Systembeschreibung WO

Systembeschreibung

11.02.2025

SimonsVoss technologies

Inhaltsverzeichnis

1. Allgemeine Sicherheitshinweise

Signalwort: Mögliche unmittelbare Auswirkungen bei Nichtbeachtung
WARNUNG: Tod oder schwere Verletzung (möglich, aber unwahrscheinlich)
ACHTUNG: Sachschäden oder Fehlfunktionen
HINWEIS: Geringe oder keine

WARNUNG

Versperrter Zugang

Durch fehlerhaft montierte und/oder programmierte Komponenten kann der Zutritt durch eine Tür versperrt bleiben. Für Folgen eines versperrten Zutritts wie Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss Technologies GmbH nicht!

Versperrter Zugang durch Manipulation des Produkts

Wenn Sie das Produkt eigenmächtig verändern, dann können Fehlfunktionen auftreten und der Zugang durch eine Tür versperrt werden.

- Verändern Sie das Produkt nur bei Bedarf und nur in der Dokumentation beschriebenen Art und Weise.

HINWEIS

Bestimmungsgemäßer Gebrauch

SmartIntego-Produkte sind ausschließlich für das Öffnen und Schließen von Türen und vergleichbaren Gegenständen bestimmt.

- Verwenden Sie SmartIntego-Produkte nicht für andere Zwecke.

Qualifikationen erforderlich

Die Installation und Inbetriebnahme setzt Fachkenntnisse voraus.

- Nur geschultes Fachpersonal darf das Produkt installieren und in Betrieb nehmen.

Änderungen bzw. technische Weiterentwicklungen können nicht ausgeschlossen und ohne Ankündigung umgesetzt werden.

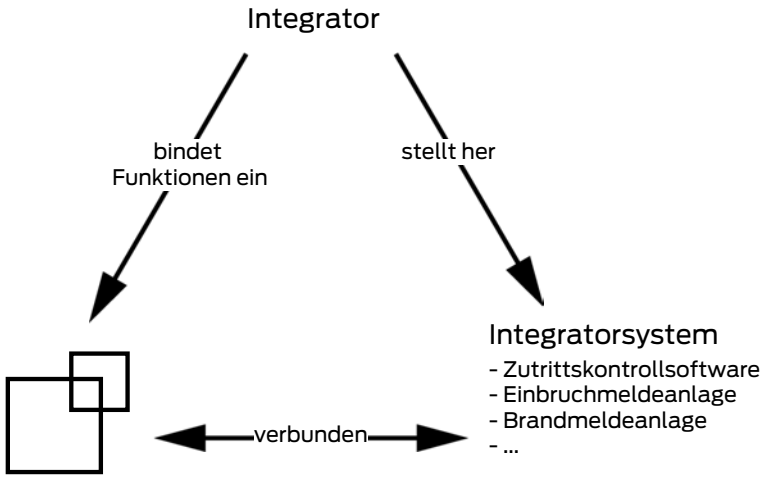
Die deutsche Sprachfassung ist die Originalbetriebsanleitung. Andere Sprachen (Abfassung in der Vertragssprache) sind Übersetzungen der Originalbetriebsanleitung.

Lesen Sie alle Anweisungen zur Installation, zum Einbau und zur Inbetriebnahme und befolgen Sie diese. Geben Sie diese Anweisungen und jegliche Anweisungen zur Wartung an den Benutzer weiter.

2. SmartIntego

SmartIntego ist eine eigenständige Produktgruppe aus dem Hause SimonsVoss. Die SmartIntego-Komponenten lassen sich durch die SimonsVoss Konfigurationssoftware einrichten und über die SmartIntego-Schnittstelle an ein Integratorsystem anbinden. Der Integrator ist in der Regel ein Hersteller einer Gebäudemanagementsoftware (Zutrittskontrollsoftware, EMEA-Lösung, Brandmeldeanlage,...), in der auch die SimonsVoss SmartIntego-Schließungen verwaltet werden. Er entwickelt die Schnittstelle an sein System eigenständig und ist auch für die angebundenen Funktionen verantwortlich. Das SmartIntego-Interface gibt es in zwei Varianten:

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



3. SmartIntego Tech-Kit

Das SmartIntego Tech-Kit hilft Ihnen bei der Inbetriebnahme und beim Betrieb Ihrer SmartIntego-Schließanlage.

Es enthält:

- Konfigurationssoftware
- Systembeschreibung
- Schritt-für-Schritt-Anleitungen
- Aktuelle Firmwareversionen
- Handbücher

Versionierung

Sie erkennen die aktuelle Version im Dateinamen (Jahreszahl-Monat, z.B. 20-01). Die neueste Version des SmartIntego-TechKits finden Sie im Partnerbeich der SmartIntego-Website (*https://www.smartintego.com/int/home/home*).

4. Konzept

SmartIntego Wireless Online (WO) ist ein vernetztes SimonsVoss-Schließsystem, das auf Karten und Batterien basiert. Es bietet folgende Funktionen:

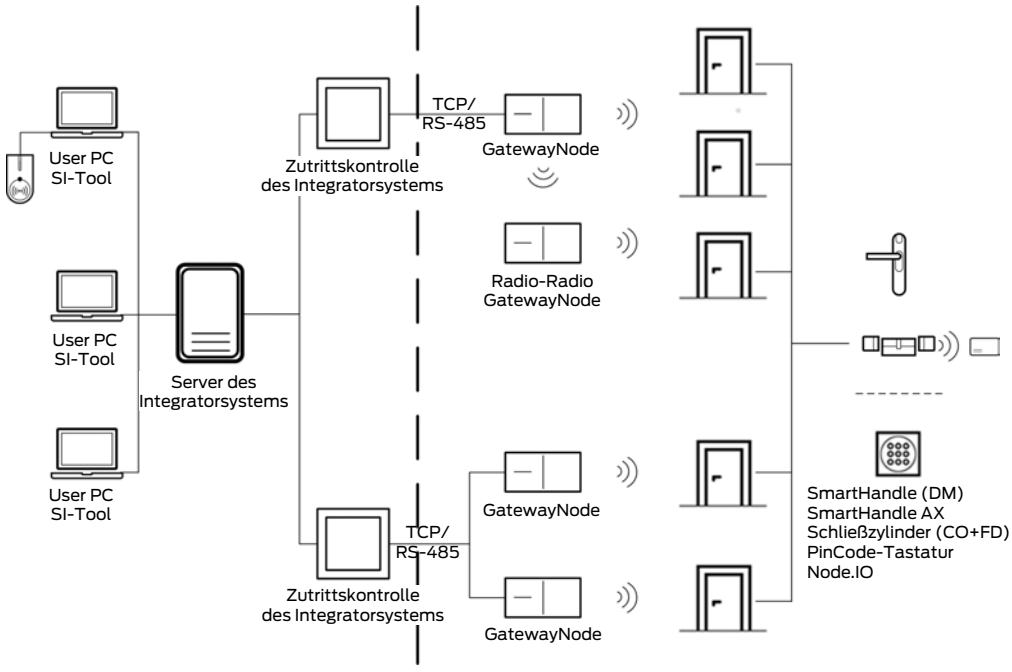
- Daten von Karten lesen (Identifikationsnummer)
- Ausgelesene Daten an Zutrittskontrolle des Integratorsystems senden (Platine, Computer, Dienst...)
- Befehl vom Zutrittskontrolle empfangen (z.B. Schließung einkuppeln)

Eine mit der Zutrittskontrolle verbundene Schließung wertet die ausgelesenen Daten nicht selbst aus. Stattdessen schickt die Schließung die Daten über einen GatewayNode an die Zutrittskontrolle des Integratorsystems. Die Zutrittskontrolle wertet die ausgelesenen Daten dann aus und reagiert darauf (zum Beispiel mit dem Befehl, die Schließung einzukuppeln).

Je nach Integrator unterscheidet sich die Basis des Integratorsystems:

- Hardwarebasis
- Softwarebasis
- Mischform

Fragen Sie Ihren Integrator, um den genauen Aufbau des Integratorsystems zu erfahren. Diese Abbildung zeigt nur den generellen Aufbau:



5. WO-Funktionen

5.1 Dokumentation

Jeder Integrator entwickelt sein Integrationssystem selbst und gibt in seiner eigenen Dokumentation Auskunft zu Themen wie:

- Ablauf der Installation
- Beschreibung der integrierten Funktionen
- Details

Der TechGuide beschreibt nur die generelle Handhabung und die Konfiguration der SmartIntego-Komponenten.

5.2 Kommunikation zwischen Integratorsystem und Schließungen

Vor der Zertifizierung eines neuen Integrators wird ein technischer Akzeptanztest durchgeführt. Während dieses Akzeptanztests prüfen SimonsVoss und der Integrator, ob das Integratorsystem und die SmartIntego-Komponenten absolut einwandfrei miteinander kommunizieren. Zertifizierte Integrationspartner werden auf der SmartIntego-Website (*https://www.smartintego.com/int/home/home*) aufgelistet.

5.3 Fehlermanagement

Smartintego Wireless Online nutzt für die drahtlosen Kommnikation zu den Schließungen ein Funknetzwerk auf 868-MHz-Basis.

Die kabellose Kommunikation auf 868 MHz ist weitverbreitet. Starke Auslastung des Frequenzbereichs führt zu vorübergehenden Engpässen in der Kommunikation.

Die SmartIntego-Komponenten ist mit Fehlerkorrektur-Routinen ausgestattet, die derartige Engpässe selbstständig abfangen.

Störungen oder Engpässe, die sich nicht mehr von den SmartIntego-Komponenten auffangen lassen, müssen durch das Integratorsystem entweder mit zusätzlichen Fehlerkorrekturen aufgefangen und/oder mit einem Display signalisiert werden.

5.4 Ereignisprotokollierung und Logfiles

Für den Fall, dass der Errichter ein potentielles Problem analysieren soll, sollte im Integratorsystem eine entsprechende Ereignisprotokollierung vorhanden sein.

Der Errichter muss mit dieser Ereignisprotokollierung potentielle Probleme aufzeichnen und nachvollziehen können.

5.5 Batteriemanagement

Die SmartIntego-Komponenten schicken Batteriewarnungen an das Integratorsystem, das dann den Schließanlagenadministrator über die schwachen Batterien informiert. Ein beauftragter Techniker oder der Endkunde sind anschließend für den rechtzeitigen Wechsel der Batterien in den Komponenten verantwortlich.

5.6 Systemüberwachung

Das Integratorsystem informiert den Schließanlagenadministrator über den Netzwerkstatus der SmartIntego-GatewayNodes.

5.7 Zutrittsberechtigungen

Das Integratorsystem bzw. dessen Zutrittskontrollen kontrollieren die Schließungen:

- Zutrittsberechtigungen
- Art der Öffnung
  - Kurzzeit-Einkuppeln (3 bis 25 Sekunden)
  - Langzeit-Einkuppeln (Eine Minute oder länger)
  - Office-Modus (Kurz: 3 bis 25 Sekunden oder lang: Eine Minute oder länger)
  - Zutrittsverweigerung
  - Automatisches Auskuppeln
  - Zeitgesteuerte Zutrittsberechtigungen

5.8 Offline-Funktionen (Whitelists)

Im Normalfall kommunizieren die Komponenten eines SmartIntego-Wireless-Online-Systems direkt mit dem Integratorsystem, das alle Anfragen online verarbeitet.

In manchen Fällen kann die Kommunikation gestört sein, zum Beispiel:

- Stromausfall
- Netzwerkprobleme

Die SmartIntego-Schließungen erreichen das Integratorsystem dann nicht mehr und umgekehrt. Für diesen Fall können als Rückfallebene in den Schließungen Whitelists mit berechtigten Karten hinterlegt werden. Mit den Whitelists können die Endnutzer weiterhin die Schließungen nutzen, ohne dass es unkontrollierte Zutritte gibt.

Whitelist-Definition

Eine Whitelist ist eine vorher definierte Liste mit berechtigten Karten. Sie wird in den Schließungen selbst gespeichert. Wenn eine Schließung das Integratorsystem nicht erreicht und die ausgelesene Karte in der Whitelist hinterlegt ist, dann kuppelt die Schließung kurzzeitig ein (5 Sekunden).

Ihnen stehen drei Arten von Whitelists zur Verfügung:

- Construction Site Whitelist
- Integrator-Whitelist
- Integrator-Whitelist mit lokaler Prüfung (Notfallzutritts- oder Feuerwehrkarten)

5.8.1 Construction Site Whitelist

Die Construction Site Whitelist ist auch als Prio-Whitelist oder temporäre Whitelist bekannt.

Manchmal ist es notwendig, dass die Schließungen auf einer Baustelle montiert werden, bevor die notwendige Infrastruktur (Stromanschlüsse, IT-Ausstattung oder Integratorsystem) vorhanden sind.

In diesem Fall können Sie Ihre Schließungen vorab übergangsweise offline verwenden, bis die Netzwerkinfrastruktur einsatzbereit ist. Dazu geben Sie Karten frei, die durch Baustellenarbeiter verwendet werden können.

Unprogrammierte SmartIntego-Schließungen können mit allen von der Schließung lesbaren Karten geöffnet werden. Die Construction Site Whitelist beschränkt die Zutrittsberechtigung auf die von Ihnen freigegebenen (d.h. in der Construction Site Whitelist eingetragenen) Karten. Sie sollte nur vorübergehend während der Aufbauphase verwendet werden. Verbinden Sie die Schließungen später in jedem Fall mit dem Integratorsystem.

Eigenschaften der Construction Site Whitelist:

- Lokale Prüfung der Zutrittsberechtigung durch Schließung
- Keine Kommunikation mit Integratorsystem
- Prüfung der Zutrittsberechtigung nur mit der Unique ID (UID) der Karte
- Beschränkung auf 128 Karten
- Gleiche Zutrittsberechtigungen für alle hinterlegten Karten (Keine Beschränkung auf einzelne Schließungen: Alle Karten der Construction Site Whitelist haben Zutrittsberechtigung an allen Schließungen, in denen die Construction Site Whitelist hinterlegt ist)
- Keine Zutrittsprotokollierung bzw. Zutrittsliste
- Standardwert: Fünf Sekunden

- Keine Batteriewarnungen
- Exklusive Verwaltung durch SmartIntego-Tool
- Kein Auskuppeln dauerhaft eingekuppelter Schließungen

Das Integratorsystem kann die Construction Site Whitelist selbst nicht verändern, aber die komplette Construction Site Whitelist in den Schließungen löschen.

HINWEIS

Überführung in Normalbetrieb

Die Construction Site Whitelist läuft nicht von selbst aus bzw. wird nicht von selbst unwirksam.

- Bei der Überführung in den Normalbetrieb muss der Erichter die Construction Site Whitelist aus den Schließungen und aus dem SmartIntego-Tool löschen.

5.8.2 Integrator-Whitelist

Die Integrator-Whitelist wird vom Integrator selbst verwaltet und ist der wichtigste Sicherheitsmechanismus in der SmartIntego-Schließanlage.

Sie dient als Rückfallebene, falls das Integratorsystem nicht mehr erreichbar ist. Mögliche Gründe für einen Ausfall:

- Stromausfall
- Störungen in der IT-Infrastruktur
- Störungen im Integratorsystem
- Hardwarefehler

Sobald die Schließungen das Integratorsystem nicht mehr erreichen, können Zutrittsberechtigungen nicht mehr online geprüft bzw. empfangen werden. Auch berechtigte Nutzer würden keine Türen mehr öffnen können.

Dafür wird während der Aufbauphase eines Projekts im Integratorsystem eine Whitelist konfiguriert und in die Schließungen programmiert.

Eigenschaften der Integrator-Whitelist:

- Lokale Prüfung durch Schließung nach Return-Timeout (Keine Antwort vom Integratorsysten innerhalb von fünf Sekunden)
- Keine Kommunikation mit Integratorsystem
- Standardwert: Fünf Sekunden
- Längeres Vorhalten der Karte (ca. fünf Sekunden) kuppelt auch dauerhaft eingekuppelte Schließungen aus

- Zusatzfunktionen wie Office-Mode oder Langzeit-Einkuppeln nicht verfügbar
- Whitelist-Authentifizierung (offline) normalerweise mit gleicher Karten-ID wie Online-Authentifizierung. In Sonderfällen kann eine Karte eine ID für Onlinezutritte und eine ID für Offlinezutritte haben.
- Beschränkung auf 250 Karten pro Schloss (siehe Dokumentation des Integratorsystems)
- Individuelle, eigene Integrator-Whitelist für jedes Schloss
- Protokollierung von Offline-Zutritten: Zutrittsliste im Schloss mit 1.000 Einträgen (rollierend überschrieben, WO Legacy 250)
- Zutrittsliste mit SmartIntego-Tool und WaveNet oder lokalem Programmiergerät auslesbar
- Keine Batteriewarnungen
- Exklusive Verwaltung durch Integratorsystem

HINWEIS

Whitelist bei beidseitig lesenden Schließungen

Schließungen mit Lesern auf beiden Seiten (FD bzw. BL) haben nur eine Whitelist für beide Seiten.

5.8.3 Notfallzutritts- oder Feuerwehrkarten mit lokaler Prüfung

Diese Karten gehören zur Integrator Whitelist, werden also auf deren Kontingent angerechnet.

Sie unterscheidet sich aber in einem für Notfälle wichtigen Punkt: Sobald die Schließung erkennt, dass die vorgehaltene Karte eine solche Karte ist, kuppelt sie für fünf Sekunden ein. Eine Kommunikation mit dem Integratorsystem kostet im Notfall wertvolle Zeit und findet deshalb für diese speziellen Karten erst im Nachhinein statt. Das Integratorsystem wird informiert, sofern eine Verbindung besteht. Die weiteren Funktionen und Einschränkungen sind identisch mit denen der Integrator Whitelist.

WARNUNG

Zutritt für Rettungskräfte bei Systemausfall

In Notfällen wie einem Brand kommt es häufig zu Störungen und versagenden Systemen. Die Schließungen können dann möglicherweise nicht mehr zentral geöffnet werden. Mit Notfallzutritts- und Feuerwehrkarten können Rettungskräfte trotzdem sehr schnell vordringen.

- Erstellen Sie mehrere Notfallzutritts- oder Feuerwehrkarten und bewahren Sie diese Karten in einem Feuerwehrschlüsseldepot auf.

5.9 Installation und Wartung

Das SmartIntego-Tool verwaltet die Schließungen:

- hinzufügen
- entfernen
- austauschen
- oder ersetzen.

Vorgenommene Änderungen müssen dem Integratorsystem mitgeteilt werden. Das Vorgehen unterscheidet sich je nach Integratorsystem. Diese Dokumentation beschreibt deshalb nur das Vorgehen im SmartIntego-Tool.

5.10 Kurzzeit-Einkuppeln

Schließungen kuppeln damit für einen kurzen Zeitraum (3 bis 25 Sekunden) ein. Während dieser Zeit kann der Nutzer mit dem Schließzylinder bzw. dem SmartHandle das Einsteckschloss der Tür bedienen.

Alternativ zu einer zutrittsberechtigten Karte kann die Schließung auch anders eingekuppelt werden:

- Aus der Ferne mit dem Integratorsystem
- Zeitgesteuert

5.11 Langzeitöffnung / Flip-Flop- oder statischer Office-Modus

Je nach Integrator heißt diese Funktion anders:

- Langzeitöffnung
- Flip-Flop-Modus
- Statischer Office-Modus

Sie bedeutet aber immer dasselbe. Schließungen kuppeln damit für einen langen Zeitraum (eine Minute und länger) ein. Während dieser Zeit kann der Nutzer mit dem Schließzylinder bzw. dem SmartHandle das Einsteckschloss der Tür bedienen.

Alternativ zu einer zutrittsberechtigten Karte kann die Schließung auch anders eingekuppelt werden:

- Aus der Ferne mit dem Integratorsystem
- Zeitgesteuert

Die Dauer des Einkuppelns ist einstellbar (Eine Minute bis unendlich, d.h. dauerhaft eingekuppelt). Kombinationen ermöglichen die Abdeckung sehr vielfältiger Anforderungen.

Beispiel:

Eine Schließung kann durch eine berechtigte Karte eingekuppelt werden:

- Während der Bürozeit zwischen 7:00 und 17:00 wird die Tür stark frequentiert:

  Die Schließung bleibt aus Komfortgründen langfristig eingekuppelt und muss nicht jedes Mal eingekuppelt werden.
- Außerhalb der Bürozeit zwischen 17:00 und 7:00 befinden sich maximal einzelne Personen im Gebäude.

  Die Schließung bleibt aus Sicherheitsgründen nur kurzzeitig eingekuppelt.

Dieses Verhalten wird häufig als Office-Modus bezeichnet. Die Schließung kann ausgekuppelt werden:

- Manuell: Mit einer berechtigten Karte
- Automatisch: Durch eine Zeitsteuerung

Details entnehmen Sie bitte der Dokumentation des Integratorsystems.

5.12 Office-Modus / Persönlicher Office-Modus

Dieser Modus ähnelt dem statischen Office-Modus. Der Nutzer kann das Verhalten der Schließung hier aber selbst kontrollieren, indem er die Karte kurz oder lange vor die Schließung hält.

Beispiel:

- Während der Arbeitszeit sollen andere Mitarbeiter das Büro betreten können:

  Der Mitarbeiter hält seine Karte länger als zwei Sekunden vor die Schließung. Damit kuppelt er die Schließung lange ein und ermöglicht jedem den Zutritt (eine Minute bis dauerhaft eingekuppelt).

- Während der Pause möchte der Mitarbeiter nicht gestört werden:

  Der Mitarbeiter hält seine Karte weniger als zwei Sekunden vor die Schließung. Damit kuppelt er die Schließung nur kurzfristig ein.

Kombinationen ermöglichen die Abdeckung vielfältiger Anforderungen.

Die Schließung kann ausgekuppelt werden:

- Manuell: Mit einer berechtigten Karte
- Automatisch: Durch eine Zeitsteuerung

Details entnehmen Sie bitte der Dokumentation des Integratorsystems.

5.13 DoorMonitoring

DoorMonitoring ist eine SimonsVoss-Technologie. SmartIntego-Schließungen mit dieser Option sind mit Sensoren ausgestattet, die den Türzustand überwachen.

Die Verwendung von DoorMonitoring in SmartIntego-Systemen erfordert erweiterte Konfiguration und Programmierung mit dem SmartIntego-Tool (WO).

Details entnehmen Sie bitte der Dokumentation des Integratorsystems.

5.13.1 Mögliche (Tür-)zustände

Die angezeigten Zustände sind komponentenabhängig.

5.13.1.1 Mögliche DoorMonitoring-Zustände SmartHandle

- Tür offen/geschlossen
- Tür zu lange offen
- Verriegelt (nur bei selbstverriegelnden Einsteckschlössern)
- Drücker gedrückt/nicht gedrückt

5.13.1.2 Mögliche Zustände RouterNode 2 / GatewayNode 2

- Input aktiv/inaktiv
- Analoge Spannung über/unter Schwellwert

5.14 Escape & Return

Diese Funktion ermöglicht kurzzeitig die Rückkehr in einen Raum, nachdem die Tür bereits zugefallen ist. Eine Karte ist dazu nicht nötig.

Ein Sensor auf der Innenseite des SmartHandles erkennt, wenn der Drücker betätigt wurde, um die Tür zu öffnen. Das SmartHandle kuppelt dann für eine vorher definierte Return-Zeit ein und gibt ein akustisches/optisches Signal.

Das SmartHandle kuppelt nach Ablauf der eingestellten Return-Zeit automatisch aus. Alternativ kann es auch vorher ausgekuppelt werden, indem der Nutzer eine Karte zwei Sekunden vor den SmartHandle-Leser hält.

HINWEIS

Escape & Return: Rechtslage

Der Escape & Return Timeout kann zwischen 30 s und 240 s betragen. Der Einsatz und die Konfiguration von Escape & Return kann gesetzlichen Bestimmungen unterliegen (z.B. Norwegen).

- Informieren Sie sich vorab über gesetzliche Bestimmungen.

5.15 PinCode-Tastatur

Die SmartIntego-PinCode-Tastatur ist eine batteriebetriebene Online-PinCode-Tastatur. Die Intelligenz ist nicht in der PinCode-Tastatur enthalten, sondern im Integratorsystem.

In der PinCode-Tastatur ist nur eine Master-PIN und die Länge der User-PINs für diese PinCode-Tastatur gespeichert. Deshalb gibt es keine Begrenzung aufgrund des vorhandenen Speicherplatzes und die Anzahl der User-PINs ist nicht durch die Hardware der PinCode-Tastatur begrenzt.

Ablauf:

✓ Master-PIN definiert.
✓ Länge der User-PINs für diese PinCode-Tastatur definiert.

1. Nutzer gibt PIN ein.
   ↳ PinCode-Tastatur prüft Länge der eingegebenen PIN (nicht die PIN selbst!)
2. PinCode-Tastatur schickt PIN mit gültiger Länge an Integratorsystem.
3. Integratorsystem prüft PIN auf Gültigkeit.
4. Integratorsystem reagiert mit einer oder mehrerer Aktionen auf die PIN.
   ↳ Beispielsweise wird eine Tür neben der PinCode-Tastatur geöffnet.

Mögliche Anwendungen:

- Eingabe einer PIN öffnet eine Tür neben der PinCode-Tastatur → Nutzer können nach Eingabe selbst passieren.
- Eingabe einer PIN öffnet eine oder mehrere beliebige Türen im Gebäude → Nutzer können andere entfernte Nutzer durch Eingabe passieren lassen.
- Eingabe einer PIN und Vorhalten einer Karte an der Schließung öffnet die Tür → Zusätzliche Absicherung (Redundanz).

Anforderungen an die PINs:

Anforderungen an die Master-PIN	Anforderungen an alle User-PINs
■ Beginnt nicht mit 0 ■ Länge genau acht Zeichen	■ Beginnt nicht mit 0 ■ Gleiche Länge (zwischen einem und neun Zeichen)

5.16 Kürzere Reaktionszeiten der LockNodes (Short Wake-Up period)

Bei allen Aktionen an Schließungen, die aus der Ferne durch das Integratorsystem initiiert werden, summieren sich die netzwerkbedingten Verzögerungen auf (siehe auch *Kommunikation zwischen Integratorsystem und Schließungen [▸ 10]*). Solche Aktionen sind beispielsweise:

- Fernöffnungen
- Öffnungen durch PinCode-Tastaturen
- Programmierungen der Whitelist

Zwischen dem Initiieren der Aktion und einer sichtbaren Reaktion können bis zu zwölf Sekunden oder mehr vergehen.

Diese Zeit kann verkürzt werden. Die LockNodes in den Schließungen sparen Energie, indem sie nur intervallweise "aufwachen" und prüfen, ob sie gerade angesprochen werden. Diese Intervalle können verkürzt werden.

Im Integratorsystem wird dazu das Aufwach-Intervall der Schließung verkürzt (Short Wake-Up period). Die Schließung merkt dann schneller, dass sie angesprochen wird und reagiert schneller.

- Diese Funktion kann für jede Schließung einzeln aktiviert oder deaktiviert werden (abhängig vom Integrator).
- Diese Funktion kann zusätzlich zeitgesteuert aktiviert oder deaktiviert werden (abhängig vom Integrator, z.B. nur zu Bürozeiten eingeschaltet werden).
- Durch das kürzere Aufwach-Intervall steigt der Stromverbrauch. Die Standby-Batterielebensdauer verkürzt sich bei dauerhaft aktivem kürzeren Aufwach-Intervall auf 3,5 Jahre.

Details entnehmen Sie bitte der Dokumentation des Integratorsystems.

5.17 IO-Node

Der SmartIntego IO-Node ist ein batteriebetriebenes Funkmodul mit drei Eingängen und einem Open-Drain-Ausgang. Durch die Verbindung mit dem Integratorsystem kann der IO-Node zur Überwachung und Steuerung von Komponenten verwendet werden.

Details entnehmen Sie bitte der Dokumentation des Integratorsystems.

5.18 Solution Guard

Der Integrator kann frei entscheiden, wie er seine Integration lizenziert und wie er seine Integration schützt.

Mit SimonsVoss Solution Guard können nur die Schließungen in Integratorsystemen verwendet werden, die zentral beim Integrator registriert wurden. Der Integrator kann ebenfalls frei entscheiden, wie er auf unlizenzierte Schließungen in seinem Integrationssystem reagiert.

Bitte entnehmen Sie der Beschreibung Ihres Integratorsystems, ob Solution Guard verwendet wird.

6. Komponenten

SmartIntego-Schließungen und Komponenten an der Tür werden batteriebetrieben und vernetzt verwendet. Alle Schließungen sind passiv (RFID-Technik mit 13,56 MHz).

Unter anderem sind folgende SmartIntego-Komponenten erhätllich:

Komponenten an der Tür

	SI Digital Cylinder AX
	SI-Schließzylinder
	SI.SmartHandle AX
	SI.SmartHandle

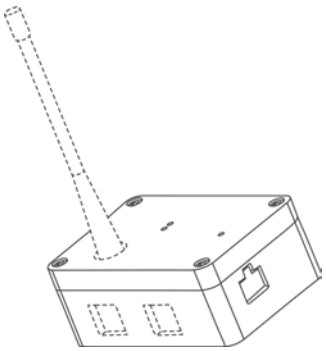
	SI Padlock AX
	SI-Vorhangschloss
	SI SmartLocker AX

Komponenten an der Tür (kein RFID)

	IO-Node

	SmartIntego PinCode-Tastatur

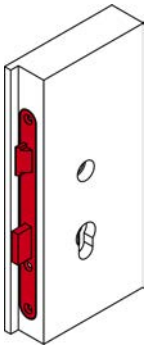
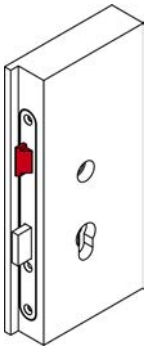
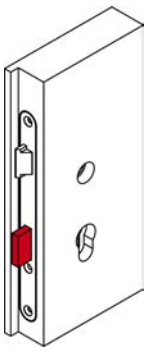
Komponenten für die Infrastruktur

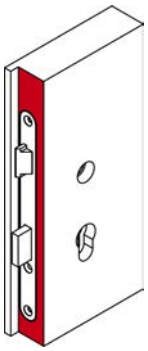
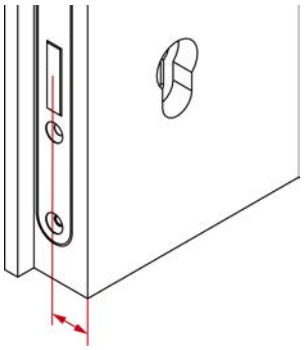
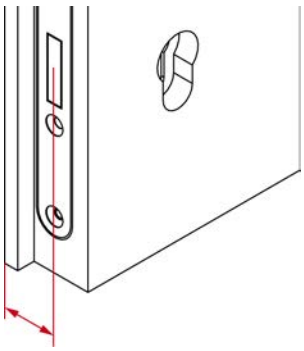
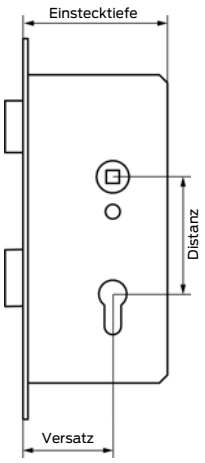
	GatewayNode 1
	GatewayNode 2
	Programmiergerät SI.SmartCD

Ihr Integrator stellt Komponenten mit Relaiskontakt und Leser mit externer Stromversorgung zur Verfügung.

6.1 Tür

Die folgende Zeichnungen erklären wichtige Fachbegriffe rund um Türen und Einsteckschlösser. Sie benötigen diese Fachbegriffe, um die richtigen SmartIntego-Schließungen zu verwenden.

	Außenseite (frei zugänglicher Bereich)
	Innenseite (gesicherter Bereich)
	Einsteckschloss
	Falle
	Riegel/Riegelblock

	Türblatt
	Außenseitiges Abmaß (Kante der Außenseite bis zur Mitte des Riegels bei max. 3 mm Projektion)
	Innenseitiges Abmaß (Kante der Innenseite bis zur Mitte des Riegels)
	■ Einstecktiefe ■ Distanz ■ Versatz

6.2 Auslieferungszustand

HINWEIS

Fehlende Zutrittskontrolle im Auslieferungszustand

Alle SmartIntego-Schließungen werden unprogrammiert ausgeliefert. Unprogrammierte Schließungen reagieren auf alle auslesbaren Karten (RFID-Frequenz 13,56 MHz und vorhandene ID). Diese Karten können unprogrammierte Schließungen für fünf Sekunden einkuppeln.

- Konfigurieren und programmieren Sie die Schließungen, bevor Sie sie in einem Produktivsystem einsetzen.

↳ Nach der Programmierung übernimmt die Zutrittskontrolle des Integratorsystems die Steuerung der SmartIntego-Schließungen.

6.3 Arten von SmartIntego-Schließungen

Es gibt mehrere Arten von SmartIntego-Schließungen:

SI Digital Cylinder AX  SI-Schließzylinder 	Verriegeln und entriegeln die Tür mit dem Riegel des Einsteckschlosses.

SI.SmartHandle AX  SI.SmartHandle 	Schließen und öffnen die Tür mit der Falle des Einsteckschlosses. SmartHandles können Türen nur in Kombination mit einem selbstverriegelnden Einsteckschloss verriegeln.
SI Padlock AX  SI-Vorhangschloss 	Verriegeln Türen zusammen mit entsprechenden Vorrichtungen. Die Funktion ist analog zu mechanischen Vorhangschlössern, aber mit den Vorteilen einer digitalen Schließung.

SI SmartLocker AX 	Verriegeln Spindtüren und Möbel. Die Funktion ist analog zu mechanischen Spindschlössern, aber mit den Vorteilen einer digitalen Schließung.

6.4 AXEOS-Betriebssystem

Alle SmartIntego-Schließungen werden mit einem SimonsVoss-Betriebssystem betrieben. Mit den SmartHandle AX führt SimonsVoss das neueste Betriebssystem ein: AXEOS.

SmartIntego-Komponenten sind generell abwärtskompatibel. Sie können zusammen mit älteren SmartIntego-Komponenten verwendet werden. Bestehende Integrationsprojekte können generell ohne zusätzlichen Integrationsaufwand mit den AX-Komponenten erweitert werden, wenn bereits integrierte Funktionen verwendet werden. Ob Ihr Integratorsystem die neuen AXEOS-Produkte unterstützt, entnehmen Sie bitte der Dokumentation des jeweiligen Integrators.

Das neue AXEOS-Betriebssystem wurde in folgenden Punkten überarbeitet:

- Neue Hardware-Komponenten
- Längere Batteriestandzeiten
- Flexibilität der Plattform für spätere Funktionen
- Wegfall der 3DES-Unterstützung für MIFARE DESFire

6.5 Digital Cylinder AX

Der SI Digital Cylinder AX ist die Weiterentwicklung des Schließzylinders TN4 auf Basis der AXEOS-Technologie.

Der SI Digital Cylinder AX bewegt den Riegel des Einsteckschlosses. Verwenden Sie einen SI Digital Cylinder AX, wenn Sie Türen verriegeln wollen.

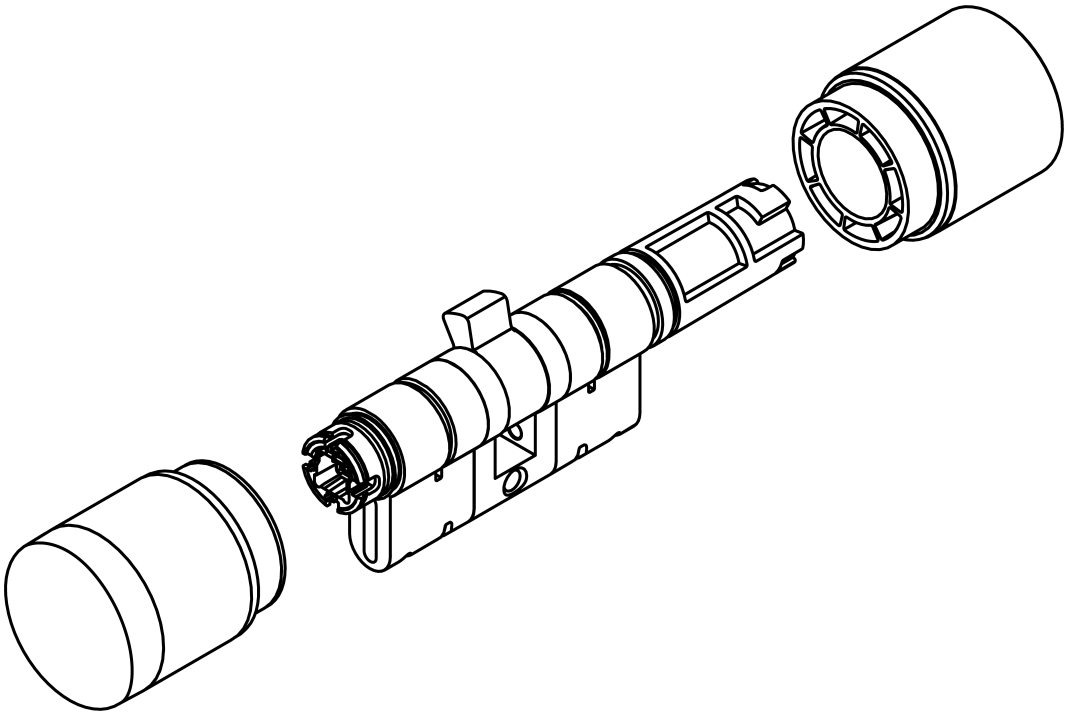
Detaillierte Informationen finden Sie im Handbuch des SI Digital Cylinder AX.

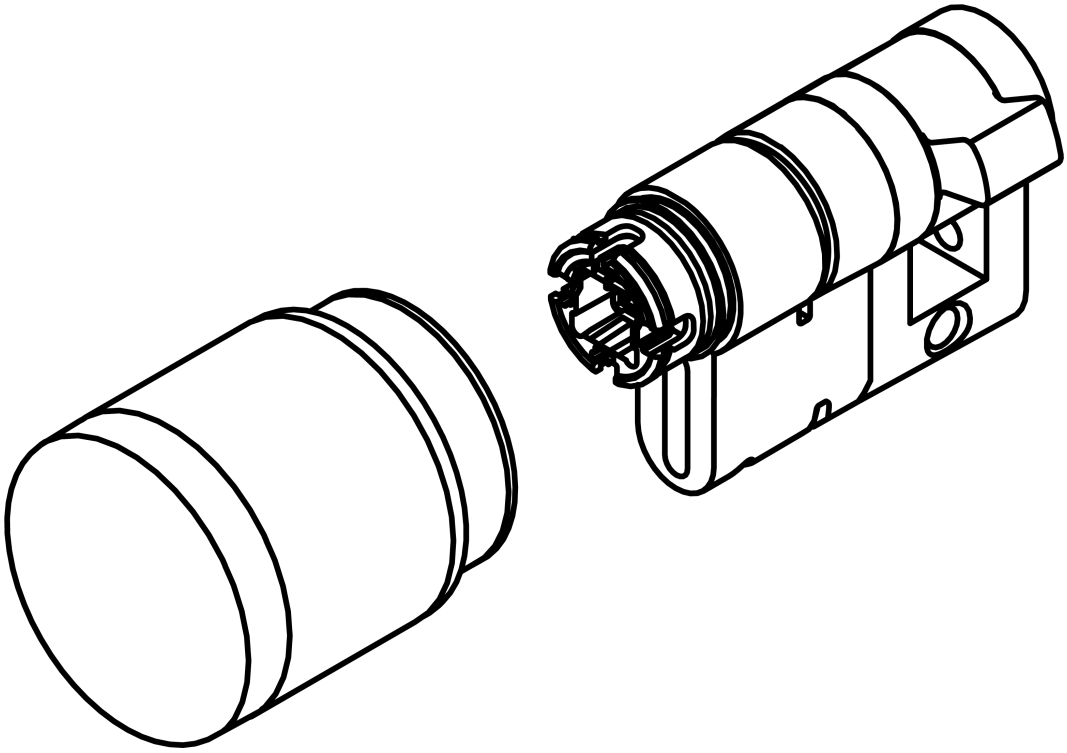
6.5.1 Aufbau

Comfort/Halbzylinder

Beim SI Digital Cylinder AX (Comfort und Halbzylinder) befindet sich die gesamte Elektronik auf der Außenseite.

- Control Unit (CU)
- Kartenleser (Card Reader = CR)
- LockNode (LN)
- Batterien
- Secure Element (SE) - im Profilkern der Außenseite

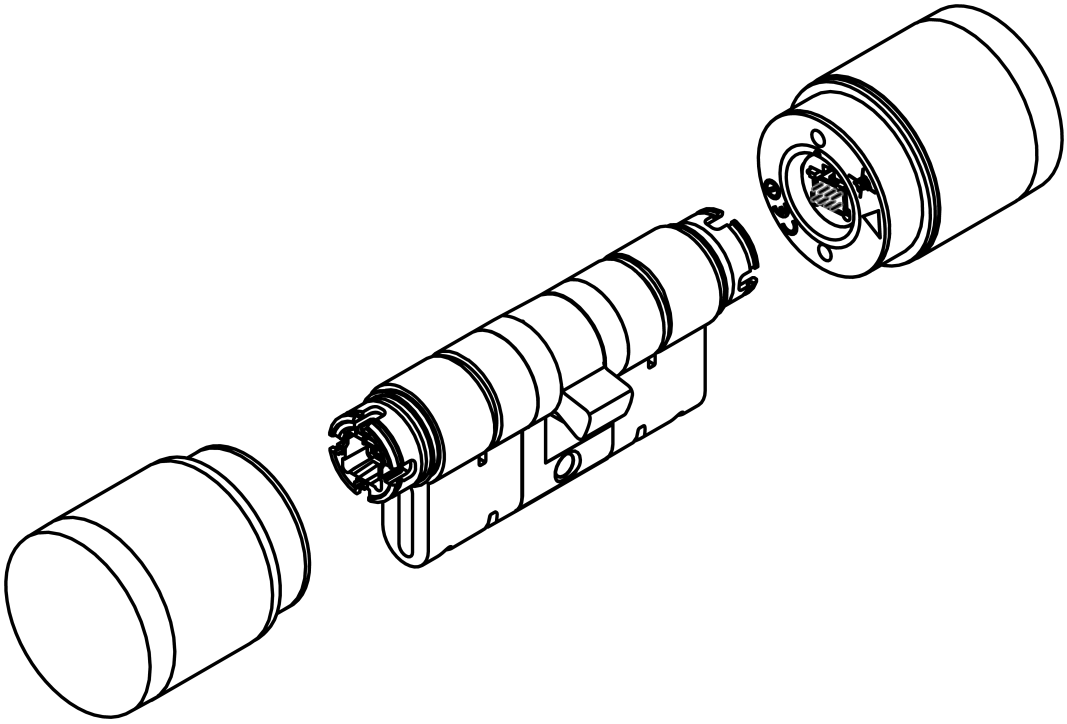




Freidrehend

Beim SI Digital Cylinder AX (Freidrehend) ist jeder der beiden Leseknäufe mit einer vollständigen Elektronik ausgestattetw.

- Control Unit (CU)
- Kartenleser (Card Reader = CR)
- LockNode (LN)
- Batterien
- Secure Element (SE) - im Profilkern der Außenseite



HINWEIS

Elektronik bei beidseitig lesenden SI Digital Cylinder AX

Der SI Digital Cylinder AX ist in der beidseitig lesenden Variante mit einem elektronischen Leseknauf auf der Außenseite und einem elektronischen Leseknauf auf der Innenseite ausgestattet. Beide Leseknäufe sind voneinander unabhängig.

1. Legen Sie die beiden elektronischen Leseknäufe separat an und konfigurieren Sie sie.
2. Programmieren Sie die beiden elektronischen Leseknäufe separat.

Längenmodularität

Die Europrofil-Variante ist modular und kann vor Ort verlängert, verkürzt oder anderweitig umgebaut werden. Details dazu finden Sie im Handbuch zur Längenmodularität.

6.5.2 Varianten und Ausstattungsmerkmale

Den SI Digital Cylinder AX gibt es sowohl einseitig lesend (Comfort = CO) als auch in einer beidseitig lesenden Variante (Freidrehend = FD).

Die Bestellnummer gibt Auskunft über die Variante und die Ausstattungsmerkmale:

Allgemein	SI	SmartIntego-Zylinder
	Z5	Technologielevel 5
	■ EU (Europrofil) ■ SR (Swiss Round) ■ SR (Scandinavian Oval) ■ RS (Round Scandinavian)	Profil
	AXX-IXX	Außenmaß-Innenmaß
	M	**M**IFARE
Aufbau	CO	Comfort - Zylinder innen dauerhaft eingekuppelt
	FD	Freidrehend - Zylinder mit zwei Kartenlesern (Innen- und Außenseite) Unterschiedliche Zutrittsberechtigungen möglich (Integratorabhängig)
Ausstattungsmerkmale	AP	Antipanik-Funktion
	WP	Wettergeschützte Version (IP 67), sonst IP54
	MS	Messing-Variante
	HZ	Halbzylinder
	MR	Multirast
Vernetzung	■ WO (Wireless Online)	Vernetzungstechnik

Weitere Details zu den einzelnen Varianten und Ausstattungsmerkmalen finden Sie im Handbuch zum SI Digital Cylinder AX.

HINWEIS

Vermeidung von Fehlbestellungen durch Bestellhilfe

SmartIntego-Komponenten bieten eine große Vielfalt an Kombinationen. Nicht jede Kombination ist sinnvoll und tatsächlich erhältlich. Eine manuelle Zusammenstellung der Ausstattungsmerkmale kann zu nicht erhältlichen Kombinationen oder Fehlbestellungen führen.

- Verwenden Sie immer die Bestellhilfe aus dem Partnerbereich der SmartIntego-Website (*www.smartintego.com)*).

6.5.3 Montage

ACHTUNG

Unbefugter Zutritt durch Aufbohren auf Innenseite

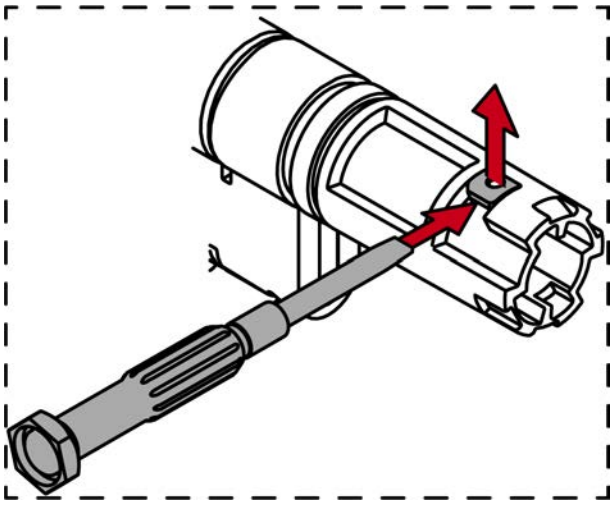
Die Außenseite der SI Digital Cylinder AX ist je nach Ausführung auf der Außenseite mit einem Bohrschutz ausgerüstet.

- Wenn Sie am Zylinderkörper eine Markierung der Innenseite (*IN*) finden, dann montieren Sie den SI Digital Cylinder AX so, dass sich diese Seite in einem geschützten Bereich befindet.

6.5.3.1 Comfortzylinder/Antipanikzylinder (CO/AP, einseitig lesend)

Standardmontage/Erstmontage

Diese Möglichkeit ist die einfachste Möglichkeit, den SI Digital Cylinder AX zu montieren. Sie benötigen bei der Erstmontage kein Spezialwerkzeug. Entfernen Sie die rote Montagesperre aus Kunststoff vor der Erstmontage.



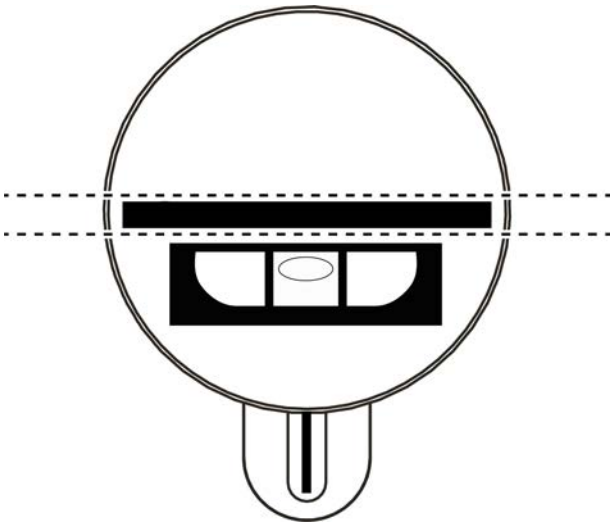
HINWEIS

Werkzeugfreie Erstmontage

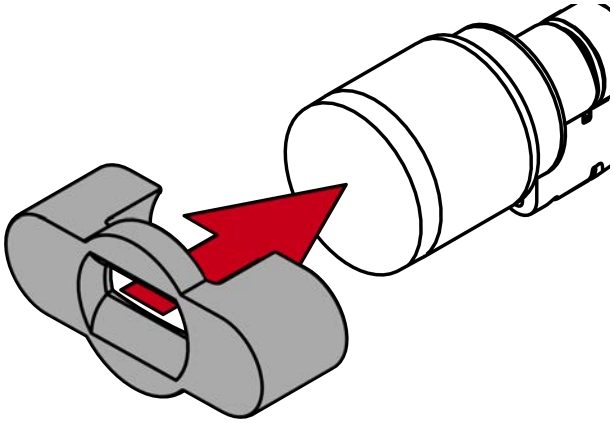
Der mechanische Knauf ist im Auslieferungszustand nur aufgesteckt. Eine Knaufsperre (rotes Kunststoffteil) verhindert, dass der Knauf einrastet. Sie können den mechanischen Knauf des Schließzylinders AX ohne Werkzeug montieren, aber ohne Spezialwerkzeug nicht mehr demontieren. Bei der Erstmontage des Schließzylinders AX entfällt deshalb die Demontage des mechanischen Knaufs. Beginnen Sie stattdessen mit dem Einstecken des Schließzylinders AX.

- ✓ Spezialwerkzeug vorhanden.
- ✓ PH2-Schraubendreher vorhanden.

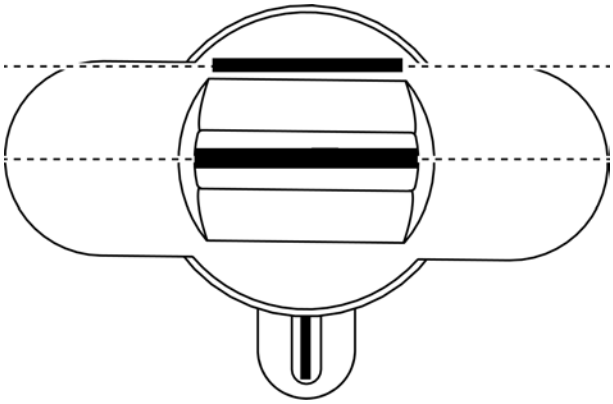
1. Richten Sie den Knauf waagrecht aus.



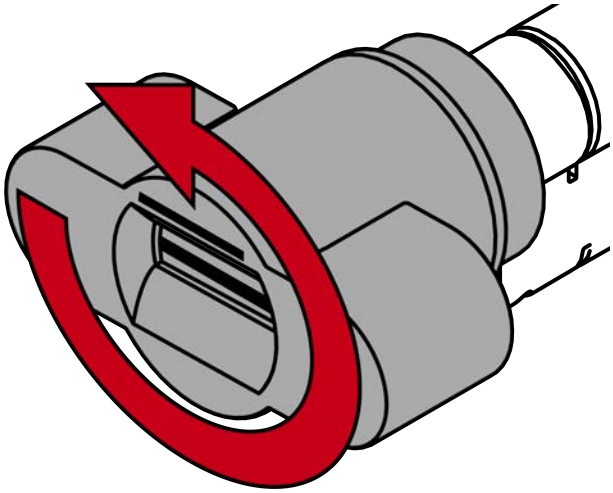
2. Setzen Sie das Spezialwerkzeug an.



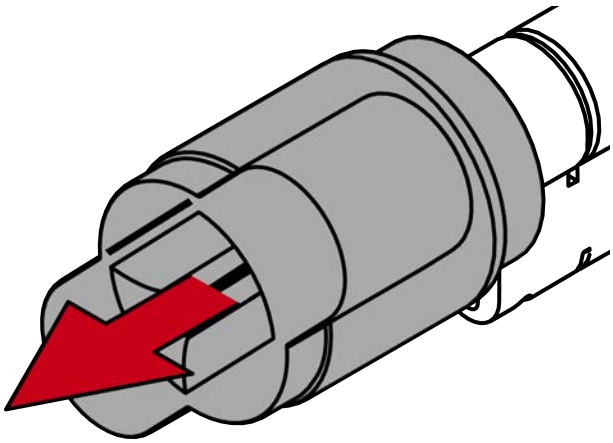
3. Richten Sie das Spezialwerkzeug so aus, dass das Logo parallel zur Aussparung ist.



4. Drehen Sie das Spezialwerkzeug und den Knauf gleichzeitig gegen den Uhrzeigersinn.

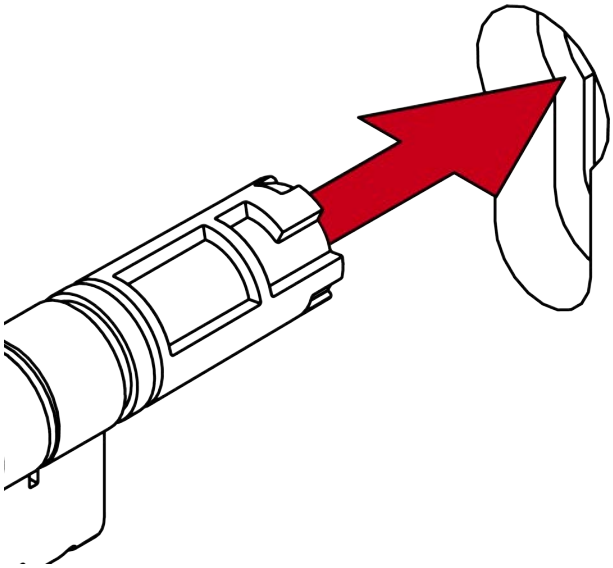


5. Ziehen Sie das Spezialwerkzeug und den Knauf gleichzeitig ab.



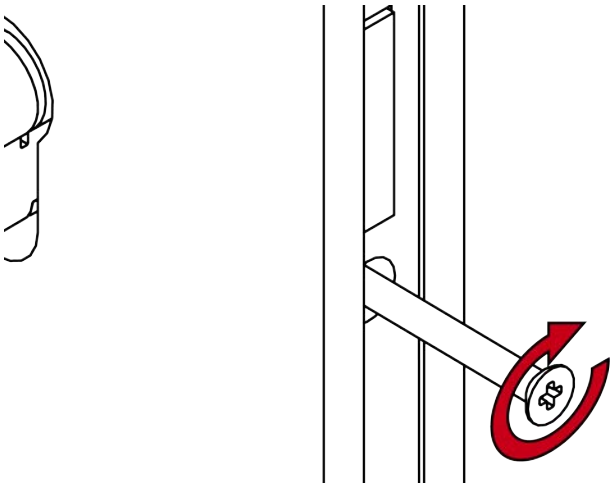
↳ Mechanischer Knauf ist demontiert.

6. Stecken Sie den SI Digital Cylinder AX mit der knauffreien Seite in das Einsteckschloss.



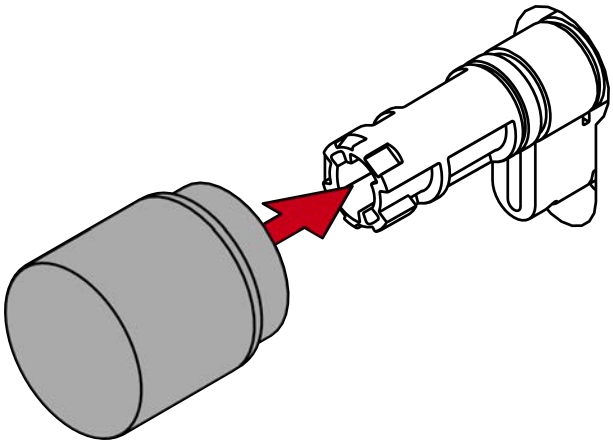
↳ SI Digital Cylinder AX ist im Einsteckschloss positioniert.

7. Schrauben Sie den SI Digital Cylinder AX mit der Stulpschraube fest.

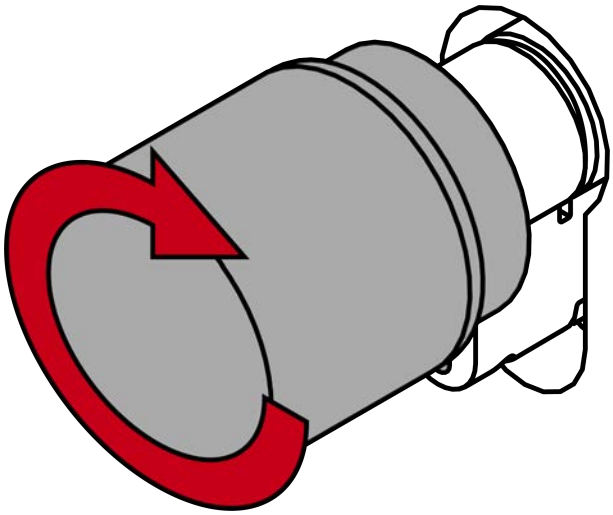


↳ SI Digital Cylinder AX ist im Einsteckschloss befestigt.

8. Stecken Sie den Knauf auf.



9. Drehen Sie den Knauf im Uhrzeigersinn.



   ↳ Knauf rastet mit einem Klicken ein.
   ↳ Mechanischer Knauf ist montiert.
10. Führen Sie einen Funktionstest durch (siehe *Funktionstest [▸ 86]*).
11. Führen Sie für Antipanik-Zylinder zusätzlich den Antipanik-Funktionstest durch (siehe Antipanik-Funktionstest).

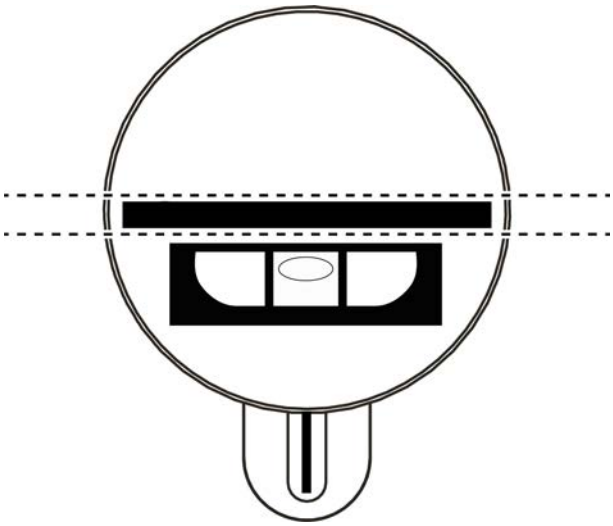
↳ SI Digital Cylinder AX ist fertig montiert.

Montage mit Aufsteckblenden

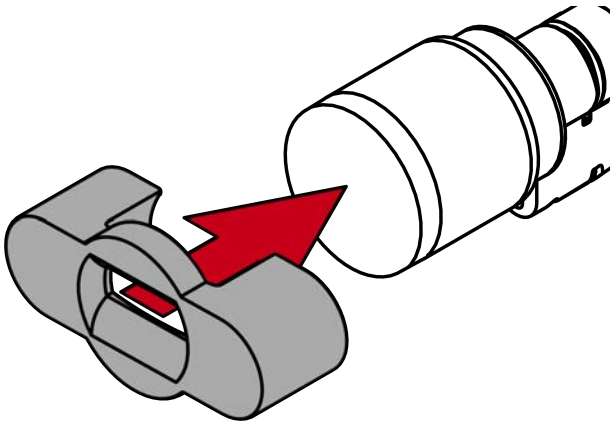
Diese Möglichkeit ermöglicht es Ihnen, den SI Digital Cylinder AX mit bestimmten Blenden zu kombinieren. Manche Blenden werden auf den montierten Zylinder aufgesteckt und befinden sich dann zwischen Knauf und Tür. Wenn Sie solche Blenden verwenden wollen, dann müssen Sie beide Knäufe demontieren.

- ✓ Spezialwerkzeug vorhanden.
- ✓ 1,5-mm-Sechskantschlüssel vorhanden.
- ✓ PH2-Schraubendreher vorhanden.

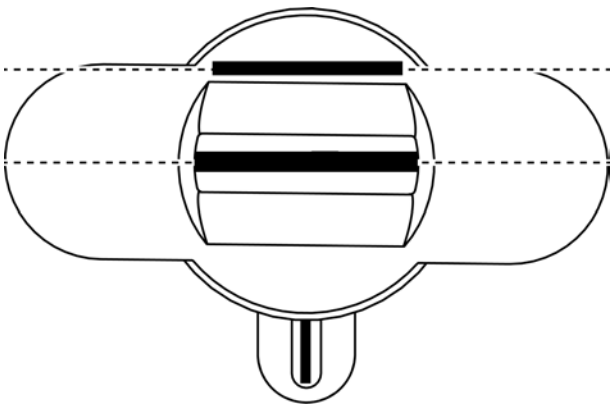
1. Richten Sie den Knauf waagrecht aus.



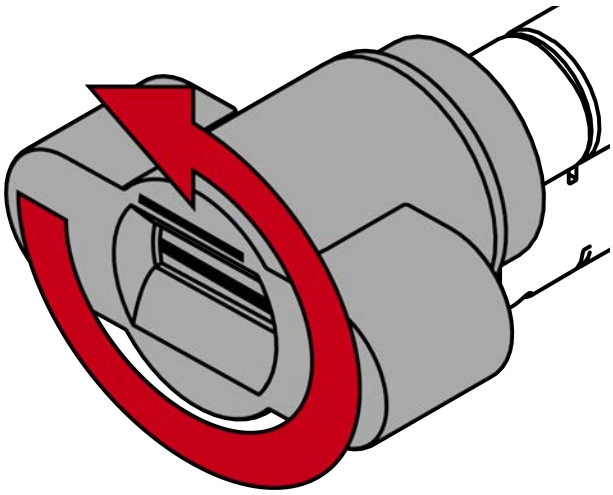
2. Setzen Sie das Spezialwerkzeug an.



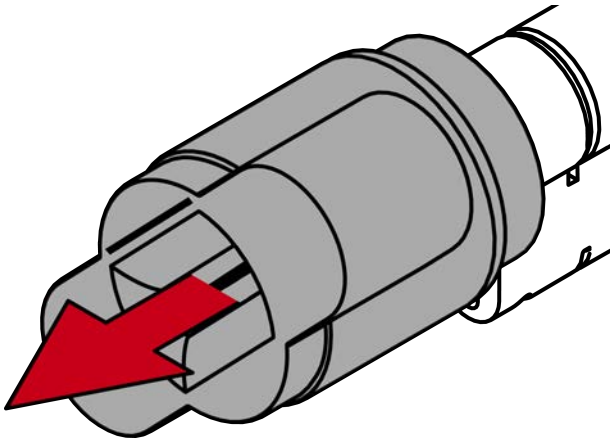
3. Richten Sie das Spezialwerkzeug so aus, dass das Logo parallel zur Aussparung ist.



4. Drehen Sie das Spezialwerkzeug und den Knauf gleichzeitig gegen den Uhrzeigersinn.

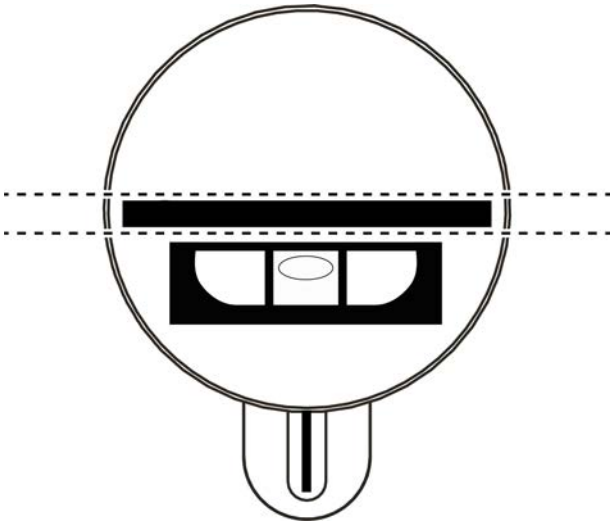


5. Ziehen Sie das Spezialwerkzeug und den Knauf gleichzeitig ab.

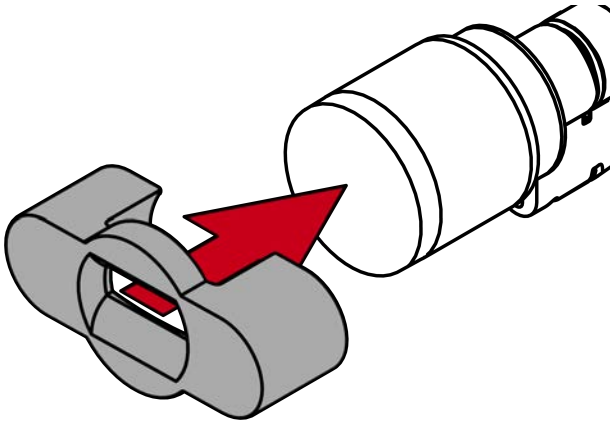


↳ Mechanischer Knauf ist demontiert.

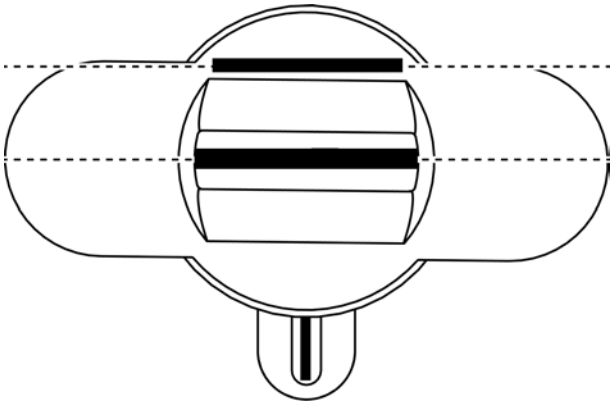
6. Richten Sie den Knauf waagrecht aus.



7. Setzen Sie das Spezialwerkzeug an.



8. Richten Sie das Spezialwerkzeug so aus, dass das Logo parallel zur Aussparung ist.



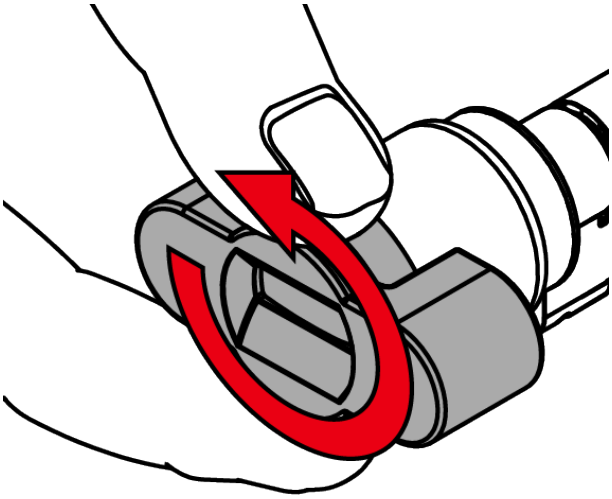
9. Halten Sie Spezialwerkzeug und Knaufkappe gleichzeitig fest und drehen Sie beides zusammen zuerst 1-2° im Uhrzeigersinn und danach gegen den Uhrzeigersinn weg.

HINWEIS

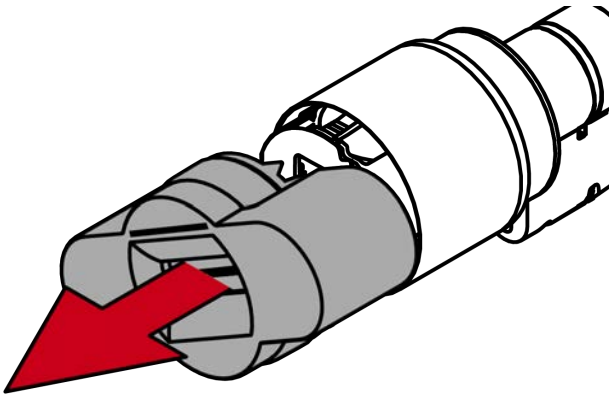
Abrutschen beim Drehen

Die Oberfläche der Knaufkappe kann rutschig sein und die Kappe sich (insbesondere bei WP-Ausführungen, erkennbar am blauen Zylinderhalsring oder der gelaserten Markierung auf der inneren Seite des Zylinderprofils) schwer drehen lassen.

- Tragen Sie rutschfeste Handschuhe.



10. Ziehen Sie das Werkzeug und die Kappe ab.



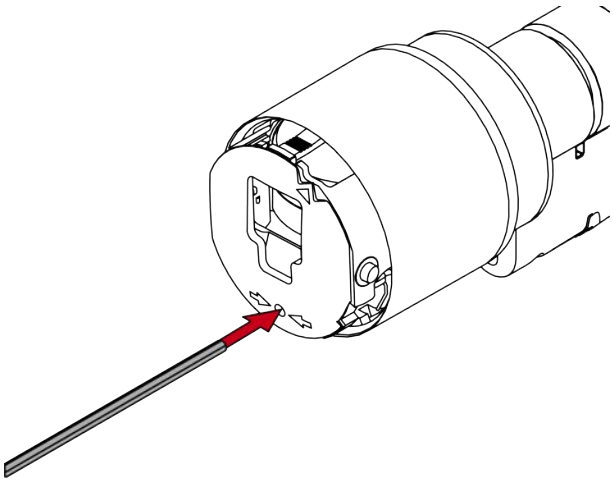
HINWEIS

Mitgelieferten Sechskantschlüssel verwenden

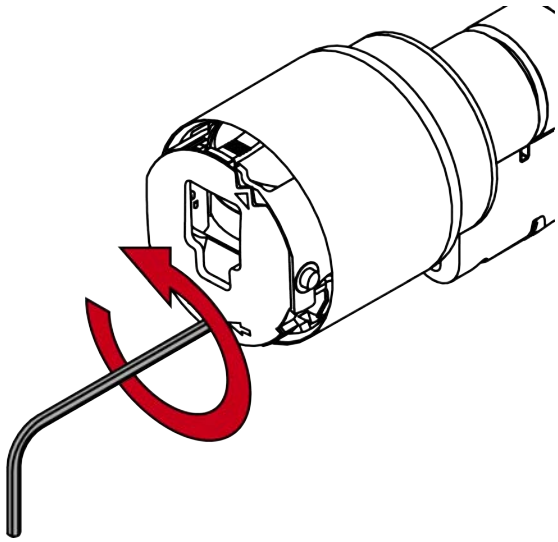
Im Lieferumfang des Spezialwerkzeugs befindet sich auch ein Sechskantschlüssel.

- Verwenden Sie diesen Sechskantschlüssel, um den elektronischen Knauf zu montieren und zu demontieren.

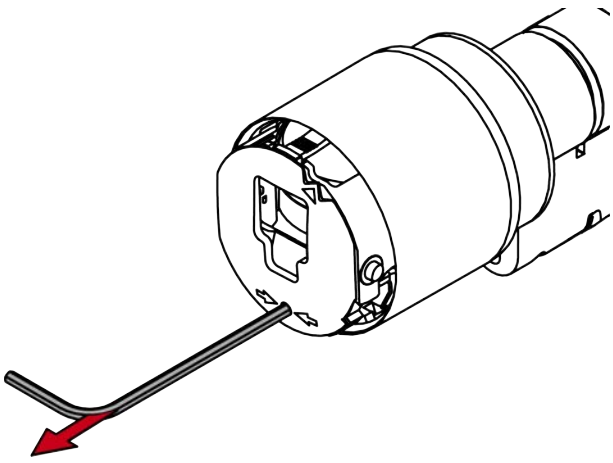
11. Stecken Sie den Sechskantschlüssel bis zum Anschlag in das dafür vorgesehene Loch.



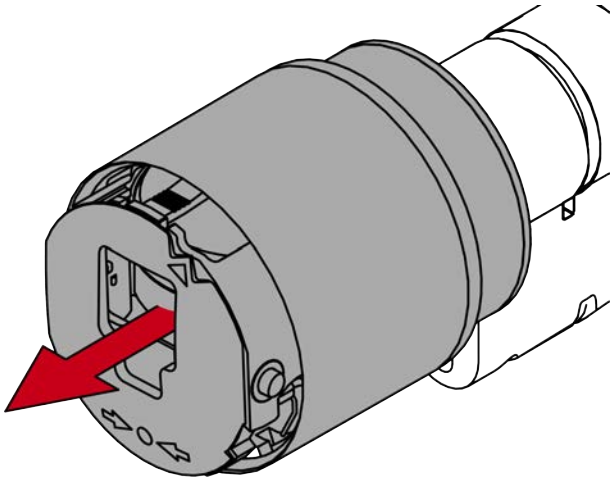
12. Drehen Sie den Sechskantschlüssel um 270 Grad gegen den Uhrzeigersinn.



13. Ziehen Sie den Sechskantschlüssel wieder heraus.

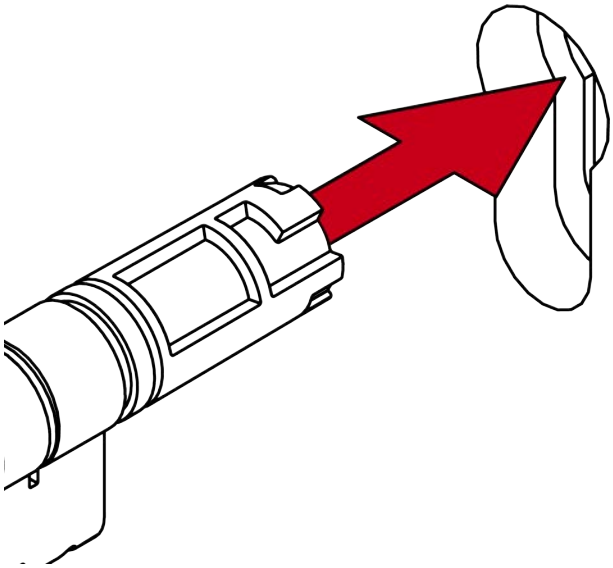


14. Ziehen Sie den Knauf ab.



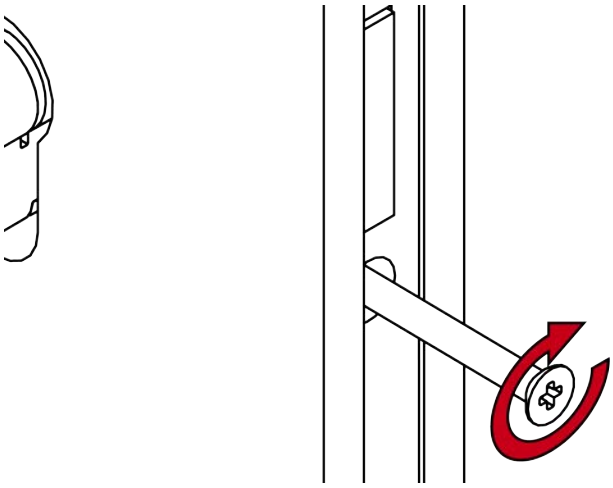
↳ Elektronischer Knauf ist demontiert.

15. Stecken Sie den SI Digital Cylinder AX in das Einsteckschloss.



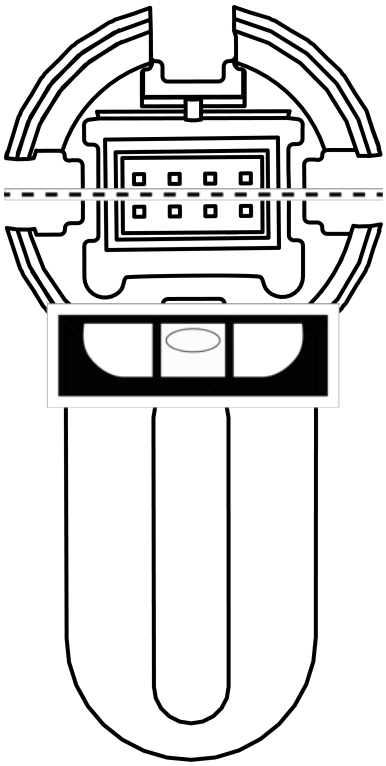
↳ SI Digital Cylinder AX ist im Einsteckschloss positioniert.

16. Schrauben Sie den SI Digital Cylinder AX mit der Stulpschraube fest.

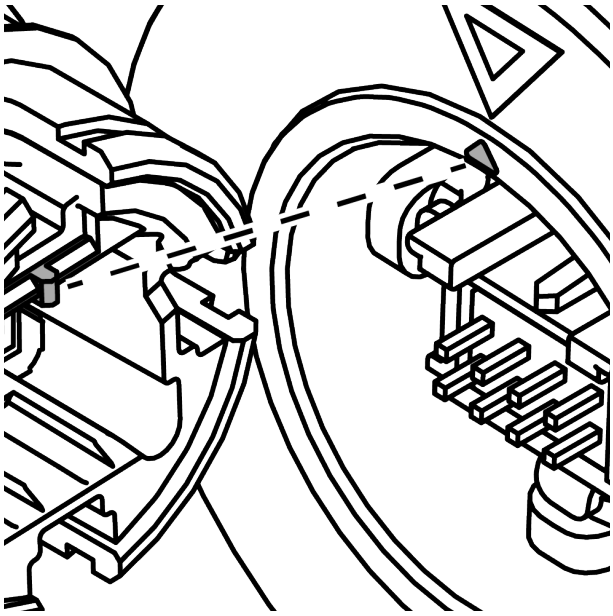


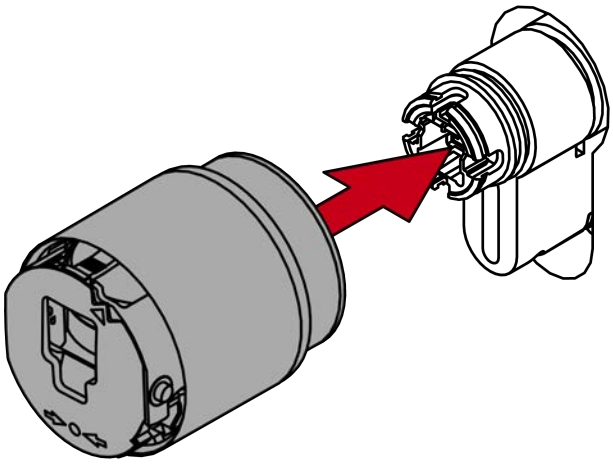
↳ SI Digital Cylinder AX ist im Einsteckschloss befestigt.

17. Montieren Sie gegebenenfalls die Blenden.
18. Richten Sie die Knaufaufnahme waagrecht aus.



19. Stecken Sie den Knauf auf.





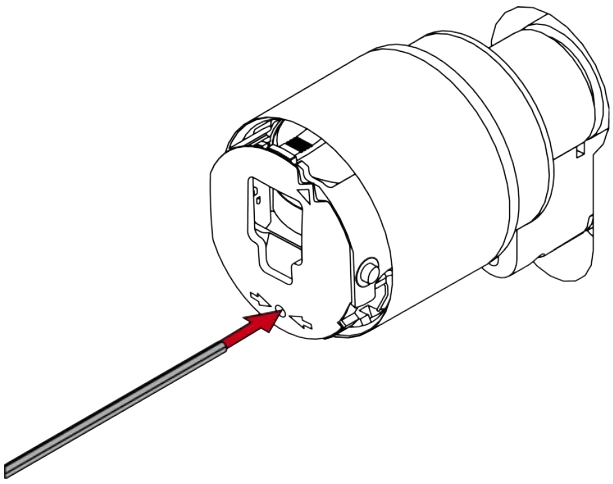
HINWEIS

Mitgelieferten Sechskantschlüssel verwenden

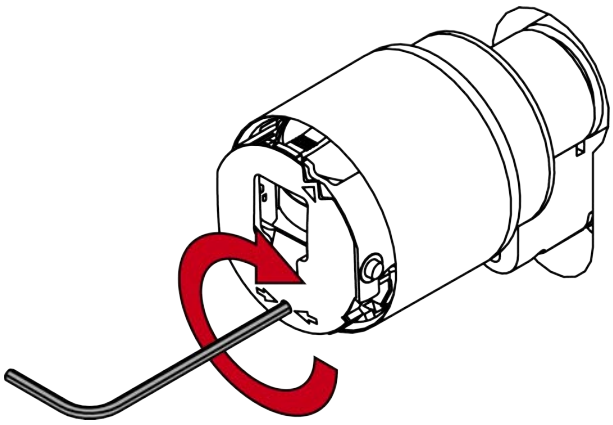
Im Lieferumfang des Spezialwerkzeugs befindet sich auch ein Sechskantschlüssel.

- Verwenden Sie diesen Sechskantschlüssel, um den elektronischen Knauf zu montieren und zu demontieren.

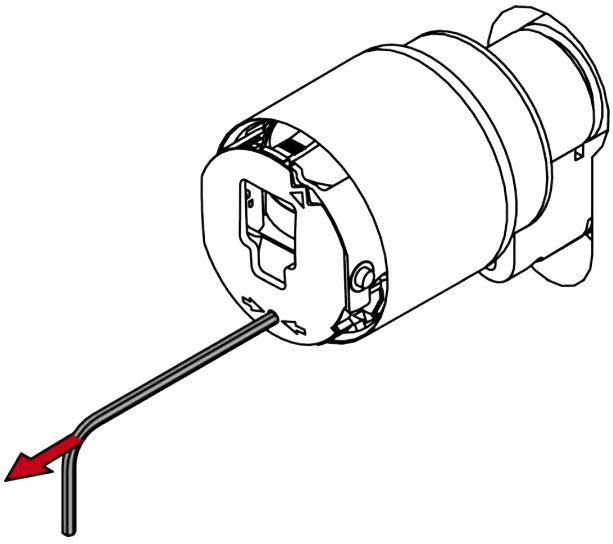
20. Stecken Sie den Sechskantschlüssel bis zum Anschlag in das dafür vorgesehene Loch.



21. Drehen Sie den Sechskantschlüssel um 270 Grad im Uhrzeigersinn.

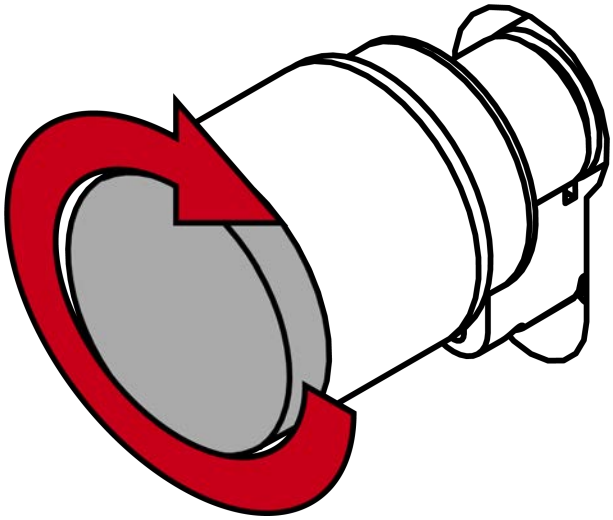


22. Ziehen Sie den Sechskantschlüssel wieder heraus.



23. Stecken Sie die Kappe auf.

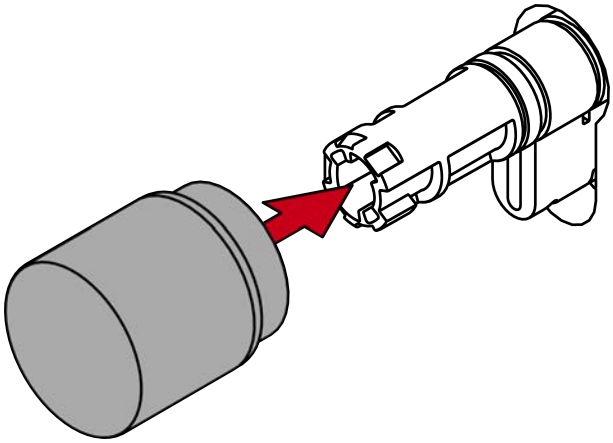
24. Drehen Sie die Kappe im Uhrzeigersinn.



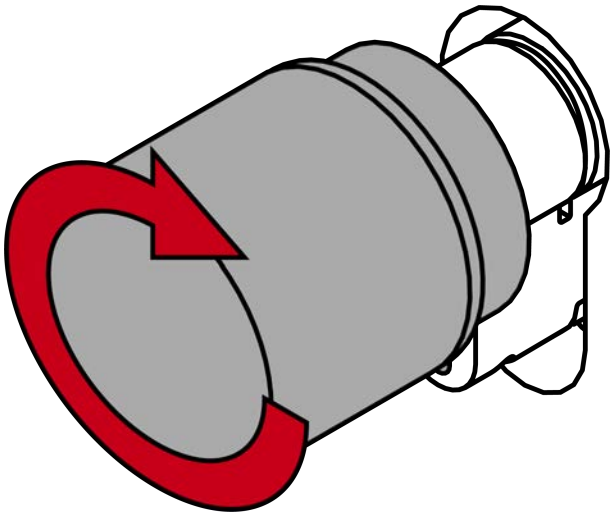
↳ Kappe rastet mit einem Klicken ein.

↳ Elektronischer Knauf ist montiert.

25. Stecken Sie den Knauf auf.



26. Drehen Sie den Knauf im Uhrzeigersinn.



↳ Knauf rastet mit einem Klicken ein.
↳ Mechanischer Knauf ist montiert.

27. Führen Sie einen Funktionstest durch (siehe *Funktionstest [▸ 86]*).
28. Führen Sie für Antipanik-Zylinder zusätzlich den Antipanik-Funktionstest durch (siehe Antipanik-Funktionstest).

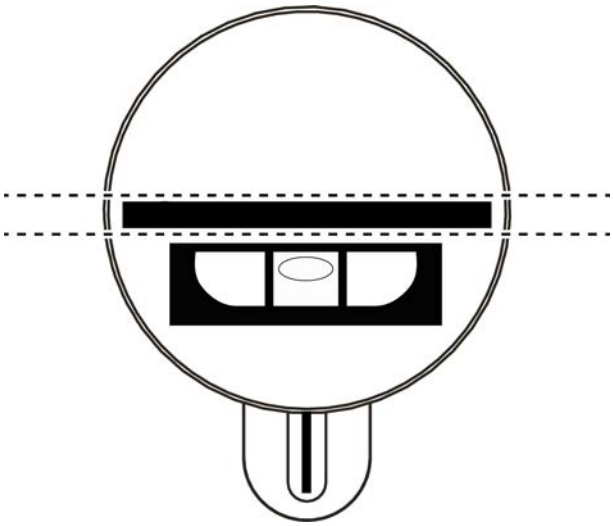
↳ SI Digital Cylinder AX ist mit Aufsteckblenden montiert.

6.5.3.2 Freidrehender Zylinder (FD, beidseitig lesend)

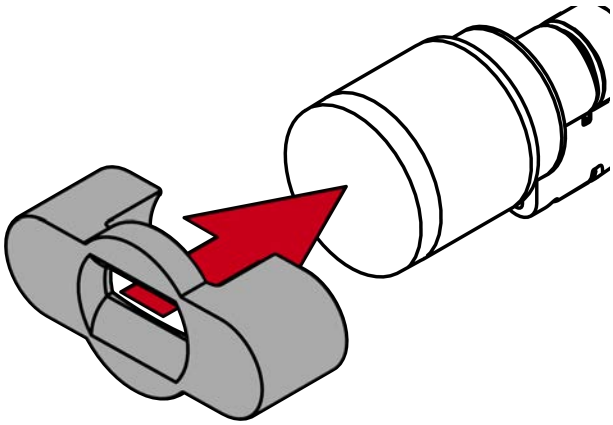
Standardmontage

- ✓ Spezialwerkzeug vorhanden.
- ✓ 1,5-mm-Sechskantschlüssel vorhanden.
- ✓ PH2-Schraubendreher vorhanden.

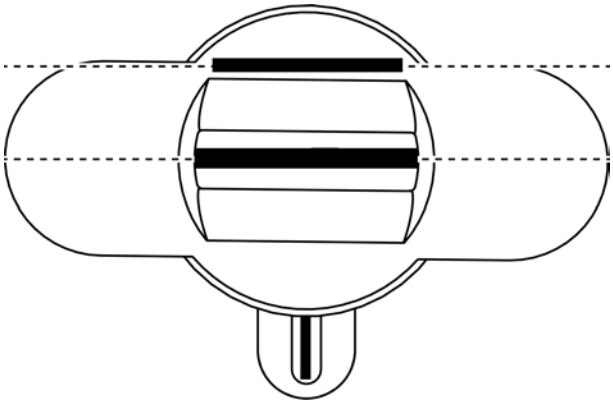
1. Richten Sie den Knauf waagrecht aus.



2. Setzen Sie das Spezialwerkzeug an.



3. Richten Sie das Spezialwerkzeug so aus, dass das Logo parallel zur Aussparung ist.



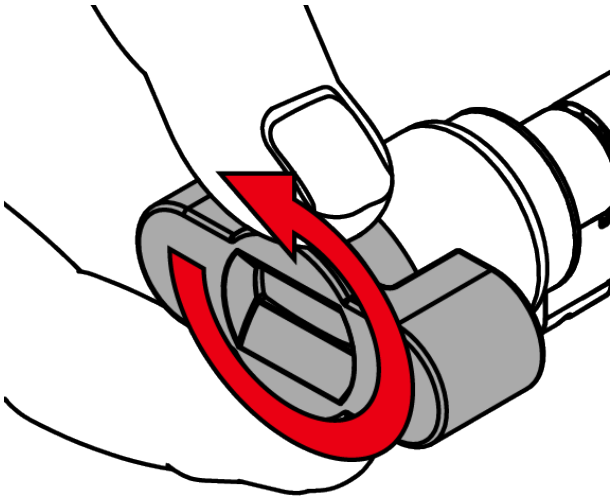
4. Halten Sie Spezialwerkzeug und Knaufkappe gleichzeitig fest und drehen Sie beides zusammen zuerst 1-2° im Uhrzeigersinn und danach gegen den Uhrzeigersinn weg.

HINWEIS

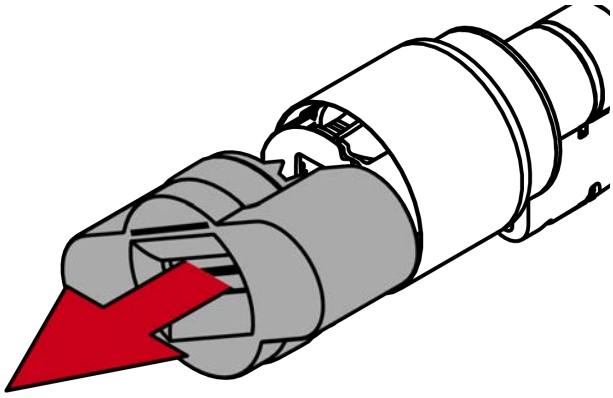
Abrutschen beim Drehen

Die Oberfläche der Knaufkappe kann rutschig sein und die Kappe sich (insbesondere bei WP-Ausführungen, erkennbar am blauen Zylinderhalsring oder der gelaserten Markierung auf der inneren Seite des Zylinderprofils) schwer drehen lassen.

- Tragen Sie rutschfeste Handschuhe.



5. Ziehen Sie das Werkzeug und die Kappe ab.



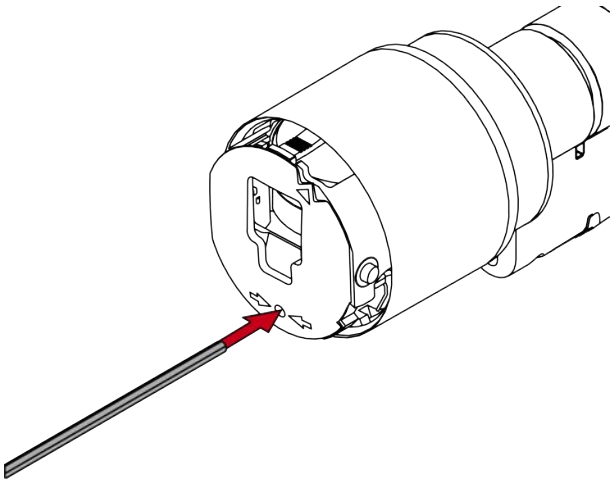
HINWEIS

Mitgelieferten Sechskantschlüssel verwenden

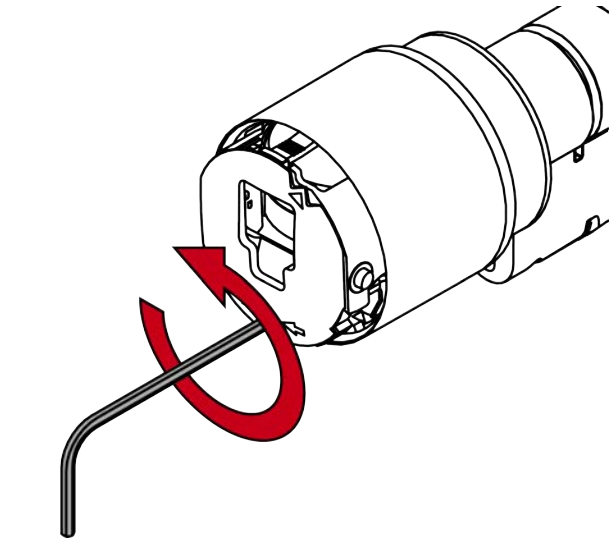
Im Lieferumfang des Spezialwerkzeugs befindet sich auch ein Sechskantschlüssel.

- Verwenden Sie diesen Sechskantschlüssel, um den elektronischen Knauf zu montieren und zu demontieren.

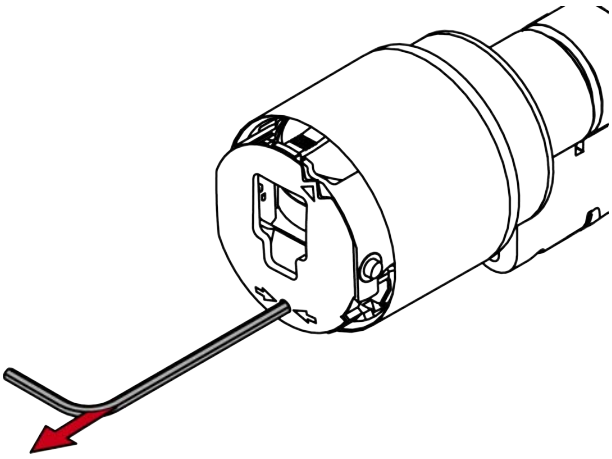
6. Stecken Sie den Sechskantschlüssel bis zum Anschlag in das dafür vorgesehene Loch.



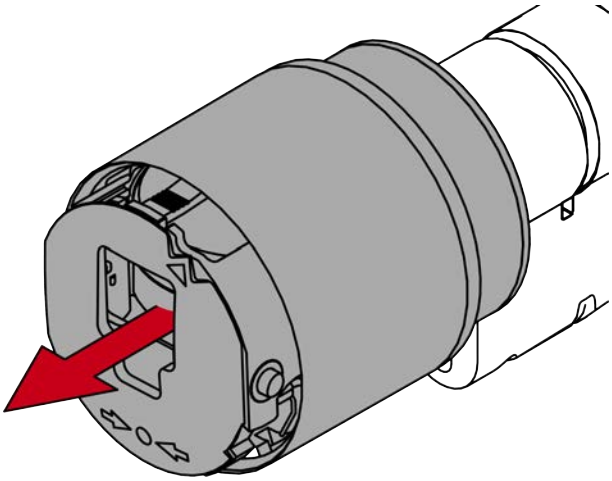
7. Drehen Sie den Sechskantschlüssel um 270 Grad gegen den Uhrzeigersinn.



8. Ziehen Sie den Sechskantschlüssel wieder heraus.

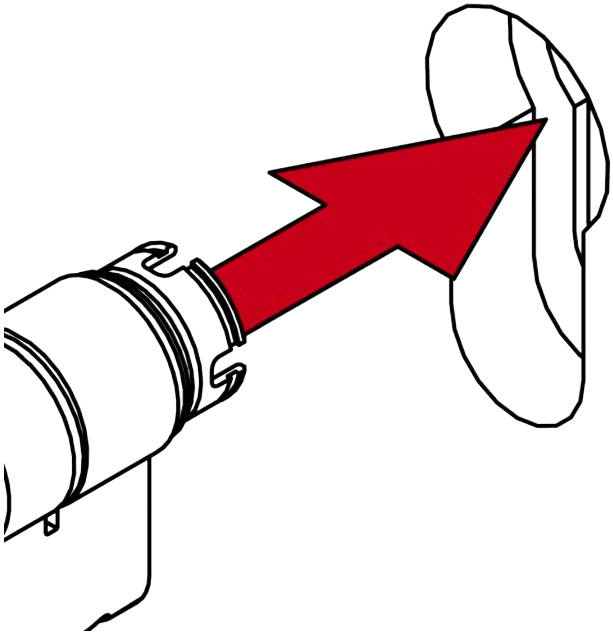


9. Ziehen Sie den Knauf ab.



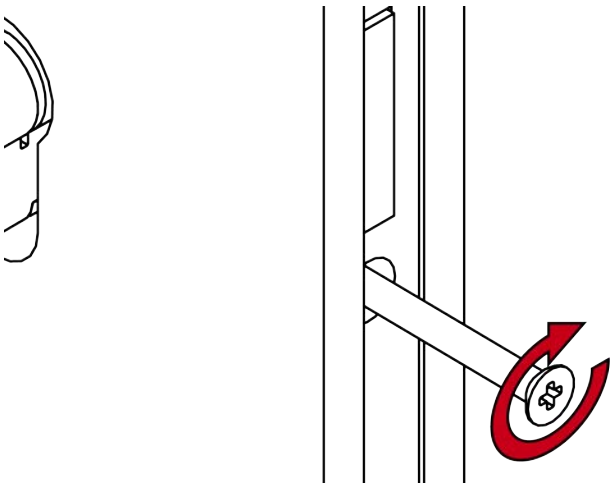
↳ Elektronischer Knauf ist demontiert.

10. Stecken Sie den SI Digital Cylinder AX mit der knauffreien Seite in das Einsteckschloss.



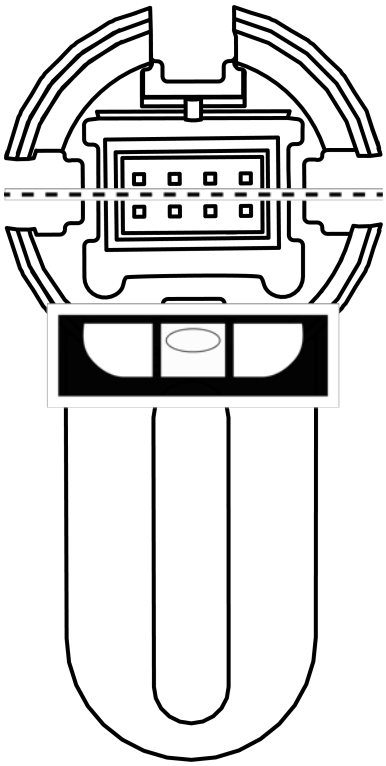
↳ SI Digital Cylinder AX ist im Einsteckschloss positioniert.

11. Schrauben Sie den SI Digital Cylinder AX mit der Stulpschraube fest.

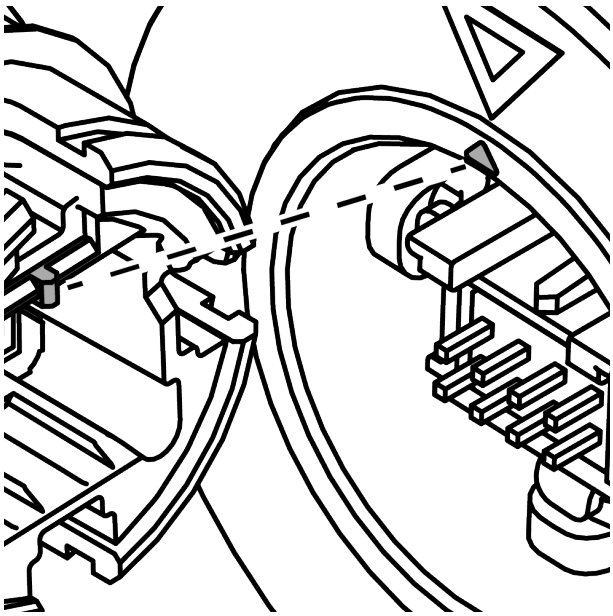


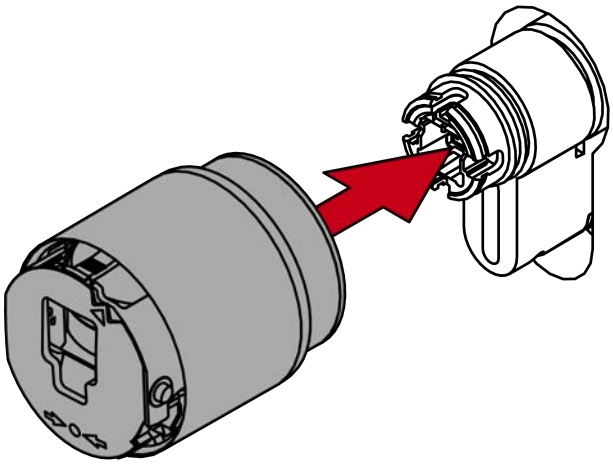
↳ SI Digital Cylinder AX ist im Einsteckschloss befestigt.

12. Richten Sie die Knaufaufnahme waagrecht aus.



13. Stecken Sie den Knauf auf.





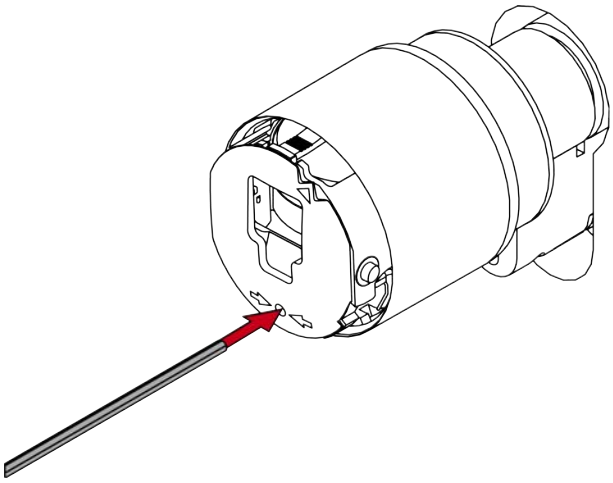
HINWEIS

Mitgelieferten Sechskantschlüssel verwenden

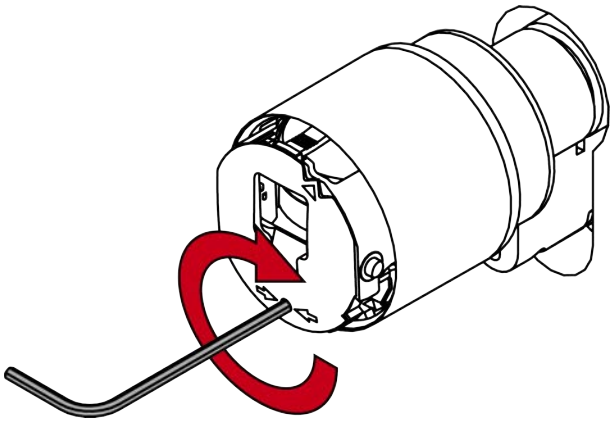
Im Lieferumfang des Spezialwerkzeugs befindet sich auch ein Sechskantschlüssel.

- Verwenden Sie diesen Sechskantschlüssel, um den elektronischen Knauf zu montieren und zu demontieren.

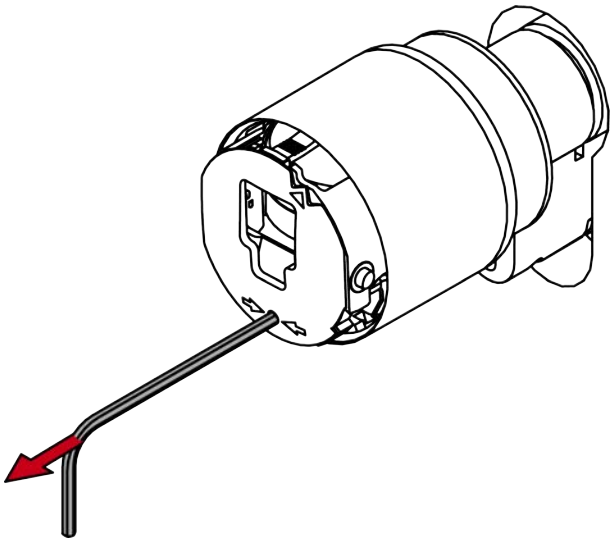
14. Stecken Sie den Sechskantschlüssel bis zum Anschlag in das dafür vorgesehene Loch.



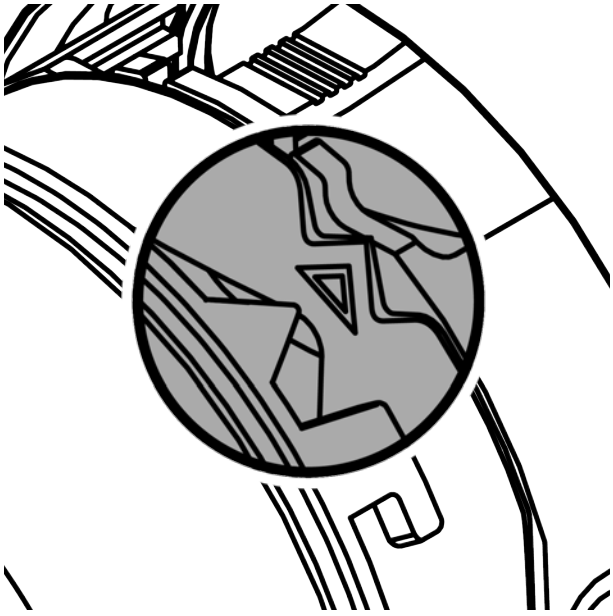
15. Drehen Sie den Sechskantschlüssel um 270 Grad im Uhrzeigersinn.

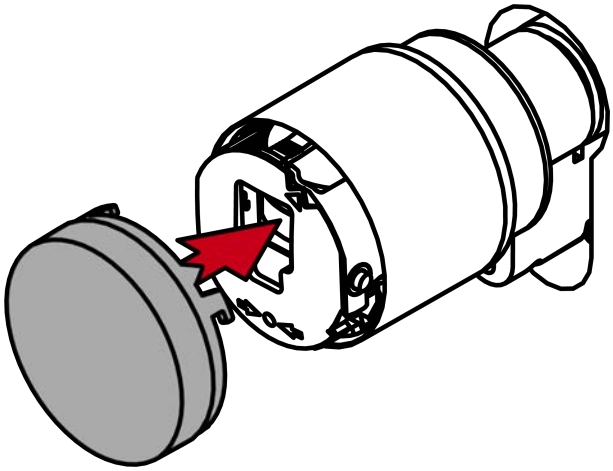


16. Ziehen Sie den Sechskantschlüssel wieder heraus.

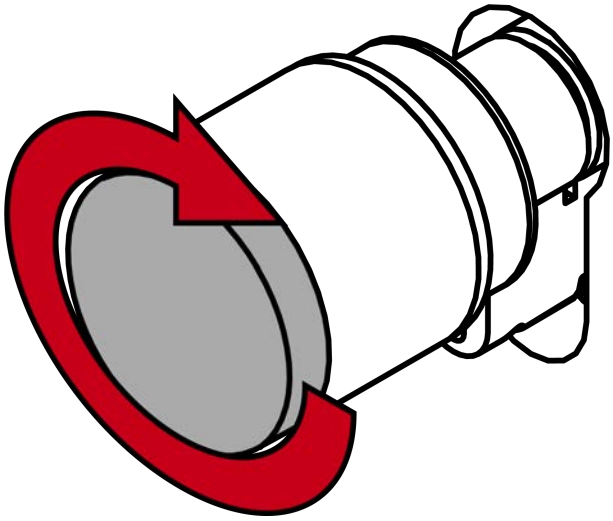


17. Stecken Sie die Kappe auf.





18. Drehen Sie die Kappe im Uhrzeigersinn.



↳ Kappe rastet mit einem Klicken ein.
↳ Elektronischer Knauf ist montiert.

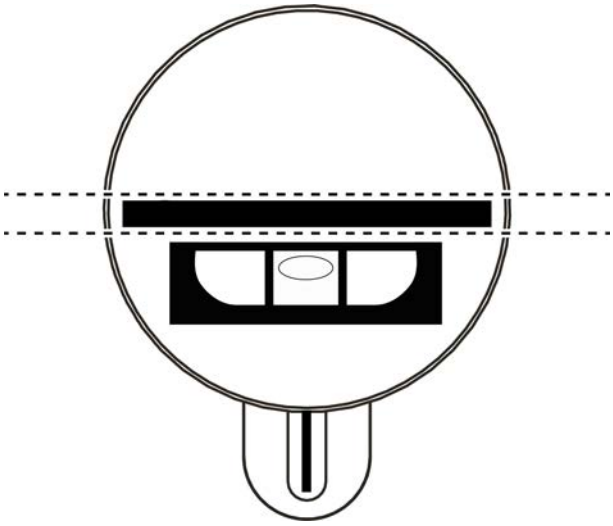
19. Führen Sie einen Funktionstest durch (siehe *Funktionstest [▸ 86]*).
20. Führen Sie für Antipanik-Zylinder zusätzlich den Antipanik-Funktionstest durch (siehe Antipanik-Funktionstest).

↳ SI Digital Cylinder AX ist fertig montiert.

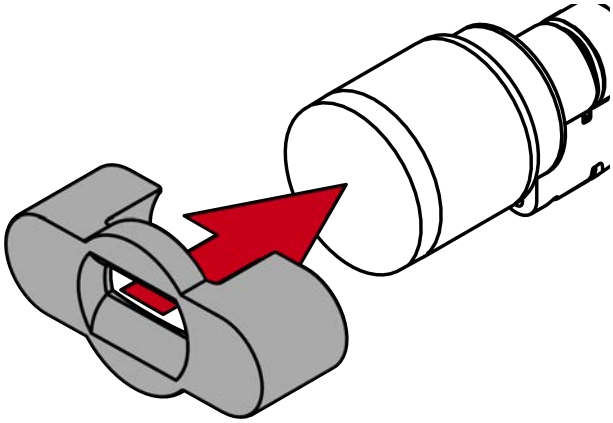
Montage mit Aufsteckblenden

- ✓ Spezialwerkzeug vorhanden.
- ✓ 1,5-mm-Sechskantschlüssel vorhanden.
- ✓ PH2-Schraubendreher vorhanden.

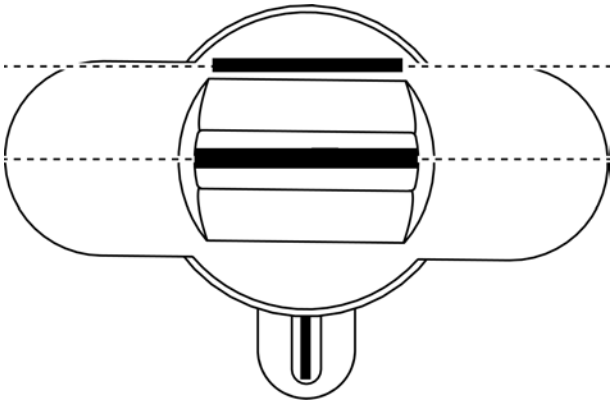
1. Richten Sie den Knauf waagrecht aus.



2. Setzen Sie das Spezialwerkzeug an.



3. Richten Sie das Spezialwerkzeug so aus, dass das Logo parallel zur Aussparung ist.



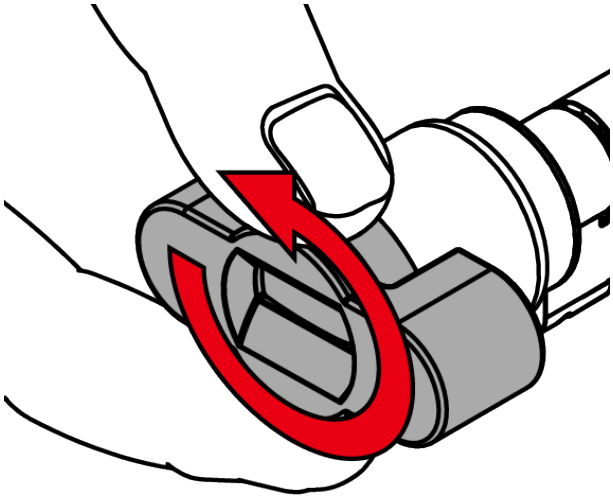
4. Halten Sie Spezialwerkzeug und Knaufkappe gleichzeitig fest und drehen Sie beides zusammen zuerst 1-2° im Uhrzeigersinn und danach gegen den Uhrzeigersinn weg.

HINWEIS

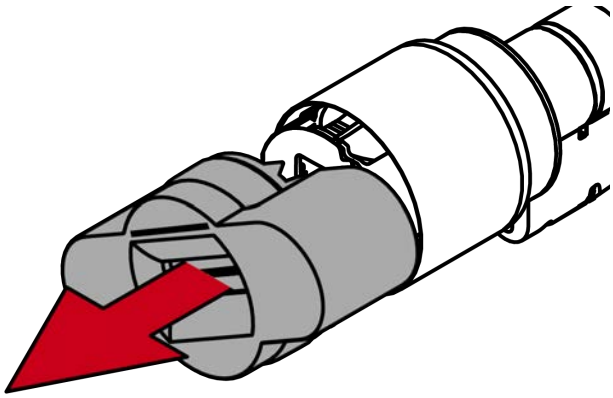
Abrutschen beim Drehen

Die Oberfläche der Knaufkappe kann rutschig sein und die Kappe sich (insbesondere bei WP-Ausführungen, erkennbar am blauen Zylinderhalsring oder der gelaserten Markierung auf der inneren Seite des Zylinderprofils) schwer drehen lassen.

- Tragen Sie rutschfeste Handschuhe.



5. Ziehen Sie das Werkzeug und die Kappe ab.



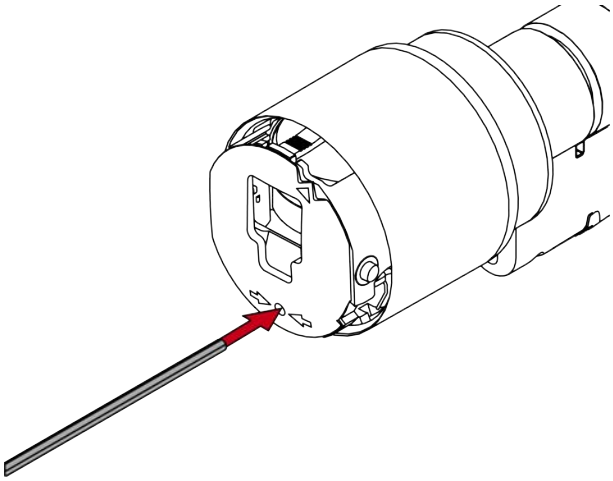
HINWEIS

Mitgelieferten Sechskantschlüssel verwenden

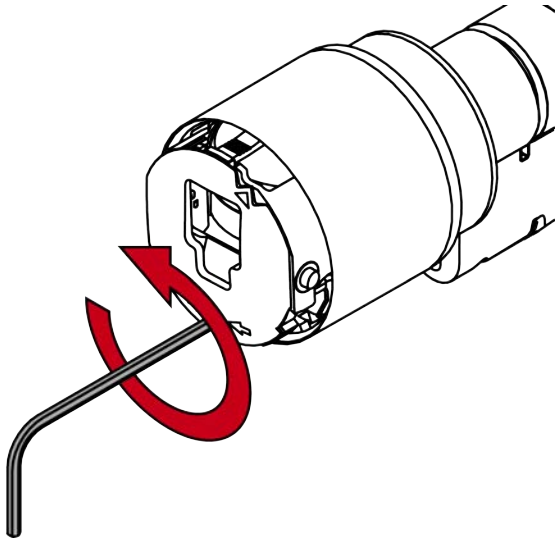
Im Lieferumfang des Spezialwerkzeugs befindet sich auch ein Sechskantschlüssel.

- Verwenden Sie diesen Sechskantschlüssel, um den elektronischen Knauf zu montieren und zu demontieren.

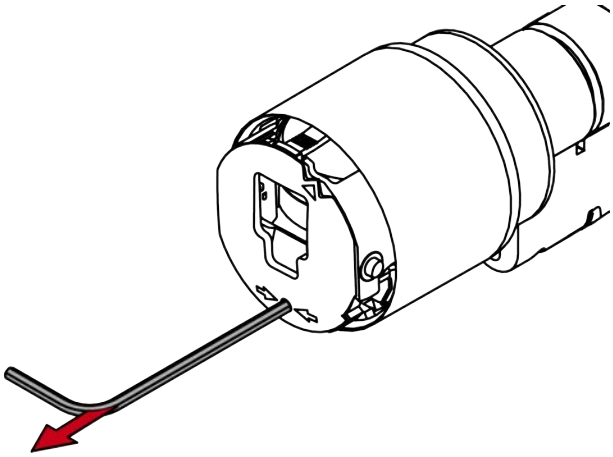
6. Stecken Sie den Sechskantschlüssel bis zum Anschlag in das dafür vorgesehene Loch.



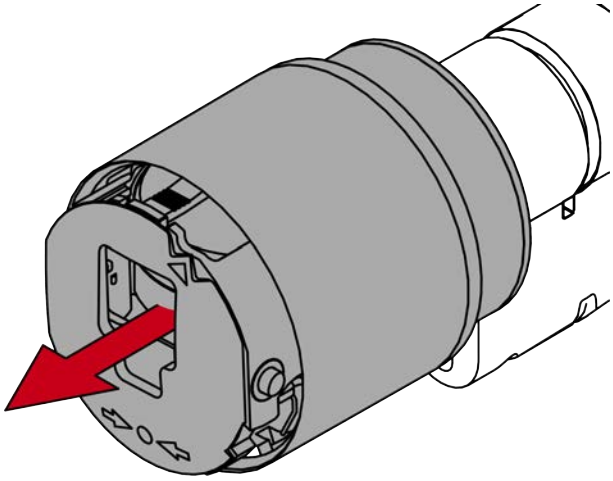
7. Drehen Sie den Sechskantschlüssel um 270 Grad gegen den Uhrzeigersinn.



8. Ziehen Sie den Sechskantschlüssel wieder heraus.



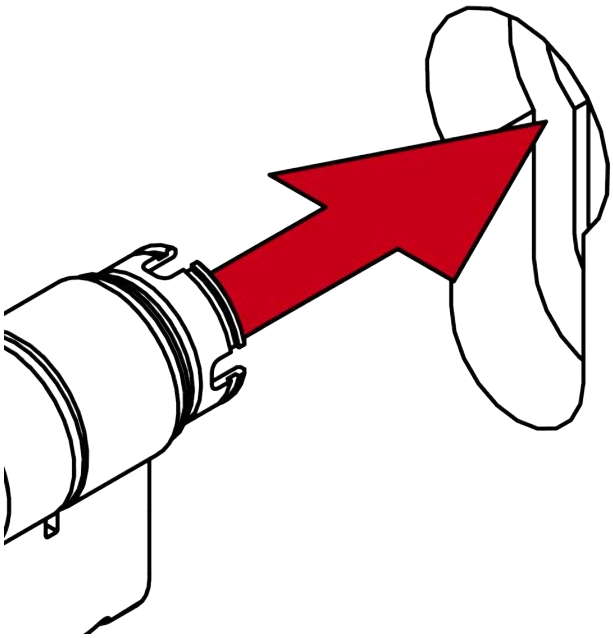
9. Ziehen Sie den Knauf ab.



↳ Elektronischer Knauf ist demontiert.

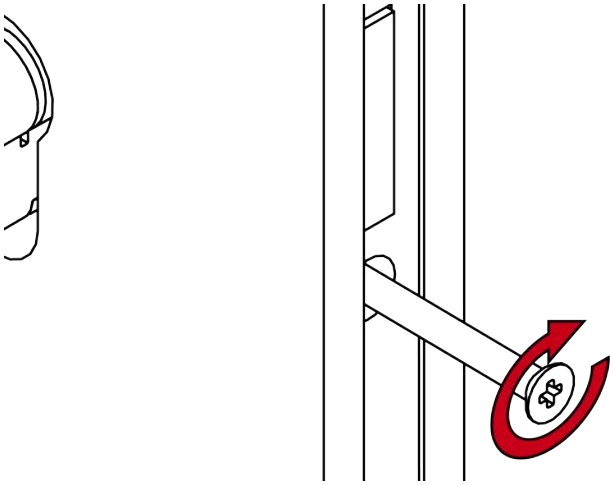
10. Demontieren Sie auch den anderen Knauf.

11. Stecken Sie den SI Digital Cylinder AX in das Einsteckschloss.



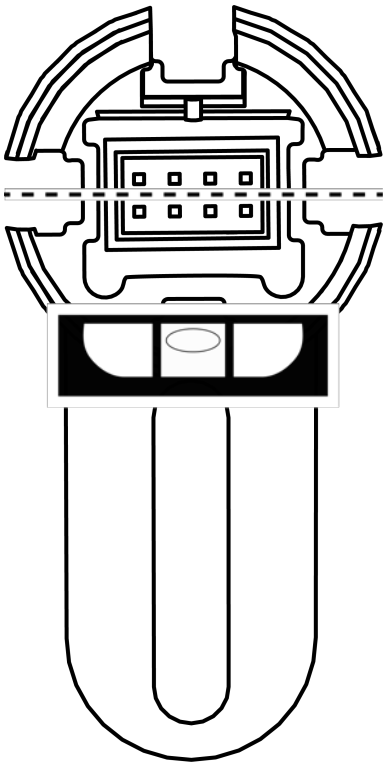
↳ SI Digital Cylinder AX ist im Einsteckschloss positioniert.

12. Schrauben Sie den SI Digital Cylinder AX mit der Stulpschraube fest.

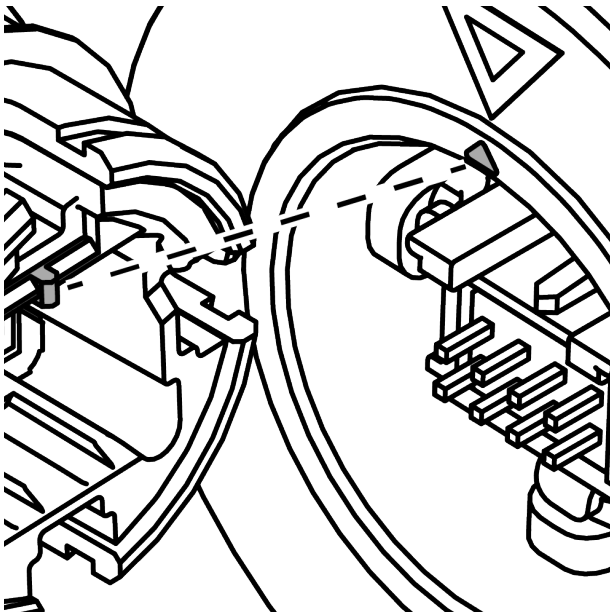


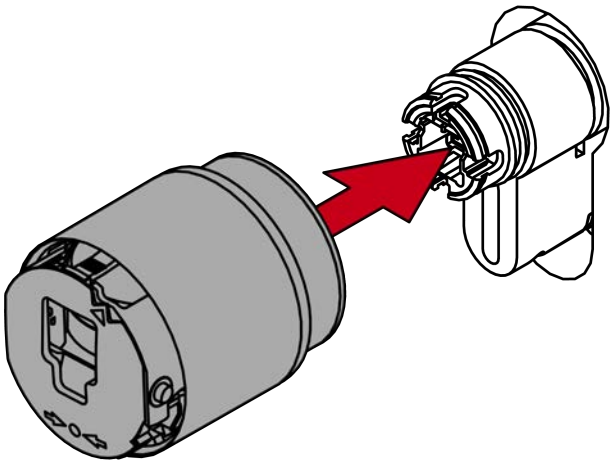
13. Montieren Sie gegebenenfalls die Blenden.

14. Richten Sie die Knaufaufnahme waagrecht aus.



15. Stecken Sie den Knauf auf.





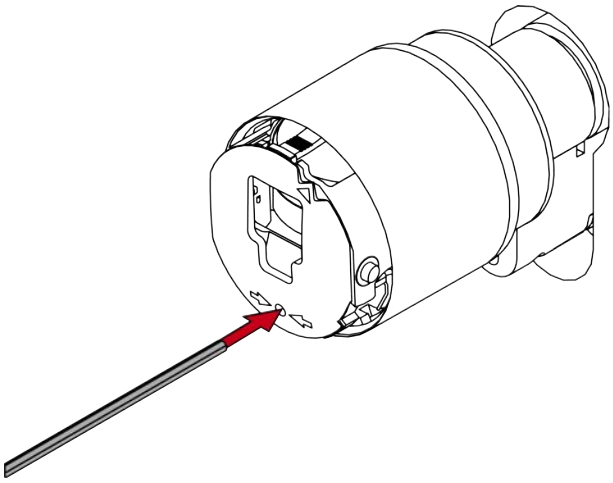
HINWEIS

Mitgelieferten Sechskantschlüssel verwenden

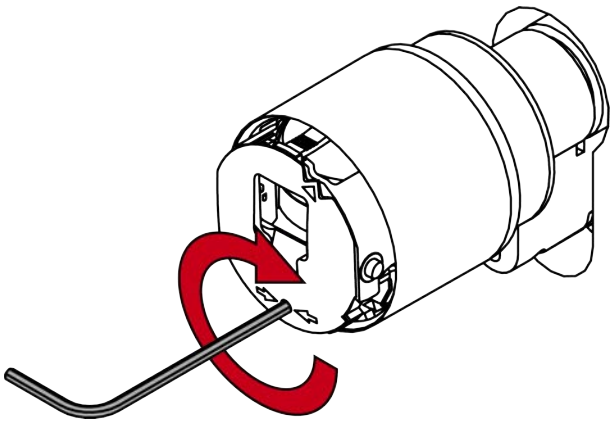
Im Lieferumfang des Spezialwerkzeugs befindet sich auch ein Sechskantschlüssel.

- Verwenden Sie diesen Sechskantschlüssel, um den elektronischen Knauf zu montieren und zu demontieren.

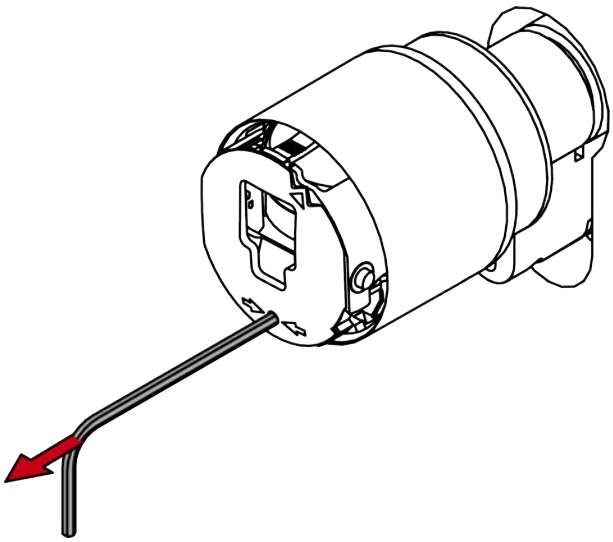
16. Stecken Sie den Sechskantschlüssel bis zum Anschlag in das dafür vorgesehene Loch.



17. Drehen Sie den Sechskantschlüssel um 270 Grad gegen den Uhrzeigersinn.

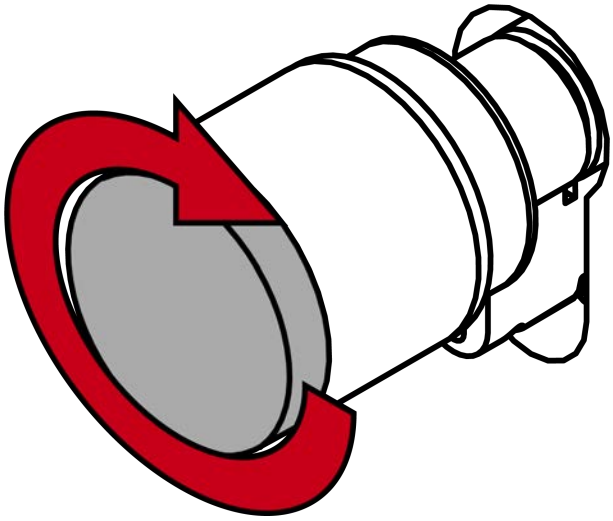


18. Ziehen Sie den Sechskantschlüssel wieder heraus.



19. Stecken Sie die Kappe auf.

20.Drehen Sie die Kappe im Uhrzeigersinn.



↳ Kappe rastet mit einem Klicken ein.

↳ Elektronischer Knauf ist montiert.

21. Montieren Sie ebenso den anderen elektronischen Knauf.
22. Führen Sie einen Funktionstest durch (siehe *Funktionstest [▸ 86]*).
23. Führen Sie für Antipanik-Zylinder zusätzlich den Antipanik-Funktionstest durch (siehe Antipanik-Funktionstest).

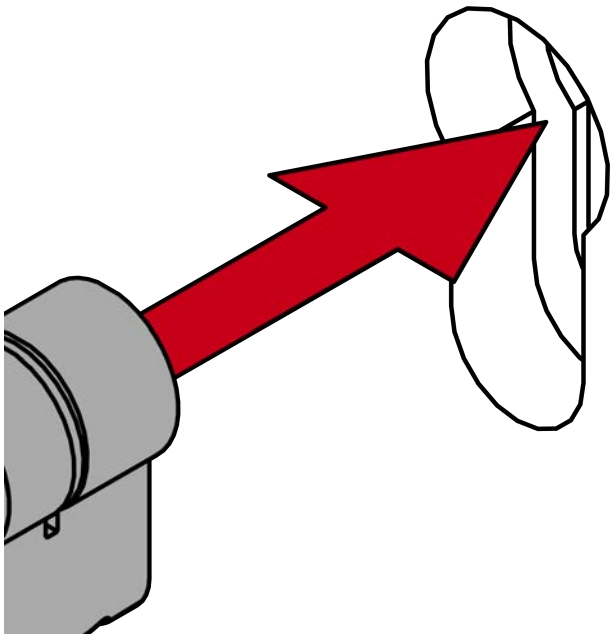
↳ SI Digital Cylinder AX ist mit Aufsteckblenden montiert.

6.5.3.3 Halbzylinder (HZ, einseitig lesend)

Standardmontage

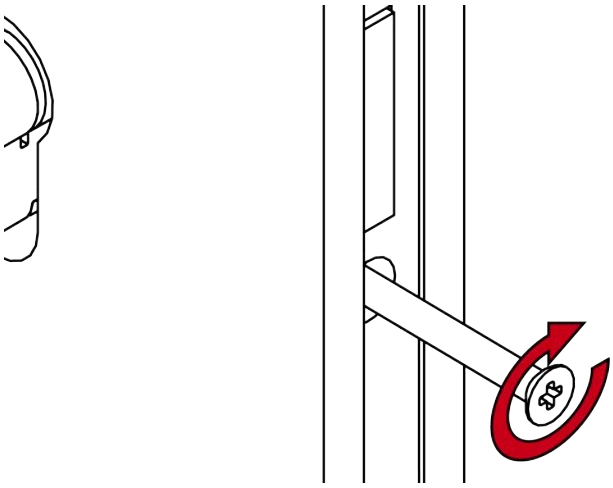
✓ PH2-Schraubendreher vorhanden.

1. Stecken Sie den SI Digital Cylinder AX mit der knauffreien Seite in das Einsteckschloss.



↳ SI Digital Cylinder AX ist im Einsteckschloss positioniert.

2. Schrauben Sie den SI Digital Cylinder AX mit der Stulpschraube fest.



↳ SI Digital Cylinder AX ist im Einsteckschloss befestigt.

↳ SI Digital Cylinder AX ist fertig montiert.

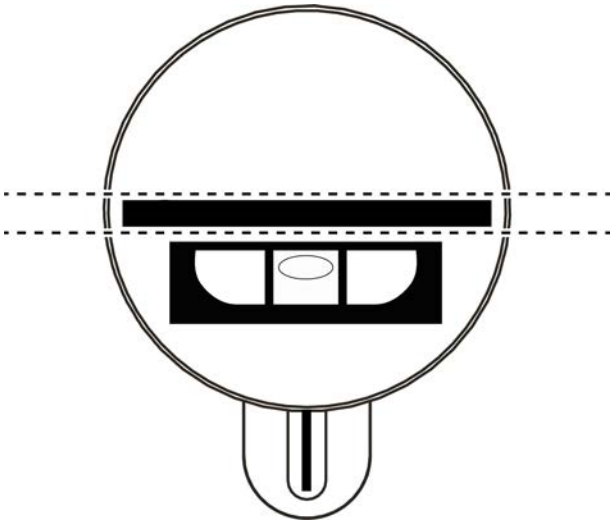
Montage mit Aufsteckblende

✓ Spezialwerkzeug vorhanden.

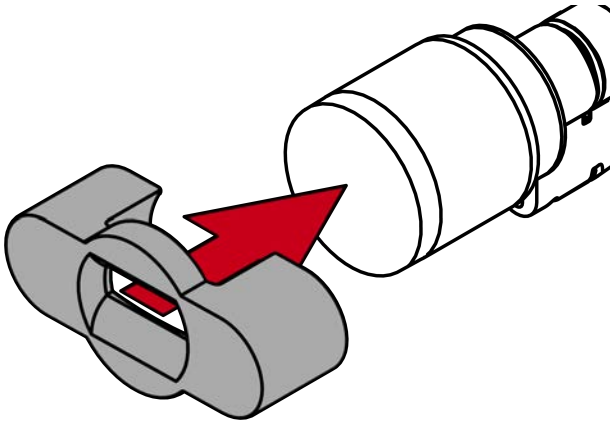
✓ 1,5-mm-Sechskantschlüssel vorhanden.

✓ PH2-Schraubendreher vorhanden.

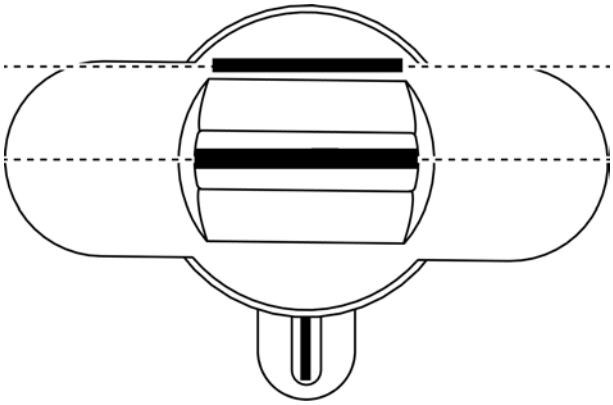
1. Richten Sie den Knauf waagrecht aus.



2. Setzen Sie das Spezialwerkzeug an.



3. Richten Sie das Spezialwerkzeug so aus, dass das Logo parallel zur Aussparung ist.



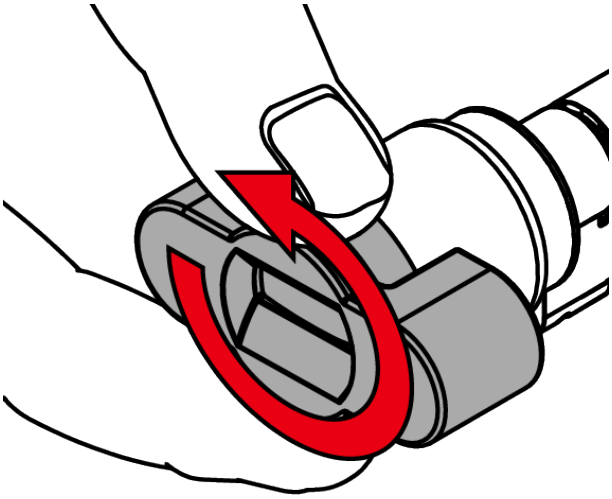
4. Halten Sie Spezialwerkzeug und Knaufkappe gleichzeitig fest und drehen Sie beides zusammen zuerst 1-2° im Uhrzeigersinn und danach gegen den Uhrzeigersinn weg.

HINWEIS

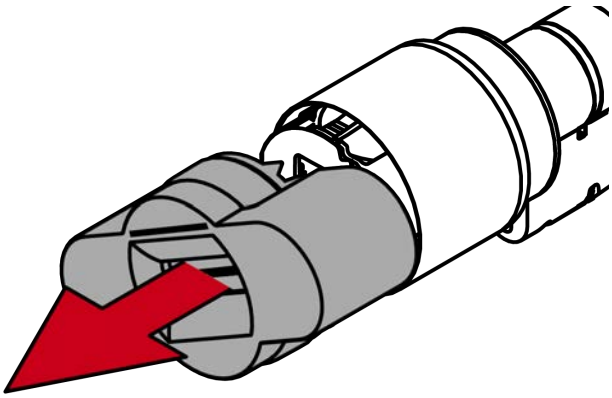
Abrutschen beim Drehen

Die Oberfläche der Knaufkappe kann rutschig sein und die Kappe sich (insbesondere bei WP-Ausführungen, erkennbar am blauen Zylinderhalsring oder der gelaserten Markierung auf der inneren Seite des Zylinderprofils) schwer drehen lassen.

- Tragen Sie rutschfeste Handschuhe.



5. Ziehen Sie das Werkzeug und die Kappe ab.



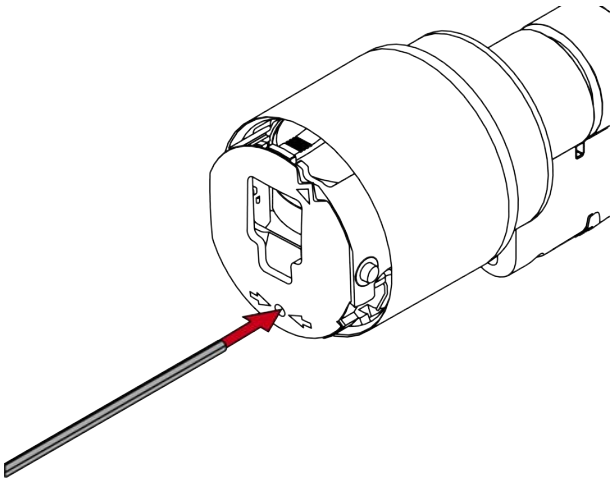
HINWEIS

Mitgelieferten Sechskantschlüssel verwenden

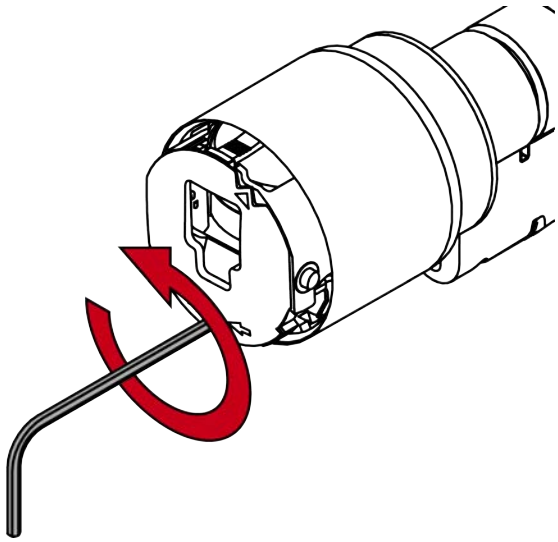
Im Lieferumfang des Spezialwerkzeugs befindet sich auch ein Sechskantschlüssel.

- Verwenden Sie diesen Sechskantschlüssel, um den elektronischen Knauf zu montieren und zu demontieren.

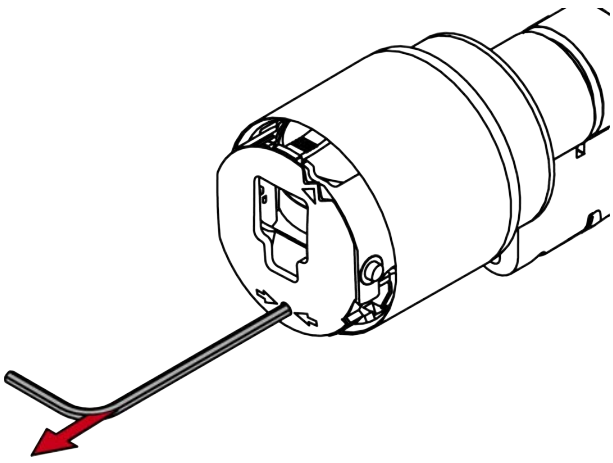
6. Stecken Sie den Sechskantschlüssel bis zum Anschlag in das dafür vorgesehene Loch.



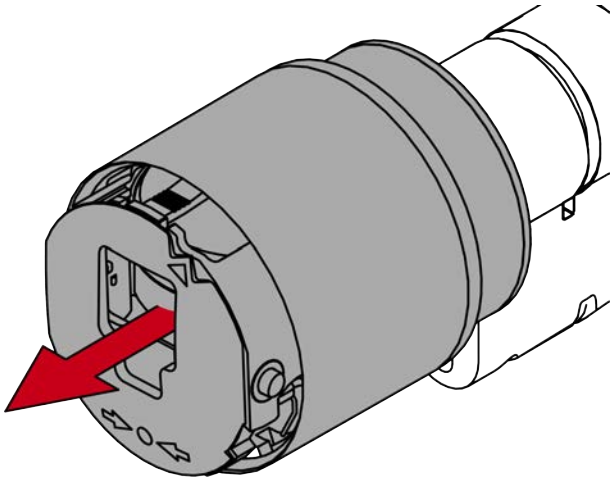
7. Drehen Sie den Sechskantschlüssel um 270 Grad gegen den Uhrzeigersinn.



8. Ziehen Sie den Sechskantschlüssel wieder heraus.

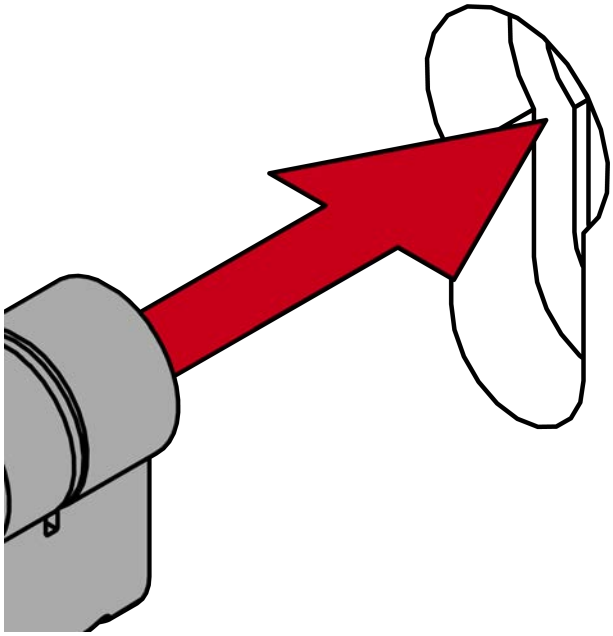


9. Ziehen Sie den Knauf ab.

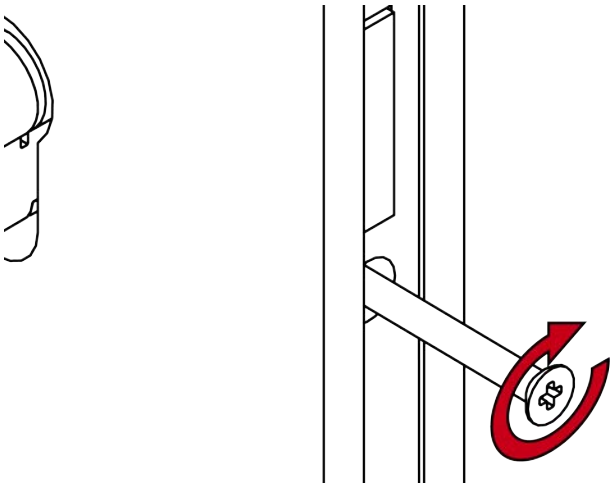


↳ Elektronischer Knauf ist demontiert.

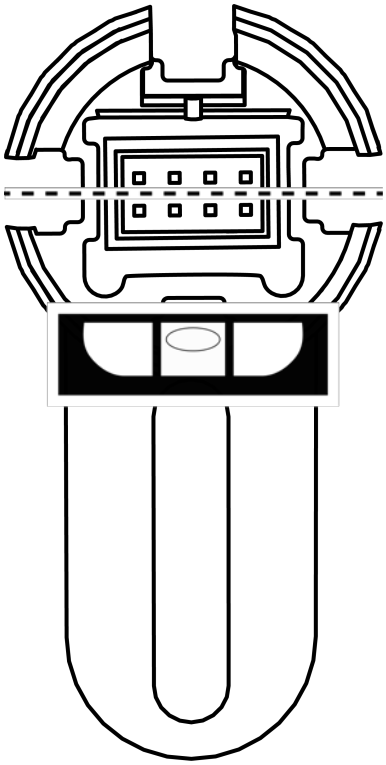
10. Stecken Sie den SI Digital Cylinder AX in das Einsteckschloss.



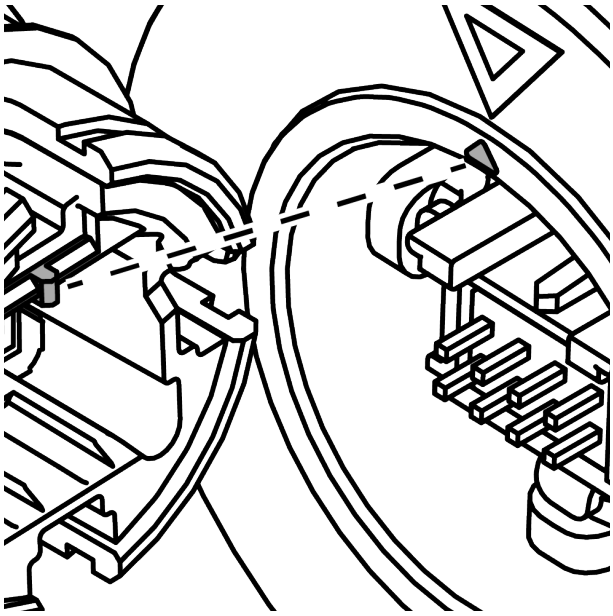
11. Schrauben Sie den SI Digital Cylinder AX mit der Stulpschraube fest.

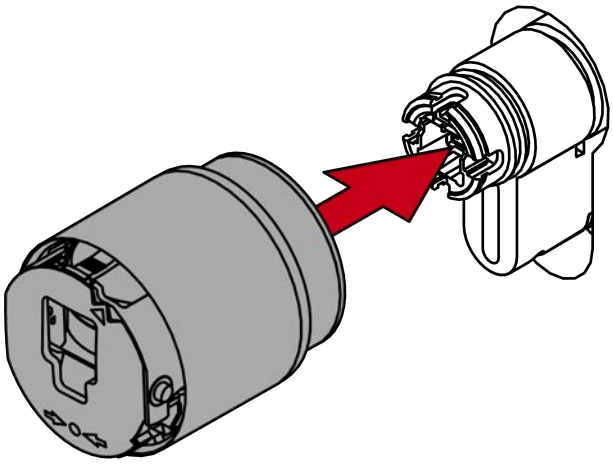


12. Montieren Sie gegebenenfalls die Blenden.
13. Richten Sie die Knaufaufnahme waagrecht aus.



14. Stecken Sie den Knauf auf.





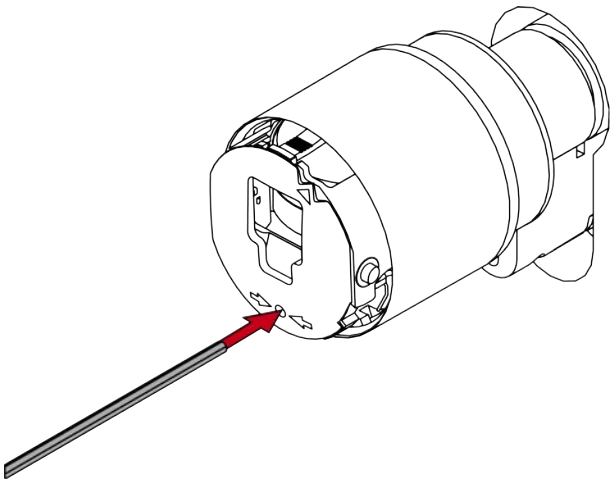
HINWEIS

Mitgelieferten Sechskantschlüssel verwenden

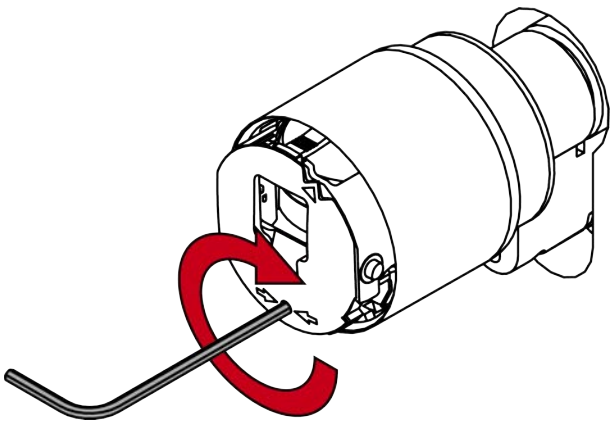
Im Lieferumfang des Spezialwerkzeugs befindet sich auch ein Sechskantschlüssel.

- Verwenden Sie diesen Sechskantschlüssel, um den elektronischen Knauf zu montieren und zu demontieren.

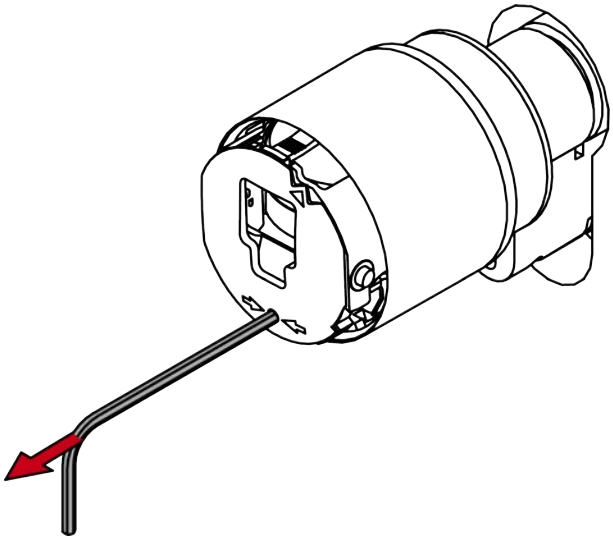
15. Stecken Sie den Sechskantschlüssel bis zum Anschlag in das dafür vorgesehene Loch.



16. Drehen Sie den Sechskantschlüssel um 270 Grad gegen den Uhrzeigersinn.

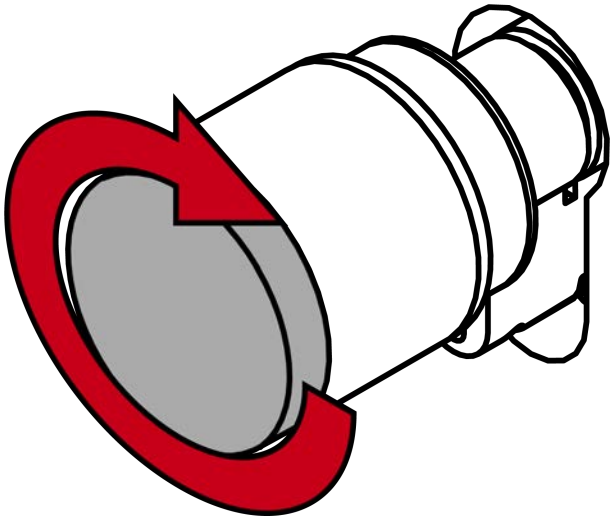


17. Ziehen Sie den Sechskantschlüssel wieder heraus.



18. Stecken Sie die Kappe auf.

19. Drehen Sie die Kappe im Uhrzeigersinn.



↳ Kappe rastet mit einem Klicken ein.

↳ Elektronischer Knauf ist montiert.

20. Führen Sie einen Funktionstest durch (siehe *Funktionstest [▸ 86]*).
21. Führen Sie für Antipanik-Zylinder zusätzlich den Antipanik-Funktionstest durch (siehe Antipanik-Funktionstest).

↳ SI Digital Cylinder AX ist mit Aufsteckblende montiert.

6.5.3.4 Scandinavian Oval/Round (SO/RS)

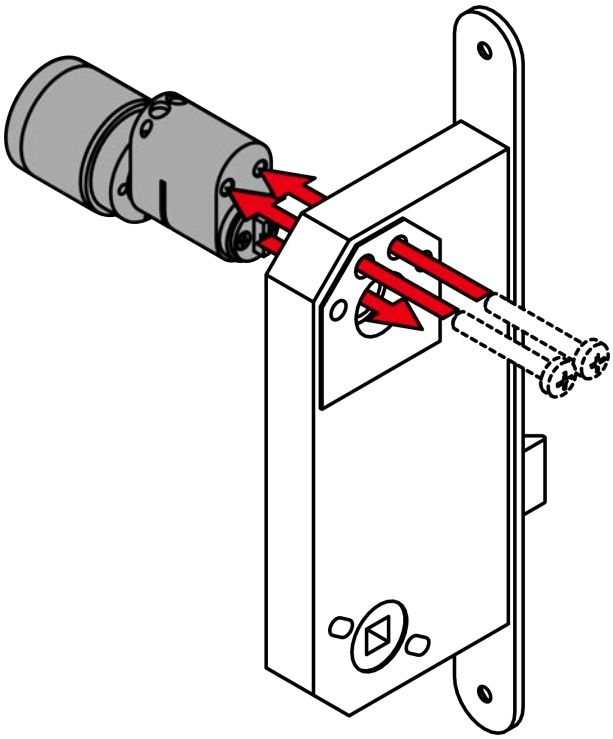
HINWEIS

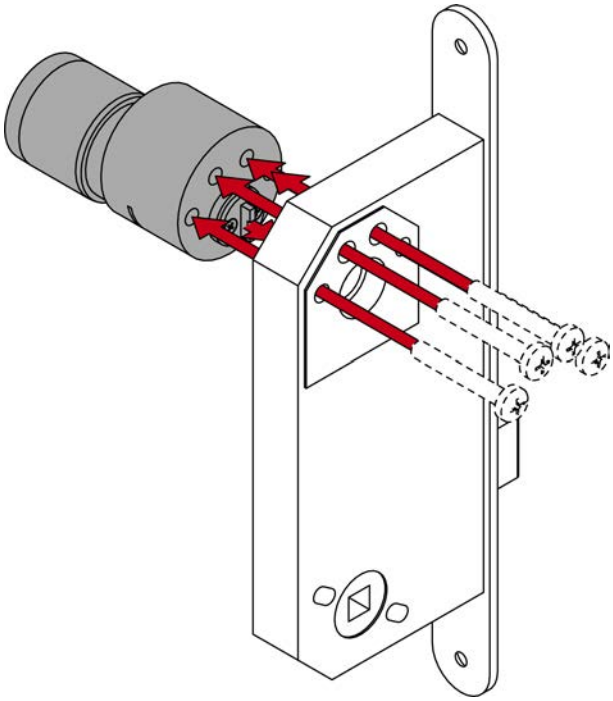
Auflagen zur SSF-Zulassung

Die Zulassung des SI Digital Cylinder AX ist an folgende Auflagen gebunden:

1. Montieren Sie den SSF-zugelassenen SI Digital Cylinder AX zusammen mit einem Schutzbeschlag nach SSF 1096 / SSF 3522.
2. Befestigen Sie den SSF-zugelassenen SI Digital Cylinder AX mit Schrauben, die einen nach SSF 1091 zulässigen Schraubenantrieb haben.

Montage





ACHTUNG

Unbefugter Zutritt durch Aufbohren auf Innenseite

Die Außenseite der SI Digital Cylinder AX ist je nach Ausführung auf der Außenseite mit einem Bohrschutz ausgerüstet.

- Wenn Sie am Zylinderkörper eine Markierung der Innenseite (*IN*) finden, dann montieren Sie den SI Digital Cylinder AX so, dass sich diese Seite in einem geschützten Bereich befindet.

✓ Rosetten ggfs. bereits montiert.

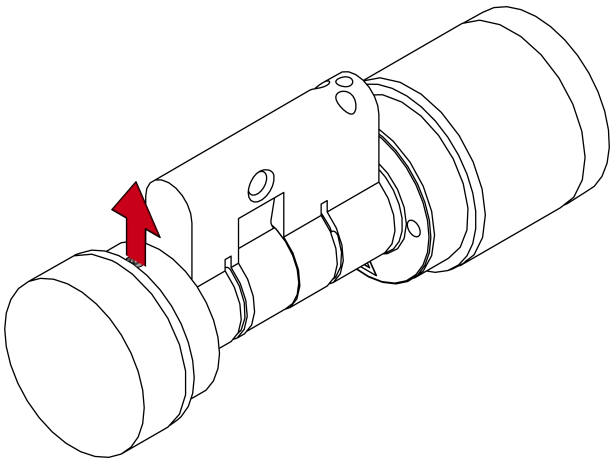
1. Stecken Sie den SI Digital Cylinder AX mit dem Mitnehmer in die Aufnahme des Einsteckschlosses.
2. Schrauben Sie den SI Digital Cylinder AX fest.
3. Montieren Sie ggfs. weitere Beschlagteile.

↳ SI Digital Cylinder AX montiert.

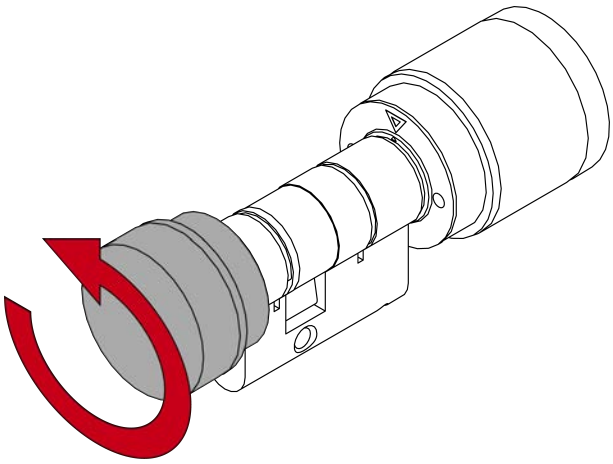
6.5.3.5 Glastürzylinder AX montieren

- ✓ 1,5-mm-Sechskantschlüssel vorhanden.
- ✓ PH2-Schraubendreher vorhanden.

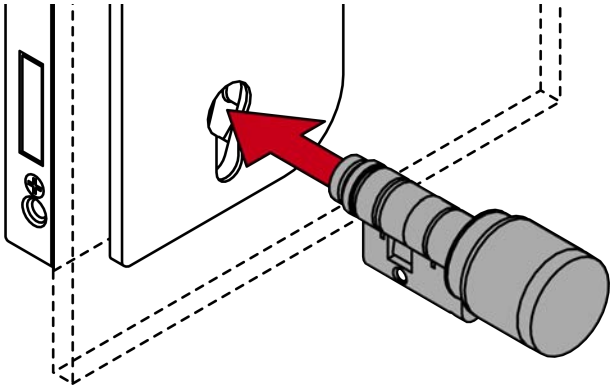
1. Schrauben Sie die Madenschraube aus dem Innenknauf (SW 1,5 mm).



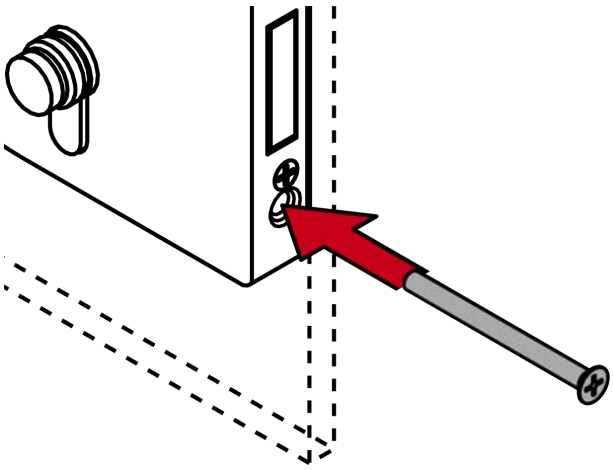
2. Drehen Sie den Innenknauf gegen den Uhrzeigersinn ab.



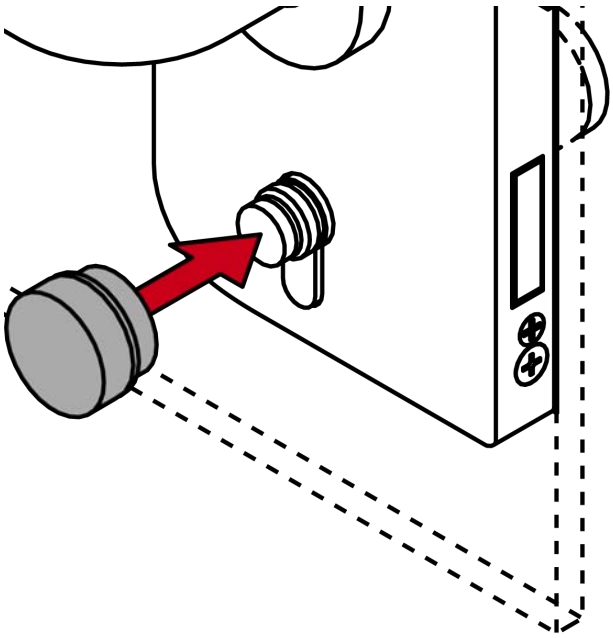
3. Stecken Sie den SI Digital Glass Door Cylinder AX in die Tür.



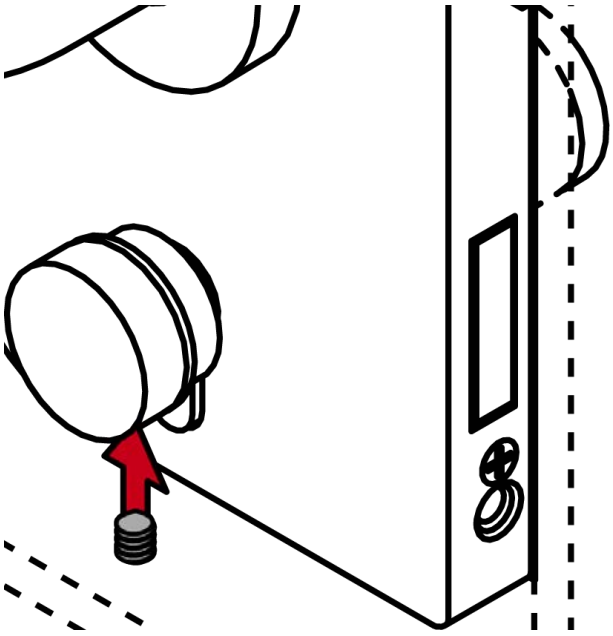
4. Schrauben Sie den SI Digital Glass Door Cylinder AX mit der Stulpschraube fest (PH2).



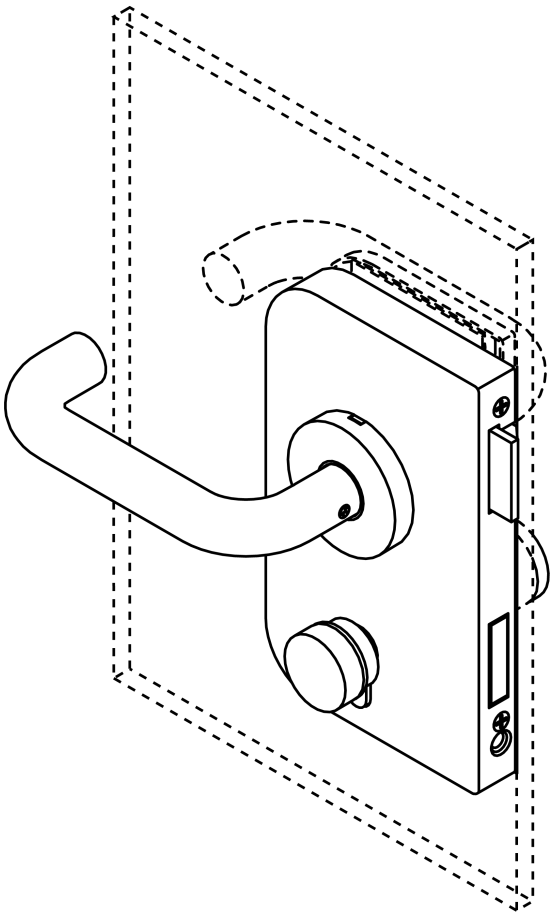
5. Drehen Sie den Innenknauf im Uhrzeigersinn wieder auf den SI Digital Glass Door Cylinder AX.



6. Sichern Sie den Innenknauf mit der Madenschraube (SW 1,5 mm).



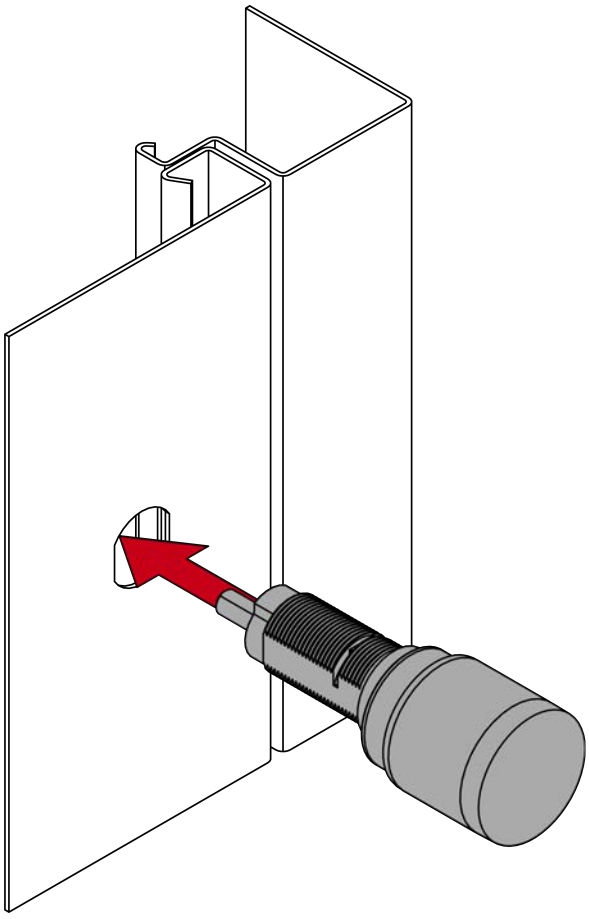
↳ SI Digital Glass Door Cylinder AX ist montiert.



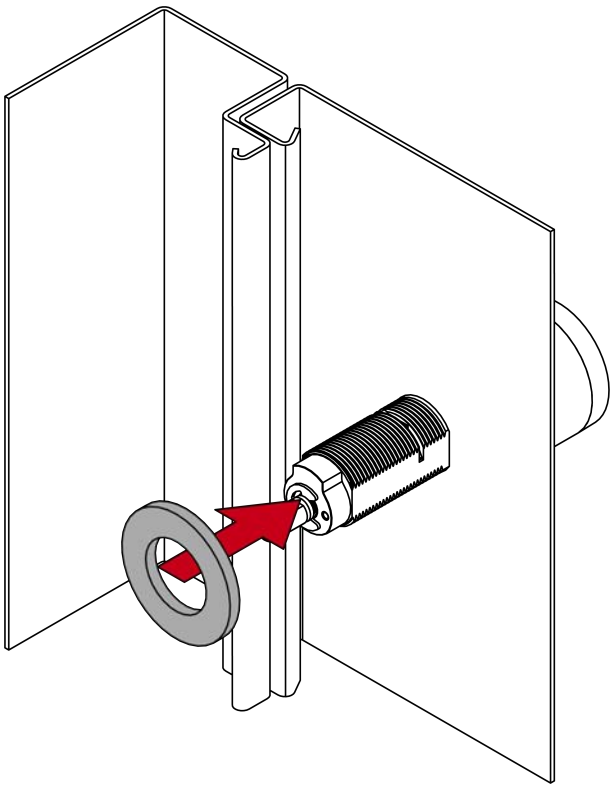
6.5.3.6 Hebelzylinder montieren

- ✓ Gabel-/Ringschlüssel SW22 vorhanden.
- ✓ Gabel-/Ringschlüssel SW10 vorhanden.

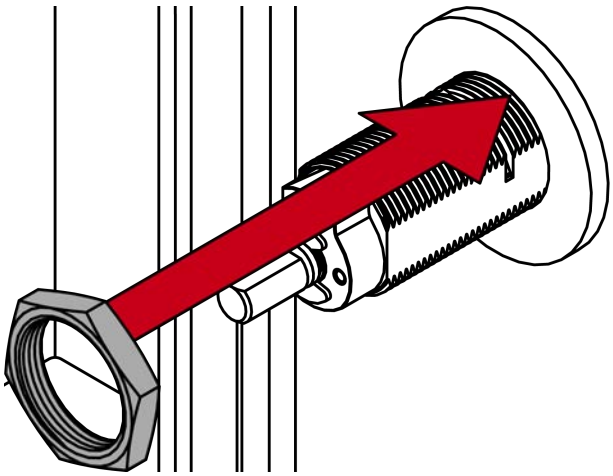
1. Stecken Sie den SI Digital Lever Cylinder AX in die vorgesehene Öffnung der Spindtür.



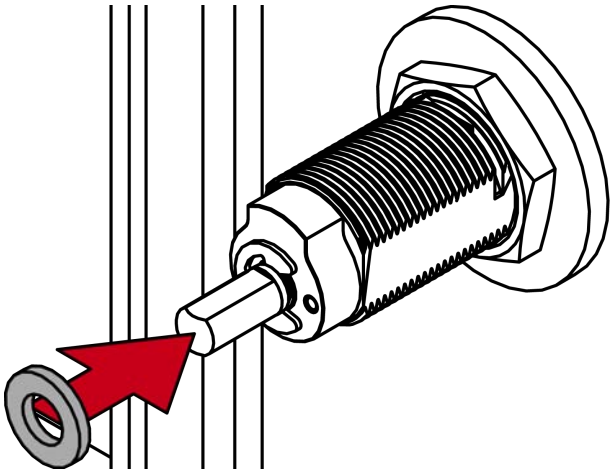
2. Stecken Sie die große runde Beilagscheibe so auf das Zylinderprofil, dass diese eben an der Innenseite der Spindtür anliegt.



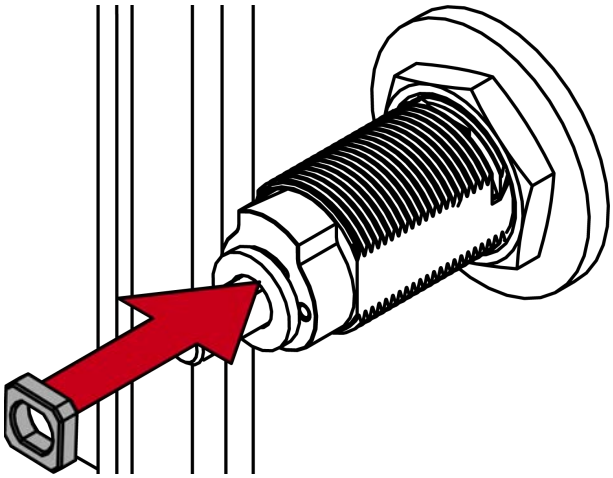
3. Stecken Sie die Mutter auf das Zylinderprofil und schrauben Sie diese fest (SW22).



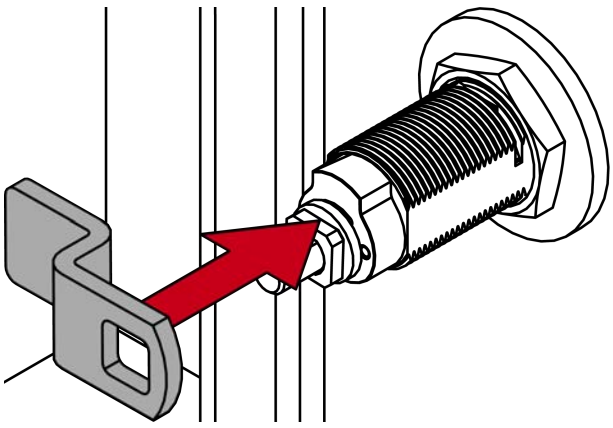
4. Stecken Sie die kleine Beilagscheibe auf das Ende des Zylinderprofils.



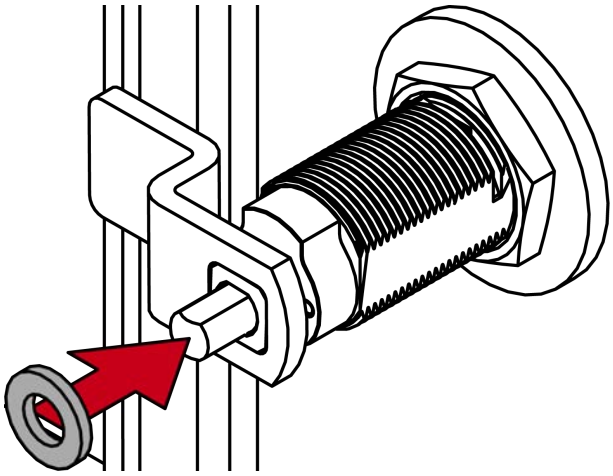
5. Stecken Sie die Vierkantbuchse auf die kleine Beilagscheibe.



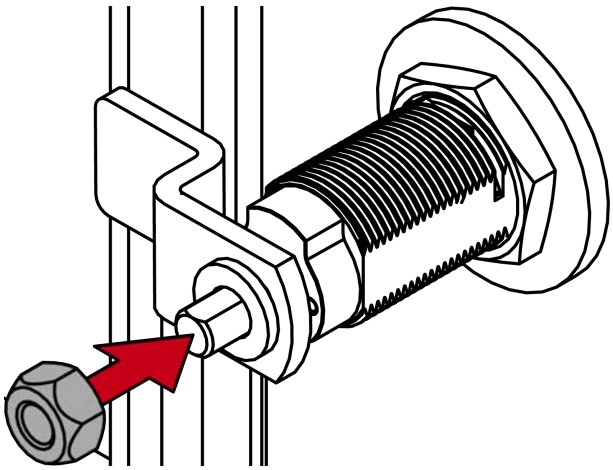
6. Stecken Sie den Hebel auf die Vierkantbuchse auf.



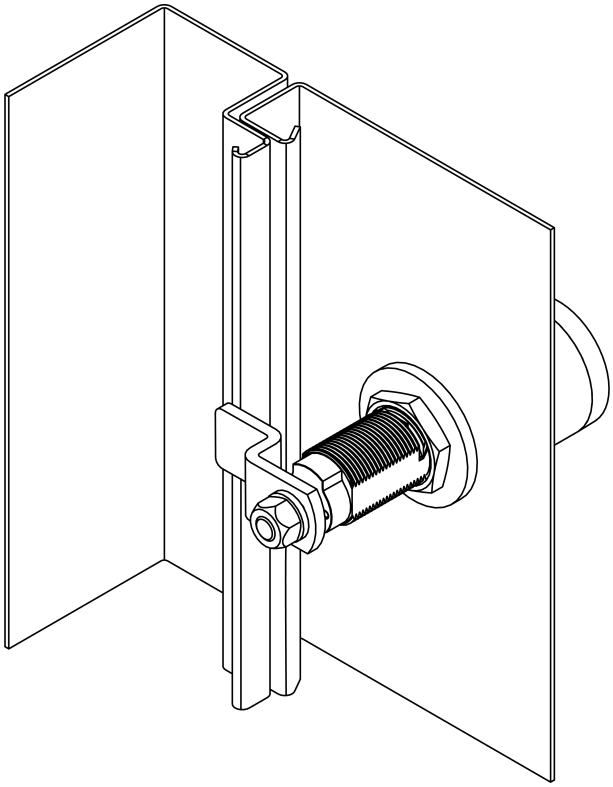
7. Stecken Sie die zweite kleine Beilagscheibe auf den Hebel.



8. Schrauben Sie anschließend die Sechskantmutter auf den Hebel (SW10).



↳ SI Digital Lever Cylinder AX ist fertig montiert.



6.5.3.7 Funktionstest

Führen Sie nach jeder Montage und jedem Batteriewechsel einen Funktionstest durch.

- ✓ Montage bzw. Batteriewechsel abgeschlossen
- ✓ SI Digital Cylinder AX programmiert
- ✓ Mindestens ein Identmedium berechtigt

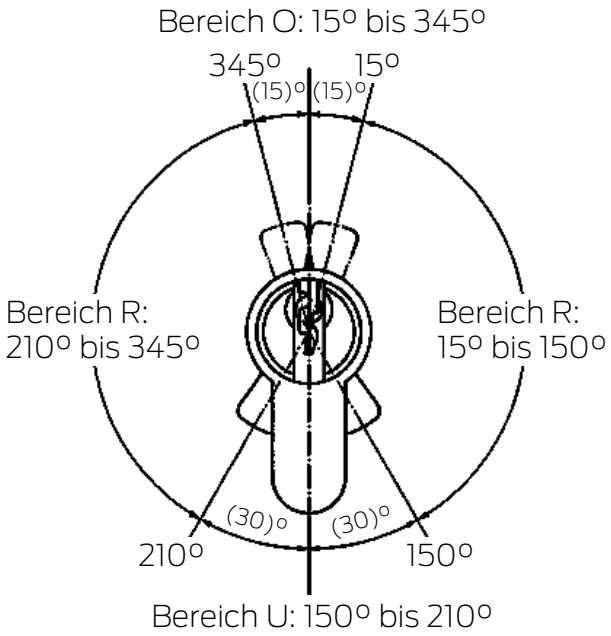
1. Ziehen Sie kräftig an den elektronischen bzw. mechanischen Knäufen.
2. Drehen Sie an den elektronischen Knäufen. Der SI Digital Cylinder AX darf nicht schwergängig sein oder den Mitnehmer drehen.
3. Betätigen Sie ein berechtigtes Identmedium.
4. Prüfen Sie, ob der SI Digital Cylinder AX eingekuppelt hat und den Schließbart herausdrückt.

↳ Montage bzw. Batteriewechsel erfolgreich durchgeführt.

6.5.3.8 Antipanik-Funktionstest

Führen Sie einen Funktionstest durch:

- Nach der Montage
- Nach einer Neuausrichtung
- Nach Änderungen an der Stulpschraube
- Nach einem Umbau (Längenmodularität)



Bereich U:	Keine Rückstellkraft auf den Mitnehmer
Bereich R:	Rückstellbereich Richtung Bereich U
Bereich O:	Oberer Totpunkt des Riegelvorschubs (Keine Rückstellkraft auf Mitnehmer)

✓ Funktionsprüfung erfolgt in Fluchtrichtung.
✓ Riegel ist eingefahren.

1. Drehen Sie den Knauf zunächst bei gekuppeltem Zylinder in Sperrrichtung des Schlosses bis zum Riegelvorschub in den Bereich R.
   ↳ Rückstellmoment spürbar..
2. Lassen Sie den Knauf los.
   ↳ Zylinder muss selbständig in den Bereich U zurückdrehen.
3. Betätigen Sie ein berechtigtes Identifikationsmedium.
   ↳ Zylinder kuppelt ein.
4. Drehen Sie den gekuppelten Knauf in Sperrichtung des Schlosses durch den Bereich R in den Bereich O.
   ↳ Riegel schiebt sich vor.
   ↳ Kein Rückstellmoment spürbar.
5. Bewegen Sie den Knauf geringfügig über die Grenze zwischen den Bereichen „O“ und „R“ in gleicher Drehrichtung weiter.
6. Lassen Sie den Knauf los.
   ↳ Rückstellkraft muss von diesem Punkt aus den Mitnehmer selbständig bis zum Bereich U weiterdrehen.
   ↳ Riegel fährt vollständig aus.

↳ Sollte sich der Knauf nicht selbstständig in den Bereich U drehen, ist entweder die Stulpschraube zu fest angezogen oder das Schloss falsch ausgerichtet worden. Nach der Fehlerbehebung ist der Test erneut durchzuführen. Eine zu fest angezogene Stulpschraube wirkt sich bremsend auf den Rückstellmechanismus aus.

7. Verschließen Sie die Tür und prüfen Sie die Funktion des Schlosses durch Drücken der Klinke/Panikstange in Richtung des Fluchtwegs.
   ↳ Riegel muss zurückschnappen.
   ↳ Tür muss sich leicht öffnen lassen.
   ↳ Sollte der Riegel beim Betätigen der Klinke nicht zurückfahren oder hakt die Klinke, ist entweder der Schließzylinder oder das Schloss falsch ausgerichtet oder defekt. Nach der vorgenannten Fehlerbehebung sind die vorherigen Tests erneut durchzuführen.

6.5.4 Werkzeug

Montage	Batteriewechsel
Erforderliches Werkzeug: ■ Erstmontage der Comfort-Variante ohne Spezialwerkzeug ■ Weitere Montagen der Comfort-Variante mit Spezialwerkzeug (abgebildet) ■ Montage anderer Varianten mit Spezialwerkzeug ■ Demontage immer mit Spezialwerkzeug	Erforderliches Werkzeug: ■ Spezialwerkzeug (abgebildet)

Das abgebildete Spezialwerkzeug ist mit der Bestellnummer Z5.TOOL erhältlich.

Der Europrofilzylinder ist modular (Längenmodularität). Hierfür sind weitere Werkzeuge und Bauteile erforderlich (Details siehe Handbuch zur Längenmodularität):

Ausheber (Z5.LIFTER)	Abstandshalter (Z5.SPACER)	Klemmblock (Z5.BLOCK)
		

Verlängerungsbolzen	Kernverlängerung des Profils	Profilverlängerung
		
▪ Z5.BOLT.XX (XX=Gewünschte Grundlänge)	▪ Z5.CORE.05: 5 mm ▪ Z5.CORE.10: 10 mm ▪ Z5.CORE.20: 20 mm	▪ Z5.PROFILE.05: 5 mm ▪ Z5.PROFILE.10: 10 mm ▪ Z5.PROFILE.20: 20 mm

Klammer

▪ Z5.CLAMPS Ein Set enthält 50 Stück.

Zylinder-Mittelstück	Halbzylinder-Mittelstück	Halbzylinder-Mittelstück mit Multirast
		
■ Z5.CNT.EU	■ Z5.CNT.HZ	■ Z5.CNT.HZ.MR

Knaufaufnahme innen	Blindprofil innen ohne Knauf	Knaufaufnahme für Glastürknauf
		
■ Z5.PR.IN	Für Variante .OK ■ Z5.PR.OK	Profillänge 30 mm (verlängerbar) ■ Z5.PR.GD

6.5.5 Deckelkontakt

Der SI Digital Cylinder AX erkennt mit einem Deckelkontakt, ob die Kappe abgenommen oder aufgesetzt wurde. Er nimmt jede Änderung wahr und leitet sie weiter (WaveNet) und misst nach dem Wiederaufsetzen den Batteriezustand.

Zusätzlich kuppeln SI Digital Cylinder AX, die gerade dauerhaft eingekuppelt sind (Dauerhaftes Einkuppeln, Office-Modus oder Notfallöffnung), wieder aus.

6.5.6 Technische Daten

6.5.6.1 Europrofil und SwissRound

Maße Knauf (ØxL)	Ø 32 mm × 39,5 mm (elektronisch), Ø 32 mm × 37,5 mm (mechanisch)
Grundlänge außen	30 mm, für Europrofil in 5 mm Schritten auf bis zu 90 mm verlängerbar (Kurzzylinder: 25 mm, weitere Längen auf Anfrage)
Grundlänge innen	30 mm, für Europrofil in 5 mm Schritten auf bis zu 90 mm verlängerbar (Kurzzylinder: 25 mm, weitere Längen auf Anfrage)
Material	Edelstahl
Farben	Standard: Edelstahl gebürstet, MS: Messingfarben beschichtet
Knaufkappen für Leseknauf	Kunststoffkappe (Passiv/Hybrid), Metallringkappe (Aktiv), Vollmetallkappe (Aktiv), SI: Nur Kunststoffkappe
VdS-Einstufung	Klasse BZ: Beantragt (nur Europrofil)
SKG-Einstufung	In Vorbereitung (nur Europrofil)
Schutzart	IP54 (Standard), IP67 (.WP)
Temperaturbereich (Betrieb)	-25 °C bis +65 °C (nach DIN EN 15684)
Batterietyp	2x CR2450 3V (Lithium) pro Leseknauf, bei Batterieknauf: 6x
Zulässige Batteriehersteller	Duracell, Murata, Panasonic
Batterielebensdauer (SI)	Bis zu 12 Jahre Standby oder 100.000 Betätigungen
Signalisierung	Akustisch (Buzzer) und/oder visuell (LED - grün/rot)
Netzwerkfähigkeit	Ja (integrierter LockNode bestell- und nachrüstbar, bei VdS nicht zugelassen), SI: LockNode als Austauschteil für WO erhältlich
Öffnungs-Modi	Impuls, Flipflop

Upgradefähigkeit	Firmware upgradefähig über BLE

Funkemissionen

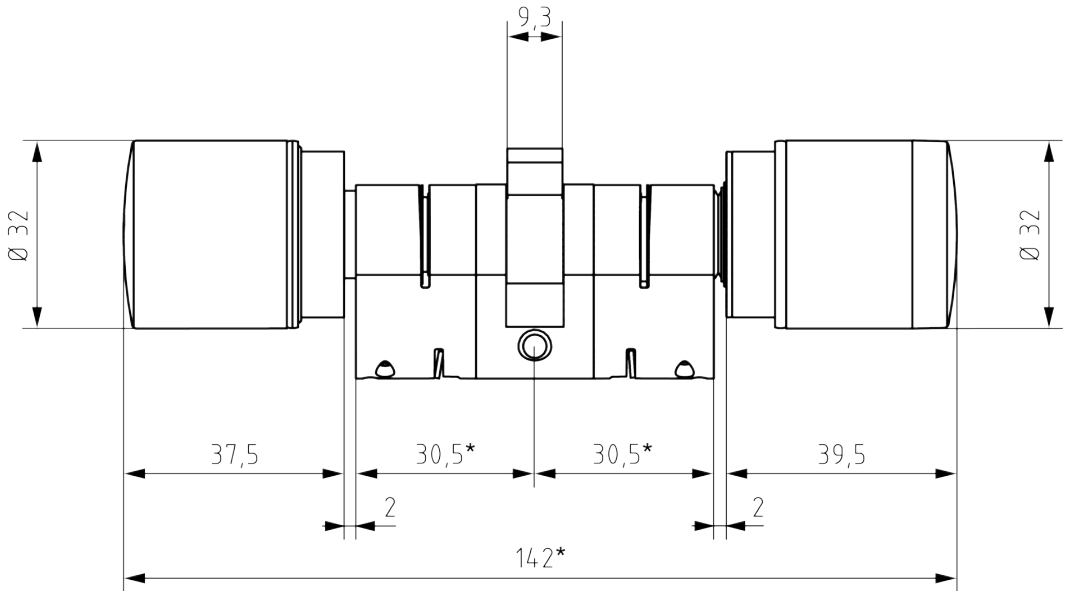
6.5.6.2 Scandinavan Oval und Scandinavian Round

Maße Knauf (ØxL)	Ø 32 mm × 39,5 mm (elektronisch), Ø 32 mm × 37,5 mm (mechanisch)
Material	Edelstahl
Farben	Standard: Edelstahl gebürstet, MS: Messingfarben beschichtet
Knaufkappen für Leseknauf	Kunststoffkappe (Passiv/Hybrid), Metallringkappe (Aktiv), Vollmetall-kappe (Aktiv), SI: Nur Kunststoff-kappe
Schutzart	IP54 (Standard), IP67 (.WP)
Temperaturbereich (Betrieb)	-25 °C bis +65 °C (nach DIN EN 15684)
Batterietyp	2x CR2450 3V (Lithium) pro Lese-knauf, bei Batterieknauf: 6x
Zulässige Batteriehersteller	Duracell, Murata, Panasonic
Batterielebensdauer (SI)	Bis zu 12 Jahre Standby oder 100.000 Betätigungen
Signalisierung	Akustisch (Buzzer) und/oder visuell (LED - grün/rot)
Netzwerkfähigkeit	Ja (integrierter LockNode bestell- und nachrüstbar, bei VdS nicht zu-gelassen), SI: LockNode als Aus-tauschteil für WO erhältlich
Öffnungs-Modi	Impuls, Flipflop
Upgradefähigkeit	Firmware upgradefähig über BLE

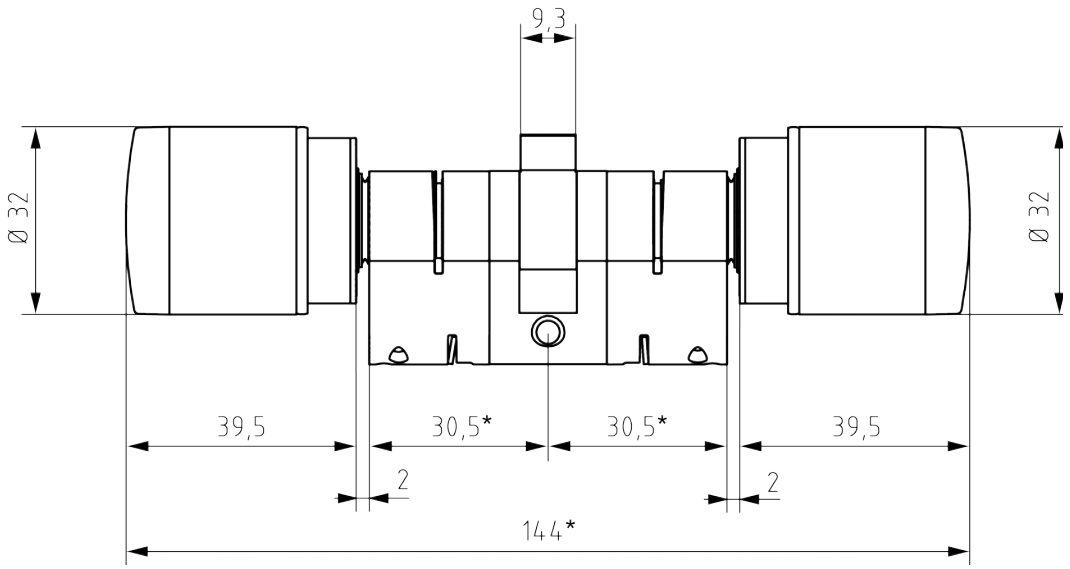
Funkemissionen

6.5.6.3 Abmessungen

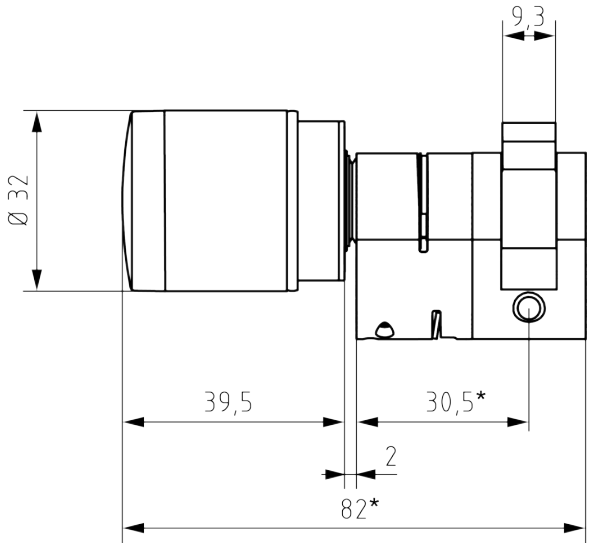
CO (Comfortzylinder)



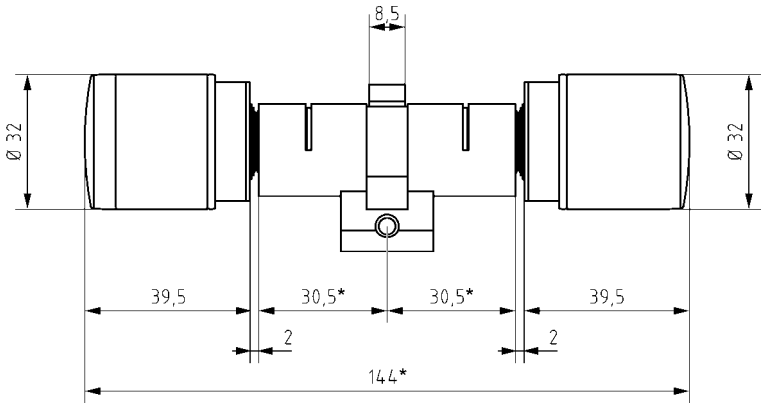
FD (freidrehender Zylinder)



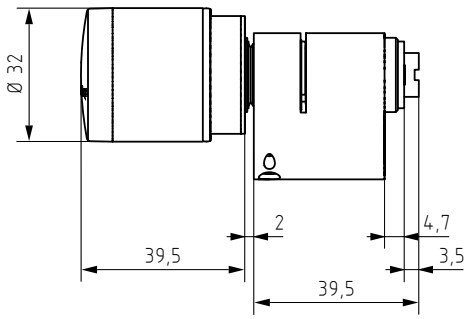
HZ (Halbzylinder)



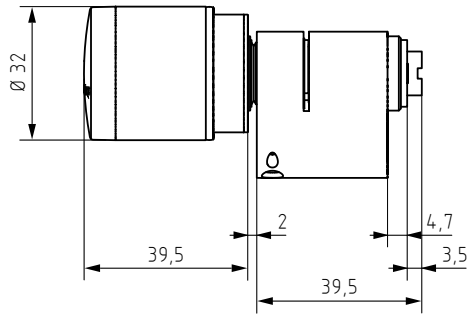
SR (Schweizer Rundprofil)



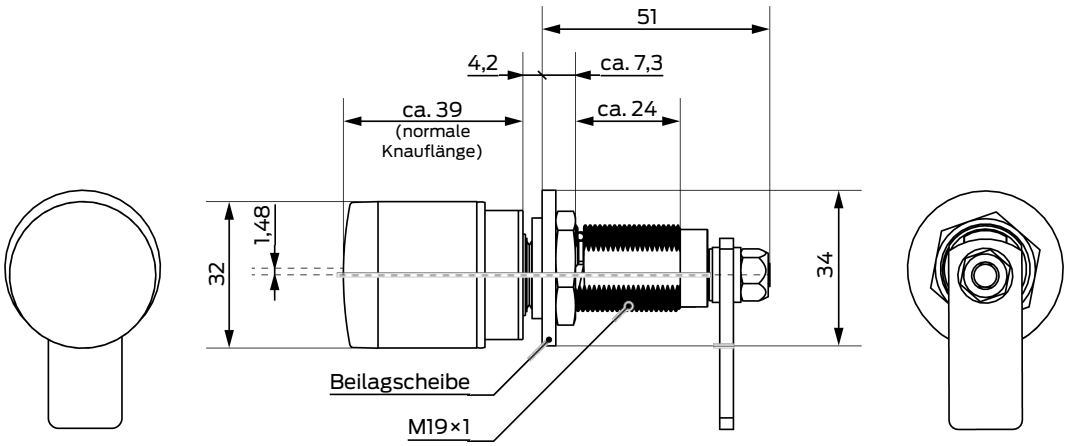
SO (Scandinavian Oval)



RS (Scandinavian Round)

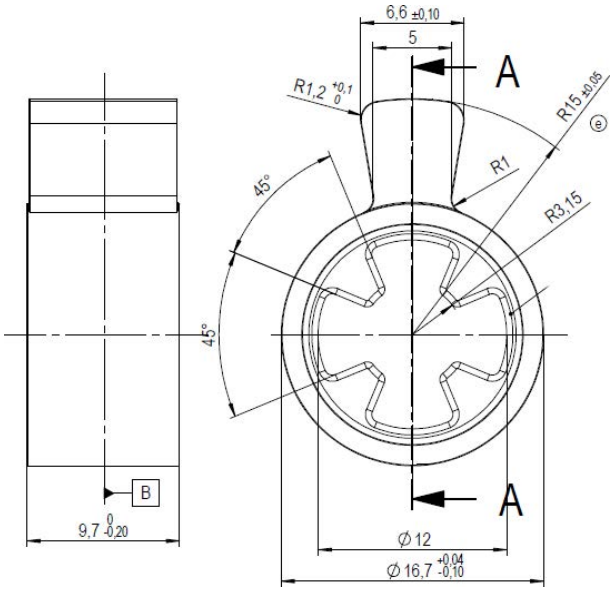


LE (Hebelzylinder)

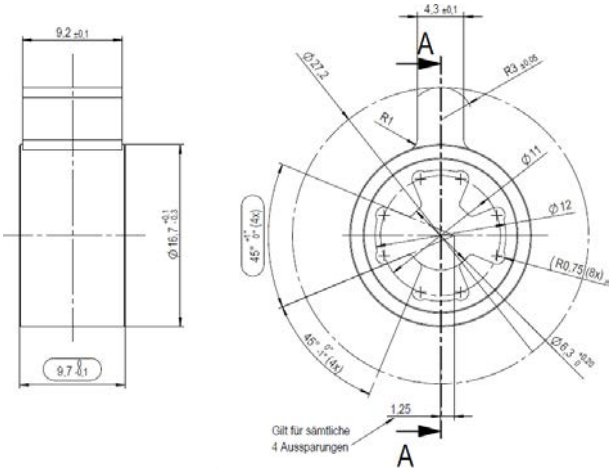


Abmessungen der Mitnehmer

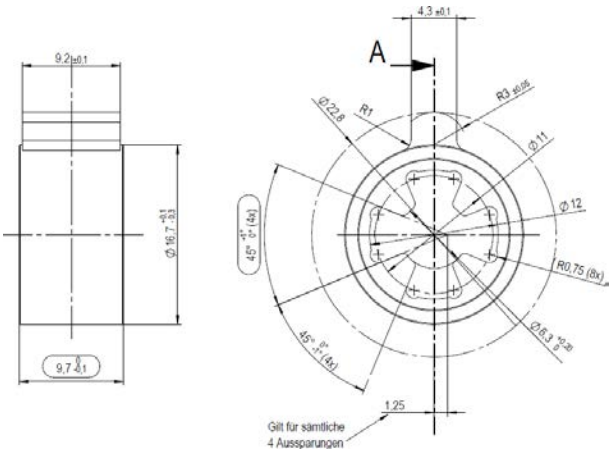
Mitnehmer Standard (Z5.CAM.WP)



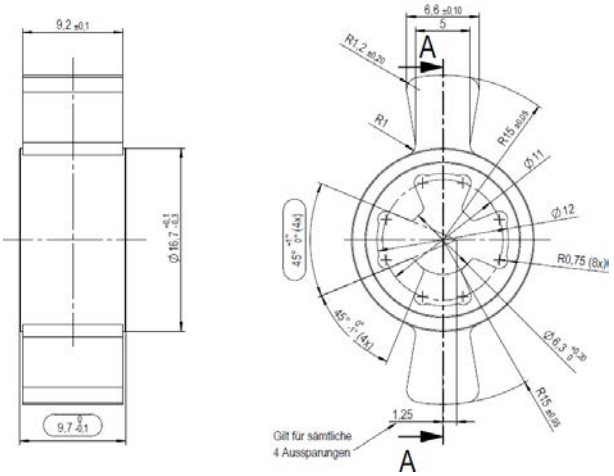
Mitnehmer PM1, lang (Z5.CAM.PM1)



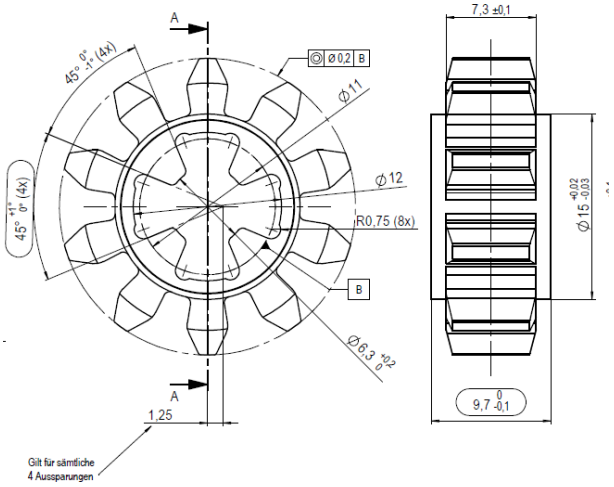
Mitnehmer PM2 ,kurz (Z5.CAM.PM2)



Doppelmitnehmer (Z5.CAM.DOUBLE)

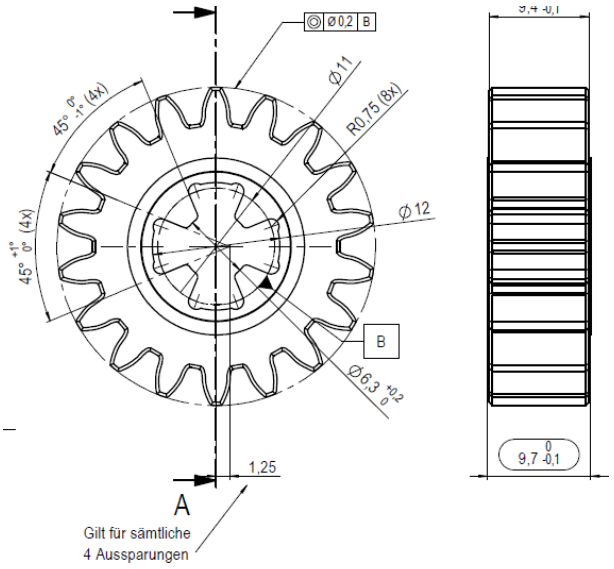


Mitnehmer Zahnrad 10 Zähne (Z5.CAM.GEAR10)



Modul	m	2
Zähnezahl	z	10
Flankendurchmesser	d	20

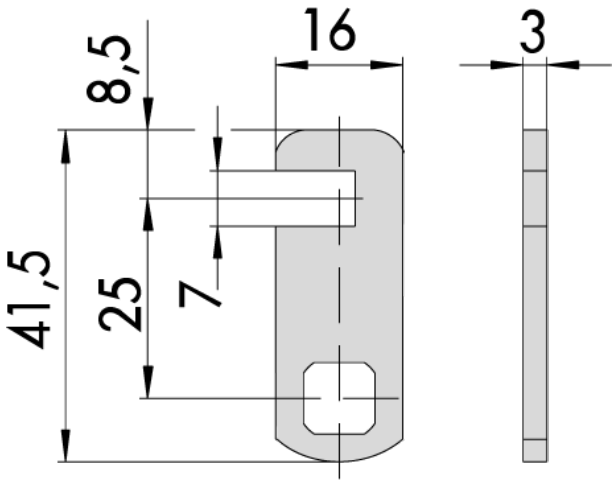
Mitnehmer Zahnrad 18 Zähne (Z5.CAM.GEAR18)



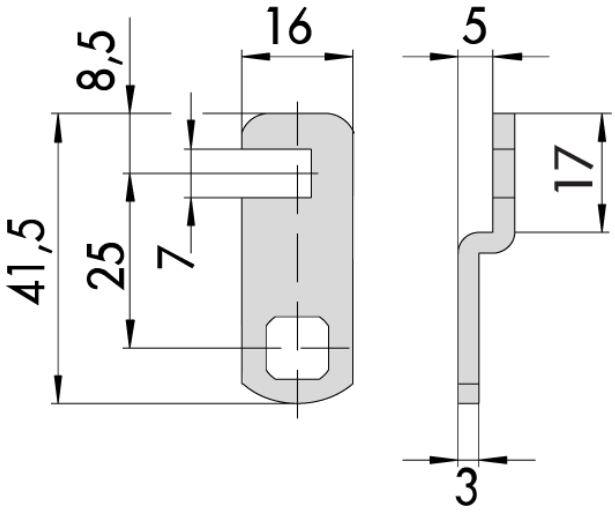
Modul	m	1,5
Zähnezahl	z	18
Flankendurchmesser	d	27

Abmessungen der Hebel

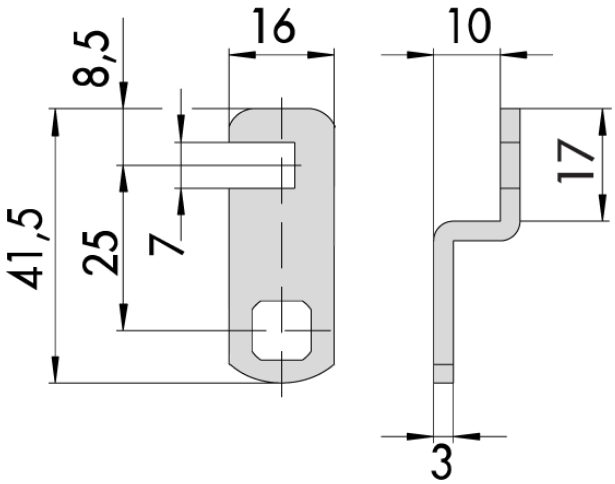
Z5.LE.11.01



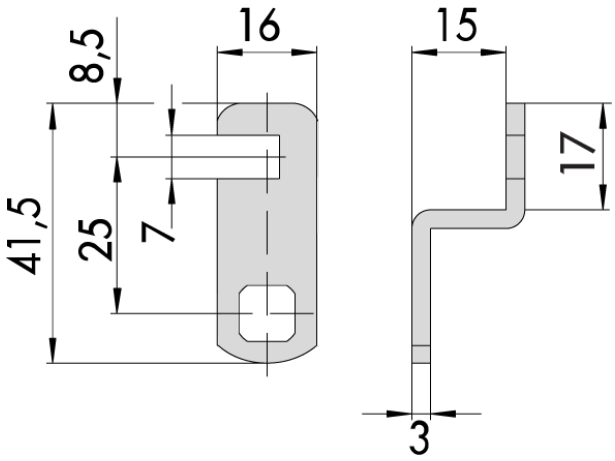
Z5.LE.11.02



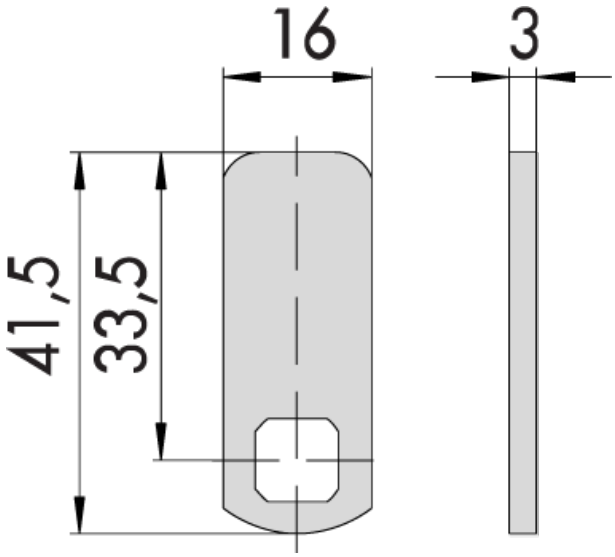
Z5.LE.11.03



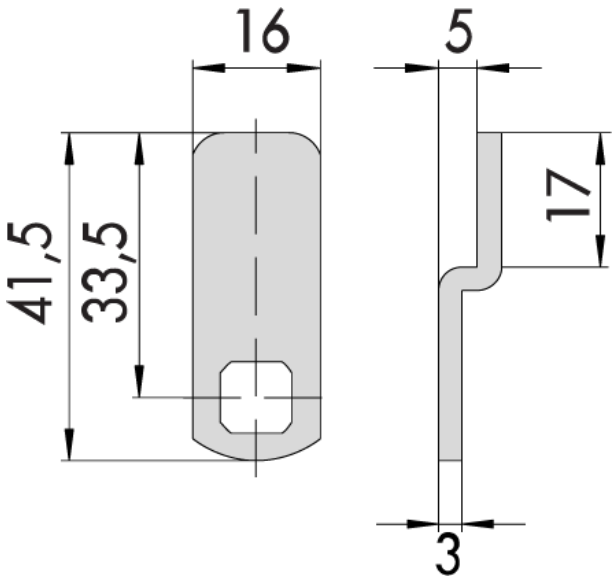
Z5.LE.11.04



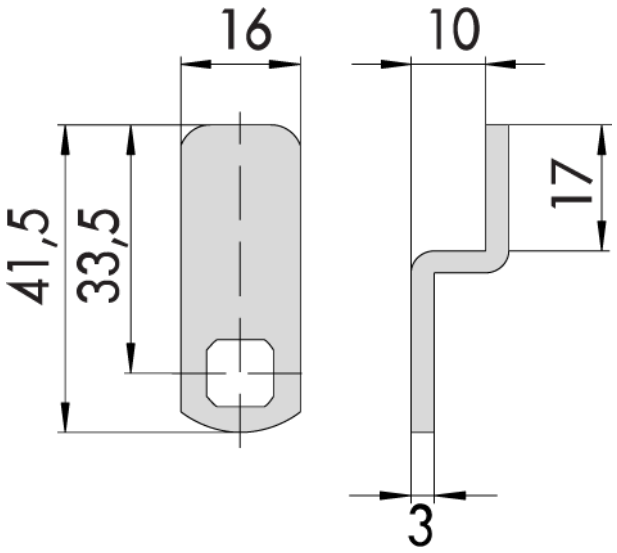
Z5.LE.12.01



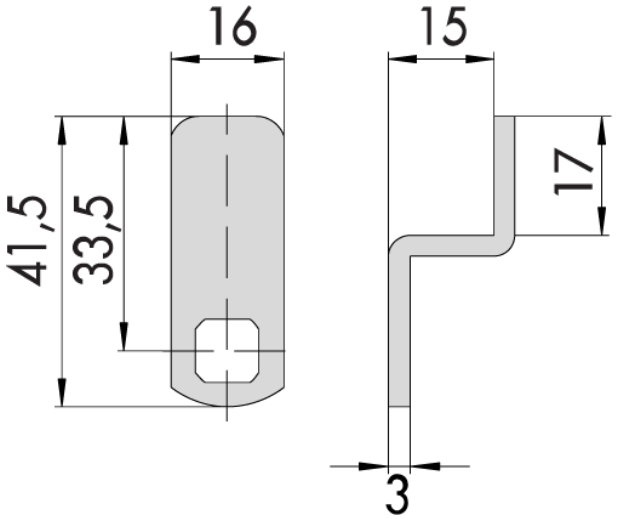
Z5.LE.12.02



Z5.LE.12.03



Z5.LE.12.04



6.6 Schließzylinder (TN4)

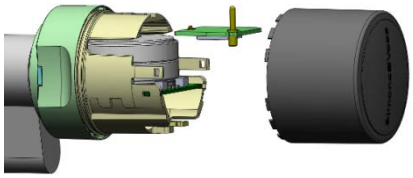
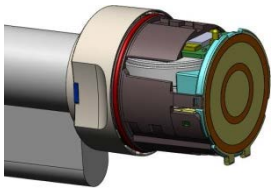
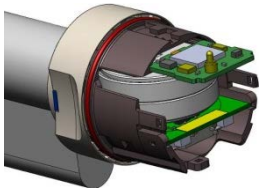
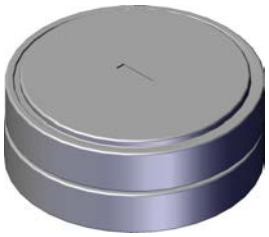
Der Schließzylinder bewegt den Riegel des Einsteckschlosses. Verwenden Sie einen Schließzylinder, wenn Sie Türen verriegeln wollen.

6.6.1 Aufbau

Schließzylinder bestehen grundsätzlich aus zwei Hälften:

Master (Central Unit = CU)	Slave
Knauf kann nicht demontiert werden.	Knauf kann für Montage demontiert werden.
Erkennungsmerkmal: Schwarzer Ring zwischen Knauf und Profilzylinder.	

Schließzylinder bestehen aus mehreren Teilen:

	Control Unit (CU): Baugruppe unter dem Batteriefach des Master-Knaufs
	Kartenleser (Card Reader = CR): Master-Leser (bei beidseitig lesenden Zylindern (FD und BL): Zusätzlicher Slave-Leser)
	LockNode (LN): Baugruppe über dem Batteriefach des Master-Knaufs
	Batterien im Batteriefach des Master-Knaufs

Der Schließzylinder sollte immer mit der Innenseite im Innenbereich montiert werden. Sie finden die Markierung zur Innenseite:

- In den Maßzeichnungen (siehe *Maßzeichnungen Zylinder [▸ 107]*)
- Auf dem Profilgehäuse (IN)

Comfort (CO)	Seite	Verhalten (ausgekuppelter Zustand)	Bestandteile	Batterien
Master	Außen	Freidrehend	▪ Control Unit ▪ Kartenleser	2
Slave	Innen	Dauerhaft eingekuppelt	Keine Elektronik	Keine

Freidrehend (FD)	Seite	Verhalten (ausgekuppelter Zustand)	Bestandteile	Batterien
Master	Innen	Freidrehend	▪ Control Unit ▪ Kartenleser	2
Slave	Außen	Freidrehend	Zweite Control Unit	2

Antipanik Freidrehend (AP2 FD)	Seite	Verhalten (ausgekuppelter Zustand)	Bestandteile	Batterien
Master	Außen	Freidrehend	■ Control Unit ■ Kartenleser	2
Slave	Innen	Einkuppeln nicht möglich	Keine Elektronik	Keine

Antipanik Beidseitig lesend (AP2 BL)	Seite	Verhalten (ausgekuppelter Zustand)	Bestandteile	Batterien
Master (innen)	Beidseitig verwendbar	Freidrehend	■ Control Unit ■ Kartenleser ■ LockNode	2
Slave (außen)		Freidrehend	■ Control Unit ■ Kartenleser	2

HINWEIS

Programmierfehler bei unterbrochener oder geänderter Master-Slave-Paarung

Der Master und der Slave sind werkseitig als zusammengehörig konfiguriert. Der Austausch von Knäufen führt zu Programmierfehlern.

Bei der Programmierung kommunizieren Master und Slave.

- Stellen Sie sicher, dass Master und Slave während einer Programmierung physisch verbunden sind.

6.6.2 Varianten und Ausstattungsmerkmale

Die Bestellnummer gibt Auskunft über die Variante und die Ausstattungsmerkmale:

Allgemein	SI	SmartIntego-Zylinder
	Z4	Technologielevel 4
	AXX-IXX	Außenmaß-Innenmaß
	▪ MI (bei SmartIntego WirelessOnline) ▪ M (bei SmartIntego Virtual Card Network)	▪ **M**IFARE & LockNode **I**ntegrated (bei SmartIntego Wireless Online) MIFARE Integrated ist eine Abkürzung für *MIFARE-Technologie mit integriertem LockNode*. ▪ **M**IFARE (bei SmartIntego Virtual Card Network)
Aufbau	CO	Comfort - Zylinder innen dauerhaft eingekuppelt
	FD (nur bei SmartIntego Wireless Online)	Freidrehend - Zylinder mit zwei Kartenlesern (Innen- und Außenseite) Unterschiedliche Zutrittsberechtigungen möglich (Integratorabhängig)

Ausstattungsmerkmale	WP	Wettergeschützte Version (IP 66), sonst IP54
	AP2	Antipanik-Funktion
	BL	Beidseitig lesend (nur zusammen mit Antipanik-Funktion für Smart-Intego Wireless Online erhältlich)
	DK	Abnehmbarer Knauf (z.B. für Einbau hinter Blenden ohne Zylinderlochung, nur als Halbzylinder erhältlich)
	HZ	Halbzylinder
	MR	Multirast-Variante
	MS	Messing-Variante
	OK	Ohne Innenknauf
	SL	Selbstverriegelnd (nur als Halbzylinder erhältlich)

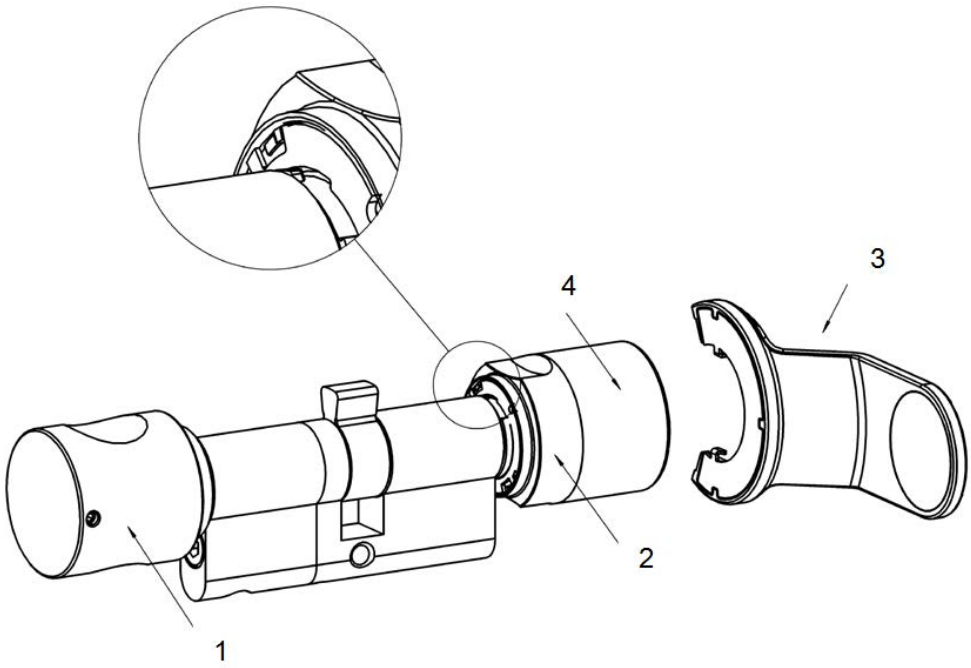
HINWEIS

Vermeidung von Fehlbestellungen durch Bestellhilfe

SmartIntego-Komponenten bieten eine große Vielfalt an Kombinationen. Nicht jede Kombination ist sinnvoll und tatsächlich erhältlich. Eine manuelle Zusammenstellung der Ausstattungsmerkmale kann zu nicht erhältlichen Kombinationen oder Fehlbestellungen führen.

- Verwenden Sie immer die Bestellhilfe aus dem Partnerbereich der SmartIntego-Website (*www.smartintego.com)*).

6.6.3 Montage



1. Innenknauf
2. Vertiefter Griffring
3. Batteriewechselschlüssel
4. Außenknauf

Der Slave-Knauf wird mit dem Montage- oder dem Batteriewechselschlüssel montiert. Das genaue Vorgehen ist in der mitgelieferten Kurzanleitung des Schließzylinders beschrieben.

6.6.4 Werkzeug

Montage	Batteriewechsel
Erforderliches Werkzeug: ■ Montageschlüssel oder ■ Batteriewechselschlüssel (abgebildet)	Erforderliches Werkzeug: ■ Batteriewechselschlüssel (abgebildet) und ■ Batteriewechselkarte (siehe Schritt-für-Schritt-Anleitung)

Der abgebildete Batteriewechselschlüssel ist mit der Bestellnummer Z4.SCHLUESSEL erhältlich.

6.6.5 Technische Daten

Profilzylinder

Grundlänge:	Außen 30 mm, innen 30 mm (AP/ WP 35mm)

Baulängen in 5 mm Abstufungen bis 140 mm Gesamtlänge (max. 90 mm auf einer Seite), Sonderlängen auf Anfrage.

Umgebungsbedingungen

Betriebstemperatur:	-25°C bis +65°C
Schutzklasse:	IP 54 (im eingebauten Zustand) Variante .WP: IP 66
Luftfeuchtigkeit:	<95%; nicht kondensierend

Batterien

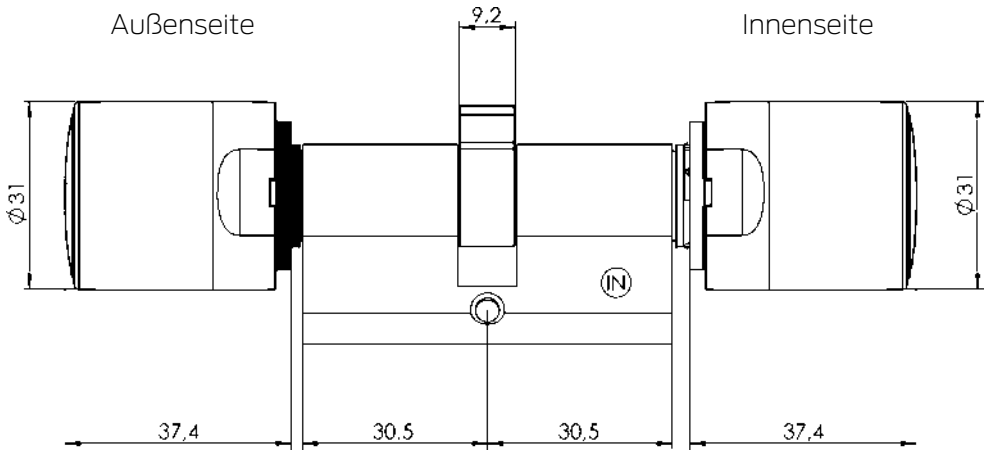
Typ:	CR 2450 3V
Hersteller:	Duracell, Murata, Panasonic
Anzahl:	2 Stück
Batterielebensdauer:	SmartIntego Wireless Online (WO): ■ Bis zu 5 Jahre ■ Bis zu 80000 Betätigungen Karte für SmartIntego Virtual Card Network (SVCN): ■ Bis zu 6 Jahre ■ Bis zu 50000 Betätigungen

Bitterstoff-beschichtete Batterien sind nicht geeignet.

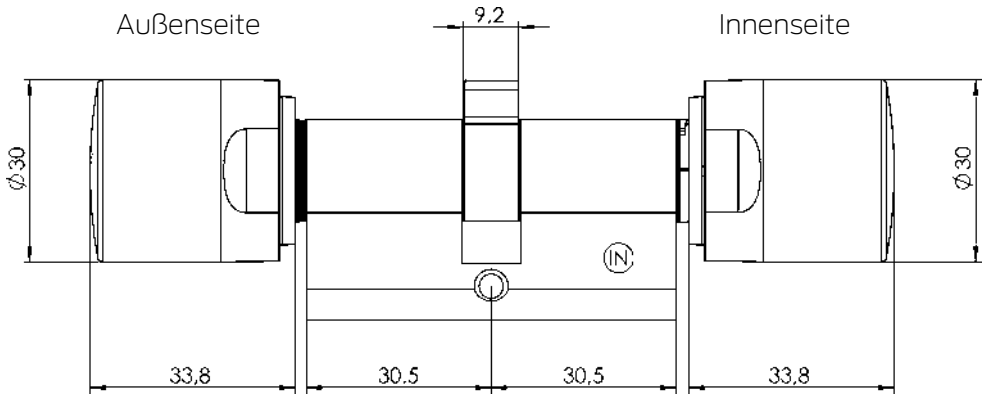
Der Zylinder gibt akustisches und optisches (blaue/rote LED) Feedback.

6.6.6 Maßzeichnungen Zylinder

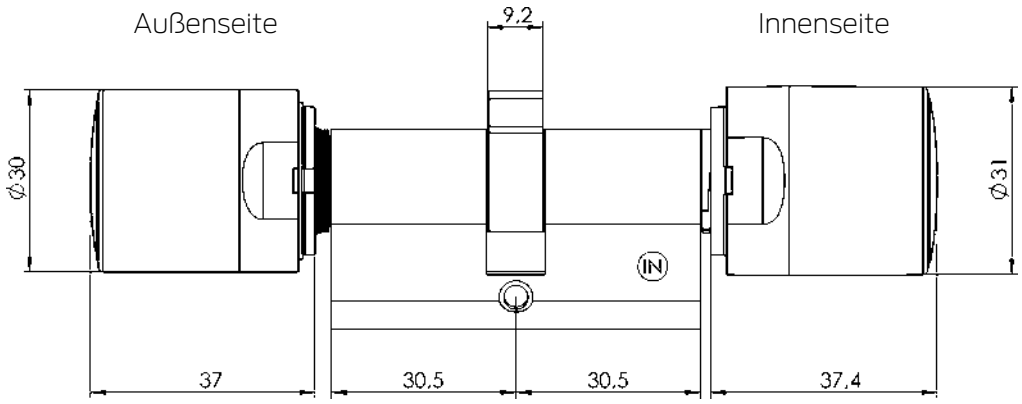
Comfort - Passiv (CO MP)



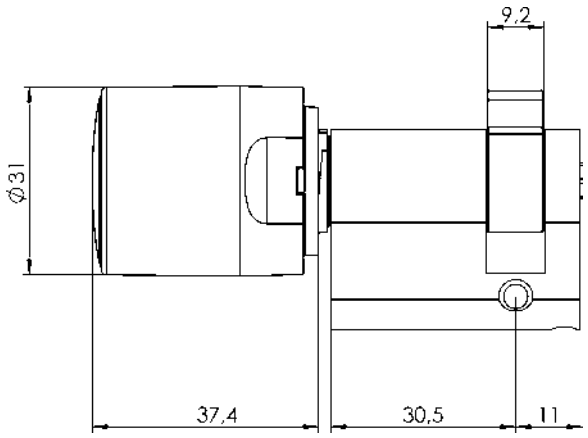
Freidrehend - Aktiv (FD)



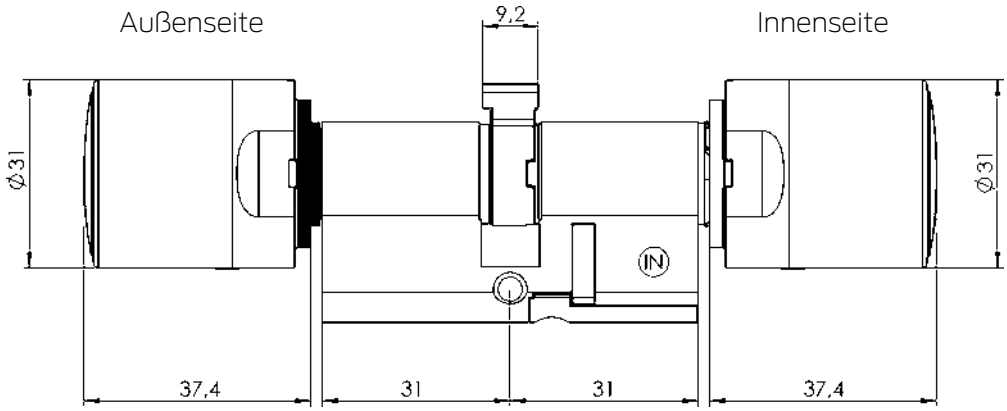
Freidrehend - Passiv/Hybrid (FD MP/MH)



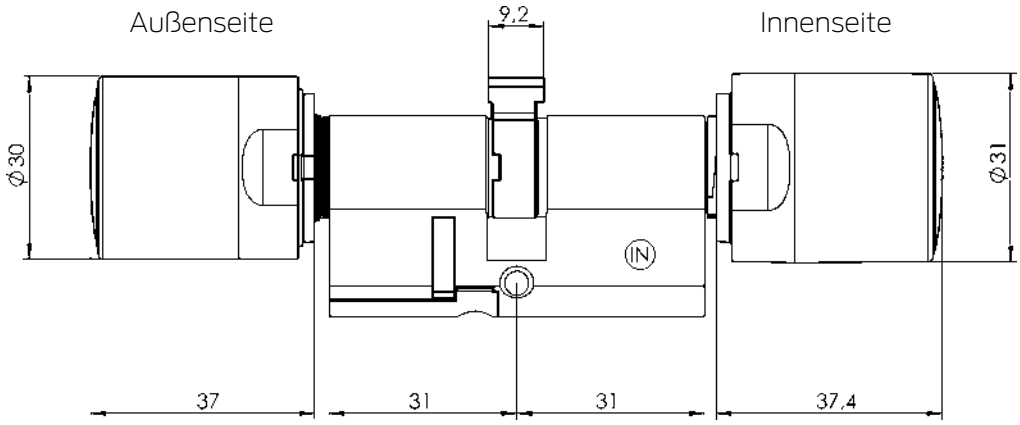
Halbzylinder - Passiv (HZ MP)



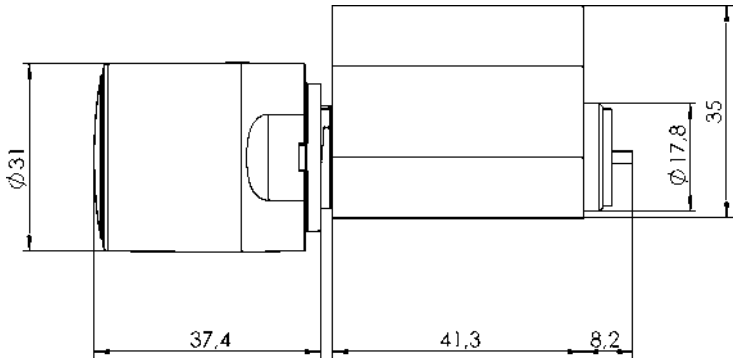
Antipanik Freidrehend - Passiv (AP2 FD MP)



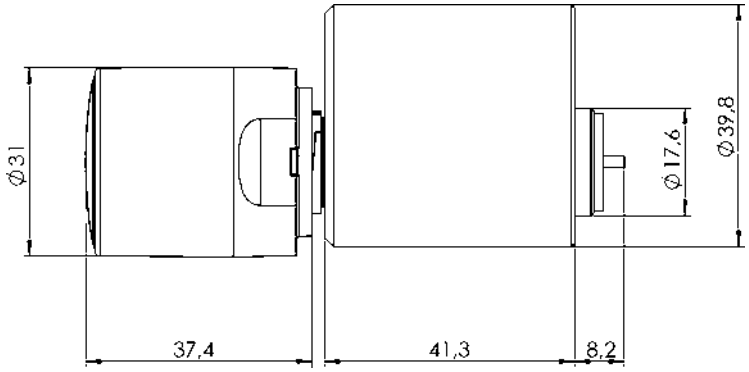
Antipanik Beidseitig lesend - Passiv (AP2 BL MP)



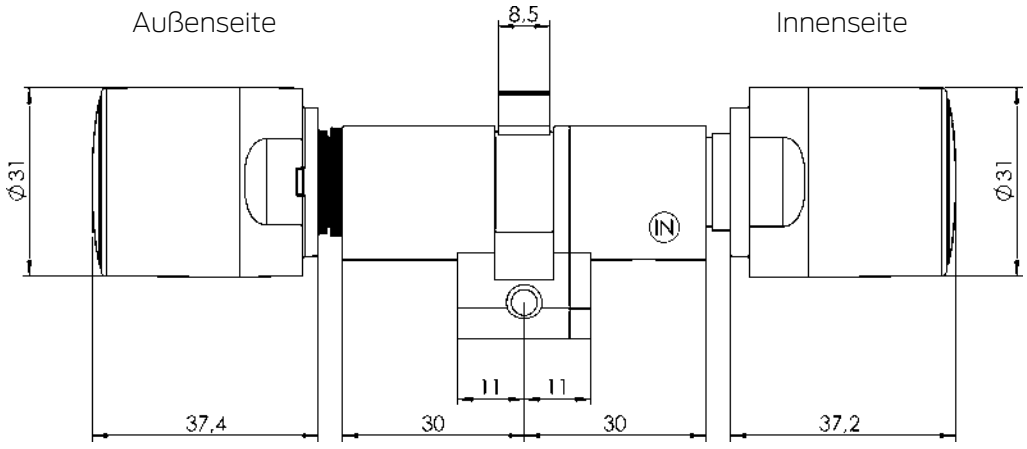
Scandinavian Oval - Passiv (SO MP)



Scandinavian Round - Passiv (RS MP)



Swiss Round Comfort - Passiv (SR CO MP)



6.7 SmartHandle AX

Das SmartHandle AX bewegt die Falle des Einsteckschlosses. Verwenden Sie ein SmartHandle AX oder ein SmartHandle 3062, wenn Sie Türen nur schließen wollen (Innentüren).

Wenn Türen auch verriegelt werden sollen, dann können Sie ein SmartHandle mit einem selbstverriegelnden Einsteckschloss kombinieren.

Varianten, Ausstattungsmerkmale, Montage...

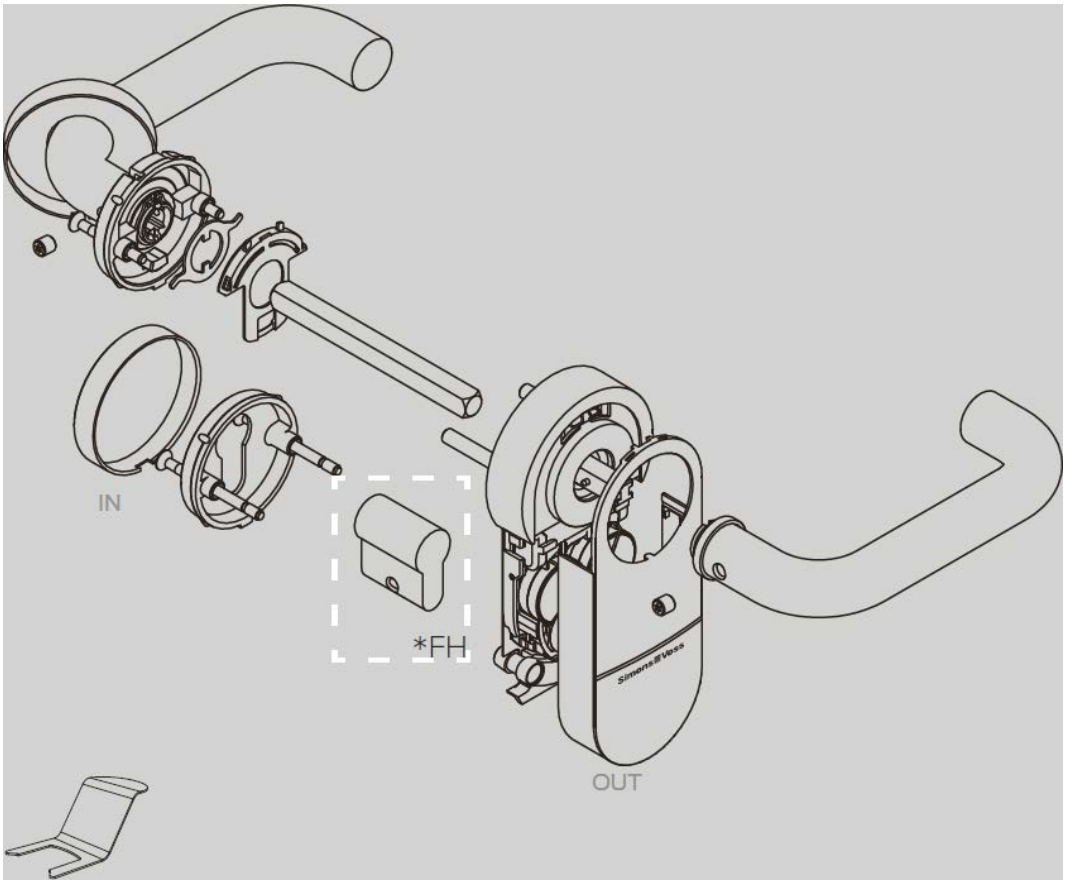
Detaillierte Informationen finden Sie im Handbuch des SI.SmartHandle AX.

6.7.1 Aufbau

Beim SmartHandle AX befindet sich die gesamte Elektronik auf der Außenseite:

- Control Unit (CU)
- Kartenleser (Card Reader = CR)
- LockNode (LN)
- Batterien

Das SmartHandle AX ist in mehreren Ausführungen erhältlich. Die Abbildung zeigt beispielsweise den Aufbau mit der hängenden Montage:



6.7.2 Werkzeug

Das mitgelieferte SmartHandle-Tool wird benötigt, um das Cover abzunehmen. Informationen zu weiteren benötigten Werkzeugen entnehmen Sie bitte der mitgelieferten Kurzanleitung.

6.7.3 Deckelkontakt

Das SI.SmartHandle AX erkennt mit einem Deckelkontakt, ob das Gehäuse abgenommen oder aufgesetzt wurde. Es nimmt jede Änderung wahr und leitet sie weiter (WaveNet) und misst nach dem Wiederaufsetzen den Batteriezustand.

Zusätzlich kuppeln SI.SmartHandle AX, die gerade dauerhaft eingekuppelt sind (Dauerhaftes Einkuppeln, Office-Modus oder Notfallöffnung), wieder aus.

6.7.4 Technische Daten

Typen	■ Euro-PZ ■ Scandinavian Oval ■ Swiss Round
Leseverfahren	■ Passiv ■ BLE ready

Unterstützte Karten (Wireless Online WO)	■ MIFARE® Classic ■ MIFARE DESFire® EV1/EV2 ■ UID (Karten-Seriennummer) nach ISO 14443 (z.B. MIFARE, Legic Advant, HID® SEOS)
Unterstützte Karten (SmartIntego Virtual Card Network SVCN)	■ MIFARE® Classic ■ MIFARE DESFire® EV1/EV2
Lesereichweiten	Nahfeld
Stromversorgung	
Batterietyp	4× CR2450 (3 V)
Batteriehersteller	■ Duracell ■ Murata ■ Panasonic
Batterielebensdauer (Wireless Online WO)	■ Bis 180.000 Betätigungen ■ Bis 9 Jahre Stand-By ohne Betätigung
Batterielebensdauer (SmartIntego Virtual Card Network SVCN)	■ Bis 150.000 Betätigungen ■ Bis 9 Jahre Stand-By ohne Betätigung
Umgebungsbedingungen	
Temperaturbereich	Betrieb: -25 °C bis +50 °C
	Lagerung (kurzzeitig): -40 °C bis +50 °C
	Lagerung (langfristig): 0 °C bis +30 °C
Schutzart	IP40
Feedback	
Signalisierung	■ Akustisch (Piepser) ■ Optisch (Zweifarbige LED)
Verwaltung und Einstellungen	
Netzwerkfähigkeit	■ Wireless Online (WO): Integrierter LockNode (LNI) ■ SmartIntego Virtual Card Network (SVCN): Nicht netzwerkfähig
Sonstiges	
Upgradefähigkeit	Upgradefähige Firmware
Einträge in der Zutrittsliste	Max. 1.000

Funkemissionen

6.7.4.1 Mechanik

Maße

Die Maßangaben beziehen sich auf die Seite mit dem elektronischen Beschlag.

Höhe	■ A0 (stehend) ■ A3 (Rohrrahmen) ■ DS (Beidseitig lesend)	120 mm
	A1 (hängend kurz)	140 mm
	■ A2 (hängend lang) ■ E0/E1 (Scandinavian Oval)	174 mm
	A4 (Panikstange)	■ BKS (Entfernung: 72 mm): 193,4 mm ■ BKS (Entfernung: 92 mm): 213,4 mm ■ CISA (Entfernung: 72 mm): 224,4 mm (Angaben mit Adapterplatte)
Breite	66 mm	

Tiefe	■ A0 (stehend) ■ A1 (hängend kurz) ■ A2 (hängend lang) ■ E0/E1 (Scandinavian Oval)	21 mm
	A3 (Rohrrahmen)	26 mm (Angaben mit Adapterplatte)
	A4 (Panikstange)	25 mm (Angaben mit Adapterplatte)
	DS (Beidseitig lesend	■ 21 mm (Seite ohne Adapterplatte) ■ 26 mm (Seite mit Adapterplatte

Verfügbare detaillierte Maßzeichnungen finden Sie am Ende des Kapitels.

Entfernungen und Türdicken

A* = Europrofil, B* = Swiss Round, E* = Scandinavian Oval

Variante	Entfernung	Türdicken
A0/B0 Stehend	nicht relevant (stehende Montage: Drückerwellenachse und Profilzylinderachse am Beschlag nicht verbunden)	S: 38 - 60 mm
		M: 59 - 80 mm
		L: 79 - 100 mm
		X: 100 - 200 mm
A0.PAS Stehend (PAS24)	nicht relevant (stehende Montage: Drückerwellenachse und Profilzylinderachse am Beschlag nicht verbunden)	S: 38 - 60 mm
		M: 59 - 80 mm
		L: 79 - 100 mm
A1/B1 Hängend, kurz	70 - 79 mm	S: 38 - 60 mm
		M: 59 - 80 mm
		L: 79 - 100 mm
		X: 100 - 200 mm

Variante	Entfernung	Türdicken
A2/B2 Hängend, lang	70 - 110 mm	S: 38 - 60 mm
		M: 59 - 80 mm
		L: 79 - 100 mm
		X: 100 - 200 mm
A3 Rohrrahmen	nicht relevant (stehende Montage: Drückerwellenachse und Profilzylinderachse am Beschlag nicht verbunden)	S: 38 - 57 mm
		M: 58 - 77 mm
		L: 78 - 97 mm
		X: 97 - 196 mm
A4 Panikstange	92 mm (BKS Vollblattür ohne Schild) 72 mm (CISA Vollblattür mit Schild oder BKS Vollblattür ohne Schild)	S: 38 - 60 mm
		M: 59 - 80 mm
		L: 79 - 100 mm
		X: 100 - 200 mm
DS Beidseitig lesend (Double-sided)	nicht relevant (stehende Montage: Drückerwellenachse und Profilzylinderachse am Beschlag nicht verbunden)	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
F1 Französisches 195-mm-Schild	70 mm	S: 38 - 60 mm
		M:58 - 80 mm
		L: 78 - 100 mm

Drückerbetätigungswinkel und Farben

Drückerbetätigungswinkel	48° effektiv

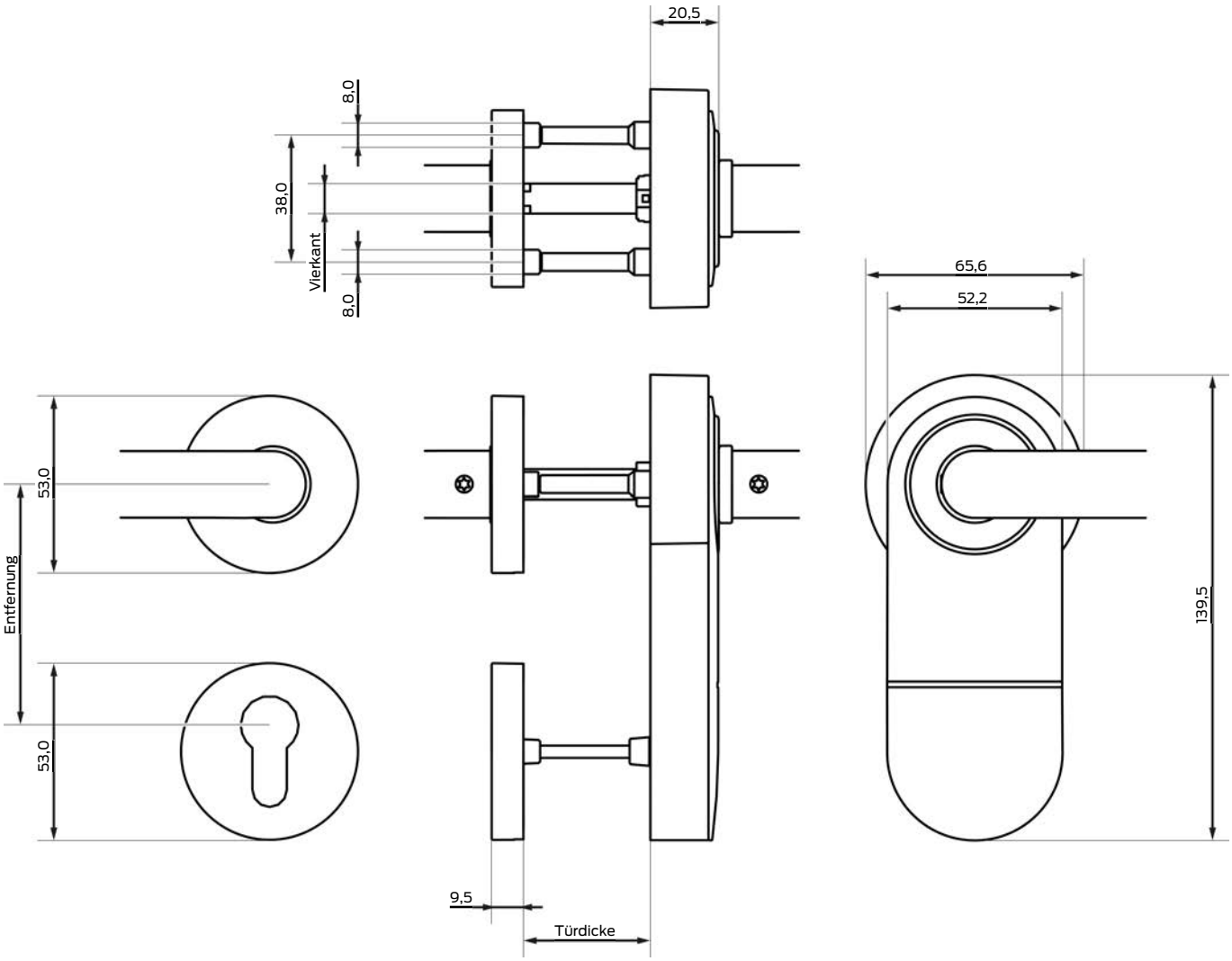
Farben	Cover	■ Verkehrsweiß (ähnlich RAL 9016) ■ Dunkelgrau (ähnlich RAL 7021) ■ Tiefschwarz (ähnlich RAL 9005) ■ Messing Zu Farben der Cover siehe auch Oberflächen
	Rosette	■ Nickel gebürstet, lackiert ■ Messing gebürstet, lackiert
	Drücker	■ Edelstahl gebürstet, lackiert ■ Messing gebürstet, lackiert

Maßzeichnungen SmartHandle AX

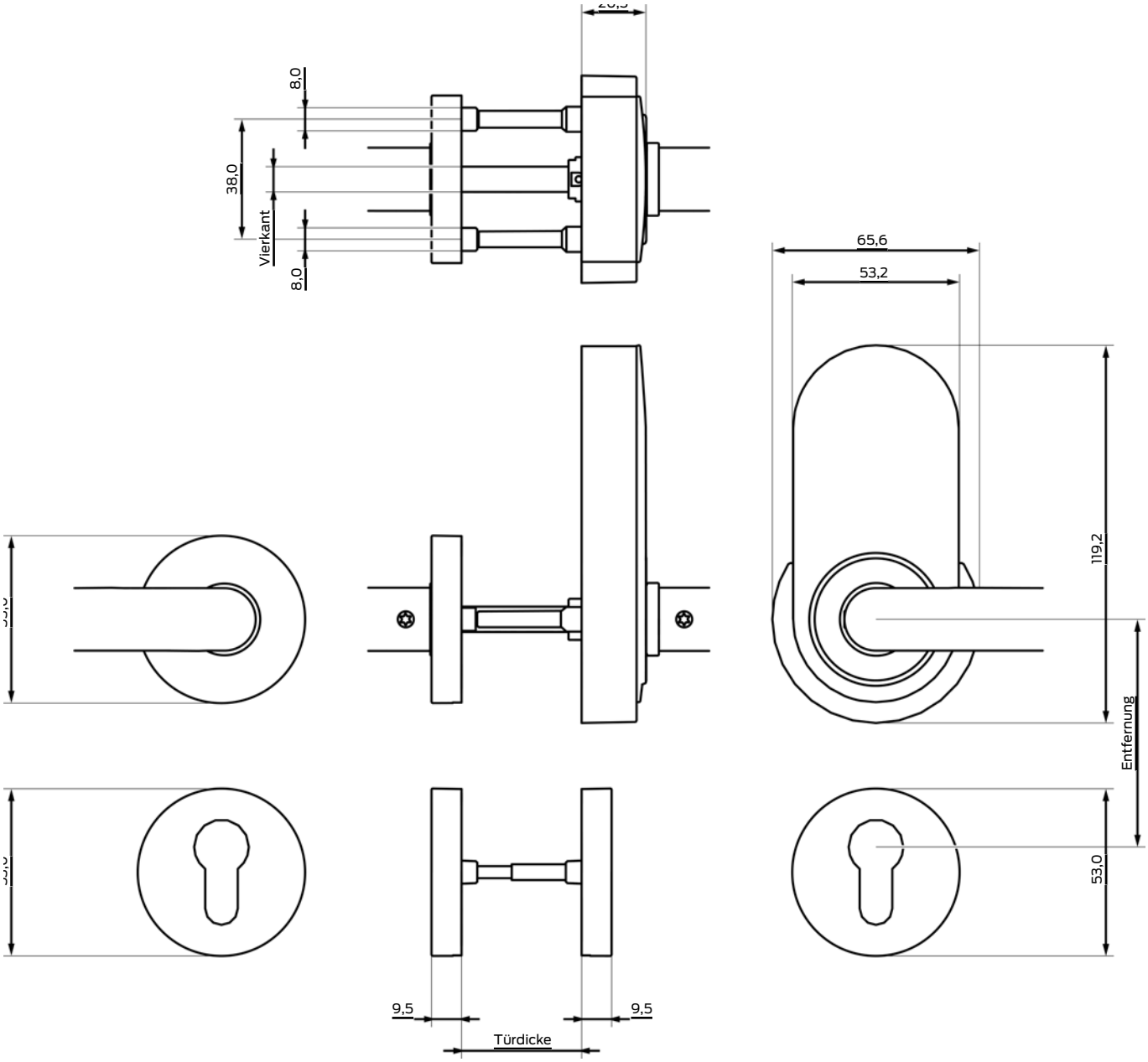
HINWEIS

Höhe ist variantenabhängig (siehe Tabelle).

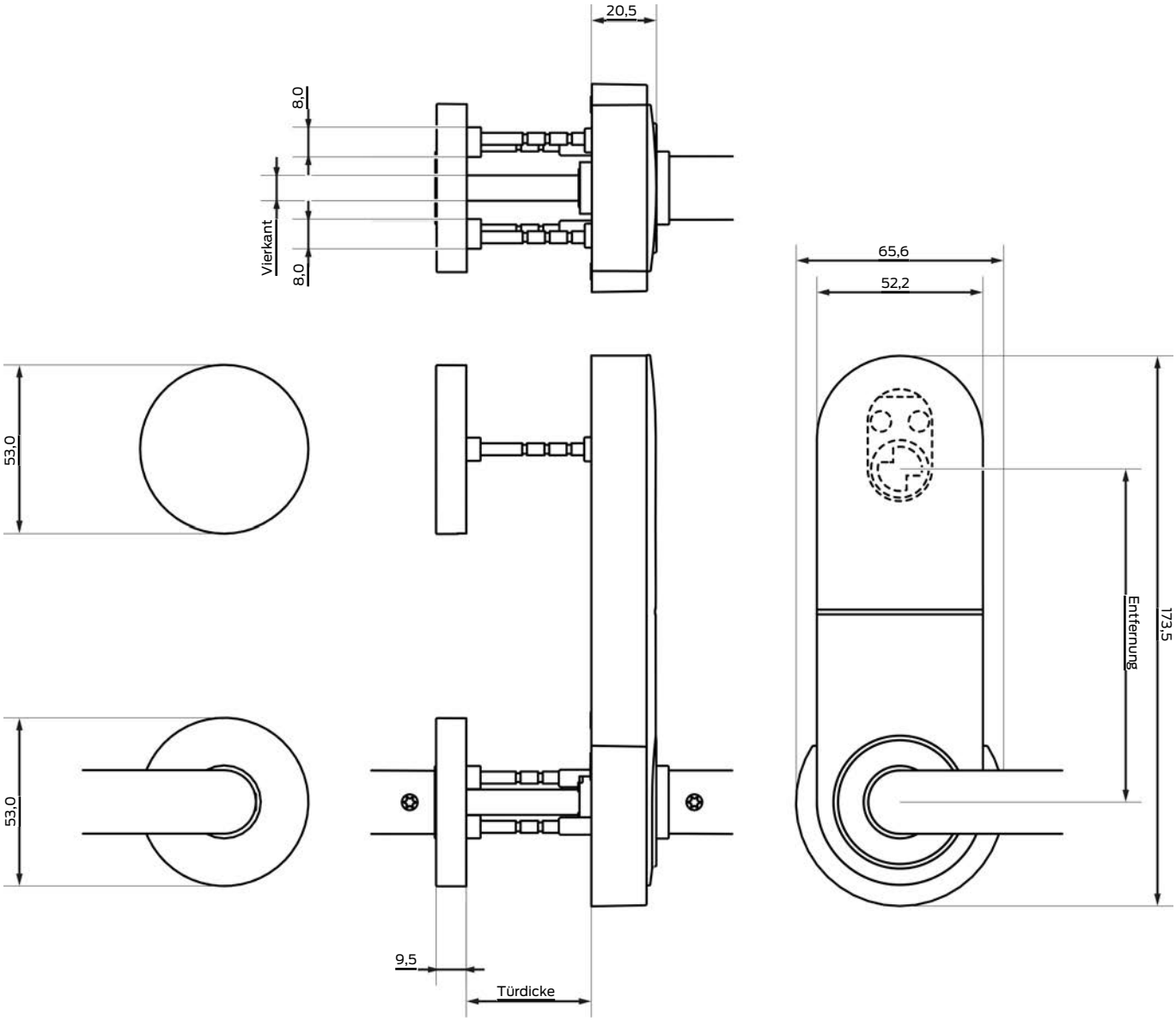
Hängende Montage



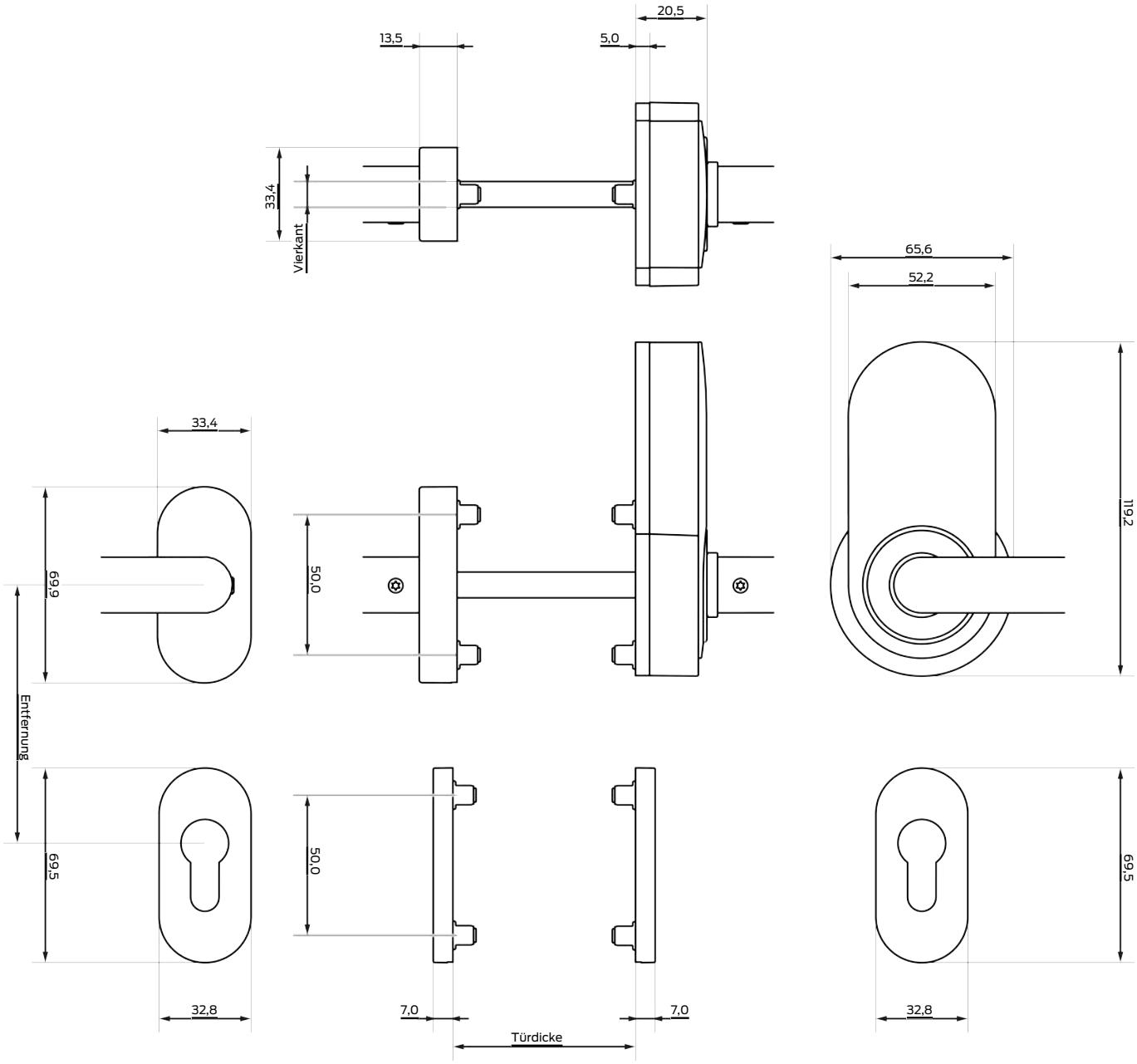
Stehende Montage



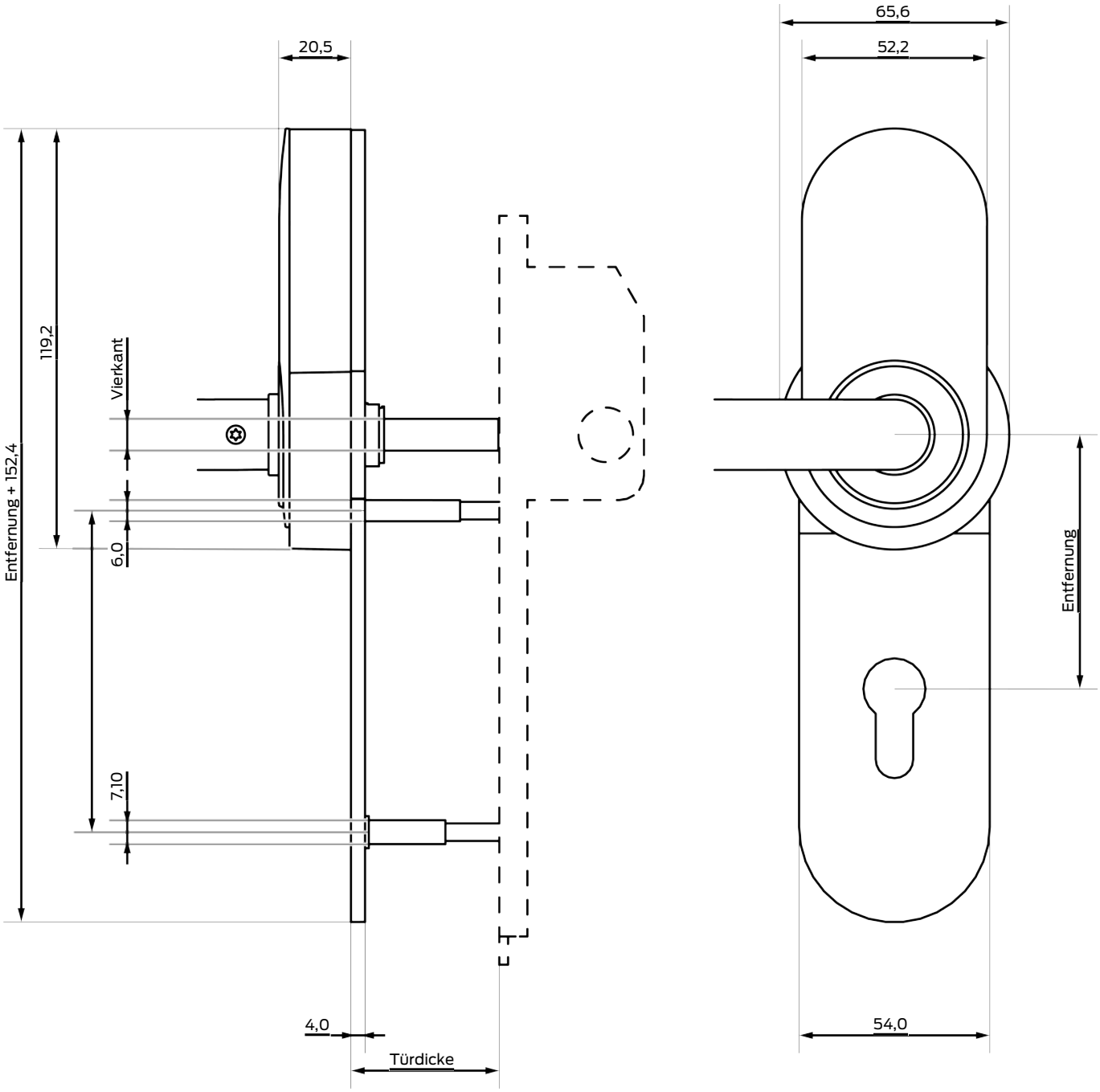
Scandinavian Oval



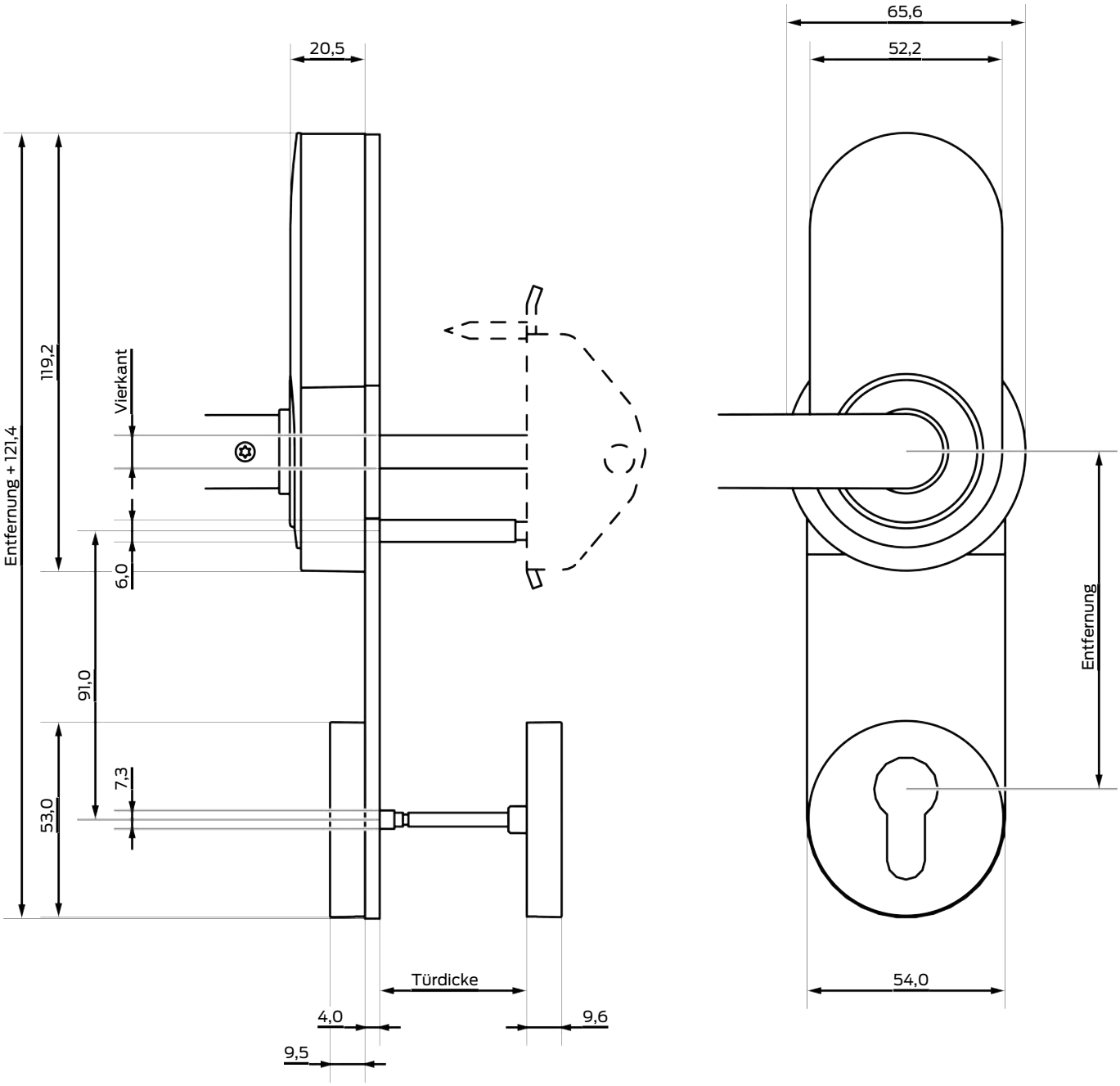
Rohrrahmen


20,5
13,5
5,0
33,4
Vierkant
65,6
52,2
33,4
69
50,0
119,2
Entfernung
69,5
50,0
69,5
32,8
7,0
7,0
Türdicke
32,8

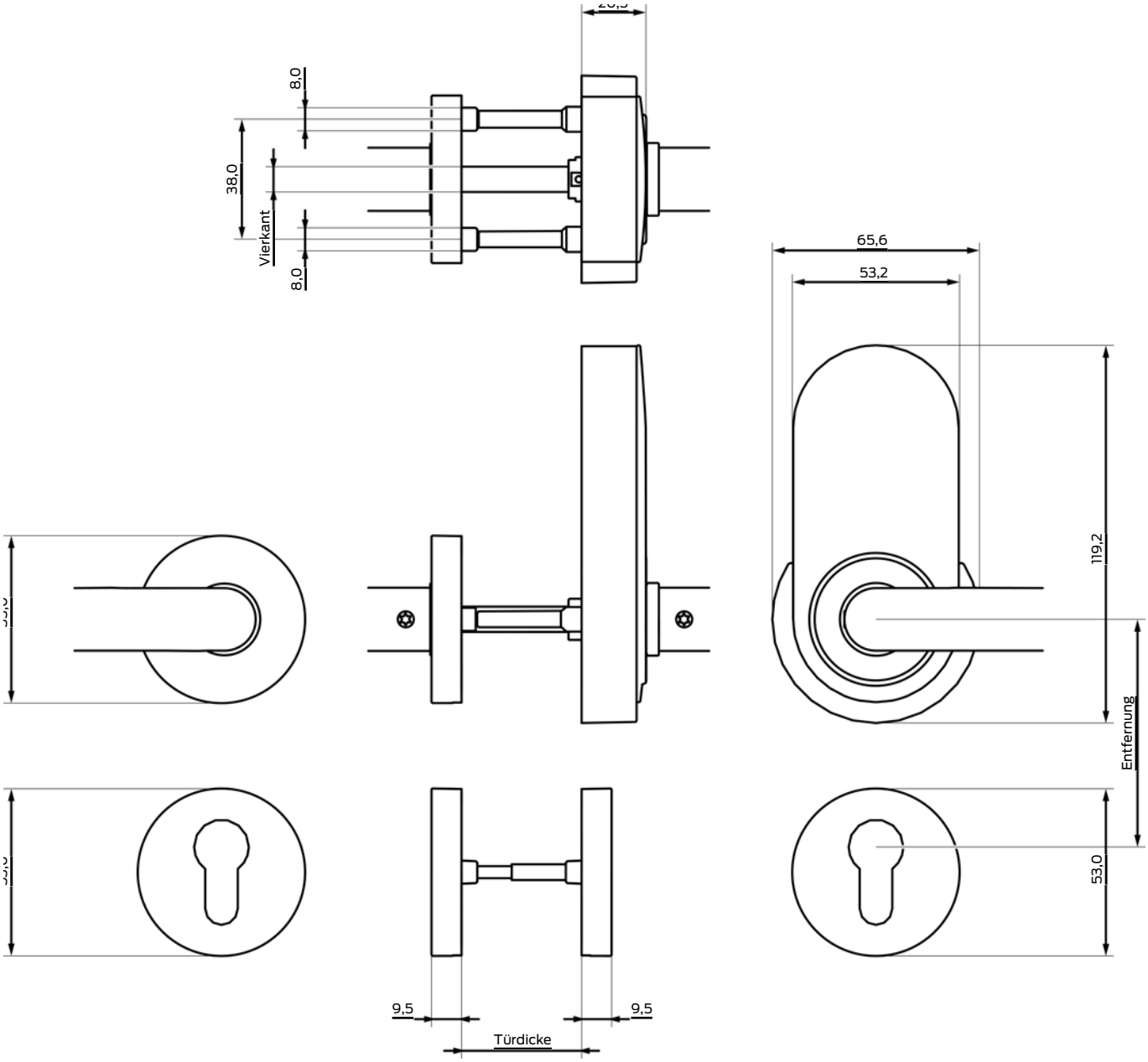
Panikstangen (CISA)



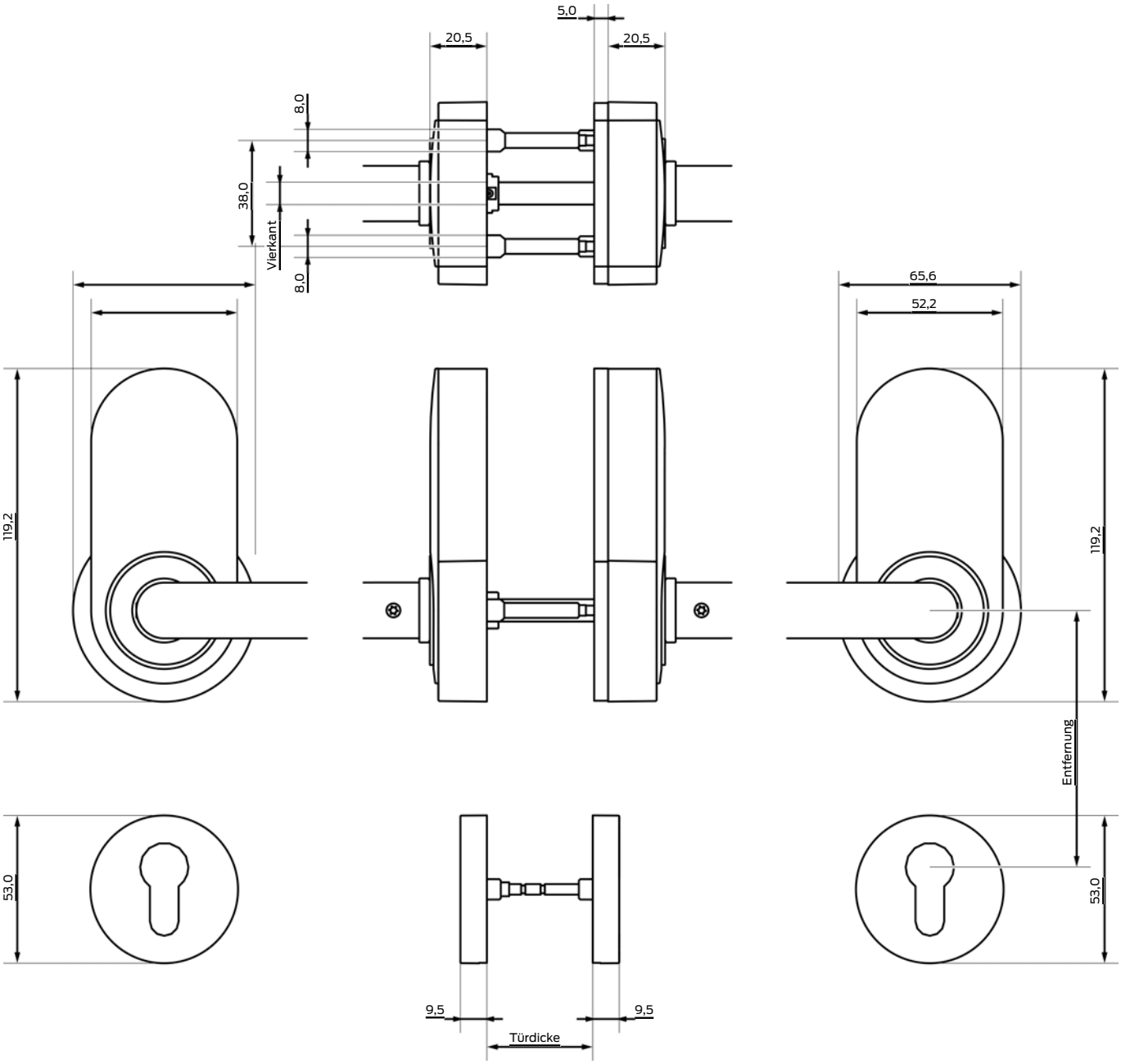
Panikstange (BKS)



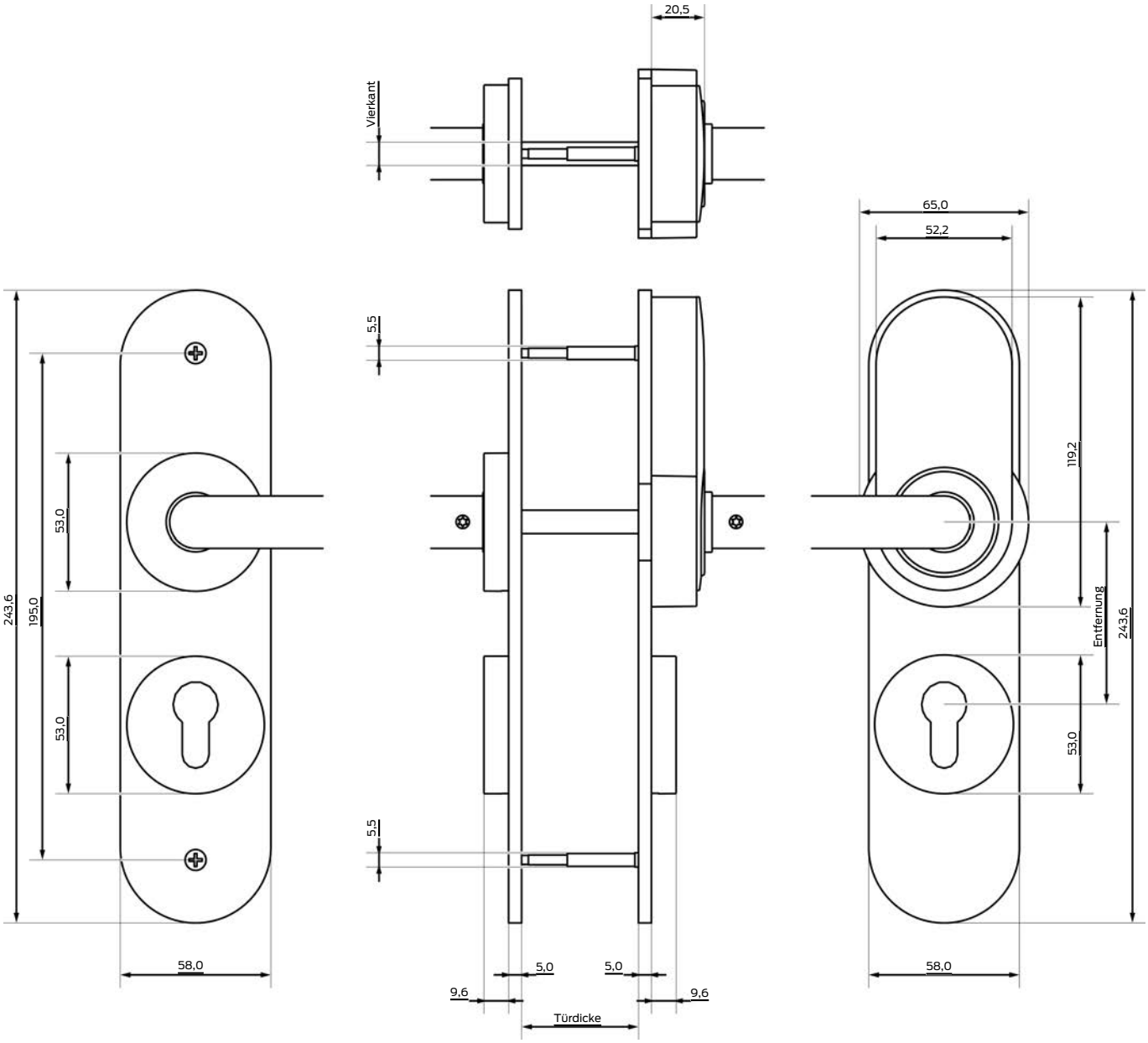
PAS24


8,0
38,0
Vierkant
8,0
65,6
53,2
119,2
Entfernung
53,0
9,5
9,5
Türdicke

Beidseitig lesend

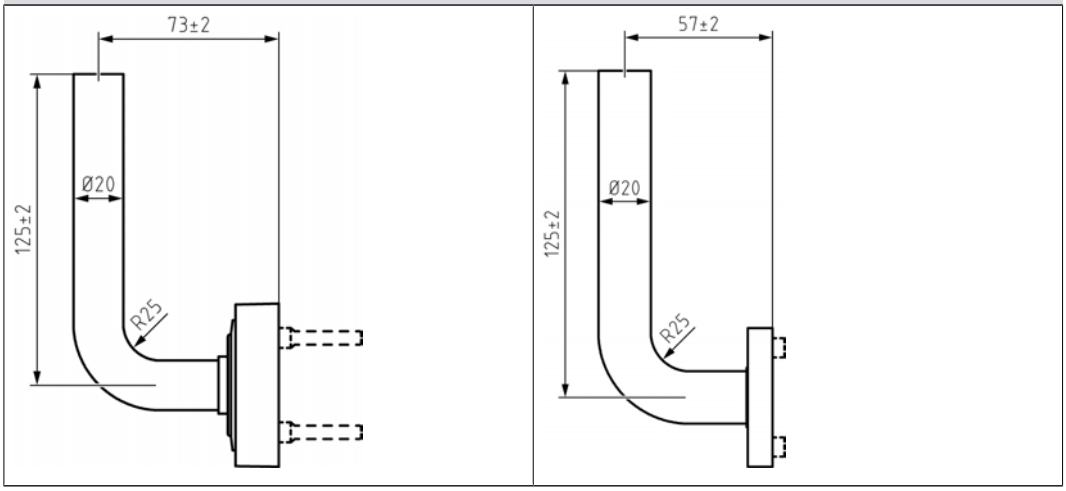


Französisches 195-mm-Schild

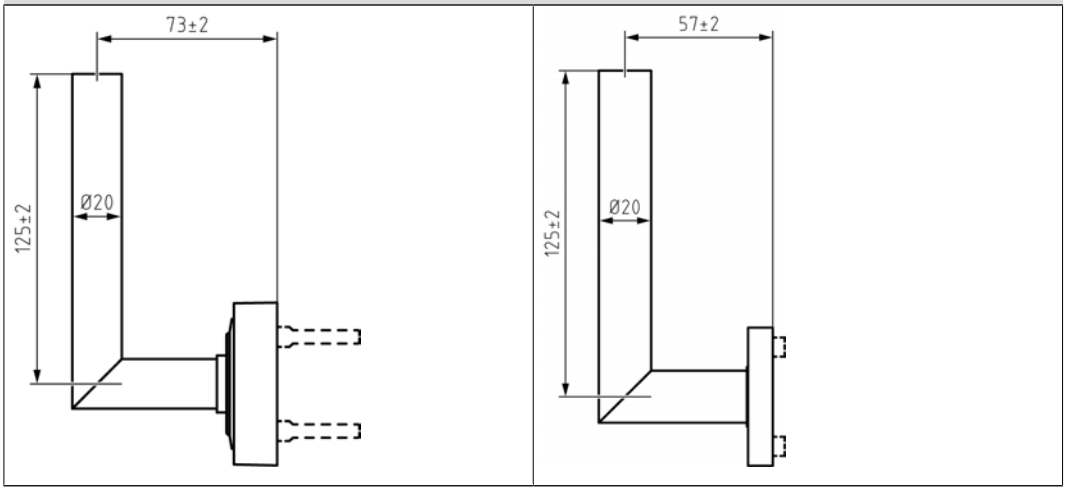


Maßzeichnungen Drücker

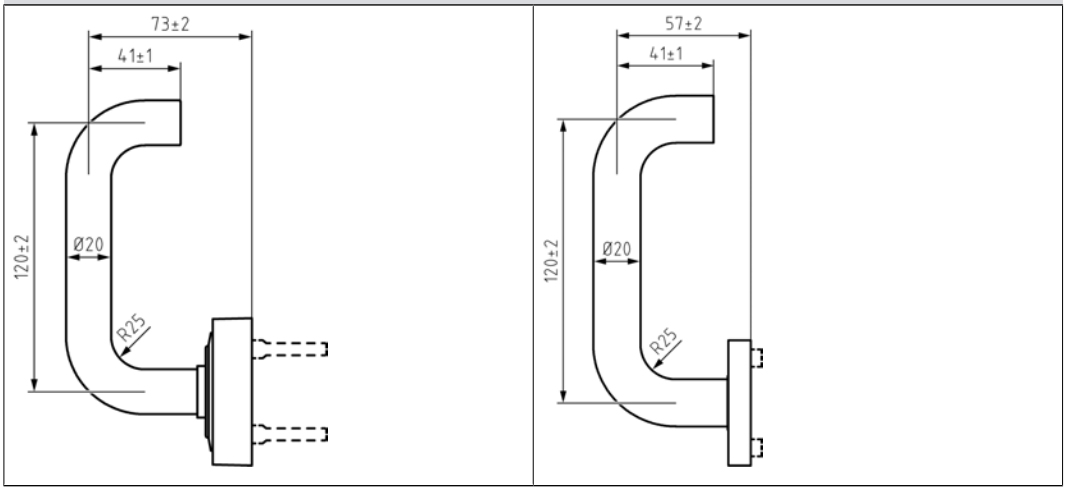
Form A (Außen/Innen)



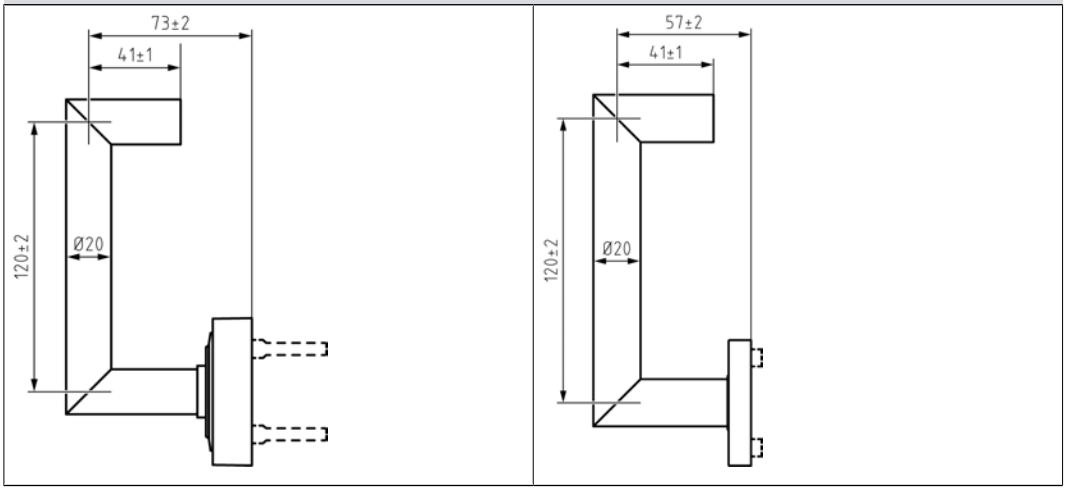
Form B (Außen/Innen)



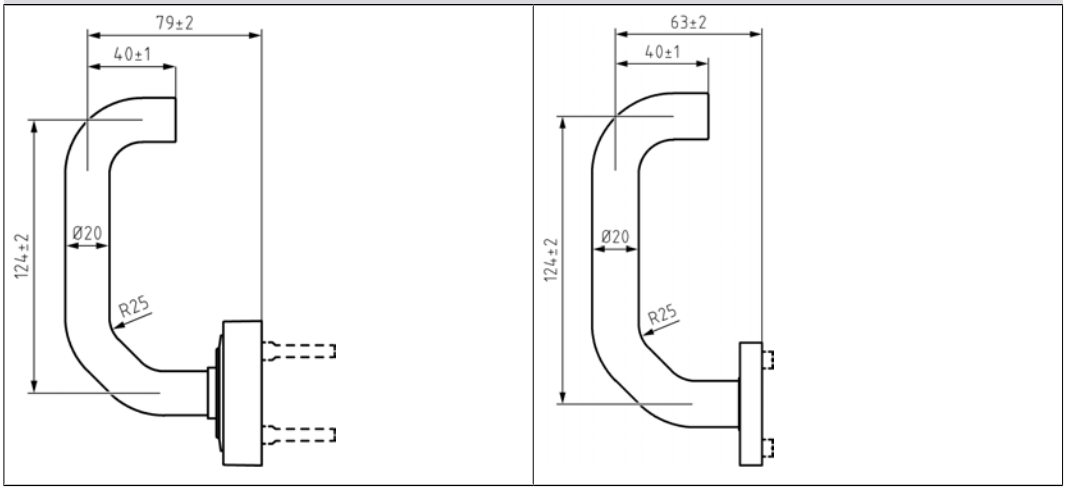
Form C (Außen/Innen)



Form D (Außen/Innen)

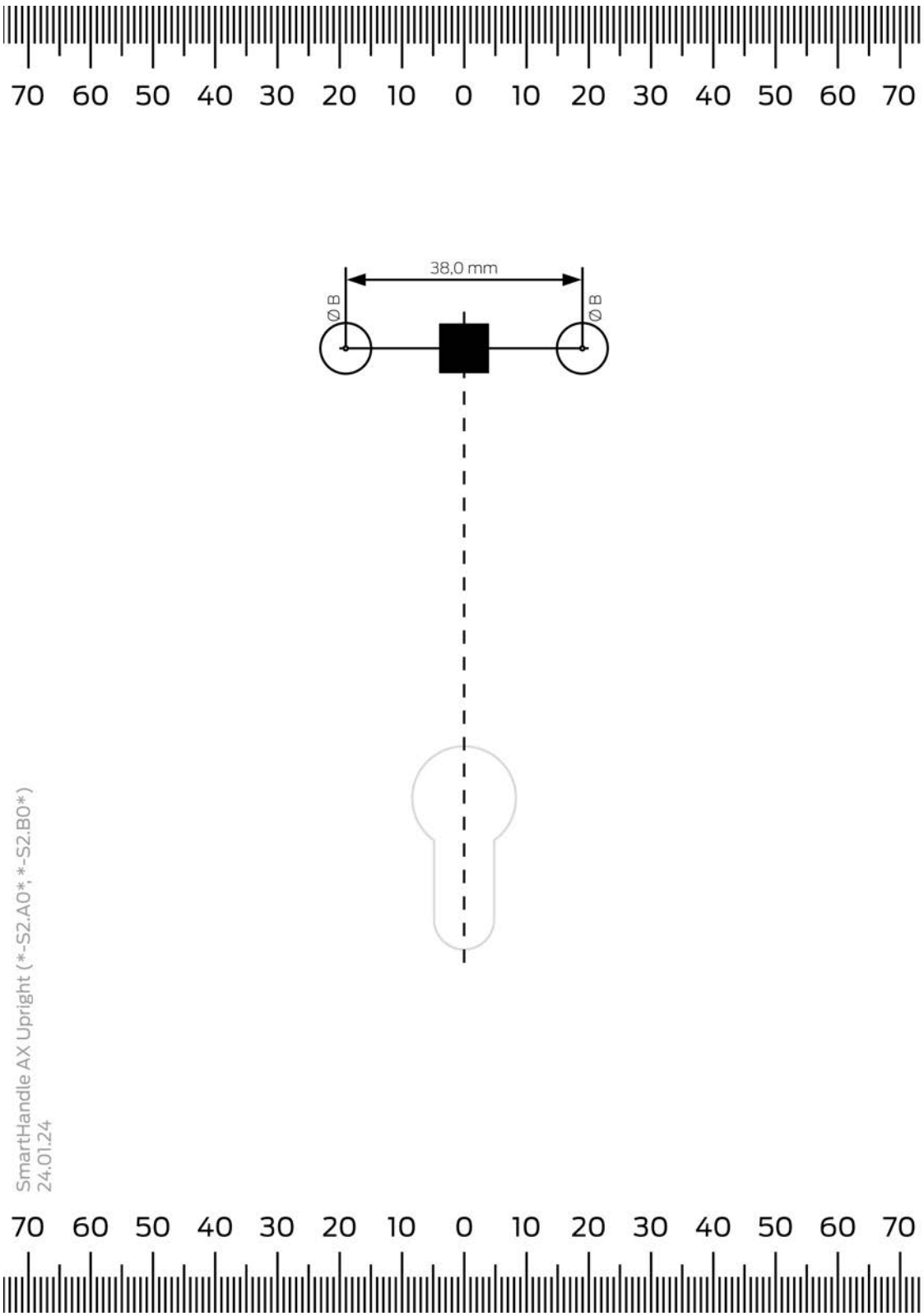


Form L (Außen/Innen)

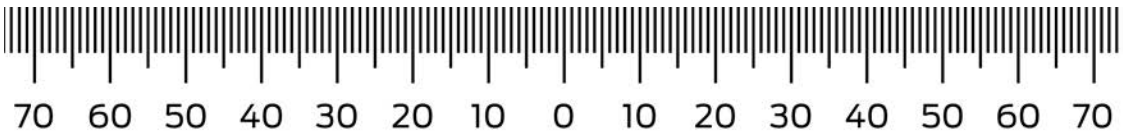


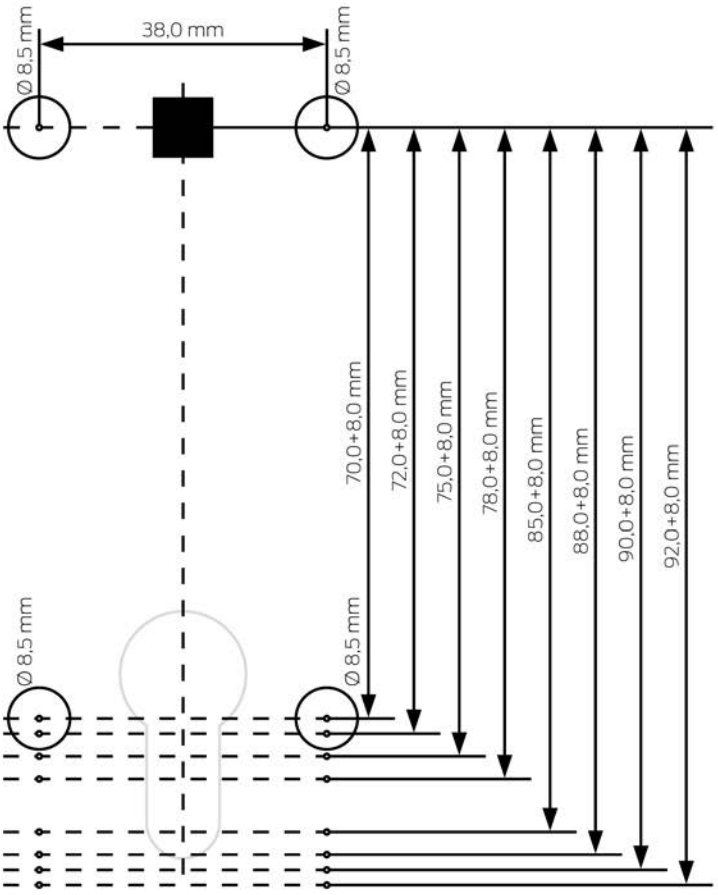
Bohrschablonen

Bohrschablone für Variante A0 (Stehende Montage)



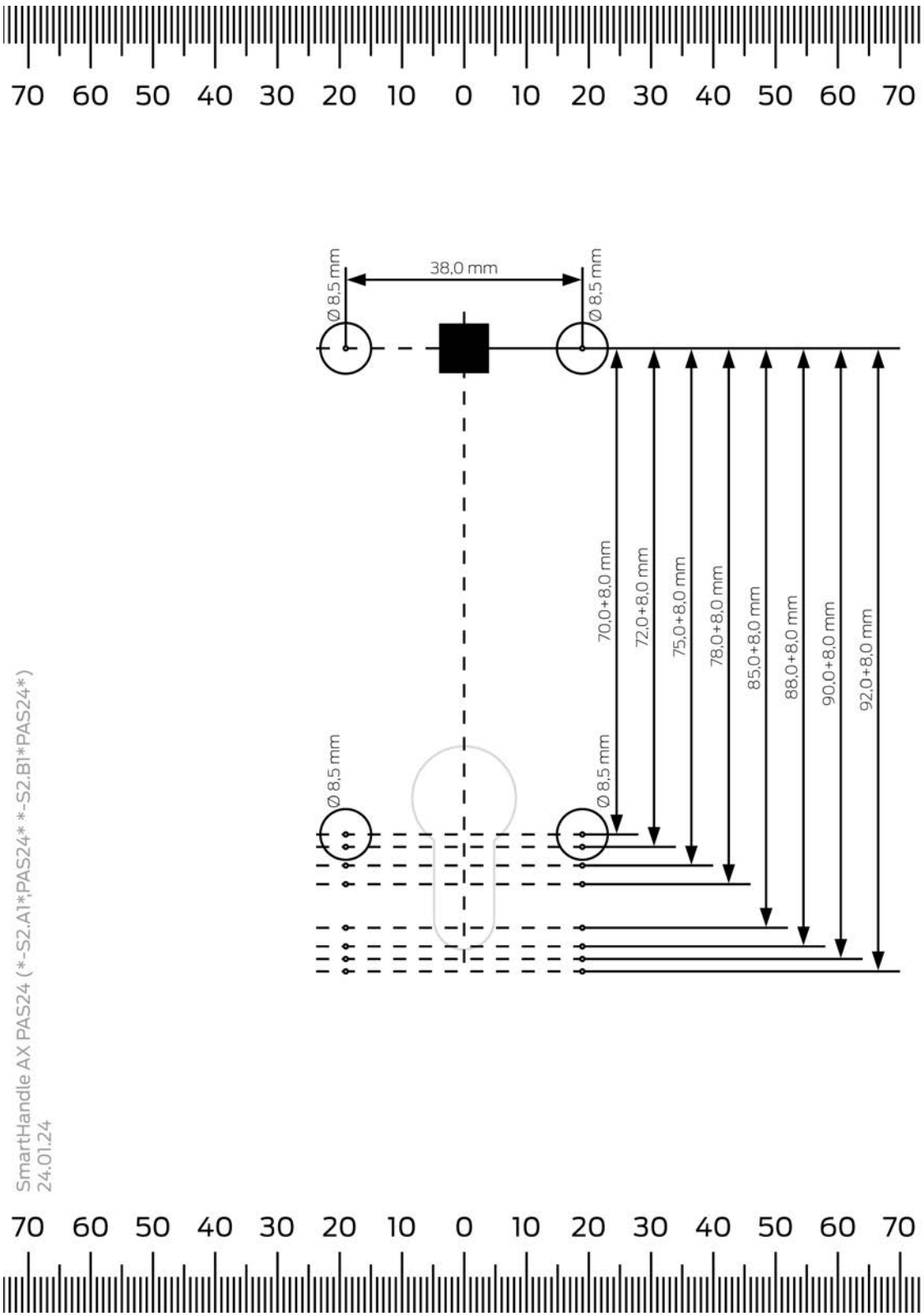
Bohrschablone für Variante A1 und A2 (Hängende Montage)



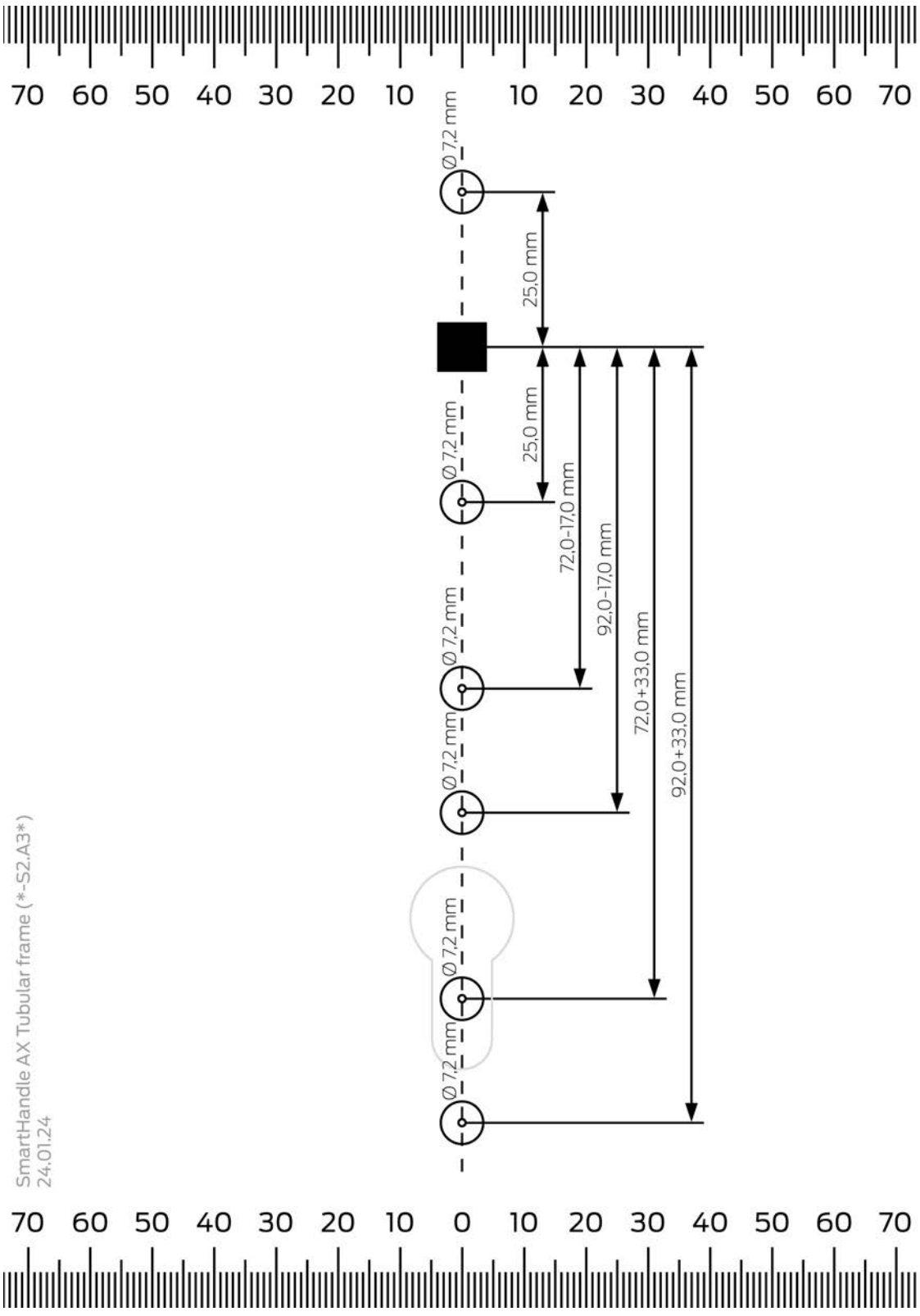


SmartHandle AX Downward installation (*-S2.A1*; *-S2.B1*)
24.01.24

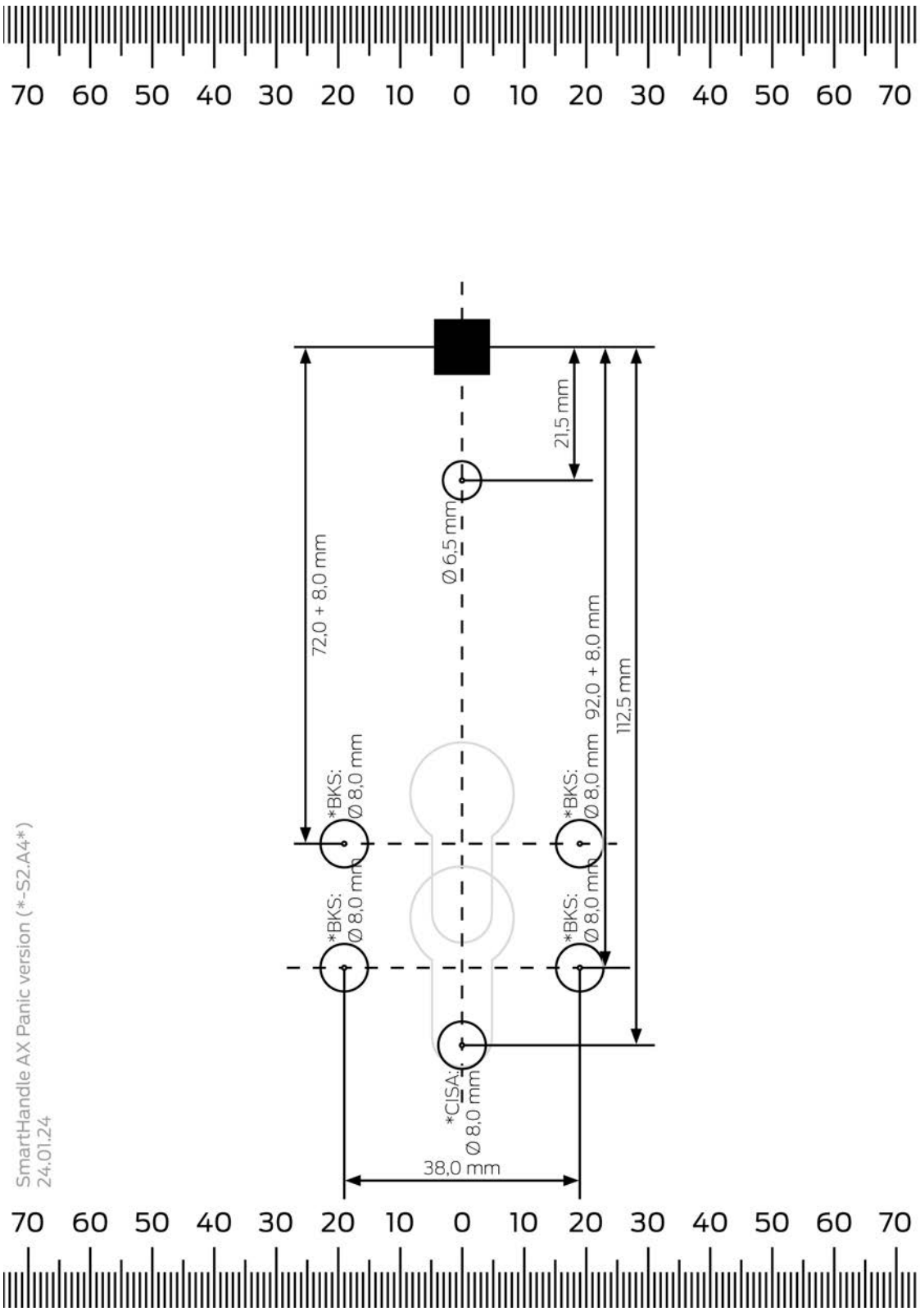
Bohrschablone für Variante A1.PAS24 (Hängende Montage mit PAS24)



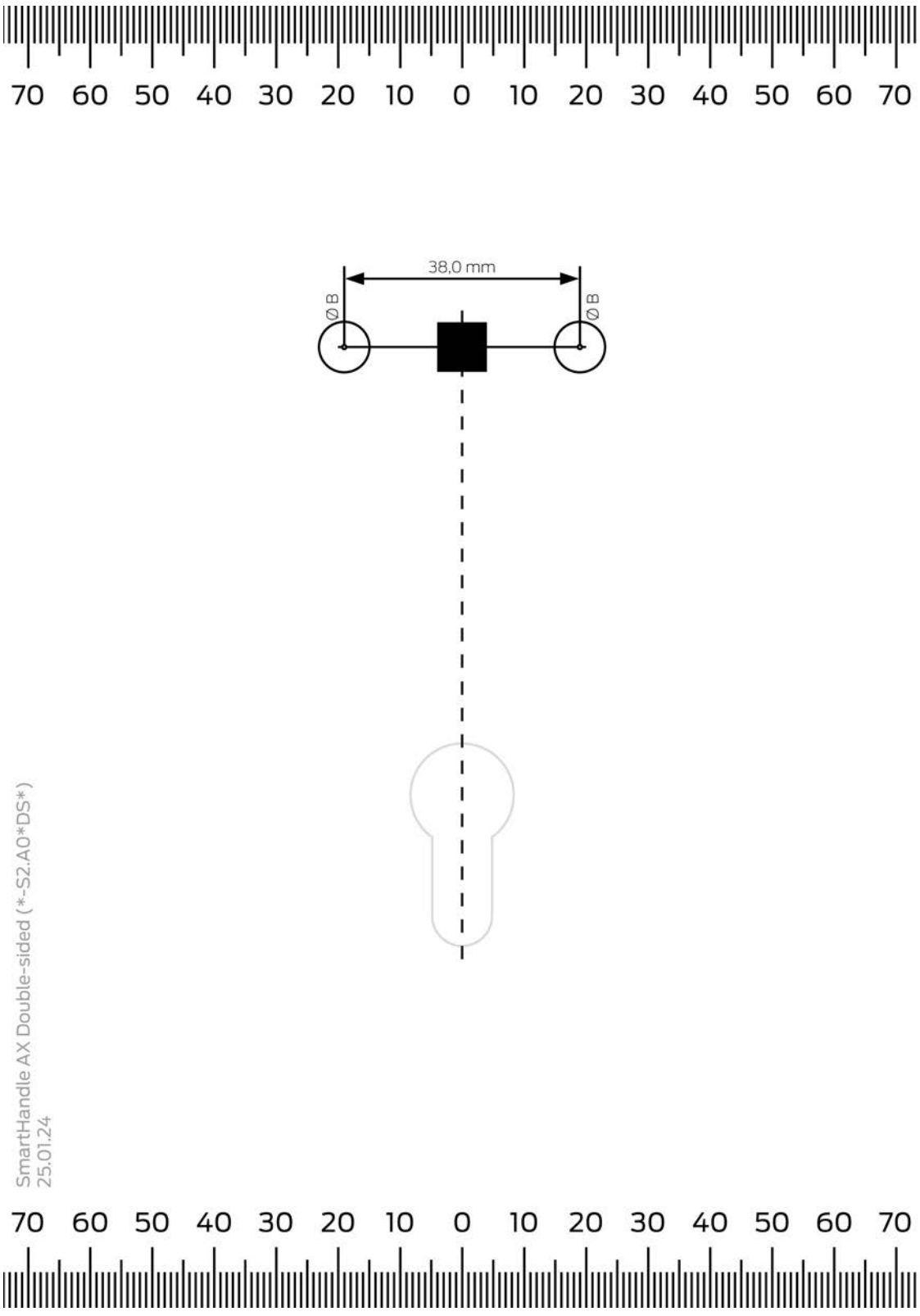
Bohrschablone für Variante A3 (Rohrrahmen)



Bohrschablone für Variante A4.P11/A4.P1/A4.P2 (Panikstangen)



Bohrschablone für Variante DS (Beidseitig lesend)



6.8 SmartHandle 3062

Das SmartHandle 3062 bewegt die Falle des Einsteckschlosses.
Verwenden Sie ein SmartHandle AX oder ein SmartHandle 3062, wenn Sie Türen nur schließen wollen (Innentüren).

Wenn Türen auch verriegelt werden sollen, dann können Sie ein SmartHandle mit einem selbstverriegelnden Einsteckschloss kombinieren.

Varianten, Ausstattungsmerkmale, Montage...

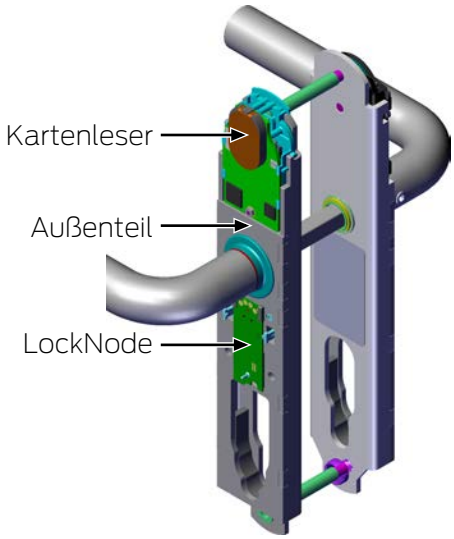
Detaillierte Informationen finden Sie im Handbuch des SI.SmartHandle.

6.8.1 Aufbau

Das SmartHandle 3062 besteht immer aus zwei Seiten:

Master (Innenseite)	Slave (Außenseite)
■ Central Unit (= CU) ■ Batterien	■ Kartenleser (Card Reader = CR) ■ LockNode (LN)
■ Immer auf der Innenseite der Tür ■ Dauerhaft eingekuppelt	■ Immer auf der Außenseite der Tür ■ Nur mit Identifikationsmedium einkuppelbar

Während der Montage werden die beiden Hälften voneinander getrennt.



Je nach Variante und Ausstattung unterscheidet sich der Aufbau:

Escape&Return (.ER)

Master (Innenseite)	Slave (Außenseite)
■ Central Unit (= CU) ■ Batterien ■ Sensoren für Escape&Return	■ Kartenleser (Card Reader = CR) ■ LockNode (LN)

Master (Innenseite)	Slave (Außenseite)
■ Immer auf der Innenseite der Tür ■ Dauerhaft eingekuppelt	■ Immer auf der Außenseite der Tür ■ Nur mit Identifikationsmedium einkuppelbar

DoorMonitoring (.DM)

DoorMonitoring-SmartHandles erkennen mithilfe von Sensoren verschiedene Türzustände.

Master (Innenseite)	Slave (Außenseite)

■ Central Unit (= CU)
■ Batterien
■ Sensoren für DoorMonitoring
  ■ Innendrücker-Sensor
  ■ Riegel (nur zusammen mit einem selbstverriegelnden Einsteckschloss, in dem wahlweise ein SimonsVoss-Sensor oder ein Fremdhersteller-Sensor verbaut ist - siehe Liste der kompatiblen Sensorschlösser)
  ■ Stulpschraubensensor im Einsteckschloss
	■ Kartenleser (Card Reader = CR)
	■ LockNode (LN)

■ Immer auf der Innenseite der Tür ■ Dauerhaft eingekuppelt	■ Immer auf der Außenseite der Tür ■ Nur mit Identifikationsmedium einkuppelbar

Die Empfindlichkeit der Sensoren wird im SmartIntego-Tool eingestellt. Wenn einer der Sensoren eine Änderung wahrnimmt, dann wird diese Änderung sofort an das Integratorsystem weitergeleitet.

Das DoorMonitoring-SmartHandle 3062 kann folgende Zustände erkennen:

- Eingekuppelt/Ausgekuppelt
- Drücker gedrückt/nicht gedrückt (Innendrücker und wenn eingekuppelt auch Außendrücker)
- Tür offen

- Tür geschlossen
- Tür zu lange offen (Einstellbarer Timer im SmartHandle)
- Tür geschlossen, nachdem sie zu lang offen war
- Tür verriegelt (nur zusammen mit einem selbstverriegelnden Einsteckschloss)
- Tür entriegelt (nur zusammen mit einem selbstverriegelnden Einsteckschloss)
- Manipulationsversuche
  - Stulpschraube
  - Einbruchsversuch
  - Störung der Sensorik
  - Manipulation am Drücker

Details entnehmen Sie bitte der Dokumentation des Integratorsystems.

HINWEIS

Programmierfehler bei unterbrochener oder geänderter Master-Slave-Paarung

Der Master und der Slave sind werkseitig als zusammengehörig konfiguriert. Der Austausch von Knäufen führt zu Programmierfehlern.

Bei der Programmierung kommunizieren Master und Slave.

- Stellen Sie sicher, dass Master und Slave während einer Programmierung physisch verbunden sind.

6.8.2 Werkzeug

Das mitgelieferte SmartHandle-Tool wird benötigt, um das Cover abzunehmen. Informationen zu weiteren benötigten Werkzeugen entnehmen Sie bitte der mitgelieferten Kurzanleitung.

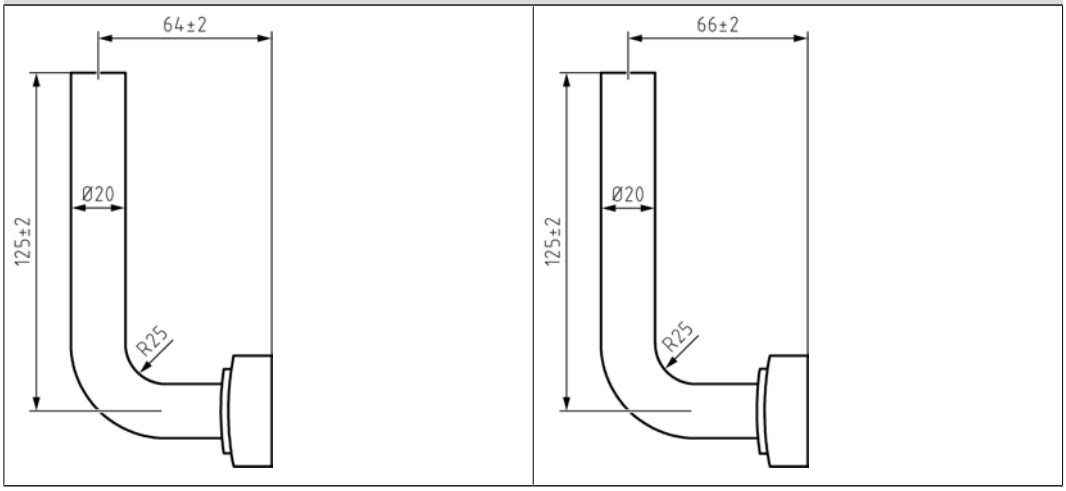
6.8.3 Technische Daten

Abmaße schmal (BxHxT)	41 x 224 x 14 mm
Abmaße breit (BxHxT)	53 x 224 x 14 mm
Batterielebensdauer (Online-Vernetzung WO):	80.000 Schließzyklen, 5 Jahre Standby
Batterielebensdauer (Offline-Vernetzung bzw. "virtuelle Vernetzung" SVCN):	50.000 Schließzyklen , 6 Jahre Standby
Batterietyp:	CR2450 3V Lithium
Batteriehersteller	■ Duracell ■ Murata ■ Panasonic
Anzahl Schließungen pro GatewayNode:	16
Temperaturbereich (Betrieb)	–20 °C bis +50 °C
Whitelistfunktion:	250 Offlinekarten
Einträge in der Zutrittsliste	Max. 1.000 (WO: 250)
Schutzart	IP 40 (WP Version: IP 45 für Außenseite)
Online-Vernetzung: Kartentechnologie	■ MIFARE Classic ■ MIFARE DESFire EV1 ■ UID nach 14443 von MIFARE, LEGIC advant und HID iCLASS
Virtuell (VN-Offline): Kartentechnologie	■ MIFARE Classic ■ MIFARE DESFire EV1
Feedback:	Buzzer + LED (Blau/rot)
Direkt vernetzbar (nur bei SmartIntego Wireless Online)	Integrierter LockNode

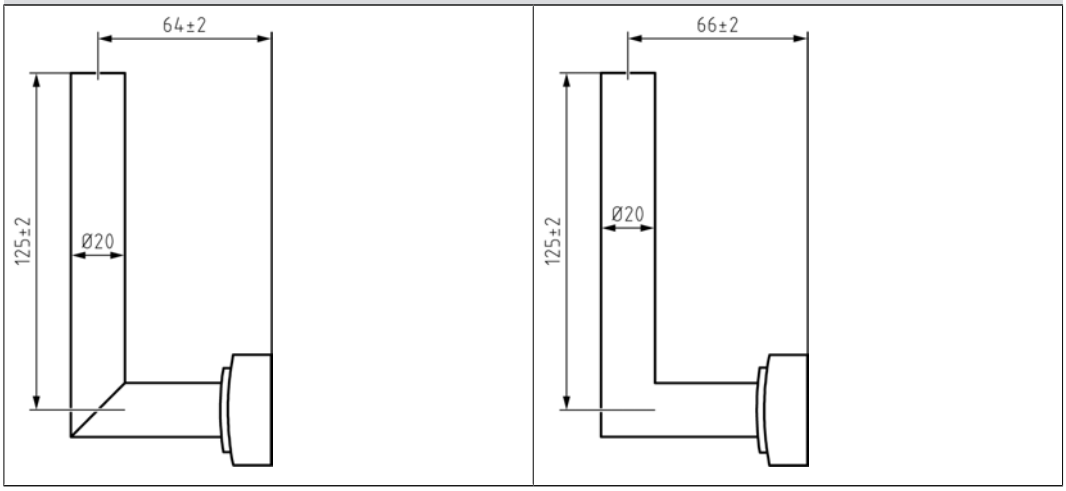
Funkemissionen

6.8.3.1 Maßzeichnungen Drücker

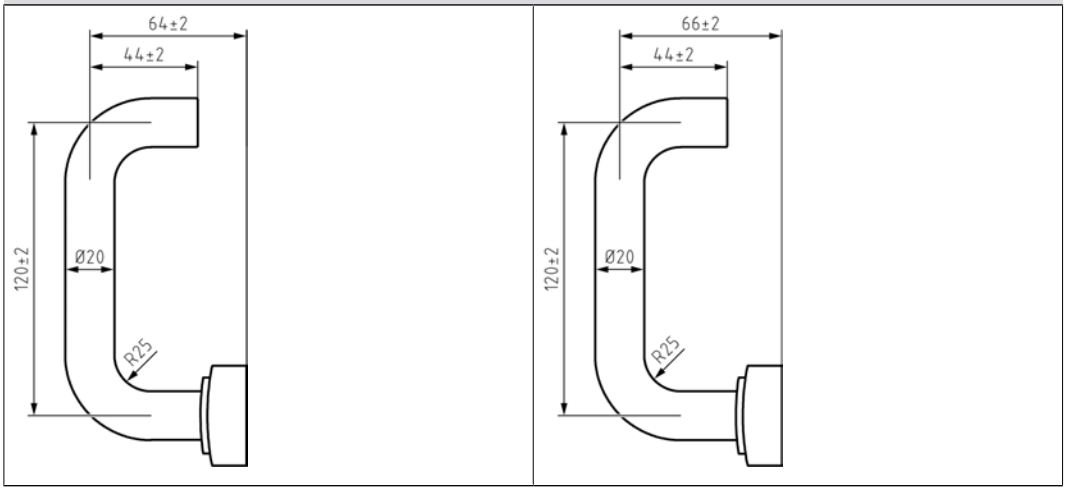
Form A (Außen/Innen)



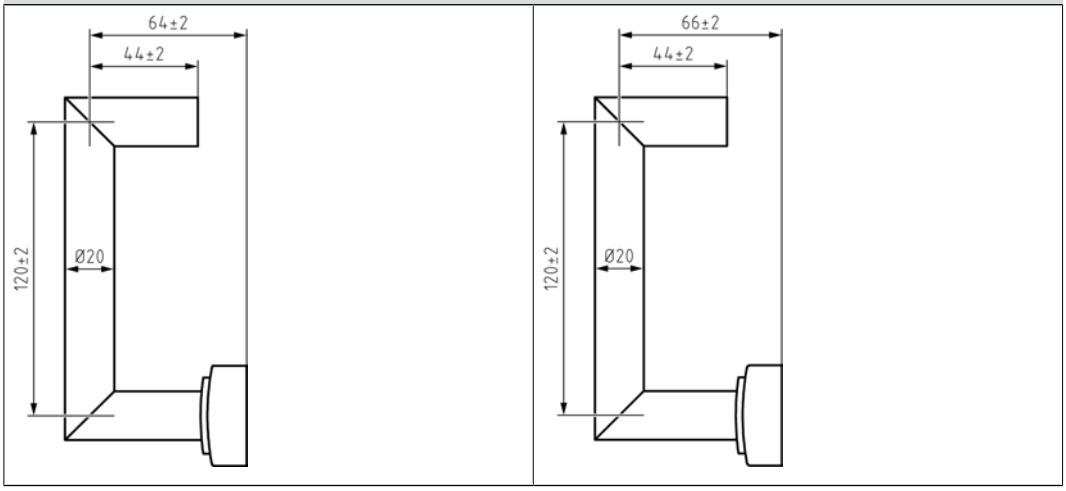
Form B (Außen/Innen)



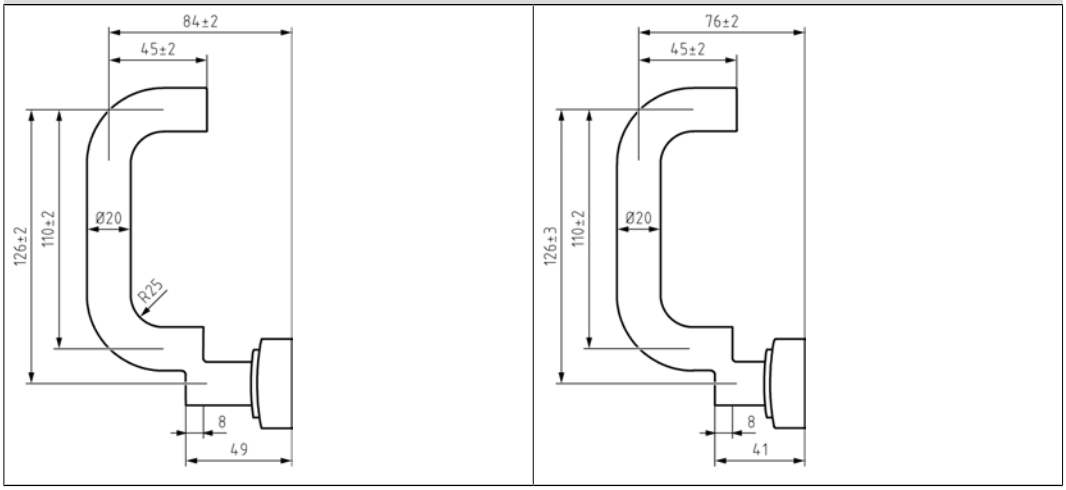
Form C (Außen/Innen)



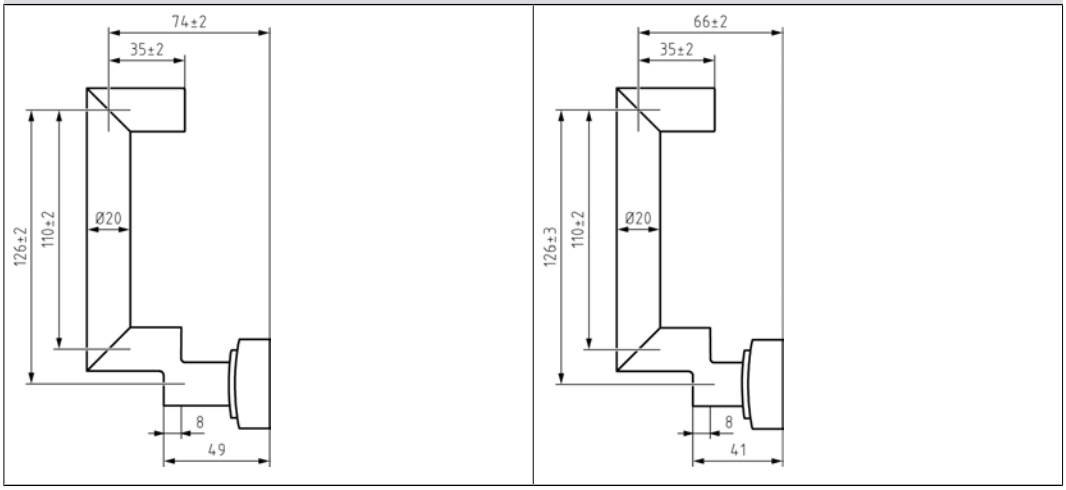
Form D (Außen/Innen)

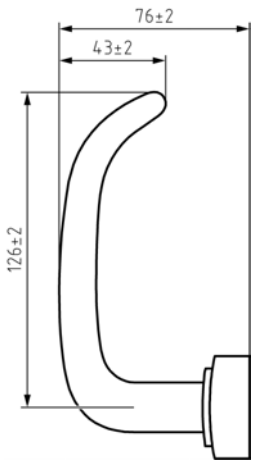
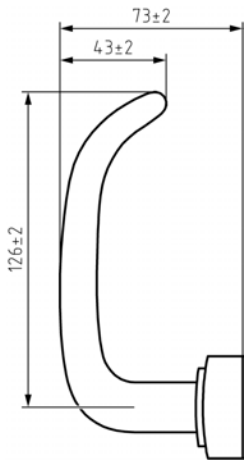


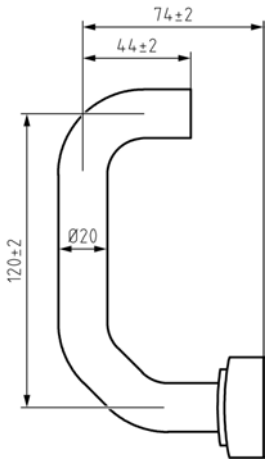
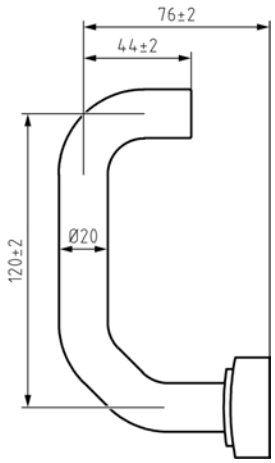
Form E (Außen/Innen)



Form F (Außen/Innen)



Form G (Außen/Innen)	
	

Form H (Außen/Innen)	
	

6.9 Vorhangschloss

Das SimonsVoss-Vorhangschloss funktioniert wie ein normales mechanisches Vorhangschloss. Es wird jedoch durch einen elektronischen Knauf entriegelt und verriegelt und erweitert die Funktionen eines mechanischen Vorhangschlosses mit den Vorteilen elektronischer Schließungen.

6.9.1 Technische Daten

Vorhangschloss mit 8 mm Bügeldurchmesser	
Abmessungen Schloss (BxHxT)	51 x 70 x 25 mm *(ohne Zylinderknauf; ohne Bügel)*
Bügelinnenhöhe	25 mm oder 60 mm (jeweils Manuellverriegelnd oder Selbstverriegelnd)
Schutzklasse Schloss	Klasse 3 nach EN12320

Vorhangschloss mit 11 mm Bügeldurchmesser

Abmessungen Schloss (BxHxT)	60 x 72,5 x 25 mm *(ohne Zylinderknauf; ohne Bügel)*
Bügelinnenhöhe	Manuellverriegelnd: 35 mm Selbstverriegelnd: 50 mm
Schutzklasse Schloss	Klasse 4 nach EN12320

Technische Daten zur Schließung	
Batterietyp	2x CR2450 3V Lithium *(Duracell, Murata, Panasonic)*
Batterielebensdauer SmartIntego	Wireless Online (WO): Bis zu 5 Jahre Standby / 80000 Betätigungen SmartIntego Virtual Card Network (SVCN): Bis zu 6 Jahre Standby / 50000 Betätigungen

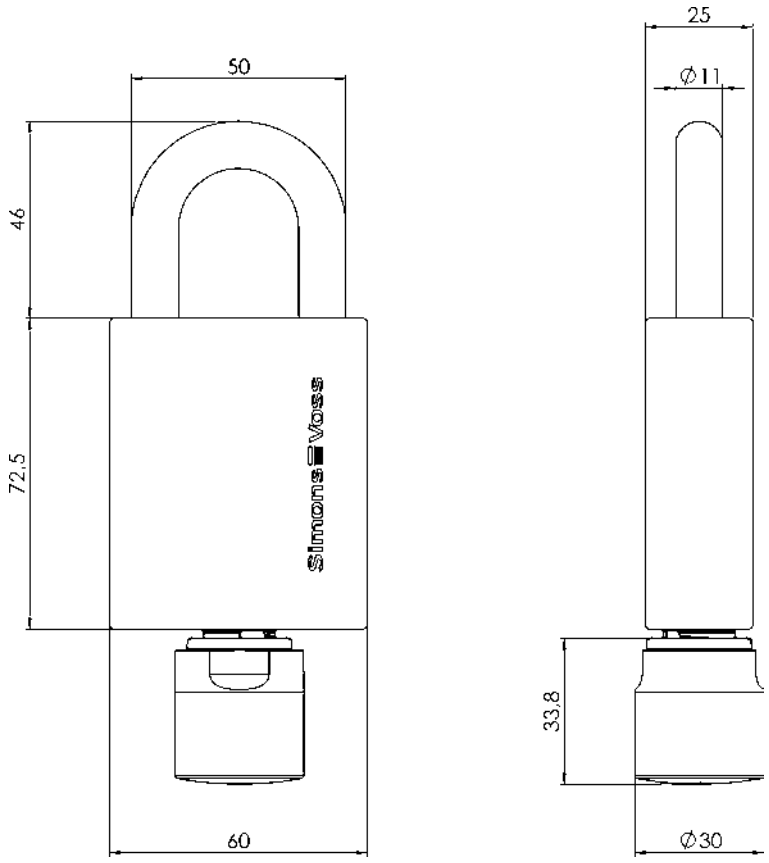
Schutzart	IP66
Temperaturbereich	Betrieb: -25°C bis +65°C Lagerung: -35°C bis +50°C
Speicherbare Zutritte (.ZK für System 3060 bzw. MobileKey)	▪ System 3060 bzw. MobileKey: Bis zu 3.000 ▪ SmartIntego: Bis zu 1.000 (WO: 250)
Zeitzonengruppen (.ZK)	100+1 (G2)

Anzahl der Medien, die pro Vorhangschloss verwaltet werden können	Transponder: bis zu 64.000 (G2) SmartCards (G2): bis zu 32.000 (in Abhängigkeit der Konfiguration / Template)
Netzwerkfähigkeit	Direkt vernetzbar mit integriertem LockNode, LockNode nachrüstbar
Sonstiges	Version mit Zutrittskontrolle, Zeitzonensteuerung und Protokollierung
Dauer/offen Modi	Zeitgesteuerter Flip-Flop-Modus (Zeitumschaltung) möglich: zeitgesteuert automatisches bzw. zeitgesteuert manuelles (in Zusammenspiel mit Transponder) ein- und auskuppeln. Einkuppelphase kann optional mit einem Transponder unterbrochen werden.

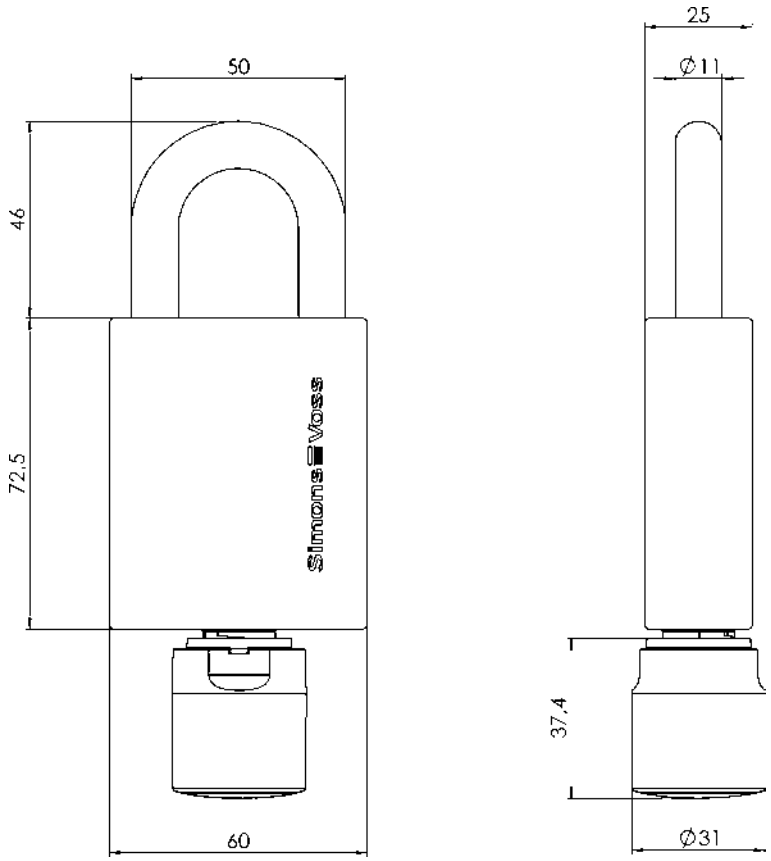
Funkemissionen

6.9.1.1 Maßzeichnungen Vorhangschlösser

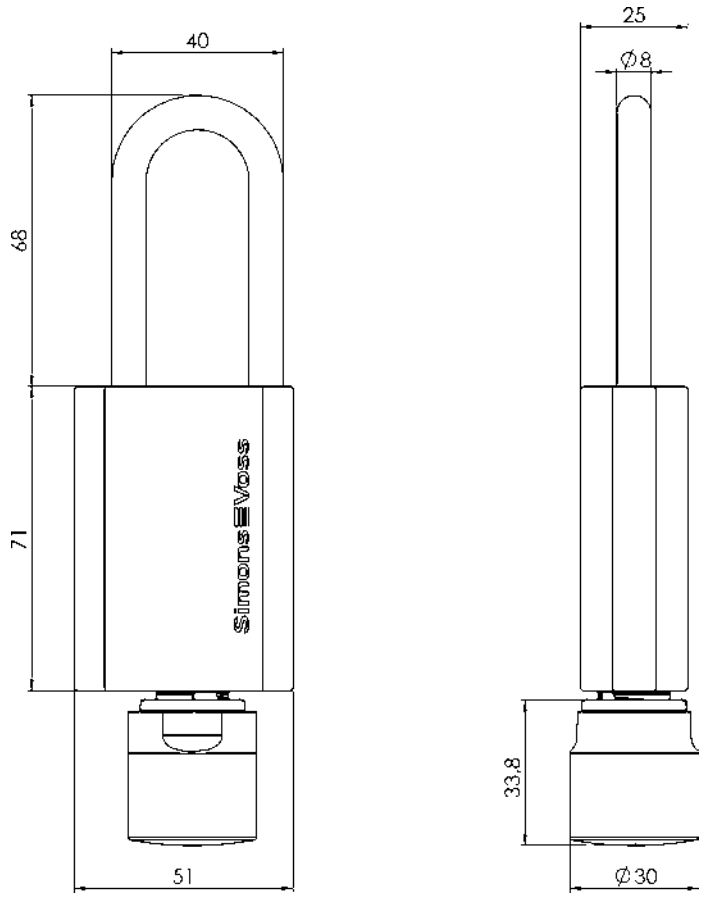
Vorhangschloss 11 mm - Aktiv (PL)



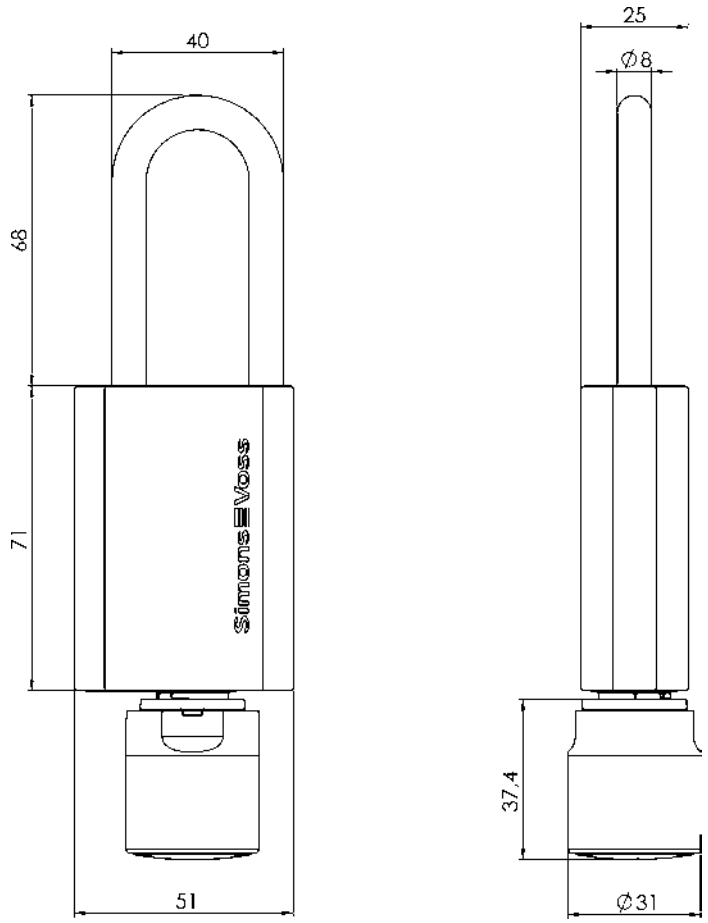
Vorhangschloss 11 mm - Passiv (PL MP)



Vorhangschloss 8 mm - Aktiv (PL)



Vorhangschloss 8 mm - Passiv (PL MP)



6.10 Generelle Signalisierung und Abläufe der SmartIntego-Schließungen

Die Signale sind generell in folgendes Schema aufgeteilt:

- Vorgang
- Aktion/Reaktion der Schließung
- LED (Anzahl, Farbe, Dauer)
- Töne (Anzahl, Dauer)

Kurzzeit-Kuppeln

Vorgang	Aktion/Reaktion	LED	Töne
Kurzzeit-Einkuppeln (Karte)	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Einkuppeln	2× Blau (kurz)	2× Piepen (kurz)
	Während der Einkuppeldauer (Drei bis 25 Sekunden)		
	Auskuppeln		1× Piepen (kurz)

Vorgang	Aktion/Reaktion	LED	Töne
Kurzzeit-Einkuppeln (Remote-Befehl)	Einkuppeln	2× Blau (kurz)	2× Piepen (kurz)
	Während der Einkuppeldauer (Drei bis 25 Sekunden)		
	Auskuppeln		1× Piepen (kurz)

Langzeit-Kuppeln

Vorgang	Aktion/Reaktion	LED	Töne
Langzeit-Einkuppeln / FlipFlop (Karte)	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Einkuppeln	2× Blau (kurz-lang)	2× Piepen (kurz-lang)
	Während der Einkuppeldauer (Eine Minute bis dauerhaft)	Keine Reaktion	
Langzeit-Auskuppeln / FlipFlop (Karte)	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Auskuppeln	2× Blau (lang-kurz)	2× Piepen (lang-kurz)
Langzeit-Einkuppeln / FlipFlop (Remote-Befehl)	Einkuppeln	2× Blau (kurz-lang)	2× Piepen (kurz-lang)
	Während der Einkuppeldauer (Eine Minute bis dauerhaft)	Keine Reaktion	
Langzeit-Auskuppeln / FlipFlop (Remote-Befehl)	Auskuppeln	2× Blau (lang-kurz)	2× Piepen (lang-kurz)
Langzeit-Einkuppeln / FlipFlop (Zeitgesteuert)	Einkuppeln	2× Blau (kurz-lang)	2× Piepen (kurz-lang)
	Während der Einkuppeldauer (Eine Minute bis dauerhaft)	Keine Reaktion	
Langzeit-Auskuppeln / FlipFlop (Zeitgesteuert)	Auskuppeln	2× Blau (lang-kurz)	2× Piepen (lang-kurz)

Office-Modus

Vorgang	Aktion/Reaktion	LED	Töne
Office-Modus aktivieren (Karte kurz vorhalten)	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Einkuppeln	2× Blau (kurz)	2× Piepen (kurz)
	Während der Einkuppeldauer (Drei bis 25 Sekunden)	Keine Reaktion	
	Auskuppeln	2× Blau (kurz)	2× Piepen (kurz)
Office-Modus aktivieren (Karte lang vorhalten)	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Einkuppeln	2× Blau (kurz)	2× Piepen (kurz)
	Warten bis zweiten Lesevorgang	Keine Reaktion	
	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Während des Langzeit-Einkuppelns (Eine Minute bis dauerhaft)	Keine Reaktion	
Office-Modus deaktivieren (Karte lang vorhalten)	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Warten bis zweiten Lesevorgang	Keine Reaktion	
	Karte lesen und auskuppeln	2× Blau (lang-kurz)	2× Piepen (lang-kurz)
Office-Modus deaktivieren (Remote-Befehl)	Auskuppeln	2× Blau (lang-kurz)	2× Blau (lang-kurz)
Office-Modus deaktivieren (Zeitgesteuert)	Auskuppeln	2× Blau (lang-kurz)	2× Blau (lang-kurz)

Escape&Return

Vorgang	Aktion/Reaktion	LED	Töne
Escape&Return	Innendrücker betätigen und einkuppeln	2× Blau (kurz-lang)	2× Piepen (kurz-lang)
	Während der Einkuppeldauer (Signal kontinuierlich)	1× Rot (kurz)	1× Piepen (kurz)
	Auskuppeln	2× Blau (lang-kurz)	2× Piepen (lang-kurz)

Batterien

Vorgang	Aktion/Reaktion	LED	Töne
Batteriewarnung		Keine Reaktion	
Batteriewechselkarte	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Während der Batteriemessung	1× Blau (Zwei Sekunden)	
	Abschluss der Batteriemessung		1× Piepen (kurz)

WaveNet-Testkarte

Vorgang	Aktion/Reaktion	LED	Töne
WaveNet-Testkarte erfolgreich	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Kommunikation erfolgreich	4× Blau (kurz)	4× Piepen (kurz)
WaveNet-Testkarte nicht erfolgreich	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Während der Timeout-Wartezeit: Standardwert fünf Sekunden	Keine Reaktion	
	Kommunikation nicht erfolgreich	1× Rot (lang)	1× Piepen (lang)

Sonstiges

Vorgang	Aktion/Reaktion	LED	Töne
Unprogrammierte Schließung mit Karte aktivieren	Karte lesen und einkuppeln	2× Blau (kurz)	2× Piepen (kurz)
	Während der Einkuppeldauer (Fünf Sekunden)	Keine Reaktion	
	Auskuppeln		1× Piepen (kurz)
Timeout	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Während der Timeout-Wartezeit: Standardwert fünf Sekunden	Keine Reaktion	
	Timeout-Signal	1× Rot (lang)	1× Piepen (lang)
Zutritt verweigern	Karte lesen	1× Blau (kurz)	1× Piepen (kurz)
	Zutritt-verweigert-Signal	1× Rot (kurz)	1× Piepen (kurz)
Kartenlesefehler		1× Rot (kurz)	1× Piepen (kurz)
Karte mit anderer Kartenkonfiguration als in der Schließung		Keine Reaktion	
LockNode initialisieren		4× Rot (kurz)	4× Piepen (kurz)

6.11 IO-Node

Der SmartIntego IO-Node ist ein batteriebetriebenes Funkmodul mit drei Eingängen und einem Open-Drain-Ausgang. Durch die Verbindung mit dem Integratorsystem kann der IO-Node zur Überwachung und Steuerung von Komponenten verwendet werden. Sie benötigen die abgebildeten Komponenten:

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

Anwendungsbeispiele:

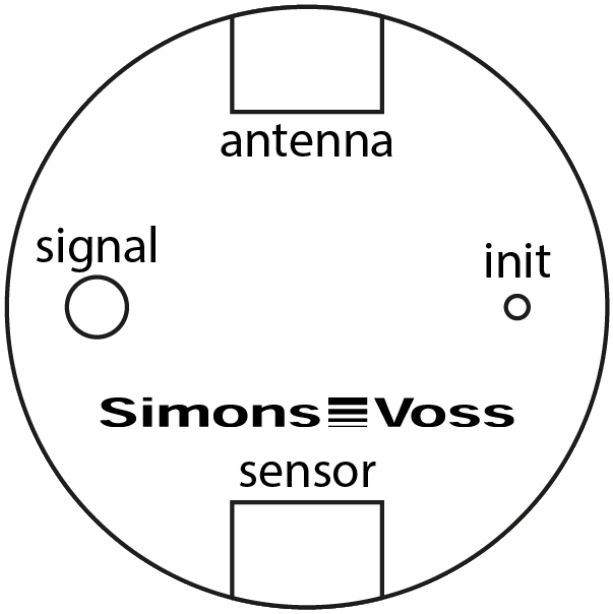
- Überwachung von Türen mit Reedkontakten von Fremdherstellern (Nutzungs der Inputs)
- Einschalten von Überwachungskameras (Nutzung des Oputputs)

6.11.1 Installation

1. Packen Sie den LockNode aus.
2. Prüfen Sie, ob der LockNode beschädigt ist.
3. Schließen Sie ggfs. das WN.LN.SENSOR.CABLE an.
4. Verbinden Sie ggfs. das WN.LN.SENSOR.CABLE mit den anzuschließenden Komponenten.
5. Schließen Sie die Stromversorgung an bzw. setzen Sie die Batterien ein.

↳ LockNode ist installiert.

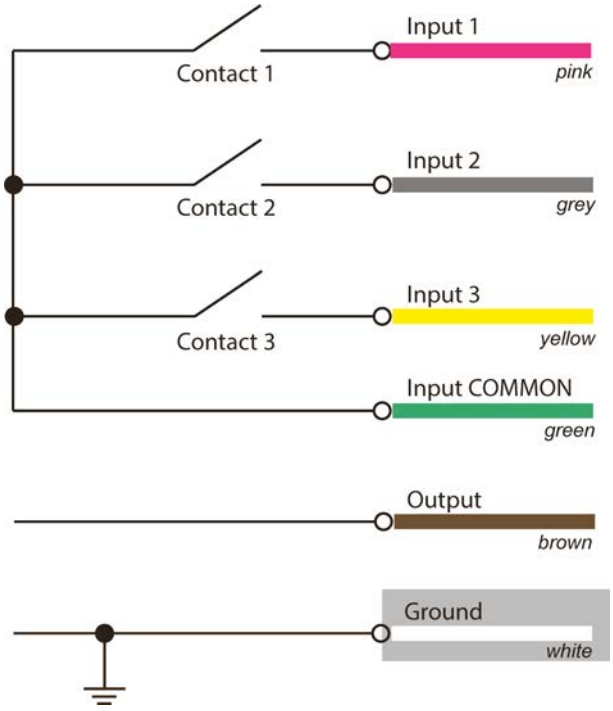
6.11.2 Anschlüsse



antenna	Direktanschluss für SREL.ADV (WN.KAB.WIRED-BF). Nur für System 3060.

sensor	I/O-Panel (WN.LN.SENSOR.CABLE) ■ grün (In-Common) ■ rosa (Input 1, Verbindung mit grün = 1, sonst 0) ■ grau (Input 2, Verbindung mit grün = 1, sonst 0) ■ gelb (Input 3, Verbindung mit grün = 1, sonst 0) ■ braun (Open-Collector-Ausgang) ■ weiß (Masse)

Die folgende Abbildung zeigt die Belegung des Sensorkabels.



Die Signal-LED zeigt den Betriebszustand an, der Init-Taster kann WNM-LockNodes zurücksetzen (siehe Hardware-Reset externer LockNodes) bzw. bei WN-LockNodes die Signalqualität testen.

SmartIntego

Ihr Integrator gibt den genauen Anschlussplan der Inputs vor. Änderungen an den Eingängen werden von den Inputs an das Integratorsystem weitergeleitet (Node-IO-Events).

Details entnehmen Sie bitte der Dokumentation des Integratorsystems.

6.11.3 Technische Daten

Maße	37xØ53 mm, geeignet für Standard-Unterputzdose (DIN 49073 Teil 1)
Stromversorgung	2x Batterie, Typ 2/3 AA Lithium 3,6V (Tadiran SL-761)
Stromaufnahme	■ Senden: 32 mA ■ Empfangen: 18 mA ■ Standby: ca. 20 µA (abhängig vom Datenverkehr und der Auslastung des Frequenzbands)
Batterielebensdauer	ca. 6 Jahre
Empfindlichkeit	-95 dBm
Schnittstellen	■ Anschluss für SREL.ADV (nur System 3060) ■ Anschlüsse für digitale Ein- und Ausgänge ■ 3x Input (Alle 0,5 s für 1 ms 35 µA), 1x Common-In ■ 1x Open-Drain-Ausgang (max. 25 V_{DC}, 650 mA dauerhaft bis 2 A Spitze, Übergangswiderstand 0,5 Ω)
Maximale Sendeleistung	ca. 1 mW

6.12 PinCode-Tastatur

6.12.1 Bestimmungsgemäßer Gebrauch

Mit Hilfe der netzwerkfähigen SmartIntego PinCode-Tastatur können Schlösser über die Eingabe einer berechtigten User-PIN betätigt werden (siehe Kapitel *Bedienung [▸ 153]*). Dafür sind folgende Schritte notwendig:

- Mit dem Tastenfeld: SmartIntego PinCode-Tastatur konfigurieren (siehe Konfiguration).
- Mit dem Integratorsystem: SmartIntego PinCode-Tastatur einer Schließung zuweisen und mindestens eine User-PIN anlegen.

Die SmartIntego PinCode-Tastatur kann mit Hilfe des SmartIntego-Managers und des Integratorsystems eingerichtet werden. Die SmartIntego PinCode-Tastatur wird als "Schlüssel" mit PINs angelegt und einem Schloss zugewiesen.

Die SmartIntego PinCode-Tastatur enthält einen LockNode mit „Chip-ID“ und wird bei der Netzwerkkonfiguration dem sich in Reichweite befindlichen GatewayNode zugeordnet. Wurde eine korrekte User-PIN-Länge eingegeben, wird die PIN über das Netzwerk zum Integratorsystem übermittelt und bewertet.

6.12.2 Bedienung

HINWEIS

Damit die SmartIntego PinCode-Tastatur Signale über das Netzwerk an ein vernetztes Schloss senden kann, müssen sowohl SmartIntego PinCode-Tastatur als auch das Schloss über eine stabile Netzwerkverbindung verfügen.

Abbruch von Aktionen

Alle Aktionen können abgebrochen werden, indem keine weiteren Eingaben getätigt werden. Nach einer Wartezeit bricht die SmartIntego PinCode-Tastatur die Aktion ab.

- ✓ SmartIntego PinCode-Tastatur wurde erfolgreich konfiguriert. (Master-PIN)
- ✓ User-PIN-Länge wurde ordnungsgemäß programmiert.
- ✓ Stabile Netzwerkverbindung besteht.

- ■ Geben Sie eine User-PIN ein. Zwischen den Eingaben der einzelnen Ziffern dürfen maximal 3 Sekunden verstreichen.
- ↳ SmartIntego PinCode-Tastatur piept und blinkt nach Eingabe einer User-PIN mit einer gültigen Länge einmal grün.

Die SmartIntego PinCode-Tastatur sendet die eingegebene User-PIN via Funk. Der Ablauf im Detail:

1. Die SmartIntego PinCode-Tastatur sendet die eingegebene User-PIN über das WaveNet an den GatewayNode.

   Wenn der GatewayNode das PIN-Event erfolgreich erhalten hat, dann gibt die SmartIntego PinCode-Tastatur eine positive Quittierung aus (siehe *Signalisierungen [▸ 154]*, evtl. abweichend).
2. Der GatewayNode sendet die eingegebene User-PIN über das Netzwerk (TCP/IP) an das Integratorsystem.
3. Das Integratorsystem vergleicht die eingegebene User-PIN mit den in dem Integratorsystem erstellten User-PINs.
4. Bei Übereinstimmung wird ein Öffnungsbefehl über das Netzwerk (TCP/IP) an den GatewayNode gesendet, der dann über das WaveNet das vernetzte Schloss öffnet (evtl. abweichend).

6.12.3 Signalisierungen

Informationen zur Signalisierung der SmartIntego-Variante finden Sie auch im SmartIntego TechGuide.

LED-Farbe	LED-Blinken	Summer	Ereignis	Erklärung
Rot	8x	4x	Power „On“ Reset	Reset nach Batteriewechsel, Batterien nicht in Ordnung
	1x	1x	Fehler	Fehler aufgetreten
			User-PIN-Länge falsch	Länge der eingegebenen User-PIN nicht korrekt
			User-PIN nicht empfangen	Eingegebene User-PIN nicht von Funk-Gegenstelle empfangen
Orange	3x	3x	Abbruch	Aktuelle Aktion wurde abgebrochen
	4x	4x	Power „On“ Reset	Reset nach Batteriewechsel im Betriebsmodus, Batterien in Ordnung
Grün	2x	2x	Master-PIN geändert	Master-PIN erfolgreich geändert
			Pinlänge geändert	Länge der User-PIN erfolgreich geändert
			User-PIN empfangen	Eingegebene User-PIN von Funk-Gegenstelle empfangen
	1x	1x	User-PIN-Länge korrekt	Länge der eingegebenen User-PIN korrekt

Tab. 1: Allgemeine Signale

LED-Farbe	LED-Blinken	Summer	Ereignis	Erklärung
Rot	4x	4x	Batteriewarnung 2	Batterien sehr schwach
Orange	4x	4x	Batteriewarnung 1	Batterien schwach
Grün	3x	3x	Volle Kapazität	Batterien voll
	1x	1x	Batterie „ok“	Batterien in Ordnung

Tab. 2: Batterietest

6.12.4 Technische Daten

Batterien	4 x 3 V Lithium Typ CR 2032 (Duracell, Murata, Panasonic, Varta) *Bei einem Batteriewechsel immer alle 4 Batterien durch neue, zugelassene Markenbatterien ersetzen!* Bitterstoff-beschichtete Batterien sind nicht geeignet.
Batterielebensdauer	Bis zu 500.000 Betätigungen oder bis zu 12 Jahren Stand-By
Schutzklasse	IP 65
Einsatztemperatur	-20°C bis +50°C
Abmessungen in mm	96 × 96 × 14
Signalelemente	Verschiedenfarbige LED (rot, grün, orange) + Signaltöne
Kennzeichnung	PHI-Nummer (Physical Hardware Identifier) = Chip ID
Gehäuse	Silberfarbenes ABS-Kunststoffgehäuse mit semi-transparenter Rückwand/Grundplatte
Grundfarbe	ähnlich RAL 9007
Tastenbeschriftung	Anthrazitgrau RAL 7016

6.13 Batterien

Alle SmartIntego-Komponenten sind batteriebetrieben:

- Schließzylinder
- Vorhangschlösser
- SmartHandles (AX und 3062)

- IO-Node
- PinCode-Tastatur

Ein dreistufiges Batteriemanagementsystem verhindert unerwartet völlig entleerte Batterien:

1. Batterie ist OK
2. Batterie ist schwach (Warnung)

   Je nach Nutzung bleiben noch bis zu dreißig Tage. Danach wechselt die Schließung in die letzte Warnstufe.
3. Batterie ist sehr schwach (Alarm)

   Je nach Nutzung bleiben noch bis zu zwanzig Tage.

6.13.1 Batteriestandsmessung (Schließzylinder und SmartHandles)

Ihre SmartIntego-Schließungen messen selbständig täglich zwischen Mitternacht und vier Uhr morgens (eingestellte Zeit) den Batteriestand. Die Messung dauert einige Sekunden. Während der Messung kann die Schließung nicht geöffnet werden. Das Messergebnis wird bis zur nächsten Messung gespeichert.

Die ermittelte Batteriewarnstufe wird als Kartenevent oder einmal täglich (je nach Integratorsystem) an das Integratorsystem übermittelt. Das Integratorsystem muss den Batteriezustand anzeigen. Die Schließungen selbst zeigen den Batteriezustand nicht an.

6.13.2 Batteriewechsel (Schließungen und SmartHandles)

Wenn das Integratorsystem eine Batteriewarnung anzeigt, dann müssen die Batterien gewechselt werden:

✓ Batteriewechselkarte erstellt (siehe Schritt-für-Schritt-Anleitung).

1. Tauschen Sie alle Batterien der betroffenen Schließung wie in der mitgelieferten Kurzanleitung beschrieben aus.
   ↳ Schließung signalisiert erfolgreichen Batteriewechsel (blinkt mehrfach).
2. Halten Sie bei den Komponenten eine Batteriewechselkarte vor die Schließung (entfällt bei AX).
   ↳ Schließung misst sofort den Batteriezustand.
   ↳ Batteriezustand wird bei der nächsten Betätigung einer Karte an das Integratorsystem übermittelt.
   ↳ Integratorsystem zeigt keine Batteriewarnung für diese Schließung mehr an.
3. Testen Sie den LockNode.

Detaillierte Informationen entnehmen Sie der Dokumentation der jeweiligen Komponente.

Empfohlene Hersteller

SimonsVoss verwendet ausschließlich Batterien von Markenherstellern:

- Murata
- Varta
- Panasonic
- Tadiran

Batterietypen

Schließungen	CR2450
PinCode-Tastatur	CR2032
IO-Node	2/3AA (Tadiran)

6.13.3 Batteriestandsmessung (NodeIO und PinCode-Terminal)

Der Batteriestand wird laufend überwacht.

Die ermittelte Batteriewarnstufe wird als Event oder einmal täglich (je nach Integratorsystem) an das Integratorsystem übermittelt. Die Komponenten selbst zeigen den Batteriezustand nicht an.

7. Infrastruktur

7.1 LockNodes

Ein LockNode ist ein Netzwerkknoten, der eine Schließung (Lock) oder einen Knoten (IO-Node oder PinCode-Tastatur) über einen GatewayNode mit dem Integratorsystem verbindet.

7.1.1 LockNode in Schließungen (LNI)

LNI bedeutet LockNode Integrated. Das sind kleine Platinen, die bei SmartIntego-Komponenten ab Werk installiert sind.

Ein kleiner Metallpin auf den Platinen stellt den Kontakt zu den Knaufkappen (Zylindern) bzw. dem Cover (SmartHandles) her. Die Knaufkappen bzw. Cover dienen so als verlängerte Antenne.

Ohne die Knaufkappen bzw. die Cover als verlängerte Antenne ist die Signalstärke der WaveNet-Verbindung deutlich schlechter und reicht möglicherweise nicht mehr aus.

Schließungen und LockNodes sind unabhängig voneinander konfiguriert. Die Konfigurationen bauen jedoch aufeinander auf.

Programmieren

1. Konfigurieren Sie den LockNode.
2. Programmieren Sie die Schließung.

↳ LockNode und Schließung sind nach der Programmierung miteinander gekoppelt.

Zurücksetzen

1. Setzen Sie die Schließung zurück.
2. Setzen Sie den LockNode zurück.

↳ LockNode und Schließung sind nach dem Zurücksetzen der Schließung wieder voneinander getrennt.

7.1.2 LockNode in Knoten (LN)

Die PinCode-Tastatur und der IO-Node sind keine Komponenten mit zusätzlichem LockNode. Der LockNode ist hier fest auf die Platine der jeweiligen Komponente montiert.

7.2 GatewayNode (GN)

Ein GatewayNode verbindet mehrere Schließungen/LockNodes über das WaveNet mit dem Integratorsystem. Aus Sicht der LockNodes handelt es sich um einen Accesspoint.

Für die Verbindung zum Integratorsystem gibt es zwei Optionen:

- Ethernet
- RS-485

7.2.1 TCP

Im Auslieferungszustand erwarten die GatewayNodes einen DHCP-Server im Netzwerk, der ihnen eine IP-Adresse zuweist. Wenn im Netzwerk kein DHCP-Server vorhanden ist, dann weisen sich die GatewayNodes Standard-Zugangsdaten zu.

Schnittstellen

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

Stromversorgung

SI.GN.ER	SI.GN2.ER, SI.GN2.ER.M
WN.POWER.SUPPLY.PPP 	POWER.SUPPLY.2 
Power over Ethernet (PoE, IEEE802.af, galvanisch getrennt	

Varianten:

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

	SI.GN.ER (Ethernet)

Technische Daten:

SI.GN2.ER

Allgemein	
Maße	172 mm × 86 mm × 33 mm
Gewicht	ca. 100 g
Material	ABS-Kunststoff, UV-stabil
Farbe	Weiß (wie RAL 9016 "Verkehrsweiß")
Montage	■ horizontal ■ vertikal ■ Wandmontage möglich ■ integrierte Zugentlastung (3x)
Anschlüsse	■ RJ45 (Netzwerk/PoE) ■ Rundstecker Ø 5,5 mm, Ø Stift 2,0 mm (Stromversorgung) ■ Schraubklemmblock 2-pol, Aderdurchmesser 0,14 mm^2 bis 1,5 mm^2 (Stromversorgung für externe Anwendungen) ■ MCX-Buchse (Optionale externe Antenne)
Umgebung	
Temperatur	■ Betrieb: -10 °C bis +55 °C ■ Lagerung: -20 °C bis +60 °C
Luftfeuchtigkeit	Max. 90% ohne Kondensation
Schutzklasse	IP20
Elektrik	

Betriebsspannung	9 V_{DC} bis 32 V_{DC} (verpolungssicher) oder PoE nach IEEE 802.3af Stromversorgung über PoE und Rundstecker gleichzeitig möglich: Rundstecker > 12 V_{DC} → Rundstecker verwendet, Rundstecker < 12 V_{DC} → PoE verwendet
Leistung	max. 3 W
Ausgang VOUT	3,0 V_{DC} bis 3,3 V_{DC}, max. 200 mA
Schnittstellen	
RJ45	■ Netzwerkschnittstelle ■ 10T/100T ■ HP Auto_MDX ■ DHCP-Client (DHCP: on) ■ IPv4 ■ Services: ■ TCP: 1x am Port 2101 ■ UDP: 1x für Digi-Scan (OAM-Tool) ■ Webserver: Enable
868-MHz-Funk	WaveNet-Schnittstelle, Reichweite bis zu 30 m
Signalisierung	
LED	RGB-LED (Gehäusemitte)
Software	
Programmierung	via TCP/IP-Schnittstelle

Übertragungs-medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz ■ Ethernet	■ RJ45 (Netzwerk/PoE) ■ Rundstecker Ø 5,5 mm, Ø Stift 2,0 mm (Stromversorgung) ■ MCX-Buchse (optionale externe Antenne)	9 V_{DC} bis 32 V_{DC} oder PoE nach IEEE 802.3af, 3 W Stromversorgung über PoE und Rundstecker gleichzeitig möglich: Rundstecker > 12 VDC → Rundstecker verwendet, Rundstecker < 12 VDC → PoE verwendet	172,1×85,9×32,8 mm

SI.GN.ER

Übertragungs-medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz ■ Ethernet	■ Anschlussklemmen für externes Steckernetzteil ■ RJ45 (Netzwerk/PoE) ■ FME-Buchse (Antenne)	9 V_{DC} bis 24 V_{DC}, min. 3 VA	98×64×40 mm bzw. 98×64×130 mm mit Antenne

7.2.1.1 Konfiguration und Betrieb

Generell bietet sich der Einsatz eines unabhängigen IP-Adressbereichs für die GatewayNodes an. Eine Möglichkeit dafür ist ein virtuelles lokales Netzwerk (V-LAN), das vom normalen Netzwerk getrennt arbeitet.

Voraussetzung für den störungsfreien Betrieb ist eine dauerhafte Verbindung der GatewayNodes zum Integratorsystem. Zusätzlich kann während der Einrichtung eine weitere Verbindung der SmartIntego-Komponenten zum SmartIntego-Tool (WO) hergestellt werden.

Verwendete TCP-Ports

Port (TCP)	Richtung	Beschreibung
80	Einrichtungs-PC zu GatewayNodes	Aufruf der Konfigurationswebsite der GatewayNodes
2101	■ Einrichtungs-PC zu GatewayNodes ■ Integratorsystem zu GatewayNodes	■ Kommunikation zwischen SmartIntego-Tool (WO) auf Einrichtungs-PC zu GatewayNodes ■ Kommunikation zwischen Integratorsystem und GatewayNodes im Betrieb
2153	Integratorsystem zu GatewayNodes	Kommunikation zwischen Integratorsystem und GatewayNodes im Betrieb (wenn TLS-Verschlüsselung verwendet wird)

7.2.1.2 Konfiguration TCP-GatewayNodes

Die TCP-GatewayNodes können an die jeweilige IT-Infrastruktur angepasst werden (siehe Integrator-Dokumentation). Dazu stellen die angeschlossenen GatewayNodes im Netzwerk eine Website bereit, die über die IP oder den DNS-Namen mit einem Browser geöffnet werden kann. Folgende Einstellungsmöglichkeiten stehen zur Verfügung:

| SYSTEM INFORMATION |	[ÜBERSICHT]	Zeigt die IT-Einstellungen an.
	[WAVENET]	Zeigt die WaveNet-Einstellungen an.
	[VERBINDUNG]	Zeigt die aktive Verbindung zum Integratorsystem an.
| KONFIGURATION |	[NETZWERK]	Verändert generelle Netzwerkeinstellungen.
	[PORT]	Stellt den Port für die TCP-Verbindung ein.
	[ETHERNET VERBINDUNG]	Stellt die Geschwindigkeit und IEEE802.1X ein.
	[WAVENET]	Setzt die WaveNet-Einstellungen zurück.

| ADMINISTRATION |	[PASSWORT]	Ändert das Login-Passwort.
	[AES]	Ändert die AES-Einstellungen (Verschlüsselungspasswort zwischen GatewayNode und Integratorsystem), Bindung des GatewayNodes an das jeweilige Integratorsystem. Nur sichtbar bei Aufruf über HTTPS.
	[ZERTIFIKATE]	Stellt TLS-Verschlüsselung zwischen GatewayNode und Integratorsystem ein.
	[WERKSEINSTELLUNG]	Setzt den GatewayNode auf die Werkseinstellungen zurück.
	[NEUSTART]	Startet den GatewayNode neu (Je nach Browsereinstellungen kann diese Funktion auch deaktiviert sein).

Website öffnen

Sie erhalten das Gerät mit folgender werkseitiger Konfiguration:

IP-Adresse	192.168.100.100 (falls kein DHCP-Server gefunden wird)
Subnetz-Maske	255.255.0.0
Benutzername	SimonsVoss
Passwort	SimonsVoss

Geben Sie in der Addresszeile https://IP-Adresse ein (Computer und GatewayNode müssen sich im gleichen Netzwerk befinden). Ändern Sie anschließend das Passwort.

Einige Browser übertragen keine Leerzeichen, die am Anfang des Passworts stehen. Beginnen Sie das Passwort deshalb nicht mit Leerzeichen.

✓ Browserschnittstelle geöffnet.

1. Öffnen Sie über | ADMINISTRATION | die Registerkarte [PASSWORT].

2. Geben Sie Ihr neues Passwort ein.
3. Wiederholen Sie Ihr neues Passwort.
4. Klicken Sie auf die Schaltfläche Passwort speichern.

↳ Passwort ist geändert.

ACHTUNG

Zugang über Standardpasswort

Über die werksseitig eingestellten Zugangsdaten können andere Personen auf das Produkt zugreifen.

Einige Browser übertragen keine Leerzeichen, die am Anfang des Passworts stehen.

1. Ändern Sie das Standardpasswort.
2. Beginnen Sie das Passwort nicht mit Leerzeichen.

HINWEIS

Verlust der Passwörter

Ihre Passwörter sind die Grundlage für die Verwaltung Ihrer Schließanlage. Verlorene oder öffentlich bekanntgewordene Passwörter sind ein schwerwiegendes Sicherheitsrisiko und/oder führen zum Kontrollverlust über die Anlage.

1. Notieren Sie sich Ihre Passwörter.
2. Verwahren Sie Ihre Passwörter sicher.

7.2.1.3 Verschlüsselung

GatewayNodes ab Firmware 40.X oder neuer unterstützen:

- AES-Verschlüsselung für die Datenpakete

- TLS-Verschlüsselung für die Verbindung

AES-Verschlüsselung

Bei der AES-Verschlüsselung wird in den Einstellungen eines jeden GatewayNodes ein geheimer Schlüssel hinterlegt.

Derselbe Schlüssel wird im Integratorsystem hinterlegt.

Dieser Schlüssel verknüpft die GatewayNodes mit dem Integratorsystem und verschlüsselt die Datenpakete mit 128-Bit-AES.

Details zu den Einstellungen entnehmen Sie bitte der Dokumentation des Integratorsystems.

TLS-Verschlüsselung

Die optionale TLS-Verschlüsselung verschlüsselt die aktive Verbindung zwischen einem GatewayNode und dem Integratorsystem. Dazu kann es notwendig sein, über die Konfigurationswebsite der GatewayNodes eigene Zertifikate auf den GatewayNodes zu speichern.

Details zu den Einstellungen entnehmen Sie bitte der Dokumentation des Integratorsystems.

7.2.2 RS-485

Schnittstellen

- Funk (WaveNet)
- RS-485
- Ethernet (TCP/IP) - nur für das Konfigurationsgerät (SI.GN.CONFIG.EC)

Stromversorgung

SI.GN.CR oder SI.GN.CONFIG.EC können entweder über jeweils ein WN.POWER.SUPPLY.PPP oder über die Anschlussklemmen versorgt werden.

Varianten:

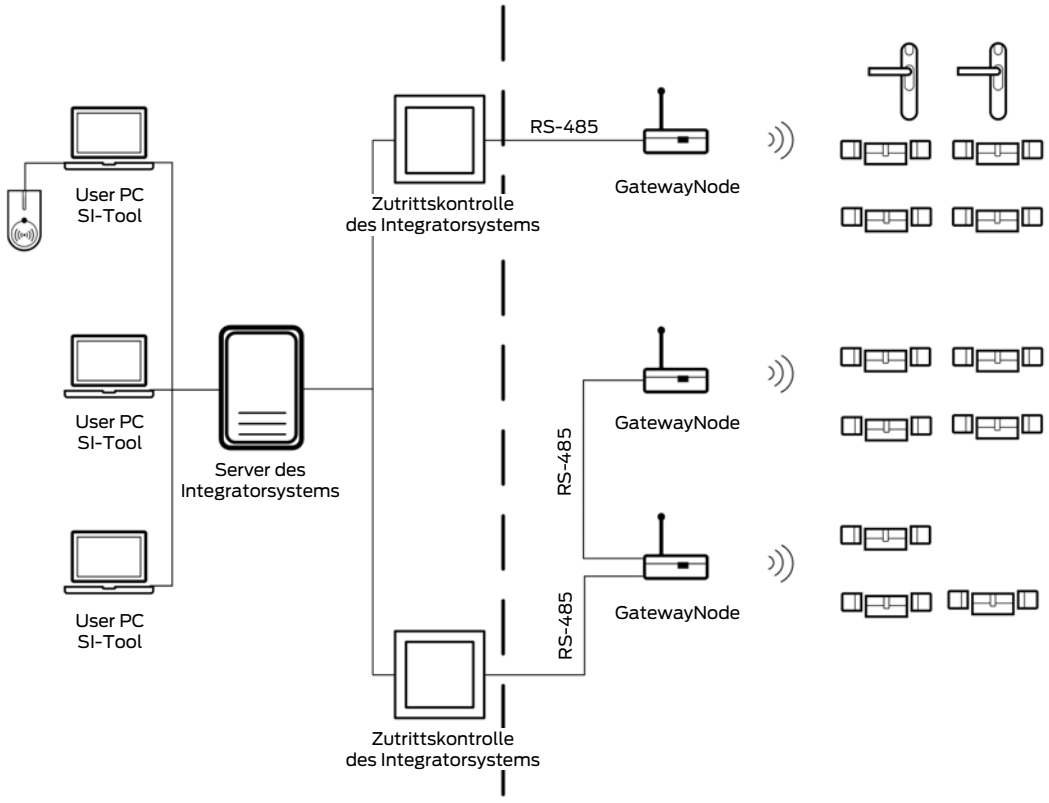
	SI.GN.CR (RS-485)
	SI.GN.CONFIG.EC

SI.GN.CR

Übertragungs-medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz ■ RS-485	■ Anschlussklemmen für externes Steckernetzteil ■ Anschlussklemmen für RS-485 ■ FME-Buchse (Antenne)	9 V_{DC} bis 24 V_{DC}, min. 3 VA	98×64×40 mm bzw. 98×64×130 mm mit Antenne

7.2.2.1 Konfiguration und Betrieb

Während des täglichen Betriebs des RS-485-Netzwerks sind alle RS-485-GatewayNodes (SI.GN.CR) direkt mit der RS-485-Schnittstelle des Integratorsystems verbunden.



Der ConfigNode wird nur für die Konfiguration der RS-485-GatewayNodes und der damit verbundenen Schließungen benötigt. Er stellt die Schnittstelle zum SmartIntego-Tool (WO) dar.

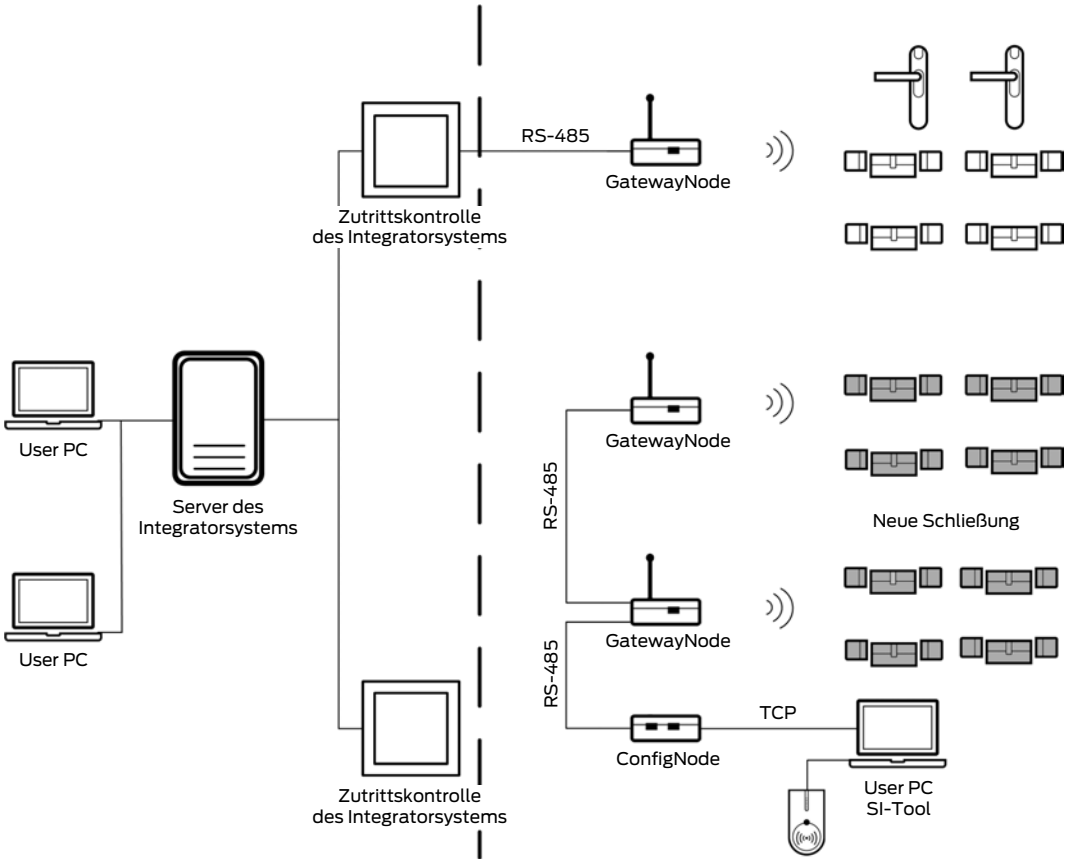
Während der Konfiguration wird die RS-485-Verbindung zwischen dem Integratorsystem und den GatewayNodes getrennt. Die GatewayNodes werden stattdessen mit dem ConfigNode verbunden (RS-485) und dieser via Ethernet mit dem Einrichtungs-PC samt SmartIntego-Tool (WO).

HINWEIS

Schließungen während der Konfiguration offline

Die Verbindung der Schließungen zum Integratorsystem wird während der Konfiguration unterbrochen. Die Schließungen sind deshalb offline und arbeiten nur mit einer zuvor hinterlegten Whitelist.

- Stellen Sie sicher, dass in den Schließungen eine Whitelist hinterlegt ist, bevor Sie die Verbindung zum Integratorsystem trennen.



In diesem Beispiel sind die grauen Schließungen nicht mehr mit dem Integratorsystem verbunden und offline.

Mit einem ConfigNode lassen sich maximal 255 Adressen verwalten. Jeder LockNode verbraucht eine Adresse dieses Kontingents, jeder GatewayNode jedoch zwei. Wenn im System mehr LockNodes bzw. GatewayNodes vorhanden sind, dann muss nach dem ersten ein zweiter ConfigNode eingesetzt werden. Ein Parallelbetrieb von mehreren ConfigNodes ist nicht möglich.

Mehrere kleinere Projekte können auch direkt mit einem ConfigNode betrieben werden. Dabei ist zu beachten, dass die Einstellungen im ConfigNode zum Projekt passen müssen:

- Neue Projekte müssen immer mit einem neuen oder zurückgesetzten ConfigNode erstellt werden. Beim Erstellen des Projekts werden die passenden Einstellungen in den ConfigNode geschrieben.
- Wenn der ConfigNode in einem anderen Projekt verwendet werden soll, dann muss er vorher zurückgesetzt werden. Über den SmartIntego-Manager wird der im Projekt vorhandene ConfigNode mit der Option Replace with durch einen neuen oder zurückgesetzten ConfigNode ersetzt. Dabei schreibt der SmartIntego-Manager die zum Projekt passenden Einstellungen in den ConfigNode.
- Derselbe ConfigNode kann also für mehrere Projekte verwendet werden, muss aber bei jedem Projektwechsel wie beschrieben zurückgesetzt werden, bevor er wieder verwendet werden kann.

7.2.2.2 Adressierung

Jeder ConfigNode kann 255 Adressen verwalten, jeder GatewayNode braucht zwei. Ein ConfigNode kann also maximal 127 GatewayNodes konfigurieren.

Die Adressen der GatewayNodes werden mit dem ConfigNode verknüpft:

- Im SmartIntego-Manager
- Im ConfigNode selbst

7.2.2.3 Physische Verbindung

Die GatewayNodes sind untereinander mit einem Kabel verbunden.

Kleinere Gruppen von GatewayNodes können mit einer gemeinsamen Leitung verbunden werden (Daisy-Chain). In einem Projekt können aber auch mehrere Leitungen verwendet werden (sternförmig). Beide Verkabelungstechniken können auch kombiniert werden (Mehrere Daisy-Chains, die an einem Punkt zusammengeführt werden). Der Aufbau und die Verteilung ist normalerweise vom Hardware-Controller des Integrators vorgegeben.

Ein ConfigNode ist in der Lage, mehrere physische Verbindungen zu adressieren (Kabelleitungen).

7.2.2.4 Namenskonvention

Den GatewayNodes können eigene Namen zugewiesen werden. In den Namen sollten die physischen Verbindungen erkennbar sein.

Je nach Aufbau (bei mehreren ConfigNodes im Projekt) ist es hilfreich, zusätzlich die logischen Verbindungen zu den ConfigNodes in die Namen aufzunehmen.

Eine detaillierte Systemdokumentation ist in diesem Zusammenhang insbesondere in RS-485-Projekten wichtig.

7.2.3 Signalisierung

Die GatewayNodes signalisieren ihren momentanen Zustand mit einer LED im Gehäuse:

LED	Zustand
Langsam blinkend (1 s grün, dann 1 s Pause)	Keine WaveNet-Konfiguration
Schnell blinkend (0,5 s grün, dann 05 s Pause)	WaveNet-Konfiguration vorhanden
Sehr schnell blinkend (maximal 12 s lang kontinuierlich)	Aktive Datenübertragung

7.2.4 Variante für Mercury Security

Die Mercury-Variante (SI.GN2.ER.M) ist technisch identisch mit dem normalen GatewayNode (SI.GN2.ER). Sie unterscheidet sich in der Zuweisung der Device-Adressen (Device-Adressen sind an WaveNet-Adressen gekoppelt).

Mercury-GatewayNodes sind deshalb nur mit Integratorsystemen kompatibel, die auf einem Mercury-Security-Controller basieren, beispielsweise (Liste unvollständig):

- Genetec
- Lenel
- Avigilon
- Keri Systems

Beachten Sie deshalb:

- Mischen Sie keine Mercury-Verianten mit Nicht-Mercury-Varianten.
- Verwenden Sie Mercury-GatewayNodes nur in Integratorsystemen mit Mercury-Security-Controller.
- Die Schließungen werden nicht mit einer eigenen Device-Adresse verknüpft. Stattdessen wird das Handling der WaveNet-Adresse genutzt.

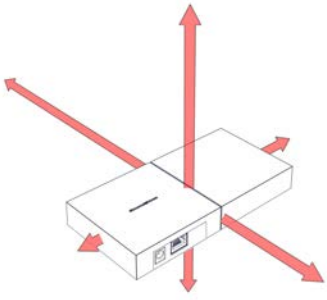
Der Unterschied zwischen der Device-Adresse und der WaveNet-Adresse beeinflusst die Handhabung in verschiedenen Situationen im System (siehe *Topologie [▸ 175]*). Wenn beispielsweise Schließungen umgezogen werden, dann ändert sich bei Mercury-Varianten die Device-Adresse.

Schließungen sind nicht direkt mit dem Integratorsystem verbunden. Deshalb können in Mercury-Systemen reguläre SmartIntego-Schließungen verwendet werden und es gibt keine Mercury-Variante der SmartIntego-Schließungen.

7.2.5 Externe Antenne

Manchmal erreicht ein GatewayNode einzelne Schließungen nicht optimal. In diesen Fällen verbessert eine optionale externe Antenne (Bestellnummer: ANTENNA.EXT.868) die Reichweite.

Auch die Abstrahlcharakteristik ist signifikant anders, womit Schließungen möglicherweise besser erreicht werden können.

Abstrahlcharakteristik	
Interne Antenne	Externe Antenne
	Näherungsweise kugelförmige Abstrahlcharakteristik  (Abbildung für 850 MHz, Az=45, EL=45)

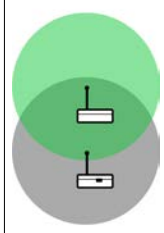
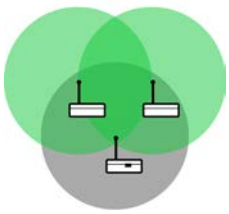
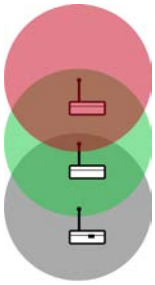
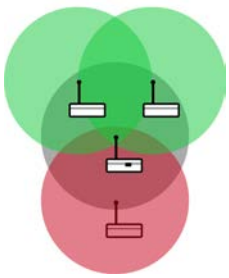
7.2.6 GatewayNode Radio-Radio

Wenn eine externe Antenne zur Reichweitenerweiterung nicht ausreicht, dann kann alternativ ein GatewayNode-Repeater (SI.GN.R) im nächsten Segment installiert werden.

Der GatewayNode Radio-Radioöffnet an einem vorhandenen Segment ein neues Segment (über die Radio-Schnittstelle). Ein normales Segment kann maximal einmal mit einem Repeater erweitert werden, aber an einem normalen Segment können zwei voneinander unabhängige GN.R angeschlossen werden (Y-Form).

Andere Verwendungen von Repeatern sind nicht möglich.

Bedenken Sie, dass der gesamte Traffic aller erweiterten Segmente über das ursprüngliche Segment "fließt" und deshalb das ursprüngliche Segment zu einem Flaschenhals werden kann.

✓	✓	✗	✗
			

Ein vorhandenes Segment (grau), das physisch angeschlossen ist (RS-485/TCP) wird mit einem Repeater erweitert (grün).	Ein vorhandenes Segment (grau), das physisch angeschlossen ist (RS-485/TCP) wird mit zwei Repeatern erweitert (grün).	Ein vorhandenes Segment (grau), das physisch angeschlossen ist (RS-485/TCP) wird mit einem Repeater erweitert (grün). Ein weiterer Repeater in Reihe, um das erweiterte Segment nochmals zu erweitern, ist nicht zulässig (rot).	Ein vorhandenes Segment (grau), das physisch angeschlossen ist (RS-485/TCP) wird mit zwei Repeatern erweitert (grün). Ein dritter Repeater ist nicht zulässig (rot).

Schnittstellen

- Funk (WaveNet)

Stromversorgung

SI.GN.R wird mit WN.POWER.SUPPLY.PPP versorgt.

7.2.6.1 Konfiguration

Der Repeater (SI.GN.R) wird ausschließlich über den SmartIntego-Manager verwaltet.

7.3 WaveNet

7.3.1 Beschreibung

Das WaveNet-Protokoll ist ein SimonsVoss-Kommunikationsstandard zwischen Gateway- und LockNodes:

- Frequenz: 868 MHz
- Interne Topologie (Adressierung)
- Verschlüsselt (AES-128-bit)

7.3.2 Frequenz

Das WaveNet arbeitet im 868-MHz-Bereich und verwendet eine der beiden Frequenzen:

1. 868,3 MHz
2. 868,5 MHz

Der Kanalabstand beträgt 199,951172 kHz. Frequenz 1 ist die Standardfrequenz. Wenn andere Systeme vorhanden sind und sich die Systeme stören, dann kann auf die zweite Frequenz ausgewichen werden. Diese Änderung betrifft alle Komponenten im WaveNet und ist nur während des ersten Setups möglich.

7.3.3 Topologie

Chip-ID

Die Chip-ID ist eine eindeutige Nummer, die fest im LockNode einprogrammiert ist. Mit der Chip-ID ist jeder LockNode eindeutig ansprechbar (vergleichbar mit der MAC-Adresse einer IT-Komponente). Im SmartIntego-Manager kann mit der Option Find Chip ID nach einer Chip-ID und damit nach einem bestimmten LockNode gesucht werden. Chip-IDs haben acht Ziffern im Hexadezimalformat, z.B. 00017FD8.

Net-ID

Die Netzwerk-ID (Net-ID) ist der Name des WaveNet-Netzwerks. Sie besteht aus acht Ziffern im Hexadezimalformat, z.B. 2DA9. Der SmartIntego-Manager erzeugt die Netzwerk-ID automatisch, sobald der erste GatewayNode zum Projekt hinzugefügt wird (Dieser GatewayNode muss neu oder zurückgesetzt sein!). Danach kann die Netzwerk-ID nicht mehr geändert werden und wird auf allen Komponenten dieses WaveNets gespeichert. Projekte mit der gleichen Netzwerk-ID dürfen nicht in Funkreichweite zueinander liegen und sollten deshalb generell vermieden werden.

WaveNet-Adresse

Die WaveNet-Adresse ist eine für jede Komponente individuelle Netzwerkadresse. Sie dient der internen Kommunikation zwischen Gateway- und LockNodes innerhalb des WaveNets. Der SmartIntego-Manager erzeugt die WaveNet-Adressen automatisch, wenn Gateway- oder LockNodes zum Projekt hinzugefügt werden.

Im Normalfall können das Integratorsystem und die LockNodes miteinander kommunizieren, ohne dass Sie wissen, welcher LockNode welche WaveNet-Adresse hat. Mercury-Systeme händeln die Adressierung anders und stellen deshalb einen Sonderfall dar (siehe *Variante für Mercury Security [▸ 171]*).

Netzwerkmaske

Der WaveNet-Adressbereich umfasst 65535 Adressen. Dieser Adressbereich teilt sich in zwei Gruppen auf:

1. Adressen für GatewayNodes
2. Adressen für LockNodes

Die Aufteilung wird durch die Netzwerkmaske festgelegt:

Netzwerkmaske	GatewayNode-Adressen (GatewayNodes im Projekt)	LockNode-Adressen (=Segmentadressen) (LockNodes pro GatewayNode)
8_8	$2^8 = 256$	$2^8 = 256$
11_5	$2^{11} = 2048$	$2^5 = 32$
12_4	$2^{12} = 4096$	$2^4 = 16$

In jedem Segment sind die ersten sechs und die letzte Adresse für interne Zwecke reserviert.

Einige Adressen für GatewayNodes sind ebenfalls für interne Zwecke reserviert und können deshalb nicht genutzt werden.

Das WaveNet bildet das Rückgrat für SmartIntego-Wireless-Online-Projekte. Die WaveNet-Qualitätsrichtlinien für SmartIntego sehen maximal 16 LockNodes pro GatewayNode vor.

Device Adress

Die *Device Adress* ist ein Identifikationsattribut der LockNodes und GatewayNodes, mit dem sie vom Integratorsystem identifiziert werden. Der SmartIntego-Manager erzeugt die Device-Adresse, wenn LockNodes und GatewayNodes verknüpft werden und weist sie anschließend den LockNodes und den GatewayNodes individuell zu.

Jeder LockNode und jeder GatewayNode hat eine im Projekt einzigartige Device-Adresse.

	Device-Adresse	Mercury-Device-Adresse
Strukturadresse	■ 0100 ■ 0200 ■ 0300 ■ usw.	Abhängig vom Wave-Net-Segment: ■ 002100 ■ 002600 ■ 002700 ■ usw.
Schließung erstellen	Wird aus einem Pool freier Device-Adressen zugewiesen.	Wird aus einem Pool freier WaveNet-Adressen zugewiesen.
Schließung austauschen	Device-Adresse ändert sich.	Device-Adresse kann sich ändern. Die erste freie WaveNet-Adresse wird immer als Device-Adresse verwendet und zugewiesen..
Schließung ersetzen	Device-Adresse bleibt unverändert.	Device-Adresse bleibt unverändert.
Schließung versetzen	Device-Adresse bleibt unverändert.	Device-Adresse kann sich ändern. Die erste freie WaveNet-Adresse wird immer als Device-Adresse verwendet und zugewiesen.
Schließung löschen	Device-Adresse wird von der Komponente gelöst und nicht mehr für neue Komponenten verwendet.	Device-Adresse wird von der Komponente gelöst und kann für neue Komponenten verwendet werden.

Import mit CSV-Datei

Die beschriebenen Topologie-Eigenschaften, also die SmartIntego-Systemstruktur, kann automatisch in das Integratorsystem importiert werden (CSV-Datei). Wenn das gewünschte Integratorsystem diese Funktion nicht unterstützt, dann kontaktieren Sie bitte den Integrator, der das Integratorsystem bereitstellt.

7.3.4 Kommunikation

Jeder GatewayNode im WaveNet spannt sein eigenes Segment auf und verwaltet die LockNodes innerhalb seines Segments. Pro GatewayNode sehen die WaveNet-Qualitätsrichtlinien maximal 16 LockNodes vor. Pro verkabelten (Ethernet/RS-485) sind maximal zwei Repeater (SI.GN.R) zulässig (siehe *GatewayNode Radio-Radio [▸ 173]*).

Die Kommunikation zwischen GatewayNode und LockNode ist auf eine aktive Kommunikation pro Segment beschränkt. Ein GatewayNode kann also nur mit einem LockNode gleichzeitig kommunizieren. Während dieser Kommunikation kann in diesem Segment keine andere Kommunikation zwischen dem GatewayNode und einem anderen LockNode stattfinden.

Sämtliche Kommunikation ist eventbasiert. Wenn es nichts mitzuteilen gibt, dann wird auch keine Verbindung aufgebaut.

Davon sind auch GatewayNodes betroffen, deren Funkreichweiten sich überlagern, sogenannte überlappende Segmente (Übersprechen/ Crosstalk).

Die Kommunikation zwischen GatewayNode und LockNode für das Einkuppeln dauert üblicherweise maximal 500 ms. Durch diese kurze Dauer ist die Beschränkung auf maximal eine aktive Verbindung normalerweise kein Problem. Größere Vorgänge wie umfangreiches Programmieren von Schließungskonfigurationen (beispielsweise nach dem Aktualisieren einer Whitelist mit vielen Einträgen) kann die verfügbare Bandbreite im WaveNet reduzieren und zu vorübergehenden Störungen führen. Das Integratorsystem ist hier für die sequenzielle Abarbeitung zuständig.

Alle Komponenten verwenden ein Listen-Before-Talk-Verfahren. Vor dem Senden prüfen die Komponenten immer zuerst, ob innerhalb ihres Segments gerade kommuniziert wird.

- Nur wenn im Segment gerade nicht kommuniziert wird (das Segment also frei ist), dann wird eine neue Kommunikation aufgebaut.
- Wenn im Segment gerade kommuniziert wird (das Segment also nicht frei ist), dann wartet die Komponente und versucht bis zu drei Mal, das Datenpaket zu versenden. Nach dem dritten erfolglosen Versuch wird das Datenpaket verworfen.

Zwischen dem Integratorsystem und dem LockNode gibt es drei Arten von Kommunikation:

1. LockNode zu GatewayNode: Events (z.B. Karte lesen)
2. GatewayNode zu LockNode: Befehle (z.B. Schließung einkuppeln)
3. LockNode zu GatewayNode: Antworten auf Befehle (z.B. erfolgreich bzw. warum nicht erfolgreich)

Um die Batteriestandzeiten der batteriebetriebenen Schließungen zu verlängern, befinden sich folgende Bestandteile der Schließung grundsätzlich im Standby-Modus:

- Kartenleser
- LockNode

Sie werden nur aktiv, wenn sie benötigt werden. Der LockNode prüft alle drei Sekunden für eine sehr kurze Zeitspanne, ob gerade ein GatewayNode versucht, mit ihm zu kommunizieren. Die Häufigkeit dieser Prüfungen ist einstellbar (siehe *Kürzere Reaktionszeiten der LockNodes (Short Wake-Up period) [▸ 19]*).

Beispiel: Ein Benutzer öffnet eine Tür mit seiner Karte

Event	1. Ein Benutzer hält seine Karte vor die Schließung. 2. Die Schließung registriert ein Event. 3. Die Schließung aktiviert unverzüglich den LockNode. 4. Der LockNode verschickt das Event sofort über das WaveNet. 5. Der LockNode bleibt für einige Sekunden aktiv, um ggfs. Befehle des Integratorsystems zu empfangen.
Befehl	1. Das Integratorsystem empfängt das Event über WaveNet. 2. Das Integratorsystem entscheidet über die Öffnung. 3. Das Integratorsystem versendet einen Öffnungsbefehl über das WaveNet an den LockNode der Schließung.
Antwort	1. Der LockNode empfängt den Öffnungsbefehl über das WaveNet und leitet den Öffnungsbefehl an seine Schließung weiter. 2. Die Schließung kuppelt ein. 3. Die Schließung übermittelt über ihren LockNode und das WaveNet das Ergebnis der Ausführung des Befehls an das Integratorsystem.

Beispiel: Eine wird ohne ein Event geöffnet (z.B. Fernöffnung aus dem Integratorsystem)

Befehl	1. Das Integratorsystem sendet einen an die Schließung gerichteten Öffnungsbefehl. 2. Der entsprechende GatewayNode versucht für maximal 12 Sekunden Kontakt mit dem LockNode der Schließung aufzunehmen. (Wake-Up-Signal mit Unterbrechungen gemäß 868-MHz-Spezifikationen)
Antwort	1. Der LockNode prüft alle drei Sekunden (einstellbar), ob gerade ein GatewayNode mit ihm Kontakt aufnimmt. 2. Der LockNode empfängt den Öffnungsbefehl vom GatewayNode und leitet ihn an seine Schließung weiter. 3. Die Schließung kuppelt ein. 4. Die Schließung übermittelt über ihren LockNode und das WaveNet das Ergebnis der Ausführung des Befehls an das Integratorsystem.

Zwischen dem Versand eines Befehls, der direkt aus dem Integratorsystem kommt und keine Antwort auf ein Event an der Schließung ist, und der entsprechenden Reaktion an der Schließung können bis zu zwölf Sekunden vergehen. In einigen wenigen Fällen (Starke Auslastung der Frequenz, Störungen) können mehrere Versuche notwendig sein, bis ein Befehl an der Schließung ankommt. Dieser Prozess wird vom Integratorsystem kontrolliert.

7.3.5 Synchronisation

Während einer Kommunikation im WaveNet werden die Datenpakete mehrfach intern verifiziert, um die Kommunikation zusätzlich abzusichern.

Die Verbindung zwischen GatewayNodes und Integratorsystem kann unterbrochen werden, beispielsweise durch Neustarts der GatewayNodes oder des Integratorsystems. Nach einer Unterbrechung der Verbindung müssen einige Prüfsummen wieder synchronisiert werden.

Das Integratorsystem und die SmartIntego-Komponenten synchronisieren die Prüfsummen automatisch. Wenn die Prüfsummen nicht automatisch synchronisiert wurden, dann wird die Synchronisation spätestens bei der ersten aktiven Kommunikation nachgeholt. Der Benutzer muss dann seine Karte nochmals vor den Leser halten.

7.3.6 Messung der Signalqualität

Die Signalqualität kann zu verschiedenen Zeitpunkten mit verschiedenen Methoden gemessen werden:

1. Vor dem Projekt mit dem BAMO
2. Während der Installation mit dem SmartIntego-Manager
3. Laufende Messung im Betrieb und Anzeige im Integratorsystem

Die Signalqualität hängt von verschiedenen Einflüssen ab, zum Beispiel:

- Andere elektronische Geräte, die schlecht geschirmt sind oder über Funk kommunizieren
- Umgebungshindernisse (Feuerschutztüren aus Metall, neue Mauern mit Restfeuchtigkeit...)
- Abstand zwischen Gateway- und LockNode

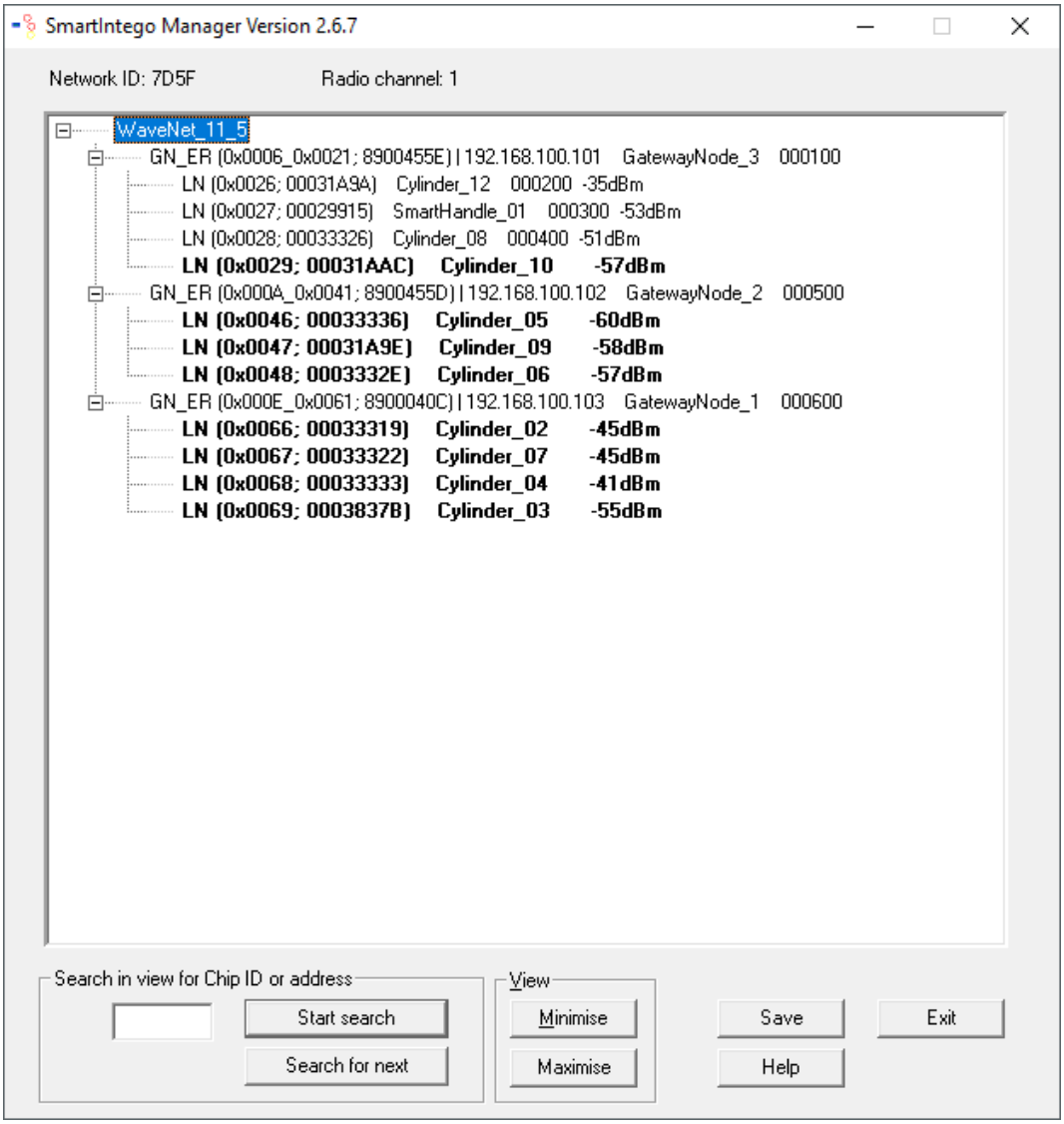
Messung vor dem Projekt (BAMO)

Mit dem SimonsVoss-WaveNet-Testwerkzeug (BAMO.EU) kann eine Bestandsaufnahme der Situation während der Messung gemacht werden. Das Objekt, in dem das Projekt realisiert werden soll, sollte nach der Messung nicht mehr verändert werden. Deshalb ist eine Messung in einem unfertigem Gebäude bzw. in einem Rohbau nicht zu empfehlen. Das BAMO liefert mit zwei Messungen drei Werte:

1. Messung	■ Signalstärke (mindestens 70%) ■ Erfolgreich gesendete Datenpakete (mindestens 80%)
2. Messung	■ Störsignale (0%)

Messung während der Installation (SmartIntego-Manager)

Während der Installation zeigt der SmartIntego-Manager die RSSI-Werte an (Received Signal Strength Indication), die zwischen GatewayNode und LockNode gemessen wurden.



Dieser Wert in dBm (Dezibel Milliwatt) ist:

- Aktuell: Eine Bestandaufnahme des Zustands während der Installation (letztes Paket der Kommunikation zwischen dem SmartIntego-Manager und dem LockNode).
- Logarithmisch: Eine Verbesserung um 10 dBm bedeutet in der Praxis die doppelte Signalstärke.
- Negativ: Der theoretische Bestwert beträgt 0 dBm und wird nur durch Kabelverbindungen erreicht. Je näher der Wert an 0 dBm ist, desto besser ist der Empfang.

Der im SmartIntego-Manager angezeigte Wert sollte für einen Sicheren Betrieb nicht schlechter als -75 dBm sein. Während des normalen Betriebs ändern sich Umgebungsbedingungen und damit die Messwerte. Die angezeigten Werte sind deshalb nur zusammen mit definierten Umgebungsbedingungen gültig. Diese Umgebungsbedingungen müssen miteinbezogen und dokumentiert werden:

- Position der GatewayNodes
- Position der Schließungen (Türen offen oder geschlossen)
- Störeinflüsse (Keine beweglichen Hindernisse zwischen der Schließung und dem GatewayNode)

Messung im normalen Betrieb (QoS-Wert im Integratorsystem)

Nach jeder Kommunikation zwischen GatewayNode und LockNode, bei der ein Paket gesendet und empfangen wurde, wird die Signalqualität als QoS-Wert (Quality of Service) berechnet und an das Integratorsystem gesendet. Dieser Qualitätsindex ist ein Mittelwert aus:

- Erfolgreich empfangenen Paketen
- Erfolgreich gesendeten Paketen
- Anzahl aller Pakete
- Verlorene oder fehlerhafte Pakete
- Nicht empfangene ACKs (interne Antworten im WaveNet)
- Anzahl belegter Kanäle (Kommunikation durch andere Kommunikation blockiert)

Das Integratorsystem kann den empfangenen QoS-Wert anzeigen. Aufgrund der Zusammensetzung und der Mittelwertbildung ist der QoS-Wert ein langfristig ermittelter Wert. Er eignet sich nicht, um kurzfristige Ausschläge der Signalqualität zu erkennen. Kurzfristige Störungen können mit einer WaveNet-Testkarte (siehe Schritt-für-Schritt-Anleitung) oder dem SmartIntego-Manager ermittelt werden.

Verbesserungen der Signalqualität sind erst nach einiger Zeit in den QoS-Werten erkennbar.

Ein PowerOn-Reset an der Schließung löscht auch den QoS-Wert.

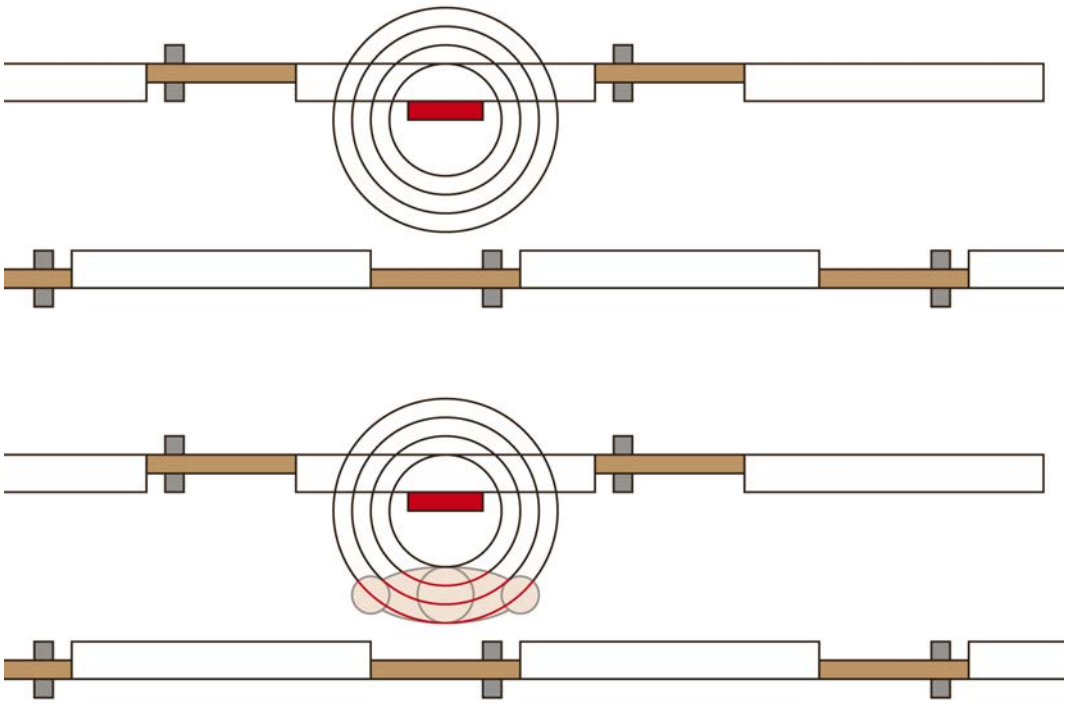
WaveNet-Qualitätsrichtlinien für den Betrieb mit SmartIntego

Die Qualität des WaveNets wird im Vergleich zu anderen SimonsVoss-Produkten für SmartIntego kritischer betrachtet. Das WaveNet ist das Rückgrat einer SmartIntego-Wireless-Online-Anlage, und das Öffnen von Türen hängt zu großen Teilen vom WaveNet und dessen Infrastruktur ab.

Die empfohlenen Grenzwerte enthalten einen Puffer. Grund: Häufig ist der GatewayNode so positioniert, dass er möglichst viele Schließungen ohne Hindernisse erreicht:

- GatewayNode im Gang
- Schließungen mit LockNodes auf den Außenseiten der Türen

Personen, die die Türen öffnen, stehen normalerweise direkt vor den Türen und schirmen somit mit ihrem Körper den LockNode ab. Damit verschlechtert sich die Signalqualität erheblich. Die Verschlechterung der Signalqualität durch das Öffnen der Tür ist beim empfohlenen Grenzwert von -75 dBm berücksichtigt.



7.4 Programmiergerät (SI.SmartCD)

Das SI.SmartCD ist ein lokales USB-Programmiergerät und wird vom SmartIntego-Tool verwendet:

- Programmieren von Schließungen
  - Über WaveNet (SI.SmartCD bleibt am Konfigurations-PC angeschlossen)
  - Direkt
- Notfallöffnungen
- Auslesen von Offline-Zutritten (auch über WaveNet möglich)
- Auslesen von Schließungen (auch über WaveNet möglich)

Das SI.SmartCD benötigt eine direkte physische Verbindung zur Schließung, mit der kommuniziert werden soll. Der Abstand des SI.SmartCD zum Kartenleser der Schließung darf aufgrund der geringen Reichweite (Nahfeld) nur wenige Millimeter betragen.

Während der Programmierung über das WaveNet muss das SI.SmartCD nur an einem freien USB-Anschluss angeschlossen sein, bis die erste Schließung programmiert ist. Danach ist die Konfiguration vollständig im SmartIntego-Tool gespeichert und das SI.SmartCD kann entfernt werden.

Sobald die Kartenkonfiguration jedoch geändert wurde, muss das SI.SmartCD einmalig angeschlossen werden. Nach der Programmierung der ersten Schließung kann es dann wieder entfernt werden.

8. Software

Diese Programme sind erforderlich, um ein SmartIntego-WirelessOnline-System einzurichten:

- SmartIntego-Tool (WirelessOnline WO)
- SmartIntego-Manager (im SmartIntego-Tool WO enthalten)
- Integratorsystem (Beispiel: SmartIntego-Config-Tool)

Zusätzlich hilfreich:

- OAM-Tool
- Firmware-Update-Tool
- SV-QR-Code-Scanner (Chip-IDs)

8.1 SmartIntego-Tool (WO)

Das SmartIntego-Tool (WO) dient zur Verwaltung der SmartIntego-Systemkonfiguration und der Schließungen.

Konfiguriert werden:

- Passwörter
- Kartenkonfigurationen
- Construction Site Whitelist
- Schließungen (Ausstattungsmerkmale und Konfiguraiton)
- WaveNet-Konfiguration (mit dem enthaltenen SmartIntego-Manager)

Diese Daten sind in einer für jedes Schließsystem separaten Projektdatei (*.ikp) gespeichert. Diese Datei ist dementsprechend wichtig und muss nach den folgenden Regeln behandelt werden.

1. Arbeiten Sie nur mit einer einzigen Kopie der Projektdatei.
   ↳ Konfigurationsstatus in der Software und in den Schließungen muss mit dem übereinstimmen, was tatsächlich programmiert ist.
   ↳ Ältere Projektdateien mit einem abweichenden Status sind ein Verwaltungs- und Sicherheitsrisiko!
2. Speichern Sie die Datei in einer gesicherten und gemanagten IT-Umgebung.
3. Erstellen Sie ein Backup der Projektdatei.

Weitere Informationen finden Sie im Schritt-für-Schritt-Handbuch.

Damit es nicht zur Vermischung verschiedener Projekte und Systeme kommt, muss für jedes Kundenprojekt eine eigene Projektdatei mit einem eigenen Passwort erstellt werden.

HINWEIS

Mehrere Projektdateien für ein Integrationsprojekt

Die Verwendung einer eigenen Projektdatei für jeden Hardwarecontroller des Integratorsystems erhöht den Verwaltungsaufwand für den Errichter erheblich.

1. SimonsVoss rät von dieser Art der Verwaltung ab.
2. Stellen Sie ggfs. sicher, dass das Integratorsystem die Verwendung mehrerer Projektdatei unterstützt.

Verlust der Projektdatei (*.ikp)

Wenn die Projektdatei trotz gesicherter Umgebung und Backup verloren geht, dann können Sie nicht mehr mit dem bestehenden Projekt weiterarbeiten.

1. Setzen Sie die Schließungen mit dem Schließanlagenpasswort zurück.
2. Setzen Sie ggfs. die LockNodes mit einem Hardware-Reset zurück.
3. Setzen Sie ggfs. die GatewayNodes mit einem Hardware-Reset zurück.
4. Programmieren Sie anschließend die gesamte Schließanlage neu.

8.2 SmartIntego-Manager

Der SmartIntego-Manager ist im SmartIntego-Tool (WO) enthalten und konfiguriert mit ihm zusammen das WaveNet (GatewayNodes und LockNodes). Der SmartIntego-Manager funktioniert nur zusammen mit dem SmartIntego-Tool (WO).

Folgende Daten werden erzeugt:

- WaveNet-Konfiguration
- GatewayNode-Konfiguration
- LockNode-Konfiguration

Wenn der SmartIntego-Manager beendet wird, dann übergibt er diese Daten an das SmartIntego-Tool (WO). Von dort werden sie in der Projektdatei (*.ikp) gespeichert.

Über | Tools | und SmartIntego-Manager - SmartIntego-Manager wird der SmartIntegoManager geöffnet.

8.3 OAM-Tool

Das OAM-Tool kann:

- IP-Einstellungen eines GatewayNodes verändern
- Konfigurationswebsite eines GatewayNodes öffnen
- HTTPS-Konfigurationswebsite eines GatewayNodes öffnen (erforderlich für AES-Verschlüsselungseinstellungen)

- Firmware eines GN2 aktualisieren

Die nachfolgenden Kapitel beschreiben das Vorgehen detaillierter. Sie sind teilweise für den RouterNode 2 (System 3060) geschrieben. Das Vorgehen für den GatewayNode 2 ist analog.

Um sicheren Betrieb in der IT-Infrastruktur zu gewährleisten, ist es notwendig, dass einige Einstellungen direkt über die Konfigurationswebsite der GatewayNodes vorgenommen werden (siehe *Konfiguration TCP-GatewayNodes [▸ 163]*).

8.4 QR-Code-Scanner (Chip-ID)

Der QR-Code-Scanner ist ein Hilfstool zur Errichtung der Schließanlage. Die gelieferten SimonsVoss-Komponenten müssen vor der Konfiguration den richtigen Türen zugewiesen werden, damit Größe und Eigenschaften passen.

Normalerweise wird der Name der Tür, an der die Schließung verwendet werden soll, auf Basis einer Namenliste auf die Verpackung der Schließung geschrieben. Auf der Verpackung befindet sich außerdem ein Datamatrix-Code, der die Chip-ID enthält. Dieser Code kann mit einem Datamatrix-Code-fähigen Lesegerät gescannt werden (USB). Dieser Schritt verknüpft die Türen und GatewayNodes mit den Chip-IDs (und somit auch mit den LockNodes und Schließungen).

Das genaue Vorgehen ist auch im Schritt-für-Schritt-Handbuch beschrieben.

1. Öffnen Sie die Namenliste (Namen den Türen und GatewayNodes) mit dem SimonsVoss-QR-Code-Scanner.
2. Beschriften Sie die Verpackungen der Schließungen und GatewayNodes mit den Namen aus der Namenliste.
3. Scannen Sie die jeweiligen Datamatrix-Codes auf den Verpackungen.
   ↳ QR-Code-Scanner extrahiert Chip-IDs und speichert sie in der Namenliste.
4. Verfahren Sie ebenso mit den restlichen SmartIntego-Komponenten.
5. Speichern Sie die Namenliste mit den gelesenen Chip-IDs.

↳ Namenliste wird später im SmartIntego-Manager verwendet.

9. Passwörter

Die Schließanlage und die Schließungen sind mit mehreren Passwörtern geschützt. Der Betreiber der Schließanlage ist verantwortlich für die Verwaltung und Verwahrung der Passwörter.

Fahrlässiger Umgang mit Passwörtern kann die Sicherheit der Schließanlage beeinträchtigen und/oder SmartIntego-Komponenten unbrauchbar machen.

Schließungen

Passwort	Schutz
Projektpasswort	Schützt vor unbefugtem Umprogrammieren, Auslesen oder Öffnen
Schließanlagen-passwort	Schützt vor unbefugtem Umprogrammieren, Auslesen oder Öffnen
Leseschlüssel der Karte	■ Entscheidet, ob die Schließung die Karte lesen kann ■ Sicherheitsrelevant für Türöffnung

LockNodes

Passwort	Schutz
Projektpasswort	Schützt Systemaufbau vor unbefugten Änderungen
WaveNet-Pass-wort	Schützt vor versehentlicher oder unbefugter Änderung (Auswirkung z.B. Gerät offline)

GatewayNodes

Passwort	Schutz
Projektpasswort	Schützt Systemaufbau vor unbefugten Änderungen
WaveNet-Pass-wort	Schützt vor versehentlicher oder unbefugter Änderung (Auswirkung z.B. Komponente offline)
GatewayNode-Konfigurations-passwort	Schützt vor unbefugter Änderung der Konfiguration
AES-Verschlüs-selungspasswort	■ Schützt die Kommunikation zwischen GatewayNode und Integratorsystem ■ Authentifizierung des GN am Integratorsystem

Integratorsystem

Passwort	Schutz
AES-Verschlüs-selungspasswort	■ Schützt die Kommunikation zwischen GatewayNode und Integratorsystem ■ Authentifizierung des GN am Integratorsystem

Projektdatei

Passwort	Schutz
Projektpasswort	Schützt vor unbefugtem Öffnen der Datei samt Inhalt

Kartenkonfiguration

Passwort	Schutz
Projektpasswort	Schützt Kartenkonfiguration vor unbefugter Einsicht oder Änderung
Kartenkonfigura-tionspasswort	Schützt Kartenkonfiguration innerhalb der Projektdatei zusätzlich vor unbefugter Einsicht oder Änderung
Leseschlüssel der Karte	Leseschlüssel ist hinterlegt in Kartenkonfiguration der Schließung

9.1 Umgang mit Passwörtern

HINWEIS

Verlust der Passwörter

Ihre Passwörter sind die Grundlage für die Verwaltung Ihrer Schließanlage. Verlorene oder öffentlich bekanntgewordene Passwörter sind ein schwerwiegendes Sicherheitsrisiko und/oder führen zum Kontrollverlust über die Anlage.

1. Notieren Sie sich Ihre Passwörter.
2. Verwahren Sie Ihre Passwörter sicher.

HINWEIS

Sichere Passwörter

Für alle hier beschriebenen Passwörter gelten die allgemein gültigen Regeln im Umgang mit Passwörtern.

1. Verwenden Sie komplexe Passwörter.
2. Verwenden Sie für jedes Projekt bzw. jeden Kunden individuelle Passwörter/Keys.
3. Verwenden Sie keine Passwörter mehrfach (egal ob im Projekt oder projektübergreifend).
4. Schützen Sie Ihre Passwörter vor Verlust und bewahren Sie sie sicher auf.

9.2 Projektpasswort

Das SmartIntego-Tool speichert globale Daten zur Schließanlage wie

- Kartenkonfiguration
- Hardwarekonfiguration
- WaveNet-Topologie
- ...

in einer Projektdatei (*.ikp). Die Projektdatei kann ohne das Projektpasswort nicht geöffnet werden. Somit schützt das Projektpasswort die Projektdaten vor unbefugtem Zugriff.

Änderung/Verlust

- Änderbar im SI-Tool
- Bei Verlust keine Wiederherstellung möglich

9.3 Schließanlagenpasswort

Das SmartIntego-Tool programmiert mithilfe des Schließanlagenpassworts die Konfiguration in die Schließungen. Die Konfiguration kann anschließend nur mit dem Schließanlagenpasswort aus den Schließungen ausgelesen werden. Somit schützt das Schließanlagenpasswort die Konfiguration der Schließungen vor unbefugtem Zugriff.

Das Schließanlagenpasswort wird für jede Programmierung benötigt. Sobald das Schließanlagenpasswort einmal eingegeben wurde, kann es nicht mehr einfach geändert werden.

Die Projektdatei (*.ikp) enthält ebenfalls das Schließanlagenpasswort in verschlüsselter Form.

ACHTUNG

Verlust von Schließanlagenpasswort und Projektdatei

Wenn Sie sowohl das Schließanlagenpasswort als auch die Projektdatei verlieren, dann können Komponenten nicht mehr zurückgesetzt oder konfiguriert werden, auch nicht von SimonsVoss. Die Komponenten sind dann unbrauchbar!

1. Notieren Sie sich Ihre Passwörter.
2. Verwahren Sie Ihre Passwörter sicher.
3. Erstellen Sie Backups Ihrer Projektdatei.

HINWEIS

Verlust der Passwörter

Ihre Passwörter sind die Grundlage für die Verwaltung Ihrer Schließanlage. Verlorene oder öffentlich bekanntgewordene Passwörter sind ein schwerwiegendes Sicherheitsrisiko und/oder führen zum Kontrollverlust über die Anlage.

1. Notieren Sie sich Ihre Passwörter.
2. Verwahren Sie Ihre Passwörter sicher.

Änderung/Verlust

1. Anlage zurücksetzen (Schließung und WaveNet).
2. Neue Projektdatei erstellen.
3. Anlage mit neuem Passwort aufbauen (Schließung und WaveNet).

- Bei Verlust kann mit der Projektdatei gearbeitet (zurückgesetzt) werden
- Wiederherstellung nicht möglich

Bei Verlust der Projektdatei und des Schließanlagenpassworts muss die Schließungshardware ausgetauscht werden.

9.4 WaveNet-Passwort

Die Netzwerkkonfiguration ist auf allen SmartIntego-WirelessOnline-Komponenten gespeichert. Unabhängig vom Zugriff auf die Schließungskonfiguration schützt das WaveNet-Passwort die Netzwerkkonfiguration vor unberechtigtem Zugriff.

Der SmartIntego-Manager fordert beim ersten Start dazu auf, ein WaveNet-Passwort zu vergeben. Während der Konfiguration der WaveNet-Komponenten speichert der SmartIntego-Manager das WaveNet-Passwort auf den SmartIntego-WirelessOnline-Komponenten.

Um das WaveNet-Passwort zu ändern, müssen erst alle Komponenten mit der Konfiguration aus der Projektdatei zurückgesetzt werden.

Änderung/Verlust

1. Anlage zurücksetzen (Schließung und WaveNet).
2. Neue Projektdatei erstellen.
3. Anlage mit neuem Passwort aufbauen (Schließung und WaveNet).

- Bei Verlust kann mit der Projektdatei gearbeitet (zurückgesetzt) werden

9.5 Kartenkonfigurationspasswort

Die Schließungen benötigen die Kartenkonfiguration, um die Karten lesen zu können. Die Kartenkonfiguration ist in der Projektdatei (*.ikp) gespeichert.

Die Kartenkonfiguration kann optional zusätzlich innerhalb der Projektdatei mit dem Kartenkonfigurationspasswort vor versehentlichen Änderungen geschützt werden.

Das Kartenkonfigurationspasswort kann mit dem SmartIntego-Tool geändert werden.

Änderung/Verlust

- Änderbar im SI-Tool

9.6 Leseschlüssel der Kartendaten

Abhängig von den auszulesenden Kartendaten kann es notwendig sein, den Leseschlüssel der Kartendaten zu speichern (DESFire: Leseschlüssel der Applikation/Datei bzw. Classic: Leseschlüssel des Sektors). Der Leseschlüssel ist Teil der Kartenkonfiguration und wird zusammen mit dieser in der Projektdatei (*.ikp) und in den Schließungen gespeichert.

Der Leseschlüssel wird von den Schließungen verwendet, um nur den relevanten Teil des Speicherplatzes der Karte auszulesen.

Der Kartenhersteller oder andere Nutzer der Karte stellen den Leseschlüssel der Karte zur Verfügung, beispielsweise als Template-Datei (*.ikt) oder direkt im Klartext. Informationen finden Sie im Schritt-für-Schritt-Handbuch.

Änderung/Verlust

- Änderbar im SI-Tool
- Alle Schließungen und Karten müssen umprogrammiert werden

9.7 Passwort für GatewayNode-Konfigurationswebsite

Der TCP-GatewayNode ist eine IT-Komponente. Die TCP-Konfiguration wird auf der Konfigurationswebsite des GatewayNodes eingegeben. Die Konfigurationswebsite kann nur mit einem Passwort aufgerufen werden.

Sie erhalten das Gerät mit folgender werkseitiger Konfiguration:

IP-Adresse	192.168.100.100 (falls kein DHCP-Server gefunden wird)
Subnetz-Maske	255.255.0.0
Benutzername	SimonsVoss
Passwort	SimonsVoss

ACHTUNG

Zugang über Standardpasswort

Über die werksseitig eingestellten Zugangsdaten können andere Personen auf das Produkt zugreifen.

Einige Browser übertragen keine Leerzeichen, die am Anfang des Passworts stehen.

1. Ändern Sie das Standardpasswort.
2. Beginnen Sie das Passwort nicht mit Leerzeichen.

HINWEIS

Verlust der Passwörter

Ihre Passwörter sind die Grundlage für die Verwaltung Ihrer Schließanlage. Verlorene oder öffentlich bekanntgewordene Passwörter sind ein schwerwiegendes Sicherheitsrisiko und/oder führen zum Kontrollverlust über die Anlage.

1. Notieren Sie sich Ihre Passwörter.
2. Verwahren Sie Ihre Passwörter sicher.

Änderung/Verlust

- Änderbar auf der GatewayNode-Konfigurationswebsite
- Bei Verlust kann der GatewayNode zurückgesetzt werden

9.8 AES-Verschlüsselungspasswort

Das Integratorsystem ist normalerweise mit den GatwayNodes verbunden. Der Datenverkehr über diese Verbindung sollte mithilfe des geheimen AES-Passworts verschlüsselt sein (siehe auch Beschreibung des Integratorsystems).

Dieses Passwort wird über die HTTPS-Konfigurationswebsite auf den GatewayNodes gespeichert und auch im Integratorsystem selbst.

Das AES-Verschlüsselungspasswort kann über die HTTPS-Konfigurationswebsite eingesehen und geändert werden.

Änderung/Verlust

- Änderbar auf der GatewayNode-Konfigurationswebsite und im Integratorsystem
- Bei Verlust kann der GatewayNode zurückgesetzt werden

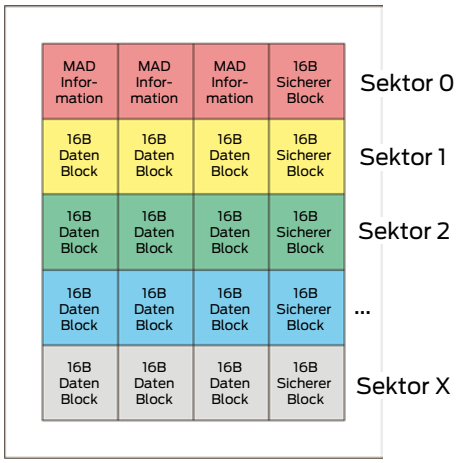
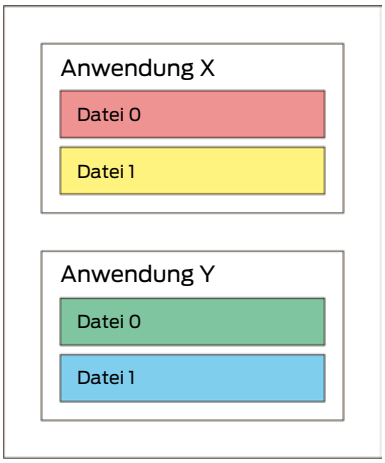
10. Karten

10.1 Kartentypen (WirelessOnline)

- Frequenzbereich: 13,56 MHz (RFID)
- Lesetechnologien:
  - ISO 14443-A
  - ISO 14443-B

Datentypen	
Unique ID Kartenseriennummer (CSN)	ID der Karte als Datensatz
MIFARE Ultralight MIFARE Classic (1K/4K/Mini) MIFARE DESFire Legic advant (ISO 14443)	MIFARE Classic (Sektoren oder Mifare Application Directory=MAD) MIFARE DESFire (Application)
Keine Vorabprogrammierung der Karte notwendig Unsicher (Skimmen und Duplizieren möglich) Keine parallele Verwendung mit Daten auf der Karte im gleichen System	Vorabprogrammierung der Karte notwendig Sicher Bis zu fünf Setups in einem System möglich

MIFARE Classic	MIFARE DESFire
Daten in Sektoren gespeichert Adressierung direkt mit Sektoren oder Mifare Application Directory (=MAD) Sektorschutz über Key im MAD MIFARE-Classic-Verschlüsselung gehackt und inzwischen unsicher	Daten in Dateien gespeichert Adressierung mit Application ID und File ID Datei durch Leseschlüssel der Datei gesichert Karten-ID muss in einer Datei einer Applikation gespeichert sein, Lesezugriff auf die Datei ist notwendig Verschlüsselung mit AES

MIFARE Classic	MIFARE DESFire
Aufteilung des Speichers: 	Aufteilung des Speichers: 

10.2 Karteneinstellungen

SmartIntego WirelessOnline kann verschiedene Karten lesen.

Mindestanforderungen für die Verwendung einer Karte:

Frequenz	13,56 MHz (RFID)
Unterstützte Lesetechnologien	ISO 14443-A ISO 14443-B
Unique Identifier/Kartenseriennummer	Statisch

10.2.1 UID-Modus (Unique Identifier)

Die Karte wird in diesem Modus nur anhand des ausgelesenen Unique Identifiers bzw. der Kartenseriennummer identifiziert.

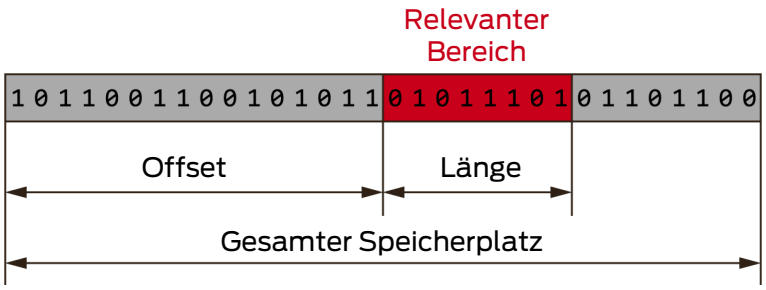
Weder der Unique Identifier noch die Kartenseriennummer sind in irgendeiner Art und Weise geschützt. Angreifer können die Karte mitsamt Unique Identifier und Kartenseriennumnmer identifizieren.

Frequenz	13,56 MHz (RFID)
Unterstützte Lesetechnologien	ISO 14443-A ISO 14443-B
Unique Identifier/Kartenseriennummer	Statisch

Unterstützte Kartentypen	■ MIFARE Classic ■ MIFARE DESFire ■ Legic advant (ISO 14443) ■ HID iCLASS SEOS UID (ISO 14443)

Im Bereich "Custom portion" stellen Sie ein, welche zusammenhängenden Bytes der Identifikationsnummer von der Schließung ausgelesen werden sollen. Im Normalfall wird die gesamte Identifikationsnummer ausgewertet, Einschränkungen gibt der Kartenhersteller oder der Integrator vor.

Offset Online Connection (Bytes)	Length Online Connection (Bytes)	Offset Whitelist (Bytes)	Length Whitelist (Bytes)
■ Gibt an, ab welchem Byte die Identifikationsnummer gelesen wird. ■ Nutzung für Online-Zutritt	■ Gibt an, wieviele Bytes der Identifikationsnummer gelesen werden. ■ Nutzung für Online-Zutritt	■ Gibt an, ab welchem Byte die Identifikationsnummer gelesen wird. ■ Nutzung für Whitelist-Zutritt	■ Gibt an, wieviele Bytes der Identifikationsnummer gelesen werden. ■ Nutzung für Whitelist-Zutritt



Die genauen Parameter finden Sie in der Dokumentation Ihres Integratorsystems.

Die Identifikation mit einer Random ID (RID) ist nicht möglich.

10.2.2 Passwortgeschützter Datenbereich

Wenn ein Datensatz auf der Karte verwendet wird (mit UID der Karte oder einer anderen eindeutigen ID), dann hat jede Karte im System eine eigene Identifikation. Diese Identifikation ist in einem passwortgeschützten Bereich der Karte gespeichert.

Die Zugriffsrechte auf diesen Bereich der Karte ist Teil der Kartenkonfiguration und auf den SmartIntego-Schließungen gespeichert. Nach dem Vorhalten einer solchen Karte liest die Schließung nur diesen Bereich aus.

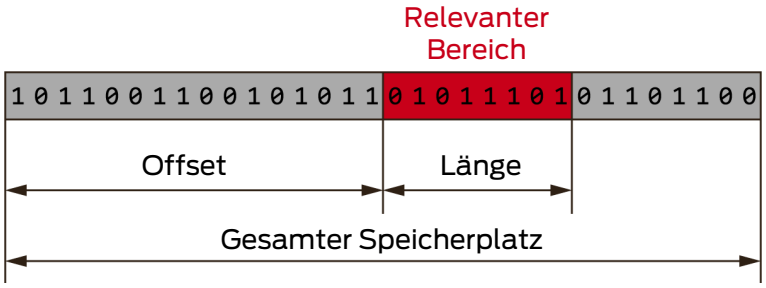
Frequenz	13,56 MHz (RFID)
Unterstützte Lesetechnologien	ISO 14443-A
Unique Identifier/Kartenseriennummer	Statisch oder zufällig
Unterstützte Kartentypen inklusive Konfigurationseinstellungen	■ MIFARE Classic: IsMad (0 oder 1) KeyType (KEY A oder KEY B) Key MadAid SectorList ■ MIFARE DESFire: AppID (dezimal) Communication Mode (Encrypted, plain oder mac) CryptoMode (AES, 3DES - 3DES nicht AX-kompatibel, ggfs. vorher zu AES konvertieren) File No. ReadKey No. ReadKey (hexadezimal)

Bis zu fünf solcher Kartenkonfigurationen können gleichzeitig in einer Schließanlage verwendet werden. Alle Kartenkonfigurationen sind global gültig: Alle Schließungen der Schließanlage verwenden dieselben Kartenkonfigurationen.

Für jede Kartenkonfiguration muss angegeben werden, wo sich die für die jeweilige Kartenkonfiguration relevanten Daten auf der Karte befinden.

Die Schließung soll nicht den ganzen Datensatz der Karte auslesen. Sie benötigt nur eine Nummer (max. 32 Byte), die die Karte eindeutig identifiziert. Im Bereich "Location of the data (e.g. card ID)" stellen Sie ein, welche zusammenhängenden Daten von der Schließung ausgelesen werden sollen.

Offset Online Connection (Bytes)	Length Online Connection (Bytes)	Offset Whitelist (Bytes)	Length Whitelist (Bytes)
▪ Gibt an, ab welchem Byte die Daten gelesen werden. ▪ Nutzung für Online-Zutritt	▪ Gibt an, wieviele Bytes der Daten gelesen werden. ▪ Nutzung für Online-Zutritt	▪ Gibt an, ab welchem Byte die Daten gelesen werden. ▪ Nutzung für Whitelist-Zutritt	▪ Gibt an, wieviele Bytes der Daten gelesen werden. ▪ Nutzung für Whitelist-Zutritt



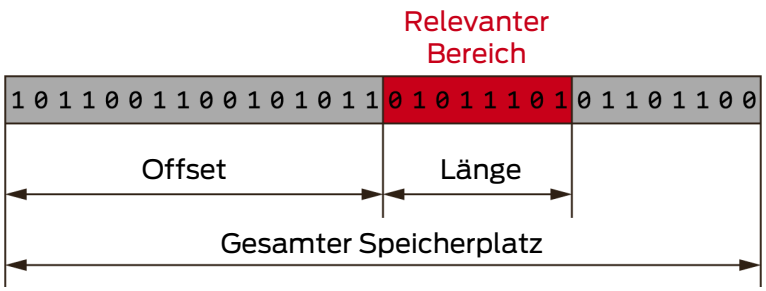
Die genauen Parameter finden Sie in der Dokumentation Ihres Integratorsystems.

10.2.3 Calypso-Karten mit Seriennummer

Die Calypso-Seriennummer ist eine Anwendungs-ID für eine 1TIC.ICA-Anwendung.

Das System ist so voreingestellt, dass es die gesamte Seriennummer einer Calypso-Karte mit einer Länge von 8 Byte ausliest und verarbeitet.

Manche Integratorsysteme können nicht die ganze Länge von 8 Byte verarbeiten. In diesem Fall bietet das SmartIntego-Tool im Bereich "Custom portion" an, einen Offset und die Länge des relevanten Bereichs anzugeben. Dann kann die volle Länge von 8 Byte auf beispielsweise ein Byte gekürzt werden.



Die genauen Parameter finden Sie in der Dokumentation Ihres Integratorsystems.

10.2.4 ISO7816-4-Karten

- Dateityp nach ISO 7816-4: Elementar
- Kartentyp: ISO 14443-A oder ISO 14443-B
- ReadCmd
- SelectCmd

Die Seriennummer einer Karte nach ISO 7816-4 wird mit einem entsprechenden Lesebefehl (ReadCmd) und Auswahlbefehl (SelectCmd) ausgelesen. Anschließend kann die Seriennummer verarbeitet werden.

Diese Befehle müssen nach der folgenden Struktur formatiert sein (Application Protocol Data Unit (= APDU) der ISO 7816-4):

	APDU-Header (obligatorisch)				APDU-Body (optional)		
Case 1	CLA	INS	P1	P2			
Case 2	CLA	INS	P1	P2	Le		
Case 3	CLA	INS	P1	P2	Lc	Data	
Case 4	CLA	INS	P1	P2	Lc	Data	Le

Die genauen Parameter finden Sie in der Dokumentation Ihres Integratorsystems.

10.2.5 Return-Timeout nach Lesevorgang

Nach einem Karten-Event wartet die Schließung eine begrenzte Zeit auf eine Antwort des Integratorsystems. Diese Zeitspanne ist der Return-Timeout.

Eine Antwort des Integratorsystems (z.B. ein Öffnungsbefehl) wird nur innerhalb dieser Zeitspanne angenommen und ausgeführt (Online-Zutritt). Falls die Antwort zu spät oder gar nicht kommt, greift die Schließung nach Ablauf des Return-Timeouts auf die lokal gespeicherte Whitelist zurück. Karten auf dieser Whitelist kuppeln die Schließung dann ein (Offline-Zutritt), alle anderen Karten werden abgewiesen.

Der Nutzer hat in diesem Fall zwei Möglichkeiten:

- Karte entweder erneut präsentieren (Neuer Versuch)
- Karte verwenden, die auf der Whitelist enthalten ist

Der Return-Timeout ist eine globale Einstellung für alle Schließungen.

11. Changelog

Versions	Changes	Chapter
01.00	FIRST RELEASE	...
01.01	Preparation AX	*SmartHandle AX [▸ 109]*
01.02	Several preparation for AX	Documents
01.03	Bugfix AP2+FD Cylinder	*Schließzylinder (TN4) [▸ 100]*
	Adjustments regarding support for AX components	Documents
01.04	Internal bugfixing	Documents
01.05	Support SI Digital Cylinder AX	*Digital Cylinder AX [▸ 28]*

12. Hilfe und weitere Informationen

Infomaterial/Dokumente

Detaillierte Informationen zum Betrieb und zur Konfiguration sowie weitere Dokumente finden Sie auf der Homepage:

https://www.smartintego.com/de/home/infocenter/dokumentation

Software und Treiber

Software und Treiber finden Sie auf der Website:

https://www.simons-voss.com/de/service/software-downloads.html

Konformitätserklärungen und Zertifikate

Konformitätserklärungen und Zertifikate finden Sie auf der Homepage:

https://www.simons-voss.com/de/zertifikate.html

Technischer Support

Unser technischer Support hilft Ihnen gerne weiter (Festnetz, Kosten abhängig vom Anbieter):

+49 (0) 89 / 99 228 333

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

si-support-simonsvoss@allegion.com

FAQ

Informationen und Hilfestellungen finden Sie im FAQ-Bereich:

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

Adresse

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Deutschland

Das ist SimonsVoss

SimonsVoss, der Pionier funkgesteuerter, kabelloser Schließtechnik, bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, kleine und große Unternehmen sowie öffentliche Einrichtungen. SimonsVoss-Schließsysteme verbinden intelligente Funktionalität, hohe Qualität und preisgekröntes Design Made in Germany.

Als innovativer Systemanbieter legt SimonsVoss Wert auf skalierbare Systeme, hohe Sicherheit, zuverlässige Komponenten, leistungsstarke Software und einfache Bedienung. Damit wird SimonsVoss als ein Technologieführer bei digitalen Schließsystemen angesehen.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs.

SimonsVoss ist ein Unternehmen der ALLEGION Group – ein global agierendes Netzwerk im Bereich Sicherheit. Allegion ist in rund 130 Ländern weltweit vertreten (www.allegion.com).

Made in Germany

Für SimonsVoss ist „Made in Germany“ ein ernsthaftes Bekenntnis: Alle Produkte werden ausschließlich in Deutschland entwickelt und produziert.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION