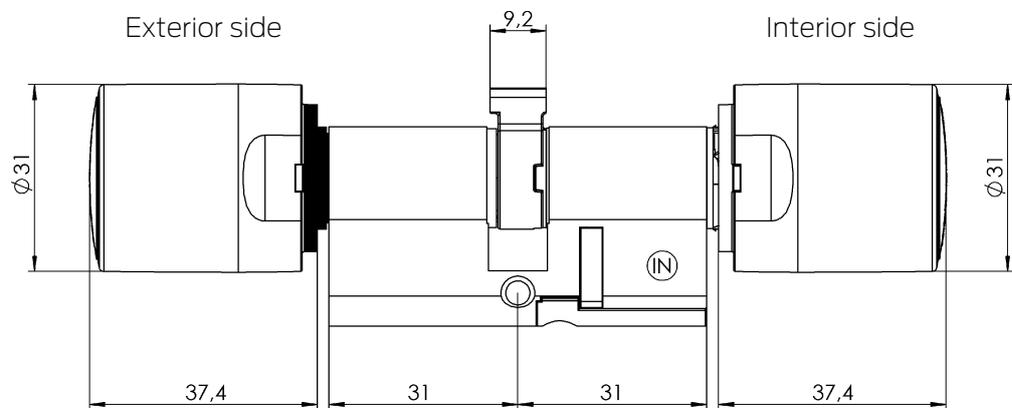
Comfort - Passive (CO MP)



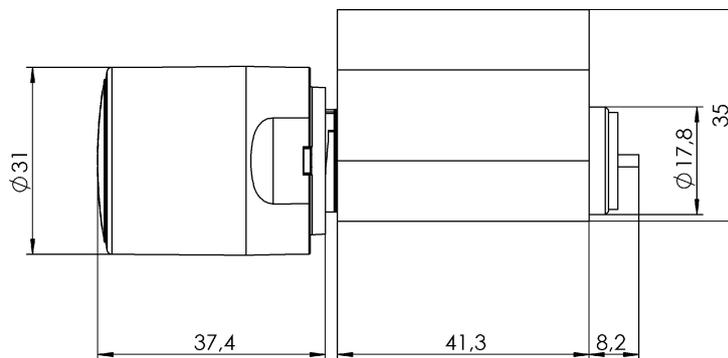
Half Cylinder - Passive (HZ MP)



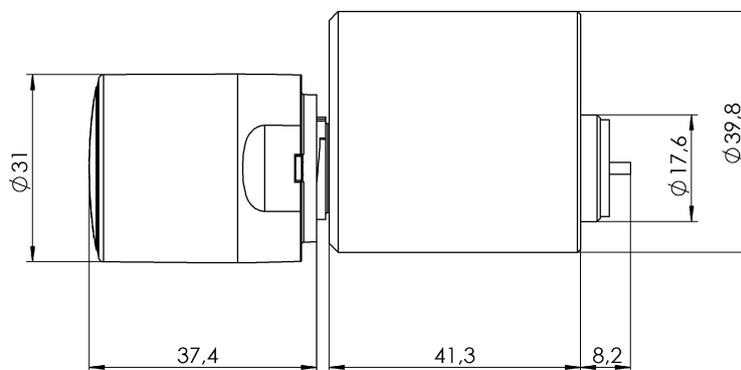
Anti-panic Free rotating - passive (AP2 FD MP)



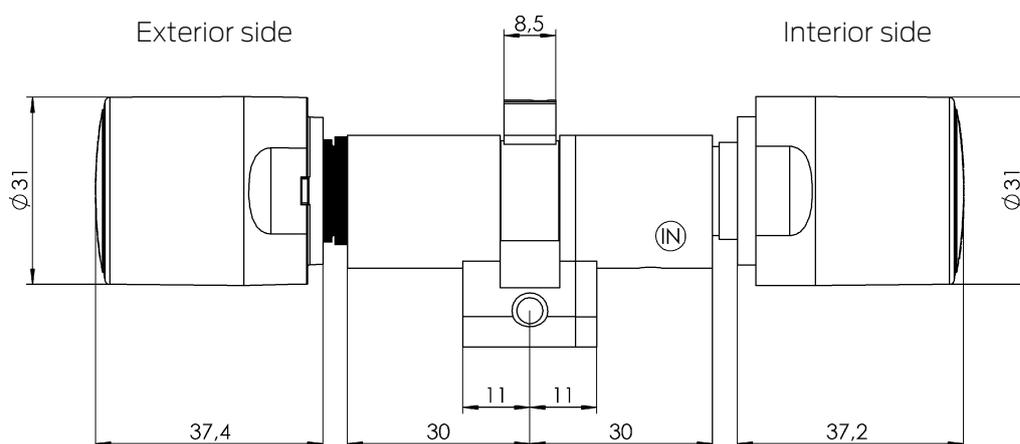
Scandinavian Oval - Passive (SO MP)



Scandinavian Round - Passive (RS MP)



Swiss Round Comfort - Passive (SR CO MP)



8.7 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...

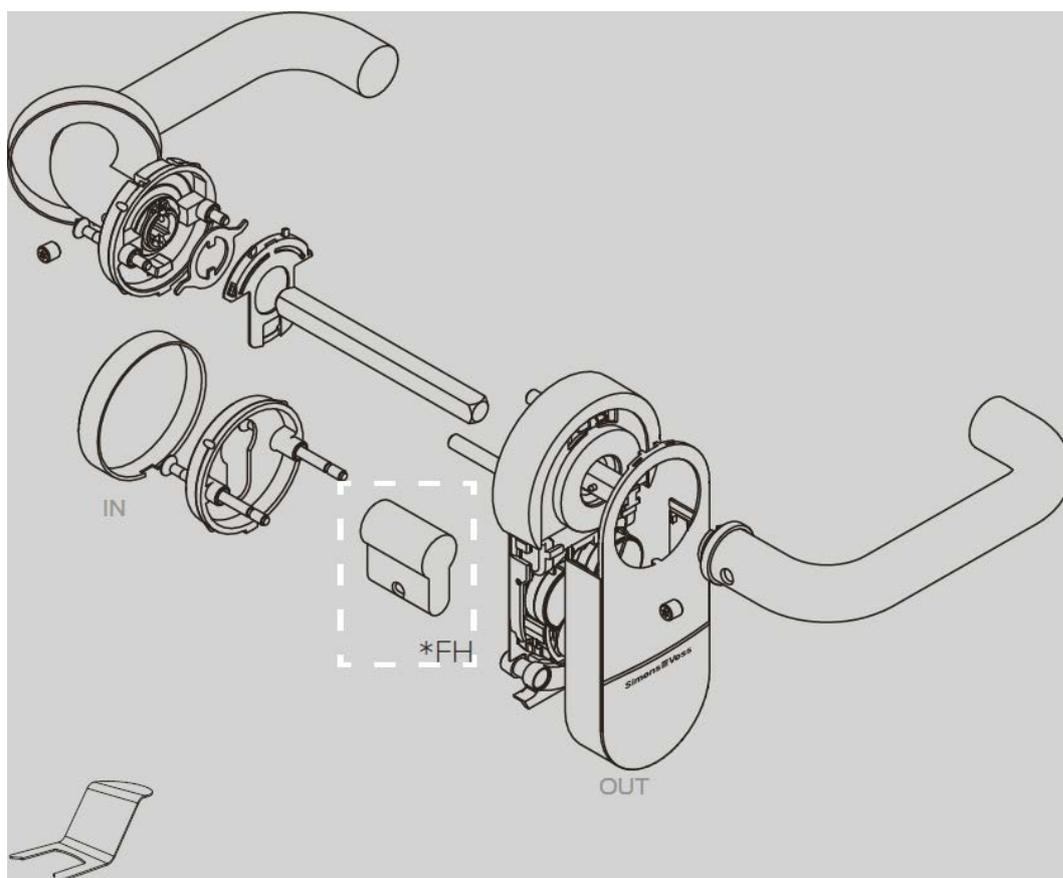
Please refer to the manual of SI.SmartHandle AX for more information.

8.7.1 Structure

SmartHandle AX contains all the electronics on the outside:

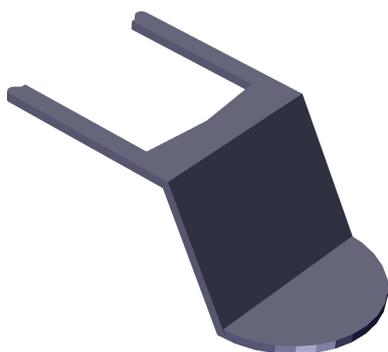
- Control Unit (CU)
- Card Reader (CR)
- Batteries

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



8.7.2 Tool

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



8.7.3 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).



8.7.4 Technical specifications

Types	<ul style="list-style-type: none"> ❑ Euro Profile cylinder ❑ Scandinavian Oval ❑ Swiss Round
Read systems	<ul style="list-style-type: none"> ❑ Passive ❑ BLE ready
Supported cards (Wireless Online WO)	<ul style="list-style-type: none"> ❑ 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)	<ul style="list-style-type: none"> ❑ MIFARE® Classic ❑ MIFARE DESFire® EV1/EV2
Reading ranges	Near field
Power supply	
Battery type	4× CR2450 (3 V)

Battery manufacturer	<ul style="list-style-type: none"> ■ Murata ■ Varta ■ Panasonic
Battery life (Wireless Online WO)	<ul style="list-style-type: none"> ■ Up to 180,000 activations ■ Up to 9 years stand-by without operation
Battery life (SmartIntego Virtual Card Network SVCN)	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Acoustic (beeper) ■ Optical (two-colour LED)
Administration and settings	
Networking capability	<ul style="list-style-type: none"> ■ 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

There are no geographical restrictions within the EU.

8.7.4.1 Mechanical system

Dimensions

The dimensions refer to the side with the electronic fitting.

Height	<ul style="list-style-type: none"> ■ A0 (standing) ■ A3 (tubular frame) ■ DS (reader on both sides) 	120 mm
	A1 (suspended, short)	140 mm
	<ul style="list-style-type: none"> ■ A2 (suspended, long) ■ E0/E1 (Scandinavian Oval) 	174 mm
	A4 (panic bar)	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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)	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Traffic white (RAL 9016) ■ Dark grey (RAL 7021) ■ Brass Also see Surface finishes for cover colours
	Escutcheon	<ul style="list-style-type: none"> ■ Brushed nickel, coated ■ Brushed brass, coated
	Handle	<ul style="list-style-type: none"> ■ Brushed stainless steel, painted ■ Brushed brass, coated

Dimensional drawings SmartHandle AX



NOTE

Height depends on the variant (see table).

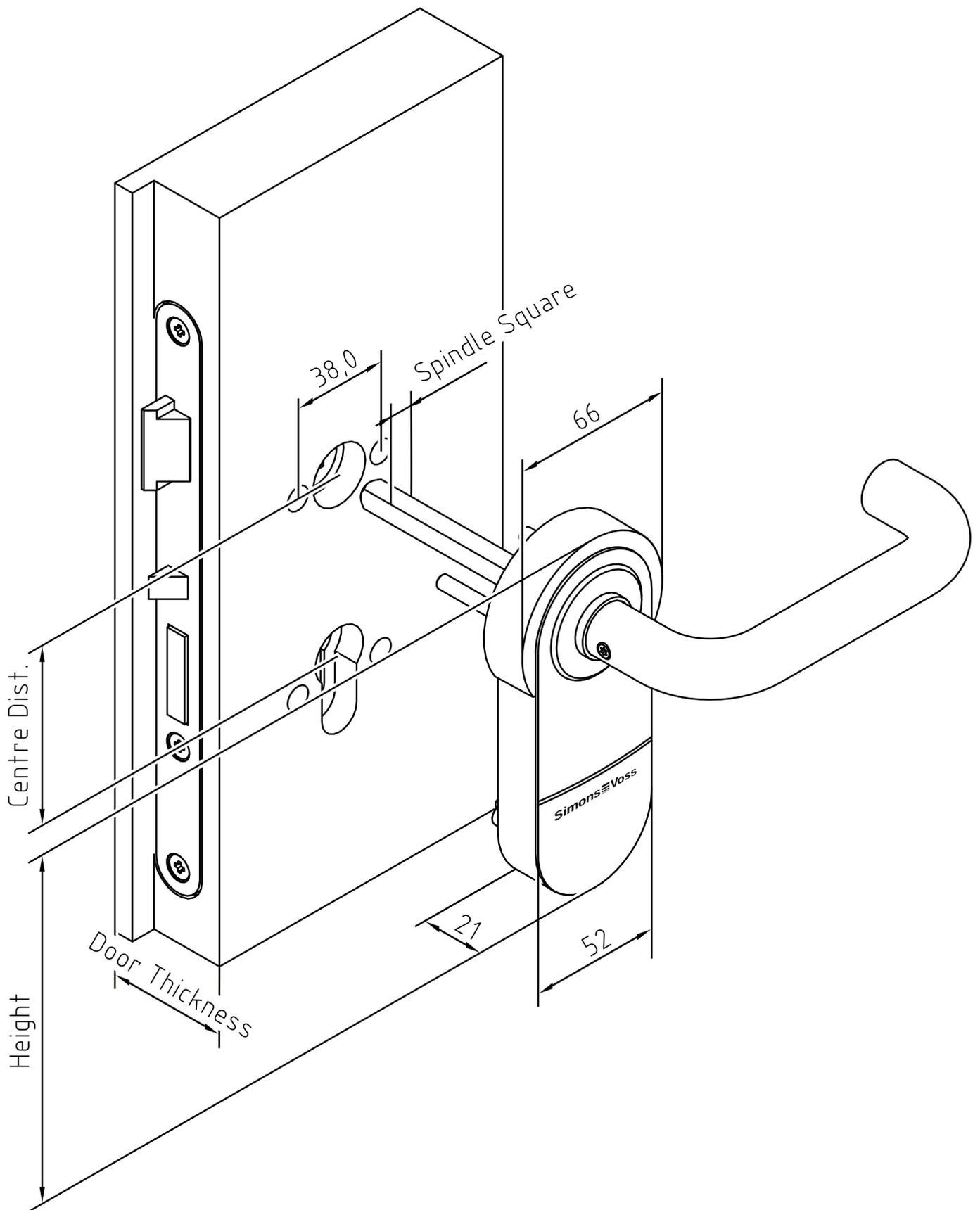


Fig. 1: Dimensioning SmartHandle AX suspended (A1, A2)

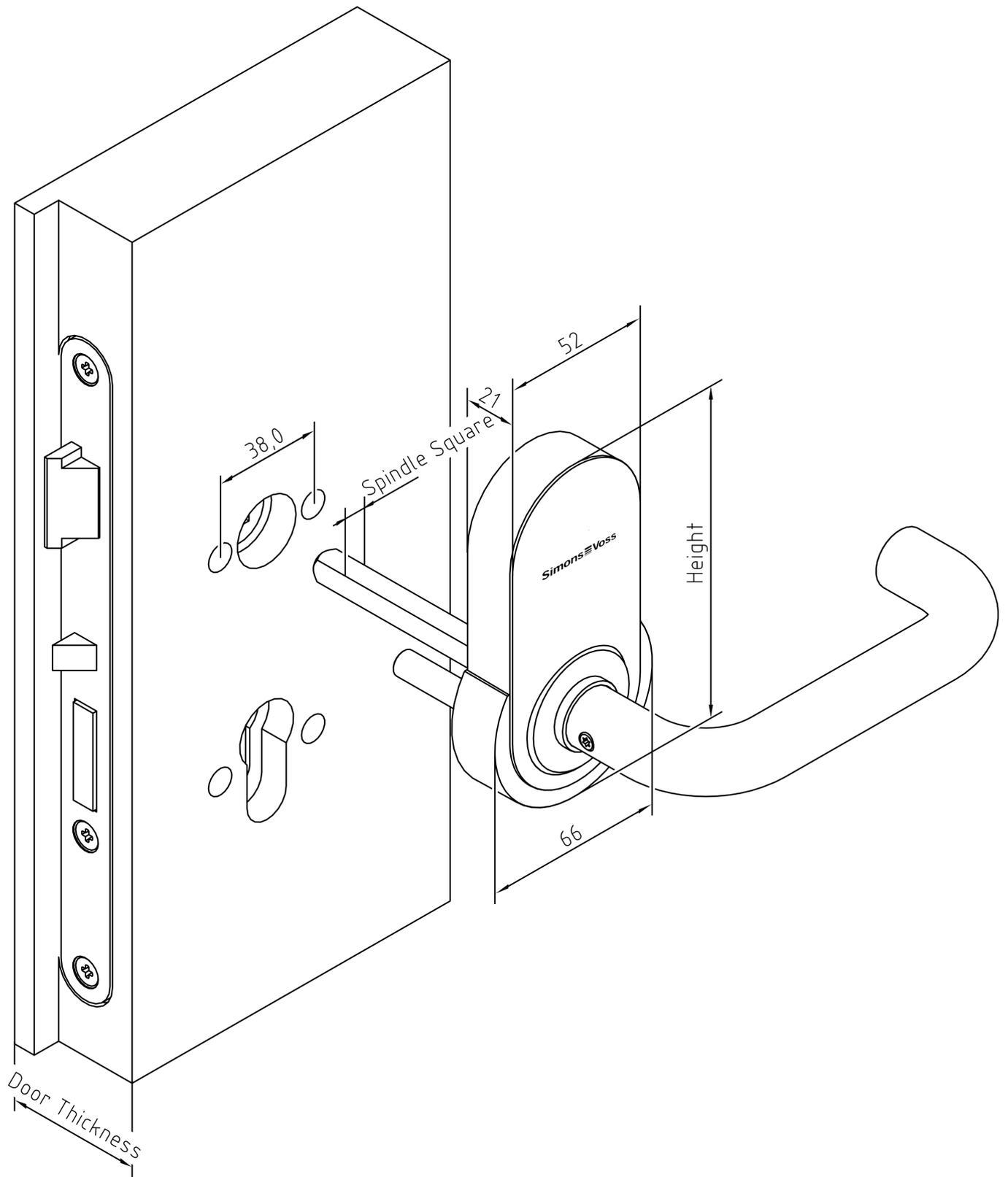


Fig. 2: Dimensioning SmartHandle AX stationary (A0)

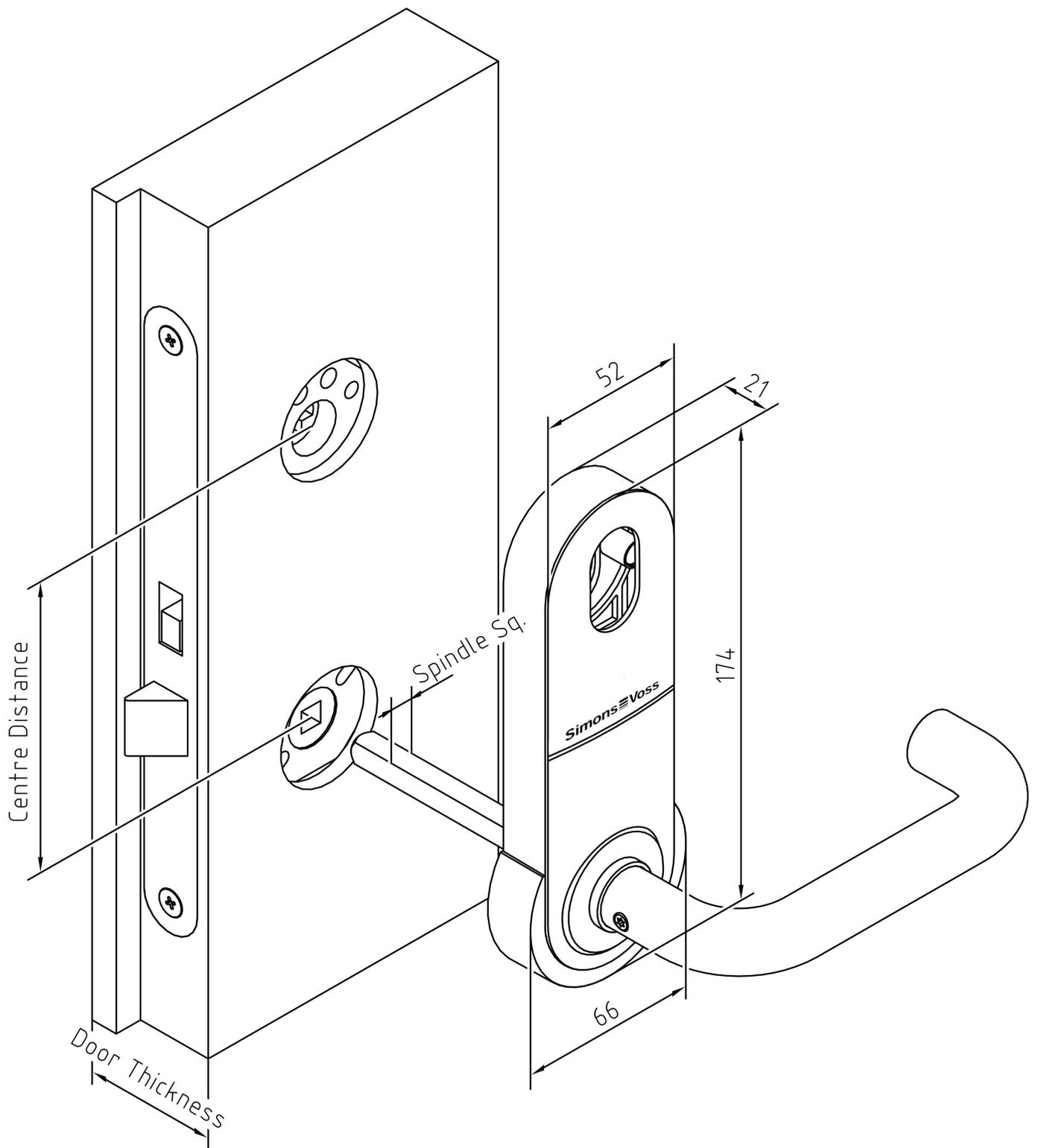


Fig. 3: Dimensioning SmartHandle AX Scandinavian Oval (E0, E1)

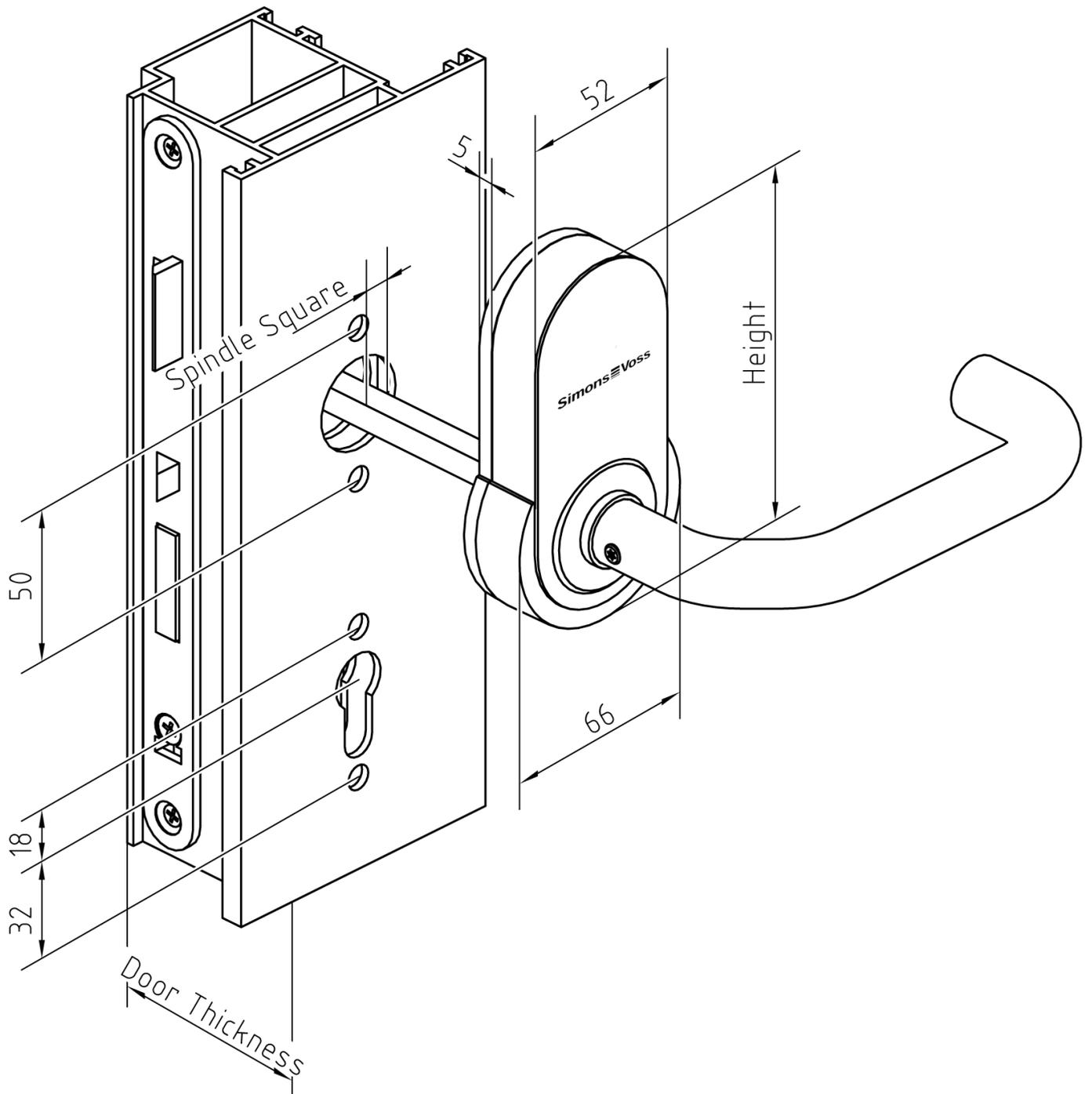


Fig. 4: Dimensioning SmartHandle AX metal frame (A3)

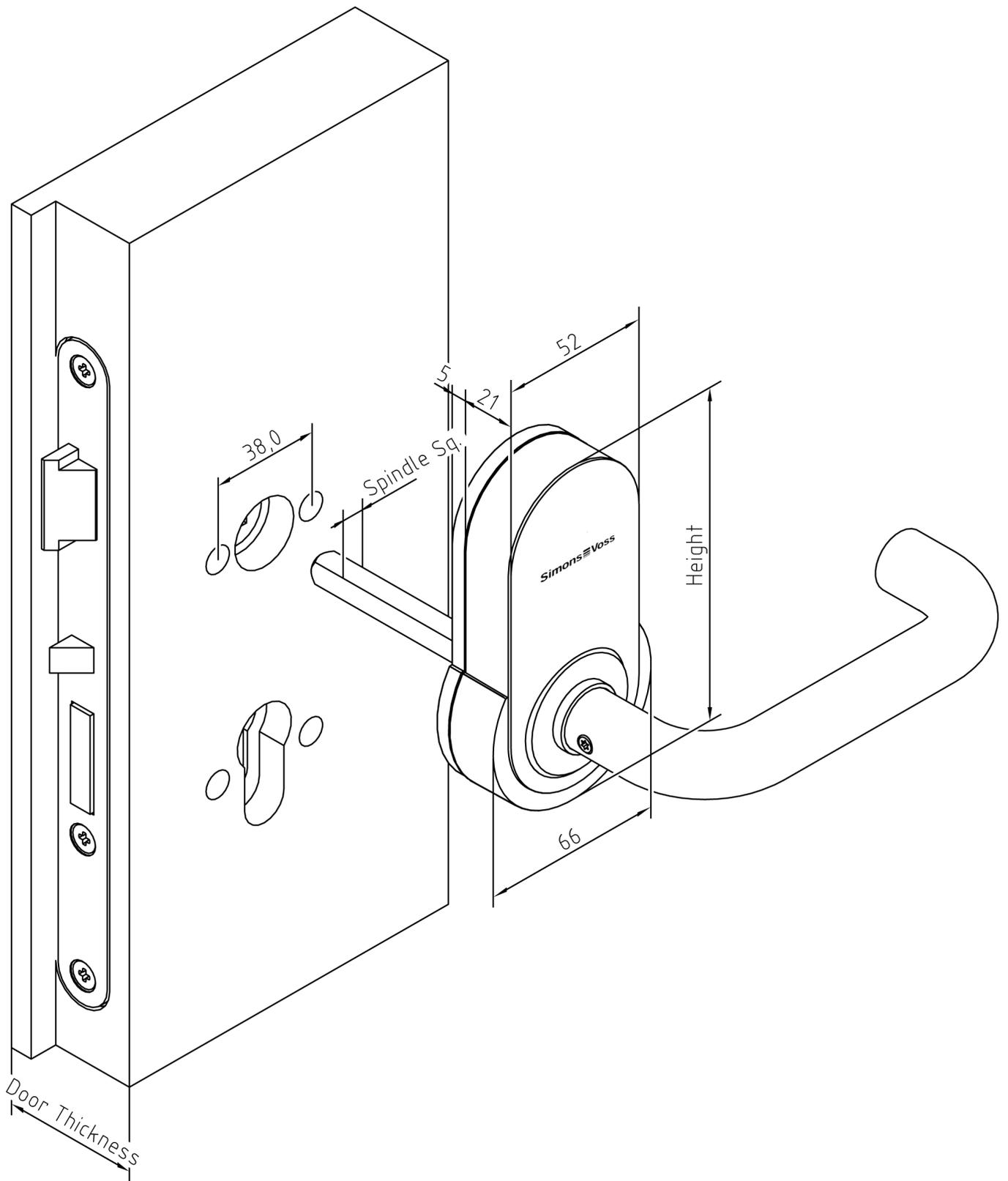
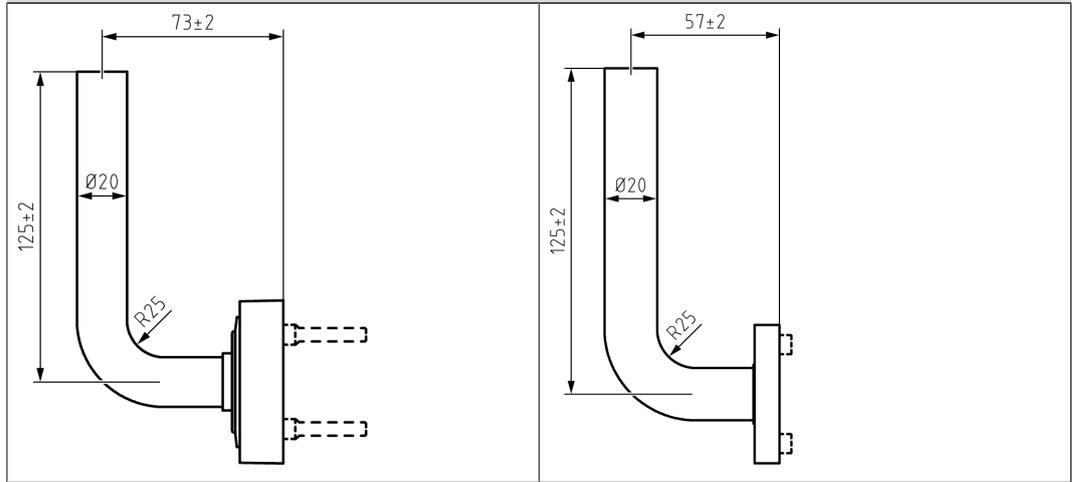


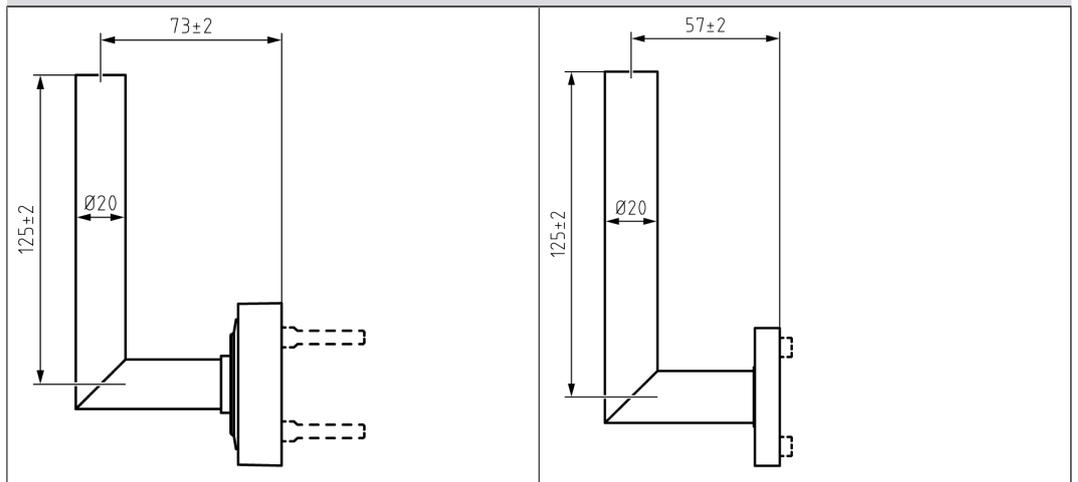
Fig. 5: Dimensioning SmartHandle AX BSL (DS)

Dimensional drawings handles

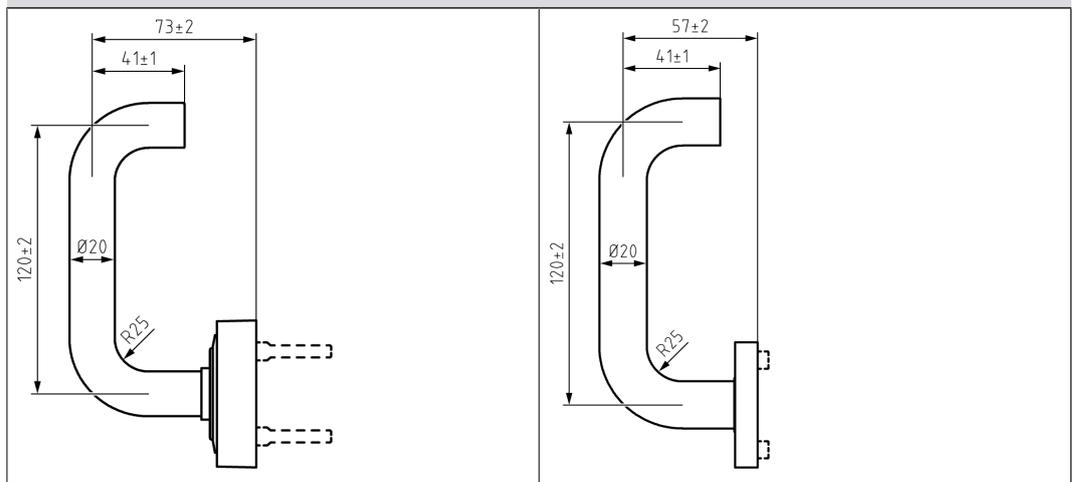
Shape A (Outside/Inside)

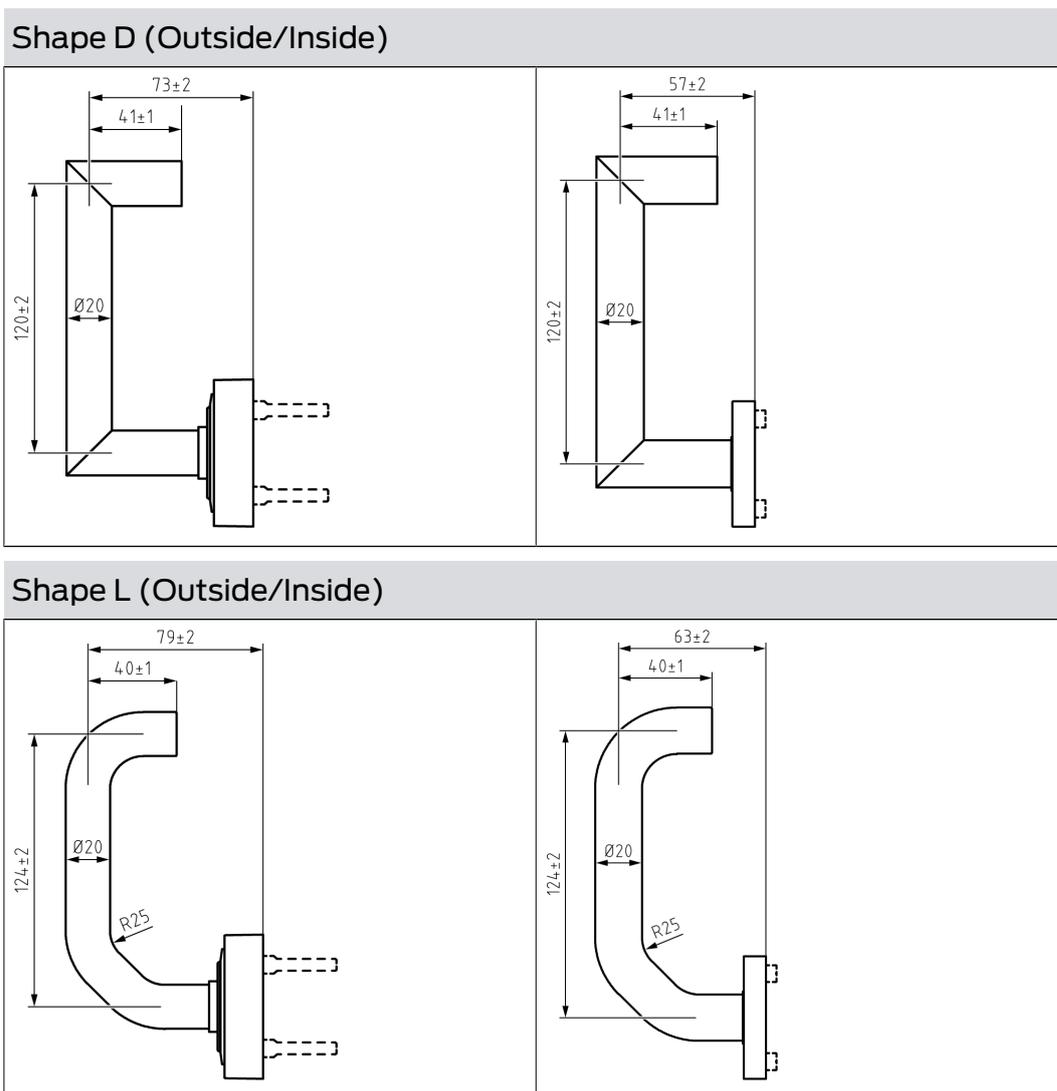


Shape B (Outside/Inside)



Shape C (Outside/Inside)





8.8 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.

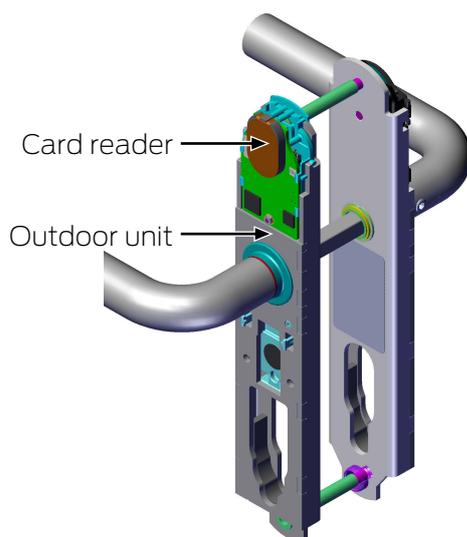
8.8.1 Structure

SmartHandle 3062 always consists of two sides:

Master (inner side)	Slave (outside)
<ul style="list-style-type: none"> ■ Central Unit (= CU) ■ Batteries 	<ul style="list-style-type: none"> ■ Card Reader (CR)

Master (inner side)	Slave (outside)
<ul style="list-style-type: none"> ❑ Always inside the door ❑ Permanently engaged 	<ul style="list-style-type: none"> ❑ Always on the outside of the door ❑ Can only be engaged with identification medium

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



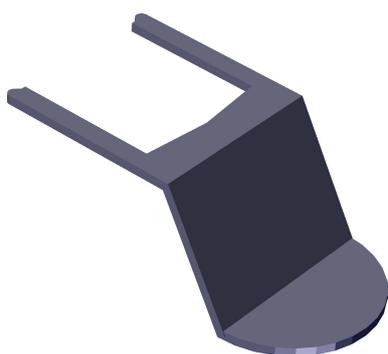
The body differs depending on the variant and equipment:

Escape&Return (.ER)

Master (inner side)	Slave (outside)
<ul style="list-style-type: none"> ❑ Central Unit (= CU) ❑ Batteries ❑ Sensors for Escape&Return 	<ul style="list-style-type: none"> ❑ Card Reader (CR)
<ul style="list-style-type: none"> ❑ Always inside the door ❑ Permanently engaged 	<ul style="list-style-type: none"> ❑ Always on the outside of the door ❑ Can only be engaged with identification medium

8.8.2 Tool

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



8.8.3 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	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ MIFARE Classic ■ MIFARE DESFire EV1 ■ UID according to 14443 from MIFARE, LEGIC advant and HID iCLASS
Virtual (VN Offline): Card technology	<ul style="list-style-type: none"> ■ MIFARE Classic ■ MIFARE DESFire EV1
Feedback signals:	Buzzer + LED (blue/red)

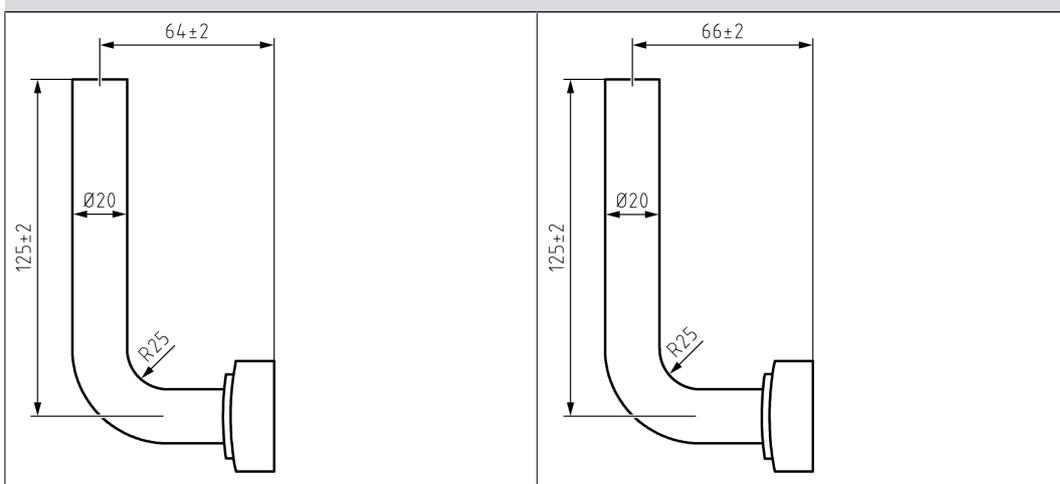
Directly networkable (only with SmartIntego Wireless Online)	Integrated LockNode
--	---------------------

Radio emissions

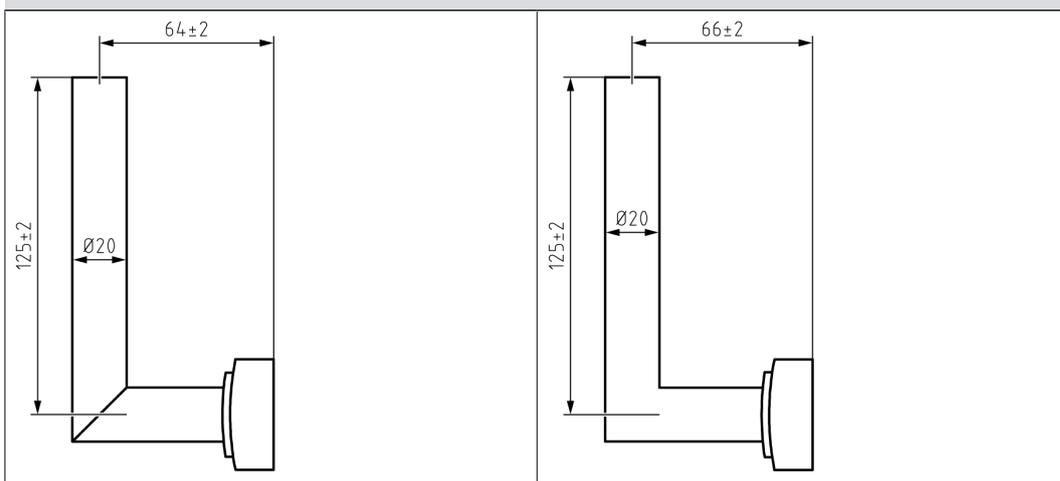
There are no geographical restrictions within the EU.

8.8.3.1 Dimensional drawings handles

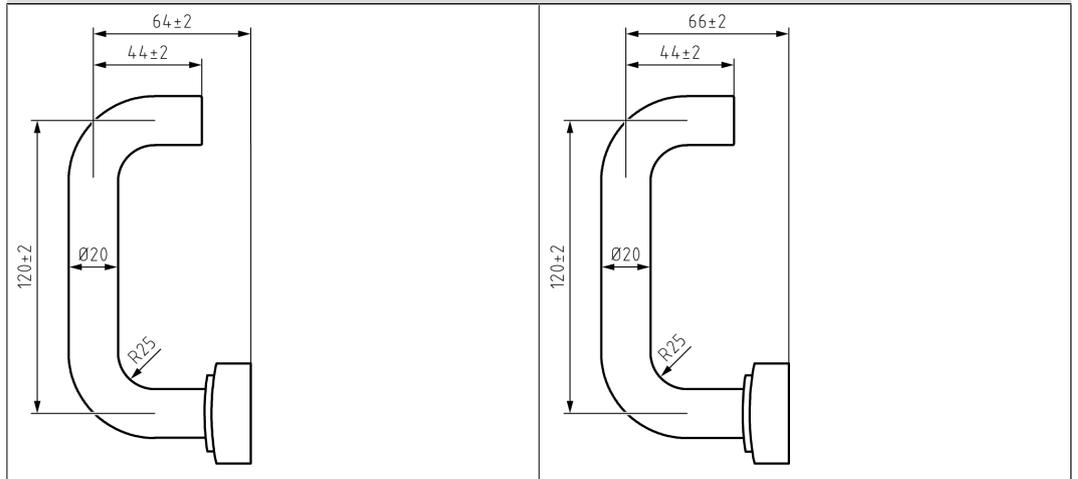
Shape A (Outside/Inside)



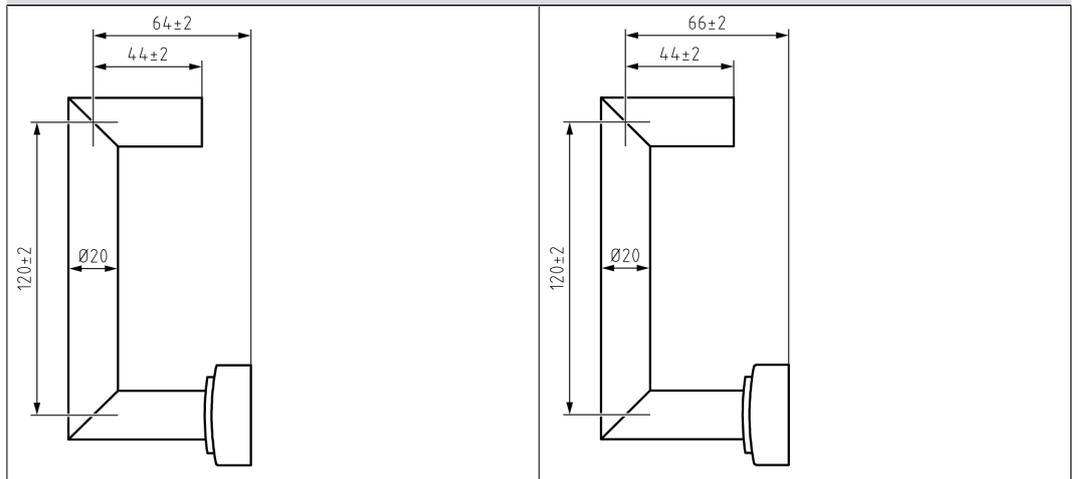
Shape B (Outside/Inside)



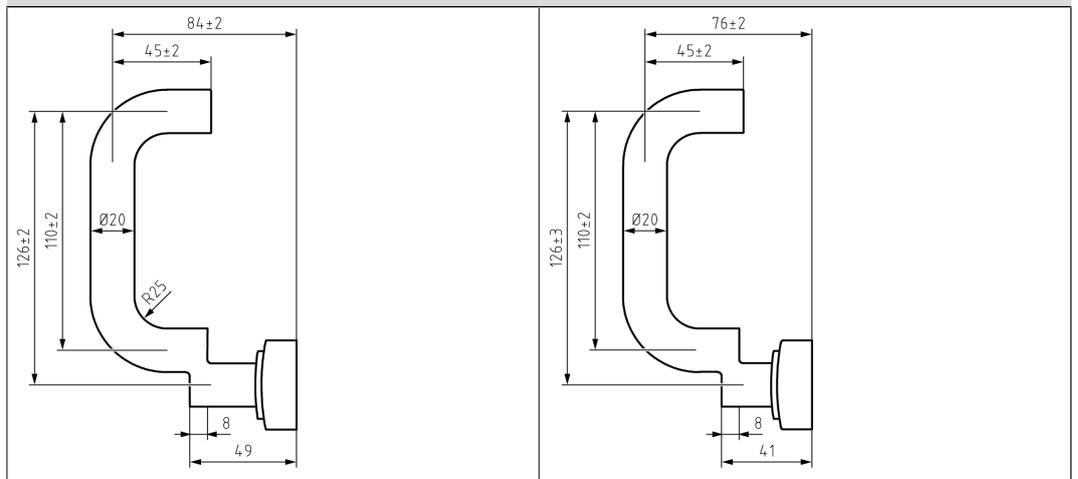
Shape C (Outside/Inside)



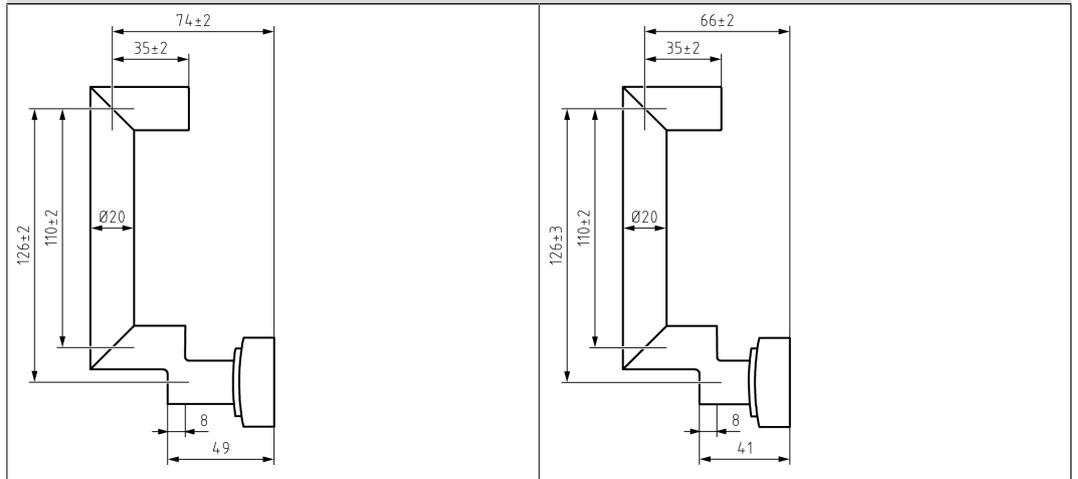
Shape D (Outside/Inside)



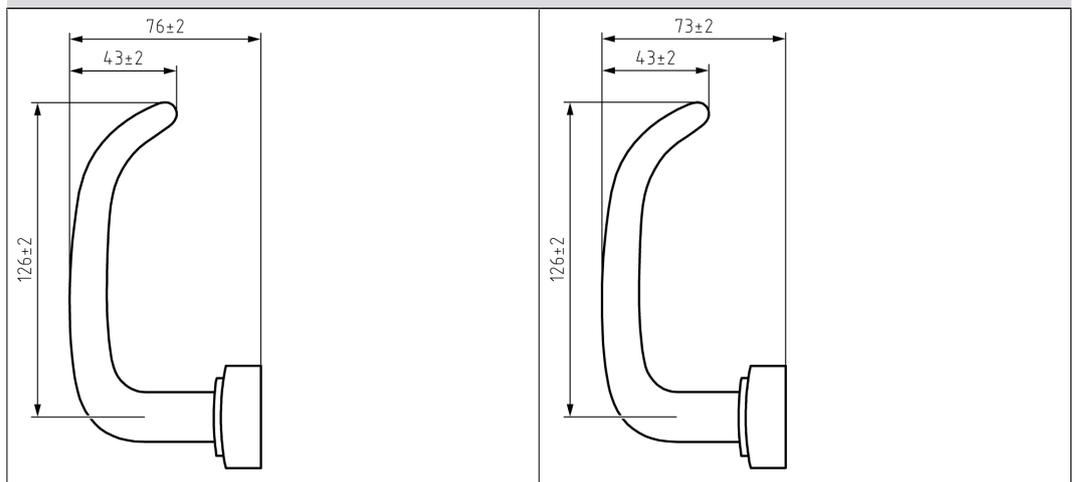
Shape E (Outside/Inside)



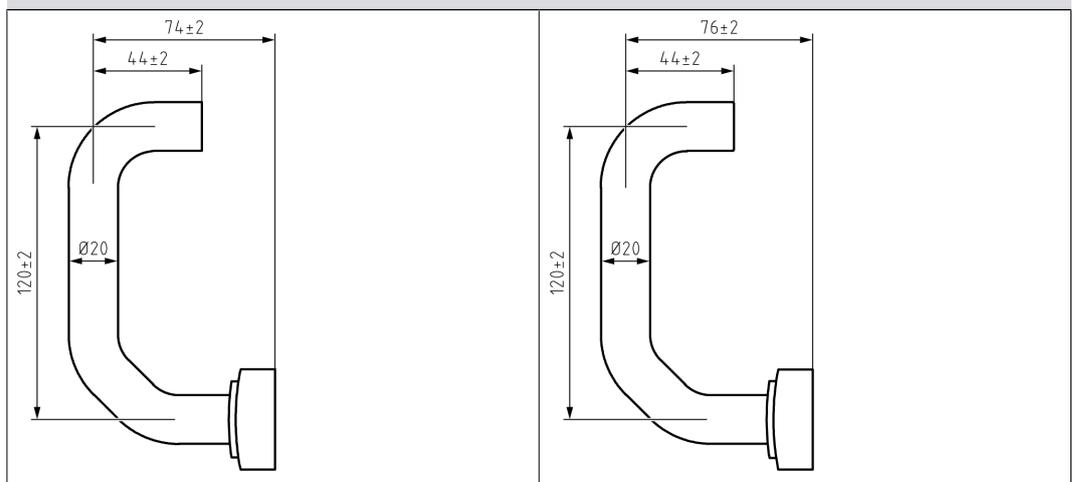
Shape F (Outside/Inside)



Shape G (Outside/Inside)



Shape H (Outside/Inside)



8.9 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.

8.9.1 Technical specifications

Padlock with shackle 8 mm in diameter	
Locking device dimensions (W x H x D)	51 x 70 x 25 mm (<i>without cylinder knob or shackle</i>)
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 (<i>without cylinder knob or shackle</i>)
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 (<i>Murata, VARTA, Panasonic</i>)
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)

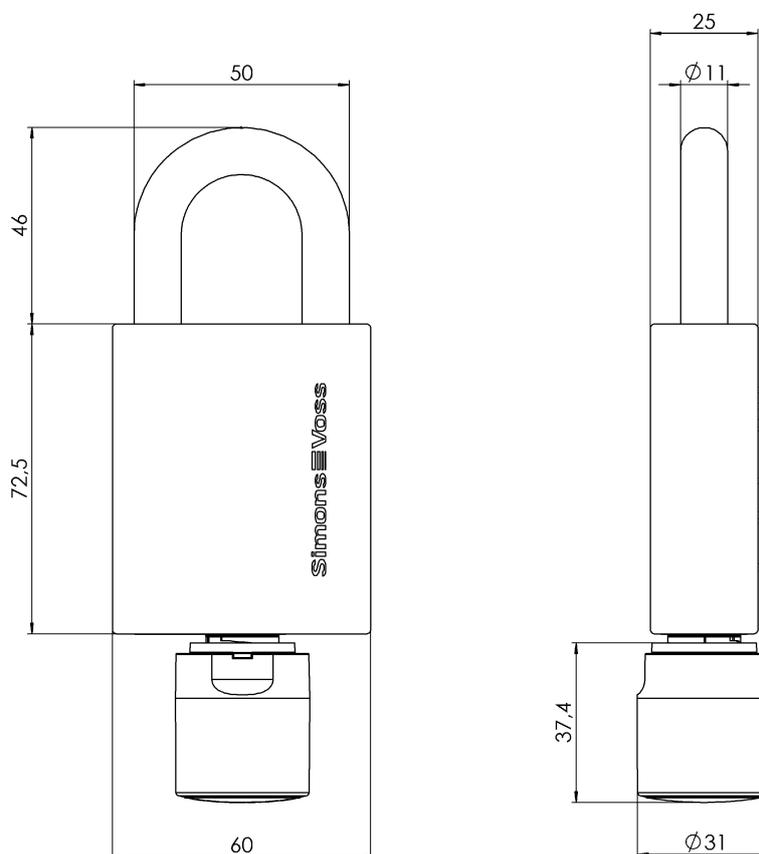
Number of media which can be managed per padlock	Transponders: up to 64,000 (G2) Smart cards (G2): up to 32,000 (depending on the configuration / template selected)
Networking capability	Directly network-ready with integrated LockNode; LockNode can be retrofit
Other information	Version with access control, 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

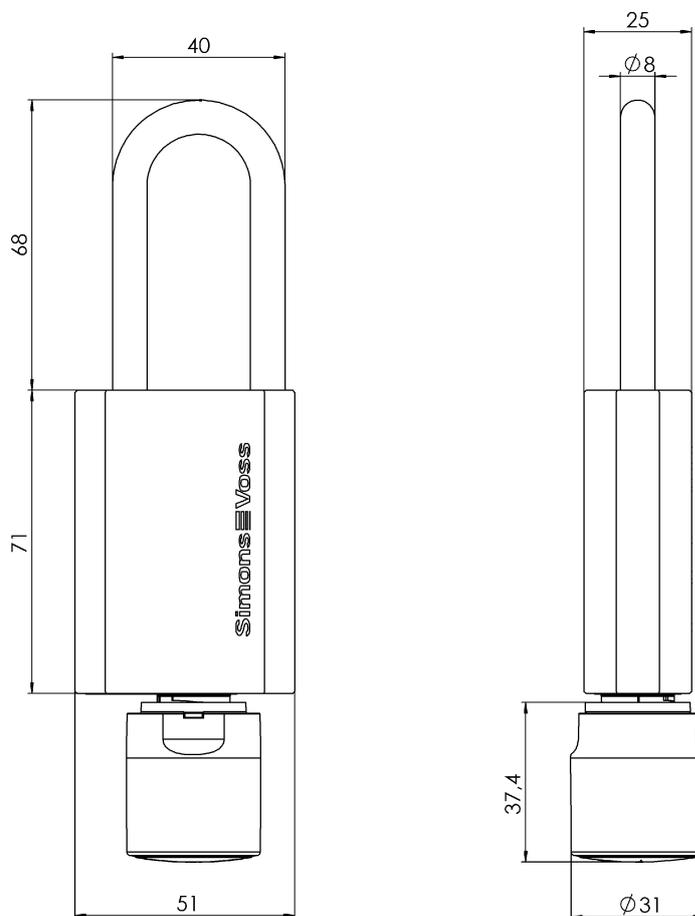
There are no geographical restrictions within the EU.

8.9.1.1 Dimensional drawings padlocks

Padlock 11 mm - Passive (PL MP)



Padlock 8 mm - Passive (PL MP)



8.10 SmartLocker AX

The SI SmartLocker AX is a locker lock that can be installed without any drilling.

The user holds the card in front to the lock and the dead bolt moves to the open or closed position.

SmartLocker AX does not allow the user to freely choose a locker.

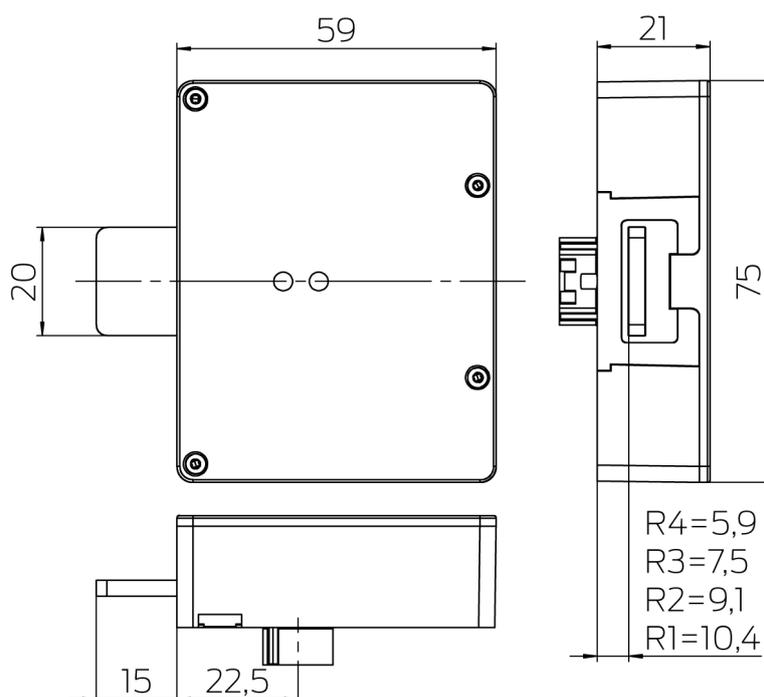
See the SI SmartLocker AX manual for more details on SI SmartLocker AX.

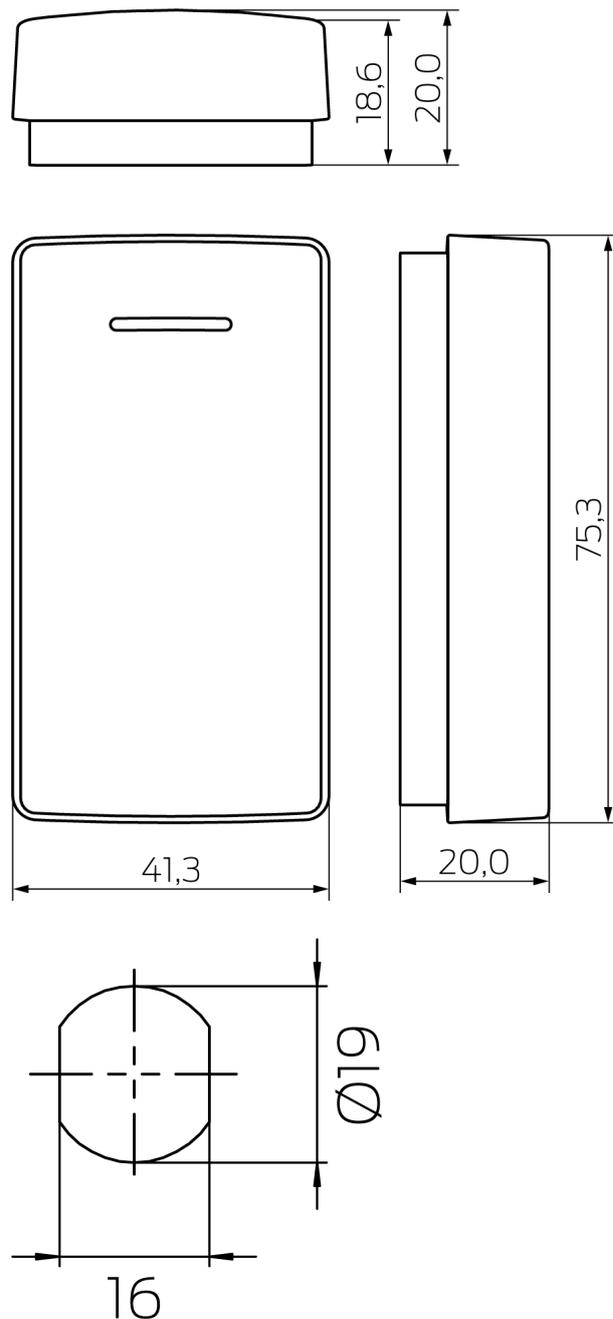
8.10.1 Technical specifications

Dimensions (WxHxD)	Reader: 41.3×75.3×20.0 mm, motor block: 59×75×21 mm, bolt: 15×20×3 mm
Fastening	Standard locker lock flange (Ø19×16 mm) with double D punch
Material	Glass-fibre reinforced plastic
Colours	Anthracite

Weather protection	IP40
Temperature range (operation)	0 °C to +65 °C
Battery type	2x AA cell 1.5 V (alkaline)
Battery lifetime (SI)	SVCN: Up to 50,000 openings or 40 years standby (limited by the life of the battery itself).
Signalisation	- Audible signal (buzzer) and/or visual signal (LED – green/red)
Network capability	Yes (integrated LockNode can be ordered and retrofitted)
Frequency range; max. transmission power RFID (~13,56 MHz)	13.560060 MHz - 13.560719 MHz; -14 dBµA/m (10 m distance)
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	2360 MHz - 2500 MHz; 4 mW
Geographical restrictions within the EU	No

8.10.1.1 Dimensional drawings





To assess compatibility, please note the following information:

Wooden doors

- The door must be between 10 mm and 25 mm thick.
With metal spindles, at least two adapter plates must therefore be used for standard material thicknesses (1 mm to 2 mm).
- Depending on the bolt block, the bolt has a clearance of 5.9 mm to 10.4 mm from the claw of the engine block. If necessary, you must attach adapter plates to the door frame so that the bolt rests on the door frame without play and the door does not fold.

Metal doors

- The door panel and adapter plates must be between 10 mm and 25 mm thick altogether.

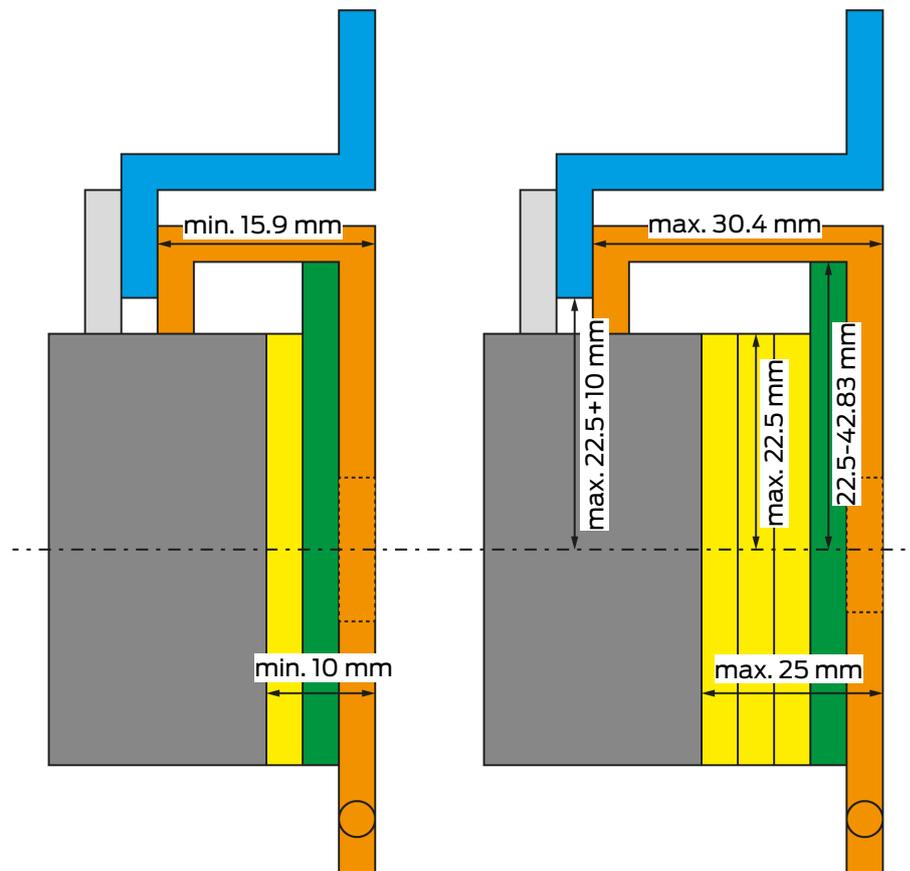
With metal spindles, at least two adapter plates must therefore be used for standard material thicknesses (1 mm to 2 mm). However, due to the rebate in the door or frame, the use of adapter plates is usually required anyway.

- The deadbolt stop of the frame may not be more than 30.4 mm from the inside of the door when closed.
- The distance between the outside of the door and the inside of the bolt must not exceed 35.4 mm. This means that the maximum height of the rebate for metal doors is 10.4 mm (A).

8.10.1.2 Drawings of installation situations

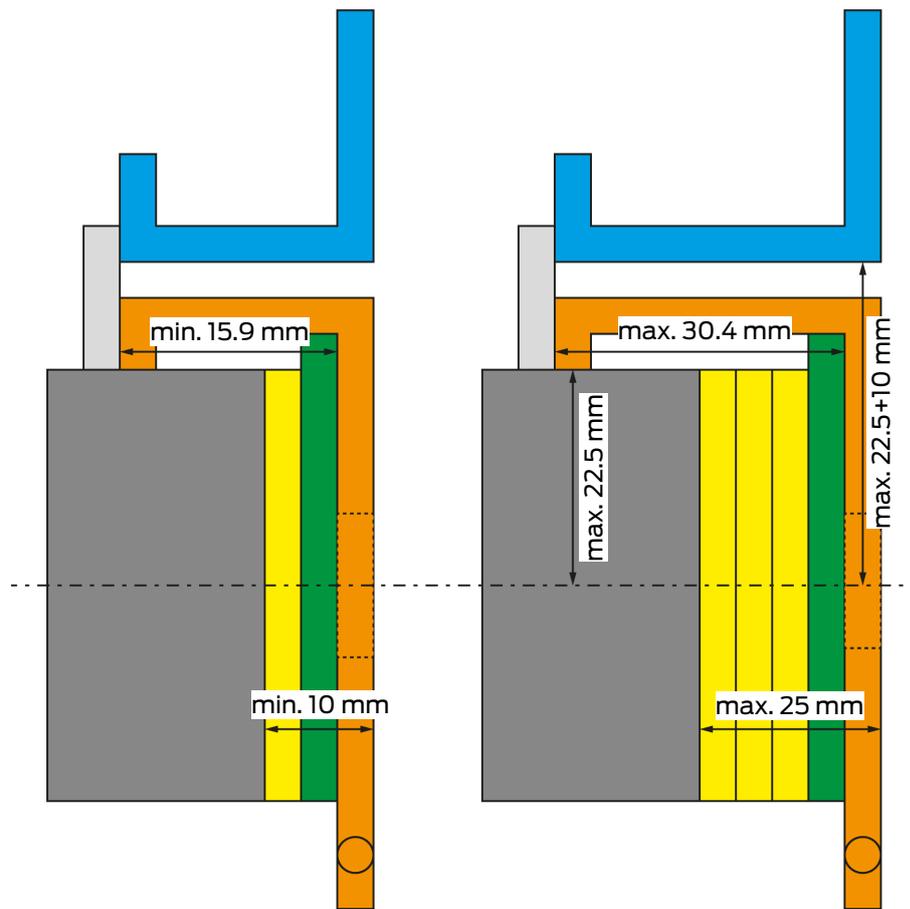
Lockers and cupboards are available in many different designs. Compare your locker or cupboard with the drawings below to assess your personal installation situation.

Metal locker 1



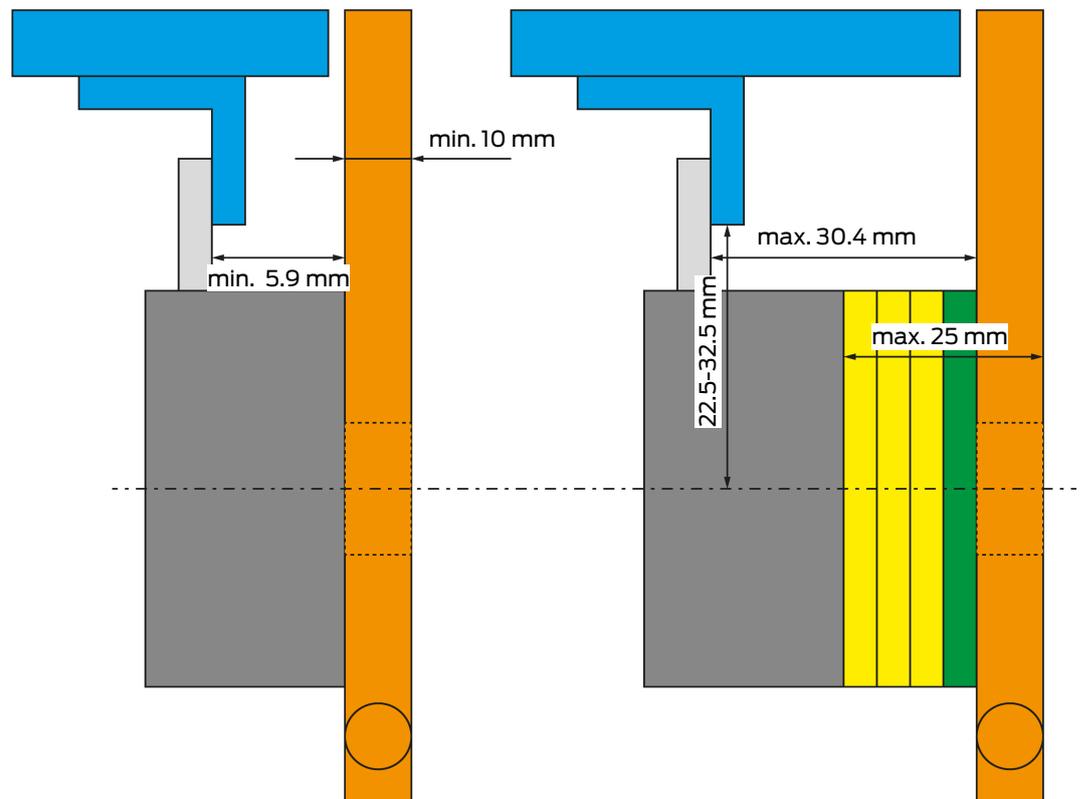
- Locker frame
- Bolt
- Motor block
- Door with hole and hinge
- Adapter plate 5 mm (variable)
- Adapter plate 5mm

Metal locker 2



- Locker frame
- Bolt
- Motor block
- Door with hole and hinge
- Adapter plate 5 mm (variable)
- Adapter plate 5mm

Wooden locker



- Door frame with stop bracket
- Bolt
- Motor block
- Door with hole and hinge
- Adapter plate 5 mm (variable)
- Adapter plate 5 mm

8.11 Batteries

All SmartIntego components are battery-powered:

- Locking cylinder
- Digital padlocks
- SmartHandles (AX and 3062)

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.

For information on battery level measurement and battery warnings, see *Battery management* [▶ 27].

8.11.1 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.
- ↳ New battery status saved in locking device.

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

Recommended manufacturers

SimonsVoss only uses batteries from brand manufacturers:

- Murata
- Varta
- Panasonic
- Tadiran

Battery types

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

9 Infrastructure

9.1 Update

The updater is a component connected to your integrator system, for example:

- Update terminal
- Punch/shoe
- Electric strike

It reads and describes cards and thus connects the virtual network to your integrator system.

9.2 Programming Device (SI.SmartCD)



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

- Programming of locking devices
- Reading access lists
- Resetting locking devices
- Emergency opening

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.



9.3 Software

These programs are required to set up a SmartIntego Virtual Card Network:

- SmartIntego Tool (SVCN)
 - Securing the system
 - Programme locking device
- Integrator system (example: SmartIntego Config Tool)
 - Managing doors
 - Manage SVCN functions

Additional helpful features:

- Firmware update tool
 - Updating locking device firmware

9.3.1 SmartIntego Tool (SVCN)

The SmartIntego tool (SVCN) configures locking components with the general SmartIntego Virtual Card Network functions, including:

- Security and encryption (different password levels)
- Card configuration (s) used in the system
- Required locking device configuration

9.3.1.1 Project file

The SmartIntego tool (SVCN) contains all security- and encryption-relevant information to secure the system:

- Project Password
- Card configuration password
- Locking system password
- Card configuration

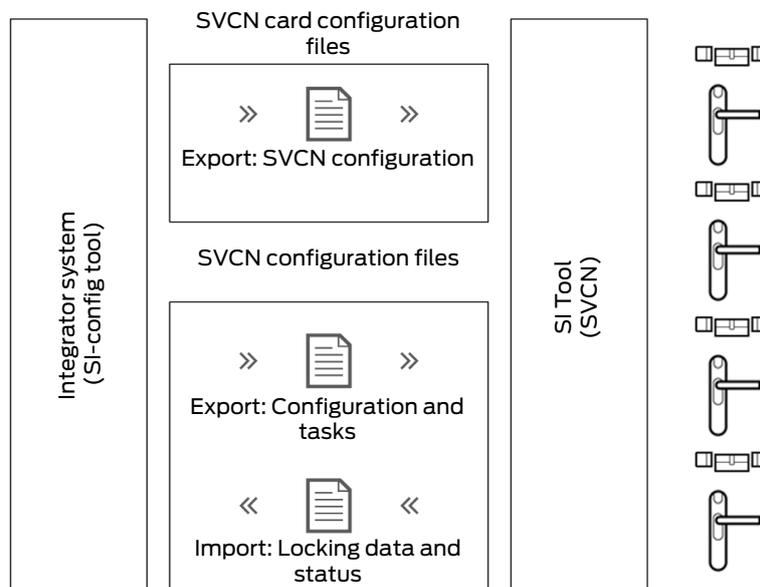
This information is stored in the encrypted project file (*.ikp).

9.3.1.2 Data transfer

The SmartIntego tool (SVCN) receives all information on the locking devices and their status:

- From integrator system (XML file): Required locking device configuration
- From locking devices (SI.SmartCD): Actual status of locking devices

The SmartIntego tool (SVCN) communicates between the SmartIntego components and the integrator system.



The SmartIntego tool (SVCN) itself cannot programme locking devices. This always requires a valid XML file from the integrator system.

9.3.1.3 Programming of locking devices

The locking devices must be programmed before installation. The SmartIntego tool (SVCN) programs the functions into the locking devices together with the SI.SmartCD.



This initial programming does not necessarily have to be carried out at the installation site. Instead, the locking devices can be programmed together in a location with a computer on which the SmartIntego tool (SVCN) is installed and the SI.SmartCD.

If the configuration is changed, the new information must be programmed into the locking device using the SI.SmartCD and the SmartIntego tool (SVCN). Such changes include, for example:

- Change to card configuration
- Change of group assignment

The SI.SmartCD is also required during annual maintenance to adjust the time in the locking devices.

9.3.1.4 Backup

Regular backups reduce the workload if the project file is lost, damaged or otherwise unusable.

The backup of the SmartIntego system is a copy of the project file (*.ikp). This file contains relevant hardware configuration data, e.g:

- Passwords
- Card configurations
- Locking device information from the last XML import
- Lock information from the last readout of the locking device

It is protected with the project password.

Alternatively, the backup can be carried out with the integrator system's import/export function. Please refer to the documentation of your integrator system for details.



NOTE

Restoring old versions

The hardware configuration in old backup files may differ from the current hardware configuration.

1. You still need the project password to recover/edit the project file.
2. If necessary, correct existing differences manually.

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.

9.3.2 Integrator system (SmartIntego Config Tool)

The integrator system manages in the virtual network:

- Doors/locking devices
- Persons/cards
- Authorisations
- Data

The SmartIntego Config Tool is automatically installed together with the SmartIntego tool (SVCN). Locking device configurations can thus be created and edited for demonstration purposes. For the realisation of an integration project, only use your integrator's integration system.

Together with the SmartIntego tool (SVCN), the integrator system can:

- Configuring locking devices
- Creating tasks for the SmartIntego tool (SVCN) (XML export)
- Status of locking devices

The Integrator System and SmartIntego Tool (SVCN) share information using XML files. There are two XML files:

- Configuration file for the cards in SVCN
- Configuration file for locking devices in SVCN

Card configuration

The configuration file for the cards contains the entire card configuration. The integrator system sends this file to the SmartIntego tool (SVCN).

SmartIntego Tool (SVCN): | File | - [Import](#) - [VCN Configuration](#)

Locking device configuration

The configuration file for the locking devices contains:

- Locking device configurations
- SmartIntego Tool (SVCN) Integrator System Tasks

The integrator system sends this file to the SmartIntego tool (SVCN) and receives the following response:

- Locking plan information
- Task Execution Results
- Access list of locking devices

Tasks

The files transferred to the SmartIntego tool (SVCN) only become useful together with tasks. The tasks regulate what the user may do with the locking devices, for example:

- Programme
- Reset
- Import access list
- Carry out emergency opening
- Set time

The SmartIntego tool imports these tasks together with the XML file and can then execute them.

The tasks have an expiry date and can therefore only be executed for a limited time.

The result of the task execution is saved back to the XML file. This must then be imported back into the integrator system.

10 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.

10.1 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.

10.2 Project Password

The SmartIntego tool stores global locking system data such as

- Card configuration
- Softwareconfiguration
- ...

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

10.3 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).
2. Create a new project file.
3. Set up system with new password (locking device).

- ❑ 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.

10.4 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

10.5 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.

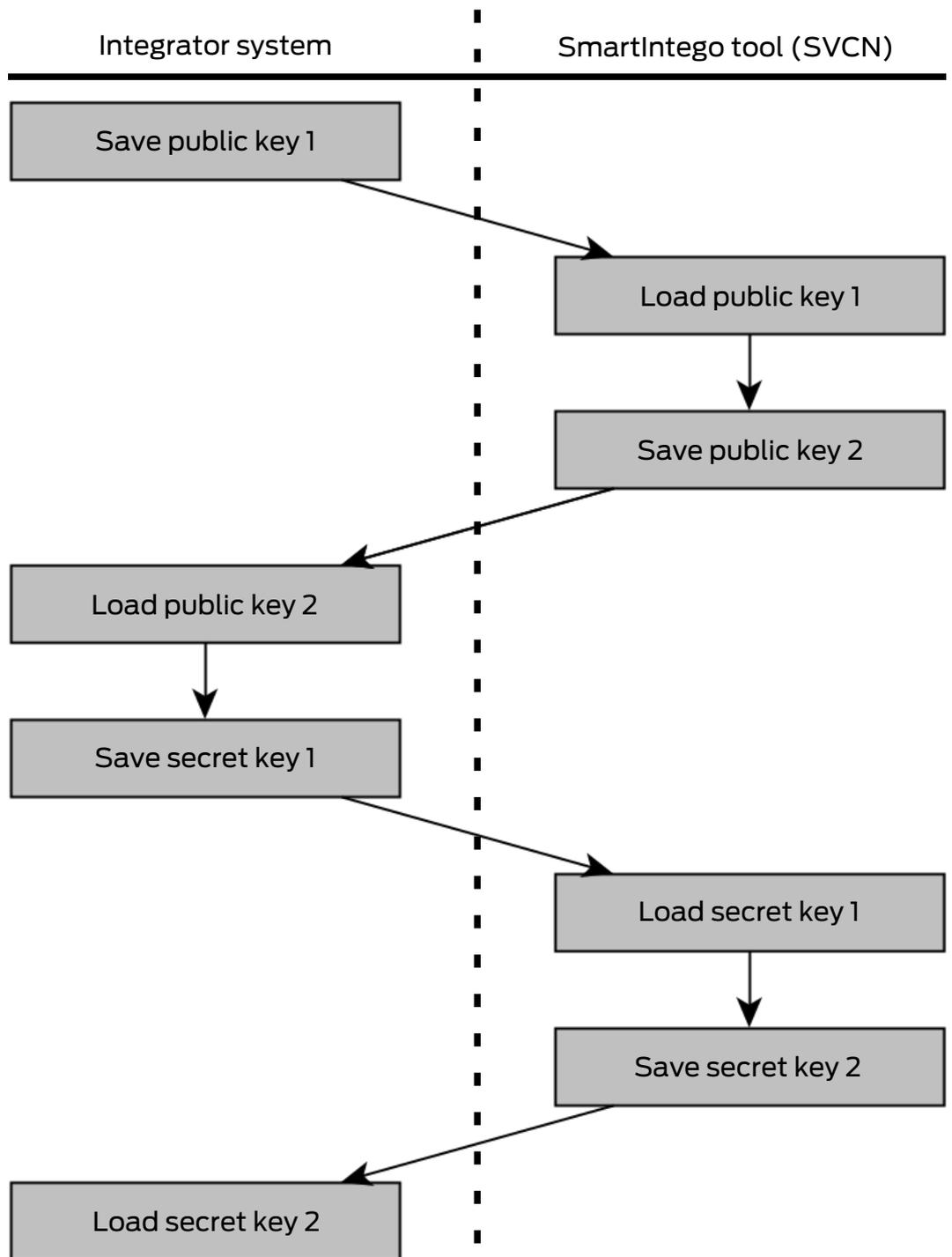
The card manufacturer or other users of the card provide the card's reading key, for example as a template file (*.ikt) or directly in plain text. For information, see the step-by-step manual.

Change/Loss

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

10.6 Encrypting the transfer between SmartIntego tool (SVCN) and integrator system

Data is transferred between the SmartIntego tool (SVCN) and the integrator system in an XML file. If the integrator system supports encryption, you can transfer the data in encrypted form.



1. In the integrator system, export the key via **Save Public Key 1**.
↳ Public key 1 exported.
2. In the SmartIntego tool (SVCN) via | Tools | select the entry **Options - Project - Load Public Key 1**.
↳ Public key 1 imported.
3. In the SmartIntego tool (SVCN) via | Tools | select the entry **Options - Project - Save Public Key 2**.
4. Define an output directory.

5. Click on the button **OK**.
 - ↳ Public key 2 exported.
6. In the integrator system, import the key via **Load Public Key 2**.
 - ↳ Public key 2 imported.
7. In the integrator system, export the key via **Save Secret Key 1**.
 - ↳ Secret key 1 exported.
8. In the SmartIntego tool (SVCN) via | Tools | select the entry **Options** - **Project** - **Load Secret Key 1**.
 - ↳ Secret key 1 imported.
9. In the SmartIntego tool (SVCN) via | Tools | select the entry **Options** - **Project** - **Save Secret Key 2**.
 - ↳ Secret key 2 exported.
10. In the integrator system import via **Load Secret Key 2**
 - ↳ Secret key 2 imported.
 - ↳ Key for encrypted communication exchanged.

11 Card Types (SVCN)

SmartIntego Virtual Card Network supports two card types:

- MIFARE Classic
- MIFARE DESFire

Only one of these card types can be used in a project, mixed operation is not possible.

The card type in your integration is selected in the SmartIntego tool. There are two ways to do this:

- Semi-automatic with an XML import: | File | - Import - VCN Configuration.
- Manual: Card Configuration
- Template file

The card type can be changed afterwards.

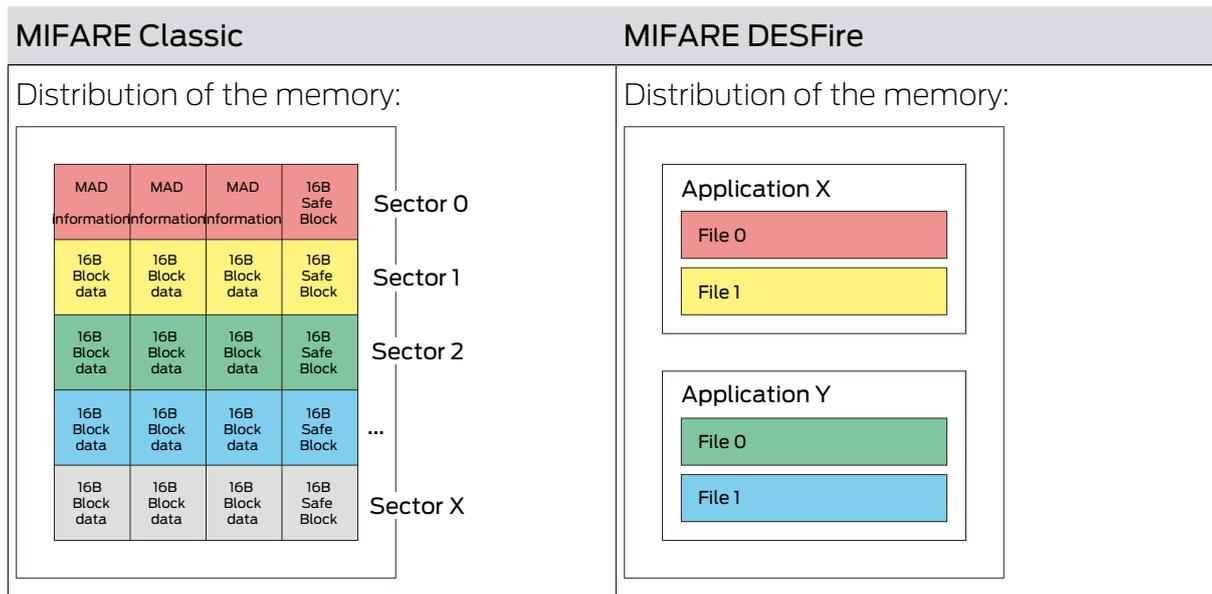


NOTE

Programming requirement not displayed

The locking devices in your project are not managed in the SmartIntego tool (SVCN). Therefore, the SmartIntego tool (SVCN) does not "know" whether programming is required after changes to the card configuration.

MIFARE Classic	MIFARE DESFire
<ul style="list-style-type: none"> ■ Data stored in sectors ■ Addressing with Mifare Application Directory (=MAD) ■ Sector protection via key in MAD ■ MIFARE Classic encryption hacked and now insecure 	<ul style="list-style-type: none"> ■ 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



11.1 MIFARE Classic

Value	Note
Application code	ID for MIFARE Application Directory (=MAD)
Function Cluster Code	Specified by integrator
Lock Key	Specified by integrator

11.2 MIFARE DESFire

Value	Note
Application ID	Application ID
ID file (File 1)	ID of the ID file (Identifies card)
Access file (File 2)	ID of the access file (authorisations)
Upstream file (File 3)	Upstream file ID (return transport to updater)
Lock Gateway Key	Key value with: <ul style="list-style-type: none"> ■ Read-only access to the ID file and the access file ■ Read and write permission for the upstream file

Value	Note
Lock Gateway Key no.	Key number of the key with: <ul style="list-style-type: none"><li data-bbox="963 389 1433 465">■ Read-only access to the ID file and the access file<li data-bbox="963 490 1426 566">■ Read and write permission for the upstream file

12 Changelog

Versions	Changes	Chapter
01.00	FIRST RELEASE	...
01.01	Preparation AX	Documents
01.02	Several preparation for AX	Documents
01.03	Bugfix AP2+FD Cylinder	Documents
	Adjustments regarding support for AX components	<i>Card loss [▶ 29]</i>
	Internal bugfixing	Documents
01.04	New chapter	<i>Cover contact [▶ 76]</i>
	Changes	<i>Card Types (SVCN) [▶ 115]</i>
	Card configurations	Documents

13 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.

© 2021, SimonsVoss Technologies GmbH, Unterföhring

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

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

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



SimonsVoss
technologies

Made in Germany